En ny kamerabevakningslag

Betänkande av Utredningen om kameraövervakning – brottsbekämpning och integritetsskydd

Stockholm 2017

STATENS OFFENTLIGA UTREDNINGAR

SOU 2017:55

SOU och Ds kan köpas från Wolters Kluwers kundservice.
Beställningsadress: Wolters Kluwers kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@wolterskluwer.se
Webbplats: wolterskluwer.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Wolters Kluwer Sverige AB
på uppdrag av Regeringskanslietsförvaltningsavdelning.
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck: Elanders Sverige AB, Stockholm 2017

ISBN 978-91-38-24633-7
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Den 26 november 2015 bemyndigade regeringen statsrådet och chefen för Justitiedepartementet Morgan Johansson att ge en särskild utredare i uppdrag att utreda vissa frågor om kameraövervakning. Regeringen beslutade samtidigt om direktiv för utredningen (dir. 2015:125). Den 16 juni 2016 beslutade regeringen om tilläggsdirektiv (dir. 2016:54). Genom dessa vidgades uppdraget till att avse en analys av hur regleringen i kameraövervakningslagen (2013:460) borde anpassas till ny EU-rättslig dataskyddsreglering. Samtidigt förlängdes utredningstiden.

Biträdande tillsynschefen vid Åklagarmyndigheten Susanne Kaevergaard förordnades som särskild utredare från och med den 26 november 2015.

Som experter att biträda utredaren förordnades den 1 januari 2016 advokaten Jan-Mikael Bexhed, juristen Martin Hemberg, Datainspektionen, juristen Karin Höglund, Polismyndigheten, utredaren Johanna Kindgren, Brottsförebyggande rådet, juristen Maria Leijon, Länsstyrelsen Norrbotten, och rättssakkunnige Mattias Råbe, Justitiedepartementet. Den 21 januari 2016 förordnades som expert rådmannen tillika enhetschefen Ronny Idstrand, Förvaltningsrätten i Linköping. Den 1 juni 2016 entledigades Karin Höglund och samma dag förordnades som expert juristen Sara Markstedt, Polismyndigheten. Den 9 januari 2017 entledigades Mattias Råbe och samma dag förordnades som expert rättssakkunniga Ia Hamlin, Justitiedepartementet.

Den 1 januari 2016 anställdes rättssakkunnige Johan Stensbäck som sekreterare i utredningen. Den 12 september 2016 anställdes hovrättsassessorn Fredrik Lövkvist som sekreterare i utredningen och den 1 oktober 2016 entledigades Johan Stensbäck.

Härmed överlämnas betänkandet *En ny kamerabevakningslag*, SOU 2017:55. Till betänkandet har fogats två särskilda yttranden, ett av experten Sara Marklund och ett av experten Ronny Idstrand. Med undantag av vad som framgår där har experterna ställt sig bakom utredningens bedömningar och förslag.

Utredningens uppdrag är med detta slutfört.

Stockholm i juni 2017

Susanne Kaevergaard

/ Fredrik Lövkvist

Innehåll

Bilagor

Sammanfattning

Uppdraget

Utredningens uppdrag har varit att utreda vissa frågor om kameraövervakning enligt kameraövervakningslagen (2013:460). I uppdraget har även ingått att göra en analys av hur kameraövervakningslagen behöver anpassas till EU:s nya reglering om behandling av personuppgifter. EU-regleringen består av en förordning och ett direktiv. Direktivet gäller för personuppgiftsbehandling hos vissa myndigheter och andra för syften som avser bl.a. brottsbekämpning, lagföring och straffverkställighet medan förordningen omfattar annan personuppgiftsbehandling hos myndigheter och andra. Kameraövervakning utgör många gånger personuppgiftsbehandling och träffas därför av EU-regleringen. I direktiven till utredningen har det angetts att en strävan bör vara att behålla huvuddragen i den nuvarande lagen.

Kameraövervakningslagen tar sikte på viss kameraanvändning i samhället som sker öppet. Enligt lagen gäller som huvudregel ett krav på tillstånd för att kameraövervakning ska få ske av platser dit allmänheten har tillträde. Vidare finns ett krav på att det ska upplysas om kameraövervakning både vad gäller platser dit allmänheten har tillträde och vad gäller andra platser. Lagen reglerar inte s.k. hemlig kameraövervakning, som omfattas av annan lagstiftning.

I uppdraget har ingått att undersöka hur lagens tillämpningsområde förhåller sig till användning av ny teknik, såsom kamerautrustade drönare. Vad gäller brottsbekämpning har uppdraget varit att överväga om möjligheterna till kameraövervakning på särskilt brottsutsatta platser behöver förbättras, att analysera om andra relevanta aktörer än brottsbekämpande myndigheter har ändamålsenliga möjligheter till sådan övervakning och att bedöma om det finns tillräckliga möjligheter att ta hänsyn till hotbilder av mer gene-

rellt slag vid tillståndsprövningen enligt lagen. Uppdraget har dessutom innefattat bl.a. en analys av om integritetsskyddet på arbetsplatser behöver förbättras.

I utredningsuppdraget har inte ingått att överväga att avskaffa eller genomgripande förändra den särskilda lagstiftningen på kameraövervakningsområdet. Uppdraget har alltså inte omfattat att helt slopa det krav på tillstånd till kamerabevakning som gäller i dag eller att ta bort eller avsevärt begränsa den skyldighet att upplysa om kameraövervakning som finns i dag. I uppdraget har inte heller ingått att helt undanta vissa rättssubjekt från lagstiftningens tillämpningsområde eller från tillståndskravet och upplysningskravet. Det har vidare inte ingått i uppdraget att överväga utvidgningar i annan lagstiftning som reglerar kameraanvändning, t.ex. att föreslå ökade möjligheter för polisen att bedriva hemlig kameraövervakning enligt rättegångsbalken eller lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

Med anledning av den nya EU-regleringen har det ändå övervägts varför en fortsatt särskild svensk lagstiftning på kameraövervakningsområdet är motiverad och prövats vilka svenska bestämmelser som är tillåtna enligt EU-regleringen och huruvida dessa bestämmelser också är påkallade av principiella och praktiska skäl. Övervägandena har gjorts i ljuset av det beskrivna innehållet i uppdraget.

Uppdraget har genomförts med beaktande av det arbete som utförts av två andra utredningar, vilka haft i uppdrag att föreslå de nya generella svenska författningar som förordningen och direktivet kräver. De utredningarna har föreslagit en lag som kompletterar förordningen, dataskyddslagen, och föreskrifter till denna respektive en lag som genomför direktivet, brottsdatalagen, och föreskrifter till denna. Vidare har kontakter skett även med andra utredningar, som på olika områden överväger vilka förändringar som EU-regleringen och de nya generella författningarna ger anledning till. Dessutom har ett flertal möten ägt rum med myndigheter och andra som berörs av de frågor som uppdraget omfattat.

En ny kamerabevakningslag

I betänkandet föreslås att kameraövervakningslagen ska ersättas av en ny lag, som ska heta kamerabevakningslagen. Lagen ska träda i kraft den 25 maj 2018.

Skälen för att en helt ny lag föreslås är följande. Den nya EU-förordningen kommer att gälla direkt i Sverige, vilket innebär att bestämmelser om kameraövervakning som upprepar eller avviker från innehållet i förordningen inte kan behållas i svensk lagstiftning annat än om förordningen lämnar utrymme för det. Många av kameraövervakningslagens bestämmelser kan inte behållas alls eller kan inte behållas i sin nuvarande form när det gäller kameraövervakning som omfattas av förordningen. Vad gäller det nya EU-direktivet ska detta genomföras i svensk rätt. Svenska bestämmelser som omfattar kameraövervakning som träffas av direktivet måste uppfylla direktivets krav. Kraven uppfylls dock endast delvis av kameraövervakningslagens bestämmelser. Vidare har en utvärdering av kameraövervakningslagen som utredningen gjort visat att det finns vissa tillämpningssvårigheter med lagen. Sammantaget innebär detta att det krävs en stor reform av den svenska lagstiftningen på området för kameraövervakning.

Som utgångspunkter för kamerabevakningslagen har slagits fast att den – jämfört med kameraövervakningslagen – bör ge ökade möjligheter till kamerabevakning både för brottsbekämpande ändamål och för andra berättigade ändamål, t.ex. ändamål som avser kamerabevakning inom jordbruk och skogsbruk samt annan näringsverksamhet, och samtidigt ge ett förstärkt skydd för den personliga integriteten vid kamerabevakning, bl.a. på arbetsplatser.

Kamerabevakningslagens syfte ska vara att tillgodose behovet av kamerabevakning för berättigade ändamål och att skydda enskilda mot otillbörliga intrång i den personliga integriteten vid sådan bevakning.

Lagen ska endast innehålla de bestämmelser som särskilt behövs för kamerabevakning till skillnad mot annan behandling av personuppgifter som omfattas av EU-regleringen.

I frågor som inte regleras i lagen ska gälla antingen förordningen och dataskyddslagen med föreskrifter eller brottsdatalagen med föreskrifter beroende på om kamerabevakningen i det enskilda fallet

omfattas av förordningen eller dataskyddslagen eller av brottsdatalagen.

Kamerabevakningslagen ska ha ett förhållandevis brett tillämpningsområde. Med kamerabevakning ska förstås att kameror eller därmed jämförbara utrustningar, utan att manövreras på platsen, används varaktigt eller regelbundet upprepat för personbevakning. Med personbevakning menas att människor kan identifieras genom bevakningen. Så är t.ex. fallet om hela personen eller personens ansikte syns tydligt. Om en människa endast av en tillfällighet kan hamna i en kameras blickfång, är det inte fråga om personbevakning. Även separata tekniska anordningar för avlyssning eller upptagning av ljud, som används för personbevakning, ska omfattas av begreppet kamerabevakning. Dessutom ska användning av separata tekniska anordningar för att behandla upptaget bild- och ljudmaterial omfattas.

Exempel på kameraanvändning som i regel inte ska träffas av lagen är användning av handhållna kameror och kameror som på annat sätt bärs på kroppen. Lagen ska inte heller omfatta t.ex. en kamera som är placerad på vindrutan i en bil eller monterad på ett cykelstyre när användaren av kameran är i kamerans omedelbara närhet och fortlöpande styr över denna. Däremot ska lagen omfatta kameror på drönare och på eller i bussar, tågvagnar och liknande objekt förutsatt att kamerorna inte manövreras på platsen. Lagen ska också omfatta kameror som är placerade på eller inuti byggnader, på stolpar och på liknande geografiskt bestämda platser.

Lagen ska endast gälla om de kameror eller separata ljudanordningar som används finns i Sverige och den som bedriver bevakningen är etablerad här eller i tredjeland. Vad gäller separata anordningar för att behandla material från sådan bevakning ska lagen gälla så länge behandlingen utförs av samma person som tagit upp materialet eller för dennes räkning.

Från lagen ska undantas kamerabevakning som en fysisk person utför som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll. Vidare ska hemlig kameraövervakning undantas. Dessutom ska undantag göras för kamerabevakning som sker i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen och kamerabevakning som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

Sådan kameraanvändning som faller utanför lagens tillämpningsområde kan i stället omfattas av andra bestämmelser, främst bestämmelserna i förordningen och dataskyddslagen eller bestämmelserna i brottsdatalagen.

Ett upplysningskrav

I lagen ska – i likhet med kameraövervakningslagen – finnas ett krav på att det ska lämnas upplysning om kamerabevakning. Upplysningskravet ska gälla oavsett vem som bedriver kamerabevakningen och oavsett om bevakningen avser en plats dit allmänheten har tillträde eller en annan plats. Kravet ska delvis vara strängare än tidigare. Den som bedriver kamerabevakning ska genom tydlig skyltning eller på något annat liknande verksamt sätt lämna upplysning om bevakningen, sin identitet och sina kontaktuppgifter och kontaktuppgifter till ett eventuellt dataskyddsombud. Om ljud kan avlyssnas eller tas upp vid bevakningen, ska en särskild upplysning lämnas om detta. Dessutom ska viss ytterligare information göras tillgänglig, t.ex. via en webbsida. Det gäller bl.a. information om ändamålet med kamerabevakningen och möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifterna till den myndigheten.

Från upplysningskravet ska gälla vissa undantag. Några av dessa har gällt även enligt den tidigare lagen och några är nya. De nya undantagen avser kamerabevakning som bedrivs i brådskande fall från ett luftfartyg, t.ex. en drönare. Det ena undantaget gäller när sådan bevakning bedrivs av Polismyndigheten eller Säkerhetspolisen i ett fall där det av särskild anledning finns risk för viss allvarlig brottslighet och syftet med bevakningen är att förebygga, förhindra, upptäcka, utreda eller lagföra denna. Det andra undantaget gäller när bevakning bedrivs av Polismyndigheten eller den som är räddningsledare enligt lagen (2003:778) om skydd mot olyckor i ett fall där bevakningen är av vikt för att avvärja en hotande olycka eller begränsa verkningarna av en inträffad olycka.

I enskilda fall ska dessutom tillsynsmyndigheten kunna besluta om undantag från upplysningskravet, om det finns synnerliga skäl för det. Ett sådant beslut ska kunna ändras eller återkallas vid ändrade förhållanden.

Ökade möjligheter till kamerabevakning – ett begränsat tillståndskrav

Kamerabevakningslagen ska – till skillnad mot kameraövervakningslagen – inte innehålla något generellt krav på tillstånd för att kamerabevakning ska få ske. Inte heller ska lagen innehålla något krav på anmälan som motsvarar den gamla lagens anmälningsskyldighet. Däremot ska den nya lagen innehålla ett begränsat tillståndskrav.

Eftersom en utgångspunkt för lagen är att den bör ge ökade möjligheter till kamerabevakning, finns det redan av den anledningen skäl att ifrågasätta om det är motiverat att behålla ett allmänt krav på tillstånd. Vidare innebär EU-regleringen att det inte längre är möjligt att upprätthålla en generell tillståndsplikt för sådan kamerabevakning som omfattas av förordningen. Förordningen tillåter endast krav på tillstånd i vissa fall. För kamerabevakning som träffas av direktivet kan däremot ett generellt sådant krav gälla.

Genom att slopa dagens generella tillståndskrav och anmälningsskyldighet kommer kamerabevakning i många verksamheter framöver att bli tillstånds- och anmälningsfri. Därmed kan möjligheterna att bedriva kamerabevakning i dessa verksamheter öka. Även om andra bestämmelser ska gälla för sådan kamerabevakning kan det förutses att den svenska tillsynsmyndigheten på området, liksom svenska domstolar och ytterst EU-domstolen, kommer att ha en mer generös syn på utrymmet för kamerabevakning än vad som hittills gällt enligt svensk rätt. Rättsläget är helt nytt med den nya EU-regleringen. Den skiljer sig i olika delar från den unionsrättsliga reglering som fram till nu har gällt på området och legat till grund för dagens kameraövervakningslag. Exempelvis kan fler berättigade ändamål åberopas enligt den nya regleringen för att kamerabevakning ska få ske.

Även det tillståndskrav som kamerabevakningslagen ska innehålla därför att principiella och praktiska skäl motiverar det kan förenas med ökade möjligheter till kamerabevakning. Tillståndsförfarandet innebär en prövning enligt vissa i lagen på förhand givna kriterier, som är särskilt anpassade för de behov och de integritetsaspekter som gör sig gällande just på kamerabevakningsområdet. Kriterierna kan främja att prövningen blir förutsebar och enhetlig samt att tillstånd beviljas i en större omfattning än vad som varit fallet enligt kameraövervakningslagen i motsvarande situationer.

Tillsynsmyndighetens beslut i en sådan fråga ska kunna överklagas till domstol. När ett tillstånd har meddelats kan tillståndshavaren inrätta sig efter detta.

Utan ett tillståndsförfarande skulle mer allmänna bestämmelser i förordningen eller de generella svenska författningarna gälla. Det skulle innebära att den som vill bedriva kamerabevakning ska göra en konsekvensbedömning av den planerade bevakningen i vissa fall och eventuellt samråda med tillsynsmyndigheten, som kan ingripa mot – t.ex. förbjuda – denna. I så fall finns det en risk för att rättsläget kommer att vara osäkert under en längre tid vad gäller sådana verksamheter som tillståndskravet annars kan avse. Det finns också en risk för att rättspraxis inte utvecklas på ett sätt som säkerställer att kamerabevakning kan användas i dessa verksamheter i situationer där sådan bevakning måste anses behövlig.

För kamerabevakning som ska omfattas av tillståndskravet ska den nya lagen ge ökade möjligheter att få tillstånd dels genom att de intressen av kamerabevakning som ska tillmätas betydelse vid tillståndsprövningen utökas jämfört med den gamla lagen, dels genom att undantagen från tillståndskravet vidgas något jämfört med den lagen.

Tillståndskravet ska gälla endast för vissa subjekt och för platser dit allmänheten har tillträde. Kravet ska gälla för myndigheter, både statliga och kommunala. Det ska också gälla för andra juridiska personer eller fysiska personer när de utför en uppgift som följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning, om uppgiften avser brottsbekämpning, lagföring, straffverkställighet, upprätthållande av allmän ordning och säkerhet eller nationell säkerhet eller om uppgiften annars är av allmänt intresse.

Kravet på tillstånd till kamerabevakning ska alltså träffa samtliga myndigheter, i den mån viss bevakning som dessa bedriver inte är undantagen från kravet, och dessutom privaträttsliga subjekt som driver exempelvis skolverksamhet, kollektivtrafik, hälso- och sjukvård och förläggningar för asylsökande.

Tillståndskravet ska däremot inte gälla t.ex. privaträttsliga subjekts kamerabevakning i butikslokaler, av medieredaktioner, av lokaler som används av religiösa samfund och av idrottsarenor. Inte heller ska det omfatta exempelvis kamerabevakning inom jordbruk och

skogsbruk eller av vilt, t.ex. vid åtlar. I dessa fall ska inte heller gälla någon anmälningsskyldighet.

Från kravet på tillstånd ska gälla vissa undantag som i huvudsak motsvarar undantagen från tillståndsplikten enligt kameraövervakningslagen. Några av den lagens undantag ska vidgas. Exempelvis undantas kamerabevakning som bedrivs under högst en månads tid av Polismyndigheten eller Säkerhetspolisen när det av särskild anledning finns risk för viss allvarlig brottslighet och syftet med bevakningen är att förebygga, förhindra, upptäcka, utreda eller lagföra denna. Vidare ska undantas viss kamerabevakning som hittills varit anmälningsskyldig, t.ex. bevakning i tunnelbanan.

Tillstånd till kamerabevakning ska ges om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad. Vid bedömningen av intresset av kamerabevakning ska det särskilt beaktas om bevakningen behövs för att

- förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats,
- förebygga, förhindra, upptäcka, utreda eller lagföra angrepp på någons liv, hälsa eller trygghet till person eller på egendom på en plats där det av särskild anledning finns risk för sådana angrepp,
- förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller begränsa verkningarna av sådana störningar,
- utöva kontrollverksamhet,
- förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor, eller
- tillgodose andra därmed jämförliga ändamål.

Vid ändrade förhållanden ska ett tillstånd kunna ändras eller återkallas.

Ett förstärkt integritetsskydd på arbetsplatser

I fråga om kamerabevakning på arbetsplatser som ska omfattas av kravet på tillstånd till sådan bevakning ska – liksom enligt kameraövervakningslagen – ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på

arbetsplatsen lämnas in tillsammans med en ansökan om tillstånd. Detsamma ska gälla i fråga om en ansökan om undantag från upplysningskravet vid kamerabevakning på arbetsplatser.

När det gäller kamerabevakning på arbetsplatser som inte ska omfattas av tillståndskravet ska införas en ny skyldighet för arbetsgivaren att först förhandla om bevakningen med en organisation som företräder arbetstagarna på arbetsplatsen. Förhandlingsskyldigheten ska fullgöras på det sätt som anges i lagen (1976:580) om medbestämmande i arbetslivet. Från förhandlingsskyldigheten ska avvikelse få göras genom kollektivavtal.

En organisation som företräder arbetstagarna på arbetsplatsen ska ha rätt att överklaga beslut om tillstånd till kamerabevakning och beslut om undantag från upplysningskravet.

Ett förstärkt integritetsskydd i övrigt

Vid kamerabevakning ska i övrigt gälla de bestämmelser som finns i förordningen och dataskyddslagen med föreskrifter eller brottsdatalagen med föreskrifter och som avser principer för behandling av personuppgifter, rättigheter för enskilda, skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden samt överföring av personuppgifter till tredjeland eller internationella organisationer. Att låta dessa bestämmelser gälla för kamerabevakning ger ett förstärkt integritetsskydd jämfört med vad som gällt hittills.

Tillsyn, sanktioner och rättsmedel

Tillsynen över kamerabevakning ska samlas hos en enda myndighet, Datainspektionen, och inte längre vara uppdelad mellan länsstyrelserna och Datainspektionen.

I ett ärende enligt kamerabevakningslagen hos tillsynsmyndigheten ska bestämmelser om undersökningsbefogenheter för den myndigheten i förordningen och dataskyddslagen med föreskrifter eller i brottsdatalagen med föreskrifter tillämpas. Vid underlåtenhet att bistå tillsynsmyndigheten i ett sådant ärende ska bestämmelser om sanktionsavgifter tillämpas. Bestämmelserna om sanktionsavgifter ska även tillämpas vid överträdelser av kamerabevakningslagen eller

av beslut som meddelats med stöd av lagen. Vid sådana överträdelser ska dessutom bestämmelser om skadestånd tillämpas.

Något straffansvar för den som bryter mot kamerabevakningslagen eller beslut som meddelats med stöd av lagen ska inte längre kunna följa.

Tillsynsmyndighetens beslut enligt lagen, t.ex. i frågor om tillstånd till kamerabevakning, undantag från kravet på upplysning om kamerabevakning och sanktionsavgifter, ska få överklagas till allmän förvaltningsdomstol. Beslut om tillstånd till kamerabevakning och om undantag från upplysningskravet ska få överklagas även av den kommun där bevakningen ska ske. Som framgått ovan ska ett sådant beslut – när kamerabevakningen ska avse en arbetsplats – också få överklagas av en organisation som företräder arbetstagarna på arbetsplatsen.

I övrigt ska bestämmelser om tillsynsmyndighetens befogenheter, sanktioner, överklagande m.m. i förordningen och dataskyddslagen med föreskrifter eller i brottsdatalagen med föreskrifter gälla för kamerabevakning såvitt avser ärenden, beslut, överträdelser m.m. som inte regleras direkt i kamerabevakningslagen.

1 Författningsförslag

1.1 Förslag till kamerabevakningslag

Härigenom föreskrivs följande.

Allmänna bestämmelser

Inledande bestämmelse

1 § I denna lag finns bestämmelser om kamerabevakning som

– kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), nedan kallad dataskyddsförordningen,

– genomför Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, nedan kallat dataskyddsdirektivet, eller

– avser sådan kamerabevakning som inte omfattas av dataskyddsförordningen eller dataskyddsdirektivet.

Lagens syfte

2 § Syftet med denna lag är att tillgodose behovet av kamerabevakning för berättigade ändamål och att skydda enskilda mot otillbörliga intrång i den personliga integriteten vid sådan bevakning.

Lagens tillämpningsområde

3 § Denna lag gäller vid kamerabevakning. Med kamerabevakning förstås

1. att en TV-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning, utan att manövreras på platsen, används varaktigt eller regelbundet upprepat för personbevakning,
2. att en separat teknisk anordning för avlyssning eller upptagning av ljud används för personbevakning i samband med användning av sådan utrustning som avses i 1, och
3. att en separat teknisk anordning för att behandla upptaget bild- och ljudmaterial används.

4 § Lagen gäller endast om

1. kamerabevakning enligt 3 § 1 eller 2 sker med utrustning som finns i Sverige och den som bedriver bevakningen är etablerad i Sverige eller i tredjeland, eller
2. kamerabevakning enligt 3 § 3 avser behandling av bild- och ljudmaterial som tagits upp vid bevakning som avses i 1 och behandlingen utförs av den som bedriver bevakningen eller för hans eller hennes räkning.

5 § Lagen gäller inte vid

1. kamerabevakning som en fysisk person utför som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,
2. hemlig kameraövervakning enligt 27 kap. rättegångsbalken eller lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott,
3. kamerabevakning som sker i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, och
4. kamerabevakning som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

Lagens förhållande till andra bestämmelser

6 § Utöver vad som föreskrivs i denna lag gäller i tillämpliga delar

1. dataskyddsförordningen, lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning, föreskrifter som meddelats med stöd av den lagen eller annan författning som kompletterar dataskyddsförordningen vid kamerabevakning som omfattas av förordningen eller den angivna lagen, eller

2. brottsdatalagen (2018:000), föreskrifter som meddelats med stöd av den lagen eller annan författning som genomför dataskyddsdirektivet vid kamerabevakning som omfattas av brottsdatalagen.

Uttryck i lagen

7 § Uttryck som används i denna lag har samma betydelse som i dataskyddsförordningen när det gäller kamerabevakning som omfattas av förordningen eller lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning eller som i brottsdatalagen (2018:000) när det gäller kamerabevakning som omfattas av den lagen.

Tillstånd till kamerabevakning

Krav på tillstånd

8 § Tillstånd krävs till kamerabevakning av en plats dit allmänheten har tillträde, om bevakningen ska bedrivas av en myndighet. Detsamma gäller om kamerabevakning av en sådan plats ska bedrivas av en annan juridisk person eller en fysisk person vid utförande av en uppgift som följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning och

1. avser brottsbekämpning, lagföring eller straffverkställighet eller upprätthållande av allmän ordning och säkerhet,

2. avser nationell säkerhet, eller

3. annars är av allmänt intresse.

9 § Tillstånd till kamerabevakning ska ges om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad.

Vid bedömningen av intresset av kamerabevakning ska det särskilt beaktas om bevakningen behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats eller på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet till person eller på egendom,
2. förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller begränsa verkningarna av sådana störningar,
3. utöva kontrollverksamhet,
4. förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor, eller
5. tillgodose andra därmed jämförliga ändamål.

Vid bedömningen av den enskildes intresse av att inte bli kamerabevakad ska det särskilt beaktas

1. hur bevakningen ska utföras,
2. om teknik som främjar skyddet av den enskildes personliga integritet ska användas, och
3. vilket område som ska bevakas.

Undantag från tillståndskravet

10 § Tillstånd till kamerabevakning krävs inte vid

1. bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning,
2. bevakning som sker för att skydda en byggnad, en annan anläggning eller ett område som enligt 4 § 4, 5 § 1–4 eller 6 § första stycket skyddslagen (2010:305) har förklarats vara skyddsobjekt, om bevakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet,
3. bevakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning,
4. bevakning som Trafikverket bedriver

a) av vägtrafik eller av sjötrafik vid en rörlig bro,

b) vid en betalstation som avses i bilagorna till lagen (2004:629) om trängselskatt och som sker för att samla in endast uppgifter som behövs för att beslut om trängselskatt ska kunna fattas och för att kontrollera att sådan skatt betalas, och

c) vid en betalstation på allmän väg som används vid uttag av infrastrukturavgifter enligt lagen (2014:52) om infrastrukturavgifter på väg och som sker för att samla in endast uppgifter som behövs för att beslut om infrastrukturavgift ska kunna fattas och för att kontrollera att sådan avgift betalas,

5. sådan trafikbevakning i en vägtunnel som avses i lagen (2006:418) om säkerhet i vägtunnlar och som bedrivs av någon annan tunnelhållare än Trafikverket,

6. bevakning i en tunnelbanevagn eller av en tunnelbanestation, om bevakningen har till enda syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott eller förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor,

7. bevakning i en lokal där det bedrivs postverksamhet eller av området omedelbart utanför in- och utgångar till en sådan lokal eller av en yta i en butikslokal på vilken det bedrivs postverksamhet, om bevakningen har till enda syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott,

8. bevakning i ett parkeringshus, om bevakningen har till enda syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott, och

9. bevakning som sker för säkerheten i trafiken eller arbetsmiljön från ett fordon, en maskin eller liknande för att förbättra sikten för föraren eller användaren.

Undantaget från tillståndskravet i första stycket 2 gäller inte för sådana byggnader, andra anläggningar och områden som används för eller är avsedda för fredstida krishantering enligt 4 § 4 skyddslagen.

Tillfälliga undantag från tillståndskravet

11 § Kamerabevakning får ske under högst en månad utan att en ansökan om tillstånd har gjorts vid

1. bevakning som bedrivs av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet som innebär fara för liv eller hälsa eller för omfattande förstörelse av egendom på en viss plats och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott,

2. bevakning som bedrivs av Polismyndigheten eller den som är räddningsledare enligt lagen (2003:778) om skydd mot olyckor, om bevakningen är av vikt för att avvärja en hotande olycka eller begränsa verkningarna av en inträffad olycka, och

3. bevakning som bedrivs av den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att efterforska en försvunnen person.

Om en ansökan om tillstånd görs inom en månad från det att kamerabevakningen inleddes, får bevakningen bedrivas utan tillstånd till dess att ansökningen har prövats.

Ansökan om tillstånd

12 § En ansökan om tillstånd till kamerabevakning ska göras skriftligen hos tillsynsmyndigheten.

Ansökningen ska innehålla

1. uppgift om den som ska bedriva bevakningen och i förekommande fall den som ska ha hand om bevakningen för tillståndshavarens räkning,

2. uppgift om bevakningens ändamål,

3. en beskrivning av bevakningen, särskilt den utrustning som ska användas, var utrustningen ska placeras, det område som ska bevakas och de tider då bevakning ska ske,

4. en bedömning av behovet av och proportionaliteten i bevakningen i förhållande till ändamålet,

5. en bedömning av riskerna för intrång i den personliga integriteten och en beskrivning av de åtgärder som planeras för att hantera riskerna, och

6. uppgift om de omständigheter i övrigt som är av betydelse för prövningen av ärendet.

Om bevakningen avser en arbetsplats, ska ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med ansökningen.

Yttrande av kommunen

13 § Innan tillsynsmyndigheten beslutar om tillstånd till kamerabevakning ska den kommun där bevakningen ska ske få tillfälle att yttra sig, om det behövs.

Beslut om tillstånd

14 § Ett beslut om tillstånd till kamerabevakning ska ange vem som ska bedriva bevakningen och i förekommande fall vem som ska ha hand om bevakningen för tillståndshavarens räkning.

Beslutet ska förenas med villkor om hur kamerabevakningen får anordnas. Villkoren ska avse

1. bevakningens ändamål,

2. den utrustning som får användas och var utrustningen får placeras,

3. det område som får bevakas och de tider då bevakning får ske, och

4. upplysning om bevakningen, behandling av bilder eller ljud och andra förhållanden som har betydelse för att skydda enskildas personliga integritet, om sådana villkor behövs för tillståndet.

Ett tillstånds giltighet får begränsas till en viss tid.

15 § Om förutsättningarna för ett tillstånd ändras, får tillsynsmyndigheten besluta om nya villkor eller, om förutsättningarna för tillstånd inte längre är uppfyllda, återkalla tillståndet.

Upplysning om kamerabevakning

Krav på upplysning

16 § Vid kamerabevakning ska genom tydlig skyltning eller på något annat liknande verksamt sätt lämnas upplysning om

1. kamerabevakningen,
2. identiteten hos och kontaktuppgifterna till den som ska bedriva bevakningen, och
3. kontaktuppgifter till ett eventuellt dataskyddsombud.

Om ljud kan avlyssnas eller tas upp vid bevakningen, ska en särskild upplysning lämnas om detta.

Information ska även göras tillgänglig för dem som kan bli kamerabevakade om

1. ändamålet med och den rättsliga grunden för kamerabevakningen,
2. hur länge upptaget bild- och ljudmaterial får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa detta, och
3. möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifterna till den.

Undantag från upplysningskravet

17 § Upplysning om kamerabevakning behöver inte lämnas vid

1. bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning,
2. bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet som innebär fara för liv eller hälsa eller för omfattande förstörelse av egendom på en viss plats och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott,
3. bevakning som sker för att skydda en byggnad, en annan anläggning eller ett område som enligt 4 § 4, 5 § 1–4 eller 6 § första stycket skyddslagen (2010:305) har förklarats vara skyddsobjekt, om bevakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet,

4. bevakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning,

5. bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller den som är räddningsledare enligt lagen (2003:778) om skydd mot olyckor, om bevakningen är av vikt för att avvärja en hotande olycka eller begränsa verkningarna av en inträffad olycka, och

6. bevakning som bedrivs av den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att efterforska en försvunnen person.

Undantaget från upplysningskravet i första stycket 3 gäller inte för sådana byggnader, andra anläggningar eller områden som används för eller är avsedda för fredstida krishantering enligt 4 § 4 skyddslagen.

18 § Undantagen från upplysningskravet gäller inte, om ljud ska avlyssnas eller tas upp vid kamerabevakningen.

Undantag från upplysningskravet i enskilda fall

19 § Om det finns synnerliga skäl, får tillsynsmyndigheten i enskilda fall besluta om undantag från upplysningskravet.

Ansökan om undantag

20 § En ansökan om undantag från upplysningskravet ska göras skriftligen hos tillsynsmyndigheten.

Ansökningen ska innehålla uppgift om den som ska bedriva kamerabevakningen och i förekommande fall den som ska ha hand om bevakningen för hans eller hennes räkning samt skälen för ansökningen.

Om bevakningen avser en arbetsplats, ska ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med ansökningen.

Yttrande av kommunen

21 § Innan tillsynsmyndigheten beslutar om undantag från upplysningskravet ska den kommun där kamerabevakningen ska ske få tillfälle att yttra sig, om bevakningen ska avse en plats dit allmänheten har tillträde och det behövs ett yttrande.

Beslut om undantag

22 § Ett beslut om undantag från upplysningskravet ska ange vem som ska bedriva kamerabevakningen och i förekommande fall vem som ska ha hand om bevakningen för hans eller hennes räkning.

Beslutet ska förenas med de villkor som behövs.

23 § Om förutsättningarna för ett beslut om undantag ändras, får tillsynsmyndigheten ändra beslutet eller, om förutsättningarna för ett sådant beslut inte längre är uppfyllda, återkalla detta.

Förhandlingsskyldighet för arbetsgivare

Förhandlingsskyldighet

24 § Innan en arbetsgivare beslutar om kamerabevakning som avser arbetsplatsen och som inte omfattas av kravet på tillstånd ska arbetsgivaren förhandla med berörd arbetstagarorganisation på det sätt som anges i 11–14 §§ lagen (1976:580) om medbestämmande i arbetslivet.

Undantag från förhandlingsskyldigheten

25 § Från förhandlingsskyldigheten för arbetsgivare får avvikelse göras genom kollektivavtal.

Tystnadsplikt och utlämnande av uppgifter

26 § Den som tar befattning med en uppgift som har inhämtats genom kamerabevakning får inte obehörigen röja eller utnyttja det som han eller hon på detta sätt har fått veta om någon enskilds

personliga förhållanden. I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400).

Tillsyn, sanktionsavgifter och skadestånd

Tillsynsmyndighet

27 § Den myndighet som regeringen bestämmer (tillsynsmyndigheten) utövar tillsyn över kamerabevakning enligt denna lag.

Undersökningsbefogenheter, sanktionsavgifter och skadestånd

28 § I ett ärende enligt denna lag hos tillsynsmyndigheten och vid underlåtenhet att bistå den myndigheten i ett sådant ärende tillämpas bestämmelser om undersökningsbefogenheter för tillsynsmyndigheten och sanktionsavgifter i

1. dataskyddsförordningen, lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som meddelats med stöd av den lagen när det gäller kamerabevakning som omfattas av förordningen eller den lagen, eller
2. brottsdatalagen (2018:000) och föreskrifter som meddelats med stöd av den lagen när det gäller kamerabevakning som omfattas av den lagen.

Bestämmelser i första stycket 1 eller 2 tillämpas på motsvarande sätt i fråga om sanktionsavgifter och skadestånd vid överträdelse av bestämmelserna i denna lag eller av beslut som meddelats med stöd av lagen.

Vid tillämpning av bestämmelser om sanktionsavgifter gäller för myndigheter den högre avgiftsnivå som föreskrivs i lagen med kompletterande bestämmelser till EU:s dataskyddsförordning respektive brottsdatalagen.

Överklagande m.m.

Överklagande

29 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol.

Beslut om tillstånd till kamerabevakning och om undantag från kravet på upplysning om kamerabevakning får överklagas även av den kommun där bevakningen ska ske och, om kamerabevakningen ska avse en arbetsplats, av en organisation som företräder arbetstagarna på arbetsplatsen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Föreskrifter

30 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om avgifter för ansökningar enligt denna lag.

---

1. Denna lag träder i kraft den 25 maj 2018.

2. Genom lagen upphävs kameraövervakningslagen (2013:460).

3. Tillstånd till kameraövervakning som har beslutats enligt den äldre lagen och som avser kamerabevakning som omfattas av kravet på tillstånd i den nya lagen gäller fortfarande. Övriga tillstånd som har beslutats enligt den äldre lagen gäller inte längre.

4. Undantag från upplysningsplikten som har beslutats enligt den äldre lagen gäller fortfarande.

5. Anmälningar som har gjorts enligt den äldre lagen gäller inte längre.

6. Ärenden som har inletts hos länsstyrelserna enligt den äldre lagen men ännu inte har avgjorts överlämnas till den myndighet som utövar tillsyn över kamerabevakning enligt den nya lagen.

7. Mål som har överklagats till annan förvaltningsrätt än Förvaltningsrätten i Stockholm eller till annan kammarrätt än Kammarrätten i Stockholm enligt den äldre lagen men ännu inte har avgjorts överlämnas till Förvaltningsrätten i Stockholm respektive Kammarrätten i Stockholm. Om ett mål har överklagats av en enskild, är den myndighet som utövar tillsyn över kamerabevakning enligt den nya lagen motpart.

8. Äldre föreskrifter om skadestånd gäller fortfarande för skada som har orsakats före ikraftträdandet.

9. Äldre föreskrifter gäller fortfarande för överträdelser som har skett före ikraftträdandet.

1.2 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att 32 kap. 3 § ska ha följande lydelse,

dels att rubriken närmast efter 32 kap. 2 § ska lyda ”Kamerabevakning”.

Nuvarande lydelse	*Föreslagen lydelse*
32 kap.	
3 §[1]	
Sekretess gäller för sådan uppgift om en enskilds personliga förhållanden som har inhämtats genom *kameraövervakning* som avses i *kameraövervakningslagen (2013:460)*, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.	Sekretess gäller för sådan uppgift om en enskilds personliga förhållanden som har inhämtats genom *kamerabevakning* som avses i *kamerabevakningslagen (2018:000)*, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.

Sekretessen enligt första stycket gäller hos en domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

---

1. Denna lag träder i kraft den 25 maj 2018.

2. Äldre föreskrifter gäller fortfarande för uppgift som har inhämtats före ikraftträdandet.

---

[1] Senaste lydelse 2013:461.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag och andra utredningsuppdrag av intresse

2.1.1 Inledning

Denna utredning har haft i uppdrag att utreda vissa frågor om kameraövervakning. I uppdraget har ingått att analysera vad den nya dataskyddsförordning och det nya dataskyddsdirektiv som antagits inom EU och som beskrivs översiktligt i avsnitt 6 och analyseras närmare i avsnitt 7 innebär för möjligheterna att i svensk rätt reglera frågor om kameraövervakning. Parallellt med utredningens arbete har ett flertal andra utredningar övervägt hur denna EU-reglering i olika avseenden påverkar svensk rätt. Vissa av de frågor som utredningarna har övervägt har varit desamma som denna utredning ställts inför. Det har därför krävts en samordning mellan utredningarna så att utredningarnas respektive förslag inte går i olika riktning eller i onödan överlappar varandra. Detta har fått betydelse för hur denna utredning valt att utforma sina förslag.

Nedan redovisas därför kortfattat denna utrednings uppdrag och uppdragen till dem av de andra utredningarna som varit av störst betydelse för denna utredning. De bedömningar som gjorts och de förslag som lämnats av dessa utredningar redovisas i relevanta delar i de avsnitt i detta betänkande som innehåller överväganden och förslag. I avsnitt 8 lämnas dessutom en allmän beskrivning av vad som skulle gälla för kameraanvändning om någon särskild lagstiftning på området inte skulle finnas framöver. I den beskrivningen redogörs för vissa förslag som lämnats av de nämnda utredningarna.

2.1.2 Utredningen om kameraövervakning – brottsbekämpning och integritet

Denna utredning, Utredningen om kameraövervakning – brottsbekämpning och integritetsskydd, har utrett vissa frågor om kameraövervakning (dir. 2015:125 och 2016:54) i syfte att säkerställa att kameraövervakning kan användas där det behövs för att bekämpa brott och samtidigt garantera ett starkt skydd för den personliga integriteten. Utredningen har bl.a.

- analyserat hur regleringen i kameraövervakningslagen (2013:460) bör anpassas till den nya EU-rättsliga dataskyddsregleringen,
- kartlagt och utvärderat vad kameraövervakningslagen inneburit för möjligheterna till kameraövervakning och skyddet för den personliga integriteten,
- analyserat om möjligheterna till kameraövervakning på särskilt brottsutsatta platser och andra platser med förhöjt skyddsbehov, t.ex. asylboenden, medieredaktioner och lokaler som används av religiösa samfund, behöver förbättras,
- undersökt hur lagens tillämpningsområde förhåller sig till användning av ny teknik, såsom t.ex. kamerautrustade drönare,
- tagit ställning till om integritetsskyddet på vissa platser dit allmänheten inte har tillträde, t.ex. arbetsplatser och skolor, behöver förbättras, och
- analyserat om integritetsskyddet kan förstärkas genom att Datainspektionen ges föreskriftsrätt när det gäller tillämpningen av kameraövervakningslagen.

Utredningen har inte haft i uppdrag att överväga och föreslå ändringar i bestämmelser om s.k. hemlig kameraövervakning enligt rättegångsbalken eller lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

2.1.3 Dataskyddsutredningen

Utredningen om dataskyddsförordningen (dir 2016:15), som tagit sig namnet Dataskyddsutredningen, har haft i uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som förordningen ger anledning till. Syftet har varit att säkerställa att det finns en ändamålsenlig och välbalanserad kompletterande nationell reglering om personuppgiftsbehandling på plats när förordningen börjar tillämpas. Utredningen har bl.a.

- undersökt vilka kompletterande nationella föreskrifter, exempelvis processuella bestämmelser, som förordningen kräver,
- analyserat vilka bestämmelser om administrativa sanktionsavgifter och andra sanktioner som Sverige behöver eller bör införa, och
- undersökt om det finns behov av generella bestämmelser för personuppgiftsbehandling utanför EU-rättens tillämpningsområde.

Dataskyddsutredningen har redovisat sitt uppdrag i maj 2017 i betänkandet *Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning* (SOU 2017:39). Utredningen har bl.a. föreslagit en ny lag, dataskyddslagen, som ska komplettera förordningen.

2.1.4 Utredningen om 2016 års dataskyddsdirektiv

Utredningen om genomförande av dataskyddsdirektivet (dir 2016:21), som tagit sig namnet Utredningen om 2016 års dataskyddsdirektiv, har haft i uppdrag att föreslå hur direktivet ska genomföras i svensk rätt i en ny ramlagstiftning med bestämmelser om skydd av personuppgifter inom direktivets tillämpningsområde. Utredningen har i april 2017 lämnat förslag till en sådan lagstiftning, kallad brottsdatalagen, i delbetänkandet *Brottsdatalag* (SOU 2017:29).

Utredningens arbete pågår fortfarande. Utredningen ska bl.a. lämna förslag till de författningsändringar som krävs för att anpassa vissa centrala författningar om rättsväsendets behandling av personuppgifter till de nya förutsättningarna. Ett slutbetänkande ska lämnas senast i september 2017.

2.1.5 Utredningen om tillsynen över den personliga integriteten

Utredningen om tillsynen över den personliga integriteten (dir. 2014:164 och 2015:139) har, mot bakgrund av att ansvaret för tillsyn på integritetsområdet i dag ligger på flera olika myndigheter, övervägt hur ett i högre grad samlat integritetsskydd kan fungera inom en och samma myndighetsstruktur genom att tillsynen över behandling av personuppgifter samlas hos en myndighet. Utredningen har också haft i uppdrag att lämna de förslag som behövs för att myndigheten ska kunna fullgöra de uppgifter som kan bli resultatet av reformeringen av EU:s dataskyddsreglering. I uppdraget har även ingått bl.a. att lämna förslag som medför att myndigheten är förberedd för att kunna fullgöra de uppgifter som ett integritetsskyddsråd ska ha enligt förslag av Integritetskommittén (dir. 2014:65 och 2016:12). Den kommittén har utifrån ett individperspektiv kartlagt och analyserat sådana faktiska och potentiella risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik i såväl privat som offentlig verksamhet. Kommittén har avgett delbetänkandet *Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén* (SOU 2016:41).

Utredningen om tillsynen över den personliga integriteten har i september 2016 redovisat sitt uppdrag i betänkandet *Ett samlat ansvar för tillsyn över den personliga integriteten* (SOU 2016:65).

2.2 Utredningens arbete

Denna utredning har biträtts av experter som representerat domarkåren, advokatkåren, Datainspektionen, länsstyrelserna, Polismyndigheten, Brottsförebyggande rådet och Justitiedepartementets grundlagsenhet. Utredningen har regelbundet hållit sammanträden med experterna, totalt åtta stycken, varav ett i internatform. Inför sammanträdena har utredningen producerat promemorior som i arbetets slutskede i allt väsentligt motsvarat texten i detta betänkande.

Utredningen har vidare inhämtat domstolspraxis på området och annat relevant material. Som grund för den kartläggning och utvärdering av kameraövervakningslagen som utredningen haft i upp-

drag att göra har två enkätundersökningar genomförts. Dessa undersökningar och resultatet av dem redovisas i avsnitt 5.

Utredningen har även sammanträffat med företrädare för myndigheter och andra som berörts av de frågor som utredningen haft att överväga. Dessa möten och de synpunkter som då framkommit redovisas också i avsnitt 5. Därutöver har det förekommit kontakter också med andra. Utredningen har även medverkat i vissa andra sammanhang, t.ex. i konferensen Trygghetskamerans dag 2016 och 2017 samt mässan Skydd 2016.

Under arbetets gång har utredningen fortlöpande fört en dialog med och samrått med flera av de andra utredningar på dataskyddsområdet som nämnts ovan. Det gäller i första hand Dataskyddsutredningen och Utredningen om 2016 års dataskyddsdirektiv. Utredningen har också deltagit i en samordningsgrupp för samtliga utredningar på området. Dessutom har utredningen sammanträffat med Utredningen om självkörande fordon på väg (N 2015:07).

3 Gällande ordning

3.1 Inledning

Den 1 juli 2013 trädde kameraövervakningslagen (2013:460) i kraft. I och med införandet av kameraövervakningslagen samlades bestämmelserna i den tidigare lagen (1998:150) om allmän kameraövervakning och vissa bestämmelser i personuppgiftslagen (1998:204) i en och samma lag. Syftet var att modernisera regleringen av kameraövervakning på ett sätt som skulle säkerställa balansen mellan intresset av att använda kameraövervakning för berättigade ändamål och intresset av att skydda enskildas integritet. Avsikten var också att bestämmelserna skulle bli mer överskådliga och lättillgängliga (prop. 2012/13:115 s. 1).

Vid sidan av kameraövervakningslagen finns det särskilda bestämmelser om s.k. hemlig kameraövervakning i 27 kap. rättegångsbalken och i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. Bestämmelserna om hemlig kameraövervakning innebär att sådan kameraövervakning får användas, bl.a. vid vissa förundersökningar i brottmål, utan att upplysning om övervakningen lämnas. Då hemlig kameraövervakning inte omfattas av utredningens uppdrag kommer dessa regler inte att behandlas närmare i betänkandet.

I detta avsnitt lämnas inledningsvis en översiktlig redogörelse för den generella regleringen om skydd för personuppgifter i internationella åtaganden avseende dataskydd och bestämmelser på nationell nivå. Därefter lämnas en beskrivning av innehållet i kameraövervakningslagen. För en sammanfattning av tidigare lagstiftning om kameraövervakning hänvisas till betänkandet *En ny kameraövervakningslag* (SOU 2009:87, s. 49 f.). I avsnitt 6 finns en redovisning av EU:s nya dataskyddsreglering. Avslutningsvis beskrivs kort

lagstiftning på kameraövervakningsområdet i några av våra nordiska grannländer.

3.2 Den generella regleringen om skydd för personuppgifter

3.2.1 Europarådets dataskyddsreglering

Europakonventionen

Rätten till respekt för den personliga integriteten ingår som en del i rätten till respekt för privatlivet enligt den europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Av artikel 8 i Europakonventionen följer att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. En offentlig myndighet får inte inskränka denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

Europakonventionen är sedan den 1 januari 1995 inkorporerad i svensk rätt och gäller som svensk lag (lagen [1994:1219] om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna). Artikel 8 om rätt till respekt för privatlivet m.m. gäller alltså som svensk lag. Av 2 kap. 19 § regeringsformen framgår att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av Europakonventionen.

Europarådets dataskyddskonvention

Inom Europarådet antogs år 1981 en konvention (nr 108) om skydd för enskilda vid automatisk databehandling av personuppgifter, den s.k. dataskyddskonventionen. Till konventionen hör ett tilläggsprotokoll. Dessutom kompletteras konventionen av ett antal rekommendationer på dataskyddsområdet. Konventionens syfte är att säker-

ställa den enskildes rätt till personlig integritet i samband med automatiserad behandling av personuppgifter. Regleringen kan ses som en precisering av skyddet enligt artikel 8 i Europakonventionen vad gäller just automatiserad behandling av personuppgifter. Inom Europarådet pågår för närvarande en översyn av konventionen. Samtliga medlemsstater i EU har tillträtt konventionen.

3.2.2 EU:s dataskyddsreglering

EU:s stadga om de grundläggande rättigheterna

Enligt artikel 6.1 i fördraget om Europeiska unionen ska EU:s stadga om de grundläggande rättigheterna ha samma rättsliga värde som fördragen. I stadgan bekräftas de rättigheter som har sin grund i medlemsstaternas gemensamma författningstraditioner och internationella förpliktelser, Europakonventionen, unionens och Europarådets sociala stadgor samt rättspraxis vid Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna. Stadgans huvudsakliga syfte är att kodifiera de grundläggande fri- och rättigheter som EU redan erkänner.

I stadgans artikel 7 föreskrivs, efter förebild i artikel 8 i Europakonventionen, att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sin korrespondens. Av artikel 8 följer vidare att var och en har rätt till skydd för personuppgifter. Rättighetens innebörd är att personuppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Vidare har var och en rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. En oberoende myndighet ska kontrollera att dessa regler efterlevs.

Av artikel 51 framgår att stadgan riktar sig till medlemsstaterna när de tillämpar unionsrätten.

Enligt artikel 52 måste varje begränsning i utövandet av de fri- och rättigheter som erkänns i stadgan vara föreskriven i lag och vara förenlig med det väsentliga innehållet i dessa fri- och rättigheter. Begränsningar får, med beaktande av proportionalitetsprincipen, göras endast om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors fri- och rättigheter. I den mån

en rättighet som erkänns i stadgan motsvarar en rättighet som också garanteras i Europakonventionen ska rättigheten i stadgan ha samma innebörd och räckvidd som i konventionen.

1995 års dataskyddsdirektiv och dataskyddsrambeslutet

Den allmänna regleringen inom EU om skydd av personuppgifter finns i dag i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, 1995 års dataskyddsdirektiv. Direktivet syftar till att garantera en i alla medlemsstater hög och likvärdig skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter samt att främja ett fritt flöde av personuppgifter mellan medlemsstaterna i EU.

1995 års dataskyddsdirektiv omfattar både behandling av personuppgifter som är helt eller delvis automatiserad och manuell behandling av personuppgifter som ingår eller kommer att ingå i ett register. Direktivet omfattar däremot inte behandling av personuppgifter på områden som faller utanför unionsrätten, t.ex. som avser allmän säkerhet eller försvar. Det omfattar inte heller behandling av personuppgifter av en fysisk person som är av rent privat natur.

Enligt direktivet ska all behandling av personuppgifter vara laglig och korrekt. Uppgifterna måste vara riktiga och aktuella samt adekvata, relevanta och nödvändiga med hänsyn till de ändamål för vilka de behandlas. Ändamålen ska vara uttryckligt angivna vid tiden för insamlingen av uppgifterna. De ändamål för vilka uppgifterna senare behandlas får inte vara oförenliga med de ursprungliga ändamålen. Personuppgifter får enligt direktivet behandlas bara om den registrerade otvetydigt har lämnat sitt samtycke eller om behandlingen är nödvändig för något av de ändamål som anges i direktivet, t.ex. för att utföra en arbetsuppgift som är av allmänt intresse eller utgör ett led i myndighetsutövning.

Vissa kategorier av uppgifter, s.k. känsliga personuppgifter, får som huvudregel inte behandlas. Det gäller uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt uppgifter som rör hälsa och sexualliv. Behandling av sådana uppgifter får endast ske

i vissa undantagsfall, bl.a. när det finns ett uttryckligt samtycke av den registrerade. Medlemsstaterna får också, under förutsättning att lämpliga skyddsåtgärder vidtas och av hänsyn till ett viktigt allmänt intresse, besluta om undantag från förbudet.

Vidare finns det i direktivet bestämmelser om enskildas rätt till information och tillgång till uppgifter för att kunna ta till vara sina rättigheter. Som huvudregel ska den personuppgiftsansvarige informera den registrerade om att personuppgifter behandlas. Direktivet ger också den registrerade rätt att på begäran få information om bl.a. vilka uppgifter som behandlas samt att få sådana uppgifter som inte har behandlats i enlighet med direktivet rättade, utplånade eller blockerade.

Räckvidden av de principer och de rättigheter som slås fast för enskilda i direktivet får begränsas genom undantag i nationell rätt. Begränsningar får göras bl.a. om det är nödvändigt med hänsyn till statens säkerhet, allmän säkerhet eller förebyggande, undersökning, avslöjande av brott eller åtal för brott.

Direktivet innehåller också bestämmelser om rätt att motsätta sig behandling, regler om säkerhet vid behandling och om krav på en nationell reglering rörande skadestånd och sanktioner.

Enligt direktivet får vidare en överföring av personuppgifter till tredjeland, dvs. en stat som inte är medlem i EU eller ansluten till Europeiska ekonomiska samarbetsområdet (EES), som huvudregel endast ske om det mottagande landets lagstiftning kan säkerställa en adekvat skyddsnivå.

Varje medlemsstat ska enligt direktivet utse en eller flera myndigheter som har till uppgift att inom dess territorium övervaka tillämpningen av de bestämmelser som medlemsstaterna antar till följd av direktivet. Dessa myndigheter ska fullständigt oberoende utöva de uppgifter som åläggs dem.

På EU-nivå finns även bl.a. rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, dataskyddsrambeslutet.

3.2.3 Regeringsformen

Av målsättningsstadgandet i 1 kap. 2 § regeringsformen (RF) framgår att den offentliga makten ska utövas med respekt för den enskilda människans frihet och värdighet samt att det allmänna ska värna den enskildes privatliv och familjeliv. Vidare följer av 2 kap. 6 § andra stycket RF att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, som sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Begränsningar i denna rättighet får endast göras i lag och under de förutsättningar som anges i 2 kap. 21 och 22 §§ RF.

3.2.4 Personuppgiftslagen

1995 års dataskyddsdirektiv har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen. Personuppgiftslagen följer i princip direktivet vad gäller såväl text som struktur. Utöver den generella regleringen i personuppgiftslagen finns det ett stort antal s.k. särskilda registerförfattningar med bestämmelser som främst reglerar hur olika myndigheter får behandla personuppgifter, exempelvis polisdatalagen (2010:361) och domstolsdatalagen (2015:728). Det finns också sådana bestämmelser i författningar som primärt har andra syften än att reglera personuppgiftsbehandling, exempelvis i vapenlagen (1996:67) och kreditupplysningslagen (1973:1173).

Personuppgiftslagen syftar till att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter (1 §). Lagen är generellt tillämplig och gäller alltså även inom områden utanför tillämpningsområdet för 1995 års dataskyddsdirektiv. Lagen är dock subsidiär i förhållande till annan lag eller förordning (2 §).

Med personuppgifter avses enligt personuppgiftslagen all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet (3 §). Lagen gäller för sådan behandling av personuppgifter som helt eller delvis är automatiserad samt vid behandling i manuella register (5 §). Den gäller dock inte behandling av personuppgifter som utförs av en fysisk person som ett led i en verksamhet av rent privat natur (6 §).

I lagen uppställs vissa grundläggande krav på behandling av personuppgifter (9 §). Dessa krav innebär att personuppgifter bara får behandlas om det är lagligt samt sker på ett korrekt sätt och i enlighet med god sed. Uppgifterna måste dessutom samlas in för särskilda, uttryckligt angivna och berättigade ändamål och får inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Vidare ska de behandlade personuppgifterna vara adekvata och relevanta i förhållande till ändamålet med behandlingen. Det är inte tillåtet att behandla fler personuppgifter än vad som är nödvändigt med hänsyn till ändamålet med behandlingen och inte heller att bevara uppgifterna under längre tid än nödvändigt.

Av lagen följer vidare att personuppgifter får behandlas endast om den registrerade har lämnat sitt samtycke eller behandlingen är nödvändig för ett i lagen angivet ändamål (10 §).

I lagen finns även bestämmelser om bl.a. information till den registrerade, säkerhet vid behandling, straff och skadestånd. Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen.

Enligt en särskild bestämmelse i personuppgiftslagen, den s.k. missbruksregeln, behöver de flesta av lagens regler inte tillämpas på personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter (5 a §). Behandling av personuppgifter som faller in under missbruksregeln får dock inte utföras, om den innebär en kränkning av enskildas personliga integritet.

3.3 Kameraövervakningslagen

3.3.1 Definitioner och tillämpningsområde

Kameraövervakningslagen innehåller bestämmelser om kameraövervakning, dvs. användning av övervakningskameror och övrig övervakningsutrustning. Syftet med lagen är att tillgodose behovet av kameraövervakning för berättigade ändamål samtidigt som enskilda skyddas mot otillbörliga intrång i den personliga integriteten (1 §). Lagen gäller i stället för personuppgiftslagen (6 §).

Med övervakningskameror avses enligt lagen TV-kameror, andra optisk-elektroniska instrument och därmed jämförbara utrust-

ningar som är uppsatta så att de, utan att manövreras på platsen, kan användas för personövervakning samt separata tekniska anordningar för avlyssning eller upptagning av ljud vilka i samband med användning av sådan utrustning används för personövervakning (2 §).

Med *optisk* avses alla registreringar som kan ske med instrument inom det elektromagnetiska våglängdsspektrat för optisk strålning. *Elektronisk* innebär att förmedling, visning eller lagring av bilder sker genom elektronisk påverkan. Med *därmed jämförbara utrustningar* avses t.ex. utrustning som utnyttjar sådan elektromagnetisk strålning som röntgen och radiofrekvent strålning. Detta innebär att t.ex. röntgenkameror kan omfattas av lagen. Kravet att kameran ska vara *uppsatt* innebär att placeringen av kameran ska ha en viss varaktighet. En kamera som endast används helt kortvarigt är därmed inte en övervakningskamera som omfattas av lagen. Att kameran ska kunna användas *utan att manövreras på platsen* innebär att den fortlöpande hanteringen av utrustningen inte ska ske på plats. Lagen är alltså inte tillämplig på handhållna kameror. Endast det förhållandet att en kamera sätts i gång på stället eller fungerar med inbyggd automatik innebär inte att den manövreras på platsen och att lagen inte är tillämplig. Med *personövervakning* avses att personer kan identifieras genom övervakningen. För att en möjlighet till identifiering ska anses föreligga krävs att sådana kännetecken kan iakttas som gör att man utan större osäkerhet kan skilja de personer som iakttas från andra personer. Så är fallet om hela personen eller personens ansikte syns tydligt. Även sådant som utmärkande klädsel, speciella kroppsrörelser eller särskild kroppskonstitution kan möjliggöra identifiering. Exempel på *separata tekniska anordningar för avlyssning eller upptagning av ljud* är mikrofoner och radiosändare som inte är inbyggda i en övervakningskamera (prop. 2012/13:115 s. 38 ff. och prop. 1989/90:119 s. 39 f.).

Med *övrig övervakningsutrustning* avses separata tekniska anordningar för att behandla upptaget bild- och ljudmaterial, exempelvis anordningar för att lagra inspelad film.

Lagen innehåller också definitioner av begreppen behandling, samtycke och personuppgifter (2 §). Definitionerna motsvarar i huvudsak definitionerna av dessa begrepp i personuppgiftslagen (3 §).

Kameraövervakningslagen gäller vid kameraövervakning med övervakningskameror som är uppsatta i Sverige, om den som bedriver övervakningen är etablerad i Sverige eller i tredjeland. Med

tredjeland avses en stat som varken ingår i EU eller är ansluten till EES (2 §). Lagen gäller också vid behandling av bild- och ljudmaterial som tagits upp vid sådan övervakning, om behandlingen utförs av den som bedriver övervakningen eller för hans eller hennes räkning (3 §). Lagen gäller dock inte vid kameraövervakning av en plats dit allmänheten inte har tillträde, om övervakningen bedrivs av en fysisk person som ett led i en verksamhet av rent privat natur (5 §). Undantaget kan t.ex. omfatta kameraövervakning i en privatbostad när övervakningen bedrivs av den som bor där. Lagen gäller inte heller vid hemlig kameraövervakning enligt rättegångsbalken eller lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (4 §).

3.3.2 Allmänna krav

Som allmänna krav för all kameraövervakning som omfattas av kameraövervakningslagen gäller att övervakningen ska bedrivas lagligt, enligt god sed och med tillbörlig hänsyn till enskildas personliga integritet (7 §). När kameraövervakning är laglig framgår av bestämmelserna i lagen men kan också utläsas av andra bestämmelser, t.ex. straffbestämmelsen om kränkande fotografering (4 kap. 6 a § brottsbalken). Vad som är god sed kan exempelvis framgå av allmänna råd och branschöverenskommelser.

3.3.3 Kameraövervakning av platser dit allmänheten har tillträde

Tillståndsplikt som huvudregel

Lagen skiljer mellan kameraövervakning av en plats dit allmänheten har tillträde och kameraövervakning av en plats dit allmänheten inte har tillträde. För kameraövervakning av platser dit allmänheten har tillträde gäller mer detaljerade bestämmelser, som bl.a. innebär att det som huvudregel krävs tillstånd för att övervakningen ska vara tillåten (8 §). Denna skiljelinje har funnits sedan lång tid tillbaka och begreppet plats dit allmänheten har tillträde har blivit föremål för en omfattande praxis. Till platser dit allmänheten har tillträde räknas exempelvis gator, torg, parker, butiker, banker, restauranger,

biografer och badhus. Även bussar i allmän kommunikation och taxibilar har ansetts vara platser till vilka allmänheten har tillträde. De flesta utrymmen inne i skolor och gemensamhetsutrymmen i flerfamiljshus anses däremot inte vara platser dit allmänheten har tillträde. Detsamma gäller många arbetsplatser (prop. 2012/13:115 s. 28).

Tillstånd till kameraövervakning ska ges om intresset av sådan övervakning väger tyngre än den enskildes intresse av att inte bli övervakad (9 §). Vid bedömningen av intresset av kameraövervakning ska det särskilt beaktas om övervakningen behövs för att förebygga, avslöja eller utreda brott, förhindra olyckor eller andra därmed jämförliga ändamål. Vid bedömningen av den enskildes intresse av att inte bli övervakad ska det särskilt beaktas hur övervakningen ska utföras, om teknik som främjar skyddet av den enskildes personliga integritet används och vilket område som ska övervakas. Utgångspunkten är att kameraövervakning endast ska utgöra ett komplement till andra åtgärder, särskilt brottsförebyggande åtgärder. Kameraövervakning bör alltså inte ses som ett hjälpmedel som ska användas i stället för andra säkerhetsåtgärder eller förebyggande insatser (a. prop. s. 148).

Undantag från tillståndsplikten

Det finns vissa undantag från tillståndsplikten (10 §). Tillstånd krävs inte vid övervakning som sker med en övervakningskamera som för säkerheten i trafiken eller arbetsmiljön är uppsatt på ett fordon, en maskin eller liknande för att förbättra sikten för föraren eller användaren.

Vidare är viss övervakning som bedrivs av Trafikverket tillståndsfri. Det gäller vägtrafikövervakning och övervakning vid betalstationer för trängselskatt och infrastrukturavgifter.

Tillstånd krävs inte heller vid trafikövervakning i en vägtunnel som bedrivs av någon annan tunnelhållare än Trafikverket, vid övervakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning eller vid övervakning till skydd för vissa skyddsobjekt. Undantag från tillståndsplikten gäller vidare vid övervakning som Försvarsmakten bedriver från fordon, fartyg eller luftfartyg som ett

led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan övervakning.

Slutligen krävs det inte tillstånd vid övervakning i kasinon, om övervakningen har till syfte att förebygga, avslöja eller utreda brott eller lösa tvister om spel mellan spelare och den som anordnar spelet.

Tillfälliga undantag från tillståndsplikten

I några fall får kameraövervakning bedrivas under högst en månad utan att ansökan om tillstånd har gjorts (11 §). Det gäller övervakning som bedrivs av Polismyndigheten eller räddningsledare, om övervakningen är av vikt för att avvärja en hotande olycka eller för att begränsa verkningarna av en inträffad olycka. Det gäller också övervakning som bedrivs av räddningsledare, om övervakningen är av vikt för att efterforska en försvunnen person. Slutligen gäller det övervakning som bedrivs av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för att allvarlig brottslighet som innebär fara för liv eller hälsa eller för omfattande förstörelse av egendom kommer att utövas på en viss plats och syftet med övervakningen är att förebygga eller förhindra brott.

Om ansökan om tillstånd görs inom en månad från det att övervakningen inleds, får övervakningen bedrivas utan tillstånd till dess att ansökningen har prövats.

Kameraövervakning efter anmälan

Kameraövervakning av vissa särskilda platser dit allmänheten har tillträde är tillåten efter endast anmälan (12–15 §§). För kameraövervakning av dessa platser krävs alltså inte något tillstånd. En övervakningskamera får efter anmälan sättas upp i en banklokal, en lokal hos ett kreditmarknadsföretag eller ett postkontor eller i området omedelbart utanför in- och utgångar till en sådan lokal. Detsamma gäller vid uttagsautomater eller liknande anordningar. Vidare får en övervakningskamera sättas upp efter anmälan i en butikslokal eller i en yta i en butikslokal där det bedrivs bankverksamhet genom ombud eller postverksamhet. Motsvarande gäller för kameraövervakning i en tunnelbanevagn eller av en tunnelbanestation samt i parkeringshus.

Kameraövervakning efter anmälan är dock bara tillåten om vissa särskilt angivna förutsättningar är uppfyllda. Till exempel måste kameraövervakningen ha till enda syfte att förebygga, avslöja eller utreda brott eller, vad gäller övervakning i en tunnelbanevagn eller av en tunnelbanestation, att förhindra olyckor eller begränsa verkningarna av en olycka. För butiker krävs vidare bl.a. att den som avser att bedriva övervakning har ingått en skriftlig överenskommelse om övervakningen med skyddsombudet, skyddskommittén eller en organisation som företräder de anställda på arbetsplatsen.

Ansökan och beslut om tillstånd

En ansökan om tillstånd till kameraövervakning ska göras hos länsstyrelsen i det län där övervakningen ska ske (16 §). En ansökan ska innehålla vissa uppgifter, bl.a. om vem ska bedriva kameraövervakningen, ändamålen med övervakningen och det område som kan övervakas (17 §). Om övervakningen avser en arbetsplats, ska ett yttrande från skyddsombudet, skyddskommittén, eller en organisation som företräder de anställda på arbetsplatsen lämnas in tillsammans med ansökan. Innan länsstyrelsen beslutar om tillstånd till kameraövervakning ska den kommun där övervakningen ska ske få tillfälle att yttra sig, om det inte är onödigt (18 §).

Ett tillstånd ska förenas med villkor om hur kameraövervakningen får anordnas (19 §). Villkoren ska avse övervakningens ändamål, den utrustning som får användas och det område som får övervakas. Länsstyrelsen ska också besluta om de övriga villkor som behövs för tillståndet. Sådana villkor får avse upplysningar om övervakningen, upptagning, användning, bevarande eller annan behandling av bilder, avlyssning eller upptagning av ljud samt andra förhållanden som har betydelse för att skydda enskildas personliga integritet. Ett tillstånd får meddelas för en begränsad tid.

Om förutsättningarna för ett tillstånd ändras, får länsstyrelsen besluta om nya villkor eller, om förutsättningarna för tillstånd inte längre uppfylls, återkalla tillståndet (20 §).

Anmälan

En anmälan om kameraövervakning ska göras hos länsstyrelsen i det län där kameraövervakningen ska ske (21 §). Anmälan ska innehålla vissa uppgifter, bl.a. om vem som ska bedriva kameraövervakningen, i vilken typ av verksamhet som övervakningen ska förekomma samt huruvida bilder ska spelas in och bevaras.

Om de förhållanden som har redovisats i en anmälan ändras, ska länsstyrelsen underrättas om förändringen.

3.3.4 Kameraövervakning av platser dit allmänheten inte har tillträde

För kameraövervakning av platser dit allmänheten inte har tillträde krävs varken tillstånd eller anmälan. Däremot gäller lagen i övrigt även vid sådan övervakning. Den som planerar att bedriva kameraövervakning av en plats dit allmänheten inte har tillträde måste därför bl.a. se till att övervakningen uppfyller lagens allmänna krav för kameraövervakning (7 §).

Kameraövervakning av en plats dit allmänheten inte har tillträde är tillåten i två olika situationer. För det första får sådan övervakning bedrivas, om den som ska övervakas har samtyckt till det (22 §). Med samtycke avses varje slag av frivillig, särskild och otvetydig viljeyttring genom vilken någon efter att ha fått information godtar att bli kameraövervakad (2 §). Samtycket behöver inte vara skriftligt. Den övervakade har rätt att när som helst återkalla samtycket. Om ett samtycke återkallas, får ytterligare övervakning inte ske. För det andra får sådan kameraövervakning bedrivas utan samtycke, om övervakningen behövs för att förebygga, avslöja eller utreda brott, förhindra olyckor eller för andra berättigade ändamål och övervakningsintresset väger tyngre än den enskildes intresse av att inte bli övervakad (23 §). Vid denna bedömning ska särskilt beaktas hur övervakningen ska utföras, om teknik som främjar skyddet av den enskildes personliga integritet används och vilket område som ska övervakas. Exempel på andra berättigade ändamål är skolors arbete med att förebygga och förhindra kränkningar av elever samt tillverkningsföretags kontroll av produktionsprocesser (prop. 2012/13:115 s. 154).

Den som bedriver kameraövervakning av en plats dit allmänheten inte har tillträde ska se till att övervakningen endast sker för särskilda och berättigade ändamål, att ändamålen med övervakningen dokumenteras och att övervakningen inte sker i större omfattning än vad som behövs för att tillgodose ändamålen (24 §). Dessa krav gäller övervakning i båda de situationer som beskrivits ovan.

3.3.5 Upplysningsplikt

Vid all kameraövervakning enligt kameraövervakningslagen, oavsett platsen för övervakningen, gäller som huvudregel en upplysningsplikt. Upplysning om kameraövervakning ska lämnas genom tydlig skyltning eller på något annat verksamt sätt (25 §). Upplysning ska också lämnas om vem som bedriver kameraövervakningen, om detta inte framgår av förhållandena på platsen. Om ljud kan avlyssnas eller tas upp vid övervakningen, ska det lämnas en särskild upplysning om detta. Upplysningsplikten inträder när övervakningsutrustningen sätts upp. Den som bedriver övervakningen ska på begäran även informera den övervakade om ändamålet med övervakningen (26 §).

I vissa fall behöver det inte lämnas någon upplysning om kameraövervakningen (27 §). Det gäller vid övervakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning, vid övervakning till skydd för vissa skyddsobjekt och vid viss övervakning som bedrivs av räddningsledare. Det behöver inte heller lämnas någon upplysning vid sådan övervakning som Försvarsmakten bedriver från fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan övervakning. Det finns också en möjlighet för länsstyrelsen att medge undantag från upplysningsplikten, om det finns synnerliga skäl. Undantagen från upplysningsplikten gäller dock inte övervakning som omfattar avlyssning eller upptagning av ljud.

3.3.6 Behandling av bild- och ljudmaterial från kameraövervakning och överföring till tredjeland

Kameraövervakningslagen innehåller ett antal bestämmelser som närmare reglerar hur bild- och ljudmaterial från kameraövervakning får behandlas. Flera av bestämmelserna motsvarar bestämmelser i personuppgiftslagen.

Bestämmelserna innebär att den som bedriver kameraövervakning inte får behandla bild- och ljudmaterial från övervakningen för något ändamål som är oförenligt med det som materialet samlades in för (28 §). Dessutom får tillgång till bild- och ljudmaterial från kameraövervakning inte ges till fler personer än vad som behövs för att övervakningen ska kunna bedrivas (29 §).

Vidare ska den som bedriver kameraövervakning vidta lämpliga tekniska och organisatoriska åtgärder för att skydda bild- och ljudmaterialet (30 §). Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, kostnaden för åtgärderna, de särskilda risker som finns med behandlingen av materialet och hur känsligt materialet är. Det regleras också vad som gäller när någon bedriver kameraövervakning för någon annans räkning (31 §).

Dessutom regleras hur länge bild- och ljudmaterial från kameraövervakning får bevaras (32 §). Material från kameraövervakning av en plats dit allmänheten har tillträde får bevaras under högst två månader, om inte länsstyrelsen beslutar om en längre bevarandetid. Material från övervakning av en plats dit allmänheten saknar tillträde får inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med övervakningen. Normalt bör materialet inte behöva bevaras under längre tid än vid övervakning av platser dit allmänheten har tillträde, dvs. högst två månader (prop. 2012/13:115 s. 124). När bild- eller ljudmaterial inte längre får bevaras ska det omedelbart förstöras. Om bild- eller ljudmaterial från kameraövervakning används i någon annan verksamhet hos den som bedriver kameraövervakningen, ska dock i stället regleringen i personuppgiftslagen eller annan författning som gäller för behandling av personuppgifter i den verksamheten, exempelvis polisdatalagen, tillämpas (33 §).

I kameraövervakningslagen anges också under vilka förutsättningar det är tillåtet att till tredjeland föra över bild- och ljudmaterial från kameraövervakning som innehåller personuppgifter (34–36 §§).

3.3.7 Tystnadsplikt och utlämnande av uppgifter

I kameraövervakningslagen finns en bestämmelse om tystnadsplikt och utlämnande av uppgifter (37 §). I bestämmelsen anges att den som tar befattning med en uppgift som har inhämtats genom kameraövervakning inte obehörigen får röja eller utnyttja det som han eller hon på detta sätt har fått veta om någon enskilds personliga förhållanden. För det allmännas verksamhet hänvisas i stället till bestämmelserna i offentlighets- och sekretesslagen (2009:400).

3.3.8 Tillsyn

Datainspektionen har det centrala ansvaret för tillsyn enligt kameraövervakningslagen och utövar dessutom den operativa tillsynen över kameraövervakning av platser dit allmänheten inte har tillträde (38 och 40 §§ samt 1 § kameraövervakningsförordningen [2013:463]). I Datainspektionens centrala tillsynsansvar ingår bl.a. att utvärdera rättstillämpningen och ge råd och stöd till länsstyrelserna. Dessa utövar den operativa tillsynen över kameraövervakning av platser dit allmänheten har tillträde och ska se till att tillståndskravet och anmälningsplikten för uppsatta övervakningskameror som inte har tagits i bruk följs (39 §).

Tillsynsmyndigheterna får inom ramen för sin tillsynsverksamhet meddela förelägganden, som får förenas med vite (41 och 42 §§). Tillsynsmyndigheterna har också rätt att för tillsynen få tillträde till kontrollrum och andra delar av en övervakningsanläggning. Polismyndigheten är skyldig att på begäran lämna den handräckning som tillsynsmyndigheterna behöver för att få tillträde. Den som bedriver kameraövervakning eller som för någon annans räkning har hand om övervakningen ska lämna de upplysningar som tillsynsmyndigheterna begär. Tillsynsmyndigheterna har också rätt att få tillgång till och granska bild- eller ljudmaterial (43 §).

3.3.9 Skadestånd, straff och överklagande, m.m.

Enligt kameraövervakningslagen ska den som bedriver kameraövervakning ersätta den övervakade för skada och kränkning av den personliga integriteten som kameraövervakning i strid med lagen har orsakat (44 §). Ersättningsskyldigheten kan jämkas i den utsträckning det är skäligt, om den som har bedrivit övervakningen visar att felet inte berodde på honom eller henne.

Lagen innehåller också bestämmelser om straff vid vissa överträdelser av lagen. Den som uppsåtligen eller av oaktsamhet bryter mot exempelvis någon av bestämmelserna om tillståndsplikt, anmälningsplikt eller upplysningsplikt döms till böter eller fängelse i högst ett år (45 §). Detsamma gäller den som bryter mot villkor i ett tillståndsbeslut. I ringa fall döms dock inte till ansvar. Övervakningsutrustning som har använts vid brott enligt lagen kan förklaras förverkad (46 §).

Tillsynsmyndigheternas beslut enligt lagen får överklagas till allmän förvaltningsdomstol. Datainspektionen har rätt att överklaga ett beslut om kameraövervakning av en plats dit allmänheten har tillträde. I vissa fall får beslut också överklagas av den kommun där övervakningen ska ske eller, om kameraövervakningen ska avse en arbetsplats, av en organisation som företräder de anställda på arbetsplatsen (47 § samt 3 § kameraövervakningsförordningen). Tillsynsmyndigheterna får bestämma att deras beslut ska gälla omedelbart (48 §).

I lagens avslutande bestämmelse lämnas ett bemyndigande som avser avgifter för ansökan om tillstånd och anmälan (49 §).

3.3.10 Särskild lagstiftning om kameraövervakning i Danmark och Norge

Viss särskild lagstiftning om kameraövervakning finns i våra nordiska grannländer Danmark och Norge. I Finland saknas särskild lagstiftning på området.

I Danmark finns en lov om tv-overvågning. Lagen har en huvudregel som innebär att andra än myndigheter inte får bedriva tv-overvågning av gator, vägar, platser och liknande områden. I lagen definieras tv-overvågning som ”vedvarende eller regelmæssigt gentagen personovervågning ved hjælp af fjernbetjent eller automatisk

virkende tv-kamera, fotografiapparat eller lignende apparat". På svenska motsvarar definitionen närmast "varaktig eller regelmässigt upprepad personövervakning med hjälp av fjärrstyrd eller automatiskt verkande TV-kamera, fotografiapparat eller liknande apparat".

I Norge finns i loven om behandling av personopplysninger ett särskilt kapitel med bestämmelser om kameraovervåking. Med kameraovervåking avses "vedvarende eller regelmessig gjentatt personovervåking ved hjelp av fjernbetjent eller automatisk virkende overvåkningskamera eller annet lignende utstyr som er fastmontert". På svenska motsvarar definitionen närmast "varaktig eller regelmässigt upprepad personövervakning med hjälp av fjärrstyrd eller automatiskt verkande övervakningskamera eller annan liknande utrustning som är fast monterad". Huvudregeln är att samma bestämmelser som vid annan personuppgiftsbehandling gäller med vissa preciseringar och tilläggsvillkor.

Det är för närvarande inte känt om och hur dessa regleringar i Danmark och Norge kommer att ändras till följd av EU:s nya dataskyddsreglering.

4 Syften med och effekter av kameraövervakning

4.1 Inledning

Kameraövervakning har många användningsområden både i offentliga och i privata miljöer. Förekomsten av kameror och användningen av kameror ökar också snabbt i samhället. Inte minst har teknikutvecklingen inneburit att kameror har blivit en självklar del av varje mobiltelefon. Ett annat exempel är användningen av kamerautrustade drönare, som har blivit allt vanligare på senare tid. Tekniken har många potentiella användningsområden inom både offentlig och kommersiell verksamhet. Några viktiga exempel är inom jord- och skogsbruk, för jakt, för räddningsarbete och för undersökningar, inspektioner och tillsynsarbeten av olika slag. Även inom tjänsteindustrin har tekniken stor potential.

På allmänna platser är ett av de viktigaste syftena med kameraövervakning fortfarande brottsbekämpning. I de följande avsnitten diskuteras särskilt kameraövervakning som brottsbekämpande åtgärd och allmänhetens inställning till kameraövervakning i det syftet.

4.2 Kameraövervakning som brottsbekämpande åtgärd

4.2.1 Allmänt om brottsbekämpande effekter av kameraövervakning

De åtgärder som kan vidtas för att förebygga brott delas ibland in i situationella respektive sociala åtgärder. Med situationella åtgärder avses brottsförebyggande arbete som riktas mot situationen som sådan och som exempelvis ska öka upptäcktsrisken, göra brotten

svårare att utföra eller minska utbytet av brotten. Sociala brottsförebyggande åtgärder är åtgärder, ofta långsiktiga, som ska minska individers benägenhet att begå brott. Kameraövervakning är enligt denna uppdelning att betrakta som en situationell åtgärd, liksom exempelvis belysning eller andra fysiska förändringar i miljön.

Kameraövervakning kan förebygga brott på flera sätt. Kameraövervakning kan fungera direkt avskräckande genom att potentiella gärningsmän bedömer upptäcktsrisken som större i kameraövervakade områden. I sådana fall är det alltså risken att bli upptäckt, antingen på bar gärning eller i efterhand på en inspelning, som avskräcker från att begå brott. Forskning tyder på att den avskräckande effekten av kameraövervakning är störst när det gäller planerade brott, framför allt olika typer av egendomsbrott som inbrott, stöld och skadegörelse. När det gäller mer impulsiva brott som exempelvis våldsbrott tycks kameraövervakning inte ha någon större avskräckande effekt.

I de fall där kamerabilder övervakas i realtid finns vidare möjligheter för polisen eller andra aktörer att ingripa för att avstyra förestående eller avbryta pågående brottslighet. När polisen kan följa utvecklingen på utsatta platser på distans kan polisingripanden också bättre förberedas och anpassas till den rådande situationen. Att ingripanden i förväg kan anpassas till aktuella förhållanden på platsen kan bidra både till minskad risk för hot och våld mot polismän och till minskat behov av polisiär våldsanvändning.

Inspelat bild- och ljudmaterial från kameraövervakning kan också användas i brottsutredningar och i rättegångar i domstol. Att brottslighet kan utredas och lagföras med hjälp av kamerabilder bidrar i förlängningen till att straffsystemet som sådant får avsedd generell brottsavhållande verkan.

Slutligen kan kameraövervakning skapa en positiv utveckling i det övervakade området. Övervakningen kan bidra till att öka människors trygghetskänsla och leda till att fler människor vistas där. På så sätt kan den informella sociala kontrollen förstärkas, vilket i sin tur kan minska brottsligheten.

I det följande redovisas fyra undersökningar som gäller kameraövervakningens brottsförebyggande effekter. I betänkandet *En ny kameraövervakningslag* (SOU 2009:87, s. 101 ff.) finns sammanfattningar av ytterligare några undersökningar.

Avslutningsvis ska framhållas att kameraövervakning samtidigt medför effekter för människors integritet. En avvägning mellan intresset av kameraövervakning och integritetsintresset måste därför göras i det enskilda fallet.

4.2.2 Brottsförebyggande rådets rapport 2007 – Kameraövervakning och brottsprevention

Brottsförebyggande rådet lät för ett antal år sedan göra en systematisk och omfattande genomgång av den befintliga internationella forskningen om brottsförebyggande effekter av kameraövervakning. Genomgången publicerades i en rapport 2007 *Kameraövervakning och brottsprevention* (Brå 2007:29).

Genomgången visade att kameraövervakning totalt sett ledde till en viss minskning av antalet anmälda brott. Brottsligheten minskade i genomsnitt med 16 procent i kameraövervakade områden jämfört med kontrollområden där kameror inte användes. Brottsligheten tycktes i huvudsak inte heller ha omfördelats till andra platser på grund av kameraövervakningen.

Av genomgången framgick samtidigt att kameraövervakning som brottsförebyggande åtgärd hade varierande effekter beroende på platsen för övervakningen. I vissa fall var effekten mycket god och i andra fall var effekten osäker.

Störst brottsförebyggande effekt hade kameraövervakning på parkeringsplatser. Där sjönk brottsligheten med 51 procent jämfört med kontrollområden där kameraövervakning inte användes.

I stadskärnor i städer och stora tätorter ledde kameraövervakning till en liten men inte signifikant minskning av brottsligheten. Antalet brott i de kameraövervakade områdena minskade med sju procent jämfört med kontrollområdena. I flera fall fanns belägg för att omfördelning av brottsligheten inte förekommit.

Vad gällde utsatta bostadsområden ledde kameraövervakning till en liten men inte signifikant minskning av brottsligheten. Brottsligheten sjönk med sju procent jämfört med kontrollområdena.

I kollektivtrafiken ledde kameraövervakning till en ganska stor men inte signifikant minskning av brottsligheten. Brottsligheten minskade med 23 procent jämfört med kontrollområdena.

Slutligen visade genomgången att kameraövervakning tycktes fungera bättre mot egendomsbrott eller planerade brott än mot mer impulsiva brott.

4.2.3 Rapport till Expertgruppen för studier i offentlig ekonomi – Verksamma insatser mot brott?

Inledning

Expertgruppen för studier i offentlig ekonomi (ESO) gav docent Mikael Priks i uppdrag att ur ett nationalekonomiskt perspektiv beskriva effekten av åtgärder inom det rättspolitiska området. I rapporten *Verksamma insatser mot brott? En ESO-rapport om orsak och verkan* (ESO 2015:4), som publicerades 2015, redovisades två svenska undersökningar av effekten av kameraövervakning. Den första undersökningen gällde effekten av kameraövervakning i Stockholms tunnelbana och den andra undersökningen gällde effekten av kameraövervakning avseende incidenter med inkastade föremål inne på allsvenska fotbollsarenor.

Kameraövervakning i Stockholms tunnelbana

Från 2006 till 2008 installerades övervakningskameror på 100 tunnelbanestationer. Installationerna skedde vid olika tillfällen, berodde inte på tidigare brottslighet vid de olika stationerna och var inte koordinerade med andra brottsförebyggande åtgärder. Det gick därför att studera den potentiellt avskräckande effekten av övervakningskamerorna. Undersökningen visade inte några avskräckande effekter av kameraövervakning i tunnelbanesystemet som helhet. Däremot fanns det enligt undersökningen stora effekter i innerstaden där brottsligheten minskade vid 15 av 19 stationer, ökade vid tre stationer och var opåverkad vid en station. Planerade brott som fickstölder och rån minskade men däremot inte narkotikabrott och våldsbrott. Fickstölder minskade med ca 20 procent och rån med ca 60 procent. Brottsligheten minskade på de stationer där kameror var installerade och minskade inte på närliggande stationer utan kameror. Vidare visade undersökningen att brottsligheten utanför

stationerna ökade med ca 15 procent av den minskning som skedde inne på stationerna.

Kameraövervakning av allsvenska fotbollsarenor

Undersökningen omfattade tiden 1999–2005. Kamerorna installerades relativt slumpmässigt på olika allsvenska fotbollsarenor. Undersökningen visade att antalet incidenter med inkastade föremål på spelplanen minskade drastiskt direkt efter införandet av kameraövervakningen. Matcher där kameror fanns hade i genomsnitt 65 procent färre incidenter än matcher utan kameror. Förändringen skedde exakt vid tidpunkten för införandet av kameraövervakningen, vilket enligt forskaren som gjorde undersökningen talade för att kamerorna hade en omedelbar avskräckande effekt. Det fanns inte något stöd för att våldet hade förflyttats till områdena utanför arenorna.

4.2.4 Brottsförebyggande rådets slutrapport 2015 – Kameraövervakning på Stureplan och Medborgarplatsen

Sommaren 2012 inleddes ett treårigt försök med kameraövervakning på och omkring Stureplan och Medborgarplatsen i Stockholm. Platserna är populära mötesplatser med hög krogtäthet. De är också två av de mest våldsdrabbade platserna i landet. Övervakningen utfördes av polisen.

Brå utvärderade, efter förfrågan från dåvarande Polismyndigheten i Stockholms län, kameraövervakningen under försöksperioden. Inget av de tidigare projekt med kameraövervakning i Sverige som utvärderats av Brå hade varit så omfattande och haft samma förutsättningar, t.ex. vad gällde aktiv övervakning, som detta projekt. Utvärderingen presenterades i tre delrapporter, en efter varje år som kamerorna varit i bruk. Framställningen i detta avsnitt baseras i huvudsak på den tredje och avslutande rapporten *Kameraövervakning på Stureplan och Medborgarplatsen*, som publicerades 2015 (Brå 2015:21).

Kameraövervakningen hade bedrivits med sju kameror vid Stureplan, som varit aktiva mellan kl. 23 och kl. 06, och nio kameror

vid Medborgarplatsen, som varit aktiva mellan kl. 21 och kl. 05. Under helgerna hade kamerabilderna styrts och övervakats i realtid av en särskild kameraoperatör hos polisen, vilket medfört att brott avstyrts och förhindrats i samband med att situationerna uppstått.

För att kunna jämföra brottsutvecklingen vid Stureplan och Medborgarplatsen med brottsutvecklingen vid andra platser valdes fem kontrollområden ut. Områdena hade likheter med Stureplan och Medborgarplatsen på så sätt att relativt många våldsbrott anmäldes där under kvällar och nätter. Vidare fanns det ett relativt stort antal kvällsöppna barer och restauranger i kontrollområdena. Kontrollområdena var dock långt ifrån lika brottsbelastade.

Utvärderingen visade att antalet anmälda brott mot person minskade under den period som områdena kameraövervakades. Minskningen skedde framför allt under de tider på dygnet då kamerorna var bemannade, alltså helgkvällar. Under dessa tider minskade de anmälda brotten med ca 27 procent vid Medborgarplatsen och ca 17 procent vid Stureplan under uppföljningsperioden. Under tiderna när kamerorna varit i gång men inte bemannade hade minskningen vid Medborgarplatsen varit nästan lika stor som under de tider då kamerorna varit bemannade.

När brottsutvecklingen vid Stureplan och Medborgarplatsen sattes i relation till brottsutvecklingen i kontrollområdena framkom dock att den anmälda brottsligheten minskat på liknande sätt i de senare områdena. Enligt Brå var det mot den bakgrunden inte rimligt att göra bedömningen att det var kameraövervakningen som bidragit till minskningen av antalet anmälda brott vid Stureplan och Medborgarplatsen. Det var endast sexualbrott som minskade i större utsträckning vid de kameröverv akade platserna jämfört med kontrollområdena. Sexualbrotten var dock så få att det enligt Brå var svårt att dra några säkra slutsatser om huruvida detta berodde på kameraövervakningen eller inte.

Vidare visade dokumentation från polisens kameraoperatörer att kamerorna kommit till användning varje helg. Med hjälp av kamerorna hade polisen vid flera tillfällen avbrutit potentiella våldsbrott, uppmärksammat andra typer av brottslighet, exempelvis fickstölder, och initierat omhändertaganden av berusade personer. Polisen hade också uppmärksammat personer som varit misstänkta för vålds-, narkotika- eller tillgreppsbrott. Hur stor den brottsförebyggande effekten var när det gäller denna typ av aktiv användning av kamerorna

var dock enligt Brå svårt att avgöra, eftersom det inte gick att säga hur situationen skulle ha utvecklats utan polisens ingripande. Poliserna i yttre tjänst upplevde att kamerorna varit till stor nytta då de bidragit med en överblick som annars varit svår att få.

Utvärderingen visade vidare att inspelat material från kameraövervakningen hade begärts in i 218 brottsutredningar under de studerade perioderna, vilket motsvarade ungefär en femtedel av de anmälda brotten på platserna. I 45 fall var materialet användbart i brottsutredningen och i 21 fall väcktes åtal. I åtta fall hade materialet särskild betydelse för den rättsliga uppklarningen. I sju av dessa blev domen fällande och i det åttonde fallet ogillades åtalet på grund av nödvärn.

Utvärderingen visade inga större förändringar när det gällde hur trygga platserna upplevdes efter det att kamerorna satts upp. Andelen som kände sig otrygga och oroliga för att utsättas för våld vid platserna hade inte minskat när projektet varit i gång ett år. Både vid Stureplan och vid Medborgarplatsen var det ca 20 procent av de boende som upplevde otrygghet i det egna området vid de två mättillfällena. Information om kameraövervakningen hade dock inte nått alla besökare. Vid det andra mättillfället var det en ganska stor del av de besökande som inte kände till att platserna kameraövervakades, trots att platserna då hade varit kameraövervakade i ett år. Detta kan ha haft betydelse för de uteblivna resultaten när det gäller trygghet och oro för brott vid platserna.

I sin summerande bedömning konstaterade Brå att kamerornas effekt sammantaget tycktes vara begränsad. Eventuellt skulle nyttan kunnat förstärkas av till exempel effektivare arbetsmetoder, fler kameraoperatörer eller bättre kameror.

4.3 Allmänhetens inställning till kameraövervakning

4.3.1 Inledning

Ett av de viktigaste syftena med kameraövervakning är att förebygga brott. Samtidigt medför användningen av kameraövervakning en risk för intrång i den personliga integriteten. Regleringen om kameraövervakning har till syfte att säkerställa att det ena intresset på ett välbalanserat sätt vägs mot det andra. En betydelsefull aspekt vid denna avvägning är människors inställning till kamera-

övervakning och hur man upplever kamerorna. Nedan återges översiktligt två undersökningar om allmänhetens inställning till kameraövervakning. Generellt kan här sägas att kameraövervakning har blivit allt vanligare i Sverige och att de flesta svenskar är positiva till kameraövervakning i brottsförebyggande syfte på offentliga platser såsom torg, parkeringar och butiker men mindre positiva när det gäller mer personliga och integritetskänsliga platser. Attityden till kameraövervakning är överlag mer positiv i Sverige och t.ex. Storbritannien än i många andra länder. Den positiva inställningen har ökat efter hand.

I sammanhanget kan det vara värt att notera att det inte finns någon allmängiltig definition av begreppet personlig integritet i svensk lagstiftning. Detta trots att begreppet används i både grundlag och vanlig lag (se t.ex. 2 kap. 6 § andra stycket regeringsformen och 1 § kameraövervakningslagen [2013:460]). I ett försök att beskriva vad som kan anses vara kärnan i rätten till personlig integritet har lagstiftaren uttalat att kränkningar av den personliga integriteten utgör intrång i den fredade sfär som den enskilde bör vara tillförsäkrad och där ett oönskat intrång bör kunna avvisas (se bl.a. prop. 2009/10:80 s. 175).

4.3.2 Integritetsskyddskommitténs enkätundersökning 2006

På uppdrag av Integritetsskyddskommittén genomförde Statistiska centralbyrån under 2006 en enkätundersökning i syfte att få en ungefärlig uppfattning om allmänhetens inställning till behovet av skydd för den personliga integriteten, särskilt när detta behov kommer i konflikt med andra behjärtansvärda intressen (SOU 2007:22, bilaga 4).

Undersökningen visade en starkt positiv inställning till kameraövervakning på allmän plats för att förebygga brott. Attityderna var i stora drag lika oavsett kön och ålder. Hela 97 procent av de tillfrågade ansåg att kameraövervakning ska vara tillåten på allmän plats, om det behövs för att förhindra grov brottslighet som misshandel, rån, våldtäkt och narkotikalangning. Även när det gällde mindre allvarlig brottslighet som klotter, skadegörelse och snatteri ansåg en stor majoritet, 87 procent, att kameraövervakning ska vara tillåten på allmän plats, om det behövs för att förhindra eller avslöja

sådana brott. Så många som 71 procent av de tillfrågade ansåg att kameraövervakning ska vara tillåten på allmän plats, om det behövs för att minska antalet hastighetsöverträdelser i trafiken. En mycket stor majoritet, 90 procent, accepterade kameraövervakning också när det behövs för att folk ska känna sig tryggare.

De tillfrågade fick också svara på hur de skulle uppleva att bli filmade när de besökte en familj i vars bostad övervakningskameror placerats i syfte att skydda mot inbrott. Endast åtta procent ansåg att det skulle vara så obehagligt att de inte skulle komma på besök någon mer gång. Många, 42 procent, ansåg att det skulle vara en aning obehagligt men inte så mycket att det skulle påverka deras beteende, 27 procent menade att det var något man måste vänja sig vid i dagens samhälle och 25 procent ansåg att det inte skulle vara obehagligt överhuvudtaget.

4.3.3 Datainspektionens rapport Ungdomar och integritet 2011

Datainspektionen har vid ett flertal tillfällen låtit göra undersökningar av ungdomars inställning till integritet. Med ungdomar avses personer i åldern 15–18 år. Den senaste publicerades i rapporten *Ungdomar och integritet 2011* (Datainspektionens rapport 2011:1).

En slutsats som drogs av undersökningen var att den mest accepterade formen av övervakning var kameraövervakning, vilken unga tolererade i högre utsträckning än telefonavlyssning och övervakning på Internet. Så många som 85 procent av ungdomarna ansåg att kameraövervakning kan accepteras, om syftet är att förhindra grova brott. Acceptansen för kameraövervakning för att förhindra mindre allvarliga brott såsom klotter och snatteri var också hög. Vidare accepterade ungdomar i stor utsträckning kameraövervakning på torg, i kollektivtrafiken och i butiker. Hälften accepterade kameraövervakning på restauranger. Däremot var ungdomarna negativa till övervakningskameror i bl.a. klassrum och uppehållsrum i skolan. Hela 72 procent kunde acceptera kameraövervakning, om den får människor att känna sig tryggare.

5 Tillämpningen av kameraövervakningslagen

5.1 Utredningens kartläggning

I utredningens uppdrag har ingått att kartlägga och utvärdera vad kameraövervakningslagen (2013:460) har inneburit för möjligheterna till kameraövervakning och skyddet för den personliga integriteten. Utredningen har också haft i uppdrag att utvärdera Datainspektionens centrala tillsynsansvar genom att bl.a. undersöka om länsstyrelsernas rättstillämpning har blivit mer enhetlig. Vidare har utredningen enligt uppdraget undersökt hur lagens tillämpningsområde förhåller sig till användning av ny teknik, såsom t.ex. kamerautrustade drönare, med beaktande av det pågående arbetet med att ta fram ett EU-gemensamt regelverk för drönare.

Som ett led i fullgörandet av uppdraget har utredningen genomfört två enkätundersökningar. Den ena enkäten har riktat sig till samtliga länsstyrelser och den andra till Datainspektionen. I huvudsak har enkäten till Datainspektionen innehållit samma frågor som enkäten till länsstyrelserna. Resultaten av enkätundersökningarna redovisas i avsnitt 5.2.

Utredningen har även haft ett flertal möten med olika aktörer som på olika sätt berörs av kameraövervakningslagstiftningen. Vad som framkommit vid vissa av dessa externa kontakter redovisas i avsnitt 5.3.

I avsnitt 5.4 behandlas vissa frågor om kamerautrustade drönare och ny teknik.

Avslutningsvis innehåller avsnitt 5.5 vissa sammanfattande slutsatser av kartläggningen och av de synpunkter som framkommit vid de externa kontakterna.

5.2 Enkätundersökningarna

5.2.1 Enkäten till länsstyrelserna

Inledning

Utredningen har tillställt samtliga länsstyrelser en enkät där länsstyrelserna bl.a. har ombetts att ange antal tillstånd och anmälningar till kameraövervakning som fanns i länet den 1 januari 2013 respektive den 1 januari 2016. Länsstyrelserna har även ombetts svara på ett antal frågor rörande tillämpningen och utformningen av kameraövervakningslagen.

Det ska inledningsvis påpekas att ett flertal länsstyrelser inte har haft möjlighet att svara på alla frågor i enkäten. Det gäller särskilt frågorna om antalet tillstånd och anmälningar och hur dessa fördelar sig på olika övervakningsobjekt. Anledningen till detta är enligt de berörda länsstyrelserna att de inte har ärendena registrerade på sådant sätt att uppgifter kan lämnas eller att de saknar uppdaterade register. Det har därmed inte varit möjligt att sammanställa någon närmare statistik över antalet tillstånd och anmälningar och hur dessa fördelar sig på olika övervakningsobjekt. Det kan i sammanhanget nämnas att någon länsstyrelse har påtalat att det borde finnas krav på ett register, kanske nationellt, över tillstånd och anmälningar.

Av de uppgifter som har lämnats från länsstyrelserna kan följande trender urskiljas. Både antalet tillstånd och antalet anmälningar om kameraövervakning ökade mellan den 1 januari 2013 och den 1 januari 2016. Ökningen av antalet anmälningar var större än ökningen av antalet tillstånd. Länsstyrelserna avgjorde 1 115 ärenden om tillstånd till kameraövervakning under 2012. Under 2015 var motsvarande siffra 907, en minskning av andelen avgjorda tillståndsansökningar med ca 19 procent. Av svaren framgår också att relativt få ansökningar om tillstånd avslogs. Det var också relativt få av länsstyrelsernas beslut som överklagades till domstol. Däremot ändrades en förhållandevis hög andel av de beslut som överklagades till domstol.

Förändringar i och med införandet av kameraövervakningslagen

I kameraövervakningslagen anges, till skillnad mot vad som gällde enligt tidigare lagstiftning, uttryckligen att behovet av kameraövervakning för att avslöja eller utreda brott ska beaktas vid bedömningen av övervakningsintresset vid tillståndsprövningen. I enkäten ställdes frågan om detta förtydligande i lagtexten har medfört någon förändring i praktiken.

Enligt majoriteten av länsstyrelserna har förtydligandet inte medfört någon förändring i praktiken. Några länsstyrelser har dock framhållit att det nu finns uttryckligt stöd i lagstiftningen för att beakta och ta hänsyn till om kameraövervakningen behövs för att avslöja och utreda brott, vilket framför allt kan ha betydelse för möjligheten att bevilja tillstånd till bildinspelning.

En annan förändring i och med kameraövervakningslagen är att användning av teknik som främjar skyddet av den enskildes personliga integritet ska beaktas särskilt vid bedömningen av integritetsintresset. I enkäten ställdes frågan om denna omständighet beaktas mer än tidigare och om förändringen har lett till fler tillstånd jämfört med tiden före kameraövervakningslagen.

Enligt flertalet länsstyrelser beaktas integritetsfrämjande teknik vid tillståndsgivningen. Flera av länsstyrelserna har angett att detta också leder till att fler tillstånd kan beviljas. Länsstyrelserna har angett följande exempel på integritetsvänlig teknik.

– Digital maskering av delar av kamerornas upptagningsområde.
– Kameror som aktiveras vid larm eller avvikande beteende, rörelsemönster etc.

Vidare innebar införandet av lagen lättnader för viss kameraövervakning, bl.a. övervakning i parkeringshus och tunnelbana samt viss övervakning i butiker, genom att tillståndsplikten ersattes med anmälningsplikt. I enkäten ställdes frågan om denna ändring påverkat antalet övervakade objekt och på vilket sätt. Enligt de flesta länsstyrelser har ändringarna gett en marginell eller inte någon effekt på antalet övervakade objekt. Några länsstyrelser har dock uppgett att antalet anmälningar ökat. Någon länsstyrelse har i detta sammanhang framhållit att kameraövervakning i syfte att kontrollera registreringsskyltar i parkeringshus fortfarande kräver tillstånd.

Genom kameraövervakningslagen förstärktes vidare integritetsskyddet, bl.a. genom införande av starkare sekretesskydd, ökade krav på säkerhetsåtgärder och en skadeståndsbestämmelse som ger enskilda rätt till ersättning för skada och kränkning vid överträdelser av lagen. I enkäten ställdes frågan om dessa ändringar fått något genomslag och i så fall vilket. Enligt en stor majoritet av länsstyrelserna har dessa ändringar inte fått något nämnvärt genomslag.

Datainspektionens centrala tillsynsansvar

I och med kameraövervakningslagen fick Datainspektionen ett centralt tillsynsansvar i syfte att bl.a. göra länsstyrelsernas praxis mer enhetlig. I enkäten ställdes frågan om det blivit så och i vilka avseenden.

Enligt en majoritet av länsstyrelserna har Datainspektionens centrala tillsynsansvar lett till att praxis har blivit mer enhetlig. Många av länsstyrelserna har framfört att Datainspektionen har överklagat beslut i högre grad än vad Justitiekanslern, som tidigare haft rätt att överklaga beslut om tillstånd till kameraövervakning, gjort. Detta har lett till en mer utvecklad domstolspraxis. Därutöver har flera länsstyrelser framhållit betydelsen av Datainspektionens arbete med råd och anvisningar och av Datainspektionens medverkan i länsstyrelsernas samverkansgrupp för kameraövervakning.

Kameraövervakning på särskilda platser

I enkäten ombads länsstyrelserna att ange hur många ansökningar som gjordes åren 2012 respektive 2015 avseende kameraövervakning på gator och torg där ansökan gjordes av annan än polisen, t.ex. en kommun. Enligt de inkomna svaren gjordes endast fem respektive sju stycken sådana ansökningar i hela landet under de aktuella åren. Tre respektive två av ansökningarna fick helt eller delvis bifall. Ett vanligt skäl till att ansökningarna avslogs var att integritetsintresset vägde tyngre än övervakningsintresset.

I enkäten ombads länsstyrelserna vidare att ange hur många ansökningar som gjordes åren 2012 respektive 2015 avseende lokaler som användes av religiösa samfund, medieredaktioner samt asylboenden, boenden för ensamkommande barn och transitboenden.

Enligt de inkomna svaren gjordes under 2012 endast två ansökningar om tillstånd vad gällde lokaler som användes av religiösa samfund och en ansökan vad gällde medieredaktioner. En av de förstnämnda ansökningarna och ansökningen beträffande medieredaktionen bifölls. Ett skäl till den avslagna ansökningen var att sökanden inte hade visat att platsen var särskilt brottsutsatt.

Under 2015 gjordes tolv ansökningar beträffande lokaler som användes av religiösa samfund, fem ansökningar beträffande medieredaktioner och nio ansökningar beträffande asylboenden, boenden för ensamkommande barn och transitboenden. Sju av ansökningarna beträffande lokaler som användes av religiösa samfund, alla ansökningar beträffande medieredaktioner samt sex av ansökningarna beträffande asylboenden m.m. bifölls.

Slutligen ombads länsstyrelserna ange hur många ansökningar som gjordes under åren 2012 respektive 2015 avseende maskiner, arbetsbodar och liknande ute i skog och mark. Enligt de inkomna svaren gjordes endast en sådan ansökan per respektive år i hela landet. En av dessa ansökningar bifölls.

Drönare och ny teknik

I enkäten ställdes frågan om det finns svårigheter vad gäller hur kameraövervakningslagen förhåller sig till användning av ny teknik.

En stor majoritet av länsstyrelserna har uppgett att det finns sådana svårigheter. Exempelvis har flera länsstyrelser framhållit att det uppkommer tillämpningsproblem när det gäller rekvisiten ”uppsatt” och ”utan att manövreras på platsen” i lagens definition av övervakningskamera. Vidare har länsstyrelserna som exempel på ny teknik där rättsläget är oklart nämnt bärbara kameror och mobiltelefonkameror samt kameror som monteras t.ex. i bilar, s.k. dashcams, eller på cyklar.

I enkäten ombads länsstyrelserna dessutom att ange hur många ansökningar avseende kamerautrustade drönare som gjordes under åren 2012 och 2015. Enligt de inkomna svaren gjordes inte någon sådan ansökan under 2012 och fyra sådana ansökningar under 2015. Av dessa bifölls en ansökan.

Allmänt om kameraövervakningslagen

I enkäten ställdes frågan om kameraövervakningslagen allmänt sett är utformad på ett tillfredsställande sätt. Enligt en knapp majoritet av länsstyrelserna är lagen utformad på ett tillfredsställande sätt. Flera av de länsstyrelser som är kritiska mot lagens utformning har lyft fram att lagen inte är anpassad till teknikutvecklingen och att rekvisiten ”uppsatt” och ”utan att manövreras på platsen” i lagens definition av övervakningskamera är svårtillämpliga. Några länsstyrelser har uppgett att lagens uppdelning mellan olika typer av platser leder till tillämpningsproblem och att lagen upplevs som lite rörig. Även den stränga praxisen när det gäller kameraövervakning med inspelning har framhållits som svår att motivera.

I enkäten ställdes också frågan om de förändringar som infördes genom kameraövervakningslagen har haft några praktiska konsekvenser som särskilt kan lyftas fram. Några länsstyrelser har framhållit att det inneburit en förenkling att viss tillståndsplikt för kameraövervakning i butiker har ersatts med anmälningsplikt. Andra länsstyrelser har framhållit betydelsen av att Datainspektionen getts rollen som central tillsynsmyndighet.

5.2.2 Enkäten till Datainspektionen

Förändringar i och med införandet av kameraövervakningslagen

I kameraövervakningslagen anges, till skillnad mot vad som gällde enligt tidigare lagstiftning, uttryckligen att behovet av kameraövervakning för att avslöja eller utreda brott ska beaktas vid bedömningen av övervakningsintresset vid tillståndsprövningen. I enkäten ställdes frågan om detta förtydligande i lagtexten medfört någon förändring i praktiken.

Enligt Datainspektionen har förtydligandet inte inneburit någon förändring i länsstyrelsernas praxis. Däremot är det enligt Datainspektionen sannolikt så att förtydligandet uppfattas som en lättnad jämfört med vad som gällde enligt tidigare lagstiftning.

En annan förändring i och med kameraövervakningslagen är att användning av teknik som främjar skyddet av den enskildes personliga integritet ska beaktas särskilt vid bedömningen av integritetsintresset. I enkäten ställdes frågan om denna omständighet beaktas

mer än tidigare och om förändringen har lett till fler tillstånd jämfört med tiden före kameraövervakningslagen.

Enligt Datainspektionen används integritetsvänlig teknik i relativt stor utsträckning och finns det många exempel på att sådan teknik har möjliggjort att tillstånd kunnat beviljas, t.ex. vid kameraövervakning av stora områden vid bensinstationer. Att användning av integritetsvänlig teknik har lyfts fram i den gemensamma ansökningsblankett som länsstyrelserna använder sig av kan enligt Datainspektionen ha medfört att förekomsten av sådan teknik beaktas i större utsträckning än tidigare. Datainspektionen har vidare angett följande exempel på integritetsvänlig teknik.

- Kameraövervakning som aktiveras efter olika typer av larm, t.ex. larm som reagerar på onormala rörelsemönster, inbrottslarm, överfallslarm och evakueringslarm (vanligt förekommande).
- Villkor om att områden/ytor ska maskeras (vanligt förekommande).
- Aktivering av kameror vid vissa tider, t.ex. nattetid (vanligt förekommande).
- Villkor om att inte någon annan data än t.ex. om antalet människor får lämna kameran, dvs. ”ursprungsbilden” raderas omedelbart. Används t.ex. vid kameror i stadsmiljöer som har som enda syfte att räkna antal personer (inte särskilt vanligt förekommande).
- Kryptering av bildmaterial där den som övervakar inte själv har möjlighet att dekryptera materialet (förekommer sällan).
- Teknik som omedelbart raderar bilder av människor (oklart om det finns tillförlitlig sådan teknik).

Genom kameraövervakningslagen förstärktes vidare integritetsskyddet, bl.a. genom införande av starkare sekretesskydd, ökade krav på säkerhetsåtgärder och en skadeståndsbestämmelse som ger enskilda rätt till ersättning för skada och kränkning vid överträdelser av lagen. I enkäten ställdes frågan om dessa ändringar fått något genomslag och i så fall vilket.

Enligt Datainspektionen har kraven inte fått särskilt stort genomslag vid tillståndsgivningen då länsstyrelserna enligt inspektionen inte utreder och inte heller beaktar säkerhetskraven i någon större

utsträckning. Datainspektionen har vidare uppgett att inspektionen inte har någon bra bild av hur kraven på säkerhetsåtgärder efterlevs av användarna av kameraövervakning. Enligt Datainspektionen har endast ett fåtal avslagsbeslut meddelats av länsstyrelserna med motiveringen att sökanden inte uppfyller kraven på säkerhet. Inspektionen har vidare drivit ett par processer i domstol som rört säkerhet, bl.a. gällande bildöverföring över öppet nät från kameraövervakning vid olycksplatser. Datainspektionen har ännu inte erhållit eller fått kännedom om någon dom där skadestånd enligt kameraövervakningslagen har dömts ut.

Datainspektionens centrala tillsynsansvar

I och med kameraövervakningslagen fick Datainspektionen ett centralt tillsynsansvar i syfte att bl.a. göra länsstyrelsernas praxis mer enhetlig. I enkäten ställdes frågan om det blivit så och i vilka avseenden.

Enligt Datainspektionen är det tydligt att länsstyrelsernas praxis har blivit mer enhetlig sedan inspektionen fick ett centralt tillsynsansvar och tog över rätten att överklaga beslut om kameraövervakning från Justitiekanslern. Under 2013 och 2014 var det enligt Datainspektionen vanligt förekommande att inspektionen överklagade länsstyrelsernas beslut för att bedömningen inte var korrekt eller för att obligatoriska tillståndsvillkor saknades. Under 2015 och början av 2016 rörde den större delen av överklagandena frågor av mer principiell karaktär. Dessutom sjönk andelen överklagade beslut, vilket enligt Datainspektionen visar att länsstyrelsernas praxis har blivit mer enhetlig. Den ökade enhetligheten beror enligt Datainspektionen dels på arbetet med överklagandena, dels på samverkan mellan Datainspektionen och länsstyrelserna. Även en framtagen för alla länsstyrelser gemensam beslutsmall torde ha ökat enhetligheten i besluten.

Kameraövervakning på särskilda platser

I enkäten ställdes frågan om möjligheterna för andra aktörer än Polismyndigheten att kameraövervaka särskilt brottsutsatta platser är ändamålsenliga.

Datainspektionen har uppgett att även andra aktörer än Polismyndigheten kan få tillstånd till kameraövervakning med bildinspelning, om de visar att platsen är särskilt brottsutsatt. När det gäller områden som t.ex. gator och torg, där det är Polismyndigheten som har till uppgift att upprätthålla ordningen, är dock möjligheterna för andra aktörer att få tillstånd mycket små enligt rättspraxis (se bl.a. RÅ 2010 ref. 22 I). Enligt Datainspektionen är det rimligt att det är Polismyndigheten eller annan brottsbekämpande myndighet som ensam aktör som ska ha möjlighet att få tillstånd till kameraövervakning i gatumiljöer och liknande integritetskänsliga områden när det gäller övervakning för brottsförebyggande ändamål.

I enkäten ställdes vidare frågan om lagstiftningen ger ett ändamålsenligt utrymme för att ta hänsyn till hotbilder av mer generellt slag mot t.ex. lokaler som används av religiösa samfund, medieredaktioner samt asylboenden och liknande.

Datainspektionen har framhållit att det inte finns några uttalanden vare sig i lagtext eller i förarbeten som ger stöd för att det vid tillståndsprövningen skulle vara möjligt att beakta generella hotbilder eller liknande omständigheter. Däremot har det i rättspraxis pekats ut vissa typer av platser som anses generellt utsatta, t.ex. skolor, bensinstationer, domstolar och snabbmatsrestauranger. Det är enligt Datainspektionen otillfredsställande att en generell hotbild inte kan beaktas t.ex. vad gäller nyöppnade verksamheter eller verksamheter som till sin karaktär generellt sett är brottsutsatta men där någon brottslighet inte har inträffat. Det kan dock enligt inspektionen vara problematiskt att i lagstiftning lämna utrymme för att beakta en generell hotbild. Det kan t.ex. vara svårt att i lagen peka ut vilka platser som ska anses generellt utsatta eller vilka omständigheter som ska beaktas i bedömningen.

Drönare och ny teknik

I enkäten ställdes frågan om det finns svårigheter vad gäller hur kameraövervakningslagen förhåller sig till användning av ny teknik.

Datainspektionen har svarat att de grundläggande begreppen ”uppsatt” och ”utan att manövreras på platsen” i lagens definition av övervakningskamera är svåra att applicera på t.ex. rörliga objekt/plattformar. Det är enligt Datainspektionen uppenbart att kameraövervakningslagen inte är teknikneutral.

Datainspektionen har vidare anfört att tillstånd till kameraövervakning med drönare måste kunna beviljas och att detta i och för sig är möjligt med den befintliga lagstiftningen. En sökande som t.ex. har ett samhälleligt syfte med övervakningen har möjlighet att få ett generellt tillstånd till att använda sin drönare med de integritetsskyddande villkor som länsstyrelsen anser behövs.

Datainspektionen har slutligen angett bl.a. följande exempel på ny teknik där rättsläget är oklart.

– Webbkameror hos t.ex. arbetsgivare och internetcaféer samt annan utrustning för videokonferens.
– Kroppsburna kameror, t.ex. s.k. actionkameror eller mindre kameror i kavajslag.
– Kameror som används i vårdsyfte hos vårdinrättningar av olika slag, t.ex. genom realtidsövervakning av en operationssal där bilderna visas i en monitor i ett intilliggande rum.

Överklaganden av Datainspektionen

I enkäten ombads Datainspektionen att uppge hur många beslut som inspektionen har överklagat och hur många av dessa som bifallits av förvaltningsdomstolarna. Enligt Datainspektionen har inspektionen överklagat 96 beslut under 2014 och 44 beslut under 2015. I nästan samtliga av sina överklaganden sedan den 1 juli 2013 har Datainspektionen fått bifall i någon del. En stor del av överklagandena har fått fullt bifall och en mindre del av överklagandena har fått delvis bifall. Endast ett fåtal, uppskattningsvis fem, av överklagandena har enligt Datainspektionen avslagits helt.

Allmänt om kameraövervakningslagen

I enkäten ställdes frågan om kameraövervakningslagen allmänt sett är utformad på ett tillfredsställande sätt.

Datainspektionen har svarat följande. En avvägning mellan behovet av kameraövervakning och skyddet för den personliga integriteten bör i största möjliga mån göras i varje enskilt fall. Kameraövervakningslagens tillämpningsområde är väldigt teknikberoende. Lagens tillämpning tar endast hänsyn till vilken teknik som används och beaktar inte alls ändamålet med användningen av kamerorna. Många kameror som inte är ”traditionella” övervakningskameror omfattas av lagen såsom den är utformad. Enligt Datainspektionen kan det ifrågasättas om detta är tillfredsställande utifrån de många användningsområdena och den spridning som kameror har i dagens samhälle. Samtidigt måste det finnas en lag som upprätthåller skyddet för den personliga integriteten även vid användning av ”icke-traditionella” övervakningskameror.

Datainspektionen har också framhållit att den som avser att bedriva kameraövervakning på platser dit allmänheten saknar tillträde inte får något besked från en myndighet om tillåtligheten av övervakningen, om inte inspektionen utövar tillsyn på platsen. Enligt inspektionen är det beträffande dessa platser en i många fall komplex juridisk avvägning som ska göras på egen hand av den som övervakar.

5.3 Utredningens externa kontakter

Utredningen har sammanträffat med ett antal olika aktörer, bl.a. Jernhusen AB, Transportstyrelsen, Sjöräddningssällskapet, Lantbrukarnas riksförbund (LRF), Svenska Jordägareförbundet, Sveriges Television AB samt Polismyndigheten och Säkerhetspolisen. I detta avsnitt redovisas några frågor som lyfts fram av dessa aktörer. Därutöver har det förekommit kontakter med andra, t.ex. företrädare för Volvo Personvagnar AB och branschorganisationen Visita.

Jernhusen AB har särskilt betonat vikten av kameraövervakning på samhällsviktiga platser som t.ex. järnvägsstationer. Jernhusen AB har framhållit att länsstyrelserna har haft olika praxis när det gäller sådan kameraövervakning. Enligt Jernhusen AB bör en framtida kameraövervakningslagstiftning fokusera på behandlingen av film-

materialet och syftet med övervakningen i stället för på själva kamerorna.

Sjöräddningssällskapet har framhållit vikten av att kameraövervakningslagstiftningen inte omöjliggör användning av kamerautrustade drönare inom räddningsarbete. Sådan teknik kan enligt Sjöräddningssällskapet bl.a. användas för att kunna få en tidig lägesbild och för att kunna söka efter nödställda.

LRF har redovisat undersökningar om brottslighet som lantbrukare utsätts för och en studie om vad dessa anser om kameraövervakning och i vilka situationer som kameraövervakning är intressant för dem. Brottsligheten består bl.a. i stölder av fordon och maskiner samt drivmedel, som representerar stora värden. Ofta kan brottsligheten misstänkas vara organiserad med internationella förgreningar. LRF har vidare förespråkat vissa lättnader i kraven på tillstånd till kameraövervakning i kombination med att regleringen om användningen av bildmaterialet skärps, eftersom det är den användningen som kan leda till integritetsproblem. *Svenska Jordägareförbundet* har redovisat hur kamerautrustade drönare kan användas i jord- och skogsbruk och vilka stora effektivitets- och resursvinster detta innebär. Både LRF och Svenska Jordägareförbundet har betonat att användningen av kamerautrustade drönare, kameror på maskiner och s.k. åtelkameror är av mycket stor betydelse för jord- och skogsbruket samt jakt.

Sveriges Television AB har särskilt understrukit vikten av att möjligheterna att använda ny kamerateknik, som t.ex. kamerautrustade drönare, för journalistiska ändamål inte begränsas. Sådan teknik blir ett allt viktigare inslag i t.ex. nyhetsrapportering och sportsändningar.

Polismyndigheten och Säkerhetspolisen har också framhållit betydelsen av att lagstiftningen inte begränsar användningen av ny teknik på dessa myndigheters verksamhetsområden. Polismyndigheten har framfört att myndigheten inte bör omfattas av en särskild kameraövervakningslagstiftning eller i vart fall inte av ett tillståndskrav eller generellt upplysningskrav i en sådan lagstiftning. Säkerhetspolisen har framfört att en förändrad lagstiftning inte bör innebära försämringar jämfört med vad som nu gäller för myndigheten och tagit upp en specifik spaningsmetod.

5.4 Särskilt om kamerautrustade drönare och ny teknik

Kamerautrustade drönare

En drönare är ett obemannat luftfartyg som går under ett antal olika benämningar, bl.a. UAS (Unmanned Aerial Systems), RPAS (Remotely Piloted Aircraft Systems), UAV (Unmanned Aerial Vehicle) och modellflyg. I Transportstyrelsens föreskrifter (TSFS 2009:88) om verksamhet med obemannade luftfartyg (UAS) finns följande definition (1 kap. 2 §).

> System bestående av obemannat luftfartyg samt övriga komponenter som är nödvändiga för att kunna kontrollera luftfartyget på avstånd av en eller flera personer; dessa övriga komponenter kan utgöras av t.ex. kontrollstation, kommunikationslänkar och kringutrustning som är nödvändiga för att starta, flyga eller landa det obemannade luftfartyget.

En drönare är ofta utrustad med en kamera och fjärrstyrs normalt från marken eller programmeras att automatiskt flyga till en viss plats eller enligt en angiven rutt.

Användningen av kamerautrustade drönare har blivit allt vanligare under senare år. Tekniken har många förtjänstfulla användningsområden inom både offentlig och kommersiell verksamhet. Några exempel är inom räddningsarbete, byggbesiktningar, jord- och skogsbruk, journalistisk verksamhet samt för inspektioner och tillsynsarbete.

Under utredningens arbete har det framförts från flera håll att användningen av drönare har en mycket stor potential och att kameraövervakningslagstiftningen inte bör lägga onödiga hinder i vägen för detta. En stor fördel med tekniken är att den kan användas i svårtillgängliga miljöer eller på platser som är farliga för människor. En ändamålsenlig användning av tekniken kan därför bidra till effektivisering av näringsverksamheter av en mängd olika slag men också vara ett viktigt verktyg t.ex. vid eftersökning av försvunna personer. Tekniken kan vidare ha stor betydelse i arbetet för en säkrare arbetsmiljö och är dessutom fördelaktig från miljösynpunkt i de fall där alternativet är en helikopter.

Samtidigt är det så att kamerautrustade drönare kan användas på ett sätt som innebär att enskilda utsätts för integritetskränkande övervakning. Drönare kan också användas av enskilda i samband

med terrorism, sabotage, spioneri eller annan grov brottslighet samt för att röja säkerhetsskyddad verksamhet.

Kamerautrustade drönare omfattas av kameraövervakningslagen

Det har tidigare varit oklart om kameraövervakningslagen omfattar kamerautrustade drönare. Denna fråga har numera avgjorts av Högsta förvaltningsdomstolen (HFD) i en dom den 21 oktober 2016 (HFD 2016 ref. 71 I). I domen slog HFD fast att en kamera som var monterad på en drönare omfattades av kameraövervakningslagen. Målet gällde en enskild näringsidkare som hade sökt tillstånd för att efter kundbeställningar fotografera olika objekt, mestadels fastigheter, med en kamera på en drönare. Av avgörandet framgår att en kamera som monterats på en drönare kan vara uppsatt i lagens mening och att det gäller även om kameran monteras bort efter varje flygning. Enligt HFD krävs att placeringen av kameran har en viss varaktighet eller att kameran återkommande kommer att fästas på drönaren. I det fall som domstolen prövade var kameran att anse som uppsatt. I fråga om platsen för manövrering konstaterade domstolen att kameran skulle fotografera från luften men styras och även i övrigt hanteras från marken. Hanteringen bedömdes därför ske från en plats som var klart åtskild från den där kameran var uppsatt. Kameran ansågs därmed inte manövrerad på platsen. Den omfattades följaktligen av kameraövervakningslagen.

Kameraövervakningslagen bedömdes alltså vara tillämplig på den kamera som monterats på drönaren. Eftersom kameran skulle riktas mot platser dit allmänheten hade tillträde, krävdes det enligt HFD tillstånd till kameraövervakningen. Målet återförvisades till förvaltningsrätten för prövning i själva tillståndsfrågan.

Drönare kan även omfattas av annan svensk lagstiftning

Användningen av drönare aktualiserar också viktiga frågor om luftfartssäkerhet och skydd av geografisk information som styrs av andra svenska regelverk.

Luftfartslagen (2010:500) är tillämplig på alla sorters luftfartyg, även obemannade, och Transportstyrelsen har utfärdat särskilda föreskrifter om verksamhet med obemannade luftfartyg under

150 kg (TSFS 2009:88). För sådana obemannade luftfartyg som används eller är konstruerade för bl.a. forskning, kommersiella ändamål eller för att flygas utom synhåll för piloten krävs ett särskilt tillstånd från Transportstyrelsen. Detta gäller oavsett hur litet luftfartyget är. Enligt uppgift från Transportstyrelsens webbplats hade i slutet av 2016 ca 1 600 aktörer giltiga tillstånd från myndigheten att bedriva verksamhet med obemannade luftfartyg. Bland dessa finns universitet, statliga myndigheter, kommuner, mediebolag, stora och små företag inom olika näringsgrenar samt privatpersoner. Vidare krävs tillstånd från flygtrafikledningen för flygning i kontrollzon i anslutning till flygplatser. Luftrummet kan också innehålla andra typer av begränsningar för luftfarten såsom s.k. restriktionsområden, farliga områden och förbjudna områden. Obemannade luftfartyg över 150 kg regleras i dag på EU-nivå och kräver tillstånd från Europeiska byrån för luftfartssäkerhet, EASA.

Enligt lagen (2016:319) om skydd för geografisk information och den tillhörande förordningen (2016:320) om skydd för geografisk information krävs tillstånd för att sprida flygfoton eller liknande registreringar från en luftfarkost, om dessa utgör en sammanställning av geografisk information. Vidare krävs tillstånd till sjömätning, dvs. registrering på ett beständigt sätt av geografisk information i ett visst vattenområde eller en viss sträcka av ett vattenområde, om sjömätningen utförs inom Sveriges sjöterritorium med undantag av insjöar, vattendrag och kanaler samt till spridning av sådan information. Med geografisk information avses lägesbestämd information om förhållanden på och under markytan samt på och under sjö- och havsbotten. Tillstånd ska ges, om sjömätningen eller spridningen inte kan antas medföra skada för totalförsvaret. Tillståndet får innehålla villkor om att den geografiska informationen endast får användas för ett visst ändamål eller efter iakttagande av särskilda säkerhetsåtgärder. Tillstånd till sjömätning ges av Försvarsmakten och tillstånd till spridning ges av Sjöfartsverket när det är fråga om sjögeografisk information och i övrigt av Lantmäteriet.

Ett skydd mot viss säkerhetshotande användning av drönare finns genom bestämmelserna i säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). Med säkerhetsskydd avses skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet, skydd i andra fall av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säker-

het och skydd mot terroristbrott. Den som bedriver verksamhet som omfattas av säkerhetsskyddslagen ska undersöka vilka uppgifter i dennes verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. Resultatet av undersökningen ska dokumenteras i en säkerhetsanalys. Baserat på den analysen ska verksamhetsutövaren bedöma vilket säkerhetskydd som behövs. En del av säkerhetsskyddet kan vara tillträdesbegränsning, vilket innebär ett förebyggande av att obehöriga får tillträde till platser där det bedrivs verksamhet som har betydelse för rikets säkerhet eller där de kan få tillgång till uppgifter som omfattas av sekretess och som rör rikets säkerhet.

I betänkandet *En ny säkerhetsskyddslag* (SOU 2015:25) föreslås att tillträdesbegränsningen ska utvidgas till att även innebära ett förebyggande skydd mot skadlig påverkan på sådana områden, byggnader, anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs. Syftet med detta är att säkerhetsskyddsåtgärderna ska omfatta även ett skydd mot angrepp utifrån eller på distans. Det kan t.ex. gälla då någon med tekniska hjälpmedel obehörigen får insyn i den säkerhetskänsliga verksamheten. Tillträdesbegränsning föreslås byta namn till fysisk säkerhet.

I skyddslagen (2010:305) finns bestämmelser om vissa åtgärder till förstärkt skydd för byggnader, andra anläggningar, områden och andra objekt mot sabotage, terroristbrott, spionerі samt röjande i andra fall av hemliga uppgifter som rör totalförsvaret och grovt rån. För att tillgodose behovet av skydd kan det beslutas att vissa närmare angivna civila och militära byggnader, andra anläggningar, områden eller objekt ska vara skyddsobjekt. Ett beslut om skyddsobjekt innebär att obehöriga inte har tillträde till objektet. Genom ett särskilt beslut får tillträdesförbudet förenas med ett förbud mot att göra avbildningar, beskrivningar eller mätningar av eller inom skyddsobjektet.

Slutligen kan civilrättsliga bestämmelser innebära begränsningar av hur man får flyga med drönare över fastigheter som ägs av annan.

Kommande EU-reglering av drönare

Inom EU pågår ett arbete med att ta fram en ny unionsrättslig reglering inom det civila luftfartsområdet som ska omfatta drönare. EU-kommissionen har tagit fram en luftfartsstrategi för Europa (COM[2015] 598 final) och föreslagit en ny förordning om luftfart (COM[2015] 613 final). Den föreslagna förordningen ska ersätta Europaparlamentets och rådets förordning (EG) nr 216/2008 av den 20 februari 2008 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av en europeisk byrå för luftfartssäkerhet.

Förslaget till förordning syftar till att förbättra konkurrenskraften hos EU:s luftfartssektor och att garantera säkra, skyddade och miljövänliga lufttransporter för passagerare och allmänhet. Enligt förslaget ska förordningen även omfatta obemannade luftfartyg. Bestämmelser som gäller obemannade luftfartyg innehåller bl.a. krav gällande konstruktion, tillverkning, drift och underhåll för att trygga en säker verksamhet.

Vid sidan av förslaget till förordning har EASA tagit fram en s.k. prototypförordning för viss användning av drönare.

Varken kommissionens förslag till ny förordning om luftfart eller EASA:s prototypförordning innehåller några bestämmelser som i materiellt hänseende behandlar integritet eller skydd av personuppgifter vid användning av kamerautrustade drönare. I stället förutsätts att bestämmelserna i dataskyddsförordningen och dataskyddsdirektivet, som presenteras i avsnitt 6, kommer att gälla även vid användning av kamerautrustade drönare. Enligt kommissionen kommer dock den kommande luftfartsregleringen indirekt att bidra till en mer effektiv tillämpning av bestämmelserna om skydd av personuppgifter, eftersom den kan innehålla krav på att obemannade luftfartyg ska utrustas med någon form av identifieringsanordning.

Denna nu beskrivna kommande unionsrättsliga reglering av drönare kommer alltså med all sannolikhet inte att innehålla några materiella regler om integritet eller skydd av personuppgifter och därför inte påverka utrymmet för svensk kameraövervakningslagstiftning.

Annan ny teknik

Motsvarande frågor som uppkommit vad gäller drönare har även uppkommit när det gäller viss annan ny teknik såsom vissa kameror monterade i bilar, s.k. dash-cams.

HFD har i en dom den 21 oktober 2016 (HFD 2016 ref. 71 II) prövat om en kamera monterad på ett cykelstyre eller på insidan av vindrutan i en bil föll in under kameraövervakningslagens tillämpningsområde. Av avgörandet framgår att en kamera som monteras på något av de angivna ställena kan vara uppsatt i lagens mening och att det gäller även om kameran monteras bort efter varje färd. Enligt domstolen krävs att placeringen av kameran har en viss varaktighet eller att kameran återkommande kommer att fästas på fordonet. I det fall som domstolen prövade var kameran att anse som uppsatt. I fråga om platsen för manövrering anförde domstolen att kameran skulle vara uppsatt på cykelstyret eller på vindrutans insida, dvs. i fordonsförarens omedelbara närhet, och att föraren skulle starta och stänga av kameran samt avgöra vad som skulle filmas genom att styra fordonet. All manövrering av kameran ansågs därför ske på platsen. Kameran omfattades därmed inte av kameraövervakningslagen.

5.5 Sammanfattande slutsatser

Vad har kameraövervakningslagen inneburit för möjligheterna till kameraövervakning och skyddet för den personliga integriteten?

Enligt den kartläggning som redovisats ovan har antalet tillstånd till och anmälningar om kameraövervakning ökat under den tid som kameraövervakningslagen har varit i kraft. Ökningen av antalet anmälningar har varit större än ökningen av antalet tillstånd. Samtidigt har länsstyrelserna avgjort färre ärenden om tillstånd till kameraövervakning under 2015 än under 2012. En tänkbar förklaring till detta är att införandet av kameraövervakningslagen innebar att tillståndsplikten ersattes med anmälningsplikt för viss kameraövervakning, bl.a. övervakning i parkeringshus och övervakning i butiker.

De förändringar som infördes i och med kameraövervakningslagen har fått ett visst praktiskt genomslag men inte inneburit

några mer betydande förändringar av möjligheterna till kameraövervakning eller för skyddet av den personliga integriteten.

En förändring var att användning av teknik som främjar skyddet av den enskildes personliga integritet ska beaktas särskilt vid bedömningen av integritetsintresset vid tillståndsprövningen. Enligt såväl Datainspektionen som flertalet länsstyrelser beaktas integritetsfrämjande teknik vid prövningen. Flera av länsstyrelserna har angett att detta också leder till att fler tillstånd kan beviljas. Exempel på relativt vanligt förekommande integritetsvänlig teknik är maskering av delar av kamerornas upptagningsområde och kameror som aktiveras vid larm eller avvikande beteende, rörelsemönster etc.

Införandet av bl.a. starkare sekretesskydd, ökade krav på säkerhetsåtgärder och en skadeståndsbestämmelse som ger enskilda rätt till ersättning för skada och kränkning vid överträdelser av lagen har inte ha haft några större effekter i praktiken.

Datainspektionens centrala tillsynsansvar

Enligt kartläggningen har Datainspektionens centrala tillsynsansvar lett till att länsstyrelsernas rättstillämpning har blivit mer enhetlig. Datainspektionen har överklagat beslut i högre grad än vad Justitiekanslern tidigare har gjort, vilket lett till en mer utvecklad domstolspraxis. Enligt Datainspektionen var det under 2013 och 2014 vanligt förekommande att inspektionen överklagade länsstyrelsernas beslut för att bedömningen inte var korrekt eller för att obligatoriska tillståndsvillkor saknades. Under 2015 och början av 2016 rörde den större delen av överklagandena däremot frågor av mer principiell karaktär. Vidare sjönk andelen överklagade beslut, vilket också tyder på att länsstyrelsernas praxis har blivit mer enhetlig. Även Datainspektionens arbete med råd och anvisningar och inspektionens medverkan i länsstyrelsernas samverkansgrupp har haft betydelse för den ökade enhetligheten i rättstillämpningen.

Drönare och ny teknik

Kartläggningen och de synpunkter som lämnats av aktörer som berörs av kameraövervakningslagstiftningen visar att kameraövervakningslagen är teknikberoende. Det har särskilt framhållits att lagens

definition av övervakningskamera skapar tillämpningsproblem. Sådana frågor har tidigare uppkommit särskilt vad gäller kamerautrustade drönare och dash-cams. Numera har HFD genom de ovan redovisade avgörandena klargjort hur definitionen ska tolkas i de fallen. HFD:s avgöranden innebär att en kamerautrustad drönare normalt omfattas av kameraövervakningslagen medan en sådan dashcam som var föremål för domstolens prövning inte omfattas av lagen.

Från flera olika aktörer har det framförts att kameraövervakningslagstiftningen bör fokusera mer på behandlingen av det upptagna materialet än på kameratekniken. Även lagens distinktion mellan platser dit allmänheten har tillträde och platser dit allmänheten saknar tillträde har medfört vissa tillämpningsproblem.

Kameraövervakning på särskilda platser

Av kartläggningen framgår att kameraövervakningslagen inte har inneburit någon egentlig förändring av möjligheterna till kameraövervakning på brottsutsatta platser. Vad t.ex. gäller kameraövervakning av gator och torg gäller fortsatt den restriktiva rättspraxis som etablerats innan lagen trädde i kraft. Rättspraxis är särskilt restriktiv när sådan kameraövervakning ska bedrivas av andra aktörer än brottsbekämpande myndigheter, som t.ex. kommuner. Kartläggningen visar också att det är ovanligt att sådana aktörer ansöker om tillstånd till kameraövervakning.

Vidare är det enligt kartläggningen ovanligt med ansökningar om tillstånd till kameraövervakning av asylboenden, medieredaktioner och lokaler som används av religiösa samfund. När sådana ansökningar har gjorts har en del bifallits medan andra avslagits. Avslagen har i många fall motiverats med att sökanden inte har visat att platsen är särskilt brottsutsatt. Datainspektionen har framhållit att det inte finns några uttalanden vare sig i lagtext eller i förarbeten som ger stöd för att det vid tillståndsprövningen är möjligt att beakta generella hotbilder eller liknande omständigheter. Utrymmet att beakta att vissa platser kan ha en generell hotbild riktad mot sig är alltså begränsat.

Kameraövervakning av jordbruks- och skogsbruksmaskiner

Det har framkommit att det inom jord- och skogsbruket är relativt vanligt med stölder av jordbruks- och skogsbruksmaskiner samt drivmedel. Brottsligheten gäller stora ekonomiska värden. Det har också framkommit att det finns ett stort behov av att kunna använda åtelkameror. Samtidigt visar kartläggningen att ansökningar om tillstånd till kameraövervakning avseende maskiner, arbetsbodar och liknande ute i skog och mark knappt förekommer. Även vad gäller åtelkameror förekommer i praktiken inte några ansökningar om tillstånd.

6 Den nya dataskyddsregleringen i EU

6.1 Reformen av EU:s dataskyddsreglering

Våren 2016 antogs Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), nedan kallad förordningen.

Förordningen utgör en ny generell reglering för personuppgiftsbehandling inom EU och ersätter 1995 års dataskyddsdirektiv från och med den 25 maj 2018. Förordningen baseras till stor del på den struktur och reglering som finns i direktivet men är i många avseenden mer detaljerad och den innehåller även en rad nyheter. Förordningen kommer att vara direkt tillämplig i alla EU:s medlemsstater.

Samtidigt med förordningen antogs Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, nedan kallat direktivet.

Direktivet innehåller särregler för sådan personuppgiftsbehandling som behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Direktivet ersätter dataskyddsrambeslutet och omfattar till skillnad mot detta även rent nationell personuppgiftsbehandling på området för brottsbekämp-

ning, brottmålshantering och straffverkställighet. Direktivet innehåller en delvis ny eller mer detaljerad reglering. Direktivet ska vara genomfört i svensk rätt senast den 6 maj 2018.

Förordningen finns i *bilaga 3* och direktivet finns i *bilaga 4*. I följande avsnitt redogörs översiktligt för innehållet i de båda rättsakterna.

6.2 Förordningens innehåll

Förordningen är indelad i elva kapitel och innehåller 99 artiklar.

Allmänna bestämmelser

I förordningens kapitel I, artiklarna 1–4, finns allmänna bestämmelser om syftet med och tillämpningsområdet för förordningen. Där finns också vissa definitioner.

I artikel 1 anges förordningens syfte. Av artikeln följer bl.a. att förordningen skyddar fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, och att det fria flödet av personuppgifter inom EU varken får begränsas eller får förbjudas av skäl som rör skyddet för personuppgifter.

Enligt artikel 2.1 ska förordningen tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatiserad väg samt på annan behandling av personuppgifter som ingår i eller kommer att ingå i ett register. Artikel 2.2 innehåller vissa undantag från tillämpningsområdet.

Enligt artikel 3 är förordningen tillämplig på behandling av personuppgifter inom ramen för verksamhet som bedrivs av en personuppgiftsansvarig – eller ett personuppgiftsbiträde – som är etablerad i EU, oavsett om behandlingen utförs i unionen eller inte. Förordningen är också tillämplig på behandling av personuppgifter som avser registrerade som befinner sig i unionen av en personuppgiftsansvarig som inte är etablerad i unionen, om behandlingen har anknytning till utbjudande av varor eller tjänster till sådana registrerade eller övervakning av de registrerades beteende. Slutligen är förordningen tillämplig på behandling av personuppgifter som utförs av en personuppgiftsansvarig som inte är etablerad i unionen

men på en plats där den nationella lagstiftningen i en medlemsstat gäller på grund av folkrätten.

I artikel 4 finns ett antal definitioner av begrepp som används i förordningen, t.ex. personuppgifter, behandling, personuppgiftsansvarig, personuppgiftsbiträde och samtycke.

Principer

I kapitel II i förordningen, artiklarna 5–11, finns principer för behandling av personuppgifter.

Av artikel 5 följer sammanfattningsvis att personuppgifter

a) ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till de registrerade,

b) ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål,

c) ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas,

d) ska vara korrekta och om nödvändigt uppdaterade,

e) inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka uppgifterna behandlas, och

f) ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna med användning av lämpliga tekniska eller organisatoriska åtgärder.

I artikel 6.1 finns en uppräkning av i vilka fall personuppgiftsbehandlingar är lagliga. De grunder som räknas upp är följande.

a) Den registrerade har lämnat sitt samtycke till att hans eller hennes personuppgifter behandlas.

b) Behandlingen är nödvändig för att fullgöra ett avtal.

c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter. Detta gäller inte för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

Enligt artikel 6.2 får en medlemsstat behålla eller införa mer specifika nationella bestämmelser för att efterleva bl.a. artikel 6.1 e. Av artikel 6.3 följer att grunden för behandling enligt artikel 6.1 e ska fastställas i unionsrätten eller nationell rätt. Vidare kan nationell rätt innehålla särskilda bestämmelser om bl.a. allmänna villkor för behandlingen, vilken typ av uppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka uppgifter får lämnas ut, ändamålsbegränsningar, lagringstid samt typer av behandling och förfaranden för behandling. I artikel 6.4 finns bestämmelser om behandling för något annat ändamål än det för vilket personuppgifterna ursprungligen samlades in.

I artiklarna 7 och 8 finns bl.a. bestämmelser om villkor för samtycke till personuppgiftsbehandling.

Enligt artikel 9.1 är det förbjudet att behandla personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och att behandla genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. I artikel 9.2–9.4 finns undantag från förbudet mot behandling.

I artikel 10 regleras behandling av personuppgifter som avser fällande domar och lagöverträdelser.

Artikel 11 innehåller bestämmelser om behandling som inte kräver att den registrerade identifieras.

Rättigheter för registrerade

Kapitel III i förordningen, artiklarna 12–23, innehåller bestämmelser om registrerades rättigheter.

I artiklarna 13 och 14 finns bestämmelser om vilken information som en personuppgiftsansvarig är skyldig att lämna till de registrerade. Vidare finns i artiklarna 15–18 utförliga bestämmelser om den registrerade rätt att, under vissa förutsättningar, få tillgång till personuppgifter och att få uppgifter rättade, kompletterade eller raderade.

Artiklarna 19 och 20 reglerar bl.a. den personuppgiftsansvariges anmälningsskyldighet avseende t.ex. rättelse eller radering.

I artikel 21 finns bestämmelser om den registrerades rätt att göra invändningar mot behandling av personuppgifter som grundar sig på artikel 6.1 e eller f. Artikel 22 innehåller bestämmelser om automatiserat beslutsfattande.

Enligt artikel 23.1 får medlemsstaterna i nationell rätt begränsa de registrerades rättigheter enligt kapitlet liksom kraven enligt artikel 5. I artikel 23.2 anges vad en nationell reglering med denna typ av begränsningar ska innehålla.

Skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden

Kapitel IV i förordningen, artiklarna 24–43, innehåller skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden. I kapitlet finns bestämmelser om allmänna skyldigheter, säkerhet för personuppgifter, konsekvensbedömning och samråd, dataskyddsombud samt uppförandekoder och certifiering. I detta sammanhang ska särskilt nämnas vissa artiklar.

Artiklarna 25 och 32 innehåller relativt detaljerade bestämmelser om säkerhet vid behandling av personuppgifter. Vidare innehåller artikel 28 bestämmelser om vad som gäller när behandling av personuppgifter ska genomföras på en personuppgiftsansvarigs vägnar.

Enligt artikel 35 ska en personuppgiftsansvarig i vissa fall göra en konsekvensbedömning innan en behandling av personuppgifter får ske. När en konsekvensbedömning visar att behandlingen skulle leda till en hög risk för fysiska personers rättigheter och friheter, om inte den personuppgiftsansvarige vidtar åtgärder för att minska

risken, ska enligt artikel 36.1 den personuppgiftsansvarige samråda med tillsynsmyndigheten före behandlingen.

Överföring till tredjeland eller internationella organisationer

I kapitel V i förordningen, artiklarna 44–50, regleras under vilka förutsättningar personuppgifter får överföras till tredjeland eller till internationella organisationer. Huvudregeln är att en överföring är tillåten, om det mottagande tredjelandet eller den mottagande organisationen kan säkerställa en adekvat skyddsnivå för uppgifterna. Det är kommissionen som beslutar om ett tredjeland eller en organisation uppfyller detta krav eller inte. Om kommissionen inte har fattat något sådant beslut, är det tillåtet att överföra personuppgifter förutsatt att den som ska överföra uppgifterna vidtar vissa lämpliga skyddsåtgärder. Därutöver får överföring av personuppgifter ske i vissa undantagssituationer. Vissa av dessa undantag får dock inte åberopas av myndigheter.

Tillsyn

I kapitel VI, artiklarna 51–59, finns bestämmelser om tillsyn. I artiklarna 51 och 52 anges att medlemsstaterna ska utse en eller flera oberoende tillsynsmyndigheter som ska ansvara för att övervaka tillämpningen av förordningen. I artiklarna 53 och 54 finns bestämmelser om inrättandet av en tillsynsmyndighet och om dess ledamöter. Artiklarna 55–59 reglerar tillsynsmyndighetens behörighet, uppgifter och befogenheter, såväl utredningsbefogenheter som korrigerande befogenheter.

I kapitel VII i förordningen, artiklarna 60–76, finns bestämmelser om samarbete och enhetlighet. Där finns bestämmelser som förpliktar en nationell tillsynsmyndighet att samarbeta med och assistera tillsynsmyndigheterna i andra medlemsstater. Vidare inrättas genom artiklarna 68 och 69 den Europeiska dataskyddsstyrelsen som ett oberoende unionsorgan och med ställning som juridisk person. I artiklarna 70–76 finns bestämmelser om styrelsens uppgifter, beslutsförfarande, sammansättning och sekretess för överläggningar.

Rättsmedel, ansvar och sanktioner

I kapitel VIII, artiklarna 77–84, finns bestämmelser om rättsmedel, ansvar och sanktioner.

I artikel 77 anges att en registrerad ska ha rätt att framföra klagomål hos tillsynsmyndigheten. Enligt artiklarna 78 och 79 ska fysiska och juridiska personer ha rätt till ett effektivt rättsmedel både mot tillsynsmyndighetens beslut och direkt mot en personuppgiftsansvarig eller ett personuppgiftsbiträde, om den registrerade anser sig ha fått sina rättigheter enligt förordningen åsidosatta. Artiklarna 80 och 81 innehåller bestämmelser om företrädare för registrerade och om vilandeförklaring av mål i domstol.

Enligt artikel 82 ska den som har lidit materiell eller immateriell skada till följd av en överträdelse av förordningen ha rätt till ersättning av den personuppgiftsansvarige eller personuppgiftsbiträdet under vissa förutsättningar. Av artikeln följer också i vilken medlemsstat en skadeståndstalan ska väckas.

I artikel 83 finns bestämmelser om administrativa sanktionsavgifter vid vissa överträdelser av förordningen.

Enligt artikel 84 ska medlemsstaterna fastställa effektiva, proportionella och avskräckande sanktioner för överträdelser av förordningen.

Särskilda behandlingssituationer

I kapitel IX i förordningen, artiklarna 85–91, finns bestämmelser om särskilda situationer av behandling av personuppgifter.

I artiklarna 85 och 86 finns bestämmelser som ger medlemsstaterna utrymme att reglera förhållandet mellan skyddet för personuppgifter och yttrande- och informationsfriheten respektive offentlighetsprincipen. I artikel 87 regleras behandling av nationella identifikationsnummer.

Enligt artikel 88 får medlemsstaterna i lag eller i kollektivavtal fastställa mer specifika regler för att säkerställa skyddet av rättigheter och friheter vid behandling av personuppgifter i anställningsförhållanden.

I artikel 89 finns bestämmelser om behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål och statistiska ändamål.

Enligt artikel 90 får medlemsstaterna anta särskilda bestämmelser för att fastställa tillsynsmyndigheternas befogenheter gentemot personuppgiftsansvariga eller personuppgiftsbiträden som enligt unionsrätten eller medlemsstaternas nationella rätt omfattas av tystnadsplikt eller andra motsvarande former av förbud mot att lämna ut uppgifter.

I artikel 91 regleras befintliga bestämmelser om dataskydd inom kyrkor och religiösa samfund.

Genomförandeakter och slutbestämmelser

I kapitel X och XI, artiklarna 92–99, finns bestämmelser om genomförandeakter och slutbestämmelser.

I artiklarna 92 och 93 finns bestämmelser om delegerade akter och kommittéförfarande. Artiklarna 94–99 innehåller bestämmelser om bl.a. upphävande av 1995 års dataskyddsdirektiv, förordningens förhållande till andra unionsrättsakter och tidigare ingångna avtal, kommissionens rapporteringsskyldighet samt förordningens ikraftträdande och tillämpning. Förordningen ska tillämpas från och med den 25 maj 2018.

6.3 Direktivets innehåll

Direktivet är indelat i tio kapitel och innehåller 65 artiklar.

Allmänna bestämmelser

I direktivets kapitel I, artiklarna 1–3, finns allmänna bestämmelser om syfte och mål med direktivet och tillämpningsområdet för direktivet. Där finns också vissa definitioner.

I artikel 1.1 anges att direktivet innehåller bestämmelser om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

Enligt artikel 1.2 ska medlemsstaterna dels skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, dels säkerställa att sådant informationsutbyte mellan behöriga myndigheter som är nödvändigt enligt unionsrätten eller nationell rätt inte begränsas.

I artikel 1.3 anges att direktivet inte ska hindra att medlemsstaterna föreskriver starkare skyddsåtgärder än de som fastställs i direktivet för skyddet av den registrerades rättigheter och friheter.

Artikel 2 innehåller bestämmelser om direktivets tillämpningsområde. I artikel 2.1 anges att direktivet är tillämpligt på behandling av personuppgifter som utförs av behöriga myndigheter för de ändamål som anges i artikel 1.1. Enligt artikel 2.2 ska direktivet tillämpas på behandling av personuppgifter som helt eller delvis företas på automatiserad väg samt på annan behandling än automatiserad behandling av personuppgifter som ingår i eller kommer att ingå i ett register. I artikel 2.3 finns vissa undantag från tillämpningsområdet.

I artikel 3 finns ett antal definitioner av begrepp som används i direktivet, t.ex. personuppgifter, behandling, behörig myndighet, personuppgiftsansvarig och personuppgiftsbiträde.

Principer

I kapitel II i direktivet, artiklarna 4–11, finns principer för behandling av personuppgifter. Av artikel 4 följer bl.a. att personuppgifter ska behandlas på ett lagligt och korrekt sätt samt att de ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte behandlas på ett sätt som står i strid med dessa ändamål.

Enligt artikel 5 ska medlemsstaterna föreskriva att lämpliga tidsgränser fastställs för radering av personuppgifter eller för periodisk översyn av behovet av att lagra personuppgifter. Procedurrelaterade åtgärder ska säkerställa att tidsgränserna efterlevs.

I artiklarna 6 och 7 finns bestämmelser om den personuppgiftsansvariges skyldighet att göra åtskillnad mellan olika kategorier av registrerade och mellan personuppgifter samt om kontroll av kvaliteten på personuppgifterna.

Enligt artikel 8 ska behandling vara laglig endast om och i den mån den är nödvändig för att utföra en uppgift som utförs av en

behörig myndighet för de ändamål som anges i artikel 1.1 och som sker på grundval av unionsrätten eller nationell rätt.

I artikel 9 finns bestämmelser om vad som gäller om en behörig myndighet behandlar personuppgifter för andra ändamål än de som anges i artikel 1.1.

Enligt artikel 10 ska behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att unikt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning endast vara tillåten under vissa förutsättningar.

Artikel 11 innehåller bestämmelser om automatiserat beslutsfattande.

Rättigheter för registrerade

Kapitel III, artiklarna 12–18, innehåller bestämmelser om registrerades rättigheter.

I artiklarna 12 och 13 finns bestämmelser om bl.a. vilken information som en personuppgiftsansvarig är skyldig att lämna till registrerade.

Artiklarna 14–16 innehåller bestämmelser om bl.a. registrerades rätt att, under vissa förutsättningar, få tillgång till personuppgifter och att få uppgifter rättade, kompletterade eller raderade.

Enligt artikel 17 kan vissa av de registrerades rättigheter utövas genom tillsynsmyndigheten.

I artikel 18 anges att medlemsstaterna får föreskriva att de rättigheter som avses i artiklarna 13, 14 och 16 ska utövas i enlighet med nationell rätt, om personuppgifterna ingår i ett domstolsbeslut eller ett rättsligt protokoll eller ärende som behandlas i samband med brottsutredningar och straffrättsliga förfaranden.

Skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden

Kapitel IV, artiklarna 19–34, innehåller bestämmelser om skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden.

I artiklarna 19–26 finns bestämmelser om bl.a. inbyggt dataskydd och dataskydd som standard, behandling av personuppgifter på en personuppgiftsansvarigs vägnar, förande av register, loggning samt samarbete med tillsynsmyndigheter.

Enligt artiklarna 27 och 28 är personuppgiftsansvariga i vissa fall skyldiga att upprätta en konsekvensbedömning och beroende på utfallet av bedömningen samråda med tillsynsmyndigheten.

Artiklarna 29–31 innehåller bestämmelser om säkerhet för personuppgifter och personuppgiftsincidenter.

I artiklarna 32–34 finns bestämmelser om dataskyddsombud.

Överföring till tredjeland eller internationella organisationer

I kapitel V, artiklarna 35–40, finns bestämmelser om överföring av personuppgifter till tredjeland eller internationella organisationer.

Tillsyn

I kapitel VI, artiklarna 41–49, finns bestämmelser om tillsyn. I artiklarna 41 och 42 anges att medlemsstaterna ska utse en eller flera oberoende tillsynsmyndigheter som ska ansvara för att övervaka tillämpningen av direktivet. I artiklarna 43 och 44 finns bestämmelser om inrättandet av en tillsynsmyndighet och om dess ledamöter. Artiklarna 45–49 reglerar tillsynsmyndighetens behörighet, uppgifter och befogenheter, såväl undersökningsbefogenheter som korrigerande befogenheter.

Kapitel VII, artiklarna 50 och 51, innehåller bestämmelser om samarbete. I artikel 50 finns bestämmelser som förpliktar en tillsynsmyndighet att samarbeta med och assistera tillsynsmyndigheterna i andra medlemsstater. Artikel 51 innehåller bestämmelser om uppgifter för den genom förordningen inrättade Europeiska dataskyddsstyrelsen när det gäller personuppgiftsbehandling som omfattas av direktivet.

Rättsmedel, ansvar och sanktioner

I kapitel VIII, artiklarna 52–57, finns bestämmelser om rättsmedel, ansvar och sanktioner.

I artikel 52 anges att en registrerad ska ha rätt att framföra klagomål hos tillsynsmyndigheten. Enligt artiklarna 53 och 54 ska fysiska och juridiska personer ha rätt till ett effektivt rättsmedel både mot tillsynsmyndighetens beslut och mot en personuppgiftsansvarig eller ett personuppgiftsbiträde. Artikel 55 innehåller bestämmelser om företrädare för registrerade.

Enligt artikel 56 ska den som har lidit materiell eller immateriell skada till följd av en överträdelse av direktivet ha rätt till ersättning av den personuppgiftsansvarige eller personuppgiftsbiträdet under vissa förutsättningar.

Enligt artikel 57 ska medlemsstaterna föreskriva effektiva, proportionella och avskräckande sanktioner för överträdelser av direktivet.

Genomförandeakter och slutbestämmelser

Kapitel IX och X innehåller bestämmelser om genomförandeakter och slutbestämmelser. I artikel 58 finns bestämmelser om kommittéförfarande. Artiklarna 59–65 innehåller bestämmelser om bl.a. direktivets förhållande till vissa unionsrättsakter och tidigare ingångna avtal, kommissionens rapporteringsskyldighet samt direktivets införlivande och ikraftträdande. Direktivet ska vara genomfört i medlemsstaterna senast den 6 maj 2018.

7 Kameraövervakningslagen och den nya EU-regleringen

7.1 Dataskyddsförordningen

7.1.1 Allmänt om förordningen och kameraövervakningslagen

Bedömning: Kameraövervakning enligt kameraövervakningslagen (2013:460) kan utgöra personuppgiftsbehandling som omfattas av dataskyddsförordningen. Eftersom förordningen kommer att gälla direkt i Sverige för kameraövervakning som faller in under förordningens tillämpningsområde, kan bestämmelser om kameraövervakning som upprepar eller avviker från innehållet i förordningen inte behållas eller införas i svensk lagstiftning annat än om förordningen lämnar utrymme för det. Det måste därför analyseras hur bestämmelserna i kameraövervakningslagen förhåller sig till innehållet i förordningen och vilka ramar förordningen ger för en framtida svensk lagstiftning om kameraövervakning.

Skälen för bedömningen: EU-förordningar ska enligt artikel 288 i fördraget om Europeiska unionens funktionssätt ha allmän giltighet samt vara till alla delar bindande och direkt tillämpliga i varje medlemsstat i EU. Förordningar gäller alltså fullt ut och med samma innehåll inom hela EU och ska inte genomföras i nationell rätt. De varken ska eller får inkorporeras i eller transformeras till nationell rätt. En medlemsstat kan endast behålla eller införa nationell lagstiftning på det område som en förordning omfattar, om förordningen ger utrymme för det.

Den nya dataskyddsförordningen, som presenterats i avsnitt 6.2, kommer därför att gälla direkt i Sverige liksom i EU:s övriga med-

lemsstater när den ska börja tillämpas den 25 maj 2018. Den förutsätter alltså inte att dess innehåll genomförs i svensk rätt. Tvärtom kan svenska bestämmelser om behandling av personuppgifter som upprepar innehållet i förordningen eller som avviker från förordningen inte behållas eller införas i svensk rätt annat än om förordningen lämnar utrymme för det.

Enligt förordningen finns det ett visst utrymme för medlemsstaterna att behålla eller införa en särreglering för personuppgiftsbehandling i vissa verksamheter och i vissa avseenden. Det finns även, enligt skäl 8 i ingressen till förordningen, ett visst utrymme att införliva delar av förordningen i nationell rätt. Det förutsätter att detta är nödvändigt för att göra nationella bestämmelser begripliga i tillämpningen. En nationell reglering kan gälla för främst myndigheter och utformas efter nationella regelverk och andra nationella förutsättningar för myndigheterna i en medlemsstat. En viktig fråga att besvara är därför vilka dessa verksamheter är och i vilka avseenden en särreglering är möjlig. En anknytande grundläggande fråga är vilka verksamheter som omfattas av förordningen. Vissa omfattas i stället av det nya dataskyddsdirektivet, som presenterats i avsnitt 6.3 och som ska genomföras i svensk rätt på annat sätt än förordningen, se nedan avsnitt 7.2. Andra faller utanför både förordningens och direktivets tillämpningsområde och personuppgiftsbehandling i sådana verksamheter kan regleras genom rent inhemsk svensk rätt, se avsnitt 7.3.

Förordningen innehåller vidare i vissa delar huvudregler som medlemsstaterna kan göra undantag från genom nationell lagstiftning, oavsett vem som behandlar personuppgifterna. Även i dessa avseenden finns alltså en möjlighet att vid behov behålla eller införa svenska bestämmelser under vissa förutsättningar.

Slutligen finns det utrymme för att i svensk rätt behålla eller införa bestämmelser i frågor som anknyter till förordningen men som inte regleras där. Detsamma gäller bestämmelser som kan ses som rena kompletteringar till förordningen.

Kameraövervakning enligt kameraövervakningslagen (2013:460) kan utgöra personuppgiftsbehandling som omfattas av förordningen. Eftersom förordningen kommer att gälla direkt i Sverige för kameraövervakning som faller in under förordningens tillämpningsområde, kan bestämmelser om kameraövervakning som upprepar eller avviker från innehållet i förordningen inte behållas eller införas i svensk

lagstiftning annat än om förordningen lämnar utrymme för det. Som utgångspunkt gäller alltså att svenska bestämmelser som enbart upprepar eller som avviker från innehållet i förordningen inte är möjliga. Det måste därför analyseras hur bestämmelserna i kameraövervakningslagen förhåller sig till innehållet i förordningen och vilka ramar förordningen ger för en framtida svensk lagstiftning om kameraövervakning. Denna analys görs i de följande avsnitten. Eftersom det inte är givet att kameraövervakningslagen kan eller bör behållas, anges om bestämmelser kan behållas eller kan införas i svensk lagstiftning. Frågan om det framöver behövs särskilda svenska bestämmelser på kameraövervakningsområdet och var dessa i så fall ska finnas och hur de ska utformas behandlas i avsnitt 9–15.

7.1.2 Förordningens syfte

Bedömning: Kameraövervakningslagens syfte enligt 1 § är förenligt med förordningens syfte enligt artikel 1.

En bestämmelse om syftet med bestämmelser om kameraövervakning som har ett visst självständigt innehåll jämfört med förordningen kan behållas eller införas i svensk lagstiftning som kompletterar förordningen.

Skälen för bedömningen: I artikel 1 i förordningen anges förordningens syfte. Av artikeln följer bl.a. att förordningen skyddar fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, och att det fria flödet av personuppgifter inom EU varken får begränsas eller får förbjudas av skäl som rör skyddet för personuppgifter.

I kameraövervakningslagen anges lagens syfte i 1 § vara att tillgodose behovet av kameraövervakning för berättigade ändamål samtidigt som enskilda skyddas mot otillbörliga intrång i den personliga integriteten. Detta syfte är inte likalydande med men ändå förenligt med det syfte som anges i förordningen. Syftet enligt lagen kan sägas vara särskilt anpassat för svensk kameraövervakningslagstiftning, som har ett både vidare och snävare tillämpningsområde än förordningen, se närmare i det följande. En bestämmelse om syfte som gäller just bestämmelser om kameraövervakning och

som inte innebär en ren upprepning av artikel 1 utan har ett visst självständigt innehåll kan behållas eller införas i svensk lagstiftning som kompletterar förordningen.

7.1.3 Personuppgiftsbehandling och kameraövervakning

Bedömning: Kameraövervakningslagens kameraövervakningsbegrepp enligt 2 § överensstämmer delvis med förordningens begrepp personuppgiftsbehandling enligt artiklarna 2 och 4.

Bestämmelser med ett kameraövervakningsbegrepp som är snävare eller vidare än begreppet behandling av personuppgifter kan behållas eller införas i svensk lagstiftning som kompletterar förordningen.

Skälen för bedömningen

Begreppet personuppgiftsbehandling

I artikel 2 anges förordningens materiella tillämpningsområde, däribland att förordningen ska tillämpas på behandling av personuppgifter. Till artikeln anknyter vissa definitioner, som finns i artikel 4.

Enligt artikel 2.1 ska förordningen tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatiserad väg samt på annan behandling än automatiserad av personuppgifter som ingår i eller kommer att ingå i ett register.

Av artikel 4.1 följer att med personuppgifter avses varje upplysning som avser en identifierad eller identifierbar fysisk person, en s.k. registrerad. Med identifierbar avses att en person direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Vidare följer av artikel 4.2 att med behandling avses en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, använd-

ning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Slutligen anges i artikel 4.6 att med ett register avses en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.

Begreppet kameraövervakning

I kameraövervakningslagen definieras kameraövervakning i 2 § som användning av övervakningsutrustning. Med sådan utrustning avses övervakningskameror och övrig övervakningsutrustning. Övervakningskameror är TV-kameror, andra optisk-elektroniska instrument och därmed jämförbara utrustningar som är uppsatta så att de, utan att manövreras på platsen, kan användas för personövervakning samt separata tekniska anordningar för avlyssning eller upptagning av ljud, vilka i samband med användning av sådan utrustning används för personövervakning. Övrig övervakningsutrustning är separata tekniska anordningar för att behandla upptaget bild- och ljudmaterial. Med behandling avses varje åtgärd eller serie av åtgärder som vid kameraövervakning vidtas i fråga om bild- och ljudmaterial, vare sig det sker på automatisk väg eller inte, t.ex. upptagning, organisering, lagring, bearbetning eller ändring, användning, utlämnande genom översändande, spridning eller annat tillhandahållande, sammanställning eller samkörning, utplåning eller förstöring.

Vissa bestämmelser i kameraövervakningslagen, exempelvis 8 och 25 §§, gäller redan när en kamera ska sättas upp, dvs. innan den har tagits i bruk.

En jämförelse mellan begreppen

Vid en jämförelse mellan begreppet kameraövervakning i kameraövervakningslagen och begreppet personuppgiftsbehandling i förordningen kan inledningsvis slås fast att kameraövervakning ofta utgör behandling av personuppgifter. Begreppet kameraövervakning inne-

bär dock, tillsammans med vissa anknytande bestämmelser i lagen, vissa avvikelser från vad som i förordningen avses med behandling av personuppgifter.

Förordningen avser identifierade eller identifierbara fysiska personer och gäller när behandling sker medan kameraövervakningsbegreppet omfattar användning av kameror som kan användas för personövervakning. Begreppet omfattar knappast alla sådana identifierare enligt förordningen som innebär att en viss uppgift indirekt kan härledas till en viss person. I stället tar det sikte på att en person kan iakttas direkt och urskiljas från andra, t.ex. genom att ansiktet syns eller genom att en utmärkande klädsel, speciella kroppsrörelser eller särskild kroppskonstitution möjliggör identifiering. Å andra sidan gäller lagen inte bara när fysiska personer övervakas utan också när övervakningen faktiskt inte fångar sådana på bild. Eftersom kameraövervakning, som framgår nedan, ska ha viss varaktighet och förutsätter att personer i och för sig kan fångas av kameran måste övervakningen generellt kunna sägas innebära att personer övervakas. Vidare gäller kameraövervakningslagen redan när en kamera sätts upp, dvs. innan den används.

Vid en jämförelse kan vidare noteras att begreppet behandling vad gäller åtgärder som vidtas vid kameraövervakning delvis är utformat efter de särskilda förhållanden som gäller vid sådan övervakning. Detta innebär dock inte att begreppet i sak avviker från vad som avses med behandling enligt förordningen.

Två andra kriterier som är centrala i begreppet kameraövervakning är kravet på att en övervakningskamera ska vara uppsatt och kravet på att den ska användas utan att manövreras på platsen. Med uppsatt avses att placeringen av kameran ska ha viss varaktighet. Med uttrycket utan att manövreras på platsen menas att den fortlöpande hanteringen av utrustningen inte sker på plats. En handhållen kamera faller utanför. Däremot innebär inte enbart det förhållandet att en kamera sätts igång på stället eller fungerar med inbyggd automatik att den manövreras på platsen. De nu redovisade två kriterierna måste uppfattas så att de endast tekniskt avgränsar denna typ av personuppgiftsbehandling från annan sådan behandling och inte ses som sakliga avvikelser från vad som ska förstås med personuppgiftsbehandling.

En ytterligare fråga är hur analog kameraövervakning förhåller sig till förordningens begrepp personuppgiftsbehandling. Kamera-

övervakningslagen omfattar både analog och digital kameraövervakning (prop. 2012/13:115 s. 39). Styrande för förordningens tillämpningsområde är om en behandling företas på automatiserad väg eller om det är fråga om annan behandling av personuppgifter som ingår i eller kommer att ingå i ett register. Med register avses en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier.

Tillämpningsområdet för förordningen i detta avseende är avgränsat på samma sätt som i 1995 års dataskyddsdirektiv. Enligt Datalagskommittén, som analyserade det direktivet, stod det klart att behandling i datorer av personuppgifter som finns i datorformat – inklusive överföring av uppgifter till sådant format – som regel bör anses som automatisk behandling (SOU 1997:39 s. 295 f.). Däremot var det enligt kommittén mera osäkert om och i vilken utsträckning direktivets regler om automatisk behandling skulle tillämpas på behandling av personuppgifter som inte finns i datorformat, t.ex. bilder och ljud som lagrats i något analogt format, såsom på ett negativ eller ett ljud- eller videoband. Enligt kommittén föreföll det också tveksamt om direktivets bestämmelser om automatisk behandling skulle tillämpas på en analog upptagning av en människas utseende, även om upptagningen påbörjades och avslutades utan att någon operatör var direkt inblandad eller närvarande, såsom vid vissa former av videoövervakning.

I förarbetena till kameraövervakningslagen uttalades att användning av digital kameraövervakningsutrustning utgör behandling av personuppgifter som är helt eller delvis automatiserad medan användning av analog sådan utrustning utgör icke-automatiserad behandling (a. prop. s. 38, se även SOU 2009:87 s. 158). Vidare uttalades att merparten av sådant material som spelas in vid kameraövervakning varken ingår i eller är avsett att ingå i ett register.

Frågan om förordningen är tillämplig på analog kameraövervakning eller inte kommer ytterst att få avgöras av EU-domstolen. Den bedömning som gjordes i förarbetena till kameraövervakningslagen får därför anses vara behäftad med viss osäkerhet.

Sammanfattande slutsats

Av det redovisade följer att kameraövervakningslagens kameraövervakningsbegrepp enligt 2 § endast delvis överensstämmer med förordningens begrepp personuppgiftsbehandling enligt artiklarna 2 och 4. Begreppet i förordningen är precist och detaljerat och avsett att helt harmonisera vad som ska gälla i alla medlemsstater i detta hänseende. Som kommer att framgå nedan medger inte heller vissa särskilda artiklar i förordningen, som annars öppnar för nationell särreglering, att det i svensk rätt finns ett personuppgiftsbehandlingsbegrepp som är avvikande från begreppet i förordningen. Förordningens begrepp behandling av personuppgifter kommer framöver att gälla direkt i Sverige. Ett kameraövervakningsbegrepp måste innehålla vissa avgränsningar som skiljer kameraövervakning från annan personuppgiftsbehandling. Bestämmelser med ett kameraövervakningsbegrepp som i förtydligande syfte helt eller delvis upprepar begreppet behandling av personuppgifter och som i övrigt genom andra kriterier är snävare eller vidare än det begreppet kan behållas eller införas i svensk lagstiftning som kompletterar förordningen. Det kan finnas anledning att definiera kameraövervakning på ett annat sätt än vad som gäller i dag enligt kameraövervakningslagen.

7.1.4 Vissa undantag

Bedömning: Kameraövervakningslagens undantag från lagens tillämpningsområde enligt 4 och 5 §§ överensstämmer med förordningens undantag från tillämpningsområdet för förordningen enligt artikel 2.2. Förordningens undantag är fler än lagens.

Bestämmelser om undantag från kameraövervakningsområdet som vidgar undantagen i förordningen kan inte behållas eller införas i svensk lagstiftning som kompletterar förordningen. Bestämmelser som upprepar förordningens undantag kan behållas eller införas, om sådana är nödvändiga för förståelsen av svensk lagstiftning.

Skälen för bedömningen: I artikel 2 i förordningen anges att den ska tillämpas på behandling av personuppgifter. Vad som avses med sådan behandling och hur kameraövervakningslagens begrepp kameraövervakning förhåller sig till detta har diskuterats ovan.

I artikel 2.2 finns dock vissa undantag från förordningens tillämpningsområde i detta avseende. Några av dessa är av relevans i detta sammanhang.

Där anges att förordningen inte ska tillämpas på behandling av personuppgifter som förekommer i verksamhet för brottsbekämpning, brottmålshantering eller straffverkställighet hos behöriga myndigheter. Sådan personuppgiftsbehandling omfattas i stället av det nya dataskyddsdirektivet. För svenskt vidkommande innebär det att personuppgiftsbehandling i form av kameraövervakning i sådan verksamhet hos bl.a. Polismyndigheten och Tullverket normalt faller utanför förordningens tillämpningsområde. Däremot omfattar kameraövervakningslagen sådan övervakning utom vad gäller hemlig kameraövervakning, vilket framgår av 4 §.

Vidare omfattar förordningen inte personuppgiftsbehandling som helt faller utanför unionsrätten eller som medlemsstaterna utför när de bedriver verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget, nämligen verksamhet som avser den gemensamma utrikes- och säkerhetspolitiken. Det innebär bl.a. att kameraövervakning som sker i det svenska försvarets verksamhet i regel faller utanför förordningen. Sådan kameraövervakning träffas inte heller av direktivet. Däremot omfattas övervakningen av kameraövervakningslagen.

Slutligen omfattar förordningen inte – och inte heller direktivet – personuppgiftsbehandling som en fysisk person utför som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll. EU-domstolen har prövat innebörden av motsvarande undantag i 1995 års dataskyddsdirektiv (EU-domstolens dom Ryneš, C-212/13, EU:C:2014:2428). Enligt domstolen kan videoövervakning som delvis omfattar ett område dit allmänheten har tillträde och som därmed går utanför uppgiftshanterarens privata sfär inte anses vara av rent privat natur eller ha samband med hans eller hennes hushåll i den mening som avses i undantaget. Kameraövervakningslagen omfattar enligt 5 § inte heller kameraövervakning som bedrivs av en fysisk person som ett led i en verksamhet av rent privat natur. Undantaget i lagen – utformat

med förebild i personuppgiftslagen som genomfört 1995 års dataskyddsdirektiv – anger inte det samband med hushållet som uttrycks i förordningen. Emellertid innehöll redan direktivet situationen med hushåll och undantaget i kameraövervakningslagen – och personuppgiftslagen – har varit avsett att stämma överens med direktivet (prop. 2012/13:115 s. 44 f.) Vidare anges i kameraövervakningslagen, men inte i förordningen, att undantaget avser en plats dit allmänheten inte har tillträde. Detta tillägg har dock endast ett förtydligande syfte (a. prop. a. s. och s. 146). Det ska klargöra att kameraövervakning i offentliga miljöer och av områden som är privatägda men allemansrättsligt tillgängliga inte kan utgöra ett led i en verksamhet av rent privat natur. Av EU-domstolens ovan nämnda avgörande följer också att den viktigaste faktorn för att avgöra om förordningen är tillämplig på kameraövervakning som utförs av en fysisk person är platsen. I sak får alltså kameraövervakningslagens undantag för privat kameraövervakning anses överensstämma med undantaget i förordningen.

Sammanfattningsvis överensstämmer kameraövervakningslagens undantag från lagens tillämpningsområde enligt 4 och 5 §§ med förordningens undantag från tillämpningsområdet för förordningen enligt artikel 2.2. Förordningens undantag är dock fler än lagens; lagen omfattar även kameraövervakning som omfattas av det nya dataskyddsdirektivet eller som helt faller utanför unionsrätten. Bestämmelser om undantag från kameraövervakningsområdet som vidgar undantagen i förordningen kan inte behållas eller införas i svensk lagstiftning som kompletterar förordningen. Bestämmelser som upprepar förordningens undantag kan behållas eller införas, om sådana är nödvändiga för förståelsen av svensk lagstiftning.

7.1.5 Särskilt om kameraövervakning med drönare och ny teknik

Bedömning: Både kameraövervakningslagen och förordningen omfattar i de flesta fall kameraövervakning med kamerautrustade drönare. Lagen väntas dock inskränkas i detta hänseende under hösten 2017. Sådan kameraövervakning kan i och för sig undantas från svensk lagstiftning som kompletterar förordningen.

Skälen för bedömningen: En särskild fråga som aktualiserats under senare år är hur man rättsligt ska se på kamerautrustade drönare i olika avseenden. En drönare är ett obemannat luftfartyg som kan flyga av sig självt efter programmering eller fjärrstyras av en operatör på annan plats. Den fråga som är av intresse i detta sammanhang är om kameraövervakning från drönare omfattas av den nya förordningen och dagens svenska kameraövervakningslag. Även användning av annan ny teknik för kameraövervakning kan väcka motsvarande frågor. Det gäller exempelvis mobiltelefonkameror monterade i bilar.

Användningen av kamerautrustade drönare har blivit allt vanligare under senare år. Tekniken har många förtjänstfulla användningsområden inom både offentlig och kommersiell verksamhet. Några exempel är för räddningsarbete, inom jord- och skogsbruk samt för inspektioner och tillsynsarbete. I andra fall kan kamerautrustade drönare ibland användas på ett sätt som innebär att enskilda riskerar att utsättas för integritetskränkande övervakning. Det finns i dag viss reglering som kan träffa sådan användning, t.ex. förbudet i brottsbalken mot kränkande fotografering.

Helt klart är att förordningen träffar personuppgiftsbehandling som sker genom kamerautrustade drönare eller genom användning av annan ny teknik med kamera förutsatt att förordningen i övrigt är tillämplig för den juridiska eller fysiska person som utför behandlingen. Av intresse är här förordningens undantag för fysiska personers behandling av personuppgifter som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll. Detta undantag torde dock inte omfatta, vilket framgått av föregående avsnitt, kameraövervakning av områden dit allmänheten har tillträde. Förordningen är alltså tillämplig på kameraövervakning med drönare både när övervakningen bedrivs av juridiska personer och i många fall när den bedrivs av fysiska personer. Däremot är den i avsnitt 5.4 beskrivna kommande EU-regleringen om luftfart av mindre intresse i detta sammanhang.

När det sedan gäller kameraövervakningslagen har det tidigare varit oklart om den omfattar kamerautrustade drönare. Som redogjorts för i avsnitt 5.4 har frågan numera avgjorts av Högsta förvaltningsdomstolen (HFD) i en dom den 21 oktober 2016 (HFD 2016 ref. 71 I). Av domen framgår att en kamera som monterats på en drönare kan vara uppsatt och att det gäller även om kameran mon-

teras bort efter varje flygning. Enligt HFD krävs att placeringen av kameran har en viss varaktighet eller att kameran återkommande kommer att fästas på drönaren. I det fall som domstolen prövade var kameran att anse som uppsatt. I fråga om platsen för manövrering konstaterade domstolen att kameran på drönaren skulle fotografera från luften men styras och även i övrigt hanteras från marken. Hanteringen bedömdes därför ske från en plats som var klart åtskild från den där kameran var uppsatt. Kameran ansågs därmed inte manövrerad på platsen. Den omfattades följaktligen av kameraövervakningslagen. Kamerautrustade drönare faller alltså normalt in under kameraövervakningslagens tillämpningsområde förutsatt att kameraövervakningen bedrivs antingen av juridiska personer eller av fysiska personer i en miljö som inte är rent privat.

När det gäller annan ny teknik kan nämnas att HFD i en dom samma dag (HFD 2016 ref. 71 II) prövat om en kamera monterad på ett cykelstyre eller på insidan av vindrutan i en bil, dvs. en dashcam, föll in under kameraövervakningslagens tillämpningsområde. Av avgörandet framgår att en kamera som monteras på något av de angivna ställena kan vara uppsatt, om placeringen av kameran har en viss varaktighet eller kameran återkommande kommer att fästas på eller i fordonet. I fråga om platsen för manövrering anförde domstolen att kameran skulle vara uppsatt på cykelstyret eller på vindrutans insida, dvs. i fordonsförarens omedelbara närhet, och att föraren skulle starta och stänga av kameran samt avgöra vad som skulle filmas genom att styra fordonet. All manövrering av kameran ansågs därför ske på platsen. Kameran omfattades därmed inte av kameraövervakningslagen.

Sammanfattningsvis omfattar både kameraövervakningslagen och förordningen i de flesta fall kameraövervakning med kamerautrustade drönare. Regeringen har dock nyligen föreslagit att viss kameraövervakning från drönare ska undantas från kameraövervakningslagens tillämpningsområde (prop. 2016/17:182). Lagändringen ska enligt förslaget träda i kraft den 1 augusti 2017. Riksdagen väntas besluta i frågan under senare halvan av juni 2017 (bet. 2016/17:JuU31). Användning av dash-cams och liknande kameror omfattas av förordningen men i regel inte av kameraövervakningslagen. Kameraövervakning från drönare kan i och för sig undantas från svensk lagstiftning som kompletterar förordningen. I ett sådant fall omfattas kameraövervakningen ändå av förordningens bestämmelser.

7.1.6 Territoriellt tillämpningsområde

Bedömning: Kameraövervakningslagens territoriella tillämpningsområde enligt 3 § är förenligt med förordningens territoriella tillämpningsområde enligt artikel 3.

Bestämmelser om ett territoriellt tillämpningsområde för kameraövervakning som avviker från förordningens i begränsande riktning kan behållas eller införas i svensk lagstiftning som kompletterar förordningen. Anknytande bestämmelser om företrädare för den som bedriver kameraövervakning som gör sådana bestämmelser begripliga kan införas.

Skälen för bedömningen: Förordningen är enligt artikel 3 tillämplig på behandling av personuppgifter inom ramen för verksamhet som bedrivs av en personuppgiftsansvarig – eller ett personuppgiftsbiträde – som är *etablerad* i EU, oavsett om behandlingen utförs inom unionen eller inte.

Förordningen är också tillämplig på behandling av personuppgifter som avser registrerade som befinner sig i unionen av en personuppgiftsansvarig – eller ett personuppgiftsbiträde – som *inte är etablerad* i unionen, om behandlingen har anknytning till utbjudande av varor eller tjänster till sådana registrerade eller till övervakning av de registrerades beteende så länge beteendet sker inom unionen. I dessa fall ska enligt artikel 27 den personuppgiftsansvarige eller personuppgiftsbiträdet skriftligen utse en företrädare i unionen. Företrädaren ska vara etablerad i en av de medlemsstater där de registrerade befinner sig. Företrädaren ska på den personuppgiftsansvariges eller personuppgiftsbiträdets uppdrag fungera som kontaktperson för i synnerhet tillsynsmyndigheter och registrerade i alla frågor som har anknytning till behandlingen. Att en företrädare utsetts påverkar inte de rättsliga åtgärder som ska kunna inledas mot den personuppgiftsansvarige eller personuppgiftsbiträdet. Skyldigheten att utse företrädare gäller bl.a. inte en offentlig myndighet eller ett offentligt organ.

Slutligen är förordningen tillämplig på behandling av personuppgifter som utförs av en personuppgiftsansvarig som *inte är etablerad* i unionen men på en plats där den nationella lagstiftningen i en medlemsstat gäller på grund av folkrätten.

Begreppen personuppgiftsansvarig och personuppgiftsbiträde definieras i artikel 4. Enligt artikel 4.7 avses med personuppgiftsansvarig en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Med personuppgiftsbiträde avses enligt artikel 4.8 en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Enligt 3 § första stycket kameraövervakningslagen gäller lagen vid kameraövervakning som sker med övervakningskameror som är uppsatta i Sverige, om den som bedriver övervakningen är etablerad i Sverige eller i tredjeland. Vidare gäller lagen vid behandling av bild- och ljudmaterial som tagits upp vid sådan övervakning, om behandlingen utförs av den som bedriver övervakningen eller för dennes räkning. Med tredjeland avses enligt 2 § en stat som varken ingår i EU eller är ansluten till Europeiska ekonomiska samarbetsområdet. Om den som bedriver övervakningen är etablerad i tredjeland, ska han eller hon enligt 3 § andra stycket utse en företrädare för sig som är etablerad i Sverige. Det som anges i kameraövervakningslagen om den som bedriver kameraövervakning gäller också för företrädaren.

Vid en jämförelse mellan kameraövervakningslagen och förordningen kan konstateras att lagens territoriella tillämpningsområde delvis överensstämmer men är förenligt med förordningens territoriella tillämpningsområde enligt artikel 3. Bestämmelserna om företrädare överensstämmer inte fullt ut. Artikel 3 kommer att gälla direkt i Sverige. Bestämmelser om ett territoriellt tillämpningsområde för kameraövervakning som avviker från förordningens i begränsande riktning kan behållas eller införas i svensk lagstiftning som kompletterar förordningen. Anknytande bestämmelser om företrädare för den som bedriver kameraövervakning som gör sådana bestämmelser begripliga kan införas.

7.1.7 Laglig personuppgiftsbehandling och kameraövervakning

Bedömning: Kameraövervakningslagens bestämmelser i 8–24 och 49 §§ om när kameraövervakning är tillåten är i huvudsak förenliga med förordningens bestämmelser om när personuppgiftsbehandling är laglig enligt artikel 6.1 och artiklarna 7–11.

Bestämmelser om i vilka fall kameraövervakning är laglig som enbart upprepar eller som avviker från innehållet i förordningen kan inte behållas eller införas i svensk lagstiftning som kompletterar förordningen.

Skälen för bedömningen: I artikel 6.1 i förordningen finns en uppräkning av i vilka fall personuppgiftsbehandlingar är lagliga, dvs. rättsligt grundade. För att en behandling av personuppgifter ska vara laglig måste den alltså falla in under någon av de rättsliga grunder som anges i denna artikel. Det finns inte några skarpa gränser mellan de olika grunderna, vilket innebär att en behandling kan falla in under mer än en sådan grund. Dessa grunder är följande.

a) Den registrerade har lämnat sitt samtycke till att hans eller hennes personuppgifter behandlas.

b) Behandlingen är nödvändig för att fullgöra ett avtal.

c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Enligt skäl 45 i ingressen till förordningen utesluts inte att även andra än myndigheter kan ha sådana uppgifter.

f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter. Detta gäller inte för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

I artiklarna 7–11 finns ytterligare bestämmelser om när behandling av personuppgifter är tillåten. Av dessa är artiklarna 9 och 10 av visst intresse.

I artikel 9.1 finns ett förbud mot behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och mot behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Biometriska uppgifter definieras i artikel 4.14 som uppgifter som erhållits genom en teknisk behandling avseende en persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör identifiering av personen. Av skäl 51 i ingressen till förordningen framgår att behandling av foton inte systematiskt omfattas, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person.

I artikel 9.2–9.4 finns ett antal undantag från förbudet mot behandling. Exempelvis får behandling ske om den registrerade uttryckligen har lämnat sitt samtycke till denna eller om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse på grundval av unionsrätten eller en medlemsstats nationella rätt.

Sådana känsliga uppgifter som omfattas av förbudet i artikel 9.1 kan i och för sig samlas in genom kameraövervakning. Artikelns förbud måste anses gälla när kameraövervakningen sker enbart på grund av de avbildade personernas ras eller etniska ursprung etc. Bilder på människor i mer ”normala” sammanhang kan inte anses avslöja några känsliga personuppgifter. Så har 1995 års dataskyddsdirektiv hittills uppfattats på kameraövervakningsområdet (jfr även SOU 1997:39 s. 371 och artikel 29-gruppens – en arbetsgrupp som inrättats enligt 1995 års dataskyddsdirektiv – Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillances, s. 24).

Vidare finns i artikel 10 bestämmelser som avser fällande domar och lagöverträdelser. Enligt artikeln får behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder enligt artikel 6.1 endast utföras under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Det som avses med termen överträdelser måste med hänsyn till sammanhanget anses avse överträdelser som innefattar brott. Det är inte helt klart i vilken utsträckning uppgifter som rör misstankar om brott omfattas. Uppgifter om faktiska iakttagelser av en persons handlande bör rimligen inte anses som uppgifter om brott (jfr a. SOU s. 383). Artikeln får därför förstås så att den inte tar sikte på sådana möjliga lagöverträdelser som kan fångas på bild vid kameraövervakning.

Enligt förordningen finns det inte något utrymme för medlemsstaterna att göra undantag från de rättsliga grunderna i artikel 6.1. EU-domstolen har i ett avgörande som gällde motsvarande artikel i 1995 års dataskyddsdirektiv uttalat att medlemsstaterna varken får foga ytterligare principer för tillåtligheten av behandlingen av personuppgifter till dem som nämns i artikeln eller får föreskriva ytterligare villkor som påverkar räckvidden av artikelns principer (dom ASNEF och FECEMED, förenade målen C-468/10 och C-469/10, EU:C:2011:777). Det är alltså inte möjligt att i nationell rätt generellt ange att viss personuppgiftsbehandling endast får ske i enlighet med någon eller några av grunderna i artikel 6.1.

I 8–24 och 49 §§ kameraövervakningslagen finns flera bestämmelser som anger när kameraövervakning är tillåten och ett antal därtill anknytande bestämmelser Som huvudregel gäller att det krävs tillstånd till kameraövervakning av platser dit allmänheten har tillträde och att ett sådant ska ges om intresset av övervakning väger tyngre än den enskildes intresse av att inte bli övervakad. Vid bedömningen av intresset av kameraövervakning ska det särskilt beaktas om övervakningen behövs för att förebygga, avslöja eller utreda brott, förhindra olyckor eller för andra därmed jämförliga ändamål. På platser dit allmänheten inte har tillträde får kameraövervakning ske antingen efter samtycke från den som ska övervakas eller efter en intresseavvägning där intresset av att övervaka för att förebygga, avslöja eller utreda brott, förhindra olyckor eller för att tillgodose

andra berättigade ändamål väger tyngst. Därutöver finns bestämmelser om helt eller delvis tillståndsfri kameraövervakning och kameraövervakning efter anmälan.

Kameraövervakningslagens bestämmelser är i huvudsak förenliga med förordningens bestämmelser om när personuppgiftsbehandling är laglig enligt artikel 6.1 och artiklarna 7–11. Kameraövervakning enligt lagen kan exempelvis grundas på samtycke från dem som övervakas. Det gäller emellertid bara på platser dit allmänheten inte har tillträde.

Vidare kan, som närmare kommer att utvecklas i nästa avsnitt, de statliga och kommunala myndigheternas kameraövervakning omfattas av artikel 6.1 e, eftersom myndigheternas verksamhet är att betrakta som myndighetsutövning eller i vart fall som uppgifter av allmänt intresse i den mening som avses i artikeln. Detsamma gäller för kameraövervakning som bedrivs av andra än myndigheter vid utförandet av vissa uppgifter som också kan sägas vara av allmänt intresse. Sådan kameraövervakning kan ske efter en intresseavvägning enligt lagen, ibland med och ibland utan krav på tillstånd.

I andra fall kan kameraövervakning vara tillåten enligt kameraövervakningslagen efter en intresseavvägning som i delar liknar den avvägning mellan intresset av övervakning och den enskildes integritetsintresse som anges i artikel 6.1 f. Beroende på platsen för övervakningen kan tillstånd krävas.

I ytterligare andra fall gäller en anmälningsplikt och i de fallen föreskrivs i lagen inte någon särskild intresseavvägning.

Bestämmelser om i vilka fall kameraövervakning är laglig som enbart upprepar eller som avviker från innehållet i förordningen kan inte behållas eller införas i svensk lagstiftning som kompletterar förordningen. Frågan berörs ytterligare i nästa avsnitt. Huruvida en svensk lagstiftning kan innehålla ett krav på tillstånd eller anmälan för att kameraövervakning ska få ske behandlas också i nästa avsnitt.

7.1.8 Utrymme för svensk lagstiftning om tillståndskrav m.m. vad gäller uppgifter av allmänt intresse

Bedömning: Svensk lagstiftning som kompletterar förordningen kan med stöd av artiklarna 6.2, 6.3 och 36.5 i förordningen innehålla detaljerade bestämmelser för sådan kameraövervakning som sker som ett led i myndighetsutövning eller för att utföra en uppgift av allmänt intresse men inte för kameraövervakning i övrigt. Lagstiftningen kan exempelvis innehålla ett krav på tillstånd för att kameraövervakning ska få ske vid utförandet av en sådan uppgift.

Skälen för bedömningen

Utrymme för nationell reglering när personuppgiftsbehandling sker för att utföra en uppgift av allmänt intresse

Av det föregående avsnittet framgår att personuppgiftsbehandling är laglig enligt artikel 6.1 e i förordningen när behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. När denna rättsliga grund är aktuell gäller vissa ytterligare bestämmelser i förordningen.

Enligt artikel 6.2 får en medlemsstat behålla eller införa mer specifika nationella bestämmelser för att efterleva bl.a. artikel 6.1 e. Medlemsstaten kan fastställa särskilda krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling. Av artikel 6.3 följer att grunden för behandling enligt artikel 6.1 e ska fastställas i unionsrätten eller nationell rätt. Syftet med behandlingen ska vara nödvändigt för att utföra uppgiften eller som ett led i myndighetsutövningen. Vidare kan nationell rätt innehålla särskilda bestämmelser om bl.a. allmänna villkor för behandlingen, vilken typ av uppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka uppgifter får lämnas ut, ändamålsbegränsningar, lagringstid samt typer av behandling och förfaranden för behandling.

Dessutom är artiklarna 35 och 36, som även behandlas i avsnitt 7.1.11, av relevans i sammanhanget.

Enligt artikel 35 ska en personuppgiftsansvarig i vissa fall göra en konsekvensbedömning innan en behandling av personuppgifter får ske. Av artikeln följer att om en typ av behandling – särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål – sannolikt leder till en hög risk för fysiska personers rättigheter och friheter, ska den personuppgiftsansvarige före behandlingen utföra en bedömning av behandlingens konsekvenser för skyddet av personuppgifter. En bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker. En konsekvensbedömning ska göras bl.a. när det är fråga om systematisk övervakning av en allmän plats i stor skala. I skäl 71 i ingressen anges som exempel på sådan övervakning användning av optisk-elektroniska anordningar.

När en konsekvensbedömning visar att behandlingen skulle leda till en hög risk för fysiska personers rättigheter och friheter, om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken, ska enligt artikel 36.1 den personuppgiftsansvarige samråda med tillsynsmyndigheten före behandlingen. Om tillsynsmyndigheten anser att behandlingen skulle strida mot förordningen, ska myndigheten enligt artikel 36.2 inom viss tid ge den personuppgiftsansvarige skriftliga råd. Vidare får myndigheten använda sig av befogenheter som den har enligt artikel 58 i förordningen. Exempelvis kan tillsynsmyndigheten utfärda varning eller införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, en behandling. Tillsynsmyndigheten ska enligt artikel 35.4 upprätta en förteckning över behandlingsverksamheter som omfattas av kravet på konsekvensbedömning. Myndigheten får vidare enligt artikel 35.5 även upprätta en förteckning över behandlingsverksamheter som inte kräver någon sådan bedömning.

Dessa artiklar innebär att vid vissa typer av personuppgiftsbehandlingar som omfattas av förordningen, men inte alla, ska en konsekvensbedömning göras och eventuellt följas av ett samråd, som i sin tur kan följas av t.ex. ett förbud mot behandlingen från tillsynsmyndighetens sida.

Enligt artikel 35.10 finns dock en möjlighet att i nationell rätt göra undantag från kravet på att utföra en konsekvensbedömning avseende bl.a. behandlingar enligt artikel 6.1 e. Därmed faller också det krav på samråd som baseras på en sådan bedömning. Detta gäller när en sådan behandling har en rättslig grund i medlems-

statens nationella rätt och den rätten reglerar den aktuella behandlingsåtgärden – eller serien av åtgärder – samt en konsekvensbedömning avseende dataskydd redan har gjorts i samband med införandet av den nationella regleringen.

Vidare följer av artikel 36.5 att, oaktat vad som sägs i artikel 36.1 om samråd – som baseras på en konsekvensbedömning som utvisat en hög risk i det enskilda fallet – får en medlemsstat i sin nationella rätt kräva att personuppgiftsansvariga ska samråda med och erhålla förhandstillstånd av tillsynsmyndigheten när det gäller en behandling för utförandet av en uppgift som den personuppgiftsansvarige utför av allmänt intresse. Artikeln innebär att en medlemsstat kan föreskriva en generell samråds- och tillståndsplikt. En sådan gäller då alla behandlingar som omfattas av föreskriften och inte endast behandlingar där det i det enskilda fallet konstateras finns en hög risk för fysiska personers rättigheter och friheter. Möjligheten att föreskriva krav på samråd och tillstånd i nationell rätt är dock begränsad till vissa av de fall som annars omfattas av artiklarna 35 och 36, nämligen till personuppgiftsbehandlingar som sker vid utförande av uppgifter av allmänt intresse.

Följaktligen ger artikel 36.5 utrymme för en medlemsstat att i sin nationella rätt behålla eller införa ett allmänt krav på samråd och tillstånd för personuppgiftsbehandling som behövs för att utföra en uppgift av allmänt intresse.

Avslutningsvis ska noteras att artikel 6.1 e men inte artikel 36.5 utöver behandling för att ”utföra en uppgift av allmänt intresse” anger behandling ”som ett led i myndighetsutövning”. Myndighetsutövande uppgifter måste alltid anses som uppgifter av allmänt intresse. Uppgifter av allmänt intresse kan däremot vara ett vidare begrepp. Eftersom det är det senare uttryckssättet som används i båda artiklarna, uppkommer inte någon betydelseskillnad mellan dem som är av relevans i detta sammanhang. I det följande behandlas därför båda begreppen samlat.

I sammanhanget kan också nämnas att förordningen enligt artikel 40 förutsätter att uppförandekoder utarbetas och används inom olika branscher.

Vad avses med myndighetsutövning och en uppgift av allmänt intresse?

Frågan är då vad som avses med myndighetsutövning och en uppgift av allmänt intresse.

Begreppet myndighetsutövning har en unionsrättslig innebörd. Som rättsläget ser ut i dag finns det dock inte något som hindrar att ett svenskt synsätt anläggs på den närmare innebörden av begreppet. Enligt svensk rätt karakteriseras myndighetsutövning av beslut eller andra ensidiga åtgärder som ytterst är ett uttryck för samhällets maktbefogenheter i förhållande till medborgarna. Myndighetsutövning kan medföra både förpliktelser för enskilda och åtgärder som är gynnande för enskilda. Det krävs författningsstöd för myndighetsutövning i Sverige. I första hand är det statliga och kommunala myndigheter som ägnar sig åt myndighetsutövning. Även andra juridiska personer liksom fysiska person kan dock anförtros förvaltningsuppgifter som innefattar myndighetsutövning.

När det gäller vad som avses med en uppgift av allmänt intresse är det också ett unionsrättsligt begrepp. Det finns dock inte någon definition av begreppet inom unionsrätten och inte heller någon praxis, vare sig från EU-domstolen eller svenska myndigheter, som belyser detta närmare. Vid tolkningen måste man ha i åtanke att eftersom det är fråga om ett unionsrättsligt begrepp får detta inte tolkas fritt av varje enskild medlemsstat. Bedömningen ska avse uppgiften som sådan och inte den personuppgiftsbehandling – t.ex. kameraövervakning – som ska ske vid utförandet av uppgiften.

Under begreppet bör anses falla uppgifter som utförs av statliga myndigheter för att uppfylla uttryckliga uppdrag från riksdagen eller regeringen. Detsamma bör gälla obligatoriska uppgifter som kommuner och landsting utför till följd av författningsreglerade åligganden. På samma sätt bör man rimligen se på de frivilliga åtaganden som kommuner och landsting kan göra så länge de avser angelägenheter av allmänt intresse i den mening som avses i svensk rätt. Därutöver utför myndigheter vissa andra, administrativa uppgifter – såsom säkerhetsarbete – för att de ska kunna fullgöra sin kärnverksamhet. Även sådana uppgifter bör anses vara av allmänt intresse. På samma sätt bör man se på den situationen att enskilda juridiska personer eller fysiska personer på uppdrag av en statlig eller kommunal myndighet utför förvaltningsuppgifter som åligger

myndigheten eller kommunen. Även vissa andra verksamheter som kan bedrivas av privaträttsliga subjekt kan falla in under begreppet uppgift av allmänt intresse.

Allmänt intresse – inklusive myndighetsutövning – och kameraövervakning

När det gäller just kameraövervakning får mot bakgrund av det som angetts i avsnittet ovan följande anses gälla.

Kameraövervakning som utförs av statliga eller kommunala myndigheter som ett led i kärnverksamheten utgör en personuppgiftsbehandling som sker för att utföra en myndighetsutövande uppgift eller annars en uppgift av allmänt intresse. Detsamma gäller kameraövervakning i övrigt hos myndigheterna, åtminstone när det finns en koppling till kärnverksamheten, såsom att övervakningen sker för att skydda de anställda eller verksamheten i övrigt så att den kan utföras. Sådan övervakning kan t.ex. ske av yttre in- och utgångar för personalen och av väntrum för allmänheten.

Också kameraövervakning som bedrivs av privaträttsliga subjekt som ett led i förvaltningsuppgifter som anförtrotts dem utförs för att fullgöra antingen en myndighetsutövande uppgift eller någon annan uppgift av allmänt intresse. Även vissa andra verksamheter som drivs av sådana subjekt kan med hänsyn till verksamhetens syfte ha ett allmänt intresse. Kameraövervakning kan då ske för att utföra denna uppgift. Vilka sådana verksamheter, där kameraövervakning kan förekomma, som kan anses vara av allmänt intresse är svårt att i detalj uttala sig om. Generellt gäller att det är verksamheten eller uppgiften som sådan som ska vara av allmänt intresse, inte kameraövervakningen. Som exempel kan nämnas bedrivande av kollektivtrafik. Enligt Artikel 29-gruppen, som är en arbetsgrupp som inrättats enligt 1995 års dataskyddsdirektiv, kan kameraövervakning anses avse en uppgift av allmänt intresse när det gäller övervakning för att upptäcka våldsamt beteende i kollektivtrafik i brottsbelastade områden (Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillances, s. 17).

Vad gäller brottsbekämpning är det en verksamhet som i princip är förbehållen Polismyndigheten, Åklagarmyndigheten och ytterligare några myndigheter. Kameraövervakning i den verksamheten regleras inte genom förordningen utan i direktivet. När däremot andra

aktörer bedriver kameraövervakning för att motverka brottslighet i sina verksamheter omfattas övervakningen av förordningen men många gånger är det inte fråga om en kameraövervakning som sker för att utföra en uppgift av allmänt intresse. Visserligen kan kameraövervakning även i sådana verksamheter sägas gagna det allmänna intresset av att brott förebyggs, upptäcks, utreds och lagförs. Enligt förordningen är det dock inte syftet med kameraövervakningen utan själva verksamhetens syfte som är det centrala i sammanhanget. Om verksamheten inte kan anses vara av allmänt intresse, saknas möjlighet att med stöd av artiklarna 6.2, 6.3 och 36.5 reglera kameraövervakningen i nationell rätt, t.ex. genom att ställa upp ett krav på tillstånd för övervakningen. Detta gäller t.ex. enskilda som bedriver butiksverksamhet och kameraövervakar sina butiker för att skydda anställda och egendom mot brott. Sådana enskilda kan i stället, om förutsättningar för det föreligger, bedriva kameraövervakning med stöd av artikel 6.1 f i förordningen (EU-domstolens dom Ryneš, C-212/13, EU:C:2014:2428).

Sammanfattningsvis får frågan om kameraövervakning behövs för att en uppgift av allmänt intresse ska kunna utföras avgöras utifrån vem som vill bedriva övervakningen och i vilket sammanhang samt med beaktande av en viss restriktivitet i tolkningen av begreppet uppgift av allmänt intresse.

Kameraövervakningslagen och utrymmet för allmänt intresse

Vad då gäller hur dagens kameraövervakningslag förhåller sig till de redovisade artiklarna kan först konstateras att lagen inte innehåller någon uttrycklig bestämmelse med en sådan rättslig grund som avses i artikel 6.3 när det gäller kameraövervakning som sker som ett led i myndighetsutövning eller för att utföra en uppgift av allmänt intresse. Den i avsnitt 2.1.3 nämnda Dataskyddsutredningen har gjort bedömningen att artikel 6.3 ska förstås så att för att en behandling av personuppgifter ska vara laglig enligt artikel 6.1 e måste behandlingen dels vara nödvändig antingen som ett led i myndighetsutövning eller för att kunna utföra en uppgift av allmänt intresse, dels vara fastställd i enlighet med unionsrätten eller den nationella rätten. Vidare måste ändamålet med behandlingen vara nödvändigt för myndighetsutövningen respektive utförandet av

uppgiften. Enligt utredningen gäller kravet på uttryckligt författningsstöd den övergripande uppgiften. Artikeln innebär alltså inte ett krav på stöd i nationell rätt för den specifika behandlingsåtgärden, i detta sammanhang kameraövervakningen som sådan. Detta innebär att kameraövervakning är tillåten enligt artikel 6.1 e, om övervakningen är nödvändig som ett led i myndighetsutövning eller för att utföra en uppgift av allmänt intresse som följer av gällande rätt. Enligt utredningen finns stöd i svensk rätt för myndighetsutövning och utförande av uppgifter av allmänt intresse. Utredningen har ändå föreslagit bestämmelser som tydliggör att personuppgifter får behandlas endast om minst ett av de villkor som anges i artikel 6.1 är uppfyllt. Enligt dessa får personuppgifter behandlas med stöd av artikel 6.1 e i förordningen, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning eller om behandlingen är nödvändig som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning.

Vidare innehåller kameraövervakningslagen andra bestämmelser av det slag som är tillåtna att ha i nationell rätt med stöd av artikel 6.3 förutsatt att kameraövervakningen är nödvändig för myndighetsutövning eller för att utföra en uppgift av allmänt intresse. Exempelvis finns bestämmelser om lagringstid i 32 §. Lagen innehåller också i 8 § ett krav på tillstånd till kameraövervakning som i och för sig kan behållas med stöd av artikel 36.5 i den utsträckning övervakningen sker för att utföra en uppgift av allmänt intresse. En ren anmälningsskyldighet som liknar den anmälningsplikt som finns i 12–16 §§ i lagen kan däremot knappast behållas, eftersom det i förordningen anges att ett nationellt krav ska avse samråd och tillstånd. I kameraövervakningslagen finns i 9 § även bestämmelser om hur intresseavvägningen ska göras i de fall där det krävs tillstånd till kameraövervakning. Någon form av sådan avvägning måste anses möjlig att fortsatt föreskriva i svensk rätt för det fall ett tillståndskrav bör gälla. Artikel 6.3 lämnar utrymme för nationella regler om allmänna villkor för personuppgiftsbehandling och ett nationellt tillståndskrav enligt artikel 36.5 förutsätter också vissa kompletterande bestämmelser om hur tillståndsprövningen ska gå till, dvs. vilka närmare omständigheter som ska beaktas vid bedömningen av om

tillstånd ska ges eller inte. Det kan också erinras om att artikel 6.1 e innehåller ett krav på nödvändighet, som i någon form måste återspeglas i en eventuell tillståndsprövning.

I sammanhanget förtjänar att upprepas att myndigheter som rättslig grund för kameraövervakning inte kan åberopa en intresseavvägning enligt artikel 6.1 f men däremot kan artikel 6.1 e utgöra rättslig grund för deras kameraövervakning. Därutöver kan ett svenskt tillståndskrav för myndigheters kameraövervakning i och för sig gälla. Ett tillståndsförfarande förutsätter naturligen att prövningen av om tillstånd ska ges eller inte sker enligt vissa kriterier och av artikel 58 följer också att tillsynsmyndigheten ska ha befogenhet att ge tillstånd till behandling. En anknytande fråga är om andra subjekt som skulle kunna omfattas av ett sådant tillståndskrav och som i och för sig kan åberopa den rättsliga grunden i artikel 6.1 f kan kringgå tillståndsförfarandet genom att åberopa den grunden. Svaret måste vara nej. Detta kan rimligen inte anses ha varit förordningens mening när den lämnat utrymme för att kräva tillstånd för personuppgiftsbehandling som sker vid utförandet av vissa uppgifter.

I de verksamheter där kameraövervakning sker och där övervakningen omfattas av dagens tillstånds- eller anmälningsplikt men verksamheten inte utgör myndighetsutövning eller är av allmänt intresse enligt artikel 36.5 kommer kameraövervakning framöver att få ske tillstånds- eller anmälningsfritt. I dessa fall gäller förordningens bestämmelser om när och hur kameraövervakning får ske.

Avslutningsvis ska nämnas att förordningen i artikel 88 lämnar utrymme för nationella regler i lagstiftning eller kollektivavtal om kameraövervakning i anställningsförhållanden. Denna artikel behandlas i avsnitt 7.1.12.

Ett utrymme för svensk lagstiftning om kameraövervakning, t.ex. ett tillståndskrav

Av avsnitten ovan följer sammanfattningsvis följande. Svensk lagstiftning som kompletterar förordningen kan med stöd av artiklarna 6.2, 6.3 och 36.5 i förordningen innehålla detaljerade bestämmelser för sådan kameraövervakning som sker som ett led i myndighetsutövning eller för att utföra en uppgift av allmänt intresse men inte för kameraövervakning i övrigt.

Lagstiftningen kan exempelvis innehålla ett krav på tillstånd för att kameraövervakning ska få ske vid utförandet av en sådan uppgift. Ett tillståndskrav kan gälla för statliga och kommunala myndigheters kameraövervakning men också för kameraövervakning som utförs av privaträttsliga subjekt i samband med vissa särskilda verksamheter, såsom i kollektivtrafiken. För anställningsförhållanden finns enligt förordningen ett särskilt utrymme för eventuella svenska regler i lagstiftning eller kollektivavtal, se avsnitt 7.1.12.

7.1.9 Vissa definitioner och principer

Bedömning: Kameraövervakningslagens definitioner enligt 2 §, utöver de som behandlats i avsnitt 7.1.3, är förenliga med förordningens definitioner enligt artikel 4. Lagens allmänna krav för kameraövervakning enligt 7 § och bestämmelser om behandling av bild- och ljudmaterial i 28–33 §§ överensstämmer delvis med förordningens principer enligt artikel 5.

Bestämmelser på kameraövervakningsområdet om definitioner m.m. som enbart upprepar eller som avviker från innehållet i förordningen kan inte behållas eller införas i svensk lagstiftning som kompletterar förordningen.

Skälen för bedömningen: I förordningens kapitel I och II med allmänna bestämmelser respektive principer finns, utöver de ovan behandlade artiklarna om bl.a. syfte, tillämpningsområde, vissa definitioner och rättsliga grunder för behandling, vissa ytterligare bestämmelser av intresse i detta sammanhang.

I artikel 4.11 finns en definition av begreppet samtycke. En sådan definition finns även i 2 § kameraövervakningslagen. Den motsvarar i sak den som finns i artikeln, även om den är anpassad till sådan personuppgiftsbehandling som sker genom kameraövervakning. Något utrymme att i svensk lagstiftning som kompletterar förordningen upprepa denna definition finns inte. Kameraövervakningslagen innehåller även ett antal ytterligare definitioner som inte finns i förordningen och som i och för sig är förenliga med förordningen. Samtidigt saknar lagen ett antal definitioner som finns i förordningen.

Vidare innehåller artikel 5 i förordningen vissa principer för behandling av personuppgifter. Dessa krav utgör tillsammans med de rättsliga grunderna enligt artikel 6, som behandlats ovan, de allmänna förutsättningarna för att en behandling av personuppgifter ska vara tillåten. I förordningen finns sedan ett flertal artiklar med ett närmare innehåll som bygger på dessa principer. Vissa av dessa och därmed artikel 5 kan enligt artikel 23 begränsas i nationell rätt, se avsnitt 7.1.10. I artikel 5 anges sammanfattningsvis att personuppgifter

a) ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade,

b) ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål,

c) ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas,

d) ska vara korrekta och om nödvändigt uppdaterade; alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål,

e) inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas, och

f) ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna med användning av lämpliga tekniska eller organisatoriska åtgärder.

Kameraövervakningslagen innehåller flera bestämmelser vars innehåll kan sägas motsvara de principer som anges i artikel 5. Enligt 7 § i lagen gäller som allmänna krav för kameraövervakning att övervakningen ska bedrivas lagligt, enligt god sed och med tillbörlig hänsyn till enskildas personliga integritet. Vidare regleras i 28–33 §§ hur bild- och ljudmaterial från kameraövervakning får behandlas. Till exempel anges att den som bedriver kameraövervakning inte får behandla bild- och ljudmaterial från övervakningen för något ändamål som är oförenligt med det som materialet samlades in för. Det

finns också exempelvis angivet hur länge material från kameraövervakning får bevaras, se även avsnittet nedan. Lagens allmänna krav för kameraövervakning och bestämmelser om behandling av bild- och ljudmaterial överensstämmer dock endast delvis med förordningens principer enligt artikel 5. Eftersom förordningen kommer att gälla direkt i Sverige, kan bestämmelser på kameraövervakningsområdet som enbart upprepar eller som avviker från innehållet i förordningen inte behållas eller införas i svensk lagstiftning som kompletterar förordningen.

7.1.10 Rättigheter för registrerade

Bedömning: Kameraövervakningslagens upplysningsplikt och tider för bevarande av bild- och ljudmaterial från kameraövervakning enligt 25–27 §§ och 32 § är i huvudsak förenlig respektive är förenliga med förordningens rättigheter för registrerade och möjligheter att begränsa dessa rättigheter enligt artiklarna 12–23. Bestämmelser om tystnadsplikt och utlämnande av uppgifter i 37 § kameraövervakningslagen och i offentlighets- och sekretesslagen (2009:400) är förenliga med förordningen. Rättigheterna enligt förordningen är fler än vad som följer av lagen.

Vissa bestämmelser på kameraövervakningsområdet om upplysningsplikt och bevarandetider samt andra bestämmelser som innebär undantag från rättigheterna för de registrerade kan behållas eller införas i svensk lagstiftning som kompletterar förordningen.

Skälen för bedömningen: Kapitel III i förordningen, artiklarna 12–23, innehåller bestämmelser om registrerades rättigheter. Rättigheterna gäller insyn och villkor, information och tillgång till personuppgifter, rättelse och radering samt rätt att göra invändningar. Kapitlet innehåller också bestämmelser som ger en medlemsstat möjlighet att i sin nationella rätt begränsa både dessa rättigheter och de krav som följer av artikel 5, se ovan angående innehållet i den artikeln.

I kapitlet finns bl.a. en detaljerad reglering om vilken information som en personuppgiftsansvarig är skyldig att lämna till den

registrerade. Information ska t.ex. lämnas om vem som behandlar uppgifterna och om ändamålet med behandlingen.

Vidare finns utförliga bestämmelser om den registrerades rätt att, under vissa förutsättningar, få tillgång till personuppgifter och viss information i samband med det och att få uppgifter rättade, kompletterade eller raderade samt att få behandlingen begränsad. Exempelvis ska personuppgifter raderas när de inte längre är nödvändiga för de ändamål för vilka de samlats in eller annars behandlats. Den registrerade har även rätt att göra invändningar mot behandling av personuppgifter som grundar sig på artikel 6.1 e eller f.

I artikel 23.1 ges medlemsstaterna dock en möjlighet att i nationell rätt begränsa de registrerades rättigheter enligt kapitlet liksom kraven enligt artikel 5. Sådana begränsningar får göras endast om de sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa vissa angivna intressen, såsom den nationella säkerheten, försvaret, den allmänna säkerheten, verkställande av straffrättsliga sanktioner eller förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott. I artikel 23.2 anges vad en nationell reglering med denna typ av begränsningar ska innehålla. Exempelvis ska en sådan innehålla, om det är relevant, bestämmelser om lagringstid.

Enligt 25 § kameraövervakningslagen gäller som huvudregel en upplysningsplikt vid all kameraövervakning som omfattas av lagen. Upplysning om kameraövervakning ska lämnas genom tydlig skyltning eller på något annat verksamt sätt. Upplysning ska också lämnas om vem som bedriver kameraövervakningen, om detta inte framgår av förhållandena på platsen. Om ljud kan avlyssnas eller tas upp, ska det lämnas en särskild upplysning om detta. Upplysningsplikten inträder när övervakningsutrustningen sätts upp. Den som bedriver övervakningen ska enligt 26 § på begäran även informera den övervakade om ändamålet med övervakningen. I vissa i 27 § angivna fall behöver det inte lämnas någon upplysning, t.ex. när övervakning bedrivs av en räddningsledare för att efterforska en försvunnen person.

Vidare följer av 32 § kameraövervakningslagen att bild- eller ljudmaterial från kameraövervakning av en plats dit allmänheten har tillträde får bevaras under högst två månader, om inte en längre bevarandetid beslutas. Material från övervakning av en plats dit

allmänheten inte har tillträde får inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med övervakningen. Material som inte längre får bevaras ska omedelbart förstöras.

I 37 § kameraövervakningslagen finns också en bestämmelse med rubriken tystnadsplikt och utlämnande av uppgifter. Av bestämmelsen följer att den som tar befattning med en uppgift som har inhämtats genom kameraövervakning inte obehörigen får röja eller utnyttja det som han eller hon på detta sätt har fått veta om någon enskilds personliga förhållanden. Vidare innehåller bestämmelsen en upplysning om att i det allmännas verksamhet ska i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400), OSL, tillämpas. Enligt 32 kap. 3 § OSL gäller sekretess för sådan uppgift om en enskilds personliga förhållanden som har inhämtats genom kameraövervakning som avses i kameraövervakningslagen, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Hos en domstol i dess rättskipande eller rättsvårdande verksamhet gäller sekretessen endast om det kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs. Av 12 kap. 1 § OSL följer att sekretess till skydd för en enskild inte gäller i förhållande till den enskilde själv, om inte annat anges i lagen.

Detta innebär att när det gäller kameraövervakning i det allmännas verksamhet kan en enskild normalt få tillgång till material från övervakningen som avser honom eller henne själv. Om materialet omfattar även andra personer, kan den enskilde få tillgång till materialet förutsatt att ett utlämnande inte är till men för någon sådan annan person eller dennes närstående. Detta gäller under förutsättning att det inte finns någon annan bestämmelse i OSL som reglerar sekretess i den aktuella verksamheten. Under motsvarande förutsättningar kan en enskild vid kameraövervakning i annan verksamhet än det allmännas få tillgång till material som avser honom eller henne själv. Vid tolkningen av bestämmelsen om tystnadsplikt för privata aktörer i 37 § kameraövervakningslagen ska ledning sökas i regleringen i OSL (se bl.a. prop. 2012/13:115 s. 161).

Det kan konstateras att förordningen innehåller omfattande rättigheter för registrerade och fler än vad som följer av kameraövervakningslagen men samtidigt ger visst utrymme för en medlemsstat att göra undantag från dessa rättigheter. Kameraövervakningslagens upplysningsplikt och tider för bevarande av bild- och ljudmaterial

från kameraövervakning är i huvudsak förenlig respektive är förenliga med förordningens rättigheter för registrerade och möjligheter att begränsa dessa rättigheter. Bestämmelserna om tystnadsplikt och utlämnande av uppgifter i lagen och i OSL är förenliga med förordningen. Förordningens rättigheter kommer att gälla direkt i Sverige, om inte svensk rätt innehåller andra bestämmelser. Vissa bestämmelser på kameraövervakningsområdet om upplysningsplikt och bevarandetider samt andra bestämmelser som innebär undantag från rättigheterna för de registrerade kan behållas eller införas i svensk lagstiftning som kompletterar förordningen.

7.1.11 Skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden

Bedömning: Kameraövervakningslagens skyldigheter avseende säkerhet vid kameraövervakning enligt 30 och 31 §§ överensstämmer med förordningens motsvarande skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden enligt artiklarna 24–43. Skyldigheterna enligt förordningen är fler än vad som följer av lagen. De innefattar inte något generellt krav på tillstånd eller anmälan men innebär bl.a. att en konsekvensbedömning ska göras och att ett samråd med tillsynsmyndigheten ska ske i vissa fall. Ett tillståndskrav för vissa särskilda fall får dock ställas upp i svensk rätt.

Bestämmelser på kameraövervakningsområdet om skyldigheter som enbart upprepar eller som avviker från innehållet i förordningen kan inte behållas eller införas i svensk lagstiftning som kompletterar förordningen. Lagstiftningen kan innehålla ett visst tillståndskrav.

Skälen för bedömningen

Allmänt om skyldigheterna

Kapitel IV i förordningen, artiklarna 24–43, innehåller långtgående skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden. Begreppen personuppgiftsansvarig och personuppgiftsbiträde definieras i artikel 4. I kapitlet finns bestämmelser om allmänna skyldig-

heter, säkerhet för personuppgifter, konsekvensbedömning och samråd med tillsynsmyndigheten, dataskyddsombud samt uppförandekoder och certifiering. Av skyldigheterna i kapitlet kan skyldigheten enligt artikel 34, som gäller information om en inträffad personuppgiftsincident, begränsas i nationell rätt med stöd av artikel 23.1. Denna begränsningsmöjlighet har behandlats i avsnitt 7.1.10 ovan.

Av intresse i detta sammanhang är främst de artiklar som behandlas i de två följande avsnitten.

Skyldigheter avseende säkerhet vid personuppgiftsbehandling

Artiklarna 25 och 32 innehåller relativt detaljerade bestämmelser om säkerhet vid behandling av personuppgifter. Vidare innehåller artikel 28 bestämmelser om vad som gäller när behandling av personuppgifter ska genomföras på en personuppgiftsansvarigs vägnar.

I kameraövervakningslagen finns skyldigheter avseende säkerhet vid kameraövervakning i 30 och 31 §§. Där föreskrivs bl.a. att den som bedriver kameraövervakning ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda bild- och ljudmaterial från övervakningen. Vidare anges vad som gäller om någon bedriver kameraövervakning för någon annans räkning. Bestämmelserna överensstämmer med förordningens motsvarande skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden. Skyldigheterna enligt förordningen är dock fler än vad som följer av lagen. Dessa kommer att gälla direkt i Sverige. Bestämmelser på kameraövervakningsområdet om skyldigheter som enbart upprepar eller som avviker från skyldigheterna enligt förordningen kan inte behållas eller införas i svensk lagstiftning som kompletterar förordningen.

Skyldigheter att göra en konsekvensbedömning och samråda

I artiklarna 35 och 36 finns bestämmelser om skyldighet att göra en konsekvensbedömning och skyldighet att samråda med tillsynsmyndigheten i vissa fall samt en möjlighet att i nationell rätt ställa upp ett tillståndskrav för vissa särskilda fall. Bestämmelserna har behandlats ingående i avsnitt 7.1.8 ovan och det hänvisas till det

avsnittet vad gäller innehållet i dessa. Här ska endast framhållas följande.

I kameraövervakningslagen finns inte några motsvarigheter till skyldigheterna i förordningen att i vissa fall göra en konsekvensbedömning och, beroende på utfallet av bedömningen, samråda med tillsynsmyndigheten. Däremot innehåller lagen ett generellt tillståndskrav och ett krav på anmälan i vissa fall som inte innefattas i förordningens skyldigheter. Skyldigheterna i förordningen kommer att gälla direkt i Sverige i den utsträckning det inte i stället ställs upp ett tillståndskrav i svensk rätt. Ett sådant kan gälla för viss kameraövervakning, nämligen sådan kameraövervakning som sker för att en uppgift av allmänt intresse ska kunna utföras. Vid kameraövervakning som inte kan omfattas av ett eventuellt svenskt tillståndskrav men som är särskilt integritetskänslig måste alltså den personuppgiftsansvarige göra en konsekvensbedömning av den planerade kameraövervakningen och eventuellt samråda med tillsynsmyndigheten om denna enligt förordningens bestämmelser. Myndigheten kan vidta åtgärder, t.ex. förbjuda övervakningen, om denna skulle strida mot förordningen.

Bestämmelser på kameraövervakningsområdet om skyldigheter som enbart upprepar eller som avviker från innehållet i förordningen kan inte behållas eller införas i svensk lagstiftning som kompletterar förordningen.

7.1.12 Rättsmedel, ansvar och sanktioner m.m.

Bedömning: Kameraövervakningslagens bestämmelser i 44–48 §§ om överklagande, skadestånd och straffansvar överensstämmer delvis med förordningens bestämmelser om rättsmedel, ansvar och sanktioner enligt artiklarna 77–84. Förordningens bestämmelser är mer omfattande än lagens.

Bestämmelser på kameraövervakningsområdet som enbart upprepar eller som avviker från innehållet i förordningen kan inte behållas eller införas i svensk lagstiftning som kompletterar förordningen. Vissa kompletterande processuella bestämmelser kan finnas i svensk rätt.

Förordningens bestämmelser om särskilda situationer av personuppgiftsbehandling enligt artiklarna 85–91 ger utrymme för

svensk lagstiftning eller saknar relevans på kameraövervakningsområdet. Med stöd av artikel 88 kan bestämmelser om kameraövervakning i anställningsförhållanden behållas eller införas i svensk lagstiftning som kompletterar förordningen.

Skälen för bedömningen

Rättsmedel, ansvar och sanktioner

I kapitel VIII i förordningen, artiklarna 77–84, finns bestämmelser om rättsmedel, ansvar och sanktioner. Även i bl.a. kapitel VII finns vissa bestämmelser om rättsmedel, artikel 58.4. Bestämmelserna är omfattande och innebär bl.a. följande.

En registrerad ska ha rätt att framföra klagomål hos tillsynsmyndigheten. Vidare ska fysiska och juridiska personer ha rätt till ett effektivt rättsmedel mot beslut av tillsynsmyndigheten som rör dem. En registrerad ska också ha rätt till ett effektivt rättsmedel direkt mot en personuppgiftsansvarig eller ett personuppgiftsbiträde, om den registrerade anser sig ha fått sina rättigheter enligt förordningen åsidosatta. Dessutom ska den som har lidit materiell eller immateriell skada till följd av en överträdelse av förordningen ha rätt till ersättning av den personuppgiftsansvarige eller personuppgiftsbiträdet under vissa förutsättningar. I förordningen regleras i vilken medlemsstat en talan om skadestånd ska väckas medan nationell rätt styr vilken domstol i den medlemsstaten som är behörig. Vid överträdelser av förordningen ska administrativa sanktionsavgifter kunna påföras. Dessutom kan sanktioner för överträdelser, särskilt för sådana som inte är föremål för administrativa sanktionsavgifter, fastställas genom nationell rätt. Dessa sanktioner ska vara effektiva, proportionella och avskräckande.

I 44–48 §§ kameraövervakningslagen finns vissa bestämmelser om överklagande, skadestånd och straffansvar. Enligt dessa får tillsynsmyndighetens beslut överklagas till allmän förvaltningsdomstol. Dessutom får beslut om tillstånd till kameraövervakning och om undantag från upplysningsplikten i vissa fall överklagas av den kommun där övervakningen ska ske och, om kameraövervakningen ska avse en arbetsplats, av en organisation som företräder de anställda på arbetsplatsen. Vidare ska den som bedriver kameraövervakning ersätta den övervakade för skada och kränkning av den

personliga integriteten som kameraövervakning i strid med lagen har orsakat. Slutligen ska den som uppsåtligen eller av oaktsamhet bryter mot exempelvis någon av bestämmelserna om tillståndsplikt, anmälningsplikt eller upplysningsplikt dömas till böter eller fängelse i högst ett år. Detsamma gäller den som bryter mot villkor i ett tillståndsbeslut.

Kameraövervakningslagens bestämmelser om överklagande, skadestånd och straffansvar överensstämmer alltså endast delvis med förordningens bestämmelser om rättsmedel, ansvar och sanktioner. Förordningens bestämmelser är mer omfattande än lagens. Samtidigt kräver förordningen t.ex. inte ett *straffrättsligt* ansvar. Flertalet av förordningens bestämmelser kommer att gälla direkt i Sverige. Bestämmelser på kameraövervakningsområdet som enbart upprepar eller som avviker från innehållet i förordningen kan inte behållas eller införas i svensk lagstiftning som kompletterar förordningen. Vissa kompletterande processuella bestämmelser kan finnas i svensk rätt.

Särskilda behandlingssituationer

I kapitel IX i förordningen, artiklarna 85–91, finns bestämmelser om särskilda situationer av behandling av personuppgifter, bl.a. behandling i förhållande till yttrande- och informationsfriheten och behandling i anställningsförhållanden. Dessa bestämmelser bedöms sakna relevans på kameraövervakningsområdet utom vad gäller artiklarna 85, 86, 88 och 90. Artiklarna 85 och 86 ger utrymme för en nationell reglering om förhållandet mellan, å ena sidan, skyddet för personuppgifter och, å andra sidan, yttrande- och informationsfriheten och offentlighetsprincipen. Artikel 90 behandlas i avsnitt 7.1.14.

Enligt artikel 88 får medlemsstaterna i lag eller i kollektivavtal fastställa mer specifika regler för att säkerställa skyddet av rättigheter och friheter vid behandling av personuppgifter i anställningsförhållanden, särskilt när det gäller t.ex. säkerhet på arbetsplatsen eller skydd av arbetsgivarens eller kundens egendom. Dessa regler ska innehålla lämpliga och specifika åtgärder för att skydda den registrerades mänskliga värdighet, berättigade intressen och grundläggande rättigheter, varvid hänsyn särskilt ska tas till insyn i behandlingen, överföring av personuppgifter inom en koncern eller

en grupp av företag som deltar i gemensam ekonomisk verksamhet samt övervakningssystem på arbetsplatsen. En medlemsstat ska anmäla sådana bestämmelser till kommissionen senast den 25 maj 2018 och även anmäla eventuella senare ändringar av bestämmelserna.

I kameraövervakningslagen finns vissa bestämmelser som tar sikte på kameraövervakning i anställningsförhållanden. Kameraövervakning får enligt 23 § ske efter en intresseavvägning eller, såvitt avser platser dit allmänheten har tillträde, efter tillstånd eller anmälan enligt 8 och 12–15 §§, se avsnitt 7.1.7. Enligt 17 § andra stycket ska en ansökan om tillstånd till kameraövervakning av en arbetsplats innehålla ett yttrande från skyddsombudet, skyddskommittén eller en organisation som företräder de anställda på arbetsplatsen. Detsamma gäller enligt 27 § tredje stycket vid en ansökan om undantag från upplysningsplikten. Enligt 47 § tredje stycket får beslut om tillstånd till kameraövervakning och om undantag från upplysningsplikten som avser en arbetsplats överklagas av en organisation som företräder de anställda på arbetsplatsen. För att kameraövervakning av butiker ska vara tillåten efter anmälan krävs enligt 13 § första stycket 3 att den som avser att bedriva övervakning har ingått en skriftlig överenskommelse om övervakningen med skyddsombudet, skyddskommittén eller en organisation som företräder de anställda på arbetsplatsen.

Bestämmelserna i kameraövervakningslagen bedöms vara förenliga med artikel 88. Med stöd av den artikeln kan bestämmelser om kameraövervakning i anställningsförhållanden behållas eller införas i svensk lagstiftning som kompletterar förordningen.

7.1.13 Överföring till tredjeland eller internationella organisationer

Bedömning: Kameraövervakningslagens bestämmelser i 34–36 §§ om överföring av bild- och ljudmaterial till tredjeland överensstämmer delvis med förordningens bestämmelser om överföring av personuppgifter till tredjeländer eller internationella organisationer enligt artiklarna 44–50.

Bestämmelser på kameraövervakningsområdet om överföring som enbart upprepar eller som avviker från innehållet i förord-

ningen kan inte behållas eller införas i svensk lagstiftning som kompletterar förordningen.

Skälen för bedömningen: I kapitel V i förordningen, artiklarna 44–50, regleras under vilka förutsättningar personuppgifter får överföras till tredjeland eller till internationella organisationer. Huvudregeln är att en överföring är tillåten, om det mottagande tredjelandet eller den mottagande organisationen kan säkerställa en adekvat skyddsnivå för uppgifterna. Det är kommissionen som beslutar om ett tredjeland eller en organisation uppfyller detta krav eller inte. Om kommissionen inte har fattat något sådant beslut, är det tillåtet att överföra personuppgifter förutsatt att den som ska överföra uppgifterna vidtar vissa lämpliga skyddsåtgärder, t.ex. använder standardiserade dataskyddsbestämmelser. Därutöver får överföring av personuppgifter ske i vissa undantagssituationer. Det gäller bl.a. när den registrerade har samtyckt till överföringen och när överföringen är nödvändig i vissa avtalssituationer, av viktiga skäl som rör ett allmänintresse som är erkänt i unionsrätten eller i nationell rätt, för att göra gällande rättsliga anspråk eller för att skydda enskildas grundläggande intressen. Vissa av dessa undantag får dock inte åberopas av myndigheter.

I 34–36 §§ kameraövervakningslagen finns vissa bestämmelser om överföring till tredjeland av bild- och ljudmaterial från kameraövervakning som innehåller personuppgifter. Även vissa bestämmelser i personuppgiftsförordningen (1998:1191) är av intresse. Av bestämmelserna följer bl.a. att en överföring får ske, om det finns en adekvat nivå för skyddet av personuppgifterna i det mottagande landet, om samtycke från den övervakade föreligger eller om överföringen är nödvändig med avseende på vissa avtalssituationer, rättsliga anspråk eller vitala intressen för den övervakade. Bestämmelserna reglerar inte överföringar till internationella organisationer.

Kameraövervakningslagens bestämmelser om överföring av bild- och ljudmaterial till tredjeland överensstämmer endast delvis med förordningens bestämmelser om överföring av personuppgifter till tredjeländer eller internationella organisationer. Förordningens artiklar om överföring kommer framöver att gälla direkt i Sverige. Bestämmelser på kameraövervakningsområdet om överföring som enbart upprepar eller som avviker från innehållet i förordningen

kan inte behållas eller införas i svensk lagstiftning som kompletterar förordningen.

7.1.14 Tillsyn

Bedömning: Kameraövervakningslagens bestämmelser i 38–43 §§ om tillsyn överensstämmer delvis med förordningens bestämmelser om tillsyn och samarbete mellan tillsynsmyndigheter enligt artiklarna 51–76 och artikel 90. Förordningens bestämmelser är mer omfattande än lagens.

Bestämmelser på kameraövervakningsområdet om tillsyn som enbart upprepar eller som avviker från innehållet i förordningen kan inte behållas eller införas i svensk lagstiftning som kompletterar förordningen. Vissa svenska kompletterande bestämmelser om tillsyn måste behållas eller införas. Svenska bestämmelser om ytterligare befogenheter för en tillsynsmyndighet utöver de som följer av förordningen får behållas eller införas.

Skälen för bedömningen: I kapitel VI i förordningen, artiklarna 51–59 finns bestämmelser om tillsyn. Bestämmelserna innebär att medlemsstaterna ska utse en eller flera självständiga tillsynsmyndigheter som ska ansvara för att övervaka tillämpningen av förordningen. Bestämmelserna innehåller en detaljerad reglering av tillsynsmyndighetens oberoende ställning och myndighetens behörighet samt uppgifter och befogenheter, såväl utredningsbefogenheter som korrigerande befogenheter. I några avseenden förutsätter eller tillåter förordningen kompletterande nationell reglering. Det gäller exempelvis tillsynsmyndighetens befogenheter. Det är också upp till medlemsstaterna att inom vissa ramar reglera bl.a. tillsynsmyndighetens organisation och utnämning respektive avsättande av myndighetens medlemmar.

Vidare finns i kapitel VII i förordningen, artiklarna 60–76, bestämmelser som förpliktar en nationell tillsynsmyndighet att samarbeta med och assistera tillsynsmyndigheterna i andra medlemsstater.

Slutligen finns i artikel 90 i kapitel IX en bestämmelse som ger utrymme för nationella regler om hur tillsynsmyndighetens befogenheter förhåller sig till personuppgiftsansvariga som omfattas av tystnadsplikt.

Även i kameraövervakningslagen finns i 38–43 §§ vissa bestämmelser om tillsyn. Till dessa anknyter bestämmelser i kameraövervakningsförordningen (2013:463). Enligt bestämmelserna är det Datainspektionen som har det centrala ansvaret för tillsynen enligt lagen. Datainspektionen utövar vidare den operativa tillsynen över kameraövervakning av platser dit allmänheten inte har tillträde. Däremot är det enligt lagen länsstyrelserna som utövar den operativa tillsynen över kameraövervakning av platser dit allmänheten har tillträde och som ska se till att tillståndskravet och anmälningsplikten för uppsatta övervakningskameror som inte har tagits i bruk följs. Vidare ger lagen tillsynsmyndigheterna vissa befogenheter exempelvis en rätt att meddela förelägganden och en rätt att få tillträde till övervakningsanläggningar. Några bestämmelser om samarbete med andra länders tillsynsmyndigheter på kameraövervakningsområdet finns inte i lagen.

Kameraövervakningslagens bestämmelser om tillsyn överensstämmer följaktligen endast delvis med förordningens bestämmelser om tillsyn och samarbete mellan tillsynsmyndigheter. Förordningens bestämmelser är mer omfattande än lagens. Flertalet av dessa kommer att gälla direkt i Sverige. Bestämmelser på kameraövervakningsområdet om tillsyn som enbart upprepar eller som avviker från innehållet i förordningen kan inte behållas eller införas i svensk lagstiftning som kompletterar förordningen. Vissa svenska kompletterande bestämmelser om tillsyn måste behållas eller införas. Det gäller bl.a. bestämmelser om vilken myndighet eller vilka myndigheter som ska utöva tillsyn på kameraövervakningsområdet. Vidare får svenska bestämmelser om ytterligare befogenheter för en tillsynsmyndighet utöver de som följer av förordningen behållas eller införas.

7.1.15 Sammanfattande slutsats

Bedömning: Förordningen, som kommer att gälla direkt i Sverige, innebär att många av kameraövervakningslagens bestämmelser inte kan behållas alls eller inte kan behållas i sin nuvarande form vad gäller kameraövervakning som omfattas av förordningens tillämpningsområde.

Skälen för bedömningen: Av avsnitten ovan har framgått att kameraövervakning kan utgöra behandling av personuppgifter som omfattas av förordningen. Vidare har framgått att förordningen kommer att gälla direkt i Sverige och att bestämmelser om kameraövervakning som upprepar eller avviker från innehållet i förordningen därför inte kan behållas i svensk lagstiftning som kompletterar förordningen annat än om förordningen lämnar utrymme för sådana bestämmelser. Som också framgått kan många av kameraövervakningslagens bestämmelser inte behållas alls eller inte behållas i sin nuvarande form vad gäller kameraövervakning som omfattas av förordningens tillämpningsområde.

7.2 Dataskyddsdirektivet

7.2.1 Allmänt om direktivet och kameraövervakningslagen

Bedömning: Kameraövervakning enligt kameraövervakningslagen (2013:460) kan utgöra personuppgiftsbehandling som omfattas av dataskyddsdirektivet. Eftersom direktivet ska genomföras i svensk rätt, måste kameraövervakning som faller in under direktivets tillämpningsområde omfattas av bestämmelser i svensk lagstiftning som uppfyller direktivets krav. Det måste därför analyseras hur bestämmelserna i kameraövervakningslagen förhåller sig till kraven enligt direktivet.

Skälen för bedömningen: EU-direktiv ska genomföras i medlemsstaternas nationella rätt. Enligt artikel 288 i fördraget om Europeiska unionens funktionssätt är direktiv bindande för medlemsstaterna när det gäller det resultat som ska uppnås. Det överlåts i princip åt medlemsstaterna att bestämma form och tillvägagångssätt för

genomförandet. Det innebär att medlemsstaterna inte är bundna av ett direktivs terminologi eller systematik, om det avsedda resultatet kan uppnås på annat sätt.

Det nya dataskyddsdirektivet, som presenterats i avsnitt 6.3, ska alltså genomföras i svensk rätt. Det betyder att det i svensk rätt måste finnas bestämmelser om behandling av personuppgifter som uppfyller direktivets krav. Genomförandet ska ha skett senast den 6 maj 2018.

Kameraövervakning enligt kameraövervakningslagen (2013:460) kan utgöra personuppgiftsbehandling som omfattas av direktivet. Eftersom direktivet ska genomföras i svensk rätt, måste kameraövervakning som faller in under direktivets tillämpningsområde omfattas av bestämmelser i svensk lagstiftning som uppfyller direktivets krav. Det måste därför göras en analys av hur bestämmelserna i kameraövervakningslagen förhåller sig till kraven enligt direktivet. Denna analys görs i de följande avsnitten. Däremot görs inte några uttryckliga bedömningar av om lagens olika bestämmelser kan behållas eller måste ändras. Det är inte givet att ett svenskt genomförande av direktivet på kameraövervakningsområdet måste ske genom att bestämmelserna i kameraövervakningslagen behålls i de delar som de uppfyller direktivets krav och ändras i de delar som direktivet kräver det. Ett alternativ kan vara att allmänna bestämmelser om behandling av personuppgifter i andra författningar om personuppgiftsbehandling helt eller delvis får reglera sådan kameraövervakning som omfattas av direktivets tillämpningsområde. En annan variant är att särskilda bestämmelser om kameraövervakning tas in i en helt ny lag. Dessa frågor diskuteras i avsnitt 9.1. Oavsett vilket alternativ som väljs måste sådan kameraövervakning som träffas av direktivet omfattas av svenska bestämmelser som är förenliga med kraven i direktivet.

Redan här ska nämnas att direktivet enligt artikel 1.3 inte hindrar medlemsstaterna från att föreskriva starkare skyddsåtgärder än de som fastställs i direktivet. Detta innebär att direktivets bestämmelser utgör en miniminivå som medlemsstaternas nationella rätt ska nå upp till vad gäller skyddet för personuppgifter. Det finns alltså ett utrymme att behålla eller införa bestämmelser i svensk rätt som ställer upp strängare krav än de som följer av direktivet. Utrymmet begränsas av att sådana bestämmelser inte får komma i konflikt med direktivets bestämmelser.

7.2.2 Direktivets syfte

Bedömning: Kameraövervakningslagens syfte enligt 1 § är förenligt med direktivets syfte enligt artikel 1.

En svensk lagstiftning som omfattar kameraövervakning kan innehålla en bestämmelse om syftet med bestämmelser om kameraövervakning, som då måste uppfylla direktivets krav.

Skälen för bedömningen: Enligt artikel 1 i direktivet är syftet med direktivet dels att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, dels att säkerställa att sådant informationsutbyte mellan behöriga myndigheter som är nödvändigt enligt unionsrätten eller nationell rätt inte begränsas. Syftet är formulerat på ett sätt som liknar syftet enligt förordningen, som behandlats i avsnitt 7.1.2.

Syftet med kameraövervakningslagen anges i 1 § vara att tillgodose behovet av kameraövervakning för berättigade ändamål samtidigt som enskilda skyddas mot otillbörliga intrång i den personliga integriteten. Lagen har ett vidare tillämpningsområde än direktivet och syftesbestämmelsen kan därför sägas vara vidare än direktivets artikel 1. Direktivet omfattar endast personuppgiftsbehandling som behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, se närmare nedan. Syftet med kameraövervakningslagen är dock i relevant del förenligt med direktivets syfte.

En svensk lagstiftning som omfattar kameraövervakning kan, men måste inte, innehålla en bestämmelse om syftet med bestämmelser om kameraövervakning. En sådan syftesbestämmelse måste då uppfylla direktivets krav.

7.2.3 Direktivets tillämpningsområde

Bedömning: Kameraövervakningslagens kameraövervakningsbegrepp enligt 2 § överensstämmer delvis med direktivets begrepp personuppgiftsbehandling enligt artiklarna 2.2 och 3. Lagens tillämpningsområde i övrigt enligt 2–5 §§ överensstämmer med direktivets tillämpningsområde enligt artiklarna 2 och 3.

En svensk lagstiftning som omfattar kameraövervakning kan ha ett tillämpningsområde som är vidare eller, förutsatt att annan svensk lagstiftning då gäller, snävare än vad som följer av direktivet.

Skälen för bedömningen

Begreppet personuppgiftsbehandling och begreppet kameraövervakning

Frågan hur kameraövervakningslagens kameraövervakningsbegrepp enligt 2 § förhåller sig till förordningens begrepp personuppgiftsbehandling har behandlats i avsnitt 7.1.3. Där har sammanfattningsvis gjorts den bedömningen att begreppet kameraövervakning endast delvis överensstämmer med begreppet personuppgiftsbehandling enligt förordningen. I avsnitt 7.1.5 har också berörts om användning av kamerautrustade drönare och annan ny kamerateknik omfattas av lagen.

Personuppgiftsbehandling definieras på samma sätt i direktivet i artiklarna 2.2 och 3 som i förordningen. Samma bedömning görs därför vad gäller hur begreppet kameraövervakning förhåller sig till direktivets begrepp. Kameraövervakningsbegreppet överensstämmer alltså inte fullt ut med direktivets begrepp personuppgiftsbehandling.

En svensk lagstiftning som omfattar kameraövervakning kan ha ett kameraövervakningsbegrepp som är vidare eller, förutsatt att annan svensk lagstiftning då gäller, snävare än sådan kameraövervakning som innefattas i direktivets begrepp personuppgiftsbehandling. Ett kameraövervakningsbegrepp måste innehålla vissa avgränsningar som skiljer denna form av personuppgiftsbehandling från annan behandling av personuppgifter. Det kan finnas anledning att avgränsa begreppet på ett annat sätt än vad som gäller i dag enligt kameraövervakningslagen.

Vilka subjekt och vilka verksamheter omfattas av direktivet?

Enligt artikel 2.1 jämförd med artikel 1.1 omfattar direktivet personuppgiftsbehandling som behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa

straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Enligt artikel 3.7 avses med behörig myndighet

a) en offentlig myndighet som har behörighet att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga hot mot den allmänna säkerheten, eller

b) annat organ eller annan enhet som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten.

Direktivet gäller alltså myndigheter som har i uppgift att bedriva verksamhet som avser brottsbekämpning, brottmålshantering och straffverkställighet och andra subjekt som genom nationell rätt har anförtrotts myndighetsutövning för sådan verksamhet. Begreppet *brott* i direktivet är enligt skäl 13 i direktivets ingress ett självständigt unionsrättsligt begrepp. Begreppet har i tidigare lagstiftningsärenden som avsett EU-instrument tolkats så att det omfattar såväl konkreta brott som icke-preciserad brottslig verksamhet (prop. 2012/13:73 s. 63). Samma tolkning görs nu. Detta innebär att direktivet omfattar både vad som i svensk rätt brukar benämnas underrättelseverksamhet och verksamhet som går ut på att utreda och beivra konkreta brott. Direktivet omfattar också ännu inte inträffade brott som en särskild åtgärd vidtagits mot, såsom kameraövervakning, just för att förebygga brotten.

I direktivet finns inte några bestämmelser om direktivets territoriella tillämpningsområde. Tillämpningsområdet i det hänseendet följer dock indirekt av bestämmelserna om det materiella tillämpningsområdet.

Frågan om vilka svenska myndigheter som omfattas av direktivet har analyserats och beskrivits av den i avsnitt 2.1.4 presenterade Utredningen om 2016 års dataskyddsdirektiv. Enligt utredningen ska de myndigheter som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet omfattas. Som exempel anges Polismyndigheten, Kust-

bevakningen, Skatteverket, Tullverket, Åklagarmyndigheten, Ekobrottsmyndigheten, de allmänna domstolarna och Kriminalvården.

Det innebär att kameraövervakning som utgör personuppgiftsbehandling och som förekommer i brottsbekämpande verksamhet hos t.ex. Polismyndigheten, Kustbevakningen och Tullverket faller in under direktivets tillämpningsområde. Detsamma gäller t.ex. eventuellt förekommande kameraövervakning i verksamhet som bedrivs av de allmänna domstolarna på det straffrättsliga och straffprocessuella området eller i samband med verkställande av straffrättsliga påföljder hos främst Kriminalvården. Eventuell kameraövervakning vid andra myndigheter, exempelvis Statens institutionsstyrelse, kan också i vissa fall omfattas av direktivet.

Av artikel 9.2 följer att om de behöriga myndigheterna genom nationell rätt anförtros att utföra andra uppgifter än brottsbekämpning, brottmålshantering och straffverkställighet är i stället förordningen tillämplig på personuppgiftsbehandling för dessa ändamål. Vidare får enligt artikel 9.1 uppgifter som samlas in av behöriga myndigheter i syfte att bekämpa brott, hantera brottmål eller verkställa straff endast behandlas för andra ändamål om det är tillåtet enligt unionsrätten eller nationell rätt. När personuppgifter behandlas för andra ändamål ska förordningen tillämpas såvida inte behandlingen utgör ett led i en verksamhet som överhuvudtaget inte omfattas av unionsrätten.

De svenska myndigheter som nämnts ovan ska alltså tillämpa bestämmelserna i förordningen när de behandlar personuppgifter i verksamhet som utförs i annat syfte än att bekämpa brott, hantera brottmål eller verkställa straff. Exempelvis kommer kameraövervakning som bedrivs av Polismyndigheten i syfte att förhindra eller begränsa verkningarna av olyckor att falla in under förordningens tillämpningsområde förutsatt att verksamheten inte kan anses avse förebyggande av hot mot den allmänna säkerheten.

Vid en jämförelse mellan direktivets tillämpningsområde och kameraövervakningslagens tillämpningsområde kan det konstateras att lagen omfattar sådana myndigheter och andra subjekt samt verksamheter som avses i direktivet. Det gäller dock inte hemlig kameraövervakning, som enligt 4 § undantas från lagens tillämpningsområde. Hemlig kameraövervakning regleras i stället i 27 kap. rättegångsbalken och i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. I kameraövervakningslagen finns i 3 §

särskilda bestämmelser om lagens territoriella tillämpningsområde, som innefattar kameraövervakning av myndigheter och andra i de verksamheter som avses i direktivet.

Slutligen ska nämnas att det i artikel 2 i direktivet finns vissa undantag från direktivets tillämpningsområde. Av intresse i detta sammanhang är det undantag som framgår av artikel 2.3 a. Där anges att direktivet inte ska tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten. I skäl 14 i ingressen till direktivet ges som exempel verksamhet som rör nationell säkerhet, verksamhet som utförs av byråer och organ som hanterar nationella säkerhetsfrågor och medlemsstaternas behandling av personuppgifter när de utför verksamhet som gäller den gemensamma utrikes- och säkerhetspolitiken enligt avdelning V kapitel 2 i EU-fördraget.

Detta innebär för svenskt vidkommande att kameraövervakning i vissa svenska verksamheter faller utanför direktivets tillämpningsområde. Det gäller bl.a. normalt för kameraövervakning i Säkerhetspolisens verksamhet och i försvarets verksamhet. Sådan kameraövervakning omfattas däremot av kameraövervakningslagen. Lagens tillämpningsområde i de nu diskuterade avseendena hindras inte av direktivet. I sammanhanget ska också nämnas att det i lagens 5 § finns ett undantag för fysiska personers privata kameraövervakning. Detta undantag saknar relevans på direktivets område.

Sammanfattningsvis överensstämmer kameraövervakningslagens tillämpningsområde i nu diskuterade avseenden med direktivets tillämpningsområde. En svensk lagstiftning som omfattar kameraövervakning kan i och för sig ha ett tillämpningsområde som är vidare eller, förutsatt att annan svensk lagstiftning då gäller, snävare än vad som följer av direktivet. Ett vidare territoriellt tillämpningsområde torde dock inte vara möjligt.

7.2.4 Definitioner, principer, laglig personuppgiftsbehandling och kameraövervakning, m.m.

Bedömning: Kameraövervakningslagens definitioner enligt 2 §, utöver de som behandlats i avsnitt 7.2.3, är förenliga med direktivets definitioner enligt artikel 3.

Lagens allmänna krav för kameraövervakning enligt 7 § och bestämmelser om behandling av bild- och ljudmaterial i 28–31 §§ överensstämmer delvis med direktivets principer enligt artiklarna 4–11.

Lagens tider för bevarande av bild- och ljudmaterial från kameraövervakning enligt 32 och 33 §§ är förenliga med direktivets krav på tidsgränser för lagring av personuppgifter enligt artikel 5.

Lagens bestämmelser i 8–24 och 49 §§ om när kameraövervakning är tillåten är förenliga med direktivets bestämmelser om när personuppgiftsbehandling är laglig enligt artikel 8. Lagens bestämmelse om när det krävs tillstånd till kameraövervakning är förenlig med artikel 1.3.

En svensk lagstiftning som omfattar kameraövervakning måste uppfylla direktivets krav vad gäller definitioner, principer, tidsgränser för lagring och laglig behandling av personuppgifter. Lagstiftningen kan innehålla t.ex. ett krav på tillstånd för att kameraövervakning ska få ske.

Skälen för bedömningen

Allmänt

I kapitel I och II i direktivet med allmänna bestämmelser och principer, artikel 3 respektive artiklarna 4–11, finns, utöver de tidigare behandlade artiklarna om bl.a. syfte och tillämpningsområde, ett antal artiklar av intresse i detta sammanhang. Det gäller främst bestämmelser om definitioner, principer för behandling av personuppgifter, tidsgränser för lagring, laglig – dvs. tillåten – behandling av personuppgifter och behandling av särskilda kategorier av personuppgifter.

Definitioner

I artikel 3 finns ett flertal definitioner av olika begrepp som används i direktivet. Flertalet av definitionerna överensstämmer helt eller i allt väsentligt med definitionerna av samma begrepp i förordningen. Det gäller t.ex. begreppen *personuppgiftsansvarig* och *personuppgiftsbiträde*. Begreppet personuppgiftsbehandling och hur begreppet kameraövervakning förhåller sig till detta har behandlats ovan.

Vid en jämförelse mellan kameraövervakningslagens övriga definitioner enligt 2 § och direktivets definitioner kan det konstateras att lagen saknar ett antal definitioner som finns i direktivet samtidigt som den innehåller definitioner som inte har några motsvarigheter i direktivet. Som exempel på det senare kan nämnas lagens definition av samtycke. Samtycke torde, som framgår nedan, inte kunna utgöra en grund för behandling av personuppgifter enligt direktivet och saknar därför relevans på direktivets område.

Kameraövervakningslagens definitioner är förenliga med direktivets definitioner. En svensk lagstiftning som omfattar kameraövervakning måste innehålla definitioner eller andra bestämmelser vars innehåll uppfyller direktivets krav vad gäller definitioner. Direktivet hindrar inte att en sådan lagstiftning innehåller andra definitioner än de som finns i direktivet.

Principer

Artikel 4 innehåller vissa principer för behandling av personuppgifter. Dessa krav utgör tillsammans med kravet på rättslig grund enligt artikel 8 de allmänna förutsättningarna för att en behandling av personuppgifter ska vara tillåten. I direktivet finns sedan ett flertal artiklar med ett närmare innehåll som bygger på dessa principer. Enligt artikel 4 ska medlemsstaterna föreskriva att personuppgifter ska

a) behandlas på ett lagligt och korrekt sätt,

b) samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte behandlas på ett sätt som står i strid med dessa ändamål,

c) vara adekvata, relevanta och inte för omfattande i förhållande till de syften för vilka de behandlas,

d) vara korrekta och, om nödvändigt, uppdaterade; alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål,

e) inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas, och

f) behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna med användning av lämpliga tekniska eller organisatoriska åtgärder.

Kameraövervakningslagen innehåller flera bestämmelser vars innehåll kan sägas motsvara principerna enligt artikel 4. Av 7 § följer att som allmänna krav för kameraövervakning gäller att övervakning ska bedrivas lagligt, enligt god sed och med tillbörlig hänsyn till enskildas personliga integritet. Vidare regleras i 28–33 §§ hur bild- och ljudmaterial från kameraövervakning får behandlas. Till exempel anges att den som bedriver kameraövervakning inte får behandla bild- och ljudmaterial från övervakningen för något ändamål som är oförenligt med det som materialet samlades in för. Det finns också exempelvis angivet hur länge material från kameraövervakning får bevaras, se vidare nedan. Lagens allmänna krav för kameraövervakning och bestämmelser om behandling av bild- och ljudmaterial överensstämmer dock endast delvis med direktivets principer enligt artikel 4. En svensk lagstiftning som omfattar kameraövervakning måste uppfylla direktivets krav vad gäller principer.

Tidsgränser för lagring

Enligt artikel 5 ska medlemsstaterna föreskriva att lämpliga tidsgränser fastställs för radering av personuppgifter eller för periodisk översyn av behovet av att lagra personuppgifter. Procedurrelaterade åtgärder ska enligt artikeln säkerställa att tidsgränserna efterlevs.

I 32 och 33 §§ kameraövervakningslagen finns bestämmelser om hur länge bild- och ljudmaterial från kameraövervakning får bevaras. Material från kameraövervakning av en plats dit allmänheten har tillträde får bevaras under högst två månader, om inte en längre bevarandetid beslutas. Material från övervakning av en plats dit

allmänheten saknar tillträde får inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med övervakningen. När materialet inte längre får bevaras ska det omedelbart förstöras. Bestämmelserna är förenliga med direktivets krav. En svensk lagstiftning som omfattar kameraövervakning måste uppfylla direktivets krav vad gäller tidsgränser för lagring.

Laglig personuppgiftsbehandling och kameraövervakning

Enligt artikel 8 ska personuppgiftsbehandling vara laglig endast om och i den mån behandlingen är nödvändig för att utföra en uppgift som utförs av en behörig myndighet för de ändamål som anges i artikel 1.1 och som sker på grundval av unionsrätten eller nationell rätt. Den nationella rätt som reglerar behandling ska åtminstone specificera syftet med behandlingen, vilka personuppgifter som ska behandlas och behandlingens ändamål. Enligt Utredningen om 2016 års dataskyddsdirektiv innebär detta att personuppgiftsbehandling ska ha stöd i myndighetens arbetsuppgifter så som de kommer till uttryck i unionsrätten eller nationell lagstiftning och andra bindande beslut. Utredningen har föreslagit att det ska framgå av den generella lag som utredningen har föreslagit ska genomföra direktivet, brottsdatalagen. Samma bedömning görs i detta sammanhang. Det innebär att det måste finnas författningsstöd för att svenska behöriga myndigheter ska kunna bedriva kameraövervakning för brottsbekämpning, brottmålshantering och straffverkställighet. Motsvarande bedömning har gjorts i fråga om en liknande artikel i förordningen, se avsnitt 7.1.8. Artikel 8 innebär alltså inte ett krav på stöd i nationell rätt för den specifika behandlingsåtgärden, t.ex. kameraövervakning.

I sammanhanget ska också kort nämnas artikel 1.3, som behandlas närmare i avsnitt 7.2.6 nedan. Enligt den artikeln får en medlemsstat föreskriva starkare skyddsåtgärder än de som följer av direktivet.

I 8–24 och 49 §§ kameraövervakningslagen finns flera bestämmelser som anger när kameraövervakning är tillåten och ett antal därtill anknytande bestämmelser. Som huvudregel gäller att det krävs tillstånd till kameraövervakning av platser dit allmänheten har tillträde och att ett sådant ska ges om intresset av övervakning väger

tyngre än den enskildes intresse av att inte bli övervakad. Vid bedömningen av övervakningsintresset ska särskilt beaktas bl.a. om övervakningen behövs för att förebygga, avslöja eller utreda brott. I några fall får kameraövervakning bedrivas under högst en månad utan att en ansökan om tillstånd har gjorts. Det gäller t.ex. övervakning som bedrivs av Polismyndigheten när det finns risk för att viss allvarlig brottslighet kommer att begås. Vidare är övervakning av vissa särskilda platser dit allmänheten har tillträde tillåten efter endast en anmälan. Sådan kameraövervakning torde dock inte bedrivas i de verksamheter som omfattas av direktivet. Kameraövervakning av en plats dit allmänheten inte har tillträde är tillåten bl.a. om övervakningen behövs för att förebygga, avslöja eller utreda brott och övervakningsintresset väger tyngre än den enskildes intresse av att inte bli övervakad.

De myndigheter och andra subjekt samt verksamheter som avses i direktivet har stöd i gällande svensk rätt för sina verksamheter. Kameraövervakningslagens bestämmelser i 8–24 §§ om när kameraövervakning är tillåten är förenliga med direktivets bestämmelser om när personuppgiftsbehandling är laglig enligt artikel 8. Lagens bestämmelse om när det krävs tillstånd till kameraövervakning är förenlig med artikel 1.3, som ger utrymme för t.ex. ett krav på tillstånd i nationell rätt. Det ska samtidigt understrykas att kameraövervakning inom direktivets tillämpningsområde inte kan bedrivas med stöd av samtycke. Detta torde dock inte heller förekomma.

En svensk lagstiftning som omfattar kameraövervakning måste uppfylla direktivets krav vad gäller laglig behandling av personuppgifter. Lagstiftningen kan innehålla t.ex. ett krav på tillstånd för att kameraövervakning ska få ske.

Särskilda kategorier av personuppgifter

Enligt artikel 10 ska behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att unikt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning endast vara tillåten under vissa förutsättningar. Biometriska uppgifter definieras i artikel 3.13 som upp-

gifter som erhållits genom en teknisk behandling avseende en persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör unik identifiering av personen. Av ingressen till förordningen, men inte till direktivet, framgår att behandling av foton inte systematiskt omfattas, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person. Motsvarande måste antas gälla i fråga om direktivet. Behandling av sådana uppgifter som omfattas av artikel 10 får bl.a. ske när det är absolut nödvändigt, det finns lämpliga skyddsåtgärder för den registrerades rättigheter och friheter och behandlingen är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt.

Sådana känsliga uppgifter som omfattas av artikel 10 kan i och för sig samlas in genom kameraövervakning. Artikeln måste dock anses gälla när kameraövervakningen sker enbart på grund av de avbildade personernas ras eller etniska ursprung etc. Samma bedömning har gjort i avsnitt 7.1.7 i fråga om motsvarande bestämmelse i förordningen. Bilder på människor i mer ”normala” sammanhang kan inte anses avslöja några känsliga personuppgifter.

7.2.5 Rättigheter för registrerade

Bedömning: Kameraövervakningslagens upplysningsplikt enligt 25–27 §§ är i huvudsak förenlig med direktivets rättigheter för registrerade och möjligheter att begränsa dessa rättigheter enligt artiklarna 12–18. Bestämmelser om tystnadsplikt och utlämnande av uppgifter i 37 § kameraövervakningslagen och i offentlighets- och sekretesslagen (2009:400) är förenliga med direktivet. Rättigheterna enligt direktivet är fler än vad som följer av lagen.

En svensk lagstiftning som omfattar kameraövervakning måste innehålla bestämmelser om rättigheter för registrerade eller om undantag från rättigheterna som uppfyller direktivets krav.

Skälen för bedömningen: Kapitel III i direktivet, artiklarna 12–18, innehåller bestämmelser om registrerades rättigheter. Rättigheterna gäller information och tillgång till personuppgifter, rättelse och radering samt begränsning av behandling. Vissa av artiklarna innehåller också bestämmelser som ger medlemsstaterna möjlighet att

begränsa rättigheterna. Enligt artikel 18 får medlemsstaterna föreskriva att vissa av rättigheterna ska utövas i enlighet med nationell rätt, om personuppgifterna ingår i ett domstolsbeslut eller ett rättsligt protokoll eller ett ärende som behandlas i samband med brottsutredningar och straffrättsliga förfaranden. Rent nationell rätt kan alltså reglera behandling av material från kameraövervakning inom ramen för ett sådant förfarande.

I artiklarna 12 och 13 finns detaljerade bestämmelser om information som en personuppgiftsansvarig ska lämna till den registrerade. Informationen ska tillhandahållas på lämpligt sätt, t.ex. elektroniskt, och lämnas i en koncis, begriplig och lättillgänglig form samt på ett klart och tydligt språk. Vidare ska den personuppgiftsansvarige göra åtminstone följande information tillgänglig för den registrerade.

a) Den personuppgiftsansvariges identitet och kontaktuppgifter.

b) Dataskyddsombudets kontaktuppgifter, i tillämpliga fall.

c) Ändamålen med den behandling för vilken personuppgifterna är avsedda.

d) Rätten att lämna in klagomål till en tillsynsmyndighet samt tillsynsmyndighetens kontaktuppgifter.

e) Rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter och begränsning av behandlingen av personuppgifter som rör den registrerade.

Att informationen ska göras tillgänglig får förstås så att informationen inte faktiskt måste lämnas till varje enskild registrerad. Stöd för denna bedömning finns i skäl 42 i ingressen till direktivet där det anges att informationen kan lämnas på den behöriga myndighetens webbplats.

Därutöver ska den personuppgiftsansvarige i specifika fall lämna viss ytterligare information till den registrerade för att göra det möjligt för honom eller henne att utöva sina rättigheter. Det gäller bl.a. information om behandlingens rättsliga grund och den period under vilken personuppgifterna kommer att lagras. Det är dock möjligt att under vissa förutsättningar begränsa rätten till denna information.

Enligt 25 § kameraövervakningslagen gäller som huvudregel en upplysningsplikt vid all kameraövervakning som omfattas av lagen.

Upplysning om kameraövervakning ska lämnas genom tydlig skyltning eller på något annat verksamt sätt. Upplysning ska också lämnas om vem som bedriver kameraövervakningen, om detta inte framgår av förhållandena på platsen. Om ljud kan avlyssnas eller tas upp vid övervakningen, ska det lämnas en särskild upplysning om detta. Upplysningsplikten inträder när övervakningsutrustningen sätts upp. Den som bedriver övervakningen ska enligt 26 § på begäran även informera den övervakade om ändamålet med övervakningen. I vissa i 27 § angivna fall behöver det inte lämnas någon upplysning.

Kameraövervakningslagens upplysningsplikt ligger i linje med direktivets reglering om information enligt artiklarna 12 och 13 men överensstämmer inte helt med denna.

Direktivet innehåller vidare i artiklarna 14–17 bestämmelser om den registrerades rätt att få tillgång till personuppgifter och att få uppgifter rättade, kompletterade eller raderade samt bestämmelser om begränsning av behandling, t.ex. när den registrerade bestrider uppgifternas korrekthet och denna inte kan fastställas. Vissa av dessa rättigheter kan inskränkas, t.ex. om syftet är undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller om syftet är att skydda den allmänna säkerheten eller andra personers rättigheter och friheter.

Kameraövervakningslagen innehåller inte några bestämmelser som uttryckligen ger den övervakade rätt att få tillgång till personuppgifter i form av bild- eller ljudmaterial från kameraövervakning. I lagens 37 § finns en bestämmelse om tystnadsplikt och utlämnande av uppgifter. Bestämmelsen och bestämmelser om utlämnande av uppgifter i offentlighets- och sekretesslagen (2009:400) har behandlats i avsnitt 7.1.10.

Slutligen kan det konstateras att rättigheterna enligt direktivet är fler än vad som följer av kameraövervakningslagen, som t.ex. saknar bestämmelser om rätt till rättelse eller radering.

Sammanfattningsvis görs bedömningen att kameraövervakningslagens upplysningsplikt i huvudsak är förenlig med direktivets rättigheter för registrerade och möjligheter att begränsa dessa rättigheter. Bestämmelserna om tystnadsplikt och utlämnande av uppgifter i kameraövervakningslagen och i offentlighets- och sekretesslagen är förenliga med direktivet. Rättigheterna enligt direktivet är fler än vad som följer av lagen. En svensk lagstiftning som omfattar kamera-

övervakning måste innehålla bestämmelser om rättigheter för registrerade eller om undantag från rättigheterna som uppfyller direktivets krav.

7.2.6 Skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden

Bedömning: Kameraövervakningslagens skyldigheter avseende säkerhet vid kameraövervakning enligt 30 och 31 §§ överensstämmer med direktivets motsvarande skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden enligt artiklarna 19–34. Skyldigheterna enligt direktivet är fler än vad som följer av lagen. De innefattar inte något generellt krav på tillstånd eller anmälan men innebär bl.a. att en konsekvensbedömning ska göras och ett samråd med tillsynsmyndigheten ska ske i vissa fall. Ett tillståndskrav får dock ställas upp i svensk rätt med stöd av artikel 1.3.

En svensk lagstiftning som omfattar kameraövervakning måste innehålla bestämmelser om skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden som uppfyller direktivets krav. Lagstiftningen kan vidare innehålla t.ex. ett krav på tillstånd.

Skälen för bedömningen

Allmänt om skyldigheterna

Kapitel IV i direktivet, artiklarna 19–34, innehåller långtgående skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden. Begreppen personuppgiftsansvarig och personuppgiftsbiträde definieras i artikel 4. I kapitlet finns bestämmelser om allmänna skyldigheter, t.ex. om inbyggt dataskydd och dataskydd som standard, behandling av personuppgifter på en personuppgiftsansvarigs vägnar, förande av register, loggning, samarbete med tillsynsmyndigheten samt konsekvensbedömning och samråd med tillsynsmyndigheten. Slutligen innehåller kapitlet bestämmelser om säkerhet för personuppgifter och om dataskyddsombud.

Av intresse i detta sammanhang är främst de artiklar som behandlas i de följande avsnitten.

Skyldigheter avseende säkerhet vid personuppgiftsbehandling

Artiklarna 19–23 och 29 innehåller relativt detaljerade bestämmelser om säkerhet vid behandling av personuppgifter och om vad som gäller när behandling av personuppgifter ska genomföras på en personuppgiftsansvarigs vägnar. Bestämmelserna överensstämmer i huvudsak med motsvarande artiklar i förordningen, som behandlats i avsnitt 7.1.11.

Även i kameraövervakningslagen finns skyldigheter avseende säkerhet vid behandling av personuppgifter i 30 och 31 §§. Där föreskrivs bl.a. att den som bedriver kameraövervakning ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda bild- och ljudmaterial från övervakningen. Vidare anges vad som gäller om någon bedriver kameraövervakning för någon annans räkning.

Som framgått av avsnitt 7.1.11 har kameraövervakningslagens skyldigheter avseende säkerhet vid kameraövervakning bedömts överensstämma med förordningens motsvarande skyldigheter. Samma bedömning görs vad gäller hur lagen förhåller sig till direktivets skyldigheter. Skyldigheterna enligt direktivet är dock, liksom skyldigheterna enligt förordningen, fler än vad som följer av lagen. En svensk lagstiftning som omfattar kameraövervakning måste innehålla bestämmelser om skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden som uppfyller direktivets krav.

Skyldigheter att göra en konsekvensbedömning och samråda

I artiklarna 27 och 28 finns bestämmelser om skyldighet att göra en konsekvensbedömning och skyldighet att samråda med tillsynsmyndigheten.

Av artikel 27 följer att om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter, ska medlemsstaterna säkerställa att den personuppgiftsansvarige, eller personuppgiftsbiträdet, före behandlingen utför en bedömning av dess konsekvenser för skyddet av personuppgifter.

Enligt artikel 28 ska medlemsstaterna föreskriva att den personuppgiftsansvarige i vissa fall ska samråda med tillsynsmyndigheten före en behandling av personuppgifter som kommer att ingå i ett

nytt register som ska inrättas. Det gäller när en konsekvensbedömning visar att behandlingen skulle leda till en hög risk – om inte den registeransvarige vidtar åtgärder för att minska risken – eller när typen av behandling, särskilt vid användning av ny teknik eller nya rutiner eller förfaranden medför en hög risk för de registrerades rättigheter och friheter.

Enligt artikel 28 ska medlemsstaterna vidare föreskriva att om tillsynsmyndigheten anser att den planerade behandlingen inte skulle vara förenlig med de bestämmelser som antas i enlighet med direktivet, ska tillsynsmyndigheten inom visst tid ge den personuppgiftsansvarige skriftliga råd. Vidare får tillsynsmyndigheten utnyttja alla de befogenheter som den har enligt artikel 47, bl.a. förbjuda behandlingen.

Av artikel 1.3 följer att direktivet inte hindrar medlemsstaterna från att föreskriva starkare skyddsåtgärder än de som fastställs i direktivet för skyddet av den registrerades rättigheter och friheter med avseende på behöriga myndigheters behandling av personuppgifter.

I kameraövervakningslagen finns inte några motsvarigheter till skyldigheterna enligt direktivet att i vissa fall göra en konsekvensbedömning och, beroende på utfallet av bedömningen, samråda med tillsynsmyndigheten. Skyldigheten att samråda med tillsynsmyndigheten enligt direktivet gäller endast om personuppgifterna ska ingå i ett nytt register. Merparten av sådant material som spelas in vid kameraövervakning kommer inte ingå i ett register i direktivets mening (jfr artikel 3.6 och avsnitt 7.1.3). Någon skyldighet att samråda enligt artikel 28 inför bedrivandet av kameraövervakning gäller därmed normalt inte. Det ska dock noteras att Utredningen om 2016 års dataskyddsdirektiv har föreslagit en samlad reglering om skyldighet att göra konsekvensbedömning och samråda som inte knyter an endast till registerfallen. Direktivets skyldigheter innefattar inte något generellt krav på tillstånd eller krav på anmälan av det slag som finns i kameraövervakningslagen. Ett tillståndskrav får dock ställas upp i svensk rätt med stöd av artikel 1.3. En svensk lagstiftning som omfattar kameraövervakning måste innehålla bestämmelser om skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden som uppfyller direktivets krav. Lagstiftningen kan vidare innehålla t.ex. ett krav på tillstånd.

7.2.7 Överföring till tredjeland eller internationella organisationer

Bedömning: Kameraövervakningslagens bestämmelser i 34–36 §§ om överföring av bild- och ljudmaterial till tredjeland överensstämmer delvis med direktivets bestämmelser om överföring av personuppgifter till tredjeländer eller internationella organisationer enligt artiklarna 35–40.

En svensk lagstiftning som omfattar kameraövervakning måste innehålla bestämmelser om överföring som uppfyller direktivets krav.

Skälen för bedömningen: I kapitel V i direktivet, artiklarna 35–40, finns bestämmelser om överföring av personuppgifter till tredjeländer eller internationella organisationer. Bestämmelserna motsvarar i stort bestämmelserna om sådan överföring i förordningen, se avsnitt 7.1.13.

I 34–36 §§ kameraövervakningslagen finns vissa bestämmelser om överföring till tredjeland av bild- och ljudmaterial från kameraövervakning som innehåller personuppgifter. Även vissa bestämmelser i personuppgiftsförordningen (1998:1191) är av intresse. Dessa bestämmelser har redovisats i avsnitt 7.1.13. Där har bedömningen gjorts att bestämmelserna delvis överensstämmer med förordningens bestämmelser om överföring. Samma bedömning görs vad gäller hur lagens bestämmelser förhåller sig till direktivets bestämmelser. En svensk lagstiftning som omfattar kameraövervakning måste innehålla bestämmelser om överföring som uppfyller direktivets krav.

7.2.8 Tillsyn

Bedömning: Kameraövervakningslagens bestämmelser i 38–43 §§ om tillsyn överensstämmer delvis med direktivets bestämmelser om tillsyn och samarbete mellan tillsynsmyndigheter enligt artiklarna 41–51. Direktivets bestämmelser är mer omfattande än lagens.

En svensk lagstiftning som omfattar kameraövervakning måste innehålla bestämmelser om tillsyn som uppfyller direktivets krav.

Skälen för bedömningen: I kapitel VI i direktivet, artiklarna 41–49, finns bestämmelser om tillsyn. Av artiklarna 41 och 42 följer att medlemsstaterna ska utse en eller flera självständiga tillsynsmyndigheter som ska ansvara för att övervaka tillämpningen av direktivet. Medlemsstaterna får föreskriva att en tillsynsmyndighet som har inrättats enligt förordningen ska vara tillsynsmyndighet även enligt direktivet. I artiklarna 43 och 44 finns bestämmelser om inrättandet av tillsynsmyndigheten och om dess ledamöter. I artiklarna 45–49 regleras myndighetens behörighet, uppgifter och befogenheter, såväl undersökningsbefogenheter som korrigerande befogenheter. Bestämmelserna motsvarar i stort bestämmelserna om tillsyn i förordningen, se avsnitt 7.1.14.

Vidare finns i kapitel VII i direktivet, artiklarna 50 och 51, bestämmelser som förpliktar en nationell tillsynsmyndighet att samarbeta med och assistera tillsynsmyndigheterna i andra medlemsstater.

Dessutom ska nämnas att artikel 1.3 i direktivet tillåter en medlemsstat att föreskriva starkare skyddsåtgärder än de som fastställs i direktivet.

Även i kameraövervakningslagen finns i 38–43 §§ vissa bestämmelser om tillsyn. Till dessa anknyter bestämmelser i kameraövervakningsförordningen (2013:463). Innehållet i dessa bestämmelser har beskrivits i avsnitt 7.1.14. Där har bedömningen gjorts att bestämmelserna endast delvis överensstämmer med förordningens bestämmelser om tillsyn och samarbete mellan tillsynsmyndigheter. Samma bedömning görs vad gäller hur bestämmelserna i lagen och dess förordning förhåller sig till direktivets bestämmelser. Direktivets bestämmelser är dessutom mer omfattande än lagens. En svensk lagstiftning som omfattar kameraövervakning måste innehålla bestämmelser om tillsyn som uppfyller direktivets krav.

7.2.9 Rättsmedel, ansvar och sanktioner m.m.

Bedömning: Kameraövervakningslagens bestämmelser i 44–48 §§ om överklagande, skadestånd och straffansvar överensstämmer delvis med direktivets bestämmelser om rättsmedel, ansvar och sanktioner enligt artiklarna 52–57. Direktivets bestämmelser är mer omfattande än lagens.

En svensk lagstiftning som omfattar kameraövervakning måste innehålla bestämmelser om rättsmedel, ansvar och sanktioner som uppfyller direktivets krav.

Skälen för bedömningen: I kapitel VIII i direktivet, artiklarna 52–57, finns bestämmelser om rättsmedel, ansvar och sanktioner. Bestämmelserna motsvarar i stort bestämmelserna om rättsmedel, ansvar och sanktioner i förordningen, se avsnitt 7.1.12.

En registrerad ska ha rätt att framföra klagomål hos tillsynsmyndigheten. Vidare ska fysiska och juridiska personer ha rätt till ett effektivt rättsmedel både mot tillsynsmyndighetens beslut och direkt mot en personuppgiftsansvarig eller ett personuppgiftsbiträde. Dessutom ska den som har lidit materiell eller immateriell skada till följd av en överträdelse av direktivet ha rätt till ersättning av den personuppgiftsansvarige, eller personuppgiftsbiträdet, under vissa förutsättningar. Medlemsstaterna ska föreskriva effektiva, proportionella och avskräckande sanktioner för överträdelser av direktivet.

I 44–48 §§ kameraövervakningslagen finns vissa bestämmelser om överklagande, skadestånd och straffansvar. Innehållet i dessa har beskrivits i avsnitt 7.1.12. Där har bedömningen gjorts att bestämmelserna endast delvis överensstämmer med förordningens bestämmelser om rättsmedel, ansvar och sanktioner. Samma bedömning görs vad gäller hur lagens bestämmelser förhåller sig till bestämmelserna i direktivet. Direktivets bestämmelser är dessutom mer omfattande än lagens. En svensk lagstiftning som omfattar kameraövervakning måste innehålla bestämmelser om rättsmedel, ansvar och sanktioner som uppfyller direktivets krav.

7.2.10 Sammanfattande slutsats

Bedömning: Direktivet, som ska genomföras i svensk rätt, innehåller krav som endast delvis uppfylls av kameraövervakningslagens bestämmelser. En svensk lagstiftning som omfattar kameraövervakning måste fullt ut uppfylla de krav som följer av direktivet.

Skälen för bedömningen: Av avsnitten ovan har framgått att kameraövervakning kan utgöra behandling av personuppgifter som omfattas av tillämpningsområdet för direktivet. Vidare har framgått att direktivet ska genomföras i svensk rätt och att svenska bestämmelser som omfattar sådan kameraövervakning som faller in under direktivets tillämpningsområde måste uppfylla direktivets krav. Som också framgått innehåller direktivet krav som endast delvis uppfylls av kameraövervakningslagens bestämmelser. En svensk lagstiftning som omfattar kameraövervakning måste fullt ut uppfylla de krav som följer av direktivet.

7.3 Kameraövervakning som inte omfattas av EU-regleringen

Bedömning: Sådan kameraövervakning som inte omfattas av förordningens och direktivets tillämpningsområden kan i och för sig regleras i svensk rätt utan beaktande av EU-regleringen.

Skälen för bedömningen: Som redan har framgått ovan finns det personuppgiftsbehandling som faller utanför den nya EU-regleringen. Det gäller behandling som helt faller utanför unionsrätten och behandling som medlemsstaterna utför när de bedriver verksamhet som omfattas av EU:s gemensamma utrikes- och säkerhetspolitik, se avsnitt 7.1.4 och 7.2.3.

Detta innebär att kameraövervakning som sker främst i det svenska försvarets verksamhet och Säkerhetspolisens verksamhet normalt inte omfattas av förordningens och direktivets tillämpningsområden. Sådan kameraövervakning kan i och för sig regleras i svensk rätt utan beaktande av EU-regleringen.

8 Vad gäller utan särskilda bestämmelser om kameraanvändning?

8.1 Inledning

För förståelsen av övervägandena i de kommande avsnitten redovisas nedan översiktligt vad den nya dataskyddsförordningen och det nya dataskyddsdirektivet samt den nya lagstiftning som de i avsnitt 2 nämnda utredningarna Dataskyddsutredningen och Utredningen om 2016 års dataskyddsdirektiv föreslagit innebär för kameraanvändning, om särskilda svenska bestämmelser för sådan användning inte ska gälla framöver.

Förordningen kommer att gälla direkt i Sverige och ska börja tillämpas från och med den 25 maj 2018. Dataskyddsutredningen har föreslagit en ny generell lag som ska komplettera förordningen, lagen med kompletterande bestämmelser till EU:s dataskyddsförordning, nedan kallad dataskyddslagen. Dessutom har föreskrifter till lagen föreslagits. Lagen ska träda i kraft samma dag som förordningen ska börja tillämpas. Bestämmelserna i förordningen och dataskyddslagen och dess föreskrifter ska – i den mån särskilda bestämmelser för kameraanvändning inte införs – tillämpas på sådan kameraanvändning som utgör personuppgiftsbehandling och som i övrigt faller in under den regleringens tillämpningsområde.

Utredningen om 2016 års dataskyddsdirektiv har föreslagit att direktivet i huvudsak genomförs genom en ny generell lag, benämnd brottsdatalagen. Lagen ska träda i kraft den 1 maj 2018. Dessutom har föreskrifter till lagen föreslagits. Bestämmelserna i brottsdatalagen och dess föreskrifter ska – i den mån särskilda bestämmelser för kameraanvändning inte införs – tillämpas på sådan kamera-

användning som utgör personuppgiftsbehandling och som i övrigt faller in under den regleringens tillämpningsområde.

Därutöver kommer bestämmelser i s.k. registerförfattningar att gälla i den mån de kan tillämpas på kameraanvändning. Sådana författningar är nu föremål för översyn med anledning av den nya dataskyddsregleringen.

8.2 Kameraanvändning som omfattas av förordningen och dataskyddslagen

Förordningens och dataskyddslagens tillämpningsområde

Förordningen gäller för behandling av personuppgifter som helt eller delvis företas på automatiserad väg samt för annan behandling än automatiserad av personuppgifter som ingår i eller kommer att ingå i ett register. Med personuppgifter avses varje upplysning som avser en identifierad eller identifierbar fysisk person, en s.k. registrerad. Med identifierbar avses att en person direkt eller indirekt kan identifieras genom t.ex. namn eller en eller flera faktorer som är specifika för den personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet. Med behandling avses en åtgärd eller kombination av åtgärder beträffande personuppgifter – oberoende av om de utförs automatiserat eller inte – såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Förordningen omfattar personuppgiftsbehandling, däribland kameraanvändning, som utförs av både offentligrättsliga och privaträttsliga subjekt med några undantag, t.ex. för behandling i Polismyndighetens brottsbekämpande verksamhet, som i stället omfattas av direktivet och brottsdatalagen, se nedan. Enligt dataskyddslagen ska dessutom, om inte annat föreskrivs, förordningen och lagen gälla vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten, t.ex. i verksamhet som rör nationell säkerhet, och i verksamhet som omfattas av EU:s gemensamma utrikes- och säkerhetspolitik.

Förordningen kan alltså omfatta t.ex. användning av handhållna kameror eller kameror på drönare och i bilar men även användning av kameror som är monterade på fasta geografiska platser såsom byggnader o. dyl. Den gäller när kameraanvändningen sker av myndigheter, bolag, föreningar och andra juridiska personer samt fysiska personer. Den omfattar dock inte en fysisk persons kameraanvändning när användningen sker som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll.

I dataskyddslagen finns en upplysningsbestämmelse som tydliggör att bestämmelserna i förordningen och lagen inte ska tillämpas i den utsträckning det skulle strida mot svenska grundlagsbestämmelser om tryck- och yttrandefrihet. Utanför det grundlagsskyddade området ska vidare gälla ett undantag från förordningen för sådan behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande. Vissa av förordningens bestämmelser, bl.a. de som rör säkerhet för personuppgifter, ska dock tillämpas i dessa fall. Förordningen hindrar inte att tryckfrihetsförordningens reglering om allmänhetens tillgång till handlingar kan fortsätta att tillämpas även när det gäller allmänna handlingar som innehåller personuppgifter.

Rättslig grund och principer för behandling av personuppgifter

För att kameraanvändning som utgör personuppgiftsbehandling som träffas av förordningen ska få ske måste den vara laglig enligt någon av de grunder som räknas upp i förordningen. Enligt uppräkningen är kameraanvändning laglig, t.ex.

– om den som ska bli föremål för fotografering eller filmning har lämnat sitt samtycke,
– om kameraanvändningen är nödvändig för att fullgöra ett avtal,
– om kameraanvändningen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den som vill använda kameran,
– om kameraanvändningen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den ansvariges myndighetsutövning, eller

– om kameraanvändningen är nödvändig för ändamål som rör den ansvariges eller en tredje parts berättigade intressen, om inte den fotograferade eller filmade personens intressen eller grundläggande rättigheter och friheter väger tyngre.

Det torde ofta vara den sistnämnda grunden som blir aktuell för privaträttsliga subjekts kameraanvändning. Huruvida kameraanvändning i ett visst enskilt fall är laglig eller inte beror alltså på vilket intresset av att använda kameran är, om detta kan anses vara berättigat och i så fall väger över det motstående intresset av integritetsskydd samt om det är nödvändigt med kameraanvändning.

Enligt förordningen måste en rättslig förpliktelse, myndighetsutövning eller uppgift av allmänt intresse vara fastställd i enlighet med nationell rätt eller unionsrätten för att kunna utgöra rättslig grund för behandling av personuppgifter. I dataskyddslagen förtydligas detta. En rättslig förpliktelse är enligt svensk rätt fastställd, om den gäller enligt lag eller annan författning eller följer av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Myndighetsutövning fastställs i svensk rätt genom lag eller annan författning. Uppgifter av allmänt intresse är fastställda i enlighet med svensk rätt, om de följer av lag eller annan författning eller av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

Vidare innehåller förordningen vissa principer. Personuppgifter ska samlas in för särskilda och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Uppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för dem. Uppgifterna ska behandlas på ett lagligt och korrekt sätt och vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Dessutom gäller bl.a. att personuppgifter inte får förvaras i en form som möjliggör identifiering av den registrerade under längre tid än vad som är nödvändigt för ändamålen med behandlingen.

Enskildas rättigheter och personuppgiftsansvarigas skyldigheter

Förordningen innehåller ett antal rättigheter för dem som blir föremål för personuppgiftsbehandling, inklusive kameraanvändning. Det gäller exempelvis en rätt att få information om behandlingen, rätt att få tillgång till material och rätt att få material raderat.

Det finns också bestämmelser om skyldigheter för personuppgiftsansvariga, även för dem som vill använda kameror, t.ex. vad gäller säkerhet vid användningen och för materialet samt överföring av material till tredjeland eller till internationella organisationer. Det finns vidare en skyldighet att i vissa fall göra en konsekvensbedömning och eventuellt samråda med tillsynsmyndigheten. Om en typ av kameraanvändning – särskilt med ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål – sannolikt leder till en hög risk för fysiska personers rättigheter och friheter, ska den ansvarige före användningen utföra en bedömning av konsekvenserna för skyddet av personuppgifter. En konsekvensbedömning ska göras bl.a. när det är fråga om systematisk övervakning av en allmän plats i stor skala. Tillsynsmyndigheten ska upprätta en förteckning över i vilka fall konsekvensbedömning ska göras.

När en konsekvensbedömning visar att kameraanvändningen skulle leda till en hög risk för fysiska personers rättigheter och friheter, om inte åtgärder vidtas för att minska risken, ska den ansvarige samråda med tillsynsmyndigheten före användningen. Om tillsynsmyndigheten anser att kameraanvändningen skulle strida mot förordningen, ska myndigheten ge den ansvarige skriftliga råd. Vidare får myndigheten använda sig av befogenheter som den har enligt förordningen. Exempelvis kan tillsynsmyndigheten utfärda varning eller tillfälligt eller definitivt begränsa, inklusive förbjuda, användningen.

Rättsmedel, skadestånd, tillsyn och sanktioner

I förordningen och dataskyddslagen finns dessutom bestämmelser om rättsmedel, skadestånd, tillsyn och sanktioner.

Beslut som en myndighet fattar med anledning av att den enskilde utövar sina rättigheter enligt förordningen ska kunna överklagas till allmän förvaltningsdomstol. Det kan t.ex. röra sig om

avslagsbeslut på en begäran om att få tillgång till sina personuppgifter, att uppgifter ska rättas eller raderas eller att en behandling ska begränsas eller upphöra.

Den som har lidit en materiell eller immateriell skada till följd av en överträdelse av förordningen ska, under vissa förutsättningar, ha rätt till ersättning av den som ansvarar för kameraanvändningen eller av den som biträder den ansvarige. I dataskyddslagen förtydligas att denna rätt även gäller vid överträdelser av den lagen och andra författningar som kompletterar förordningen.

Tillsynsmyndighetens tillsynsbefogenheter anges i förordningen. Dessa ska enligt dataskyddslagen gälla även vid tillsynen över att den lagen och annan kompletterande lagstiftning till förordningen följs.

Vid överträdelser av förordningens bestämmelser ska tillsynsmyndigheten kunna besluta om sanktionsavgifter. Detsamma gäller vid underlåtenhet att rätta sig efter tillsynsmyndighetens instruktioner, förelägganden eller beslut. Av förordningen följer direkt att sanktionsavgifter kan påföras privaträttsliga subjekt. Enligt dataskyddslagen ska sanktionsavgifter även kunna åläggas statliga och kommunala myndigheter.

För något mindre allvarliga överträdelser av förordningen, såsom överträdelse av kravet på konsekvensbedömning, är maxbeloppet tio miljoner euro eller två procent av den globala årsomsättningen när det gäller företag beroende på vilket belopp som är högst. För allvarligare överträdelser, t.ex. överträdelser av de grundläggande principerna för behandling, rätten till information eller rätten till rättelse eller radering och vid underlåtenhet att rätta sig efter tillsynsmyndighetens instruktioner, förelägganden eller beslut, är maxbeloppet 20 miljoner euro eller fyra procent av den globala årsomsättningen. Enligt dataskyddslagen ska sanktionsavgifter för myndigheter dock vara begränsade till högst tio miljoner kronor eller högst 20 miljoner kronor beroende på vilken typ av överträdelse det är fråga om.

Tillsynsmyndighetens beslut enligt förordningen och dataskyddslagen ska få överklagas till allmän förvaltningsdomstol.

8.3 Kameraanvändning som omfattas av direktivet och brottsdatalagen

Brottsdatalagens tillämpningsområde

Brottsdatalagen ska tillämpas av myndigheter som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder vid deras behandling av personuppgifter. Lagen ska också gälla för personuppgiftsbehandling vid upprätthållande av allmän ordning och säkerhet. De som har sådana arbetsuppgifter betecknas behöriga myndigheter. Lagen ska även tillämpas av andra aktörer som har fått i uppgift att utöva myndighet för något av de nämnda syftena.

I övrigt kommer förordningen att vara tillämplig, t.ex. när Polismyndigheten behandlar personuppgifter i tillståndsärenden eller när en allmän domstol handlägger tvistemål. Det som blir avgörande för om brottsdatalagen är tillämplig är dels om det är en behörig myndighet som behandlar personuppgifterna, dels syftet med behandlingen.

Lagen ska i huvudsak gälla för sådan behandling av personuppgifter som är helt eller delvis automatiserad.

Lagen ska inte tillämpas på Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet. Undantag ska också gälla för Polismyndigheten när myndigheten har övertagit en uppgift som rör nationell säkerhet från Säkerhetspolisen.

Rättslig grund och principer för behandling av personuppgifter

Det ska alltid finnas en rättslig grund för att personuppgifter ska få behandlas med stöd av brottsdatalagen. Den huvudsakliga grunden är att behandlingen av personuppgifterna ska vara nödvändig för att en behörig myndighet ska kunna utföra en sådan arbetsuppgift som gör lagen tillämplig. Arbetsuppgiften ska framgå av en bindande unionsrättsakt, en lag, en förordning eller ett särskilt beslut av regeringen.

Vidare ska vissa principer gälla för behandlingen. Personuppgifter får bara behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Uppgifterna ska behandlas författningsenligt och på ett korrekt sätt. De personuppgifter som behandlas ska vara korrekta

och, om det är nödvändigt, uppdaterade. De ska också vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler uppgifter än nödvändigt får inte behandlas och uppgifter får inte behandlas längre än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Enskildas rättigheter och personuppgiftsansvarigas skyldigheter

När det gäller enskildas rättigheter kommer till stora delar samma reglering som i dag att gälla men rätten till information blir tydligare i vissa avseenden. Utgångspunkten är att den som vill kontrollera om hans eller hennes personuppgifter behandlas får vända sig till den personuppgiftsansvarige, som utan onödigt dröjsmål ska lämna skriftligt besked om uppgifterna behandlas. Om så är fallet har den registrerade rätt att få del av uppgifterna och få viss information om behandlingen. Informationsskyldigheten gäller dock inte, om uppgifterna inte får lämnas ut på grund av att vissa i lagen angivna intressen kan skadas.

Den personuppgiftsansvarige ska på begäran av den registrerade utan onödigt dröjsmål rätta eller komplettera personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen. En motsvarande skyldighet gäller bl.a. i fråga om radering av personuppgifter som behandlas på ett otillåtet sätt. I vissa fall ska behandlingen av personuppgifterna i stället begränsas.

De skyldigheter som personuppgiftsansvariga har i dag kommer till stor del att gälla även i fortsättningen. Vissa regler blir dock mer preciserade och det tillkommer också vissa nya skyldigheter. Kraven på säkerhets- och skyddsåtgärder blir mer preciserade liksom kravet på att det ska finnas en behandlingshistorik. Det ställs exempelvis krav på inbyggt dataskydd och dataskydd som standard. Det införs också en generell bestämmelse om att tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Det införs t.ex. ett generellt krav på att personuppgiftsansvariga som planerar en ny typ av behandling eller betydande förändringar i pågående behandling ska göra en bedömning av konsekvenserna för registrerades personliga integritet och, beroende på framför allt

risken för intrång, samråda med tillsynsmyndigheten innan behandlingen påbörjas eller förändras.

Rättsmedel, skadestånd, tillsyn och sanktioner

Tillsynsmyndighetens huvuduppgifter och befogenheter regleras i brottsdatalagen.

Tillsynsmyndigheten ska kunna besluta om att ta ut sanktionsavgift av personuppgiftsansvariga och i vissa fall av personuppgiftsbiträden. Sanktionsavgift får tas ut av personuppgiftsansvariga vid överträdelse av de grundläggande bestämmelserna om skydd för enskildas integritet. Det gäller bl.a. om personuppgifter behandlas utan rättslig grund eller utan ett särskilt angivet och berättigat ändamål, om personuppgifterna inte uppfyller kraven på att vara korrekta, aktuella, adekvata och relevanta eller om fler uppgifter än nödvändigt behandlas eller om de behandlas längre än vad som är nödvändigt med hänsyn till ändamålen. Det gäller också t.ex. om den personuppgiftsansvarige inte vidtar tillräckliga säkerhets- och skyddsåtgärder. Sanktionsavgift får även tas ut om den personuppgiftsansvarige inte bistår tillsynsmyndigheten vid tillsyn eller inte rättar sig efter tillsynsmyndighetens förelägganden eller beslut.

Sanktionsavgiften ska bestämmas till lägst 25 000 kronor och högst tio miljoner kronor för mindre allvarliga överträdelser och det dubbla vid andra överträdelser.

Den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning som behandling av personuppgifter i strid med brottsdatalagen med tillhörande förordning har orsakat.

Vissa beslut som en myndighet har fattat i egenskap av personuppgiftsansvarig ska kunna överklagas. Det gäller bl.a. beslut i fråga om rättelse, komplettering, radering eller begränsning av behandlingen och beslut att inte lämna ut information på begäran av en registrerad. Tillsynsmyndighetens beslut enligt lagen får också överklagas.

9 En ny kamerabevakningslag

9.1 En ny lag

Förslag: Kameraövervakningslagen (2013:460) ska ersättas av en ny lag. Den nya lagen ska heta kamerabevakningslagen.

Skälen för förslaget

En stor reform

Av avsnitt 7 har framgått att det inom EU har antagits en ny dataskyddsförordning och ett nytt dataskyddsdirektiv om behandling av personuppgifter och att dessa instrument får stor betydelse för svensk lagstiftning om kameraövervakning, eftersom kameraövervakning ofta utgör personuppgiftsbehandling som omfattas av den nya EU-regleringen. Förordningen gäller för ett stort antal myndigheter och andra rättssubjekt medan direktivet endast gäller för särskilda myndigheter och andra aktörer när de utför vissa uppgifter. För några verksamheter gäller varken förordningen eller direktivet.

Som vidare framgått kommer förordningen att gälla direkt i Sverige, vilket innebär att bestämmelser om kameraövervakning som upprepar eller avviker från innehållet i förordningen inte kan behållas i svensk lagstiftning som kompletterar förordningen annat än om förordningen lämnar utrymme för det. Enligt den analys som gjorts i avsnitt 7 kan många av kameraövervakningslagens bestämmelser inte behållas alls eller inte behållas i sin nuvarande form när det gäller sådan kameraövervakning som omfattas av förordningens tillämpningsområde.

Vad gäller direktivet har framgått att detta ska genomföras i svensk rätt och att svenska bestämmelser som omfattar kameraövervak-

ning som faller in under direktivets tillämpningsområde måste uppfylla direktivets krav. Direktivets krav uppfylls dock endast delvis av kameraövervakningslagens bestämmelser. En svensk lagstiftning som omfattar kameraövervakning måste fullt ut uppfylla de krav som följer av direktivet.

Slutligen har framgått att kameraövervakning som inte omfattas av förordningens och direktivets tillämpningsområden i och för sig kan regleras i svensk rätt utan beaktande av EU-regleringen. Som utvecklas nedan bör dock bestämmelser om sådan kameraövervakning inte avvika från övrig lagstiftning om kameraövervakning.

Utöver den påverkan på svensk kameraövervakningslagstiftning som EU-regleringen innebär har den kartläggning och utvärdering av kameraövervakningslagen som gjorts och som redovisats i avsnitt 5 visat att det finns vissa tillämpningsproblem med lagen.

Detta innebär att det krävs en stor reform av den svenska lagstiftningen på området för kameraövervakning. Reformen blir så omfattande att det inte är lämpligt att genomföra den genom att behålla kameraövervakningslagen och göra ändringar i den lagen. Att behålla kameraövervakningslagen skulle inte heller på samma sätt som en ny lagstiftning tydliggöra att bestämmelserna i stora delar har sin bakgrund i den nya EU-regleringen. Kameraövervakningslagen bör därför inte behållas.

En ny lag

Kameraövervakningslagen bör alltså inte behållas. Ett alternativ är att inte införa någon ny särskild lag eller några nya särskilda bestämmelser på kameraövervakningsområdet överhuvudtaget. I stället skulle, som översiktligt beskrivits i avsnitt 8, kameraövervakning uteslutande kunna regleras av bestämmelserna i förordningen och den av Dataskyddsutredningen föreslagna kompletterande lagen till förordningen, dataskyddslagen, med förordning respektive av den av Utredningen om 2016 års dataskyddsdirektiv föreslagna brottsdatalagen med tillhörande förordning som genomför direktivet. Dessa nya svenska lagar innehåller generella bestämmelser om behandling av personuppgifter och ska gälla i den utsträckning det saknas särskild lagstiftning om sådan behandling på ett visst område. Lagarna skulle kunna gälla som enda reglering för kameraövervakning som

utgör personuppgiftsbehandling. Därutöver finns det s.k. registerförfattningar som specifikt reglerar personuppgiftsbehandling inom olika sektorer och som kommer att anpassas till den nya EU-regleringen.

Det andra alternativet är att införa nya särskilda bestämmelser om kameraövervakning. Redan vid en övergripande analys kan det konstateras att det behövs åtminstone vissa sådana bestämmelser vad gäller både kameraövervakning på förordningens och direktivets tillämpningsområden och kameraövervakning på det område som faller utanför EU-regleringen. Exempelvis kräver de speciella förhållanden som råder vid kameraövervakning en särskild reglering om hur det ska upplysas om kameraövervakning som skiljer sig från den informationsskyldighet som annars ska gälla vid personuppgiftsbehandling enligt EU-regleringen. I denna utrednings uppdrag har inte heller ingått att avskaffa eller genomgripande förändra en särskild svensk lagstiftning på kameraövervakningsområdet eller att frångå de principer på vilka lagstiftningen vilar. Av dessa skäl bör det införas särskilda bestämmelser om kameraövervakning.

Dessa bestämmelser bör samlas i en ny för all kameraövervakning gemensam lag och inte tas in i två eller tre nya lagar där t.ex. en avser kameraövervakning på förordningens område och den andra eller de två andra avser övervakning på direktivets område respektive på det område som faller utanför EU-regleringen. Inte heller bör bestämmelserna tas in i dataskyddslagen eller brottsdatalagen eller i olika registerförfattningar. Att i stället samla de särskilda bestämmelserna om kameraövervakning i en enda ny lag innebär att lagstiftningen på området kan bli något enklare att tillämpa, även om många av förordningens bestämmelser kommer att gälla direkt och lagen kan komma att hänvisa till de nya generella lagarna. Det förhållandet att bestämmelserna delvis kommer att grunda sig på skilda typer av EU-rättsliga instrument och delvis kommer att avse även kameraövervakning som inte direkt omfattas av EU-regleringen kan inte anses hindra att de tas in i en gemensam lag.

Följaktligen föreslås att kameraövervakningslagen ska ersättas av en ny lag.

Lagen ska heta kamerabevakningslagen

En ny lag som ska ersätta kameraövervakningslagen bör av flera skäl ges ett annat namn än den lag som den ersätter.

Ett skäl är att det tydliggörs att det är fråga om en helt ny lag. Det gäller särskilt som bakgrunden till lagen är en annan än tidigare, nämligen att den i delar kompletterar den nya förordningen eller med stöd i förordningen avviker från denna samt genomför det nya direktivet.

Ett annat skäl är att det språkligt kan diskuteras om ordet övervakning är helt rättvisande för att beskriva den användning av kameror som ska omfattas av den nya lagen enligt vad som föreslås nedan. Sådan kameraanvändning ska endast få ske för berättigade ändamål. Dessa kan vara av olika slag, varav flera syftar till att generellt skydda människors liv och hälsa mot exempelvis brott och olyckor. Kameraanvändning kan vidare många gånger skapa trygghet för det stora flertalet av de människor som kommer att träffas av användningen. Ordet övervakning kan dessutom föra tankarna till en kontroll där enskildas intresse av att inte bli föremål för fotografering eller filmning inte har beaktats i tillräcklig utsträckning. Ordet bevakning beskriver bättre den kameraanvändning som ska omfattas av lagen. Att det ordet används även i annan lagstiftning med en något annan innebörd hindrar inte att det används i den nya lagen och medför inte heller någon svårighet att förstå ordets innebörd enligt denna lag.

Mot denna bakgrund föreslås att den nya lagen ska heta kamerabevakningslagen.

9.2 Utgångspunkter för den nya lagen

9.2.1 Allmänna utgångspunkter

Bedömning: Kamerabevakningslagens bestämmelser ska vara förenliga med bestämmelserna i förordningen och direktivet och bör även i delar där de i och för sig kan utformas annorlunda anpassas till EU-regleringen. Lagen bör endast innehålla de bestämmelser som särskilt behövs för kamerabevakning till skillnad mot annan personuppgiftsbehandling. Bestämmelserna bör, så

långt det är förenligt med EU-regleringen och ändamålsenligt, vara desamma för all kamerabevakning.

Skälen för bedömningen

Lagen ska vara förenlig med och bör även i övrigt anpassas till förordningen och direktivet

En självklarhet är att bestämmelserna i den nya kamerabevakningslagen ska vara förenliga med bestämmelserna i förordningen och direktivet.

Att kamerabevakning ofta innebär behandling av personuppgifter som omfattas av förordningen eller träffas av direktivet talar vidare för utgångspunkten att lagens bestämmelser även i delar där de i och för sig kan utformas annorlunda anpassas till EU-regleringen, dvs. – i den utsträckning det är möjligt – anpassas till vad som annars gäller för behandling av personuppgifter enligt den regleringen. För det talar också att lagen ska betraktas som en dataskyddsreglering och inte någon annan typ av reglering. Redan dagens kameraövervakningslag innehåller ett flertal bestämmelser som utgör renodlade regler om personuppgiftsbehandling. När nu EU:s medlemsstater har enats om ett nytt vidsträckt och detaljerat gemensamt regelverk på dataskyddsområdet finns det anledning att ytterligare närma sig detta på kamerabevakningsområdet. I diskussionen om kamerabevakning har det vidare skett en viss förskjutning från att kameror används till hur material från sådan bevakning behandlas, vilket mer liknar hur diskussionen om personuppgiftsbehandling i allmänhet förs.

Lagen bör endast innehålla de bestämmelser som särskilt behövs för kamerabevakning

Den utgångspunkt som slagits fast ovan innebär inte att kamerabevakningslagen uttömmande eller utförligt måste eller bör reglera allt som ska gälla för sådan kameraanvändning som ska omfattas av lagen. Tvärtom innebär en anpassning till övrig reglering om behandling av personuppgifter att många av bestämmelserna i den regleringen kan gälla även för kamerabevakning förutsatt att de är lämpliga också för denna form av personuppgiftsbehandling.

Övergripande sett framstår de bestämmelser som ska gälla enligt dataskyddslagen, som kompletterar förordningen, och enligt brottsdatalagen, som genomför direktivet, som ändamålsenliga även på kamerabevakningsområdet. Detsamma kan generellt sett antas i fråga om registerförfattningar som reglerar behandling av personuppgifter inom särskilda sektorer och som vid behov kommer att ändras till följd av EU-regleringen. Sådana bestämmelser behöver därför inte nödvändigtvis upprepas i kamerabevakningslagen.

Vidare skulle lagen bli mycket omfattande, om den utförligt skulle ange vad som gäller på området för kamerabevakning. Visserligen skulle en sådan lag samla bestämmelserna och därigenom göra det överskådligt vad som gäller. Detta skulle dock ändå inte gälla fullt ut, eftersom förordningen kommer att vara direkt tillämplig i Sverige och behöva tillämpas för sig. Dessutom skulle överskådligheten begränsas av det stora antal bestämmelser som skulle krävas i lagen. Det skulle behövas en viss uppsättning bestämmelser som avser kamerabevakning som omfattas av förordningen. Dessa skulle i princip upprepa bestämmelserna i dataskyddslagen men däremot inte kunna upprepa många av förordningens bestämmelser, som ska gälla direkt. Vad gäller kamerabevakning som faller in under direktivets tillämpningsområde skulle det krävas en annan, utförlig uppsättning bestämmelser som fullständigt genomför hela direktivet, som bl.a. innehåller bestämmelser om skyldigheter för personuppgiftsansvariga, om rättigheter för enskilda samt om tillsyn, rättsmedel och sanktioner. Vad slutligen gäller kamerabevakning som varken omfattas av förordningen eller direktivet skulle det också behövas någon form av reglering.

Att bestämmelser om kamerabevakning finns på olika håll gör det givetvis svårare att få en överblick över vad som gäller på området och därmed svårare att tillämpa bestämmelserna både för enskilda och myndigheter. En sådan lagstiftningsteknik kommer dock att gälla generellt på dataskyddsområdet. På förordningens område ska gälla förordningen, dataskyddslagen med förordning och olika registerförfattningar. På direktivets område kommer registerförfattningar och brottsdatalagen och dess förordning att gälla. På det område som faller utanför förordningen och direktivet ska enligt dataskyddslagen förordningen och den lagen gälla.

Det redovisade talar för att en utgångspunkt för kamerabevakningslagen ska vara att den endast bör innehålla de bestämmelser

som särskilt behövs för kamerabevakning på grund av de specifika förhållanden som gäller för sådan bevakning till skillnad mot annan personuppgiftsbehandling. Lagen bör alltså inte innehålla bestämmelser som i princip skulle utgöra upprepningar av bestämmelser som annars gäller för personuppgiftsbehandling. I lagen kan det dock behöva hänvisas till dessa bestämmelser för att tydliggöra vad som gäller för kamerabevakning.

De bestämmelser som bör tas in i kamerabevakningslagen är sådana som sedan länge utgjort kärnan i svensk lagstiftning på kamerabevakningsområdet, nämligen i första hand bestämmelser om krav på tillstånd eller liknande och, som redan berörts i avsnitt 9.1 ovan, bestämmelser om krav på upplysning om kamerabevakning. Lagen måste också innehålla bestämmelser om vad som menas med kamerabevakning. Vidare kan det behövas ytterligare bestämmelser, t.ex. om vad som ska gälla om lagens krav åsidosätts.

I det nu sagda ligger också att en restriktivitet ska prägla bedömningarna av vilket innehåll kamerabevakningslagen bör ha. Lagen bör endast innehålla bestämmelser som avviker från vad som annars gäller för personuppgiftsbehandling i den utsträckning som bestämmelserna kan motiveras av principiella skäl och av ett påtagligt praktiskt behov. Det utrymme som finns i EU-regleringen för särbestämmelser i nationell rätt utgör just ett utrymme för undantag från vad som annars ska gälla och ska därför användas med försiktighet.

Övriga utgångspunkter

Som övriga utgångspunkter för bestämmelserna i kamerabevakningslagen ska gälla följande.

De bestämmelser som ska tas in i lagen bör, så långt det är förenligt med EU-regleringen och ändamålsenligt, vara desamma för all kamerabevakning, oavsett om det är kamerabevakning som omfattas av förordningen, kamerabevakning som avses i direktivet eller kamerabevakning som faller utanför förordningens och direktivets tillämpningsområden. Detta för att bestämmelserna ska bli så förutsebara och lättillämpade som möjligt.

Dessutom bör bestämmelserna i den utsträckning det är lämpligt utformas med motsvarande bestämmelser i dagens kameraövervakningslag som förebilder. Vissa begrepp i eller andra delar av den

lagen har ett innehåll som är ändamålsenligt även framöver. Att inte behålla detta skulle i onödan kräva en förändrad praxis.

9.2.2 Ökade möjligheter till kamerabevakning och ett förstärkt integritetsskydd

Bedömning: Kamerabevakningslagen bör ge ökade möjligheter till kamerabevakning. Samtidigt bör lagen ge ett förstärkt skydd för den personliga integriteten vid kamerabevakning, däribland på arbetsplatser.

Skälen för bedömningen

Inledning

I avsnittet ovan om vilka allmänna utgångspunkter som ska gälla för den nya kamerabevakningslagen har bl.a. slagits fast att lagen i första hand bör innehålla bestämmelser om krav på tillstånd eller liknande och då i den utsträckning som sådana bestämmelser kan motiveras av principiella skäl och av ett påtagligt praktiskt behov.

Även ur ett renodlat svenskt perspektiv finns det skäl att nu inta en något mer generös hållning till svenska bestämmelser som ger goda möjligheter att bedriva kamerabevakning. Dessa skäl utvecklas i det följande.

Allmänt om behov av kamerabevakning och skydd mot intrång i den personliga integriteten

Kamerabevakning kan användas i olika syften. Två viktiga syften är att förebygga, upptäcka eller utreda brott och att förhindra olyckor. Andra betydelsefulla syften kan vara kopplade till t.ex. arbetslivet, skolmiljön, jordbruk och skogsbruk eller miljön.

Den tekniska utvecklingen går fort och allt talar för att denna utveckling kommer att fortsätta. Utvecklingen har medfört att möjligheterna att bedriva kamerabevakning för sådana syften som nu angetts liksom för andra ändamål som framstår som godtagbara har förbättrats avsevärt; tekniken har blivit billigare, mer tillgänglig och

enklare att hantera och själva bevakningen kan bedrivas allt mer avancerat.

Mot behovet av kamerabevakning står skyddet mot intrång i den personliga integriteten i den meningen att enskilda inte i onödan ska bli föremål för kamerabevakning. Den nya EU-regleringen bygger på en balans mellan behovet av behandling av personuppgifter och integritetsskyddet. Detsamma gäller sedan länge för svensk lagstiftning på kamerabevakningsområdet. Detta är grundläggande och ska gälla även framöver.

Det måste följaktligen finnas en balans mellan behovet av kamerabevakning och skyddet av den personliga integriteten i nu nämnd mening.

Behovet av kamerabevakning och anspråket på integritetsskydd förändras

Den balans som måste finnas mellan behovet av kamerabevakning och skyddet av den personliga integriteten innebär att så länge intresset av kamerabevakning är berättigat och väger tyngre än integritetsskyddsintresset får den enskilde acceptera det intrång i integriteten som bevakningen innebär. Vad som utgör berättigade intressen av kamerabevakning och hur tungt dessa väger är inte en gång för alla givet utan förändras över tid i takt med samhällsutvecklingen. Detsamma gäller i viss mån synen på den personliga integriteten. Behoven av kamerabevakning i olika sammanhang kan bli starkare eller svagare och nya behov kan uppkomma, allmänhetens attityd till kamerabevakning kan förändras och tekniken för att vid kamerabevakning skydda den personliga integriteten kan utvecklas.

Närmare om behovet

Vad först gäller behovet av kamerabevakning har det skett ett flertal viktigare förändringar i samhället under senare år. Dessa förändringar kan mötas på olika sätt. Kamerabevakning kan utgöra en av flera verksamma åtgärder.

Risken för och människors oro för terrorangrepp har ökat. Nyligen har ett terrorangrepp skett i centrala Stockholm där ett tidigare terrordåd också skett. Vid angreppet dödades och skadades ett fler-

tal människor. Under senare år har flera terrorangrepp skett även i andra länder i vår närhet, bl.a. i Frankrike, Belgien, Tyskland och Storbritannien. Tidigare har också terrorhandlingar inträffat i t.ex. Köpenhamn. Angreppen har exempelvis varit riktade mot tunnelbana, restauranger, platser för musik- och idrottsevenemang samt promenadstråk och torg och har lett till att många människor mist livet eller skadats. Kamerabevakning har i flera av fallen bidragit till att brotten kunnat utredas och att terroristerna och deras medhjälpare kunnat identifieras och lagföras.

Skilda politiska eller religiösa åsikter i samhället har också i en ökande omfattning lett till olika former av angrepp på människor eller egendom som representerar en motsatt åsikt eller religion. Exempelvis har hoten mot journalister, som är en yrkesgrupp av särskild betydelse för det demokratiska samhället, ökat. Det finns också flera exempel på att personer tillhörande en viss religiös eller etnisk grupp eller lokaler som används av gruppen har utsatts för bl.a. hot och skadegörelse just p.g.a. denna tillhörighet.

Mot denna bakgrund har regeringen tagit fram en nationell strategi mot terrorism som ska vara utgångspunkten för Sveriges långsiktiga arbete på detta område både nationellt och internationellt (skr. 2014/15:146). Syftet är att skapa en tydlig struktur för det arbete som krävs för att motverka terroristbrottslighet. Vikten av samverkan mellan olika aktörer har betonats. I strategin har det vidare slagits fast att terrorism bl.a. riktar sig mot offentliga platser som platser för kollektivtrafik och kultur- och köpcentra och att även tillfälliga arrangemang som idrotts- och kulturevenemang har visat sig vara tänkbara mål för terroristattentat.

Även vissa typer av andra brott, liksom ordningsstörningar, begås ofta på och har ibland en direkt koppling till platser där ett stort antal människor samlas. Brotten och störningarna kan därför få allvarliga konsekvenser för människors liv och hälsa eller egendom. Det gäller exempelvis brott som begås av s.k. huliganer i samband med idrottsevenemang, inne på eller utanför idrottsarenorna eller på allmänna kommunikationer på vägen till eller från evenemangen. Sådan brottslighet utgör fortfarande ett stort problem.

Också andra incidenter på sådana platser kan få allvarliga följdverkningar. Som exempel kan nämnas om brand uppstår på en arena eller i en lokal som används för en konsert. Vid sådana händelser är det viktigt att platsen kan utrymmas snabbt och säkert och att

räddningsinsatser från brandkårs- och sjukvårdspersonal kan styras på ett effektivt sätt.

Ett ytterligare problem som har uppmärksammats under senare tid och som är kopplat till stora folksamlingar eller vissa särskilda platser är att det förekommer att grupper av pojkar eller yngre män tafsar eller på annat sätt förgriper sig på flickor och unga kvinnor. Det har exempelvis inträffat vid flera tillfällen på utomhuskonserter och i simhallar.

Ett annat stort problem är att vissa bostadsområden i Sverige präglas av social oro, utanförskap och kriminalitet. Det skapar otrygghet för de boende. I vissa områden förekommer att polis, räddningspersonal och andra personer som utövar någon form av samhällelig funktion möts av grupper av personer som med våld och på andra sätt hindrar dem eller försvårar för dem att utföra sina arbetsuppgifter. Att dessa centrala funktioner i samhället av sådana skäl inte kan fungera på avsett vis och att de som arbetar i dessa inte kan göra det på ett tryggt sätt är självfallet oacceptabelt. I sådana områden kan det också finnas särskilda problem med att utreda brottslighet på grund av en låg anmälningsfrekvens och ett motstånd mot att vittna.

Slutligen ska nämnas att flyktingsituationen under senare år har lett till att ett stort antal människor har sökt sig till Sverige, vilket bl.a. har medfört trångboddhet på befintliga asylboenden och behov av nya boenden. Det har i sin tur medfört brott och störningar på både befintliga och potentiella boenden, orsakade av såväl boende som externa personer.

Att brottslighet kan bekämpas och lagföras är av grundläggande betydelse för samhället. Samhället blir tryggare att leva i, om brott helt kan förebyggas eller om pågående brott kan avbrytas. Att begångna brott i efterhand kan utredas och lagföras bidrar också till ett tryggare samhälle genom att straffsystemet på det sättet får avsedd generell brottsavhållande verkan. Det visar att statsmakten menar allvar med straffbuden och beaktar brottsoffrens intressen. Uppgiften att bekämpa och lagföra brott är självfallet i första hand en fråga för polisen, åklagare och domstolar samt vissa andra myndigheter. Men även andra, t.ex. kommuner, kan ha ett ansvar för eller ett särskilt intresse av att motverka brottslighet och också goda förutsättningar att göra det. Behovet av och kraven på samverkan mellan olika aktörer för detta ändamål ökar hela tiden.

Kamerabevakning är ett verktyg bland flera som kan förebygga, förhindra eller upptäcka brottslighet eller bidra till att begångna brott kan utredas och lagföras.

Regeringen har i mars 2017 lagt fram skrivelsen *Tillsammans mot brott – Ett nationellt brottsförebyggande program* (skr. 2016/17:126). I programmet är regeringens målsättningar för det brottsförebyggande arbetet inom olika politikområden samlade. Programmet ska även bidra till att öka kunskaperna om brottsförebyggande arbete och stimulera samverkan mellan fler aktörer. Programmet är en del av en större satsning på brottsförebyggande arbete. I programmet berörs allt från individinriktade insatser till förebyggande åtgärder mot situationer eller platser där risken för brott är hög. Kamerabevakning behandlas under regeringens målsättningar vad gäller en ökad formell och informell kontroll. Där uttalas bl.a. att kamerabevakning på särskilt brottsutsatta platser och för vissa brottstyper kan fungera som ett komplement till andra brottsförebyggande åtgärder och också underlätta avslöjandet av pågående brott samt vara av betydelse i efterföljande utredningar.

Undersökningar, både svenska och utländska, visar att kamerabevakning har vissa brottsförebyggande effekter. Det gäller i första hand platser där brottsnivån är hög och koncentrerad och brotten typiskt sett är planerade, såsom egendomsbrott. I sådana situationer kan kamerabevakning ha en direkt avskräckande verkan på potentiella brottslingar.

Vidare kan realtidstillgång till material från kamerabevakning vara av stort värde för Polismyndighetens planlagda operativa brottsförebyggande insatser. Det gäller t.ex. vid riktade insatser på en särskild plats. Med ledning av information från kamerabevakning kan polisen upptäcka när kända gärningsmän rör sig i området och ingripa förebyggande eller förhindra pågående brott. Det kan också finnas ett underrättelsemässigt behov av material från kamerabevakning, t.ex. för att verifiera om information från andra källor eller hypoteser i ett ärende är riktiga. Material från kamerabevakning kan även utgöra ett viktigt underlag för planering och vidtagande av skyddsåtgärder vid allvarliga hot mot en person eller viss egendom. Exempelvis kan materialet visa om en potentiell gärningsman uppehåller sig i den hotade personens närhet.

Dessutom används material från kamerabevakning, både från Polismyndighetens egen bevakning och andra aktörers bevakning, i brotts-

utredningar. Frågan om det funnits kameror på en brottsplats kontrolleras alltid vid utredning av grova brott. Om brottet begåtts på eller i närheten av färdmedel såsom buss, tåg eller tunnelbana, tar polisen kontakt med den som ansvarar för kollektivtrafiken. Om det gäller en händelse vid en uttagsautomat, kontaktas den berörda banken. Polisen kan också uppsöka brottsplatsen för att få en uppfattning om vilket material från kamerabevakning som finns att inhämta därifrån. Materialet kan ge svar på frågor om själva händelseförloppet och vilka personer eller föremål som varit involverade. Utifrån materialet kan det också vara möjligt att bedöma t.ex. när i tiden en händelse ägt rum, hur länge den pågått eller hur långt personer kan ha hunnit under den tid då de inte syns i bild. Ofta har materialet också betydelse för att kunna bedöma tillförlitligheten i uppgifter som tilltalade, målsägande och vittnen lämnar. Materialet kan ge det ytterligare stöd som krävs för att en domstol säkert ska kunna avgöra att den åtalade är gärningsmannen och att den gärning som åklagaren påstått har begåtts har inträffat. Ibland kan sådant material utgöra den enda bevisningen. I andra fall kan materialet ge en tydligare bild än vad muntliga uppgifter kan ge av hur allvarligt ett brott, t.ex. en grov misshandel, varit och därmed ge ett något bättre underlag för att bestämma hur strängt straff som ska dömas ut. Material från kamerabevakning kan alltså föra brottsutredningar framåt och bidra till – och ibland vara avgörande för – att lagföring också sker.

Kamerabevakning kan följaktligen användas på olika sätt för att motverka brottslighet av alla typer, inte bara för att genom avskräckning förebygga planerade brott av viss typ.

Även i övrigt kan kamerabevakning bidra till säkerhet och trygghet för människor, egendom och miljö. Kamerabevakning kan t.ex. innebära att olika slag av faror i trafiken, i naturen och på andra offentliga platser kan upptäckas och avvärjas. Kamerabevakning kan också bidra till att verkningarna av inträffade olyckor och liknande händelser kan begränsas. Även andra intressen kan främjas genom användning av kamerabevakning, t.ex. intresset av att upprätthålla en god arbetsmiljö. Kamerabevakning kan även ha en funktion att fylla i olika verksamheter för planering, kontroll m.m. Möjligheterna till kamerabevakning för sådana ändamål förbättras hela tiden i takt med den tekniska utvecklingen.

Sammanfattningsvis har behoven av kamerabevakning ökat både när det gäller brottsutsatta platser eller platser med en generell hotbild riktad mot sig och andra platser.

Behovet tillgodoses inte i dag

De ovan beskrivna behoven av kamerabevakning tillgodoses dock inte i dag fullt ut av möjligheterna enligt gällande rätt att bedriva kamerabevakning.

Det kan vara svårt att visa att en plats är så drabbad av brott att den ska få kamerabevakas. För att inspelning av material ska få ske krävs vidare att platsen är särskilt brottsutsatt. Det fordrar utförlig dokumentation om att allvarlig eller omfattande brottslighet redan har inträffat på platsen. Vissa platser är inte, eller kan inte visas vara, frekvent utsatta för brott men löper likväl jämfört med andra platser i samhället en särskild risk att utsättas för brott. Det är oftast platser som drabbats av brottslighet av vissa typer och i viss omfattning eller som annars har en generell hotbild riktad mot sig. Som exempel kan nämnas lokaler och platser som används av religiösa samfund eller för asylboende. Även medieredaktioner kan ha en sådan hotbild riktad mot sig. På platser med nybyggnation, t.ex. nya bostäder, där en särskild risk för brottslighet på goda grunder kan antas i det enskilda fallet är det i regel omöjligt att på förhand visa platsens utsatthet för brott.

Också andra platser kan löpa en särskild risk, som ibland tillfälligt kan öka ytterligare, att utsättas för allvarlig brottslighet men i dag ha tillstånd till kamerabevakning som är begränsade i vissa avseenden. Det gäller t.ex. vissa platser för kollektivtrafik. På exempelvis större järnvägsstationer kan tillståndet medge bevakning endast av ett visst område eller under en viss tid trots att sådana platser kan utgöra potentiella objekt för terrorangrepp. Det har förekommit att en mer omfattande bevakning för att möta en hastigt uppkommen förhöjd risk för terrorangrepp på en sådan plats åstadkommits genom att Polismyndigheten ”tillfälligt tagit över” bevakningen från den som annars bedriver denna. Polismyndigheten har då åberopat sin möjlighet att bedriva kamerabevakning tillståndsfritt under viss tid. Huruvida ett sådant tillfälligt övertagande är invändningsfritt rättsligt sett är inte helt säkert. För kamerabevak-

ning gäller vissa bestämmelser om säkerhet m.m., som i det enskilda fallet kan lägga hinder i vägen för en sådan lösning.

Även på platser som kan visas vara brottsutsatta kan det vara svårt att få tillstånd till kamerabevakning. Det gäller främst gator och torg där det är kommunen som vill bedriva kamerabevakning i syfte att motverka brottslighet. Visserligen finns det inte något lagligt hinder mot att en kommun söker och beviljas tillstånd till sådan bevakning. I rättspraxis har det emellertid slagits fast att det är en betydande skillnad mellan kamerabevakning av gator och torg som utförs av polisen och sådan bevakning som sker i kommunal regi och att detta bör beaktas vid den avvägning som ska göras mellan intresset av kamerabevakning och intresset av integritetsskydd. Det är visserligen riktigt att det är polisen som i första hand har i uppgift att bekämpa brott och upprätthålla allmän ordning och säkerhet. Det finns dock numera, som framgått ovan, en uttalad ambition att stärka samverkan mellan rättsväsendets myndigheter och andra aktörer såsom kommuner, landsting och andra i det civila samhället vad gäller bl.a. brottsförebyggande arbete. Ett förbättrat brottsförebyggande arbete på lokal nivå kan omfatta situationella åtgärder, t.ex. kamerabevakning, som syftar till att minska sannolikheten för att brott begås. Vidare har kommuner ett eget ansvar för allmän ordning och säkerhet inom kommunen.

Även andra aktörer kan ha ett starkt intresse av att motverka brott genom egna åtgärder för att säkerställa att deras verksamheter kan bedrivas utan störningar och för att skydda personal och besökare. Det kan gälla exempelvis på platser som akutmottagningar på sjukhus och väntrum hos myndigheter. För dessa kan kamerabevakning vara ett bra komplement till andra åtgärder. Kamerabevakning kan direkt avskräcka personer från att begå brott på platsen eller öka den upplevda tryggheten för dem som vistas på platsen och därigenom öka den sociala kontrollen där. Emellertid är det inte alltid som kamerabevakning i sådana sammanhang tillåts.

Inte heller finns det allmänt sett någon möjlighet att kamerabevaka för att motverka brottslighet riktad mot vissa särskilt utsatta fordon eller personer som använder dessa, såsom räddningsfordon och brandmän eller polisbilar och polismän. Ytterligare ett exempel på brottslighet som riktas mot fordon och annan liknande lös egendom där kamerabevakning kan ha en roll att spela är jordbruks- och skogsbruksmaskiner. Sådan egendom representerar höga

värden och är stöldbegärlig. Egendomen måste ofta lämnas obevakad, inte sällan ute i skog och mark.

Generellt sett kan också sägas att kamerabevakning i syfte att utreda framtida brott ännu inte synes ha fått samma genomslag i praxis vad gäller meddelade tillstånd som syftet att direkt förebygga att brott begås. Att kamerabevakning får ske i det förstnämnda syftet tydliggjordes när kameraövervakningslagen sommaren 2013 ersatte den tidigare gällande lagen på området. Denna mer indirekta brottsförebyggande verkan tar sikte på brottslighet i allmänhet och kan därför få stor betydelse förutsatt att den ges ett genomslag i praktiken.

Avslutningsvis ska framhållas att intresset av att skydda den personliga integriteten inte alltid står i motsats till intresset av kamerabevakning utan tvärtom kan förstärka detta. Staten har ett ansvar för att i största möjliga utsträckning skydda medborgarna från integritetsangrepp av olika slag från andra enskilda. Det kan exempelvis göras genom att lagstiftningsvägen möjliggöra för staten själv, t.ex. genom Polismyndigheten, eller för andra aktörer att använda kameror i det syftet. Att minska risken för att människor blir utsatta för brott eller att åtminstone möjliggöra att brott utreds och lagförs är centralt ur ett brottsofferperspektiv. På motsvarande sätt har det allmänna ett visst ansvar för att förebygga att människor utsätts för andra faror i den offentliga miljön och för att begränsa effekterna när sådana faror har realiserats. Medborgarnas krav på det allmänna i dessa hänseenden förändras också över tid.

Sammanfattningsvis motsvarar möjligheterna att bedriva kamerabevakning i dag inte de ökade behoven av sådan bevakning.

Närmare om skyddet mot integritetsintrång och attityden till kamerabevakning

Att det finns behov av kamerabevakning innebär inte med automatik att sådan bevakning ska få ske. Kamerabevakning innebär ett intrång i enskildas intresse av att inte bli föremål för kamerabevakning och får därför inte ske slentrianmässigt. Den personliga integriteten skyddas bl.a. av Europakonventionen och regeringsformen. Även den nya EU-regleringen på dataskyddsområdet syftar till att förstärka skyddet för den personliga integriteten.

Den tekniska utvecklingen har inneburit en drastisk ökning av möjligheterna att använda kameror i olika sammanhang och att sprida materialet, som ofta är av god kvalitet. Det är därför angeläget att skyddet för den personliga integriteten är starkt så att otillbörliga integritetsintrång kan undvikas.

Samtidigt har, som framgått av avsnitt 4.3, attityden hos allmänheten i Sverige till kamerabevakning blivit allt mer positiv vad gäller bevakning på allmänna platser, såsom gator och torg samt i kollektivtrafiken. Exempelvis kamerabevakas i stor utsträckning bussar, pendeltåg, spårvagnar och tunnelbana samt vissa hållplatser och stationer. Det är platser där många människor passerar och som normalt ligger i anslutning till områden där människor bor eller befinner sig för nöje och rekreation. Det finns inte något som tyder på att det inom överskådlig framtid skulle ske en större omsvängning i denna attityd. Den ökade acceptansen för kamerabevakning torde delvis ha sin förklaring både i att bilder numera tas och sprids i en helt annan omfattning än tidigare och i att kamerabevakning bidrar till att människor i allmänhet upplever en trygghet på platser som bevakas. Det kan också vara så att människor i dag med hänsyn till hur tekniken för spridning av material har utvecklats ser det som viktigare än kamerabevakningen i sig om bilder från bevakningen sparas, vem som kan se bilderna och hur dessa behandlas vidare.

Sammanfattningsvis måste anspråket på att skydda enskilda mot intrång i den personliga integriteten vara starkt. Synen på kamerabevakning bland allmänheten i Sverige har dock blivit allt mer positiv.

Integritetsfrämjande teknik

Vad slutligen gäller de tekniska möjligheterna att skydda enskildas personliga integritet har dessa ökat efter hand som teknikutvecklingen fortskridit. Denna utveckling kan väntas fortsätta. Som exempel på integritetsfrämjande teknik kan nämnas sådan teknik som innebär att personer i bild maskeras så att det inte går att identifiera dem och teknik som krypterar upptaget bild- och ljudmaterial. Ytterligare ett exempel är kameror som aktiveras först efter olika typer av larm, t.ex. larm som reagerar på onormala rörelsemönster, inbrottslarm, överfallslarm, evakueringslarm och larm som aktiveras av skottlossning, glaskross eller människoskrik. Det förekommer

också exempelvis teknik som innebär att ”ursprungsbilden” raderas omedelbart och att endast viss information lämnar kameran, t.ex. information om antalet människor som passerat denna.

Möjligheterna till kamerabevakning bör öka – samtidigt bör skyddet för den personliga integriteten förstärkas

Den utveckling som beskrivits ovan har medfört ett ökat behov av att kunna bedriva kamerabevakning för viktiga samhälleliga och andra berättigade intressen. Samtidigt har allmänhetens attityd till kamerabevakning förändrats i en mer accepterande riktning. Vidare har de tekniska möjligheterna att skydda den personliga integriteten vid kamerabevakning förbättrats. Det måste därför anses möjligt och rimligt att öka möjligheterna till kamerabevakning för berättigade syften utan att det skapar en obalans i förhållande till skyddet för den personliga integriteten. Även med en ökad användning av kamerabevakning, som svarar mot dagens och morgondagens behov, kan alltså en godtagbar balans mellan, å ena sidan, behovet av kamerabevakning och, å andra sidan, integritetsskyddet uppnås. Mot den bakgrunden ska som utgångspunkt gälla att den nya kamerabevakningslagen bör ge ökade möjligheter till kamerabevakning. Samtidigt bör lagen ge ett förstärkt skydd för den personliga integriteten vid kamerabevakning. Det kan t.ex. åstadkommas genom generella bestämmelser om hur material från kamerabevakning får behandlas och, som tas upp i det följande avsnittet, genom särskilda bestämmelser om kamerabevakning på arbetsplatser.

Integritetsskyddet på arbetsplatser bör förstärkas

Den i avsnitt 2 nämnda Integritetskommittén har utifrån ett individperspektiv kartlagt och analyserat risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik. Kommittén har bl.a. undersökt användningen av kameror i arbetslivet. I denna del har kommittén uttalat följande (SOU 2016:41 s. 232 ff. och s. 241).

> I vissa branscher är kameraövervakning av arbetstagare mycket vanligt förekommande. Det kan röra sig om kameraövervakning både på platser dit allmänheten har tillträde och på platser dit allmänheten inte

har tillträde. Ett exempel på det förra är övervakning av butiksytor där både kunder och butikspersonal vistas. Ett exempel på det senare kan i samma butik vara övervakning av områden där bara personal får vistas såsom i lager eller pausutrymmen.

Den kameraövervakning som inbegriper arbetstagare kan i många fall egentligen vara inriktad på att övervaka eller kontrollera verksamhetens kunder, patienter eller brukare. Men eftersom arbetstagarna befinner sig i samma lokaler, träffas även de av arbetsgivarens övervakning.

År 2013 genomförde 19 av länsstyrelserna ett stort antal nationellt samordnade tillsynsinsatser inriktade på kameraövervakning i gallerior och köpcentrum och deras butiker. [– – –] I den samordnade tillsynen besöktes 116 gallerior och 693 butiker och övriga verksamheter. Efter butikerna var de flesta besökta verksamheterna restauranger och caféer. Av totalt 809 besök ledde 327 till anmärkningar. De vanligaste anmärkningarna var att det saknades överenskommelser med personalen om kameraövervakningen, att kameror var felriktade, att övervakning gjordes utanför butikslokal, att skyltningen var bristfällig eller obefintlig samt att anmälan eller tillstånd saknades.

Butiker, restauranger och caféer finns också med bland de arbetsplatser som pekades ut i Sveriges radios programserie om kameraövervakning av arbetsplatser hösten 2014. Den mest omtalade bristen som nämns i programserien är olaglig användning av inspelningar från övervakningen. I programserien förekommer exempel på att inspelat material används för att kontrollera om anställda på ett lager står och pratar med varandra eller hur länge butikspersonal samtalar med kunderna. Även övervakningskameror på äldreboenden, som anhöriga sätter upp i sina släktingars rum eller lägenheter, tas i programserien upp som något som personalen kan uppleva som ett intrång.

Under år 2015 granskade Datainspektionen kameraövervakningen hos fyra butiker tillhörande olika detaljhandelskedjor. Myndigheten granskade specifikt övervakningskameror som var riktade mot platser som lager, lastkajer och liknande, alltså områden där kunder normalt sett inte befinner sig. I besluten riktade Datainspektionen kritik mot samtliga fyra butiker för hur dessa kameraövervakade lagerutrymmen, personalingångar och lastkajer… Butikerna kritiserades även för att de inte tillräckligt tydligt informerade om den kameraövervakning som förekommer. [– – –]

Det kan således konstateras att många arbetstagare i landet övervakas för ändamål och på ett sätt som inte är förenligt med gällande lagstiftning. Om den tilltagande teknikutvecklingen och den nedåtgående prisutvecklingen för kameraövervakningsutrustning håller i sig, finns dessutom en risk för att de redan konstaterade bristerna kommer att öka i takt med att allt fler övervakningskameror installeras på arbetsplatserna. [– – –]

Risken är också stor att material från kameraövervakning kan komma att användas för andra ändamål än de som ursprungligen föranledde installationen av övervakningskamerorna. Som exempel kan nämnas

> ett ärende hos Datainspektionen där material från kameraövervakningen i en skola användes för att kontrollera hur den kontrakterade städentreprenören utförde sitt arbete på kvällarna. Kamerorna hade egentligen satts upp för att förhindra skadegörelse, inbrott och stölder.
>
> Av Sveriges Radios rapportering framgår också att länsstyrelserna vanligtvis endast förmår utföra enstaka stickprovskontroller av arbetsgivarnas tillämpning.
>
> Tillsyn av kameraövervakning på platser dit allmänheten inte har tillträde görs av Datainspektionen. Det är uppenbart att en så liten myndighet med många andra arbetsuppgifter inte kan göra annat än ett fåtal stickprovskontroller när det gäller en så pass omfattande och nationellt spridd företeelse som kameraövervakning. [– – –]
>
> Kommittén anser därför att kameraövervakning på arbetsplatser innebär en allvarlig risk för den personliga integriteten. Samtidigt måste beaktas att kameraövervakning kan medföra direkta fördelar för enskilda arbetstagare, främst när säkerheten på arbetsplatsen förbättras av övervakningen.

Samma bedömning som Integritetskommittén har gjort görs i detta sammanhang. Som en ytterligare utgångspunkt för kamerabevakningslagen ska därför gälla att integritetsskyddet vid kamerabevakning på arbetsplatser bör förstärkas.

I sammanhanget ska nämnas att när det gäller de ovan nämnda butikerna som Datainspektionen granskade och riktade kritik mot utfärdade inspektionen samtidigt vissa förelägganden. Dessa har överklagats till förvaltningsdomstol.

10 Lagens syfte och tillämpningsområde

10.1 Lagens inledande bestämmelser om syfte m.m.

Förslag: Kamerabevakningslagen ska innehålla en inledande bestämmelse som upplyser om att det i lagen finns bestämmelser om kamerabevakning som kompletterar dataskyddsförordningen, som genomför dataskyddsdirektivet eller som avser sådan bevakning som inte omfattas av förordningen eller direktivet.

I kamerabevakningslagen ska vidare anges att syftet med lagen är att tillgodose behovet av kamerabevakning för berättigade ändamål och att skydda enskilda mot otillbörliga intrång i den personliga integriteten vid sådan bevakning.

En bestämmelse som anger hur lagen förhåller sig till andra bestämmelser ska också finnas. Utöver vad som föreskrivs i kamerabevakningslagen ska i tillämpliga delar gälla

1. dataskyddsförordningen, dataskyddslagen, föreskrifter som meddelats med stöd av den lagen eller annan författning som kompletterar dataskyddsförordningen vid kamerabevakning som omfattas av förordningen eller dataskyddslagen, eller
2. brottsdatalagen, föreskrifter som meddelats med stöd av den lagen eller annan författning som genomför dataskyddsdirektivet vid kamerabevakning som omfattas av brottsdatalagen.

Bedömning: Någon allmän bestämmelse i kamerabevakningslagen om att kamerabevakning i grunden är laglig vid myndighetsutövning eller utförande av en uppgift av allmänt intresse

enligt förordningen eller vid utförande av en arbetsuppgift enligt direktivet och brottsdatalagen behövs inte.

Skälen för förslaget och bedömningen

Syfte m.m.

Den nya kamerabevakningslagen ska innehålla en inledande bestämmelse som upplyser om att det i lagen finns bestämmelser om kamerabevakning som kompletterar dataskyddsförordningen och som genomför dataskyddsdirektivet. En sådan bestämmelse ska regelmässigt tas in i svensk lagstiftning som har unionsrättslig bakgrund. För fullständighetens skull ska i bestämmelsen lämpligen också anges att lagens bestämmelser även avser sådan kamerabevakning som inte omfattas av förordningen eller direktivet.

Vidare bör lagen innehålla en bestämmelse om lagens syfte. Som framgått av avsnitt 7.1.2, 7.2.2 och 7.3 är en sådan bestämmelse möjlig att ha på både förordningens tillämpningsområde och direktivets tillämpningsområde liksom på det område för kamerabevakning som faller utanför EU-regleringen. I dagens kameraövervakningslag finns en syftesbestämmelse som, enligt vad som framgått av de angivna avsnitten, är förenlig med den nya EU-regleringen. Lagens syfte anges vara att tillgodose behovet av kameraövervakning för berättigade ändamål samtidigt som enskilda skyddas mot otillbörliga intrång i den personliga integriteten. En sådan tudelad och tydlig syftesbestämning rimmar alltså väl med förordningen och direktivet. En liknande bestämmelse i kamerabevakningslagen framstår också som lämplig. Den kan ge uttryck för det övergripande målet med bestämmelser om kamerabevakning, nämligen att åstadkomma en lämplig balans mellan nyttan med kamerabevakning och skyddet av enskilda mot integritetsintrång. En syftesbestämmelse kan vidare ge vägledning för tolkningen av de materiella bestämmelser som enligt lagen ska gälla för kamerabevakning. Att kamerabevakning också kommer att regleras genom bestämmelser i förordningen och, som föreslås nedan, genom bestämmelser i annan lagstiftning som kompletterar förordningen eller genomför direktivet kan inte anses hindra en syftesbestämmelse i kamerabevakningslagen eller att den ges en vid utformning. Den kan tjäna till vägledning även i tillämpningen av sådana bestämmelser.

I personuppgiftslagen och registerförfattningar, som bygger på 1995 års dataskyddsdirektiv, uttrycks ofta författningens syfte något annorlunda än i kameraövervakningslagen i den del som avser integriteten. Där anges syftet vara att ”skydda människor mot att deras personliga integritet kränks vid behandling av personuppgifter”. I den nya brottsdatalagen, som genomför direktivet, anges syftet bl.a. vara att ”skydda fysiska personers grundläggande fri- och rättigheter i samband med behandling av personuppgifter”. Denna formulering knyter an till hur syftet anges i direktivet. I förordningen uttrycks syftet på ett likartat sätt. I enlighet med den tidigare fastslagna utgångspunkten att kamerabevakningslagens bestämmelser bör anpassas till EU-regleringen i delar där de i och för sig kan utformas annorlunda skulle lagens syfte kunna anges på motsvarande sätt. Å andra sidan framstår kameraövervakningslagens uttryckssätt som bättre anpassat för de bestämmelser som ska finnas i kamerabevakningslagen. Syftesbestämmelserna i förordningen och brottsdatalagen är mer allmänt hållna och anpassade för det stora antal rättigheter m.m. som finns i de regleringarna. Dessa syftesbestämmelser kommer att gälla när förordningen eller brottsdatalagen ska tillämpas vid kamerabevakning. Det framstår därför som mest ändamålsenligt att uttrycka kamerabevakningslagens syfte i den diskuterade delen på samma sätt som i kameraövervakningslagen men med vissa mindre justeringar.

Följaktligen föreslås en bestämmelse i kamerabevakningslagen med innehåll att syftet med lagen är att tillgodose behovet av kamerabevakning för berättigade ändamål och att skydda enskilda mot otillbörliga intrång i den personliga integriteten vid sådan bevakning.

Förhållandet till andra bestämmelser

Som slagits fast tidigare är det en utgångspunkt för kamerabevakningslagen att den endast bör innehålla de bestämmelser som särskilt behövs för kamerabevakning. Som kommer att framgå i det följande föreslås i enlighet med denna utgångspunkt endast vissa materiella bestämmelser i lagen. I övrigt ska bestämmelser i förordningen och i andra författningar gälla för sådan kamerabevakning som avses i lagen i den utsträckning de kan tillämpas på sådan

bevakning. Det gäller främst dataskyddslagen, som kompletterar förordningen, och föreskrifter som meddelats med stöd av den lagen eller brottsdatalagen, som genomför direktivet, och föreskrifter som meddelats med stöd av den lagen beroende på om bevakningen utgör personuppgiftsbehandling som omfattas av förordningens tillämpningsområde eller direktivets och brottsdatalagens tillämpningsområde. Såväl dataskyddslagen som brottsdatalagen är subsidiära till annan lagstiftning om behandling av personuppgifter, såsom kamerabevakningslagen, och gäller därför endast i den mån den särskilda lagstiftningen saknar bestämmelser. Också registerförfattningar, som har företräde framför dataskyddslagen och brottsdatalagen, kan någon gång innehålla bestämmelser som kan tillämpas på kamerabevakning. Det föreslås därför att det ska finnas en bestämmelse i kamerabevakningslagen som anger hur lagen förhåller sig till andra bestämmelser. Bestämmelsen föreslås ange också förhållandet till förordningen. Förordningen gäller visserligen direkt för kamerabevakning i de delar den kan tillämpas på sådan bevakning och förutsatt att kamerabevakningslagen inte innehåller särskilda bestämmelser. För att göra paragrafen fullständig och begriplig bör detta dock också framgå. En sådan upplysning är förenlig med förordningen. Bestämmelsen föreslås ha det innehållet att utöver vad som föreskrivs i kamerabevakningslagen ska i tillämpliga delar gälla

1. dataskyddsförordningen, dataskyddslagen, föreskrifter som meddelats med stöd av den lagen eller annan författning som kompletterar dataskyddsförordningen vid kamerabevakning som omfattas av förordningen eller dataskyddslagen, eller
2. brottsdatalagen, föreskrifter som meddelats med stöd av den lagen eller annan författning som genomför dataskyddsdirektivet vid kamerabevakning som omfattas av brottsdatalagen.

Dataskyddsutredningen har föreslagit att bestämmelserna i förordningen – i den ursprungliga lydelsen – och dataskyddslagen i tillämpliga delar ska gälla även vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten och i verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget, dvs. som utförs inom ramen för den gemensamma utrikes- och säkerhetspolitiken. Verksamhet som inte omfattas av unions-

rätten är bl.a. verksamhet som rör nationell säkerhet och verksamhet på försvarsområdet.

Den föreslagna bestämmelsen i kamerabevakningslagen som hänvisar till bl.a. dataskyddslagen innebär att förordningen och dataskyddslagen gäller även för kamerabevakning på det nu angivna området. I sektorsspecifika författningar som avser verksamhet utanför förordningens egentliga tillämpningsområde kan det dock komma att föreskrivas undantag från den bestämmelse i dataskyddslagen som gör förordningen och den lagen tillämplig. Ett sådant undantag innebär att den sektorsspecifika författningen eller brottsdatalagen i stället gäller för personuppgiftsbehandling i en sådan verksamhet, inklusive för kamerabevakning i verksamheten.

När det gäller de materiella bestämmelser som ska finnas i kamerabevakningslagen ska vidare, vilket framgår av kommande avsnitt, bestämmelser i förordningen och dataskyddslagen med föreskrifter eller brottsdatalagen med föreskrifter göras tillämpliga i vissa avseenden som knyter an till de frågor som regleras specifikt i lagen.

En allmän bestämmelse om laglig kamerabevakning?

En annan grundläggande fråga är om det i kamerabevakningslagen behövs eller bör finnas en allmän bestämmelse vad gäller viss kamerabevakning på förordningens tillämpningsområde och kamerabevakning på direktivets tillämpningsområde för att bevakningen överhuvudtaget ska vara laglig, dvs. vila på en rättslig grund.

Enligt förordningen är personuppgiftsbehandling laglig bl.a. när behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Av förordningen följer vidare att grunden för sådan behandling ska fastställas i nationell rätt eller unionsrätten. Vidare måste ändamålet med behandlingen vara nödvändigt för att utföra uppgiften respektive myndighetsutövningen. Som framgått av avsnitt 7.1.8 har Dataskyddsutredningen kommit till slutsatsen att kravet på stöd i nationell rätt inte avser behandlingen i sig utan myndighetsutövningen eller uppgiften av allmänt intresse. Utredningen har bedömt att det inte krävs någon ny svensk reglering på generell nivå för att sådan behandling som sker som ett led i myndighetsutövning ska kunna ske, eftersom all myndighetsutövning i Sverige måste ha stöd i

gällande rätt. Vad gäller behandling som sker för att kunna utföra en uppgift av allmänt intresse har utredningen bedömt att sådana uppgifter har stöd i gällande rätt vad avser myndigheter och privata aktörer som agerar på uppdrag av myndigheter. Övrig privaträttslig verksamhet av allmänt intresse kan enligt utredningen ibland vara fastställd i lagstiftningen. Utredningen har ansett att det inte heller i fråga om dessa uppgifter behövs någon ny svensk reglering på generell nivå. Utredningen har ändå föreslagit att det i dataskyddslagen tydliggörs att personuppgifter får behandlas, om behandlingen är nödvändig antingen som ett led i myndighetsutövning som den personuppgiftsansvarige utövar enligt lag eller annan författning eller för att den personuppgiftsansvarige ska kunna utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som meddelats med stöd av lag eller annan författning.

Enligt direktivet är behandling av personuppgifter laglig endast om behandlingen är nödvändig för att en behörig myndighet ska kunna utföra en uppgift på grundval av unionsrätten eller nationell rätt i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder eller skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten. Som framgått av avsnitt 7.2.4 har Utredningen om 2016 års dataskyddsdirektiv ansett att det inte kan vara personuppgiftsbehandlingen i sig som avses. Enligt utredningen ska direktivet tolkas så att personuppgiftsbehandling alltid ska ha stöd i den behöriga myndighetens arbetsuppgifter så som de kommer till uttryck i unionsrätten eller i nationell lagstiftning och andra för verksamheten bindande beslut om arbetsuppgifter. Utredningen har föreslagit att detta ska framgå av brottsdatalagen. Utredningens bedömning är att direktivets krav uppfylls genom de författningar som reglerar verksamhet i vilken personuppgiftsbehandling förekommer på direktivets område tillsammans med brottsdatalagen och registerförfattningar.

Förordningen och direktivet måste förstås på motsvarande sätt när det gäller kamerabevakning. Någon allmän bestämmelse i kamerabevakningslagen om att kamerabevakning i grunden är laglig vid myndighetsutövning eller utförande av en uppgift av allmänt intresse enligt förordningen eller vid utförande av en arbetsuppgift enligt direktivet och brottsdatalagen behövs alltså inte. Dataskyddslagen och brottsdatalagen kommer att innehålla bestämmelser om rättslig

grund som kan gälla för kamerabevakning enligt den ovan föreslagna bestämmelsen om kamerabevakningslagens förhållande till andra bestämmelser. Det förtjänar att understrykas att för att kamerabevakning överhuvudtaget ska få ske måste den vara laglig i den mening som krävs enligt förordningen och dataskyddslagen eller direktivet och brottsdatalagen. Huruvida kamerabevakning dessutom endast ska få ske efter tillstånd behandlas i avsnitt 11.

10.2 Lagens materiella tillämpningsområde

Förslag: Kamerabevakningslagen ska gälla vid kamerabevakning. Med kamerabevakning ska förstås

1. att en TV-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning, utan att manövreras på platsen, används varaktigt eller regelbundet upprepat för personbevakning,
2. att en separat teknisk anordning för avlyssning eller upptagning av ljud används för personbevakning i samband med användning av sådan utrustning som avses i 1, och
3. att en separat teknisk anordning för att behandla upptaget bild- och ljudmaterial används.

Skälen för förslaget

Det materiella tillämpningsområdet ska i stort vara detsamma som tidigare…

I dag avgränsas kameraövervakningslagens materiella tillämpningsområde genom en definition av begreppet kameraövervakning. Med kameraövervakning avses användning av övervakningsutrustning, dvs. övervakningskameror och övrig övervakningsutrustning. Med övervakningskameror avses TV-kameror, andra optisk-elektroniska instrument och därmed jämförbara utrustningar som är uppsatta så att de, utan att manövreras på platsen, kan användas för personövervakning samt separata tekniska anordningar för avlyssning eller upptagning av ljud, vilka i samband med användning av sådan utrust-

ning används för personövervakning. Med övrig övervakningsutrustning avses separata tekniska anordningar för att behandla upptaget bild- och ljudmaterial.

Regeringen har nyligen föreslagit att kameraövervakningslagen inte ska omfatta kameraövervakning som sker från drönare, om övervakningen bedrivs av någon annan än en myndighet (prop. 2016/17:182). Undantaget ska träda i kraft den 1 augusti 2017. Riksdagen väntas besluta i frågan under senare halvan av juni 2017 (bet. 2016/17:JuU31).

Definitionen av övervakningskameror, särskilt dess första del, är den centrala för lagens materiella tillämpningsområde. Denna definition har i väsentliga delar varit densamma sedan den första lagstiftningen på området, lagen (1977:20) om TV-övervakning, infördes. Av förarbetena till den lagen (prop. 1975/76:194 s. 15 ff.) framgår att TV-apparatur då kommit till användning i allt större utsträckning. Användningen av sådan apparatur ansågs få ett inslag av försåtlighet genom att övervakaren kunde uppehålla sig på en plats där denne inte kunde iakttas av den person mot vilken apparaturen verkade och som var omedveten om dess existens. Hos den enskilde som var medveten om övervakningen kunde en känsla av otrygghet uppkomma. Det ansågs föreligga en särskild risk från integritetssynpunkt för det fall apparaturen skulle få en sådan spridning att medborgarna mer allmänt skulle utsättas för någon form av övervakning. Mot den bakgrunden bedömdes det som angeläget att genom lagstiftning begränsa möjligheterna till TV-övervakning. Dold sådan övervakning skulle i princip inte få förekomma.

Lagstiftningen på området har alltsedan den första lagen omfattat både bevakning med kameror som monterats på fasta platser, t.ex. på eller i byggnader eller på stolpar, och bevakning med kameror som monterats på eller i rörliga objekt, t.ex. fordon. Användning av handhållna kameror, dvs. kameraanvändning från rörliga subjekt, har däremot inte omfattats. Kamerabevakning av det förstnämnda slaget var ursprungligen vanligast förekommande och kom därför av naturliga skäl att stå i fokus för lagstiftningen. Även senare lagstiftning på området har i huvudsak haft samma fokus, trots att den tekniska utvecklingen inneburit att kameraanvändning från rörliga objekt fortlöpande har ökat.

Den tekniska utvecklingen och utvecklingen i samhället i övrigt har fortsatt. I dag är kameror generellt sett billigare, enklare att använda och mer tillgängliga än de varit tidigare. Kameror kan användas på en mängd olika sätt och för olika syften. Exempelvis har det blivit förhållandevis vanligt att i olika sammanhang använda kameror, vars bild- och ljudmaterial håller hög kvalitet, på eller i rörliga objekt, t.ex. på eller i bilar och på drönare. Detsamma gäller användning av kameror som bärs av människor. Stora delar av befolkningen har ofta med sig kameror, t.ex. i sina mobiltelefoner. Vissa yrkesgrupper bär kameror med eller på sig för att vid behov använda dessa i tjänsten. Utvecklingen har också lett till förändrade vanor. Det inte ovanligt att människor i dag publicerar bilder från sin vardag på sociala medier där bilderna kan få en stor spridning. Bilder tas och sprids numera på ett sätt som för inte så länge sedan var svårt att föreställa sig från såväl teknik- som integritetssynpunkt. Å ena sidan torde denna utveckling i någon mån ha fått till följd att synen på vilket integritetsintrång som det innebär att bli fotograferad eller filmad har förändrats hos många människor i en mer accepterande riktning. Å andra sidan kan utvecklingen sägas ha medfört att behovet av skydd mot otillbörliga integritetsintrång är större än tidigare.

De skäl som ursprungligen har motiverat lagstiftningen på kamerabevakningsområdet och hur denna avgränsats gör sig därför i princip fortfarande gällande. Det har inte heller i den kartläggning och utvärdering som gjorts, och som redovisats i avsnitt 5, framkommit att det finns anledning att ge den nya kamerabevakningslagen ett tillämpningsområde som genomgripande skiljer sig från vad som hittills gällt. Det har inte heller legat i utredningens uppdrag.

Integritetsskäl skulle visserligen kunna åberopas för en utvidgning till i princip all kameraanvändning, även t.ex. användning av handhållna kameror. De potentiella riskerna med användning av kameror, särskilt behandlingen av bildmaterialet och ibland även av ljudmaterial, är betydligt större nu än tidigare. För en utvidgning talar också att det skulle bli enklare att avgöra om lagen är tillämplig. Ett så omfattande tillämpningsområde skulle emellertid samtidigt medföra att t.ex. ett eventuellt krav på tillstånd till bevakning enligt lagen skulle, även om det begränsas, medföra en helt ny eller utökad skyldighet för många. Det är inte heller realistiskt att nu med den utbredda användningen av kameror i olika sammanhang

inkludera all användning i lagen och låta lagens materiella bestämmelser gälla generellt. Att viss kameraanvändning även fortsättningsvis lämnas utanför innebär, som beskrivits i avsnitt 8, inte heller att den användningen lämnas helt oreglerad. Den nya dataskyddsförordningen och den generella kompletterande lagen till förordningen, dataskyddslagen, eller den nya generella brottsdatalagen, som genomför dataskyddsdirektivet, kommer att gälla för sådan kameraanvändning.

Av de angivna skälen finns det inte heller anledning att avsevärt inskränka kamerabevakningslagens tillämpningsområde jämfört med vad som gäller enligt kameraövervakningslagen. Däremot bör kamerabevakningslagen, som framgått av avsnitt 9, endast innehålla de bestämmelser som särskilt behövs för kamerabevakning. Som framgår av senare avsnitt ska lagen bl.a. innehålla ett krav på upplysning vid kamerabevakning och ett krav på tillstånd för att få bedriva kamerabevakning. Dessa krav måste givetvis utformas med beaktande av de olika former av kamerabevakning som lagen ska omfatta. Det innebär att viss kamerabevakning kan behöva undantas från dessa krav.

Det finns dock ändå anledning att utforma lagens materiella tillämpningsområde annorlunda jämfört med vad som gäller enligt kameraövervakningslagen. Skälen för det redovisas i avsnittet nedan. I de därpå följande avsnitten diskuteras hur tillämpningsområdet kan och ska utformas.

…men bör delvis förändras

Vid den utvärdering av kameraövervakningslagen som gjorts har det framkommit att det inte sällan varit svårt att tillämpa lagen i förhållande till ny teknik. Problemen har främst rört frågan om lagen varit tillämplig eller inte. Rekvisiten *uppsatt* och *utan att manövreras på platsen* i definitionen av övervakningskameror har ansetts svårtolkade. Exempelvis har det varit svårt att avgöra i vilken utsträckning lagen är tillämplig på kameror som sätts upp på eller i rörliga objekt som t.ex. i bilar och på drönare. Andra exempel där det ibland varit oklart om lagen varit tillämplig eller inte har gällt kameror som bärs på kroppen, webbkameror för videokonferens hos

arbetsgivare eller på internetcaféer och annan utrustning för videokonferens.

Högsta förvaltningsdomstolen (HFD) har i två domar hösten 2016 (HFD 2016 ref. 71) prövat om en kamera monterad på ett cykelstyre eller på insidan av vindrutan i en bil respektive en kamera monterad på en drönare föll in under kameraövervakningslagens tillämpningsområde. Av avgörandena framgår att en kamera som monteras på något av de angivna ställena *kan* vara uppsatt och att det gäller även om kameran monteras bort efter varje färd eller flygning. Enligt HFD krävs att placeringen av kameran har en viss varaktighet eller att kameran återkommande kommer att fästas på fordonet respektive drönaren. I de fall som domstolen prövade var kamerorna att anse som uppsatta.

I fråga om platsen för manövrering anförde HFD i det först nämnda avgörandet att kameran skulle vara uppsatt på cykelstyret eller på vindrutans insida i bilen, dvs. i fordonsförarens omedelbara närhet, och att föraren skulle starta och stänga av kameran samt avgöra vad som skulle filmas genom att styra fordonet. All manövrering av kameran ansågs därför ske på platsen. Kameran omfattades därmed inte av kameraövervakningslagen.

I det andra avgörandet konstaterade domstolen att kameran på drönaren skulle fotografera från luften men styras och även i övrigt hanteras från marken. Hanteringen bedömdes därför ske från en plats som var klart åtskild från den där kameran var uppsatt. Kameran ansågs därmed inte manövrerad på platsen. Den omfattades följaktligen av kameraövervakningslagen.

Vidare har Förvaltningsrätten i Stockholm i en dom den 20 oktober 2016 (mål nr 383-16) prövat om kameraövervakningslagen var tillämplig på Försäkringskassans användning av webbkameror för videosessioner mellan personer som tar kontakt med Försäkringskassan och handläggare där. Förvaltningsrätten ansåg att en sådan webbkamera var manövrerad på platsen. Handläggaren hade under videosessionen en pågående kontroll över kameran, eftersom denna var en förutsättning för sessionen och handläggaren hela tiden befann sig i kamerans omedelbara närhet. Under sessionen skedde också en direkt styrning över vad som visades i kameran. Kameraövervakningslagen var därför inte tillämplig.

De redovisade avgörandena innebär att flera av de nämnda frågorna om kameraövervakningslagens tillämplighet på ny teknik har besva-

rats. Fortfarande kan dock förutses vissa svårigheter att tolka tillämpningsområdet, om detta skulle anges på samma sätt i den nya kamerabevakningslagen. Det gäller främst kameror som är placerade på eller i fordon, fartyg eller luftfartyg eller liknande rörliga objekt.

Det finns alltså skäl att överväga hur tillämpningsområdet i kamerabevakningslagen bör se ut och utforma detta på ett något annorlunda sätt än vad som gjorts i kameraövervakningslagen.

Utgångspunkter för utformningen av tillämpningsområdet

Frågan är då hur kamerabevakningslagens materiella tillämpningsområde övergripande sett kan och bör utformas.

Vad först gäller hur tillämpningsområdet ska förhålla sig till förordningen och direktivet får det, som framgått av avsnitt 7.1.3 respektive 7.2.3, i lagen införas ett kamerabevakningsbegrepp som både på förordningens område och på direktivets område är antingen snävare eller vidare än begreppet personuppgiftsbehandling. Vad gäller sådan kamerabevakning som inte omfattas av EU-regleringen kan, som framgått av avsnitt 7.3, i och för sig fritt väljas vilket begrepp som bör införas. Som framgått tidigare bör dock bestämmelserna i kamerabevakningslagen utformas på ett gemensamt sätt för all kamerabevakning. Tillämpningsområdet kan utformas på det sättet utan hinder av EU-regleringen och en sådan utformning är också lämplig. I sammanhanget ska erinras om att Dataskyddsutredningen har föreslagit att dataskyddslagen ska innehålla en bestämmelse om att förordningen och lagen ska tillämpas även vid personuppgiftsbehandling i verksamhet som inte omfattas av unionsrätten och i verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken. Genom en hänvisning till dataskyddslagen kan alltså bestämmelserna i förordningen och den lagen gälla för sådan kamerabevakning som avses i kamerabevakningslagen och som faller utanför förordningens egentliga tillämpningsområde.

Som utgångspunkter vid utformningen gäller vidare att kamerabevakningsbegreppet bör anpassas till EU-regleringen i delar där det i och för sig kan utformas annorlunda; i den utsträckning det är lämpligt bör dock tillämpningsområdet utformas med förebild i kameraövervakningslagen.

Vidare är det ofrånkomligt med en utformning som är teknikberoende. Detta eftersom tillämpningsområdet, som slagits fast inledningsvis, inte genomgripande ska förändras jämfört med vad som gäller enligt kameraövervakningslagen. Att viss kameraanvändning inte ska omfattas innebär med nödvändighet att denna måste särskiljas från den som ska omfattas. Vidare måste denna form av personuppgiftsbehandling särskiljas från annan sådan behandling.

En avgränsning av tillämpningsområdet som i stället utgår från syftet med en kamerabevakning i det enskilda fallet är inte lämplig. En avgränsning av det slaget medför sina och helt nya tillämpningssvårigheter och riskerar att göra lagens bestämmelser tandlösa. En sådan lösning är också svår att förena med det förhållandet att lagen inte bör omfatta t.ex. användning av handhållna kameror. Som framgår av avsnitt 12 nedan finns det vidare goda skäl att generellt sett låta ett krav på upplysning om kamerabevakning gälla oavsett i vilket syfte bevakningen bedrivs. Dessutom är förordningen och direktivet uppbyggda så att deras materiella tillämpningsområden i grunden omfattar all behandling av personuppgifter oavsett syfte.

Följaktligen görs bedömningen att kamerabevakningslagen måste avgränsas genom kriterier som delvis är av teknisk karaktär.

Olika avgränsningar är tänkbara

Olika avgränsningar är tänkbara vad gäller utformningen av det materiella tillämpningsområdet. Nedan behandlas först vilken utrustning som ska omfattas. Därefter övervägs om dagens begrepp ”utan att manövreras på platsen” bör behållas. Sedan diskuteras tre olika alternativ för att avgränsa tillämpningsområdet i övrigt och dras en slutsats om vilket alternativ som ska väljas. Som kommer att framgå finns fördelar och nackdelar med samtliga alternativ. Därefter diskuteras hur tillämpningsområdet närmare ska utformas. I ett avslutande avsnitt berörs särskilt frågan om analog kamerabevakning.

Utrustningen ska anges på samma sätt som i dag

Vad då först gäller den utrustning som ska omfattas av det materiella tillämpningsområdet kan inledningsvis konstateras att det varken vid utvärderingen av kameraövervakningslagen eller på annat sätt har framkommit att den avgränsning som görs i lagen i det avseendet har lett till några särskilda tillämpningssvårigheter. Avgränsningen fångar in ett brett spektrum av teknisk utrustning. Den är därför ändamålsenlig för att fånga in såväl dagens teknik som den teknik som kan väntas utvecklas inom den närmaste framtiden. Samma avgränsning ska därför användas i kamerabevakningslagen. Dagens begrepp TV-kamera kan visserligen synas något föråldrat med hänsyn till teknikutvecklingen. Det är dock inarbetat och används ofta vid skyltning om kamerabevakning liksom det synonyma begreppet videokamera. Begreppet bör därför behållas.

Lagen ska alltså omfatta TV-kameror, andra optisk-elektroniska instrument och därmed jämförbara utrustningar. Innebörden av dessa begrepp behandlas närmare i författningskommentaren. I ett senare avsnitt behandlas vissa andra anordningar som också ska omfattas av lagen.

Begreppet ”utan att manövreras på platsen” ska behållas

När det sedan gäller dagens avgränsning i kameraövervakningslagen att utrustningen används ”utan att manövreras på platsen” har det visserligen genom den utvärdering som gjorts framkommit att det funnits praktiska svårigheter att avgöra om viss ny teknik är att anse som manövrerad på platsen eller inte. De ovan redovisade domstolsavgörandena har dock inneburit klargöranden på ett flertal punkter.

Även om vissa kvarvarande eller framtida tolkningssvårigheter kan finnas eller uppkomma, om avgränsningen behålls, är det tveksamt om sådana helt kan undgås genom att någon annan avgränsning införs i stället. I sammanhanget kan noteras att såväl bestämmelserna om hemlig kameraövervakning som den hittillsvarande lagstiftningen i Danmark och Norge om kameraövervakning innehåller en avgränsning som knyter an till fjärrstyrning. Någon form av avgränsning i kamerabevakningslagen som skiljer en TV-kamera eller en därmed jämförbar utrustning som hanteras fortlöpande

från en annan plats från annan kameraanvändning är nödvändig med hänsyn till vad som angetts inledningsvis om att tillämpningsområdet inte genomgripande ska utvidgas. En avgränsning kan alltid medföra vissa tolkningsfrågor. Det framstår därför, och eftersom domstolspraxis under senare tid har klargjort rättsläget i vissa avseenden, som lämpligast att behålla dagens avgränsning i stället för att införa ett nytt begrepp.

Tillämpningsområdet ska följaktligen avgränsas så att det krävs att en TV-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning används utan att manövreras på platsen. Med platsen menas liksom tidigare den plats där utrustningen finns. Med att utrustningen används utan att manövreras på platsen avses att den fortlöpande hanteringen av denna sker på ett ställe som är klart åtskilt från den plats där utrustningen finns. Utrustning som fungerar med inbyggd automatik är inte heller manövrerad på platsen. Utrustning som däremot finns i användarens omedelbara närhet och som fortlöpande styrs av användaren är att anse som manövrerad på platsen.

Det innebär att handhållna kameror inte omfattas. Detsamma gäller kameror som på annat sätt bärs på kroppen. Motsvarande gäller t.ex. kameror på vindrutan i fordon. I undantagsfall kan dock omständigheterna vara sådana att manövreringen i dessa fall inte kan anses ske på platsen. Det gäller om en kroppsburen utrustning helt eller till större delen styrs från någon annan plats än den där utrustningen finns – av någon annan person än den som bär utrustningen eller annars från annat håll – och förutsatt att bäraren har en skyldighet, som har stöd i gällande rätt, att vistas på eller röra sig på en viss plats med utrustningen. En sådan skyldighet kan föreligga när bäraren tillhör en yrkeskategori som använder kameror och han eller hon bär kameran i tjänsten och har att utföra de arbetsuppgifter som arbetsgivaren bestämt. Bäraren av utrustningen avgör då inte självständigt vilka områden som fotograferas eller filmas och styr inte heller själv fortlöpande utrustningen. I motsvarande situation som för kroppsburen utrustning kan en kamera i eller på ett fordon eller liknande inte anses manövrerad på platsen när den person som använder fordonet inte är den som fortlöpande hanterar kameran genom att sätta på, styra och stänga av denna och inte heller fritt kan välja färdväg.

I dessa sistnämnda fall är det fråga om särskilda situationer där det framstår som rimligt att de bestämmelser i kamerabevakningslagen som föreslås nedan ska gälla. Nedan diskuteras huruvida kameror i eller på rörliga objekt eller kroppsburna kameror genom en annan avgränsning bör uteslutas från kamerabevakningslagens tillämpningsområde.

Tre alternativ för avgränsningen i övrigt

Vad därefter angår dagens krav i kameraövervakningslagen på att utrustningen ska vara ”uppsatt så att den kan användas för personövervakning” har detta vållat tillämpningssvårigheter, främst vad avser hur ”uppsatt” ska tolkas i fråga om ny teknik. Även om de ovan redovisade domstolsavgörandena har bidragit till att klargöra innebörden är begreppet fortfarande förenat med oklarheter och språkligt sett missvisande i vissa fall. Det bör därför inte behållas. Frågan är då vilken avgränsning som bör väljas i stället. Nedan diskuteras tre alternativ.

Ett minimalistiskt alternativ

Ett första alternativ är en minimalistisk utformning innebärande att tillämpningsområdet överhuvudtaget inte ska omfatta kameror i eller på fordon, fartyg eller luftfartyg eller liknande rörliga objekt. Med detta alternativ blir tillämpningsområdet påtagligt snävare än kameraövervakningslagens tillämpningsområde.

En fördel med detta alternativ är att det blir tydligt och enkelt att avgöra vad som faller in under respektive utanför tillämpningsområdet. Vissa praktiska svårigheter med en lagstiftning som träffar kamerabevakning från rörliga objekt kan vidare undvikas.

Det finns dock också nackdelar med detta alternativ. En nackdel är att det inger betänkligheter ur ett integritetsperspektiv. Kameraanvändning som sker inuti eller från ett fordon etc. kan från integritetssynpunkt vara jämställbar med kamerabevakning som sker t.ex. inuti eller från en byggnad. Kameror på eller i rörliga objekt kan, liksom kameror på fasta objekt, t.ex. användas för att under längre stunder eller återkommande bevaka vissa platser där många människor befinner sig. Exempelvis kan sådan varaktig eller syste-

matisk kameraanvändning avse miljön inuti bussar, tågvagnar, taxibilar eller passagerarfartyg. Det finns också en risk med en utformning som utesluter kameror i eller på fordon etc. Det kan t.ex. tänkas att ett fordon ställs upp under en längre tid på ett torg eller en annan plats där människor rör sig och har en kamera monterad som regelbundet filmar platsen och människorna där. Vidare kan teknikutvecklingen komma att innebära att rörliga objekt, såsom kamerautrustade drönare, kan användas för att under längre stunder bevaka en och samma plats där människor normalt vistas.

En annan nackdel är att en sådan utformning innebär att olika regler blir tillämpliga för vissa juridiska eller fysiska personer som använder kameror för ett och samma syfte i sin verksamhet. Som exempel kan nämnas kameraanvändning i kollektivtrafiken där den som driver verksamheten vill använda kameror såväl inuti sina bussar, tågvagnar eller dylikt som på busshållplatser, stationer eller motsvarande platser. Även om själva tillämpningsområdet blir enklare att avgöra med detta alternativ blir alltså tillämpningen av den materiella regleringen mer komplicerad i sådana fall.

Ett maximalistiskt alternativ

Ett alternativ som går i motsatt riktning jämfört med det ovan diskuterade är att låta kamerabevakningslagens tillämpningsområde omfatta både kameraanvändning som sker från fasta objekt, t.ex. från byggnader, och från rörliga objekt, t.ex. bilar och drönare. Detta alternativ inkluderar också kroppsburna kameror, som dock i regel ändå kommer att falla utanför tillämpningsområdet därför att de manövreras på platsen. Med detta alternativ blir tillämpningsområdet omfattande och likt kameraövervakningslagens tillämpningsområde.

Fördelarna respektive nackdelarna med detta alternativ kan sägas vara omvända jämfört med vad som angetts för alternativet i föregående avsnitt.

Fördelarna är att det från integritetssynpunkt blir ett sakligt sett tillfredsställande tillämpningsområde och att risken för att lagen kringgås undanröjs så långt som möjligt. De skäl som hittills motiverat ett så omfattande tillämpningsområde och som fortfarande gör sig gällande kan tillgodoses. Dessutom blir regleringen enklare på det sättet att endast kamerabevakningslagens materiella

bestämmelser i ett visst hänseende kommer att gälla för en och samma kamerabevakning eller kamerabevakning av en och samma aktör.

Nackdelarna med detta alternativ är att tillämpningsområdet fortsatt kan kräva tolkningar.

Ett alternativ däremellan

Ett alternativ som ligger emellan de två ovan redovisade alternativen är att avgränsa kamerabevakningslagen så att den *i princip* inte omfattar användning av kameror eller därmed jämförbara utrustningar som är placerade på eller i fordon, fartyg etc. och inte heller kameror som bärs på kroppen. Alternativet får lämpligen knytas till att kamerabevakningen ska avse en *viss plats*, dvs. en och samma plats. Bevakning med utrustning som är placerad på eller i byggnader eller andra fast placerade objekt omfattas då. Detsamma gäller bevakning av en bestämd plats inuti ett rörligt objekt, t.ex. inuti en buss, en tågvagn eller liknande. Bevakningen bör på samma sätt som gäller enligt kameraövervakningslagen i dag vara av viss varaktighet så att helt tillfällig bevakning på platsen inte omfattas. Även kamerabevakning som sker tillfälligt men mer systematiskt på platsen bör av integritetsskäl rimligen omfattas. Kameraanvändning som träffar ”rörliga” platser, dvs. platser som fortlöpande skiftar allt eftersom objektet med utrustningen rör sig, ska däremot i princip inte omfattas.

Ett sådant alternativ har den fördelen att det ger ett delvis tydligare och enklare tillämpningsområde än det maximalistiska alternativet. Vidare fångar detta alternativ till skillnad från det minimalistiska in situationer där integritetshänsyn gör sig gällande i samma utsträckning som kameraanvändning som sker från fasta objekt. Detta alternativ är dock förenat med ett flertal avgränsningssvårigheter.

En svårighet är att användning av kameror och därmed jämförbara utrustningar som är monterade eller placerade i fordon och liknande ofta samtidigt fångar både en ”fast” miljö inuti objektet och en ”rörlig” miljö utanför detta. Det kan gälla exempelvis för bussar där bl.a. insidan vid dörrarna och ett område strax utanför dörrarna bevakas för att trygga en säker på- eller avstigning. På

motsvarande sätt kan t.ex. kameror i fordon som används för värdetransporter eller andra tjänster samtidigt fånga både miljön inne i fordonet och en del av miljön utanför. Att ha ett tillämpningsområde för kamerabevakningslagen som endast omfattar en del av en sådan gemensam bevakning är inte lämpligt. Det skulle kunna innebära t.ex. att ett eventuellt krav på tillstånd till bevakningen behövs för en del av denna medan förordningens eller brottsdatalagens bestämmelser om konsekvensbedömning och samråd skulle gälla för den övriga delen. I vissa fall kan visserligen bevakningen av utomhusmiljön omfattas genom att det är fråga om upprepad, men tillfällig, bevakning av vissa särskilda platser. Det kan gälla t.ex. busshållplatser eller stationer. Generellt är det dock knappast så; många fordon eller andra rörliga objekt med kameror kan inte sägas systematisk avbilda samma platser. Det får då noga bedömas från fall till fall hur bevakningen ska gå till och om det finns en koppling till en viss plats på det sätt som beskrivits.

För att undvika en sådan bedömning och tolkning i varje enskilt fall skulle möjligen kunna läggas till att tillämpningsområdet omfattar även kameraanvändning som, oavsett varaktighet eller upprepning, sker i omedelbar anslutning till en sådan plats. Ett sådant tillägg kan dock också ge upphov till tolkningsfrågor. Det kan vidare delvis utesluta kameraanvändning från fordon, fartyg etc. som fångar miljön längre utanför objektet samtidigt som det fångar miljön inuti och omedelbart utanför. I ett sådant fall uppkommer det nämnda problemet med att kamerabevakningslagens krav gäller för en viss del av användningen medan andra bestämmelser gäller för användningen i övrigt. Detta kan gälla t.ex. självkörande fordon där kameror, i vart fall under den närmaste framtiden då försöksverksamheter ska pågå, kommer att filma både förarens agerande inuti fordonet och trafikmiljön på nära och längre håll utanför fordonet. Det framstår som rimligt att kameraanvändning i dylika fall helt omfattas av lagens tillämpningsområde och att det i stället görs ett särskilt undantag från lagen, om det behövs för ett visst sådant fall. Som presenterats i avsnitt 2.2 överväger en särskild utredning frågor om självkörande fordon.

Det finns följaktligen svårigheter att hitta en ändamålsenlig avgränsning för det nu diskuterade alternativet. Även om en sådan kan åstadkommas kan den inte utformas på ett sätt som tydligt och

enkelt pekar ut vad som omfattas respektive inte omfattas. Den kommer att kräva tolkning i varje enskilt fall.

Slutsats om de tre alternativen

Som framgått är inte något av de tre alternativ som diskuterats ovan invändningsfritt. Självklart är det önskvärt med ett tillämpningsområde för kamerabevakningslagen som fångar in de situationer där det är sakligt motiverat att lagens materiella bestämmelser gäller och som samtidigt innebär att det är förutsebart och enkelt att avgöra om viss kameraanvändning omfattas av lagen eller inte. Detta kan dock inte helt uppnås. I det läget måste det anses väga tyngst att lagen får det tillämpningsområde som är mest tillfredsställande ur ett integritetsperspektiv och samtidigt ger minsta möjliga tillämpningssvårigheter. Det är också viktigt att så långt möjligt undvika att olika regelsystem kommer att gälla i en viss fråga som avser en och samma kameraanvändning.

Det alternativ som bäst svarar mot detta är alternativet med det mest vittomfattande tillämpningsområdet, den maximalistiska lösningen, som omfattar kameraanvändning från såväl fasta objekt som rörliga objekt. Det omfattar också kroppsburna kameror, vilka dock som regel manövreras på platsen och därför faller utanför tillämpningsområdet.

Detta alternativ passar vidare väl med de materiella bestämmelser som lagen enligt vad som föreslås i senare avsnitt ska innehålla. Som framgår där föreslås ett fåtal materiella bestämmelser som innebär att vissa specifika svenska krav ska gälla utöver eller i stället för vissa krav som följer av EU-regleringen. Kraven är knutna till att kamerabevakning överhuvudtaget ska få ske, dvs. till den inledande behandlingen. Hanteringen av material från bevakningen ska däremot i princip styras av andra bestämmelser. Ett snävare utformat tillämpningsområde skulle dessutom innebära att lagen, med den begränsade reglering som den ska innehålla, skulle få ett mycket litet mervärde.

Den närmare utformningen

Den maximalistiska lösningen ska alltså väljas. Det innebär att en avgränsning som ligger nära men som så långt möjligt undanröjer de problem finns med kameraövervakningslagens ”uppsatt så att den kan användas för personövervakning” ska väljas.

I detta ligger ett krav på viss varaktighet. Detta krav bör förtydligas och utvecklas ytterligare. Ett krav som kopplas närmare själva användningen av en TV-kamera eller därmed jämförbar utrustning, inte placeringen av denna, och som ger uttryck för att det ska vara fråga om en varaktighet eller regelbunden upprepning passar väl in för att avgränsa tillämpningsområdet till sådan kamerabevakning som enligt vad som redovisats ovan bör omfattas av lagen. Kravet kommer genom det ytterligare kravet på att kameran inte ska manövreras på platsen att begränsas till kamerabevakning från fasta objekt och från vissa rörliga objekt, dvs. ofta till kamerabevakning av bestämda platser. En liknande utformning har de nu gällande danska och norska särskilda bestämmelserna på kamerabevakningsområdet. Det är också en utformning som mer liknar den som finns i de svenska bestämmelserna om hemlig kameraövervakning, som träffar fjärrstyrd personövervakning generellt.

Det ska alltså vara fråga om *varaktig* kameraanvändning vid ett visst tillfälle eller flera tillfällen. Vidare ska kortvarig men *regelbundet upprepad* användning av en kamera omfattas. Så är fallet när en kamera används vid ett flertal tillfällen som är åtminstone relativt närliggande i tiden. Detsamma gäller när tillfällena är mer utspridda men ändå infaller på ett planmässigt sätt eller annars följer ett särskilt mönster.

Det ska framhållas att ett tillämpningsområde för kamerabevakningslagen som knyter an till själva användningen blir annorlunda tidsmässigt jämfört med vad som gäller enligt kameraövervakningslagen, som är kopplad till att övervakningsutrustning sätts upp. Anledningen till den lagens och dess föregångares motsvarande utformning var att lagstiftaren ville undvika bevissvårigheter i fråga om en kamera används eller inte (prop. 1997/98:64 s. 22). Sådana bevissvårigheter bör emellertid inte överdrivas. Det torde i många fall vara uppenbart om utrustning som ska omfattas av kamerabevakningslagen överhuvudtaget används. Exempelvis innebär placeringen och upptagningsområdet i många fall att det står klart att

utrustningen används. Om det sker en inspelning, finns det spår från användningen i det lagrade materialet. Vidare är ett av syftena med bestämmelserna om kamerabevakning att värna den personliga integriteten genom att ge ett skydd mot behandling av bild- och ljudmaterial. Syftet är inte i första hand att skydda enskilda mot det intrång som det kan upplevas vara att en kamera som ännu inte är i bruk, och som kanske aldrig kommer till användning, är placerad på en viss plats. Kameraövervakningslagen omfattar följaktligen inte heller kameraattrapper. Sådana ska inte heller omfattas av kamerabevakningslagen.

När det sedan gäller vad användningen ska ta sikte på är ett alternativ att välja begreppet personbevakning och ge det samma innebörd som kameraövervakningslagens begrepp personövervakning och ett annat att välja begreppet behandling av personuppgifter.

Med *personövervakning* avses att människor kan identifieras genom övervakningen. För att en möjlighet till identifiering ska anses föreligga krävs att sådana kännetecken kan iakttas som gör att man utan större osäkerhet kan skilja de personer som iakttas från andra personer. Så är t.ex. fallet om hela personen eller personens ansikte syns tydligt.

I dessa fall är det också fråga om behandling av personuppgifter enligt förordningen och direktivet. Begreppet personuppgiftsbehandling är dock vidare än begreppet personövervakning. Med *personuppgifter* menas i förordningen varje upplysning som avser en identifierad eller identifierbar fysisk person. Med identifierbar avses att en person direkt eller indirekt kan identifieras, särskilt med hänvisning till bl.a. en identifierare som ett namn eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet. Avlidna personer omfattas inte, vilket framgår av ett skäl i ingressen till förordningen. Med *behandling* menas enligt förordningen en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring. Vidare gäller för-

ordningen endast sådan behandling av personuppgifter som helt eller delvis företas på automatiserad väg och annan behandling av personuppgifter som ingår i eller kommer att ingå i ett register. Samma begrepp och avgränsningar används i direktivet. I den brottsdatalag som ska genomföra direktivet i svensk rätt har dessa delvis formulerats något annorlunda.

Begreppet personuppgiftsbehandling omfattar exempelvis användning av kameror i parkeringshus för att avbilda registreringsskyltar. Även t.ex. bilder av fingeravtryck och liknande som genom användning av särskild teknik möjliggör identifiering av personer omfattas.

Begreppet är samtidigt snävare än begreppet personövervakning på det sättet att det inte gäller när en behandling sker av andra uppgifter än personuppgifter. Vid en pågående kameraanvändning är det däremot naturligt att den inte vid varje givet tillfälle innebär att personer fotograferas eller filmas. Denna skillnad är praktiskt ofrånkomlig och kan inte ges den betydelsen att det måste göras en åtskillnad mellan delar av en kameraanvändning där personuppgifter behandlas och delar av denna där så inte sker. En helhetssyn är den enda rimliga. Med en sådan syn kan antingen begreppet personuppgiftsbehandling eller begreppet personbevakning väljas och avse en kameraanvändning i dess helhet.

Det finns skäl som talar för att välja begreppet behandling av personuppgifter. Som slagits fast ovan gäller som utgångspunkter att kamerabevakningslagens bestämmelser bör anpassas till EU-regleringen och att lagen endast ska innehålla de bestämmelser som särskilt behövs för kamerabevakning. Det innebär att andra bestämmelser, som alltså inte ges några motsvarigheter i kamerabevakningslagen, ska gälla för sådan kamerabevakning som avses i lagen. Genom att då använda begreppet personuppgiftsbehandling i lagen kan regelsystemen haka i varandra på bästa möjliga sätt. Samtidigt kan det tydliggöras att kamerabevakning är en särskild form av personuppgiftsbehandling.

Vidare kan anföras att ett bruk av det snävare begreppet personbevakning innebär att kameraanvändning som faller utanför begreppet inte kommer att träffas av de särskilda bestämmelserna i kamerabevakningslagen som är anpassade för de förhållanden som gör sig gällande vid just kameraanvändning. I vissa situationer kan det också vara så att en kamera samtidigt avbildar en person och

samlar in andra, indirekta personuppgifter avseende denna. Som exempel kan nämnas det fallet att en kamera fotograferar ett fordon framifrån så att både personen på förarplatsen och registreringsskylten avbildas. Om förordningen eller brottsdatalagen då skulle komma att tillämpas parallellt med kamerabevakningslagen, skulle olika bestämmelser gälla i samma avseenden för en sådan samtidig kameraanvändning. En motsvarande situation kan dock uppstå redan enligt dagens lagstiftning och torde inte ha vållat några särskilda tillämpningssvårigheter. Som nämnts bör en helhetssyn på kameraanvändning i dylika situationer anläggas.

Det finns också skäl som talar för att använda begreppet personbevakning. Ett tungt vägande sådant är att en användning av begreppet personuppgiftsbehandling skulle föra alltför långt. Så snart en bild av ett föremål, eller en kroppsdel, indirekt kan kopplas samman med en fysisk person är det fråga om kamerabevakning och därmed aktuellt att tillämpa de särskilda bestämmelserna innehållande vissa krav i kamerabevakningslagen. Av de skäl som redovisats inledningsvis i detta avsnitt bör lagen inte ges ett tillämpningsområde som genomgripande skiljer sig från vad som gällt hittills. Några bärande sakliga skäl för en så omfattande utvidgning finns alltså inte. Vidare har dagens begrepp personövervakning inte vållat några särskilda svårigheter i tillämpningen. Att knyta an till sådan bevakning som mer direkt kan leda till identifiering av personer förefaller därför mest ändamålsenligt för att fånga in den typ av kameraanvändning som den särskilda lagstiftningen är påkallad för. De nu nämnda skälen måste anses väga tyngst. Begreppet *personbevakning* bör följaktligen väljas.

Slutligen bör lämpligen anges att utrustningen *används för* personbevakning i stället för som i kameraövervakningslagen att utrustningen ”kan användas för” personövervakning. En sådan utformning stämmer bäst överens med vad som gäller personuppgiftsbehandling generellt enligt EU-regleringen. Även de danska och norska bestämmelserna som också tar sikte på personövervakning och inte personuppgiftsbehandling är i dag utformade på ett liknande sätt utan att det, såvitt känt, inneburit ett snävare tillämpningsområde än kameraövervakningslagens. Någon betydelseskillnad kan inte ses och är inte heller åsyftad. Både kameraanvändning som sker i det direkta syftet att kontrollera människors förehavanden och kameraanvändning i situationer där detta direkta syfte

saknas men där människor normalt kan komma in i kamerans upptagningsområde omfattas. Om en människa endast av en tillfällighet kan hamna i en kameras blickfång, är det inte fråga om personbevakning.

Användning av viss annan utrustning

Med kameraövervakning enligt kameraövervakningslagen avses även användning av viss annan utrustning än sådan som behandlats ovan. Med kameraövervakning avses också användning av separata tekniska anordningar för avlyssning eller upptagning av ljud, vilka i samband med användning av sådan utrustning som redogjorts för ovan används för personövervakning. Detsamma gäller användning av separata tekniska anordningar för att behandla upptaget bild- och ljudmaterial.

Någon anledning att i sak ge kamerabevakningslagen ett annat tillämpningsområde i dessa hänseenden än vad kameraövervakningslagen har finns inte.

Särskilt om analog kamerabevakning

En särskild fråga är om kamerabevakningslagen kommer att omfatta analog kamerabevakning och hur detta i så fall förhåller sig till EU-regleringen.

I dag omfattas användning av såväl analog teknik som digital teknik av kameraövervakningslagen. Det tillämpningsområde som har föreslagits ovan för den nya kamerabevakningslagen är i de delar som är relevanta i detta sammanhang desamma som i den gamla lagen. Även kamerabevakningslagen kommer alltså formellt att omfatta analog kamerabevakning.

Den analoga tekniken är emellertid numera föråldrad. Det torde inte eller åtminstone ytterst sällan förekomma att analoga kameror eller därmed jämförbara analoga utrustningar används i sådana sammanhang som ska omfattas av kamerabevakningslagen. Det framstår inte heller som sannolikt att den analoga tekniken kommer att få ett uppsving. Den digitala tekniken ger långt fler möjligheter, bl.a. en mycket bättre bildkvalitet och en avsevärt lättare spridning av materialet.

Vidare är det inte självklart att EU-regleringen endast omfattar digital personuppgiftsbehandling. Förordningen och direktivet avser visserligen liksom 1995 års dataskyddsdirektiv sådan behandling av personuppgifter som helt eller delvis företas på automatiserad väg samt annan behandling av personuppgifter som ingår i eller kommer att ingå i ett register och som framgått av avsnitt 7.1.3 och 7.2.3 har i tidigare lagstiftningssammanhang gjorts den bedömningen att det direktivet inte avser analog personuppgiftsbehandling och därmed inte heller analog kameraövervakning. Motsvarande synsätt på den nya förordningen och det nya direktivet innebär att inte heller de omfattar analog kamerabevakning. Det är dock inte uppenbart att ett likhetstecken ska sättas mellan ”automatiserad” och ”digital”. Det är dessutom så att EU-regleringen träffar även delvis automatiserad personuppgiftsbehandling, vilket innebär att den gäller så snart något led i kedjan av behandlingen innefattar ett digitalt moment. Detta för att förhindra att regleringen kringgås och undvika gränsdragningsproblem. Frågan om EU-regleringen träffar analog personuppgiftsbehandling eller inte kan därför inte anses klart besvarad förrän den prövats av EU-domstolen eller på annat sätt fått ett gemensamt svar inom unionen.

Mot denna bakgrund kan det inte anses finnas någon bärande invändning mot att kamerabevakningslagen ges ett tillämpningsområde som formellt, men knappast i praktiken, omfattar även analog kamerabevakning.

Sammanfattande förslag

Sammanfattningsvis föreslås att kamerabevakningslagen ska gälla vid kamerabevakning. Med kamerabevakning ska förstås

1. att en TV-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning, utan att manövreras på platsen, används varaktigt eller regelbundet upprepat för personbevakning,
2. att en separat teknisk anordning för avlyssning eller upptagning av ljud används för personbevakning i samband med användning av sådan utrustning som avses i 1, och

3. att en separat teknisk anordning för att behandla upptaget bild- och ljudmaterial används.

Andra begrepp i lagen

Vad gäller begreppet behandling, som definieras i förordningen och i brottsdatalagen som genomför direktivet, kommer detta att användas i vissa hänseenden i kamerabevakningslagen. Begreppet får anses vara begripligt och därmed användbart även för kamerabevakning enligt kamerabevakningslagen. Det kommer dessutom att gälla för sådan kameraanvändning som inte omfattas av lagen. Begreppet bör därför inte anpassas särskilt i denna lag. Det föreslås att det i kamerabevakningslagen hänvisas till att uttryck som används i lagen och som definieras i förordningen eller i brottsdatalagen ska ha samma betydelse som i förordningen eller i den lagen.

10.3 Lagens territoriella tillämpningsområde

Förslag: Lagen ska gälla endast om

1. sådan kamerabevakning som sker med en TV-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning eller med en separat teknisk anordning för avlyssning eller upptagning av ljud sker med utrustning som finns i Sverige och den som bedriver bevakningen är etablerad i Sverige eller i tredjeland, eller
2. sådan kamerabevakning som sker med en separat teknisk anordning för att behandla upptaget bild- och ljudmaterial avser behandling av material som tagits upp vid bevakning som avses i 1 och behandlingen utförs av den som bedriver bevakningen eller för hans eller hennes räkning.

Bedömning: Några särskilda bestämmelser i kamerabevakningslagen om företrädare för den som bedriver kamerabevakning behövs inte.

Skälen för förslaget och bedömningen

Tillämpningsområdet

Vad gäller vilket territoriellt tillämpningsområde som kamerabevakningslagen ska ha har i avsnitt 7.1.6 och 7.2.3 gjorts bedömningen att detta kan avvika från förordningens i begränsande riktning och även vara snävare än vad som följer av direktivet. Detsamma gäller kamerabevakning som faller utanför EU-regleringen, vilket har behandlats i avsnitt 7.3. Vidare har det bedömts att vissa bestämmelser som knyter an till förordningens bestämmelser om tillämpningsområdet och gör dessa begripliga kan införas. Förordningens territoriella tillämpningsområde är av naturliga skäl utformat ur ett unionsperspektiv, eftersom förordningen ska gälla direkt i alla medlemsstater inom EU. I förordningen anges alltså inte något om medlemsstaternas respektive territoriella tillämpningsområde. Direktivets territoriella tillämpningsområde framgår inte heller uttryckligen men följer indirekt av bestämmelser om direktivets materiella tillämpningsområde.

Som framgått tidigare ska, om möjligt, bestämmelserna i kamerabevakningslagen utformas på ett gemensamt sätt för all kamerabevakning. Bestämmelser om lagens territoriella tillämpningsområde kan utformas på det sättet utan hinder av EU-regleringen och en sådan utformning är också lämplig med hänsyn till att det materiella tillämpningsområdet har angetts på ett samlat sätt.

Dagens kameraövervakningslag gäller vid kameraövervakning som sker med övervakningskameror som är uppsatta i Sverige, om den som bedriver övervakningen är etablerad i Sverige eller i tredjeland. Begreppet övervakningskameror omfattar inte separata tekniska anordningar för att behandla upptaget bild- och ljudmaterial. Användning av sådan utrustning utgör dock också kameraövervakning enligt lagen. I lagen anges därför att den gäller även vid behandling av material som tagits upp vid övervakning med övervakningskameror uppsatta i Sverige, om behandlingen utförs av den som bedriver övervakningen eller för hans eller hennes räkning.

Som framgått av föregående avsnitt ska begreppet uppsatt inte överföras till kamerabevakningslagen. Lagen bör ändå utformas så att den på samma sätt som kameraövervakningslagen träffar användning av kameror och annan därmed jämförbar utrustning samt separata tekniska anordningar för avlyssning eller upptagning av

ljud när utrustningen finns i Sverige. På samma sätt bör behandling av material som tagits upp vid sådan bevakning träffas, oavsett var anordningen för behandling finns, så länge behandlingen utförs av samma juridiska eller fysiska person som bedriver bevakningen med kameran etc. eller för hans eller hennes räkning. Vad gäller sådan behandling ska visserligen lagens bestämmelser, som kommer att framgå, i första hand ta sikte på det initiala skedet av behandling. Emellertid kommer det att finnas viss reglering om efterföljande behandling och som framgått ska dessutom bestämmelser i annan reglering, som bl.a. avser efterföljande behandling, gälla för kamerabevakning som avses i lagen. Med Sverige avses, i likhet med vad som gäller enligt kameraövervakningslagen, svenskt landterritorium och sjöterritorium samt luftrummet ovanför land- och sjöterritorierna.

En ytterligare fråga är om kamerabevakningslagen, liksom dagens kameraövervakningslag, endast bör gälla när den som bedriver bevakningen är etablerad i Sverige eller i ett tredjeland. Den som däremot är etablerad i ett annat EU-land än Sverige och som bedriver kamerabevakning här skulle då inte omfattas av lagens bestämmelser.

Skälet till denna begränsning i kameraövervakningslagens tillämpningsområde var att det ansågs att en reglering som även omfattade den som är etablerad i en annan EU-stat torde vara oförenlig med 1995 års dataskyddsdirektiv (prop. 2012/13:115 s. 40 f.). Av det direktivet framgick uttryckligen att lagen i den medlemsstat där den personuppgiftsansvarige var etablerad skulle tillämpas.

Motsvarande bestämmelse finns visserligen inte i förordningen, och inte heller i direktivet, men gäller ändå som en allmän princip inom unionsrätten. Principen har t.ex. fått genomslag i det s.k. tjänstedirektivet (2006/123/EG). Från principen kan dock normalt göras undantag bl.a. med hänvisning till allmän ordning och allmän säkerhet. Vad gäller det nya direktivet kan tilläggas att det avser särskilda verksamheter i en stat, t.ex. brottsbekämpning, som i regel bedrivs på den egna statens territorium, även om det finns ett internationellt polisiärt samarbete innebärande att tjänstemän från en stat under vissa förutsättningar kan agera på en annan stats territorium. Också i verksamheter som inte omfattas av unionsrätten, såsom militär verksamhet, förekommer samarbete som innebär

att utländska myndigheter från andra EU-stater kan agera på svenskt territorium.

Att nu föreskriva att kamerabevakningslagen, med vissa särskilda svenska krav för kamerabevakning, ska tillämpas på kamerabevakning som bedrivs av den som är etablerad i en annan EU-stat än Sverige kan på samma sätt som tidigare riskera att stå i strid med den angivna unionsrättsliga principen. De möjligheter till undantag från denna princip som finns kan knappast åberopas för att generellt inkludera subjekt som är etablerade i andra EU-stater i tillämpningsområdet.

I sak går det inte heller att se några konsekvenser med en ordning som undantar dem som är etablerade i andra EU-stater än Sverige som är svåra att acceptera, vare sig integritetsmässiga eller andra, såsom konkurrensmässiga. En begränsning till subjekt som är etablerade i Sverige eller tredjeland får visserligen den konsekvensen att subjekt etablerade i andra EU-länder kan använda kameror här utan att behöva följa lagens bestämmelser. Emellertid ska kamerabevakningslagen, som föreslås nedan, innehålla endast vissa materiella bestämmelser, bl.a. ett upplysningskrav och ett tillståndskrav. Vad gäller upplysningskravet ersätter det en informationsskyldighet som följer av EU-regleringen. Den som är etablerad i en annan EU-stat och använder kamera på svenskt territorium, t.ex. genom en kamerautrustad drönare i en näringsverksamhet, måste alltså följa förordningens bestämmelser om information. Vad gäller tillståndskravet kommer detta inte att gälla generellt för dem som är etablerade i Sverige utan endast för vissa sådana subjekt.

Mot denna bakgrund föreslås att kamerabevakningslagen ska gälla endast om sådan kamerabevakning som sker med en TV-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning eller med en separat teknisk anordning för avlyssning eller upptagning av ljud sker med utrustning som finns i Sverige och den som bedriver bevakningen är etablerad i Sverige eller i tredjeland. Vidare ska lagen gälla om sådan kamerabevakning som sker med en separat teknisk anordning för att behandla upptaget bild- och ljudmaterial avser behandling av material som tagits upp vid nu angiven bevakning och behandlingen utförs av den som bedriver bevakningen eller för hans eller hennes räkning.

En anknytande fråga är om det bör införas en definition av tredjeland i lagen. Förordningen innehåller inte någon sådan defini-

tion. Med tredjeland menas en stat som inte ingår i EU. Vidare faller stater som ingår i EES inte sällan också utanför begreppet tredjeland. I nuläget är det oklart huruvida förordningen kommer att gälla för EES-staterna. På direktivets område har det i brottsdatalagen föreslagits en definition av tredjeland. Den är dock utformad utifrån hur samarbetet inom EU ser ut på området för brottsbekämpning, lagföring, straffverkställighet och upprätthållande av allmän ordning och säkerhet och avviker därför från den nämnda innebörden av tredjeland. Med hänsyn till det nu redovisade är det inte lämpligt att införa en definition av tredjeland i kamerabevakningslagen, vars tillämpningsområde ska anges gemensamt för all kamerabevakning. Att en sådan inte införs bedöms inte medföra några problem för tillämpningen av lagen. Däremot ska, som föreslagits ovan, införas en mer allmän bestämmelse om att uttryck som används i lagen ska ha samma betydelse som i brottsdatalagen m.m. Till följd av den kommer definitionen i brottsdatalagen att gälla för den del av kamerabevakningen enligt kamerabevakningslagen som träffas av direktivet.

Företrädare för den som bedriver kamerabevakning

Av förordningen följer att när en personuppgiftsansvarig inte är etablerad inom EU ska denne skriftligen utse en företrädare för sig i unionen. Om den personuppgiftsansvarige utför personuppgiftsbehandling i flera medlemsstater, ska företrädaren vara etablerad i en av dessa. Detsamma gäller för ett personuppgiftsbiträde. I direktivet finns inte någon motsvarande bestämmelse.

Som framgått av avsnitt 7.1.6 överensstämmer kameraövervakningslagen inte fullt ut med förordningen i detta avseende. Enligt den lagen ska den som bedriver kameraövervakning i Sverige men är etablerad i tredjeland utse en företrädare för sig som är etablerad i Sverige. Något krav på skriftlighet ställs inte upp. Inte heller anges att en företrädare får vara etablerad i en annan EU-stat, om den som bedriver kamerabevakningen även behandlar personuppgifter avseende personer i den staten.

En bestämmelse om vad som gäller i fråga om företrädare skulle för förståelsen av kamerabevakningslagen kunna föras in i lagen. Bestämmelsen skulle dock vara begränsad till kamerabevakning

i verksamheter som omfattas av förordningen. Vidare skulle dess sakliga innehåll bli begränsat. Kraven i övrigt på en företrädare enligt förordningen är också få. Det finns en skyldighet för en företrädare, liksom för en personuppgiftsansvarig eller ett personuppgiftsbiträde, att lämna den information till tillsynsmyndigheten som myndigheten behöver för att kunna fullgöra sina uppgifter enligt förordningen. Om sådan information inte lämnas, ska en administrativ sanktionsavgift kunna påföras.

Det får därför anses tillräckligt att regleringen om utseende av företrädare framgår av förordningen. Som föreslagits ovan och behandlas mer nedan ska vidare förordningen och dataskyddslagen gälla för kamerabevakning, som omfattas av förordningens eller den lagens tillämpningsområde, i de avseenden som inte regleras i kamerabevakningslagen. Därigenom kommer även förordningens informationsskyldighet att gälla för en företrädare.

Sammanfattningsvis görs alltså bedömningen att det inte behövs några särskilda bestämmelser i kamerabevakningslagen om företrädare för den som bedriver kamerabevakning.

10.4 Undantag från lagens tillämpningsområde

Förslag: Kamerabevakningslagen ska inte gälla vid

1. kamerabevakning som en fysisk person utför som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,
2. hemlig kameraövervakning enligt 27 kap. rättegångsbalken eller lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott,
3. kamerabevakning som sker i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, och
4. kamerabevakning som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

Skälen för förslaget

Privat kamerabevakning

Av förordningen följer att den inte ska tillämpas på behandling av personuppgifter som en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll. Något motsvarande undantag finns inte i direktivet, eftersom det reglerar vissa myndigheters och andra aktörers behandling av personuppgifter för bl.a. brottsbekämpande ändamål.

Från kameraövervakningslagens tillämpningsområde undantas i dag övervakning av platser dit allmänheten inte har tillträde, om övervakningen bedrivs av en fysisk person som ett led i en verksamhet av rent privat natur. Som slagits fast i avsnitt 7.1.4 överensstämmer undantaget i kameraövervakningslagen i sak med undantaget i förordningen. Som också framgått kan ett undantag för privat kamerabevakning tas in även i kamerabevakningslagen. En sådan bestämmelse innebär visserligen en upprepning av undantaget i förordningen. Den bedöms dock vara nödvändig för att göra lagens tillämpningsområde begripligt. Det är därför fråga om ett tillåtet införlivande av förordningen i svensk lagstiftning. Bestämmelsen måste då till sin lydelse utformas som förordningens undantag.

Det föreslås följaktligen kamerabevakningslagen inte ska gälla vid kamerabevakning som en fysisk person utför som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll.

Hemlig kameraövervakning

Som redovisats i avsnitt 7.2.3 omfattar direktivet s.k. hemlig kameraövervakning. Sådan kameraövervakning är i dag undantagen från kameraövervakningslagens tillämpningsområde och regleras i 27 kap. rättegångsbalken och lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. Som vidare framgått kan kamerabevakningslagen ges ett tillämpningsområde som är snävare än vad som följer av direktivet förutsatt att annan svensk lagstiftning då gäller.

Mot denna bakgrund föreslås att kamerabevakningslagen inte ska gälla vid hemlig kameraövervakning.

Kamerabevakning i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, m.m.

I förordningen finns en bestämmelse som ger utrymme för nationell reglering om förhållandet mellan, å ena sidan, skyddet av personuppgifter och, å andra sidan, yttrande- och informationsfriheten. Enligt denna bestämmelse ska medlemsstaternas nationella lagstiftning förena rätten till skydd av personuppgifter i enlighet med förordningen med rätten till yttrande- och informationsfrihet, inbegripet personuppgiftsbehandling för journalistiska ändamål samt för akademiskt, konstnärligt eller litterärt skapande. Medlemsstaterna ska vidare föreskriva om undantag eller avvikelser från vissa i bestämmelsen angivna delar av förordningen, om det behövs för att förena rätten till skydd för personuppgifter med yttrande- och informationsfriheten. Kommissionen ska underrättas om sådana undantagsbestämmelser. I ingressen till förordningen finns en hänvisning till rätten till yttrande- och informationsfrihet i EU:s stadga om de grundläggande rättigheterna och anges också att medlemsstaterna bör anta lagstiftningsåtgärder som fastställer de olika undantag som behövs för att balansera de två rättigheterna samt att det bör göras en bred tolkning av vad som innefattas i yttrandefriheten.

En liknande bestämmelse fanns i 1995 års dataskyddsdirektiv. När direktivet genomfördes i svensk rätt genom personuppgiftslagen (PUL) gjordes bedömningen att bestämmelsen tillät ett hänsynstagande till bl.a. konstitutionella traditioner och att tryckfrihetsförordningen (TF) och yttrandefrihetsgrundlagen (YGL) inte behövde ändras (prop. 1997/98:44 s. 50 f.). Vidare ansågs att direktivet inte lade några hinder i vägen för ett generellt undantag från PUL:s bestämmelser. I PUL togs det därför in en upplysningsbestämmelse om att lagens bestämmelser inte skulle tillämpas i den utsträckning det skulle strida mot TF och YGL. Bestämmelsen har inte ifrågasatts av kommissionen sedan införandet och inte heller varit föremål för domstolsprövning. I PUL finns därutöver en bestämmelse om att ett flertal av lagens bestämmelser inte ska tillämpas vid personuppgiftsbehandling som inte omfattas av TF eller YGL

men som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande.

Bestämmelsen i den nya förordningen innebär på samma sätt, och ännu tydligare genom bl.a. det angivna skälet i ingressen, att EU-regleringen på dataskyddsområdet inte inkräktar på området för TF och YGL.

Dataskyddsutredningen har föreslagit att det i dataskyddslagen tas in bestämmelser som motsvarar de bestämmelser som finns i PUL. Utredningen har alltså föreslagit dels en upplysningsbestämmelse som tydliggör att bestämmelserna i dataskyddslagen och i förordningen inte ska tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i TF eller YGL, dels ett undantag för sådan behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande; förordningens bestämmelser om syfte, tillämpningsområde och definitioner samt bestämmelser om säkerhet för personuppgifter, samarbete med tillsynsmyndigheten, rättsmedel, ansvar och sanktioner ska dock tillämpas.

I kameraövervakningslagen finns inte någon motsvarighet till den beskrivna regleringen i PUL. Frågan om förhållandet mellan bestämmelser om kamerabevakning och bestämmelserna i TF och YGL har inte diskuterats närmare i lagstiftningsärenden på kamerabevakningsområdet och viss osäkerhet råder i frågan. Under senare tid har det uppkommit frågor om de traditionella mediernas användning av kameror på drönare eller kameror monterade på visst sätt för nyhetsrapportering eller under sportevenemang omfattas av lagens bestämmelser, t.ex. om tillståndsplikt. Motsvarande gäller kameraanvändning för journalistiska ändamål eller konstnärligt eller litterärt skapande på området utanför TF och YGL.

I äldre förarbeten finns uttalanden som tyder på att kameraanvändning i sådana verksamheter som avses i TF och YGL kan omfattas av tillståndsplikten förutsatt att det är fråga om kameraanvändning som faller in under lagens tillämpningsområde (se t.ex. prop. 1975/76:194 s. 22). Samtidigt torde det inte ha förekommit att tillstånd sökts i dessa fall och inte heller torde tillsyn bedrivas för att undersöka om det sker kameraövervakning som omfattas av kameraövervakningslagen och hur denna i så fall går till.

Det är inte tillfredsställande att frågan om förhållandet till TF och YGL är oklar på kamerabevakningsområdet. Detsamma kan

sägas vad gäller kameraanvändning för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande på området utanför grundlagarna.

Eftersom kamerabevakning utgör en form av personuppgiftsbehandling, görs samma principiella bedömning på kamerabevakningsområdet som gjorts i samband med införandet av PUL och som nu gjorts av Dataskyddsutredningen. Vidare är det självklart att TF och YGL ska ges företräde i en eventuell konfliktsituation vid tillämpningen av kamerabevakningslagen. När TF och YGL gäller är utgångspunkten att grundlagarnas censurförbud, etableringsfrihet, meddelarskydd, ensamansvar, särskilda brottskatalog och särskilda rättegångsordning gäller. Ett grundläggande drag hos regleringen är att innehållet i eller syftet med ett yttrande normalt inte avgör grundlagarnas tillämplighet. Grundlagsskyddet utgår i stället från vilken medieteknik som används. Innebörden av att ett medium har grundlagsskydd är att PUL:s och framöver förordningens och dataskyddslagens bestämmelser i praktiken inte blir tillämpliga på personuppgiftsbehandling som sker inom ramen för den verksamheten. Detsamma gäller vissa av bestämmelserna när det är fråga om journalistiska ändamål etc. på området utanför grundlagarna.

TF och YGL hindrar dock inte att det i vanlig lag finns bestämmelser som reglerar själva sättet på vilket ett anskaffande av information sker, t.ex. bestämmelser om straffansvar eller om krav på tillstånd, så länge regleringen inte tar sikte på innehållet som sådant, inte ens delvis.

Det kan hävdas att bestämmelser om kamerabevakning avser endast sättet för att anskaffa information. Å andra sidan finns ett nära samband mellan själva insamlingen av bilder och ljud och den information som utgörs av bilderna och ljudet. Inte sällan sker publiceringen av bilder och ljud i grundlagsskyddade medier i princip i samma stund som insamlingen sker.

Det är tveksamt om de materiella bestämmelser som ska finnas i kamerabevakningslagen – bl.a. ett upplysningskrav och ett tillståndskrav – överhuvudtaget kan tillämpas i fråga om kamerabevakning i verksamheter som omfattas av TF eller YGL. Under alla förhållanden framstår det inte som lämpligt med hänsyn till den beskrivna nära kopplingen. Några särskilda integritetsrisker med att kamerabevakningslagens bestämmelser inte ska gälla på detta område kan

inte heller förutses. För övrigt ska tillståndskravet, som kommer att framgå, inte i första hand ta sikte på kamerabevakning av det nu diskuterade slaget.

Det föreslås därför att ett uttryckligt undantag från kamerabevakningslagen görs för kamerabevakning som sker i en verksamhet som omfattas av TF eller YGL. Detsamma föreslås för kamerabevakning som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande. Av dataskyddslagen framgår vad som gäller i fråga om förordningens och den lagens bestämmelser för sådan kamerabevakning.

11 Ett tillståndskrav för myndigheter och vissa andra

11.1 Inget generellt tillståndskrav

Bedömning: Kamerabevakningslagen ska inte innehålla något generellt krav på tillstånd för kamerabevakning och inte heller något krav på anmälan som motsvarar dagens tillstånds- respektive anmälningsplikt i kameraövervakningslagen.

Skälen för bedömningen: I avsnitt 7 har analyserats om dataskyddsförordningen och dataskyddsdirektivet ger utrymme för svenska bestämmelser om krav på tillstånd eller liknande för att kamerabevakning ska få ske. Där har också behandlats vad som gäller för kamerabevakning som inte omfattas av EU-regleringen. Den kamerabevakning som bedrivs av Polismyndigheten, Tullverket och Kustbevakningen samt vissa andra subjekt sker ofta i sådana syften som gör att det är direktivets krav som gäller för kamerabevakningen. Förordningens bestämmelser omfattar kamerabevakning som bedrivs av de flesta övriga statliga myndigheter, av kommuner eller av enskilda juridiska eller fysiska personer. Utanför direktivet och förordningen faller normalt kamerabevakning som bedrivs av främst Säkerhetspolisen och myndigheter inom försvaret. Dataskyddsutredningen har dock föreslagit att förordningen och den generella lag som ska komplettera förordningen, dataskyddslagen, ska tillämpas vid personuppgiftsbehandling även i en verksamhet som inte omfattas av unionsrätten och i verksamhet som avser den gemensamma utrikes- och säkerhetspolitiken. I sektorsspecifika författningar som avser verksamhet utanför förordningens egentliga tillämpningsområde kan det komma att föreskrivas undantag från denna bestämmelse. Exempelvis kan Utredningen om 2016 års dataskyddsdirektiv

komma att göra det såvitt gäller Säkerhetspolisens verksamhet. I det fallet kommer i stora delar den generella lag som genomför direktivet, brottsdatalagen, att gälla. De slutsatser som har dragits i avsnitt 7 är följande.

För kamerabevakning som utgör personuppgiftsbehandling som omfattas av förordningen är det möjligt att i den nya kamerabevakningslagen införa ett krav på samråd och förhandstillstånd för sådan kamerabevakning som sker för att utföra en uppgift av allmänt intresse, inklusive som sker som ett led i myndighetsutövning. Ett sådant krav är däremot inte möjligt att ställa upp för kamerabevakning i annan verksamhet. För anställningsförhållanden finns ett särskilt utrymme för eventuella svenska regler. Detta utrymme behandlas för sig i avsnitt 13. Vad gäller kamerabevakning som utgör personuppgiftsbehandling som faller in under direktivets tillämpningsområde är det möjligt att ställa upp ett krav på tillstånd i kamerabevakningslagen. Det gäller generellt för kamerabevakning på det område som avses i direktivet. Slutligen kan ett tillstånds- eller anmälningskrav ställas upp för sådan kamerabevakning som inte omfattas av förordningens och direktivets tillämpningsområden.

Frågan är då om det kan eller bör ställas upp ett mer generellt krav på tillstånd eller liknande för att kamerabevakning ska få ske.

Som slagits fast i avsnitt 9.2.2 ska en utgångspunkt för kamerabevakningslagen vara att den ska ge ökade möjligheter till kamerabevakning. Teknikutvecklingen och samhällsutvecklingen har inneburit att det finns en mängd områden inom vilka kamerabevakning kan vara av stort värde samtidigt som det motstående intresset för enskilda att inte kamerabevakas kan vara begränsat. Denna utveckling kan väntas fortsätta. Det är angeläget att lagstiftningen inte förhindrar eller försvårar användning av kameror i situationer där en kameraanvändning kan tjäna ett berättigat syfte som väger tyngre än det intresse av integritetsskydd som kan finnas i det enskilda fallet. Redan detta innebär att det finns skäl att ifrågasätta om det är motiverat med ett allmänt krav på tillstånd.

Vidare måste kamerabevakningslagen vara förenlig med den nya EU-regleringen. Det innebär att det inte längre är möjligt att upprätthålla en generell tillståndsplikt för sådan kamerabevakning som omfattas av förordningen. Förordningen tillåter endast krav på tillstånd eller liknande i vissa fall. För kamerabevakning som träffas av

direktivet kan ett generellt sådant krav gälla. Detsamma gäller för övrig kamerabevakning.

Detta innebär att ett eventuellt svenskt tillståndskrav eller annat liknande krav för att kamerabevakning ska få ske kan ställas upp i första hand för statliga och kommunala myndigheter. Ett sådant krav är i och för sig möjligt även för kamerabevakning i vissa verksamheter som drivs av privaträttsliga subjekt. Däremot är ett krav uteslutet för en stor del av den kamerabevakning som i dag omfattas av tillståndsplikt eller anmälningsskyldighet.

Till detta kommer den ytterligare utgångspunkt som slagits fast tidigare att kamerabevakningslagen endast bör avvika från vad som annars gäller för personuppgiftsbehandling i den utsträckning avvikande bestämmelser kan motiveras av principiella skäl och ett påtagligt praktiskt behov. Eftersom ett krav på tillstånd eller liknande inte kommer att gälla för personuppgiftsbehandling generellt sett, bör ett sådant krav för kamerabevakning alltså bara gälla om det finns starka skäl för det. För sådan kamerabevakning som inte tidigare har omfattats av tillstånds- eller anmälningsplikt bör allmänt sett inte nu införas något sådant krav. Endast om det framkommit att det numera finns ett starkt behov av ett krav av det slaget bör denna utgångspunkt frångås.

Dessutom är det så, vilket har redovisats närmare i avsnitt 8, att i den mån ett krav på tillstånd eller liknande inte gäller för kamerabevakning kommer annan reglering att gälla för bevakningen. Det kommer att finnas ett antal olika bestämmelser om personuppgiftsbehandling som även träffar kamerabevakning och sätter gränser för när och hur bevakning får ske och hur material från bevakningen får hanteras. Både förordningen och direktivet kräver dessutom en omfattande och effektiv tillsynsverksamhet.

Sammantaget innebär det nu redovisade att det i kamerabevakningslagen inte är möjligt eller lämpligt med ett generellt krav på tillstånd för kamerabevakning eller ett krav på anmälan som motsvarar dagens tillstånds- respektive anmälningsplikt i kameraövervakningslagen. Den nya lagen ska alltså inte innehålla några sådana krav.

Genom att slopa dagens generella krav på tillstånd och krav på anmälan blir kamerabevakning i många verksamheter framöver tillstånds- och anmälningsfri. Därmed kan möjligheterna att kamerabevaka i dessa verksamheter öka. Även om andra bestämmelser

kommer att gälla, kan det förutses att den svenska tillsynsmyndigheten på området, liksom svenska domstolar och ytterst EU-domstolen, kommer att ha en mer generös syn på utrymmet för kamerabevakning än vad som gäller enligt svensk rätt i dag. Rättsläget är helt nytt med den nya förordningen, som ska tillämpas direkt i Sverige och övriga EU-medlemsstater, och det nya direktivet. Den nya EU-regleringen skiljer sig i olika delar från den unionsrättsliga reglering som hittills gällt på området och legat till grund för dagens svenska lagstiftning. Exempelvis kan fler berättigade ändamål åberopas för kamerabevakning enligt den nya regleringen än vad som är möjligt enligt kameraövervakningslagen i dag. I dessa delar kommer tillsynsmyndigheten och domstolarna inte att vara bundna av tidigare svensk praxis på kamerabevakningsområdet.

11.2 Ett tillståndskrav eller någon annan form av krav?

Bedömning: Ett eventuellt krav i kamerabevakningslagen för att kamerabevakning ska få bedrivas bör utgöras av ett krav på tillstånd. Ett sådant krav bör inträda när bevakning ska ske. Ett tillståndskrav kan förenas med ökade möjligheter till kamerabevakning.

Skälen för bedömningen

Ett tillståndskrav

Innan det diskuteras om ett tillståndskrav eller liknande ska införas i kamerabevakningslagen för att insamling och annan behandling av bild och ljud ska få ske kan det vara motiverat med en övergripande diskussion om hur ett krav kan utformas. Ett sådant krav bör, i enlighet med vad slagits fast tidigare, utformas på ett gemensamt sätt så att det kan gälla oavsett om det är fråga om kamerabevakning som omfattas av förordningen, kamerabevakning som avses i direktivet eller kamerabevakning som faller utanför EU-regleringen.

Som framgått lämnar förordningen utrymme för ett nationellt krav på samråd med och förhandstillstånd av tillsynsmyndigheten.

Denna möjlighet måste rimligen förstås så att det i nationell rätt kan föreskrivas *ett samlat förfarande* och inte måste föreskrivas både en samrådsskyldighet och ett tillståndskrav separerade från varandra. Exempelvis kan ett förfarande med ansökan om tillstånd och en prövning av denna föreskrivas.

Däremot kan förordningen knappast anses lämna utrymme för en ren anmälningsskyldighet. Enligt förordningen ska det många gånger göras en konsekvensbedömning och ibland också ske ett samråd med tillsynsmyndigheten. Ett tillkommande nationellt krav ska enligt förordningen avse *samråd och tillstånd*. Ett svenskt krav som enbart skulle bestå i en skyldighet att anmäla skulle vara mindre långtgående.

Vad gäller direktivet lämnar detta utrymme för starkare skyddsåtgärder i nationell rätt än vad som följer av kraven i direktivet. Detta kan vid ett första påseende tyckas öppna för olika alternativ, såsom ett tillståndskrav eller en anmälningsplikt. Det är dock tveksamt om en ren anmälningsskyldighet är möjlig enligt direktivet. Under alla förhållanden är det rimligt att utforma ett krav på samma sätt som för förordningsfallen, särskilt som vissa myndigheter och andra subjekt kan bedriva såväl kamerabevakning i syften som avses i direktivet som kamerabevakning som omfattas av förordningen. Att ha olika svenska krav skulle komplicera lagstiftningen och leda till svårigheter i tillämpningen.

För kamerabevakning som faller utanför förordningen och direktivet är det i och för sig tänkbart med antingen enbart ett krav på anmälan eller t.ex. ett tillståndskrav. Av de skäl som angetts ovan bör dock ett eventuellt krav utformas enhetligt.

En ren anmälningsskyldighet för kamerabevakning är följaktligen inte ett alternativ som kan eller bör väljas. Valet står därför mellan ett krav på tillstånd och ett krav på samråd. Ett samrådskrav innebär i praktiken också ett anmälningskrav men är mer långtgående än enbart en skyldighet att anmäla. Ett samrådskrav är samtidigt mindre långtgående än ett tillståndskrav och går därmed inte utöver vad förordningen lämnar utrymme för.

Det finns flera skäl som talar för att ett tillståndskrav bör väljas. Ett tillståndsförfarande är det som tidigare gällt som huvudregel för de myndigheter och andra som fortsatt kan omfattas av ett sådant krav enligt förordningen och direktivet. Detsamma gäller för de subjekt som faller utanför EU-regleringen.

Vidare kan ett tillståndskrav, som framgår strax nedan, säkerställa att möjligheterna till kamerabevakning kan öka, bl.a. i brottsbekämpande syften.

Slutligen torde ett tillståndsförfarande vara enklare både för dem som omfattas av förfarandet och för dem som ska tillämpa detta. Ett sådant förfarande innebär att tillsynsmyndigheten, eller domstol efter överklagande, på förhand gör en ingående prövning av om kamerabevakning i ett enskilt fall ska få ske. När ett tillstånd har meddelats kan tillståndshavaren inrätta sig efter detta. Ett samrådsförfarande skulle behöva kopplas samman med bestämmelser om hur samrådet ska gå till och vad tillsynsmyndigheten kan göra om kamerabevakningen enligt myndigheten inte sker i enlighet med gällande bestämmelser.

Mot denna bakgrund görs bedömningen att ett eventuellt krav i kamerabevakningslagen för att kamerabevakning ska få bedrivas bör utgöras av ett krav på tillstånd.

Avslutningsvis ska framhållas att ett grundläggande krav för att kamerabevakning ska få ske är att bevakningen är laglig enligt förordningen och dataskyddslagen eller enligt brottsdatalagen, som genomför direktivet. Ett krav på tillstånd gäller därutöver och förutsätter någon form av intresseavvägning. Detta har närmare behandlats i avsnitt 7.1.7 och 7.1.8 respektive 7.2.4.

Tidpunkten för när i tiden ett tillståndskrav bör inträda

I kameraövervakningslagen är tillståndsplikten utformad så att det krävs tillstånd för att en kamera *ska få vara uppsatt* så att den kan riktas mot en plats dit allmänheten har tillträde. För kontroll av tillståndspliktens efterlevnad har det ansetts vara av betydelse att kunna ingripa så snart en kamera är uppsatt (prop. 1975/76:194 s. 25).

Av avsnitt 10.2 har framgått att begreppet uppsatt inte ska behållas i kamerabevakningslagen. Den nya lagens tillämpningsområde knyter i stället an till användningen av kamerautrustning och behandlingen av det material som tagits upp med denna. Det är det som kan innebära risker för enskildas integritet. En tillståndsprövning är också inriktad på dessa frågor. Ett tillståndskrav som knyts till användningen innebär i praktiken att tillstånd måste sökas innan kamerabevakning får ske. Dessutom kan ett eventuellt tillstånds-

krav endast träffa vissa subjekt, som är sådana att behovet av att kravet inträder lika tidigt som i dag måste anses vara litet. Visserligen kan det inte helt uteslutas att ett sådant subjekt kan komma att använda sig av kamerabevakning utan att först ha sökt och beviljats tillstånd. Att denna situation uppkommer kan motverkas genom goda kunskaper om hur lagstiftningen ser ut. Ett tillståndskrav som i stället inträder redan tidigare, t.ex. när utrustningen placeras på ett visst sätt, hindrar inte i sig missförstånd om lagstiftningens innehåll. Det kan vidare antas att ett sådant subjekt, när det genom tillsyn eller på annat sätt uppmärksammar att det krävs tillstånd till kamerabevakning, inte osant skulle påstå att utrustningen inte är avsedd att användas. Ett sådant subjekt torde av resursskäl och andra skäl inte heller införskaffa och montera utrustning som aldrig är tänkt att komma till användning.

Mot denna bakgrund görs bedömningen att ett eventuellt krav på tillstånd i kamerabevakningslagen bör inträda när bevakning ska ske.

Ett tillståndskrav kan förenas med ökade möjligheter till kamerabevakning

En sista fråga är om och hur ett tillståndskrav kan förenas med den i tidigare avsnitt fastslagna strävan att möjligheterna till kamerabevakning ska öka.

Ett tillståndsförfarande innebär en prövning enligt vissa i svensk lag på förhand givna kriterier som är särskilt anpassade för de behov och de integritetsaspekter som gör sig gällande just på kamerabevakningsområdet. Kriterierna ska vara tydliga och enkla att tillämpa. Sådana kriterier kan främja att prövningen blir förutsebar och enhetlig, att tillstånd beviljas i en mer generös omfattning än i dag i motsvarande situationer och att den som har fått tillstånd till kamerabevakning kan inrätta sig efter det. Tillsynsmyndighetens beslut i en sådan fråga ska också kunna överklagas till domstol.

Om i stället de mer generella bestämmelserna om konsekvensbedömning av personuppgiftsbehandlingar, samråd med tillsynsmyndigheten och åtgärder av tillsynsmyndigheten skulle gälla, finns det en risk för att rättsläget vad gäller kamerabevakning kommer att vara osäkert under en längre tid i fråga om sådana verksamheter som ett tillståndskrav annars kan avse. Det finns också en risk för att rättspraxis inte utvecklas på ett sätt som säkerställer att kamera-

bevakning kan användas i dessa verksamheter i situationer där sådan bevakning – enligt vad som utvecklats tidigare – måste anses behövlig. Det gäller även i sammanhang där den enskildes intresse av att inte bli bevakad i och för sig kan väga tungt.

Följaktligen kan ett tillståndskrav mycket väl förenas med ökade möjligheter till kamerabevakning.

11.3 Ett tillståndskrav för kamerabevakning som avses i direktivet

Förslag: Ett tillståndskrav ska gälla för kamerabevakning som avses i direktivet, nämligen kamerabevakning som ska bedrivas av en myndighet som har i uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet eller av en annan aktör som utövar myndighet för något av dessa syften förutsatt att myndighetens eller aktörens kamerabevakning sker i ett sådant syfte.

Skälen för förslaget

Ett tillståndskrav ska gälla

Som framgått är det möjligt att i kamerabevakningslagen ställa upp ett krav på tillstånd för att kamerabevakning som utgör personuppgiftsbehandling som avses i direktivet ska få ske. Det gäller generellt på det område som faller in under direktivet. Direktivets tillämpningsområde bestäms dels av om det är en s.k. behörig myndighet som utför en personuppgiftsbehandling, dels av vilket syftet är med behandlingen. Utredningen om 2016 års dataskyddsdirektiv har föreslagit att brottsdatalagen ska gälla för behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Vidare har utredningen föreslagit att behörig myndighet ska definieras som en myndighet som har i uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda

eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet eller en annan aktör som utövar myndighet för något av dessa syften. Utredningen har utförligt beskrivit hur direktivets tillämpningsområde bör förstås i förhållande till förordningen och till det område som faller utanför direktivet och förordningen.

Detta innebär exempelvis att Polismyndighetens kamerabevakning för automatisk hastighetsövervakning eller för att förebygga, förhindra, upptäcka eller utreda brott träffas av direktivet och brottsdatalagen. Det sistnämnda gäller även för t.ex. Tullverket och Kustbevakningen. Detsamma gäller den som har en författningsreglerad skyldighet att biträda sådana brottsbekämpande, lagförande eller verkställande myndigheter med särskild kompetens eller särskilda resurser. Det gäller även den som av en myndighet som utför stödverksamhet har kontrakterats att för myndighetens räkning utföra sådana uppgifter. Direktivet träffar däremot inte t.ex. kamerabevakning i samband med kontrollverksamhet som utförs av Polismyndigheten, Tullverket eller Kustbevakningen. Exempel på sådan verksamhet är gränskontroll, tullkontroll och utlänningskontroll eller skattekontroll. Inte heller träffar direktivet kamerabevakning som Säkerhetspolisen bedriver i sin verksamhet som avser nationell säkerhet. Till denna verksamhet räknas bl.a. uppgiften att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet och terroristbrott och att utreda och beivra sådana brott. Om Säkerhetspolisen däremot bistår vid polisverksamhet som leds av Polismyndigheten, gäller direktivet. Detsamma gäller om Försvarsmakten ger stöd åt Polismyndigheten vid terrorismbekämpning.

För att ett tillståndskrav ska vara motiverat för kamerabevakning som ska bedrivas av de myndigheter och andra subjekt i de syften som omfattas av direktivet bör det finnas ett påtagligt praktiskt behov av och principiella skäl för ett sådant. Det finns flera skäl som talar för ett krav på tillstånd i dessa fall.

Inledningsvis kan konstateras att ett krav på tillstånd till kamerabevakning har funnits länge i svensk rätt, även om kravet efter hand har luckrats upp i vissa avseenden. Kravet gäller platser dit allmänheten har tillträde. Skälen till att ett sådant krav ursprungligen ställdes upp var att den tekniska utvecklingen hade inneburit att användning av kamerautrustning för övervakning blivit allt vanligare

och att det knappast fanns något skydd mot att utrustningen användes för personövervakning på ett sätt som kränkte enskildas personliga integritet (prop. 1975/76:194 s. 14 ff.). Det som då pekades ut var bl.a. övervakning inom sjukvården och kriminalvården samt polisbevakning på centralstationen och tunnelbanan i Stockholm. Vidare uttalades att sådan övervakning gjorde det möjligt att samla in en stor mängd information om enskilda och kunde medföra en särskild risk från integritetssynpunkt om medborgarna mer allmänt blev föremål för denna.

Tillståndskravet gäller i dag för kameraövervakning i en mängd olika verksamheter på det område som faller in under direktivet liksom på det område som faller utanför och antingen omfattas av förordningen eller inte alls träffas av EU-regleringen. Det gäller oavsett om det är en myndighet eller någon annan som bedriver övervakningen. Den distinktion mellan olika platser som görs i dag och har betydelse för om tillståndskravet gäller torde vara av mindre relevans för kamerabevakning som träffas av direktivet, eftersom sådan oftast torde förekomma på platser dit allmänheten har tillträde. Distinktionen har dock ett visst sakligt berättigande på direktivets område och är även lämplig av tydlighetsskäl, om ett tillståndskrav fortsatt ska gälla. På förordningens område kan vidare distinktionen ha en stor praktisk betydelse, vilket framgår nedan.

Ordningen med ett tillståndskrav för kamerabevakning i de verksamheter och syften som avses i direktivet är alltså etablerad. Den är avsedd att garantera ett starkt skydd mot bevakning av enskilda och samtidigt ge goda möjligheter till kamerabevakning. Förutom det som slagits fast i tidigare avsnitt om att dagens tillståndsförfarande i vissa avseenden innebär alltför begränsade möjligheter till tillstånd har det inte i den kartläggning av dagens lagstiftning som gjorts eller i övrigt framkommit att det finns några grundläggande problem med ett sådant förfarande. De skäl som ursprungligen anförts för tillståndskravet gör sig följaktligen fortsatt gällande, även om möjligheterna till kamerabevakning bör öka framöver, inte minst för syftet att motverka brott.

Kamerabevakning förekommer vidare i praktiken i relativt stor utsträckning i de verksamheter och syften som avses i direktivet. Det gäller t.ex. i Polismyndighetens verksamhet för att förebygga, förhindra, upptäcka eller utreda brott. Bevakning i dessa verksam-

heter är dessutom direkt inriktad på att kontrollera människors förehavanden.

Den tillsyn som länsstyrelserna och Datainspektionen bedriver på detta område visar att det har förekommit brister i hur myndigheterna använder kameror. Som exempel kan nämnas en tillsyn som samtliga länsstyrelser utom två gjorde under 2015 avseende Polismyndigheten och domstolar. Sammanlagt genomfördes 132 inspektioner på polisstationer och i domstolar. Antalet anmärkningar uppgick till 52 och en anmärkning kunde innehålla flera upptäckta felaktigheter. De vanligaste anmärkningarna var att det helt saknades tillstånd till kameraövervakning, att kamerornas upptagningsområde var större än vad tillståndet medgav och att skyltningen om övervakningen var bristfällig. Andra vanliga anmärkningar avsåg bl.a. otillåten bildinspelning, fler kameror än vad tillståndet medgav och övervakning på tider som inte omfattades av tillståndet. Centrala myndigheter i rättsväsendet har alltså så sent som 2015 brustit i sin tillämpning av regelverket i en omfattning och i avseenden som inte kan betecknas som endast marginella. Ett krav på tillstånd skulle följaktligen fylla ett praktiskt behov.

Vidare bör av principiella skäl kamerabevakning som bedrivs i de syften och av de myndigheter och andra som avses i direktivet kringgärdas av begränsande bestämmelser för att säkerställa att sådan bevakning sker på ett balanserat sätt. Enskilda är enligt Europakonventionen och regeringsformen garanterade ett starkt skydd mot intrång i den personliga integriteten från det allmännas sida. Kamerabevakning innebär ett sådant intrång och är dessutom som utgångspunkt en särskilt integritetskänslig åtgärd. De verksamheter som träffas av direktivet är vidare speciella på det sättet att de allmänt sett kännetecknas av att de ger många och stora möjligheter att ingripa mot eller annars utöva kontroll över enskilda. Användning av olika åtgärder i dessa verksamheter, särskilt tvångsmedel, regleras på ett restriktivt sätt. Ett närliggande exempel är hemlig kameraövervakning, som förutsätter att en domstol har gett till tillstånd till övervakningen. Även i fråga om kamerabevakning måste det visserligen ges goda och – som behandlas närmare nedan – ökade möjligheter till bevakning. Det gäller främst platser som stadskärnor, torg eller andra utomhusmiljöer där många människor rör sig t.ex. som boende eller arbetande i området eller som besökare av restauranger eller nöjesställen. På sådana platser kan brottsbekäm-

pande myndigheter ha ett berättigat intresse av att kamerabevaka. I dessa situationer gör sig emellertid samtidigt behovet av integritetsskydd starkt gällande. Det gäller inte minst eftersom sådan kamerabevakning som träffas av direktivet direkt syftar till att kontrollera människorna på platsen. Det är därför angeläget att kamerabevakning endast får ske efter en grundlig prövning av att behovet av sådan bevakning måste ges företräde.

Utan ett tillståndskrav skulle tillsynsmyndigheten återkommande behöva tillsyna kamerabevakning inom detta område för att undersöka vilken kamerabevakning som bedrivs, varför och på vilket sätt, eftersom kamerabevakning förekommer i förhållandevis stor omfattning på området. Ett krav på att den som vill bedriva kamerabevakning före bevakningen måste söka tillstånd kan ge tillsynsmyndigheten en bättre överblick över och kontroll av kamerabevakning på området.

Det nu redovisade talar med styrka för att kamerabevakningslagen ska innehålla ett krav på tillstånd för att sådan kamerabevakning som träffas av direktivet ska få ske. För detta talar också att utredningens uppdrag har varit att behålla huvuddragen i kameraövervakningslagen och inte genomgripande förändra de grundläggande kraven i lagen, t.ex. genom att helt undanta vissa myndigheter från kravet på tillstånd. Det föreslås följaktligen att ett tillståndskrav ska gälla för kamerabevakning som avses i direktivet, nämligen kamerabevakning som ska bedrivas av en myndighet som har i uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet eller av en annan aktör som utövar myndighet för något av dessa syften förutsatt att myndighetens eller aktörens kamerabevakning sker i ett sådant syfte. Nedan föreslås dock vissa undantag från tillståndskravet.

Exempel på kamerabevakning som ska omfattas av tillståndskravet

Kravet på tillstånd ska gälla för de myndigheter och andra subjekt som träffas av direktivet när de ska bedriva kamerabevakning som avses i kamerabevakningslagen i sådana syften som anges i direktivet. Annan användning av kameror som faller in under direktivets tillämpningsområde omfattas inte.

Tillståndskravet ska exempelvis omfatta Polismyndighetens kamerabevakning av ett torg i den mån bevakningen inte är undantagen från kravet i enlighet med vad som föreslås nedan. Även t.ex. kameror i polisbilar ska omfattas förutsatt att de inte manövreras på platsen.

11.4 Ett tillståndskrav för kamerabevakning som faller utanför direktivet och förordningen

Förslag: Ett tillståndskrav ska gälla för kamerabevakning som ska bedrivas av en myndighet eller en annan aktör i en verksamhet som faller utanför direktivet och förordningen.

Skälen för förslaget: Förordningen och direktivet träffar inte personuppgiftsbehandling som utförs som ett led i en verksamhet som inte omfattas av unionsrätten, såsom verksamhet rörande nationell säkerhet, eller i verksamhet som omfattas av EU:s gemensamma utrikes- och säkerhetspolitik.

Det förekommer kamerabevakning i verksamheter som faller utanför EU-regleringen. Det gäller t.ex. normalt kamerabevakning som bedrivs av Säkerhetspolisen i verksamhet som avser nationell säkerhet eller av myndigheter inom försvaret. De skäl som anförts ovan för ett krav på tillstånd när de myndigheter och andra subjekt som avses i direktivet bedriver kamerabevakning i syften som faller in under direktivet gör sig i allt väsentligt gällande även för kamerabevakning i de nu nämnda fallen. Det föreslås därför att tillståndskravet ska gälla även för kamerabevakning som ska bedrivas av en myndighet eller en annan aktör i en verksamhet som faller utanför direktivet och förordningen. Vissa undantag från kravet föreslås dock nedan.

11.5 Ett tillståndskrav för viss kamerabevakning som omfattas av förordningen

Förslag: Ett tillståndskrav ska gälla för viss kamerabevakning som omfattas av förordningen. Kravet ska omfatta kamerabevakning som ska bedrivas av en myndighet. Kravet ska också omfatta kamerabevakning som ska bedrivas av en annan juridisk person eller en fysisk person vid utförande av en uppgift av allmänt intresse som följer av lag eller annan författning, kollektivavtal eller beslut som har meddelats med stöd av lag eller annan författning.

Bedömning: Tillståndskravet ska inte gälla annan kamerabevakning som ska bedrivas av juridiska personer eller fysiska personer. Inte heller ska sådan kamerabevakning omfattas av något anmälningskrav.

Skälen för förslaget och bedömningen

Utrymmet för ett tillståndskrav

Som konstaterats tidigare är det möjligt enligt förordningen att i kamerabevakningslagen ställa upp ett tillståndskrav för kamerabevakning som omfattas av förordningens tillämpningsområde och som sker för att utföra en uppgift av allmänt intresse. Det är uppgiften som sådan som ska vara av allmänt intresse, inte kamerabevakningen i sig. I begreppet uppgift av allmänt intresse måste, som tidigare slagits fast, inkluderas kamerabevakning som sker som ett led i myndighetsutövning. Myndighetsutövning nämns visserligen inte uttryckligen i den bestämmelse i förordningen som ger utrymme för ett tillståndskrav. Bestämmelsen knyter emellertid an till andra förordningsbestämmelser som räknar upp såväl personuppgiftsbehandling som sker som ett led i myndighetsutövning som personuppgiftsbehandling som sker för att utföra en uppgift av allmänt intresse. Förordningen innehåller inte någon begränsning som avser att myndighetsutövningen eller uppgiften av allmänt intresse måste utföras av en myndighet. Inte heller krävs att myndighetsutövningen eller uppgiften utförs till följd av ett åliggande.

Kamerabevakning som sker utan samband med myndighetsutövning eller andra uppgifter av allmänt intresse kan följaktligen inte omfattas av ett tillståndskrav.

Vad avses med en uppgift av allmänt intresse?

Frågan är då vad som närmare avses med en uppgift av allmänt intresse, inklusive myndighetsutövning.

Vad först gäller myndighetsutövning är det ett unionsrättsligt begrepp. Det innebär att begreppet inte kan tolkas fritt av varje enskild medlemsstat i unionen. Som rättsläget ser ut i dag finns det dock inte något som hindrar att ett svenskt synsätt anläggs på innebörden av begreppet. Enligt svensk rätt karakteriseras myndighetsutövning av beslut eller andra ensidiga åtgärder som ytterst är ett uttryck för samhällets maktbefogenheter i förhållande till medborgarna. Myndighetsutövning kan medföra både förpliktelser för enskilda och åtgärder som är gynnande för enskilda. Det krävs författningsstöd för myndighetsutövning. I första hand är det statliga och kommunala myndigheter som ägnar sig åt myndighetsutövning. Även andra – enskilda juridiska personer liksom fysiska personer – kan med stöd i lag anförtros förvaltningsuppgifter som innefattar myndighetsutövning.

När det sedan gäller en uppgift av allmänt intresse är det också ett unionsrättsligt begrepp. Samma begrepp finns i 1995 års dataskyddsdirektiv och även i den svenska personuppgiftslagen. Det finns dock inte någon definition av begreppet inom unionsrätten och inte heller någon utvecklad praxis från EU-domstolen som belyser hur begreppet ska förstås, särskilt inte när det gäller kamerabevakning i samband med sådana uppgifter. I den praxis som finns har begreppet hittills tolkats förhållandevis snävt. I kommunallagen (1991:900) däremot används begreppet allmänt intresse i en vid mening som ger kommunerna förhållandevis långtgående möjligheter att ägna sig åt olika typer av verksamheter.

Dataskyddsutredningen har uttalat att mycket talar för att begreppet på dataskyddsområdet genom förordningen måste anses ha fått en vidare unionsrättslig betydelse än det haft tidigare. Detta bl.a. eftersom myndigheter oftare än vad som varit fallet enligt 1995 års direktiv kommer att behöva grunda sin behandling av

personuppgifter på att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse. Utredningen har föreslagit att det i dataskyddslagen tas in en förtydligande bestämmelse om när personuppgifter får behandlas i dessa fall. Enligt bestämmelsen får personuppgifter behandlas, med stöd av artikel 6.1 e i förordningen, om behandlingen är nödvändig som ett led i myndighetsutövning som den personuppgiftsansvarige utövar enligt lag eller annan författning eller för att den personuppgiftsansvarige ska kunna utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

Det är mot denna bakgrund inte en enkel uppgift att uttömmande slå fast vad som ryms i begreppet och vad som faller utanför. Som rättsläget är nu kan det vara befogat att tolka begreppet relativt generöst i förevarande sammanhang, även om det inte kan tolkas helt fritt.

Språkligt får begreppet anses avse något som är av intresse för eller berör många människor på ett bredare plan i motsats till ett särintresse. Under begreppet måste anses falla uppgifter som utförs av statliga myndigheter för att uppfylla uttryckliga uppdrag från riksdagen eller regeringen. Detsamma gäller obligatoriska uppgifter som kommuner och landsting utför till följd av författningsreglerade åligganden. Som exempel på obligatoriska uppgifter för kommuner kan nämnas barnomsorg, skola, äldreomsorg, kollektivtrafik, räddningstjänst, hälso- och sjukvård och tillsynsverksamhet. Även biblioteksverksamhet är en obligatorisk uppgift. Obligatoriska uppgifter för landstingen är bl.a. kollektivtrafik och hälso- och sjukvård. Sådana uppgifter som utförs efter ett uttryckligt uppdrag eller till följd av ett åliggande måste anses vara av allmänt intresse oavsett om de utförs i myndighetens egen regi eller om de utförs av någon annan som kontrakterats att utföra uppgiften för myndighetens räkning. När en juridisk eller fysisk person på uppdrag av en statlig eller kommunal myndighet utför en förvaltningsuppgift som åligger den statliga myndigheten eller kommunen utför alltså den personen en uppgift av allmänt intresse.

Under begreppet måste också anses rymmas de frivilliga uppgifter som kommuner och landsting kan utföra så länge det är fråga om angelägenheter av allmänt intresse i den mening som avses i kommunallagen. Kommuner och landsting har som en följd av det

kommunala självstyret en vidsträckt möjlighet att göra frivilliga åtaganden som avser angelägenheter av allmänt intresse. Som exempel kan nämnas tillhandahållande av bostäder, drift av fritids- eller idrottsanläggningar, kulturell verksamhet utom biblioteksverksamhet och drift av campinganläggningar. Sådana åtaganden ska framgå av de reglementen som kommunfullmäktige eller landstingsfullmäktige i varje kommun respektive landsting ska fastställa för sina nämnder i kommunen eller landstinget.

Därutöver utför alla myndigheter vissa administrativa uppgifter – såsom säkerhetsarbete – för att de ska kunna fullgöra sina kärnverksamheter. Även sådana uppgifter som ska säkerställa myndigheternas förvaltning och funktion får anses vara av allmänt intresse.

Vidare kan vissa verksamheter som bedrivs av privaträttsliga subjekt innefatta uppgifter av allmänt intresse som tidigare har skötts i statlig eller kommunal regi. Det gäller t.ex. avseende skola, hälso- och sjukvård och järnvägstransporter.

Det är också tänkbart att vissa andra uppgifter som utförs av privaträttsliga subjekt utan uppdrag från det allmänna eller med stöd i författning skulle kunna anses vara av allmänt intresse, såsom verksamhet som avser idrott, kultur eller vissa transporter.

Ett tillståndskrav ska gälla för myndigheter

Myndigheter med verksamheter som faller in under förordningens tillämpningsområde kan omfattas av ett krav på tillstånd till kamerabevakning. Myndigheternas verksamhet består i myndighetsutövning eller annars i uppgifter av allmänt intresse. Flera av de skäl som angetts ovan för förslaget om ett tillståndskrav på direktivets område och det område som faller utanför direktivet och förordningen kan åberopas även vad gäller kamerabevakning av myndigheter på förordningens område.

Ett krav på tillstånd har gällt länge för myndigheternas kamerabevakning såvitt gäller platser dit allmänheten har tillträde. Syftet har varit att ge ett skydd för den personliga integriteten på platser där allmänheten befinner sig. Tillståndskravet gäller i dag i en mängd olika myndighetsverksamheter på det område som omfattas av förordningen, även om det finns vissa undantag. Ordningen är alltså etablerad och avsedd att garantera ett starkt skydd för integriteten

samtidigt som den ska ge möjligheter till kamerabevakning. Som framgått tidigare har det inte framkommit att det finns några grundläggande problem med ett tillståndsförfarande, även om – som också slagits fast tidigare – möjligheterna till kamerabevakning i och för sig bör öka. De ursprungliga skälen för tillståndskravet gör sig följaktligen gällande även nu.

Till detta kommer att enskilda enligt Europakonventionen och regeringsformen är garanterade ett starkt skydd mot intrång i den personliga integriteten från det allmännas sida. Det talar för ett tillståndskrav för myndigheter, särskilt som kamerabevakning som utgångspunkt är att anse som en särskilt integritetskänslig åtgärd. För det talar också att de verksamheter som bedrivs av myndigheter enligt förordningen kan avse platser som är av speciellt integritetskänslig natur, t.ex. simhallar och badanläggningar, platser som enskilda måste uppsöka exempelvis för vård eller annan omsorg eller platser som många människor måste passera för att kunna ta sig till arbete, skola eller olika aktiviteter såsom knutpunkter för kollektivtrafik och bussar, spårvagnar och liknande.

Vidare är det så att de myndigheter som omfattas av det ovan föreslagna tillståndskravet kommer att träffas av förordningens bestämmelser i vissa fall. I den mån sådana myndigheter bedriver kamerabevakning i samband med uppgifter som faller in under förordningens tillämpningsområde framstår det som naturligt att tillståndskravet ska gälla även då. Ibland kan det också vara så att myndigheterna på en viss plats bedriver både verksamhet som avses i direktivet och verksamhet som omfattas av förordningen och på den platsen använder sig av kamerabevakning. Det är också så att vissa myndigheter som i regel träffas av förordningens bestämmelser kan ha uppdrag som i någon del innebär brottsbekämpning eller annan verksamhet enligt direktivet. Som exempel på det nu sagda kan nämnas när Polismyndigheten eller Tullverket bedriver såväl verksamhet för brottsbekämpning som kontrollverksamhet på en viss plats. Kontrollverksamhet kan bestå i t.ex. utlänningskontroll, tullkontroll och gränskontroll. Att samma regler gäller i fråga om tillstånd för samtliga myndigheter kan ge en tydlighet och förutsebarhet. Gränsdragningsproblem kan undvikas och ett tillståndskrav blir enklare att tillämpa.

Ett krav på tillstånd skulle också fylla ett praktiskt behov. Det förekommer kamerabevakning eller finns intresse av att bedriva

kamerabevakning i ett flertal av de olika verksamheter som omfattas av förordningen. Det gäller exempelvis i kollektivtrafiken, i simhallar, i myndigheters väntrum, på akutmottagningar inom vården och i olika verksamheter för kontroll av miljö m.m. I den tillsynsverksamhet som länsstyrelserna och Datainspektionen bedriver på området har det framkommit att kameraövervakning inte alltid sker på ett korrekt sätt. Som exempel kan nämnas övervakning på sjukhus, vårdcentraler och andra vårdinrättningar. Vid en tillsyn under 2014, som genomfördes av alla länsstyrelser utom en, tillsynades 195 sådana verksamheter. Av dessa fick 53 en eller flera anmärkningar. De vanligaste anmärkningarna var att tillstånd till kameraövervakning saknades eller att upplysning om övervakningen saknades. Ett krav på tillstånd till kamerabevakning kan alltså ge tillsynsmyndigheten en god överblick över och god kontroll av den bevakning som myndigheter vill bedriva. Ett annat exempel är badanläggningar. Under 2016 gjorde länsstyrelserna en nationell tillsyn av sådana anläggningar. Av de 40 badanläggningar som tillsynades, varav åtminstone flertalet bedrevs i myndighetsregi, fick 29 någon form av anmärkning. De vanligaste anmärkningarna handlade om att det saknades tydlig skyltning om övervakningen, att antalet kameror översteg beviljat tillstånd och att övervakningen skedde utanför tillåtet område. Tre av anläggningarna bedrev kameraövervakning trots att de helt saknade tillstånd.

Mot ett tillståndskrav kan invändas att myndigheternas verksamheter är mångskiftande. Behovet av kamerabevakning kan variera betydligt från fall till fall och de integritetsskyddsaspekter som gör sig gällande i olika fall kan också variera i tyngd. Vidare kan det anföras att en stor del av den kamerabevakning som omfattas av förordningen och som tidigare krävt tillstånd framöver kommer att kunna ske tillståndsfritt. Ett tillståndskrav på förordningens område blir alltså begränsat.

Ett ytterligare skäl mot ett tillståndskrav är att ett sådant kommer att innebära vissa skillnader mellan kamerabevakning i likartade situationer som kan uppfattas som svårmotiverade. Som utvecklas närmare nedan kan ett tillståndskrav komma att gälla för kamerabevakning i ett visst sammanhang men inte för kamerabevakning i ett motsvarande sammanhang trots att integritetsskyddsaspekterna i grunden är desamma.

Det kan också invändas att det finns situationer där det kan diskuteras om kamerabevakning som rör en myndighet sker i en verksamhet av allmänt intresse, såsom när bevakning sker av en myndighetsbyggnad för att motverka klotter och annan skadegörelse eller för att inspektera byggnaden. I de fall myndigheten är att anse som den som bedriver kamerabevakningen och denna har som syfte att skydda verksamheten mot brott eller andra störningar bör bevakningen dock anses ske för ett allmänt intresse. I andra fall av bevakning av det diskuterade slaget är det andra än myndigheter som bedriver bevakningen. Beroende på i vilken uppgift bevakningen då sker kan det variera om den sker vid utförande av en uppgift av allmänt intresse eller inte.

Sammanfattningsvis finns det starka skäl som talar för ett krav på tillstånd för att myndigheterna ska få bedriva kamerabevakning. Skälen mot ett sådant krav är däremot av begränsad styrka. Det föreslås därför att ett tillståndskrav ska gälla för kamerabevakning som ska bedrivas av myndigheter i verksamheter som omfattas av förordningen. I praktiken förekommer det inte att riksdagen eller kommun- eller landstingsfullmäktige – som inte är myndigheter – bedriver kamerabevakning. Det sker i stället genom riksdagsförvaltningen eller en kommunal myndighet.

Ett tillståndskrav ska också gälla för vissa privaträttsliga subjekt

Frågan är då om tillståndskravet även bör omfatta kamerabevakning som ska bedrivas av privaträttsliga subjekt. Enligt förordningen kan ett tillståndskrav gälla förutsatt att kamerabevakningen sker för att utföra en uppgift av allmänt intresse, inklusive när den sker som ett led i myndighetsutövning.

Mot ett tillståndskrav kan invändas att det inte kommer att träffa en stor del av den kamerabevakning som omfattas av förordningen och som tidigare krävt tillstånd. Betydelsen av denna invändning ska dock inte överdrivas. Ett begränsat tillståndskrav är en konsekvens av hur förordningen är utformad och alltså förutsatt i förordningen.

För ett tillståndskrav kan anföras att ett sådant har gällt länge för kamerabevakning i verksamheter med uppgifter av det angivna slaget såvitt gäller platser dit allmänheten har tillträde. Vissa undan-

tag finns dock. Ordningen med ett tillståndskrav för att kamerabevakning ska få ske i sådana verksamheter som kan anses vara av allmänt intresse är alltså vedertagen. Den är avsedd att ge ett skydd för den personliga integriteten och samtidigt ge möjligheter till bevakning. Några grundläggande problem med ett tillståndsförfarande finns såvitt framkommit inte. De skäl som ursprungligen legat till grund för tillståndskravet har alltså fortfarande bärkraft, även om – som slagits fast tidigare – möjligheterna till kamerabevakning bör öka.

Vidare talar de skäl som anförts ovan för att tillståndskravet ska gälla kamerabevakning som ska bedrivas av myndigheter för att kravet även bör gälla när förvaltningsuppgifter som innefattar myndighetsutövning har anförtrotts privaträttsliga subjekt. Detsamma gäller när juridiska och fysiska personer bedriver vissa verksamheter som tidigare drivits i offentlig regi. Avmonopolisering och konkurrensutsättning av offentlig verksamhet har inneburit att många uppgifter som tidigare utförts av statliga eller kommunala myndigheter i dag sköts av andra. Inom den traditionellt statliga sektorn kan nämnas t.ex. järnvägstransporter. Som exempel på det kommunala området kan nämnas skola och hälso- och sjukvård. Det kan hävdas vara inkonsekvent att kräva tillstånd till kamerabevakning i myndighetsfallet men inte när ett privaträttsligt subjekt ska bedriva kamerabevakning vid utförandet av en sådan uppgift av allmänt intresse, särskilt som vissa av verksamheterna kan vara mycket integritetskänsliga. Ett tillståndskrav skulle då gälla så länge som en myndighet utför uppgiften men upphöra så snart uppgiften överlåts åt ett privaträttsligt subjekt, t.o.m. när subjektet står under statligt eller kommunalt inflytande. Dessutom kan det variera från plats till plats om det är det offentliga eller någon annan som bedriver en viss verksamhet av allmänt intresse.

Ett tillståndskrav skulle också fylla ett praktiskt behov. Det förekommer kamerabevakning eller finns intresse av att bedriva kamerabevakning i ett flertal av de olika verksamheter som omfattas av förordningen och som innefattar uppgifter av allmänt intresse. Det gäller exempelvis i kollektivtrafiken och inom hälso- och sjukvården. I länsstyrelsernas tillsynsverksamhet har, som framgått av föregående avsnitt, framkommit brister i hur kameraövervakning bedrivits på bl.a. vårdinrättningar. Vanliga brister har varit att övervakningen saknat tillstånd eller att det inte lämnats upp-

lysning om övervakningen. Ett tillståndskrav för att få bedriva kamerabevakning kan ge tillsynsmyndigheten en bättre överblick över förekomsten av kamerabevakning och bättre förutsättningar att tillsyna på området än vad som annars skulle gälla.

Det finns följaktligen flera skäl som med styrka talar för ett krav på tillstånd när det gäller kamerabevakning som ska bedrivas av privaträttsliga subjekt – juridiska personer eller fysiska personer – vid utförande av uppgifter av allmänt intresse. Dessa skäl väger tyngre än skälen mot ett sådant krav. Kravet på tillstånd för att få bedriva kamerabevakning ska alltså gälla också för vissa privaträttsliga subjekt.

Avgränsningen av tillståndskravet för privaträttsliga subjekt

Frågan är då hur kravet på tillstånd till kamerabevakning ska avgränsas för privaträttsliga subjekt som utför uppgifter av allmänt intresse.

Avgränsningen måste givetvis göras så att den håller sig inom ramarna för det utrymme som förordningen ger för ett tillståndskrav. Den bör vidare göras så att den ger ett tillfredsställande integritetsskydd. Största möjliga del av den kamerabevakning som det kan krävas tillstånd för enligt förordningen bör omfattas förutsatt att det också är lämpligt för de enskilda sammanhang där bevakning kan förekomma. Dessutom bör eftersträvas en utformning som så långt det är möjligt gör det förutsebart och enkelt att avgöra vad tillståndskravet omfattar.

Med dessa hållpunkter ska till en början tillståndskravet omfatta verksamheter som i sin kärna har stöd i gällande rätt. Andra verksamheter som privaträttsliga subjekt bedriver och som i och för sig kan motsvaras av verksamheter som drivs av myndigheter, främst av kommunerna som frivilliga uppgifter, ska inte omfattas. Det gäller t.ex. verksamheter som avser fritid, inklusive idrott, och kultur och turism. Från integritetssynpunkt framstår det visserligen som sakligt motiverat att ett tillståndskrav som omfattar t.ex. kamerabevakning i en kommunal simhall också ska omfatta kamerabevakning i en simhall som drivs av ett privaträttsligt subjekt på eget initiativ. Liknande exempel kan tänkas. Ett tillståndskrav som omfattar alla verksamheter hos privaträttsliga subjekt som motsvarar

uppgifter som myndigheter kan utföra, särskilt de kommunala myndigheterna, skulle dock bli väldigt långtgående och sannolikt strida mot förordningen.

Som exempel kan tas kulturverksamhet eller turistverksamhet, som enskilda kan bedriva och som kommuner får ägna sig åt inom vissa ramar. När en sådan verksamhet bedrivs i kommunal regi kan verksamheten sägas vara av intresse för ett stort antal människor i kommunen och därmed utgöra en angelägenhet av allmänt intresse enligt förordningen. Det kan däremot knappast ha varit avsikten med förordningen att i begreppet uppgift av allmänt intresse innefatta varje kulturevenemang, stort eller litet, som anordnats av en privat aktör för allmänheten och där kamerabevakning kan förekomma. Inte heller kan t.ex. campingverksamhet eller hotellverksamhet som drivs av privaträttsliga subjekt rimligen sägas utgöra uppgifter av allmänt intresse. Kamerabevakning i sådana verksamheter kan därmed inte omfattas av ett tillståndskrav. Att motsvarande verksamheter ska omfattas av tillståndskravet i den mån kommuner driver dem och vill kamerabevaka i dessa motiveras av att verksamheterna då drivs för att det gagnar kommunen och kommunmedborgarna och att de därför är av allmänt intresse.

Vidare skulle ett så långtgående tillståndskrav medföra många och svåra gränsdragningsproblem. Som exempel kan tas fritids- och idrottsverksamhet samt kulturverksamhet. Några allmänt vedertagna definitioner av sådana verksamheter finns inte. Innebörden av begreppen kan också växla över tid. Möjligen är det inte uteslutet enligt förordningen att ett tillståndskrav skulle vara möjligt att ställa upp för kamerabevakning vid t.ex. fotbolls- eller ishockeymatcher på elitnivå på idrottsarenor eller vid större konserter i konserthallar eller på arenor. Däremot kan knappast matcher eller träningar eller musikframträdanden i mindre sammanhang, t.ex. en träningsmatch i fotboll för ungdomar på en icke inhägnad plan, betraktas på samma sätt. Vidare är det ytterst tveksamt om ett tillståndskrav skulle kunna träffa en idrottslig eller kulturell aktivitet som förekommer i vissa verksamheter av annat slag, t.ex. biljardspel på en krog eller en författares uppläsning av sin bok i en bokhandel. Restaurangverksamhet och butikverksamhet kan nämligen inte betecknas som uppgifter av allmänt intresse enligt förordningen och därmed inte omfattas av ett tillståndskrav. Det är ogörligt att tydligt och heltäckande räkna upp vilka typer eller former av idrott,

kultur etc. som skulle omfattas av ett tillståndskrav och vilka som skulle falla utanför. Vidare skulle en generell avgränsning av sådana verksamheter innebära en oförutsebar lagstiftning och medföra svårigheter i tillämpningen.

Följaktligen måste tillståndskravet ges en snävare avgränsning. Ett sätt att göra detta på är att fånga den distinktion som ligger i obligatoriska respektive frivilliga uppgifter för myndigheter och använda den för att skilja mellan motsvarande uppgifter som utförs av andra. Det är dock svårt att dra en skarp gräns mellan obligatoriska och frivilliga uppgifter, även för kommunernas del. Uppgifternas natur kan också förändras i takt med att samhället och politiken förändras. Så har t.ex. flyktingmottagandet gått från att vara en frivillig till en tvingande uppgift för kommunerna. En dylik avgränsning skulle alltså medföra gränsdragningssvårigheter.

Ett alternativ är att knyta an till förordningens begrepp uppgift av allmänt intresse och, som redan angetts ovan, kombinera detta med att uppgiften har stöd i gällande rätt, dvs. ska följa av lag eller annan författning eller av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. I detta ligger då även en anförtrodd myndighetsutövande uppgift. Huruvida kamerabevakning förekommer vid utförande av en uppgift som följer av kollektivavtal är svårt att säga men kan inte uteslutas. Uppgifter av allmänt intresse kan – som en följd av den svenska arbetsmarknadsmodellen – vara fastställda genom kollektivavtal. Kollektivavtal bör därför inkluderas, vilket överensstämmer med det ovan nämnda förslaget av Dataskyddsutredningen.

För detta alternativ talar att hela det utrymme som förordningen ger för ett svenskt tillståndskrav kan tas i anspråk. Tillståndskravet kan då ges en omfattning som mest liknar dagens tillståndsplikt. Därmed kan ett tillfredsställande integritetsskydd uppnås.

Visserligen kan invändas att begreppet allmänt intresse är vagt och att en reglering som bygger på detta därmed i vissa avseenden kommer att brista i förutsebarhet och medföra tillämpningssvårigheter. Både den enskilde som vill bedriva kamerabevakning och tillsynsmyndigheten kommer att behöva göra en bedömning av om den enskildes verksamhet är sådan att den är av allmänt intresse. Bedömningen kan ibland bli svår, åtminstone under en inledande period från det att förordningen och kamerabevakningslagen ska börja tillämpas. Det kan i sin tur vara problematiskt med hänsyn till

att överträdelser av tillståndskravet ska vara sanktionerade, vilket föreslås nedan.

Samtidigt är det en fördel att använda just det begrepp som används i förordningen. Innebörden av begreppet har diskuterats ovan och även av Dataskyddsutredningen i anslutning till den ovan redovisade bestämmelsen i dataskyddslagen till förordningen som förtydligar att personuppgiftsbehandling är tillåten som ett led i myndighetsutövning eller för att utföra en uppgift av allmänt intresse. Innebörden kommer sannolikt att utvecklas inom unionen efter hand som praxis utvecklas. Den s.k. Artikel 29-gruppen har också inrättat en arbetsgrupp som fått i uppdrag att utarbeta vägledande yttranden om vissa nyckelbestämmelser och begrepp i förordningen. Vidare har, som framgått, motsvarande begrepp i svensk rätt en relativt klar innebörd som kan ge god ledning i tillämpningen. Dessutom innebär kravet på att uppgiften av allmänt intresse måste följa av författning, kollektivavtal eller beslut som meddelats med stöd av författning en tydlig avgränsning. Den utesluter uppgifter som är eller möjligen kan vara av allmänt intresse men som saknar författningsstöd liksom uppgifter som inte kan anses vara av allmänt intresse. Till detta kommer, vilket föreslås nedan, att tillståndsprövningen ska samlas hos en myndighet. Det kommer att skapa goda förutsättningar för en tolkning som står i överenstämmelse med förordningen och som blir enhetlig.

De nackdelar från tydlighetssynpunkt som kan finnas med att knyta an till begreppet allmänt intresse är alltså begränsade och sannolikt av övergående slag. En ytterligare fördel med en sådan utformning är att den i sak kommer att korrespondera med förordningens och dataskyddslagens reglering om rättslig grund för kamerabevakning i de fall tillståndskravet ska gälla. För att tillstånd överhuvudtaget ska kunna ges måste kamerabevakningen vara laglig enligt EU-regleringen. En prövning av om en viss kamerabevakning, som det söks tillstånd för, i grunden är laglig får naturligen ske inom ramen för tillståndsprövningen.

Att i stället för förordningens begrepp använda ett specifikt svenskt begrepp av generellt slag är inte något alternativ. Ett sådant skulle kräva särskilda tolkningar i svensk praxis och i högre grad än nationella tolkningar av förordningens begrepp riskera att förstås på ett sätt som kan visa sig komma i konflikt med förordningen.

Ett annat alternativ som däremot kan övervägas är att peka ut vissa uppgifter och ange att dessa ska följa av lag eller annan författning, kollektivavtal eller beslut som har meddelats med stöd av lag eller annan författning. De utpekade uppgifterna kan då avse verksamheter där det finns ett mer påtagligt intresse av att enskilda skyddas från kamerabevakning och det därför är viktigt med en myndighetsprövning av om intresset av kamerabevakning väger över det intresset. Det handlar om verksamheter som ofta bedrivs på platser som många människor måste vistas på, passera eller uppsöka eller som är särskilt integritetskänsliga med hänsyn till verksamhetens art eller därför att bevakningen blir omfattande. Som exempel kan nämnas skola, hälso- och sjukvård, social omsorg, drift av förläggningar för asylsökande och tillhandahållande av allmänna kommunikationer. Däremot bör inte pekas ut verksamheter som den enskilde mer frivilligt kan välja att besöka eller där enskilda endast i mindre omfattning kan bli föremål för kamerabevakning med hänsyn till var verksamheten oftast är placerad.

Fördelen med detta alternativ är att regleringen blir förutsebar och enkel att tillämpa. En nackdel är att det omfattar färre situationer av kamerabevakning och därmed ger ett sämre integritetsskydd än alternativet som knyter an till begreppet allmänt intresse. Vidare riskerar en uppräkning att bli ofullständig därför att inte alla uppgifter som bör omfattas – och i samband med vilka kamerabevakning kan förekomma – kan förutses. En uppräkning kan behöva förändras över tid efter hand som samhällsutvecklingen och rättsutvecklingen fortskrider.

Det finns också nackdelar som har att göra med tydligheten i en sådan reglering. Om regleringen ska vara fullt förutsebar och enkel att tillämpa, bör den klart peka ut varje uppgift som ska träffas av tillståndskravet med angivande av relevant författning av vilken uppgiften följer och vari uppgiften ofta definieras. Vidare bör anges eventuella undantag som inte ska omfattas av tillståndskravet men som ingår i uppgiften enligt den aktuella författningen. En uppräkning av det slaget blir otymplig, särskilt i ljuset av att kamerabevakningslagen i övrigt ska innehålla ett begränsat antal bestämmelser. En variant är att i regleringen inte hänvisa till de relevanta författningarna utan endast ange själva uppgifterna, t.ex. hälso- och sjukvård och social omsorg i kombination med erforderliga undantag.

En sådan lösning medför dock att vissa tolkningar måste göras och därmed en risk för att regleringen inte tillämpas på avsett vis.

I valet mellan de alternativ som nu diskuterats måste fördelarna med alternativet att använda begreppet allmänt intresse anses väga tyngst. Nackdelarna med det alternativet kan också hanteras. Detta ska därför väljas.

De sakliga inkonsekvenser som kan följa med det alternativet får godtas. Som exempel kan nämnas uthyrning av bostäder. Ett tillståndskrav kommer att träffa kamerabevakning i en sådan verksamhet när den bedrivs i kommunal regi, t.ex. genom en stiftelse. Verksamheten kan då sägas vara av intresse för ett stort antal människor i kommunen och alltså utgöra en angelägenhet av allmänt intresse. Ett tillståndskrav kan dock inte gälla kamerabevakning vid bostadsuthyrning i annan regi. Det är nämligen svårt att hävda att en privat hyresvärd som hyr ut bostäder, kanske endast i någon enstaka fastighet, kan anses utföra en uppgift av allmänt intresse. Att i stället helt undanta kamerabevakning i fall som detta och liknande från kravet på tillstånd vore sämre från integritetssynpunkt.

När det gäller vissa juridiska personer under statligt eller kommunalt inflytande bedriver de verksamheter inom områden där ett krav på tillstånd till kamerabevakning i verksamheten inte kan ställas upp för andra privaträttsliga aktörer enligt förordningen. Som exempel kan nämnas kamerabevakning i butiker och den verksamhet som Systembolaget AB bedriver. Eftersom kamerabevakning i sådan verksamhet generellt sett enligt förordningen inte kan träffas av ett tillståndskrav, kan inte heller det bolagets verksamhet anses vara av allmänt intresse i förordningens mening och omfattas av kravet. Detsamma gäller kamerabevakning i det statliga Casino Cosmopol AB:s verksamhet. Liknande exempel kan tänkas, t.ex. vad gäller bank- och kreditverksamhet. Sådan verksamhet är visserligen samhällsviktig men kan inte heller anses utgöra en uppgift av allmänt intresse i den mening som avses här. Eventuell kamerabevakning i t.ex. det statliga bolåneföretaget SBAB:s – Statens Bostadsfinansieringsaktiebolag – verksamhet kan därmed inte omfattas av tillståndskravet. Vad gäller postverksamhet är det däremot en sådan författningsreglerad uppgift som måste anses vara av allmänt intresse och som tillståndskravet i och för sig tar sikte på. Kamerabevakning i postverksamhet omfattas i dag av en anmälnings-

skyldighet. Huruvida sådan kamerabevakning ska undantas från tillståndskravet behandlas nedan.

Det föreslås följaktligen att tillståndskravet ska gälla kamerabevakning som ska bedrivas av en annan juridisk person än en myndighet eller av en fysisk person vid utförande av en uppgift av allmänt intresse som följer av lag eller annan författning, kollektivavtal eller beslut som har meddelats med stöd av lag eller annan författning.

Inget tillståndskrav för övriga juridiska eller fysiska personer som omfattas av förordningen

Kamerabevakning kan slutligen bedrivas av juridiska eller fysiska personer i många andra verksamheter eller situationer än de som ovan har föreslagits ska omfattas av tillståndskravet. Syftena med kamerabevakning i sådana andra sammanhang kan variera. Det kan handla om kamerabevakning för att kunna planera, bedriva och kontrollera en näringsverksamhet på ett rationellt sätt. Det kan handla om att motverka brott mot personal eller egendom. Det kan också exempelvis handla om att ha uppsyn över djur eller natur i olika avseenden.

Många gånger är intresset av kamerabevakning i dessa fall berättigat och väger över det motstående intresset av att skydda enskilda mot bevakning. I vissa fall kan integritetsskyddsintresset rentav vara begränsat, t.ex. därför att sannolikheten att människor fångas av kamerabevakningen är relativt liten. I andra fall kan detta intresse väga tyngre än intresset av bevakning.

Kamerabevakning i dessa verksamheter omfattas i dag som regel av tillståndsplikt eller i vart fall av anmälningsskyldighet förutsatt att bevakningen avser en plats dit allmänheten har tillträde. Framöver kan motsvarande krav inte ställas upp, eftersom förordningen inte medger det. Endast kamerabevakning som sker för att utföra en uppgift av allmänt intresse kan omfattas av tillståndskravet och sådana uppgifter är det inte fråga om här.

Som exempel kan nämnas butiksverksamhet. Sådan verksamhet är inte av allmänt intresse i förordningens mening, inte ens om en viss butik, t.ex. en mataffär, är den enda inom rimligt avstånd för invånarna på en ort i glesbygd. Kamerabevakning av butikslokaler kommer alltså framöver att kunna ske tillstånds- och anmälnings-

fritt. I sammanhanget ska nämnas att för sådana lokaler har hittills som en förutsättning för att en anmälan om kamerabevakning ska vara tillräcklig gällt att den som avser att bedriva bevakningen ingått en skriftlig överenskommelse om denna med skyddsombudet, skyddskommittén eller en organisation som företräder de anställda på arbetsplatsen. Frågan om sådana överenskommelser behandlas i avsnitt 13.

Det förtjänar att påpekas att vissa av de verksamheter som inte ska omfattas av tillståndskravet kan vara av stor betydelse för samhället, trots att de inte är av allmänt intresse i den mening som avses här. Det gäller exempelvis massmedieverksamhet och bankverksamhet.

Det nu sagda innebär inte att kamerabevakning framöver kan ske fritt. Som beskrivits närmare i avsnitt 8 gäller då bestämmelserna i förordningen med undantag för kameraanvändning av en fysisk person inom hans eller hennes privata sfär. Detta undantag har behandlats i avsnitt 7.1.4. Normalt gäller alltså t.ex. förordningens bestämmelser om när en kamerabevakning ska anses vara lagligen grundad och när den som vill bedriva bevakningen måste göra en konsekvensbedömning av integritetsriskerna och eventuellt samråda med tillsynsmyndigheten. En kamerabevakning är laglig bl.a. när den är nödvändig för ett ändamål som rör ett berättigat intresse hos den som vill kamerabevaka och detta intresse väger tyngre än de bevakades intressen eller grundläggande rättigheter och friheter. Förordningen innehåller också ytterligare bestämmelser som måste följas. Även andra bestämmelser kan ha betydelse för frågan om en viss kamerabevakning är tillåten eller inte, t.ex. straffbestämmelsen om kränkande fotografering. Det kan förutses att kamerabevakning i många av de fall som nu diskuteras kommer att vara laglig enligt förordningen, eftersom den erkänner fler ändamål som berättigade än vad kameraövervakningslagens tillståndsreglering gör och förutsatt att det motstående integritetsintresset väger lättare.

För vissa av de verksamheter som inte kan omfattas av tillståndskravet gäller i dag att kameraövervakning såvitt avser bilder får ske tillståndsfritt eller efter enbart en anmälan medan avlyssning och inspelning av ljud kräver tillstånd. Det gäller exempelvis butikslokaler. Ett motsvarande krav på tillstånd vad gäller ljud i kamerabevakningslagen skulle stå i strid med förordningen, eftersom

verksamheterna inte kan betraktas som uppgifter av allmänt intresse enligt förordningen. Det innebär dock inte att det framöver är fritt att avlyssna eller spela in ljud. Bestämmelserna i förordningen kommer att gälla.

För banklokaler och lokaler hos kreditmarknadsföretag och området omedelbart utanför in- och utgångar till sådana lokaler samt vid uttagsautomater eller liknande anordningar gäller i dag att avlyssning eller inspelning av ljud får ske endast sedan en anordning för detta har aktiverats på grund av misstanke om brott. Eftersom kamerabevakning i sådan verksamhet inte kan omfattas av tillståndskravet, kan motsvarande krav inte införas i kamerabevakningslagen. I stället kommer förordningens bestämmelser att gälla. I praktiken torde dessa tillåta avlyssning och inspelning av ljud i samma situation.

Följaktligen ska tillståndskravet inte omfatta kamerabevakning som ska bedrivas av juridiska personer eller fysiska personer utan samband med författningsreglerade uppgifter av allmänt intresse. Inte heller ska sådan kamerabevakning omfattas av något anmälningskrav.

Exempel på kamerabevakning som ska omfattas av tillståndskravet

Tillståndskravet ska gälla dels kamerabevakning som ska bedrivas av myndigheter, dels kamerabevakning som ska bedrivas av andra juridiska personer eller fysiska personer vid utförande av en uppgift av allmänt intresse som följer av lag eller annan författning, kollektivavtal eller beslut som har meddelats med stöd av lag eller annan författning. Som föreslås i kommande avsnitt ska kravet gälla platser dit allmänheten har tillträde och vissa undantag gälla från kravet. Nedan behandlas också hur prövningen av om tillstånd ska ges eller inte ska gå till. Tillståndskravet ska däremot inte gälla kamerabevakning i samband med andra uppgifter, oavsett om bevakningen avser en plats dit allmänheten har tillträde eller en plats dit allmänheten saknar tillträde. Som exempel på kamerabevakning som omfattas respektive inte omfattas av tillståndskravet kan nämnas följande.

Tillståndskravet gäller för kamerabevakning av *gator och torg eller andra liknande platser utomhus i ett samhälle*, exempelvis en park,

när det är t.ex. en kommun som vill bedriva bevakningen. Ett privaträttsligt subjekt som inte bedriver en verksamhet av allmänt intresse och som vill använda en kamera på en viss sådan plats eller över ett större område, t.ex. med hjälp av en drönare, omfattas inte av tillståndskravet. Det gäller t.ex. ett företag som vill kamerabevaka vid sin kontorsbyggnad eller industrilokal eller ett fastighetsmäklarföretag som vill avbilda fastigheter från luften. Beroende bl.a. på syftet med kamerabevakningen och dess omfattning i det enskilda fallet torde det variera om sådan bevakning är förenlig med förordningen.

Tillståndskravet gäller i verksamhet med *räddning* oavsett vem som driver verksamheten förutsatt att uppgiften följer av lag eller annan författning eller av ett beslut som har stöd i författning. Kravet gäller även vid kamerabevakning som sker med kameror som förflyttas exempelvis med en drönare eller en ambulans. Ett tidsbegränsat undantag från tillståndskravet gäller dock för kamerabevakning som bedrivs i vissa situationer av den som är räddningsledare.

Kamerabevakning av *entréer till och väntrum för allmänheten hos myndigheter* omfattas av tillståndskravet. Vissa myndigheter har platser för att ta emot personer som har ett ärende hos myndigheten eller som annars ska besöka den. Det gäller t.ex. hos Migrationsverket och inom socialtjänsten.

Tillståndskravet omfattar kamerabevakning i *hälso- och sjukvårdens verksamhet* oavsett vem som bedriver verksamheten förutsatt att det gäller bevakning av utrymmen eller platser dit allmänheten har tillträde. Som exempel kan nämnas kamerabevakning av ett allmänt tillgängligt väntrum på en akutmottagning.

Vidare gäller tillståndskravet kamerabevakning av *förläggningar för asylsökande* oavsett om förläggningen drivs i offentlig eller privat regi. Kravet gäller endast platser dit allmänheten har tillträde och inte t.ex. i gemensamma utrymmen inomhus. Motsvarande gäller *boenden för ensamkommande flyktingbarn* liksom *boenden inom social omsorg*.

Kamerabevakning i *myndigheters kontrollverksamhet* omfattas av tillståndskravet. Det gäller t.ex. Polismyndighetens och Tullverkets verksamheter vid rikets gränser för att utföra utlänningskontroll och tullkontroll.

Tillståndskravet omfattar kamerabevakning i verksamhet som avser *kollektivtrafik, järnväg, flyg och liknande* i den mån något särskilt undantag inte gäller och förutsatt att verksamheten drivs av en myndighet eller någon annan som utför uppgiften till följd av lag eller annan författning eller av beslut som har stöd i författning. Kravet gäller såväl inomhus- som utomhusmiljöer förutsatt att allmänheten har tillträde till platsen där bevakning ska ske. Det gäller t.ex. på bussar, spårvagnar och pendeltåg och busshållplatser och perronger samt i väntsalar på stationer.

Kamerabevakning av *skolområden dit allmänheten har tillträde* omfattas av tillståndskravet. Kravet gäller oavsett vem som driver skolan.

Kravet på tillstånd till kamerabevakning omfattar *simhallar och badanläggningar samt andra idrottsanläggningar och platser där kulturverksamhet bedrivs*, om det är en myndighet eller ett privaträttsligt subjekt som med författningsstöd eller på uppdrag av en myndighet driver verksamheten på platsen. Detsamma gäller kamerabevakning av portar eller andra delar av *bostadshus*.

Kamerabevakning i *butikslokaler* omfattas inte av kravet på tillstånd. Det anmälningskrav som gällt hittills för upptagning av bilder försvinner. Detsamma gäller den tillståndsplikt som hittills gällt för avlyssning eller inspelning av ljud. Förordningens bestämmelser torde normalt inte hindra kamerabevakning i butikslokaler, åtminstone inte bevakning där ljud inte samtidigt avlyssnas eller spelas in, förutsatt att ändamålet med bevakningen kan anses berättigat, såsom när den sker för att motverka brott mot personal eller egendom i butiken. Däremot torde förordningen hindra kamerabevakning i omklädningsrum, provhytter, toalettutrymmen och liknande utrymmen.

Tillståndskravet gäller vidare inte *gemensamma utrymmen i köpcentrum*. Inte heller gäller kravet för kamerabevakning på *restauranger*. Huruvida förordningen medger bevakning på restauranger torde variera från fall till fall.

Kravet på tillstånd omfattar inte kamerabevakning i *parkeringshus*, om det inte är myndigheter som driver verksamheten, vilka dock enligt vad som föreslås nedan ska undantas från tillståndskravet. Det anmälningskrav för att ta bilder eller filma i ett parkeringshus som hittills gällt försvinner liksom dagens tillståndsplikt för att avlyssna och spela in ljud. Förordningen torde normalt

inte hindra kamerabevakning i parkeringshus, åtminstone inte bevakning där ljud inte samtidigt avlyssnas eller spelas in, förutsatt att syftet kan anses berättigat, såsom när kamerabevakning sker för att motverka brott.

Tillståndskravet gäller vidare inte kamerabevakning av *medieredaktioner*, t.ex. bevakning av ingångar till eller av fasader på en byggnad där det bedrivs medieverksamhet. Detsamma gäller för *lokaler som används av religiösa samfund*.

Tillståndskravet omfattar inte kamerabevakning inom *jordbruk och skogsbruk*. Kamerabevakning i dessa verksamheter torde normalt vara tillåten enligt förordningen. Sådan bevakning kan vara av stort värde för planering, drift och kontroll. Särskilt kamerabevakning med drönare kan ge snabb och detaljerad information på ett sätt som kameraanvändning från marken eller direkta iakttagelser med ögat inte kan ge. Kamerabevakning kan också användas för att motverka brottslighet som är särskilt riktad mot verksamheterna, såsom stölder av fordon och maskiner eller av elektronisk utrustning i dessa samt dieselstölder. Intresset av att inte bli bevakad väger ofta lättare än behovet av bevakning därför att det handlar om platser där allmänheten endast kortvarigt eller på långt avstånd kan bli föremål för bevakning.

Kamerabevakning av vilt, t.ex. vid *åtlar* – platser som iordningställs i syfte att locka vilt för att jaga viltet – omfattas inte av kravet på tillstånd annat än om det är en myndighet som ska bedriva bevakningen eller någon annan som på myndighetens uppdrag ska göra det. I betänkandet *Vildsvin och viltskador* (SOU 2014:54) och promemorian *Kameraövervakning av vildsvinsåtlar* (N2015-06665) har föreslagits att dagens tillståndsplikt ersätts med ett anmälningsförfarande vad gäller viss sådan kamerabevakning. Regeringen har i propositionen *Vildsvin och viltskador* (prop. 2015/16:199 s. 21) inte gått vidare med förslaget utan gjort bedömningen att frågan måste övervägas inom ramen för denna översyn av kameraövervakningslagen, bl.a. i ljuset av den nya förordningen. Enligt förordningen kan ett krav på tillstånd eller anmälan inte ställas upp framöver för sådan kamerabevakning. För kamerabevakning av vilt i myndighetsverksamhet kan och ska dock tillståndskravet gälla.

11.6 Tillståndskravet ska avse platser dit allmänheten har tillträde

Förslag: Kravet på tillstånd till kamerabevakning ska avse platser dit allmänheten har tillträde.

Skälen för förslaget: En särskild fråga är om kravet på tillstånd till kamerabevakning, liksom enligt gällande lagstiftning, bör knytas till bevakning av platser dit allmänheten har tillträde. Med sådana platser menas exempelvis gator, torg och parker samt transportmedel som används för allmänna kommunikationer.

Som slagits fast tidigare är det en utgångspunkt för kamerabevakningslagen att det inte nu bör införas ett tillståndskrav för sådan kamerabevakning som inte hittills har omfattats av tillståndsplikt. Endast om det framkommit att det numera finns ett starkt behov av ett sådant tillståndskrav bör utgångspunkten frångås.

Något behov av att införa ett generellt tillståndskrav för kamerabevakning på platser dit allmänheten saknar tillträde har inte framkommit.

Vad gäller vissa särskilda platser dit allmänheten saknar tillträde gör sig integritetshänsynen starkt gällande. Det gäller miljöer där människor upprepat vistas, såsom på arbetsplatser och i skolor. I tidigare lagstiftningssammanhang har frågan väckts om det inte borde införas en anmälningsskyldighet för att kamerabevakning ska få ske på sådana platser. En anmälningsskyldighet skulle kunna bidra till en bättre bild av omfattningen av sådan kamerabevakning, underlätta tillsynsmyndighetens arbete och förstärka integritetsskyddet.

Arbetsplatser diskuteras separat i avsnitt 13. Vad gäller skolor och övriga platser av det nu nämnda slaget, vilka i och för sig också kan utgöra arbetsplatser, är det som tidigare framgått inte tillåtet enligt förordningen med en ren anmälningsskyldighet. De angivna skälen för en sådan skyldighet kan dock även tala för ett tillståndskrav, vilket förordningen tillåter i viss utsträckning. Ett sådant vore emellertid mer långtgående än den anmälningsskyldighet som har efterfrågats. Vidare innehåller förordningen detaljerade bestämmelser om när och hur kameraanvändning får ske och förutsätter också att det utarbetas branschöverenskommelser. Redan i dag finns infor-

mationsmaterial vad gäller t.ex. skolors kamerabevakning och möjlighet att vända sig till tillsynsmyndigheten för vägledning. Det är också förhållandevis lätt för tillsynsmyndigheten att informera sig om vilka skolor som finns i landet och därmed att vid behov bedriva tillsyn i fråga om kamerabevakning vid dessa.

Sammantaget kan skälen för ett tillståndskrav för kamerabevakning av de platser som nu diskuterats inte anses vara av sådan tyngd att ett sådant krav bör införas.

En anknytande fråga är om begreppet plats dit allmänheten har tillträde bör definieras eller förtydligas, t.ex. genom en exemplifiering av vad som menas, eller om rentav något annat begrepp bör användas i stället. Frågan har diskuterats i tidigare lagstiftningsärenden (se bl.a. prop. 2012/13:115 s. 34). I dessa har hänvisats till att begreppet använts länge och blivit föremål för en omfattande praxis. Vidare har anförts att ett förtydligande skulle kunna leda till en detaljerad och svåröverskådlig lagtext. Dessa invändningar har fortfarande fog för sig. Begreppet bör därför behållas.

Följaktligen föreslås att kravet på tillstånd till kamerabevakning ska avse platser dit allmänheten har tillträde.

11.7 Den närmare utformningen av tillståndskravet

Förslag: Tillstånd ska krävas till kamerabevakning av en plats dit allmänheten har tillträde, om bevakningen ska bedrivas av en myndighet. Detsamma ska gälla om kamerabevakning av en sådan plats ska bedrivas av en annan juridisk person eller en fysisk person vid utförande av en uppgift som följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning och

1. avser brottsbekämpning, lagföring eller straffverkställighet eller upprätthållande av allmän ordning och säkerhet,
2. avser nationell säkerhet, eller
3. annars är av allmänt intresse.

Skälen för förslaget: Som framgått av tidigare avsnitt ska kravet på tillstånd till kamerabevakning gälla för

- kamerabevakning som avses i direktivet, nämligen kamerabevakning som ska bedrivas av en myndighet som har i uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet eller av en annan aktör som utövar myndighet för något av dessa syften förutsatt att myndighetens eller aktörens kamerabevakning sker i ett sådant syfte,
- viss kamerabevakning som omfattas av förordningen, nämligen dels kamerabevakning som ska bedrivas av en myndighet, dels kamerabevakning som ska bedrivas av en annan juridisk person eller en fysisk person vid utförande av en uppgift av allmänt intresse som följer av lag eller annan författning, kollektivavtal eller beslut som har meddelats med stöd av lag eller annan författning, och
- kamerabevakning som ska bedrivas av en myndighet eller en annan aktör i en verksamhet som faller utanför direktivet och förordningen, dvs. verksamhet som inte omfattas av unionsrätten, såsom verksamhet rörande nationell säkerhet, och verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken.

Som vidare framgått ska tillståndskravet avse platser dit allmänheten har tillträde och inträda när kamerabevakning ska ske, vilket i praktiken innebär att tillstånd måste sökas innan bevakningen får påbörjas.

Lagtekniskt föreslås att kravet på tillstånd tas in i en för samtliga fall gemensam bestämmelse där kravet uttrycks dels samlat för myndigheterna, dels gemensamt för övriga aktörer med ett tillägg för vart och ett av de fall som omfattas – direktivsfallen, förordningsfallen och övriga fall – för att tydliggöra att samtliga dessa omfattas. För aktörer som inte utgör myndigheter föreslås att den för förordningsfallen gjorda kopplingen till stöd i gällande rätt görs generell och alltså knyts även till de fall som träffas av direktivet och de fall som inte träffas av förordningen eller direktivet. I de fallen finns en underförstådd sådan koppling. Vad gäller tilläggen för dessa fall bör de utformas på ett kortfattat och relevant sätt.

För gruppen övriga fall behöver inte anges ”den gemensamma utrikes- och säkerhetspolitiken”, eftersom endast myndigheter och politiska församlingar” deltar i den. Däremot ska övrig verksamhet utanför unionsrätten, lämpligen uttryckt som nationell säkerhet, omfattas. Sådan verksamhet bedrivs i första hand inom offentlig sektor men det kan inte uteslutas att andra aktörer utför uppgifter inom ramen för den verksamheten. Denna lagtekniska lösning framstår som lättillgänglig samtidigt som den kan bli kortfattad.

I enlighet med detta föreslås att bestämmelsen ska ha följande lydelse. Tillstånd ska krävas till kamerabevakning av en plats dit allmänheten har tillträde, om bevakningen ska bedrivas av en myndighet. Detsamma gäller om kamerabevakning av en sådan plats ska bedrivas av en annan juridisk person eller en fysisk person vid utförande av en uppgift som följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning och avser brottsbekämpning, lagföring eller straffverkställighet eller upprätthållande av allmän ordning och säkerhet, avser nationell säkerhet eller annars är av allmänt intresse.

11.8 Särskilda undantag från tillståndskravet

Förslag: Från kravet på tillstånd till kamerabevakning ska göras vissa undantag som i huvudsak motsvarar undantagen från tillståndsplikten enligt kameraövervakningslagen. Några av undantagen ska vidgas. Vidare ska kamerabevakning som är anmälningsskyldig enligt den lagen, och som inte längre kan vara det, undantas från tillståndskravet.

Skälen för förslaget

Undantag från dagens tillståndsplikt

I dag är viss kamerabevakning som bedrivs i sådan verksamhet som i och för sig ska omfattas av tillståndskravet helt eller delvis tillståndsfri alternativt endast anmälningsskyldig. Det gäller både verksamheter som avses i direktivet eller som omfattas av förordningen och verksamheter som faller utanför EU-regleringen.

Exempelvis gäller inte något krav på tillstånd för kameraövervakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning. Inte heller krävs tillstånd vid övervakning som sker för att skydda vissa byggnader, anläggningar eller områden som har förklarats vara skyddsobjekt, om övervakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet. Inte heller krävs tillstånd för kameraövervakning som Försvarsmakten bedriver från fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan övervakning.

Vidare får kameraövervakning bedrivas av Polismyndigheten eller Säkerhetspolisen under högst en månad utan att tillstånd har sökts när det av särskild anledning finns risk för att allvarlig brottslighet som innebär fara för liv eller hälsa eller för omfattande förstörelse av egendom kommer att utövas på en viss plats och syftet med övervakningen är att förebygga eller förhindra brott.

Dessutom får kameraövervakning ske under högst en månad utan att en ansökan om tillstånd har gjorts t.ex. vid övervakning som bedrivs av Polismyndigheten eller den som är räddningsledare enligt lagen (2003:778) om skydd mot olyckor, om övervakningen är av vikt för att avvärja en hotande olycka eller för att begränsa verkningarna av en inträffad olycka.

Ytterligare ett exempel på kameraövervakning som inte kräver tillstånd är den som bedrivs av Trafikverket i form av vägtrafikövervakning eller vid en betalstation för trängselskatt eller för infrastrukturavgift för att samla in uppgifter som behövs för att beslut om sådan skatt eller avgift ska kunna fattas och för att kontrollera att betalning erläggs. Tillståndsfri är vidare sådan kameraövervakning som avser säkerheten i trafiken eller arbetsmiljön och som sker med en kamera på ett fordon, en maskin eller liknande för att förbättra sikten för föraren eller användaren.

Motsvarande undantag ska göras från det nya tillståndskravet

Något behov av att nu införa ett krav på tillstånd för sådan kamerabevakning som i dag är helt eller delvis tillståndsfri har inte konstaterats.

Inte heller har det framkommit några tungt vägande praktiska behov som gör att det med frångående av de grundläggande principer som bär upp kamerabevakningslagstiftningen går att motivera att undantagen utvidgas avsevärt eller att det införs fler förhållandevis vida undantag, t.ex. undantag som helt undantar Polismyndigheten och Säkerhetspolisen eller undantar dessa myndigheters brottsbekämpande verksamhet. Detta gäller även med hänsyn tagen till att den tekniska utvecklingen har inneburit att kameraanvändning i vissa situationer nu kan ske med annan teknik än tidigare och därför kan falla in under lagens tillämpningsområde. Behov av ökade möjligheter till kamerabevakning får i stället tillgodoses genom ökade möjligheter att få tillstånd till kamerabevakning, vilket föreslås nedan, och genom något vidgade möjligheter att bedriva kamerabevakning utan upplysning.

I några avseenden bör dock förändringar ske i form av att det görs undantag från tillståndskravet.

Undantag för Polismyndigheten och Säkerhetspolisen

Vad gäller det tidsbegränsade undantaget för Polismyndigheten och Säkerhetspolisen föreslås att detta vidgas till att avse även syftena upptäcka sådan brottslig verksamhet samt utreda och lagföra sådana brott som avses i undantaget. Undantaget ska visserligen inte kunna åberopas i en situation där ett visst brott redan har begåtts och polisen därefter vill kamerabevaka för att utreda brottet under förundersökningen. Undantaget innefattar dock i dag en rätt att bevara bilder och att avlyssna och spela in ljud. Att bilder och ljud spelas in sker för utredning av brott. Att polisen kan bedriva kamerabevakning med stöd av undantaget när det finns risk för sådan brottslighet som avses i undantaget innebär självfallet att polisen också kan fortsätta sin bevakning i ett fall där risken realiseras så länge situationen pågår. Kamerabevakningen kan alltså då avse ett begånget brott och utredning av detta genom att material från bevakningen spelas in. Utredningssyftet ska därför läggas till.

Detsamma gäller lagföringssyftet. Dessa myndigheter ägnar sig visserligen inte åt lagföring i de angivna fallen. Att en kamerabevakning sker för bl.a. utredning av framtida brott av de nämnda typerna syftar dock ytterst till lagföring. Noteras kan också att utredningssyftet i dag anges i andra bestämmelser i kameraövervakningslagen där det handlar om kamerabevakning av aktörer som inte själva har i uppgift att utreda brott. Vidare föreslås att syftet upptäcka läggs till för att uppnå en överensstämmelse med vad som föreslås nedan i fråga om tillståndsprövningen vid kamerabevakning i brottsbekämpande verksamhet i övrigt.

En särskild fråga är hur man ska se på möjligheten för Polismyndigheten och Säkerhetspolisen att använda en spaningsmetod som innebär att en kamera placeras på ett visst ställe och sedan styrs av en polisman på visst avstånd från det objekt som man vill spana på genom kameran. Detta kan ske både på underrättelsestadiet och förundersökningsstadiet. Syftet med att använda en kamera på håll är att polisen inte vill riskera att röja spaningen både för att skydda själva spaningsverksamheten och för att skydda de enskilda polismän som bedriver denna. Det har tidigare i olika sammanhang övervägts att införa lagstiftning som reglerar användandet av denna och andra spaningsmetoder (se bl.a. prop. 2007/08:163 och SOU 2010:103). Någon sådan lagstiftning finns dock ännu inte.

Beroende på hur metoden praktiskt arrangeras i det enskilda fallet och på vilket stadium den används kan den omfattas av såväl kameraövervakningslagens som kamerabevakningslagens tillämpningsområde och därmed omfattas av bestämmelserna om tillståndskrav och upplysningsskyldighet. Principiella skäl talar starkt emot att införa särskilda bestämmelser i kamerabevakningslagen om undantag från tillståndskravet eller om undantag från upplysningskravet för denna kameraanvändning, utan att dessa kombineras med en separat lagstiftning som anger förutsättningarna för själva metoden. Sådana bestämmelser skulle indirekt innebära en reglering av metoden och en reglering som lagstiftaren hittills ansett inte bör införas. Vidare är det fråga om en kameraanvändning som förutsätts ske dolt och som kan ske t.ex. under en förundersökning. Den liknar därför mer hemlig kameraövervakning än kamerabevakning enligt den nya lagen, som i princip alltid ska ske öppet. Hemlig kameraövervakning kräver normalt tillstånd av domstol och kringgärdas även i övrigt av rättssäkerhetsgarantier som inte har några

motsvarigheter i kameraövervakningslagen eller kamerabevakningslagen. I likhet med vad som gäller för hemlig kameraövervakning framstår det som lämpligast med en särskild reglering av metoden kombinerad med, vid behov, ett undantag från kamerabevakningslagens tillämpningsområde. En sådan reglering kräver noggranna överväganden som inte kan eller får göras i detta sammanhang. Något förslag i denna fråga läggs alltså inte.

Undantag vad gäller vägtrafik m.m.

När det gäller Trafikverkets kamerabevakning av vägtrafiken har det framkommit att dagens undantag inte anses gälla vid öppningsbara broar. Vid sådana broar behöver Trafikverket kamerabevaka trafiken på såväl sjövägen som vägen på land för att kunna öppna och stänga broarna på ett säkert sätt. I dag krävs alltså tillstånd för kamerabevakning av sjötrafiken i anslutning till en öppningsbar bro men inte för bevakning av vägen till och från samt på bron. Undantaget bör vidgas till att omfatta även den nu beskrivna situationen. Sådan kamerabevakning kan ha stor betydelse för att förhindra olyckor eller för att minska skadeverkningarna av inträffade olyckor. Samtidigt får den anses medföra begränsade risker för integritetsintrång. Det föreslås alltså att Trafikverkets undantag ska gälla även bevakning av sjötrafik vid en rörlig bro.

Vidare gäller i dag att kamerabevakning i en tunnelbanevagn eller av en tunnelbanestation får ske efter anmälan, om bevakningen har till enda syfte att förebygga, avslöja eller utreda brott, förhindra olyckor eller begränsa verkningarna av en olycka och kameran är fast monterad och försedd med fast optik. Avlyssning eller inspelning av ljud får dock inte ske utan tillstånd.

En ren anmälningsskyldighet kan som framgått ovan inte behållas för sådan kamerabevakning. Någon anledning att nu i stället införa ett krav på tillstånd finns inte. De skäl som tidigare motiverat enbart en anmälningsskyldighet talar tvärtom för att denna kamerabevakning bör undantas från tillståndskravet. Vidare är verksamheten sådan att tillsynsmyndigheten även utan ett tillståndskrav känner till att det bedrivs kamerabevakning och därför har goda möjligheter att utöva tillsyn över denna. Inte heller bör ett krav på tillstånd för att avlyssna och spela in ljud gälla. Visserligen är avlyss-

ning och inspelning av ljud generellt sett känsligare än bildupptagning. Emellertid skulle ett fortsatt tillståndskrav för ljud komplicera vad som ska gälla för kamerabevakning i tunnelbanevagnar och på tunnelbanestationer. Med ett fortsatt sådant krav skulle kamerabevakningslagens bestämmelser om ansökan om tillstånd och tillståndsprövning gälla för den delen av kamerabevakningen som avser ljud medan förordningens bestämmelser, t.ex. om konsekvensbedömning och samråd, ska gälla för bildupptagningen. En sådan ordning är inte lämplig. Vidare ska, som framgått tidigare, motsvarande tillståndskrav vad gäller ljud inte behållas för kamerabevakning i t.ex. butiker, eftersom ett tillståndskrav för kamerabevakning av sådana platser överhuvudtaget inte kan behållas.

Det föreslås alltså att det görs ett undantag från tillståndskravet som i stort motsvarar vad som hittills gällt i fråga om anmälningsskyldighet. Undantaget föreslås utformas på ett sätt som motsvarar vad som föreslås nedan för tillståndsprövningen beträffande brott och olyckor. Vidare föreslås att kravet på att kameran är fast monterad och försedd med fast optik tas bort. Kravet har visserligen ursprungligen ställts upp av integritetsskäl. Numera torde dock fast optik inte förekomma i samma utsträckning som tidigare. Samtidigt kommer många kameror i dessa fall fortfarande att vara fast monterade även utan ett sådant krav. Vidare torde de ofta ha ett brett upptagningsområde för att kunna uppfatta avvikelser från det normala och därmed fånga människor på avstånd. Vid en sådan avvikelse kan behovet av att zooma in händelsen vara påtagligt. Kravet kan därför slopas utan att det innebär någon större förändring av integritetsskyddet. Slutligen ska vad gäller ljud avlyssning och inspelning inte längre kräva tillstånd.

I ljuset av de nu diskuterade föreslagna undantagen kan det övervägas om även annan liknande kamerabevakning bör vara tillståndsfri. Det har framförts att kamerabevakning som avser järnvägstrafik och stationsområden bör kunna ske efter enbart en anmälan. Någon anmälningsskyldighet kan som sagt inte finnas i kamerabevakningslagen. Frågan är därför om sådan bevakning bör få ske utan tillstånd. Som skäl för detta har bl.a. anförts att det förekommer brottslighet av viss typ och viss omfattning på sådana platser, t.ex. i stationshus och på perronger. Vidare har det bl.a. pekats på olycksrisker på järnvägslinjen, inklusive vid plankorsningar.

Vad gäller järnvägen som sådan kan kamerabevakning ske tillståndsfritt av platser dit allmänheten inte har tillträde, såsom spårområden och bangårdar. På de platser där både passagerare och andra människor får uppehålla sig gör sig påtagliga integritetshänsyn gällande. Samtidigt föreslås nedan att möjligheterna att få tillstånd till kamerabevakning ska öka för ändamål som avser brottsbekämpning och motverkande av olyckor. Med hänsyn härtill saknas skäl att göra undantag från tillståndskravet.

Undantag för postverksamhet m.m.

Motsvarande resonemang som förts ovan angående tunnelbanevagnar och tunnelbanestationer kan föras för kamerabevakning i postverksamhet. I dag gäller en anmälningsskyldighet för sådan bevakning. En kamera får efter anmälan sättas upp för kameraövervakning i ett postkontor eller i området omedelbart utanför in- och utgångar till en sådan lokal, om övervakningen har till enda syfte att förebygga, avslöja eller utreda brott och kameran är fast monterad och försedd med fast optik. Avlyssning eller inspelning av ljud får ske endast sedan en anordning för detta har aktiverats på grund av misstanke om brott. Med postkontor avses en lokal där det huvudsakligen bedrivs verksamhet i vilken ingår postverksamhet. Samma reglering gäller i fråga om en yta i en butikslokal där det bedrivs postverksamhet. Dock gäller att avlyssning eller inspelning av ljud då inte får ske utan tillstånd. I det fallet krävs dessutom att den som avser att bedriva övervakningen har ingått en skriftlig överenskommelse om övervakningen med skyddsombudet, skyddskommittén eller en organisation som företräder de anställda på arbetsplatsen.

Dessa bestämmelser föreslås få en motsvarighet i form av ett undantag från tillståndskravet. Undantaget föreslås vidare utformas på ett sätt som överensstämmer med vad som föreslås nedan för tillståndsprövningen beträffande brott. Av samma skäl som angetts i föregående avsnitt bör det inte längre ställas upp något krav på att kameran ska vara fast monterad och försedd med fast optik. Vad gäller ljud ska avlyssning och inspelning inte längre kräva tillstånd. Frågan om skriftlig överenskommelse med en arbetstagarrepresentant behandlas i avsnitt 13.

Slutligen kan resonemanget ovan anföras även i fråga om kamerabevakning i parkeringshus. I dag gäller att en kamera efter anmälan får sättas upp för kameraövervakning i ett parkeringshus, om övervakningen har till enda syfte att förebygga, avslöja eller utreda brott. Avlyssning eller upptagning av ljud får dock inte ske utan tillstånd. Eftersom det enligt vad som framkommit förekommer att myndigheter, i första hand kommunala myndigheter, i egen regi driver parkeringshus dit allmänheten har tillträde bör denna anmälningsskyldighet ges en motsvarighet i form av ett undantag från den nya lagens krav på tillstånd. Undantaget ska utformas på ett sätt som överensstämmer med vad som föreslagits ovan för kamerabevakning i postverksamhet och tunnelbaneverksamhet.

Sammanfattning

Sammanfattningsvis föreslås att det från kravet på tillstånd till kamerabevakning ska göras vissa undantag som i huvudsak motsvarar undantagen från tillståndsplikten enligt kameraövervakningslagen. Några av undantagen ska vidgas. Vidare föreslås att kamerabevakning som är anmälningsskyldig enligt den lagen, och som inte längre kan vara det, ska undantas från tillståndskravet.

I sammanhanget ska påpekas att det utöver vad som diskuterats ovan finns viss kamerabevakning som i dag är undantagen från tillståndsplikten eller omfattad av anmälningsskyldigheten och som är sådan att den framöver inte träffas av kamerabevakningslagens tillståndskrav. Några undantag från kravet behövs därmed inte för sådan kamerabevakning. Ett anmälningskrav kan inte heller gälla.

11.9 Förutsättningarna för tillstånd

Förslag: Tillstånd till kamerabevakning ska ges om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad.

De intressen av kamerabevakning som ska tillmätas särskild betydelse ska utökas jämfört med kameraövervakningslagen.

Vid bedömningen av intresset av kamerabevakning ska det särskilt beaktas om bevakningen behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats eller på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet till person eller på egendom,
2. förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller begränsa verkningarna av sådana störningar,
3. utöva kontrollverksamhet,
4. förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor, eller
5. tillgodose andra därmed jämförliga ändamål.

Vid bedömningen av den enskildes intresse av att inte bli kamerabevakad ska det särskilt beaktas

1. hur bevakningen ska utföras,
2. om teknik som främjar skyddet av den enskildes personliga integritet ska användas, och
3. vilket område som ska bevakas.

Bedömning: Kamerabevakning bör utgöra ett komplement till andra åtgärder.

Skälen för förslaget och bedömningen

Utgångspunkter

Frågan är då hur bestämmelserna om tillståndsprövning ska utformas. Som slagits fast i avsnitt 9.2.2 bör bestämmelserna ge ökade möjligheter till kamerabevakning. Vidare ska bestämmelserna vara förenliga med EU-regleringen och även i delar där de skulle kunna utformas annorlunda anpassas till denna reglering. De bör gälla för all kamerabevakning som träffas av tillståndskravet, oavsett om det

är kamerabevakning som omfattas av förordningen, kamerabevakning som avses i direktivet eller kamerabevakning som faller utanför EU-regleringen. I den utsträckning det är lämpligt kan regleringen i kameraövervakningslagen tjäna som förebild.

Som framgått av avsnitt 7.1.8 förutsätter förordningens särskilda utrymme för ett nationellt tillståndskrav naturligen kompletterande bestämmelser om hur en tillståndsprövning ska gå till. Vidare lämnar förordningen utrymme för nationella bestämmelser om allmänna villkor för personuppgiftsbehandling när behandlingen är nödvändig som ett led i myndighetsutövning eller för att utföra en uppgift av allmänt intresse, dvs. i de fall som ska omfattas av det svenska tillståndskravet. På samma sätt ger direktivets utrymme för starkare skyddsåtgärder i nationell rätt, som behandlats i avsnitt 7.2.6, en möjlighet att i svensk rätt närmare reglera tillståndsprövningen. En sådan möjlighet finns också på det område som faller utanför EU-regleringen. Som också framgått tidigare måste en planerad kamerabevakning vara laglig i den mening som avses i förordningen eller direktivet och brottsdatalagen för att överhuvudtaget få ske. Kravet på tillstånd gäller därutöver. I tillståndsprövningen kommer naturligt att ingå en bedömning av lagligheten.

En fortsatt intresseavvägning

Tillståndsprövningen enligt kamerabevakningslagen bör ske i form av en intresseavvägning mellan intresset av kamerabevakning och den enskildes intresse av att inte bli bevakad där tillstånd ska meddelas om det förra intresset väger tyngre än det senare. Denna proportionalitetsbedömning med en överviktsprincip är förenlig med EU-regleringen och liknar den konsekvensbedömning som den som vill bedriva kamerabevakning skulle ha gjort utan ett tillståndsförfarande enligt den regleringen. En sådan intresseavvägning sker också enligt kameraövervakningslagen och är ändamålsenlig även framöver. Behovet av kamerabevakning i ett enskilt fall måste vägas mot det intrång i integriteten som en kamerabevakning i det särskilda fallet innebär. Att det räcker med att intresset av kamerabevakning väger över det motstående intresset är rimligt i ljuset av ambitionen att möjligheterna till kamerabevakning ska öka. En sådan

bestämmelse är slutligen möjlig att ha för all kamerabevakning som ska omfattas av tillståndskravet.

Vad särskilt angår intresset av kamerabevakning gäller i dag att kameraövervakning endast får utgöra ett komplement till andra åtgärder i samma syfte, särskilt brottsförebyggande åtgärder. Kameraövervakning bör alltså inte ses som ett hjälpmedel som ska användas i stället för andra säkerhetsåtgärder eller förebyggande insatser.

Motsvarande princip kan sägas gälla enligt förordningen och direktivet. Enligt den regleringen krävs att en behandling av personuppgifter är *nödvändig* för att den ska få ske. Av ingresserna till förordningen och direktivet följer vidare att personuppgifter bör behandlas endast om syftet med behandlingen inte rimligen kan uppnås genom andra medel. Även om det unionsrättsliga begreppet nödvändig inte anses ha den strikta innebörden att något absolut fordras, bör i tillståndsprövningen också fortsättningsvis kamerabevakning ses som ett komplement till andra åtgärder, särskilt brottsförebyggande åtgärder. Detta kan beaktas i prövningen utan att det behöver föreskrivas uttryckligen. Det görs inte heller i kameraövervakningslagen.

Det föreslås följaktligen att tillstånd till kamerabevakning ska ges om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad.

Intresset av kamerabevakning

När det sedan gäller vad som ska beaktas vid bedömningen av intresset av kamerabevakning har i avsnitt 9.2.2 närmare beskrivits ett flertal berättigade intressen av att bedriva kamerabevakning och att dessa inte med dagens lagstiftning kan få det genomslag i praxis som de bör ha. Den slutsats som dras är att kameraövervakningslagens bestämmelse om förutsättningarna för tillstånd till kameraövervakning är för snävt utformad både vad gäller övervakning för brottsbekämpande ändamål och vad gäller övervakning för andra ändamål. Möjligheterna till kamerabevakning ska därför öka, särskilt i fråga om kamerabevakning för syften som har att göra med brottsbekämpning men också för kamerabevakning i andra syften. Det gäller oavsett vem som vill bedriva kamerabevakning i ett visst

syfte, även om detta kan få betydelse vid bedömningen av hur tungt dennes intresse av sådan bevakning väger.

Vad först gäller brottsbekämpning anges i kameraövervakningslagen att det särskilt ska beaktas om kameraövervakning behövs för att *förebygga, avslöja eller utreda brott*. I praxis krävs att den plats som det gäller kan visas vara brottsutsatt eller, för att inspelning av material ska få ske, t.o.m. särskilt brottsutsatt. Intresset av brottsbekämpning på brottsutsatta platser ska självfallet fortsatt kunna åberopas som skäl för kamerabevakning. Vidare bör möjligheterna till inspelning öka på sådana platser, även när de inte är *särskilt* brottsutsatta. Det bör räcka att platsen är brottsutsatt. Med det menas inte varje plats där det någon gång har inträffat enstaka brott. Det krävs att människor eller egendom på platsen eller platsen i övrigt drabbats av brott i viss omfattning.

Det måste dock också vara möjligt att som skäl för kamerabevakning åberopa intresset av brottsbekämpning på vissa andra platser. Ibland kan det vara svårt att slå fast att en plats är brottsutsatt samtidigt som det ändå på objektiva grunder kan konstateras att det finns ett påtagligt behov av kamerabevakning på platsen med detta berättigade ändamål. Ett sådant behov måste kunna åberopas av såväl Polismyndigheten som andra, t.ex. en kommun. Det gäller i första hand platser som inte är, eller kan visas vara, mer frekvent drabbade av brott men där det finns en särskild risk för brott av vissa typer jämfört med andra platser i samhället dit allmänheten har tillträde. Det är platser där angrepp på liv, hälsa eller trygghet till person eller på egendom ändå har inträffat med viss upprepning eller där det finns en generell hotbild avseende de typerna av angrepp mot människor som bor, arbetar eller annars vistas regelmässigt på platsen eller mot egendom som finns där, t.ex. en viss byggnad eller fordon med anknytning till platsen. Som exempel kan nämnas förläggningar för asylsökande. Ett annat exempel kan vara en viss myndighets lokaler för anställda och myndighetens fordon. Angreppen på eller hotbilden mot människor på sådana platser kan t.ex. avse misshandelsbrott och hotbrott. Angreppen på eller hotbilden mot egendom avser handlingar som innebär förstörelse av egendom, t.ex. skadegörelse eller mordbrand. Huruvida tillstånd till kamerabevakning av sådana platser, såvitt gäller delar dit allmänheten har tillträde, ska ges får avgöras efter en

sammanvägning av intresset av kamerabevakning och intresset av skydd för integriteten för dem som bor och arbetar där.

Vidare måste intresset av att *utreda* framtida brott ges större tyngd än det haft hittills, särskilt i situationer där kamerabevakning inte samtidigt kan antas förebygga brottslighet på platsen alls eller endast i mindre utsträckning. Material från kamerabevakning kan ha stor betydelse för möjligheterna att utreda och lagföra brott, oavsett brottstyp och oavsett om bevakningen kan väntas ha någon direkt avskräckande effekt på potentiella brottslingar. Att begångna brott kan utredas och lagföras bidrar dessutom till att upprätthålla förtroendet för straffsystemet och därmed till att detta får avsedd generell brottsavhållande verkan. Utrymmet för att ge tillstånd till kamerabevakning i detta syfte, trots att en bevakning inte kan förväntas minska brottsligheten på platsen, ska alltså vidgas.

Dessa utvidgningar kan åstadkommas genom att de ändamål som avser brottsbekämpning förtydligas och utökas jämfört med kameraövervakningslagen samtidigt som de anpassas till EU-regleringen och genom att det anges för vilka platser ändamålen kan åberopas. Utredningen om 2016 års dataskyddsdirektiv har föreslagit att brottsdatalagens tillämpningsområde, i de delar som är relevanta i detta sammanhang, ska uttryckas så att lagen gäller för behandling av personuppgifter som utförs av behöriga myndigheter i syfte att *förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott*. Detta motsvarar språkbruket i direktivet, dock med den skillnaden att ordet upptäcka används i stället för ordet avslöja. En liknande uppräkning används i olika bestämmelser i förordningen. Samma uppräkning föreslås i kamerabevakningslagen. Visserligen ska kamerabevakning i syfte att utreda och lagföra inte ta sikte på bevakning som sker enbart i efterhand för att utreda ett redan begånget brott. Ordet brott och inte brottslig verksamhet bör likväl användas i dessa delar, eftersom en kommande utredning och lagföring av ett framtida brott avser ett konkret brott. Till uppräkningen ska knytas dels den situationen att en plats är *brottsutsatt*, dels den situationen att det av *särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet till person eller på egendom* på en plats.

Vidare framstår det som angeläget att tillmäta intresset av allmän ordning och säkerhet särskild tyngd i kamerabevakningslagen. Detta intresse kan delvis överlappa intresset av brottsbekämpning, efter-

som det ibland är svårt att dra en gräns mellan brottsbekämpande uppgifter och uppgifter som avser allmän ordning och säkerhet. Att upprätthålla eller på annat sätt främja ordning och säkerhet är dock många gånger en självständig uppgift. Den nämnda utredningen har föreslagit att brottsdatalagen också ska omfatta personuppgiftsbehandling som utförs av behöriga myndigheter i syfte att upprätthålla allmän ordning och säkerhet. Kamerabevakning i syfte att *förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller att begränsa verkningarna av sådana störningar* kan utgöra ett berättigat intresse inte endast för Polismyndigheten och de andra subjekt som avses i direktivet utan också för andra som omfattas av kravet på tillstånd till kamerabevakning. Det gäller kommuner och andra aktörer som har ett ansvar för ordning och säkerhet som följer av författning, t.ex. ordningslagen (1993:1617). Detta intresse ska därför anges i kamerabevakningslagen. Huruvida ett visst subjekt med fog kan åberopa detta intresse och hur tungt det då väger får avgöras i det enskilda fallet.

Vidare ska uttryckligen anges intresset av att *utöva kontrollverksamhet*. Eftersom kravet på tillstånd för att bedriva kamerabevakning endast gäller myndigheter och andra subjekt som med författningsstöd eller stöd i beslut som meddelats enligt författning – eller stöd i kollektivavtal – utför vissa uppgifter handlar det här om myndigheters eller andras författningsreglerade verksamhet av det angivna slaget. Som exempel kan nämnas gränskontroll och tullkontroll. Kamerabevakning för att utföra sådana uppgifter kan vara av stor nytta samtidigt som, beroende på platsen, intresset för den enskilde av att inte bli föremål för bevakning kan vara begränsat.

Dessutom ska liksom i dag anges intresset av att *förhindra olyckor*. Detta intresse ska vidgas så att det också kan avse att *förebygga eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor*.

Slutligen ska anges att det vid bedömningen av intresset av kamerabevakning särskilt ska beaktas om bevakningen behövs för att *tillgodose andra därmed jämförliga ändamål*, dvs. ändamål som är jämförbara med de ovan uppräknade. Detta innebär en utvidgning jämfört med kameraövervakningslagen på det sättet att jämförelsen ska ske med de i kamerabevakningslagen särskilt uppräknade ändamålen, som delvis är nya eller vidare. Som exempel på ett sådant jämförligt ändamål kan nämnas kamerabevakning vid utförande av en uppgift som avser Sveriges säkerhet och som inte omfattas av de

uppräknade intressena. Därutöver finns det, i likhet med vad som gäller enligt kameraövervakningslagen, ett utrymme att anse att andra ändamål kan vara berättigade och att intresset av kamerabevakning även i sådana fall kan väga över hänsynen till integriteten. Då krävs normalt att integritetsriskerna är försumbara. Ibland kan dock dessa risker vara större men det berättigade intresset väga mycket tungt och därför väga över den enskildes intresse av att inte bli kamerabevakad.

Den enskildes intresse av att inte bli kamerabevakad

När det sedan gäller den enskildes intresse av att inte bli kamerabevakad bör bestämmelsen om vad som särskilt ska beaktas vid bedömningen av detta intresse utformas på samma sätt som i kameraövervakningslagen. En sådan utformning är förenlig med EU-regleringen. Den är också väl avvägd, även med beaktande av de utvidgningar som föreslagits ovan i fråga om intresset av kamerabevakning. Några tillämpningsproblem har inte framkommit vid den utvärdering av kameraövervakningslagen som gjorts. Tvärtom har utvärderingen visat att användning av integritetsvänlig teknik är en viktig faktor som kan medföra att tillstånd ges i större omfattning än om sådan teknik inte används. Eftersom utvecklingen av integritetsvänlig teknik hela tiden går framåt, kan förutses att denna omständighet får allt större betydelse vid tillståndsprövningen på det sättet att intresset av att inte bli föremål för kamerabevakning väger lättare. Därmed kan intresseavvägningen oftare utfalla så att tillstånd ska meddelas. I sammanhanget ska erinras om att integritetsintresset enligt gällande praxis anses vara mindre starkt i fall där de enskilda som kan komma att bli föremål för kamerabevakning samtidigt är de som riskerar att drabbas av den brottslighet som bevakningen syftar till att motverka. Denna praxis har goda skäl för sig.

Följaktligen föreslås att det vid bedömningen av den enskildes intresse av att inte bli kamerabevakad särskilt ska beaktas hur bevakningen ska utföras, om teknik som främjar skyddet av den enskildes personliga integritet ska användas och vilket område som ska bevakas.

Särskilt om tillstånd att spela in material, m.m.

Avslutningsvis ska sägas något dels om efterföljande behandling – inklusive inspelning och lagring – av bilder, dels om avlyssning och inspelning av ljud.

Enligt kameraövervakningslagen gäller att frågan om tillstånd ska ges till att bilder får behandlas vidare prövas inom ramen för den helhetsbedömning som görs vid intresseavvägningen. Det saknas anledning att i kamerabevakningslagen ta in särskilda regler för tillståndsprövningen i detta avseende.

Vidare har hittills gällt att ett tillstånd till kameraövervakning inte regelmässigt ska avse även tillstånd till efterföljande behandling av bilder. Denna utgångspunkt bör visserligen fortsatt gälla generellt. Av de föreslagna utvidgningarna avseende vilka intressen av kamerabevakning som särskilt ska beaktas i tillståndsprövningen följer dock naturligen att synen på när sådant tillstånd ska ges också bör bli mer generös.

Exempelvis ska möjligheten att kamerabevaka för brottsbekämpande ändamål öka. Intresset av att utreda och lagföra brott ska ges en större tyngd framöver. För att sådan kamerabevakning ska fylla sitt syfte krävs i regel en rätt att inte bara bevaka i realtid utan också att spela in och lagra bilder. Sparade bilder kan bidra till och ibland vara avgörande för att brott kan utredas och lagföras. Det gäller generellt för alla brott. Vissa brott är dessutom svåra att förutse och begås under endast några enstaka sekunder, vilket innebär att en rätt till inspelning endast på förekommen anledning blir utan värde. Som exempel kan nämnas en stöld av en väska eller mobiltelefon på en bänk bredvid en sovande ägare i en vänthall som begås av en förbipasserande. Utan en inspelningsrätt kan ett sådant brott många gånger inte utredas och lagföras. Ett tillstånd till kamerabevakning för brottsbekämpande syften bör alltså i regel innefatta en rätt till efterföljande behandling av bilder både vad gäller brottsutsatta platser och andra platser där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet till person eller på egendom.

En sådan rätt bör också ges i större utsträckning i andra fall än vad som tidigare varit möjligt. Det gäller exempelvis när syftet med kamerabevakning är att förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor i en verksamhet

som avser ämnen som kan vara mycket farliga för människor eller miljön.

I sammanhanget ska nämnas att det i avsnitt 14 görs den bedömningen att kamerabevakningslagen inte ska innehålla någon bestämd längsta tid under vilken material från kamerabevakning får behandlas. Det gör att tillsynsmyndighetens prövning av frågan inom ramen för tillståndsförfarandet får stor betydelse. Som framgår av nästa avsnitt kan tillsynsmyndigheten meddela villkor om detta när den ger tillstånd till kamerabevakning. Myndigheten kan då beakta eventuella relevanta bestämmelser i registerförfattningar.

När det gäller frågan om tillstånd ska ges till avlyssning eller inspelning av ljud gäller i dag att den prövas inom ramen för den helhetsbedömning som görs vid intresseavvägningen. Detsamma bör gälla framöver. Några särskilda bestämmelser om tillståndsprövningen för ljud ska alltså inte införas.

Vidare gäller i dag att ett tillstånd som innefattar en rätt att avlyssna eller spela in ljud endast ges om ett starkt behov av en sådan möjlighet kan påvisas. Avlyssning och inspelning av ljud i samband med kameraövervakning anses innebära att övervakningen blir mer känslig från integritetssynpunkt än om endast upptagning av bilder sker. I många situationer och miljöer är det naturligt att människor kan betraktas av andra medan det normalt är så att den enskilde kan råda över vem som hör vad han eller hon säger. Denna hållning har fortfarande fog för sig och bör gälla som en utgångspunkt. Även fortsättningsvis bör alltså tillståndsgivningen vad gäller avlyssning och inspelning av ljud präglas av restriktivitet.

11.10 Tillståndsförfarandet

Förslag: En ansökan om tillstånd till kamerabevakning ska vara skriftlig och innehålla uppgifter som i princip motsvarar innehållet i en sådan konsekvensbedömning som regleras i förordningen eller direktivet.

Den kommun där kamerabevakningen ska ske ska få tillfälle att yttra sig före ett beslut om tillstånd, om det behövs.

Ett beslut om tillstånd ska förenas med villkor om hur bevakningen får anordnas. Om förutsättningarna för ett tillstånd ändras, får nya villkor beslutas eller, om förutsättningarna för tillstånd inte längre är uppfyllda, tillståndet återkallas.

Skälen för förslaget

Innehållet i en ansökan om tillstånd, m.m.

Enligt förordningen och direktivet är det den personuppgiftsansvarige som ska se till att behandlingen av personuppgifter sker i enlighet med förordningen respektive den nationella lagstiftning som genomför direktivet. Med personuppgiftsansvarig avses en fysisk eller juridisk person som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen.

I förordningen och direktivet anges vidare hur den personuppgiftsansvarige ska göra en konsekvensbedömning avseende dataskydd i de fall där en sådan behövs. En konsekvensbedömning enligt förordningen ska innehålla åtminstone

- en systematisk beskrivning av den planerade behandlingen och behandlingens syften, inbegripet – när det är lämpligt – den personuppgiftsansvariges berättigade intresse,
- en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftet,
- en bedömning av riskerna för de registrerades rättigheter och friheter, och
- de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifter och för att visa att förordningen efterlevs.

Enligt direktivet ska en konsekvensbedömning innehålla en allmän beskrivning av den planerade behandlingen, en bedömning av riskerna för de registrerades rättigheter och friheter, de åtgärder som planeras för att hantera riskerna, inklusive skyddsåtgärder, säker-

hetsåtgärder och rutiner för att säkerställa skyddet av personuppgifter och för att visa att direktivet efterlevs. Utredningen om 2016 års dataskyddsdirektiv har föreslagit att det i förordningen till brottsdatalagen tas in bestämmelser om konsekvensbedömning som genomför direktivets bestämmelse.

En konsekvensbedömning kan visserligen inte anses behöva göras i de fall av kamerabevakning som omfattas av det föreslagna tillståndskravet. Som slagits fast tidigare bör dock bestämmelserna i kamerabevakningslagen, även när det inte är nödvändigt, utformas i nära överensstämmelse med bestämmelserna i EU-regleringen. Det framstår också som lämpligt i detta avseende. De krav som ska ställas upp i kamerabevakningslagen på innehållet i en ansökan om tillstånd ska därför ansluta till förordningens och direktivets reglering om konsekvensbedömning. För förordningens del kan tilläggas att sådana svenska bestämmelser inte kan anses utgöra en otillåten nationell reglering, eftersom bestämmelsen om konsekvensbedömning i förordningen inte gäller innehållet i en ansökan.

I kameraövervakningslagen föreskrivs i dag att en ansökan om tillstånd till kameraövervakning ska göras skriftligen hos länsstyrelsen i det län där övervakningen ska ske. Enligt den lagen ska vidare en ansökan om tillstånd innehålla uppgift om och beskrivning av den som ska bedriva kameraövervakningen och i förekommande fall den som ska ha hand om övervakningen för tillståndshavarens räkning, ändamålen med övervakningen, den utrustning som ska användas, den plats där utrustningen ska placeras och det område som kan övervakas och de omständigheter i övrigt som är av betydelse för prövningen av ärendet. Om övervakningen avser en arbetsplats, krävs vidare ett yttrande från skyddsombudet, skyddskommittén eller en organisation som företräder de anställda på arbetsplatsen. Innan beslut om tillstånd fattas ska dessutom den kommun där övervakningen ska ske få tillfälle att yttra sig, om det inte är onödigt.

Som framgår av avsnitt 15 nedan föreslås att tillsynen enligt kamerabevakningslagen ska samlas hos en myndighet. Det ska därför föreskrivas att en ansökan om tillstånd till kamerabevakning ska göras hos tillsynsmyndigheten. Vidare ska föreskrivas att en sådan ansökan ska vara skriftlig och att det i den ska anges vem som ska bedriva kamerabevakningen och i förekommande fall den som ska ha hand om bevakningen för tillståndshavarens räkning. Vid kamera-

bevakning får den som bestämmer ändamålet med bevakningen anses vara den som bedriver denna. Det kan vara flera som tillsammans bedriver kamerabevakning. Att den som bedriver kamerabevakning kan överlåta åt annan att faktisk handha bevakningen medför inte att ansvaret för denna överlåts.

Vidare föreslås att en ansökan om tillstånd lämpligen ska innehålla följande.

- Uppgift om bevakningens ändamål.
- En beskrivning av bevakningen, särskilt den utrustning som ska användas, var utrustningen ska placeras, det område som ska bevakas och de tider då bevakningen ska ske.
- En bedömning av behovet av och proportionaliteten i bevakningen i förhållande till ändamålet.
- En bedömning av riskerna för intrång i den personliga integriteten och en beskrivning av de åtgärder som planeras för att hantera riskerna.
- Uppgift om de omständigheter i övrigt som är av betydelse för prövningen av ärendet.

I avsnitt 13 behandlas frågan om det vid kamerabevakning av en arbetsplats, i likhet med vad som gäller i dag, ska krävas ett yttrande i tillståndsfrågan från en arbetstagarrepresentant.

Vad slutligen gäller dagens krav på att den berörda kommunen ska yttra sig i tillståndsärendet har det framkommit att kommunerna sällan har några särskilda synpunkter samtidigt som deras hörande medför en viss tidsutdräkt i ärendena. Att ett yttrande från den kommun där kamerabevakningen ska ske ibland kommer att vara värdefullt även för prövningen av tillstånd enligt kamerabevakningslagen står klart. En bestämmelse om att kommunen före ett beslut om tillstånd ska få tillfälle att yttra sig ska därför införas i lagen. Mot bakgrund av vad som framkommit ska dock föreskrivas att ett yttrande ska lämnas endast om det behövs. Den bedömningen görs av tillsynsmyndigheten.

Tillståndsbeslutet

Eftersom förordningen och direktivet inte innehåller några bestämmelser som föreskriver ett tillståndsförfarande, saknar de naturligen bestämmelser om hur ett tillstånd till kamerabevakning får utformas. Tillståndsförfarandet enligt kamerabevakningslagen måste dock övergripande sett vara förenligt med EU-regleringen. Det innebär att bestämmelser om tillståndsbeslut måste hålla sig inom de ramar som förordningen och direktivet ger. Det finns också en särskild bestämmelse i förordningen som tillåter att det i nationell rätt föreskrivs ytterligare befogenheter för den nationella tillsynsmyndigheten utöver vad som följer av förordningen. I direktivet finns en bestämmelse om att det i nationell rätt får föreskrivas starkare skyddsåtgärder än de som fastställs i direktivet. Dessutom lämnar både förordningen och direktivet utrymme för att sanktioner föreskrivs i nationell rätt. En form av sanktion är återkallelse av tillstånd.

I dag föreskrivs i kameraövervakningslagen att ett beslut om tillstånd att kameraövervaka ska förenas med villkor om hur kameraövervakningen får anordnas. Sådana villkor ska avse övervakningens ändamål, den utrustning som får användas och det område som får övervakas. Det ska också beslutas om de övriga villkor som behövs för tillståndet. Sådana villkor får avse upplysningar om övervakningen, upptagning, användning, bevarande eller annan behandling av bilder, avlyssning eller upptagning av ljud samt andra förhållanden som har betydelse för att skydda enskildas personliga integritet. Vidare får ett tillstånd meddelas för en begränsad tid. Om förutsättningarna för ett tillstånd ändras, får nya villkor beslutas eller, om förutsättningarna för tillstånd inte längre uppfylls, tillståndet återkallas.

Dessa bestämmelser är förenliga med EU-regleringen och ändamålsenliga även för tillståndsbeslut enligt kamerabevakningslagen. Motsvarande bestämmelser, med vissa mindre sakliga och språkliga ändringar, ska därför tas in i den nya lagen.

12 Upplysning om kamerabevakning

12.1 Ett upplysningskrav

Förslag: Vid kamerabevakning ska genom tydlig skyltning eller på något annat liknande verksamt sätt lämnas upplysning om

1. kamerabevakningen,
2. identiteten hos och kontaktuppgifterna till den som ska bedriva bevakningen, och
3. kontaktuppgifter till ett eventuellt dataskyddsombud.

Om ljud kan avlyssnas eller tas upp vid bevakningen, ska en särskild upplysning lämnas om detta.

Information ska även göras tillgänglig för dem som kan bli kamerabevakade om

1. ändamålet med och den rättsliga grunden för kamerabevakningen,
2. hur länge upptaget bild- och ljudmaterial får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa detta, och
3. möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifterna till den.

Skälen för förslaget

Rätten till information enligt EU-regleringen

I dataskyddsförordningen och dataskyddsdirektivet finns bestämmelser om registrerades rättigheter. En av dessa är att den registrerade ska ha rätt till information om behandlingen av sina personuppgifter.

Rätten till information enligt förordningen är utformad som en skyldighet för den personuppgiftsansvarige att till registrerade lämna information om behandlingen av deras personuppgifter. Informationen ska lämnas självmant av den personuppgiftsansvarige. Den information som ska lämnas är omfångsrik. Rätten till information enligt direktivet är utformad som en skyldighet för den personuppgiftsansvarige att dels göra viss information tillgänglig för den registrerade, dels i specifika fall lämna viss annan information till den registrerade. Även denna information ska lämnas självmant av den personuppgiftsansvarige. Någon avgörande betydelseskillnad mellan uttrycket ”lämna” och uttrycket ”göra tillgänglig” i de delar som tar sikte på samma slags information enligt förordningen respektive direktivet kan inte anses finnas.

Såväl förordningen som direktivet innehåller också bestämmelser med allmänna krav på hur informationen ska lämnas. Av dessa bestämmelser framgår bl.a. att informationen ska tillhandahållas i en koncis, begriplig och lättillgänglig form och på ett klart och tydligt språk. Vidare ska informationen tillhandahållas på lämpligt sätt, t.ex. i elektronisk form. Informationen ska som huvudregel vara kostnadsfri.

I kameraövervakningslagen finns en upplysningsplikt som innebär att upplysning om kameraövervakning ska lämnas genom tydlig skyltning eller på något annat verksamt sätt. Upplysning ska också lämnas om vem som bedriver övervakningen, om detta inte framgår av förhållandena på platsen. Om ljud kan avlyssnas eller tas upp vid övervakningen, ska särskild upplysning lämnas om detta. Upplysningsplikten inträder när övervakningsutrustningen sätts upp. Den som bedriver kameraövervakning ska vidare lämna upplysning om ändamålen med övervakningen, om den övervakade eller den som kan komma att bli övervakad begär det.

I avsnitt 7.1.10 har gjorts den bedömningen att kameraövervakningslagens upplysningsplikt i huvudsak är förenlig med förord-

ningens rättigheter för registrerade och möjligheter att begränsa dessa rättigheter samt att vissa bestämmelser på kamerabevakningsområdet om upplysningsplikt kan införas i svensk lagstiftning som kompletterar förordningen. Enligt den bedömning som gjorts i avsnitt 7.2.5 är vidare kameraövervakningslagens upplysningsplikt i huvudsak förenlig med direktivets rättigheter för registrerade och möjligheter att begränsa dessa rättigheter. Av det avsnittet framgår också att en svensk lagstiftning som omfattar kamerabevakning måste innehålla bestämmelser om rättigheter för registrerade eller om undantag från rättigheterna som uppfyller kraven i direktivet. I avsnitt 7.3 har redovisats att sådan kamerabevakning som inte omfattas av förordningens och direktivets tillämpningsområden i och för sig kan regleras i svensk rätt utan beaktande av EU-regleringen.

Redan i avsnitt 9 har konstaterats att det krävs en särskild reglering om hur det ska upplysas om kamerabevakning. Regleringen ska vara förenlig med bestämmelserna i förordningen och direktivet och bör även i delar där den i och för sig kan utformas annorlunda anpassas till EU-regleringen. Den bör, så långt det är förenligt med EU-regleringen och ändamålsenligt, vara densamma för all kamerabevakning. I den utsträckning det är lämpligt bör den vidare utformas med förebild i kameraövervakningslagen.

Behovet av ett svenskt krav på upplysning

Enligt förslaget i avsnitt 10.2 ska kamerabevakning definieras på ett sätt som liknar kameraövervakning enligt kameraövervakningslagen. Kravet på att utrustningen inte ska manövreras på platsen innebär att den som bedriver bevakningen inte kommer att befinna sig på den plats där utrustningen är placerad. Någon faktisk identifiering av de personer som ”fångats” av en kamera sker oftast inte ens i de fall där materialet spelas in och bevaras. Det finns alltså sällan någon reell möjlighet att i efterhand lämna information till de personer som registrerats vid bevakningen. I många fall är den enda rimliga möjligheten att informera om bevakningen att lämna informationen på platsen genom skyltning. Som nämnts ovan är dock den information som ska lämnas enligt EU-regleringen omfattande. Att lämna all den informationen på skyltar i anslutning till den plats där bevakningen ska ske skulle riskera att göra skylt-

ningen svårare att upptäcka och att informationen blir otydlig. Detta innebär att det vid kamerabevakning råder särskilda förhållanden vad avser EU-regleringens krav på att lämna information till dem som kan bli kamerabevakade.

Från integritetssynpunkt är det viktigt att den som kan bli föremål för kamerabevakning får kännedom om bevakningen. Dold kamerabevakning är i princip inte acceptabel. Det är därför angeläget med ett tydligt krav på hur information ska lämnas vid just kamerabevakning så att det verkligen sker på ett verksamt sätt. Det möjliggör för enskilda att anpassa sig till att platsen är kamerabevakad och att välja om de vill bli föremål för sådan bevakning. Vidare syftar förordningens och direktivets bestämmelser om rätten till information till att registrerade ska kunna göra sina övriga rättigheter gällande. Ett upplysningskrav i fråga om kamerabevakning måste vara utformat så att det kan tjäna även detta intresse. Därigenom kan ett starkt integritetsskydd vid kamerabevakning garanteras. Till detta kommer att de förslag som lämnats ovan om kamerabevakningslagens tillämpningsområde och tillståndskrav innebär att många aktörers kamerabevakning kommer att få ske utan tillstånd. Denna förändring jämfört med kameraövervakningslagen medför att det bör ställas höga krav på upplysning i samband med kamerabevakning.

Mot denna bakgrund är det uppenbart att det finns behov av en särskild svensk bestämmelse om krav på upplysning vid kamerabevakning. En sådan kan bättre ta hänsyn till de särskilda förhållanden som gäller vid kamerabevakning och säkerställa ett starkt integritetsskydd. Det måste därför närmare undersökas om och hur en sådan bestämmelse kan förenas med EU-regleringen.

Ett svenskt upplysningskrav är möjligt

Bestämmelserna om rätten till information i förordningen och direktivet bygger vidare på motsvarande bestämmelser i 1995 års dataskyddsdirektiv. Bestämmelserna om upplysningsplikt i kameraövervakningslagen har bedömts vara förenliga med bestämmelserna i det direktivet. Frågan är om de skäl som motiverat den bedömningen kan åberopas för att göra motsvarande bedömning av den nya EU-regleringen.

Enligt 1995 års direktiv skulle informationen till den registrerade omfatta den personuppgiftsansvariges och dennes eventuella företrädares identitet, ändamålen med behandlingen och all ytterligare information som med hänsyn till de särskilda omständigheter under vilka uppgifterna samlades in var nödvändig för att tillförsäkra den registrerade en korrekt behandling.

I samband med införandet av kameraövervakningslagen bedömdes upplysningsplikten vara förenlig med 1995 års direktiv med motiveringen att kamerabevakning i de allra flesta fall är att anse som sådan ostrukturerad behandling av personuppgifter som omfattas av den s.k. missbruksregeln i personuppgiftslagen. Enligt den behöver bl.a. de bestämmelser i lagen som rör frågor om information till registrerade inte tillämpas vid ostrukturerad behandling av personuppgifter och motsvarande ansågs därför gälla vid kamerabevakning (SOU 2009:87 s. 204 ff.).

Missbruksregeln, som efter en översyn av personuppgiftslagen infördes den 1 januari 2007, innebär dels ett undantag från de viktigaste bestämmelserna i personuppgiftslagen för behandling av personuppgifter i ostrukturerat material, dels ett förbud mot att utföra sådan behandling när behandlingen innebär en kränkning av den registrerades personliga integritet. Undantaget motiverades främst av att det ansågs att hantering av ostrukturerat material, t.ex. i form av löpande text och ljud- och bildupptagningar, utgjorde ett utnyttjande av en sådan fri- och rättighet, nämligen yttrande- eller informationsfriheten, som enligt en bestämmelse i direktivet kunde motivera undantag från direktivets rättigheter (prop. 2005/06:173 s. 31 ff.) Sådan hantering skulle därför inte begränsas av de normala hanteringsreglerna i personuppgiftslagen.

Den undantagsbestämmelse i 1995 års direktiv som missbruksregeln grundas på har med vissa tillägg tagits in i förordningen (artikel 23). Bestämmelsen innebär att det är möjligt att i nationell lagstiftning begränsa tillämpningsområdet för såväl rätten till information som övriga rättigheter. Begränsningen måste dock ske med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgöra en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa skydd av den registrerade eller andras rättigheter och friheter. En liknande undantagsmöjlighet finns i direktivet (artikel 13.3) för viss del av bestämmelsen om rätten till information.

Det kan noteras att det i förordningen också finns ett särskilt undantag för yttrande- och informationsfriheten, som har en motsvarighet i 1995 års direktiv. Det förhållandet att yttrande- och informationsfriheten behandlas särskilt i en bestämmelse i förordningen kan inte anses innebära att just den fri- och rättigheten inte skulle omfattas av uttrycket fri- och rättigheter i förordningens bestämmelse om undantag från registrerades rättigheter. Motsvarande bedömning gjordes vid införandet av missbruksregeln (a. prop. s. 32).

Sammanfattningsvis finns det inte anledning att nu göra någon annan bedömning än den som regeringen gjort i förhållande till 1995 års direktiv i samband med införandet av missbruksregeln. Det innebär att rätten till yttrande- och informationsfrihet i det här fallet får anses vara en sådan fri- och rättighet som kan motivera en begränsning av EU-regleringens bestämmelser.

Denna rätt kan dock inte åberopas för myndigheter och andra subjekt som utövar myndighet eller utför uppgifter av allmänt intresse i förordningens mening. För dessa subjekt ger emellertid förordningen ett särskilt utrymme för nationella bestämmelser. Enligt förordningen får i dessa fall den nationella rätten innehålla bestämmelser om de allmänna villkor som ska gälla för behandlingen, vilken typ av uppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka uppgifterna får lämnas ut och för vilka ändamål, ändamålsbegränsningar, lagringstid samt typer av behandling och förfaranden för behandling.

Förordningen innebär samtidigt att missbruksregeln inte kan behållas. Vidare utgör kamerabevakning en form av personuppgiftsbehandling som kan vara, även när den är berättigad, särskilt integritetskänslig. Det är därför inte helt säkert hur utrymmet att göra undantag från rätten till information enligt förordningen och direktivet ska uppfattas strikt rättsligt. Ett praktiskt synsätt måste i viss mån kunna anläggas vid tolkningen. Som framgått ovan är rätten till information enligt EU-regleringen utformad på ett generellt sätt – eftersom den omfattar personuppgiftsbehandling i allmänhet – och därför dåligt anpassad till kamerabevakning. Rimligen hindrar EU-regleringen inte en tolkning som innebär att vissa avvikelser kan göras för den särskilda form av personuppgiftsbehandling som kamerabevakning utgör. Detta gäller särskilt om en avvikande nationell bestämmelse kan anpassas för att ge bästa möjliga integritetsskydd vid den formen av behandling, främst genom en reglering av

sättet för hur information ska lämnas. En godtagbar balans mot det förhållandet att viss information utelämnas kan då uppnås. I sammanhanget ska nämnas att det i avsnitt 15 nedan föreslås att överträdelse av kravet på upplysning ska sanktioneras, vilket inte föreslagits av Utredningen om 2016 års dataskyddsdirektiv för motsvarande informationskrav i brottsdatalagen. Däremot ska det påföras sanktionsavgift vid överträdelse av bestämmelserna om rätten till information enligt förordningen.

Till detta kommer att vissa delar av den information som ska lämnas enligt förordningen och direktivet inte är relevanta vid kamerabevakning. Avvikelser från regleringen i de delarna är givetvis möjliga.

Sammantaget görs därför bedömningen att det är möjligt att införa en svensk bestämmelse om krav på upplysning vid kamerabevakning som i delar kan avvika från EU-regleringen och som samtidigt kan ge ett starkt integritetsskydd vid sådan bevakning.

Hur ska upplysningskravet utformas?

Frågan är då hur en svensk bestämmelse om krav på upplysning vid kamerabevakning ska utformas.

I enlighet med de utgångspunkter som angetts ovan ska bestämmelsen gälla för all kamerabevakning som omfattas av kamerabevakningslagen. Bestämmelsen ska exklusivt reglera frågan. För att bestämmelsen ska gå att förena med EU-regleringen och ge ett starkt integritetsskydd ska den vidare innehålla krav på att relativt utförlig information ska lämnas och på hur detta ska ske. Den kommer därigenom att innebära högre krav än kameraövervakningslagens upplysningsplikt. Samtidigt kan de delar av dagens upplysningsplikt som är ändamålsenliga behållas.

I direktivet anges först vilken information den personuppgiftsansvarige alltid ska göra tillgänglig för registrerade (artikel 13.1). Det är fråga om allmän information som gäller den personuppgiftsansvariges identitet och kontaktuppgifter, dataskyddsombudets kontaktuppgifter, ändamålen med behandlingen, rätten att lämna in klagomål till en tillsynsmyndighet och tillsynsmyndighetens kontaktuppgifter, rätten att begära tillgång till personuppgifter och

rätten att begära rättelse eller radering av personuppgifter och begränsning av behandling.

Därutöver ska den personuppgiftsansvarige i specifika fall lämna viss information för att göra det möjligt för den registrerade att utöva sina rättigheter (artikel 13.2). Det gäller information om behandlingens rättsliga grund, hur länge personuppgifterna kommer att lagras eller kriterier för att fastställa det, kategorier av mottagare av uppgifterna och den ytterligare information som det finns behov av. Det finns en möjlighet att begränsa denna rätt till information (artikel 13.3). Syftet med begränsningen ska vara att undvika att officiella eller rättsliga utredningar, förundersökningar eller förfaranden hindras eller att undvika menlig inverkan på brottsbekämpande åtgärder, lagföring eller verkställighet av straffrättsliga påföljder, att skydda allmän eller nationell säkerhet eller att skydda andra personers rättigheter och friheter. En begränsning får vidtas endast i den utsträckning och så länge som den är nödvändig och proportionell.

Den närmare innebörden av begränsningen till att information endast behöver lämnas i specifika fall framgår inte av direktivet. Utredningen om 2016 års dataskyddsdirektiv har diskuterat innebörden och ansett att det kan vara fråga om ett specifikt fall när den enskilde riskerar att lida rättsförlust om han eller hon inte får del av informationen eller när det av annat skäl är viktigt för honom eller henne att känna till behandlingen för att kunna ta till vara sina rättigheter. Utredningen har som exempel angett att personuppgifter har lämnats till fel mottagare och att det kan komma att medföra negativa konsekvenser för den registrerade. Enligt utredningen bör det för att informationsskyldigheten ska inträda normalt krävas att det är fråga om överträdelser av regelverket som kan föranleda skadeståndsansvar, allvarlig kritik eller ingripande från tillsynsmyndigheten eller någon liknande reaktion. Utredningen har uttalat att den personuppgiftsansvarige i de fallen bör informera den registrerade om vad som har hänt och vilka åtgärder som han eller hon kan vidta, t.ex. lämna in klagomål till tillsynsmyndigheten eller väcka talan om skadestånd.

Det saknas anledning att på kamerabevakningsområdet göra någon annan bedömning av den sistnämnda bestämmelsens innebörd än den som Utredningen om 2016 års dataskyddsdirektiv har gjort. Som nämnts ovan är det vid kamerabevakning i de flesta fall

omöjligt att informera om bevakningen i efterhand, eftersom någon identifiering av personerna oftast inte sker. I praktiken är det då omöjligt att informera personer som förekommer i bild- och ljudmaterial om ett ”specifikt fall” skulle uppkomma vid den efterföljande behandlingen av materialet. Mot denna bakgrund görs bedömningen att den nu diskuterade bestämmelsen om information i specifika fall i och för sig inte behöver genomföras genom kamerabevakningslagens bestämmelse om krav på upplysning vid kamerabevakning. Något hinder mot att så sker genom att upplysningskravet utformas så att sådana uppgifter ska lämnas på förhand på visst sätt finns dock inte.

I förordningen finns en bestämmelse som delvis motsvarar direktivets bestämmelse om allmän information (artikel 13.1). Enligt denna ska den personuppgiftsansvarige bl.a. lämna information till registrerade om sin identitet och sina kontaktuppgifter, om kontaktuppgifter till eventuellt dataskyddsombud samt om ändamålen med behandlingen.

Av förordningen följer att viss ytterligare information ska lämnas. En del av denna information är sådan som enligt direktivet endast ska lämnas i specifika fall. För viss information enligt förordningen anges att den ska lämnas när det krävs, vilket möjligen kan tolkas som att den bara ska lämnas när den behövs i det enskilda fallet. Som exempel på ytterligare information enligt förordningen kan nämnas uppgifter om mottagare eller kategorier av mottagare av personuppgifter, uppgifter om att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland eller en internationell organisation, uppgift om behandlingens rättsliga grund, hur länge uppgifterna ska lagras, rätten till tillgång till, rättelse av eller radering av personuppgifter eller begränsning av behandling och rätten att invända mot behandling, rätten till dataportabilitet samt rätten att återkalla samtycke och att inge klagomål till tillsynsmyndigheten. Av dessa uppgifter är det vissa som är särskilt viktiga vid kamerabevakning och för ett upplysningskrav som primärt gäller själva insamlingen av ett bildmaterial och, i förekommande fall, ljudmaterial.

Det svenska upplysningskravet ska lämpligen omfatta den information som avses i direktivets allmänna bestämmelse utom det som avser en senare behandling av material. Vidare ska kravet omfatta sådan information som i övrigt anges i förordningen och direktivet

och som är av relevans och är ändamålsenlig vid kamerabevakning. Information som bedöms sakna relevans eller vara praktiskt svår att lämna vid kamerabevakning ska inte omfattas. Detta innebär att upplysningskravet lämpligen ska omfatta följande.

Upplysning ska lämnas om *kamerabevakningen*, dvs. att platsen är kamerabevakad. Detsamma ska gälla *identiteten hos och kontaktuppgifterna till den som ska bedriva bevakningen*. Även upplysning om *kontaktuppgifter till ett dataskyddsombud*, om det finns ett sådant, ska lämnas. Liksom enligt kameraövervakningslagen ska *en särskild upplysning lämnas, om ljud kan avlyssnas eller tas upp vid bevakningen*. Ett krav på att de här upplysningarna lämnas säkerställer att den som kan bli kamerabevakad eller som kamerabevakas vet att bevakning sker och till vem han eller hon kan vända sig med frågor om bevakningen.

Vidare ska upplysningskravet omfatta information om *ändamålet med kamerabevakningen*. Lämpligen ska kravet därför även avse *den rättsliga grunden för bevakningen*. Information i dessa avseenden är en förutsättning för att enskilda ska kunna förstå om kamerabevakningen omfattas av tillståndskravet och om den utförs för ett berättigat ändamål. I de fall kamerabevakning enligt förordningen kan ske utan krav på tillstånd och efter en intresseavvägning får anges vilket intresse som motiverar kamerabevakningen i det enskilda fallet.

Information ska vidare lämnas om *hur länge upptaget bild- och ljudmaterial får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa detta*. Sådan information har större relevans än tidigare till följd av att det, som framgår nedan, inte ska finnas någon bestämd tid i kamerabevakningslagen för hur länge bild- och ljudmaterial som spelats in får behandlas. Enligt kameraövervakningslagen är tiden i dag begränsad till två månader på platser som allmänheten har tillträde till. Vidare kommer tillsynsmyndigheten, till följd av att tillståndskravet ska omfatta endast vissa aktörer, i många fall inte att i förväg granska tiden för hur länge material ska behandlas. Utan ett krav på att information ska lämnas om hur länge upptaget material får behandlas skulle enskildas möjligheter att få reda på detta, och om inspelning överhuvudtaget sker, avsevärt försvåras.

Slutligen ska upplysningskravet även innefatta information om *möjligheten att lämna in klagomål till tillsynsmyndigheten och kon-*

taktuppgifterna till den. En större andel än tidigare av den kamerabevakning som bedrivs kommer att ske såväl tillståndsfritt som anmälningsfritt. Det innebär att en effektiv tillsyn i ökad utsträckning kommer att förutsätta att enskilda uppmärksammar tillsynsmyndigheten på kamerabevakning som inte uppfyller de krav som följer av kamerabevakningslagen.

Den information som upplysningskravet föreslås innehålla är i vissa avseenden mer omfattande än vad direktivets bestämmelser kräver. Direktivet hindrar inte att det i svensk rätt föreskrivs ett starkare skydd än vad som följer av det. Upplysningskravet innebär vidare att förordningens bestämmelser delvis upprepas i den svenska bestämmelsen. Detta bedöms vara förenligt med förordningen, eftersom det är fråga om dels en begränsning av förordningens bestämmelser, dels en upprepning som gör den svenska bestämmelsen tydlig och begriplig.

När det sedan gäller sättet för upplysning anges i dag i kameraövervakningslagen att upplysning ska lämnas genom tydlig skyltning eller på något annat verksamt sätt. Det har i den kartläggning och utvärdering av lagen som gjorts och redovisats i avsnitt 5 inte framkommit att det funnits några generella problem när det gäller utformningen av upplysningsplikten i denna del. Kamerabevakningslagens upplysningskrav bör därför såvitt avser vissa av upplysningarna utformas med denna som förebild men med en viss förstärkning, som också tydligt kan markera att vad gäller övriga upplysningar kan de lämnas på annat sätt.

Det föreslås att det *genom tydlig skyltning eller på något annat liknande verksamt sätt* ska lämnas upplysning om kamerabevakningen, identiteten hos och kontaktuppgifterna till den som ska bedriva bevakningen och kontaktuppgifter till ett eventuellt dataskyddsombud. Om ljud kan avlyssnas eller tas upp vid bevakningen, ska – på samma sätt – lämnas en särskild upplysning om detta.

Den ytterligare information som ska lämnas vid kamerabevakning är inte av lika omedelbart intresse för dem som kan bli bevakade som upplysningarna om att platsen är kamerabevakad och om vem som bedriver bevakningen. Vidare kan skyltning på platsen förväntas bli ett vanligt sätt att uppfylla upplysningskravet på. Som nämnts ovan kan en stor mängd information på en skylt vara svår för enskilda att tillgodogöra sig snabbt och enkelt. Det föreslås därför att denna information ska *göras tillgänglig för dem som kan bli*

kamerabevakade. Det innebär att informationen t.ex. kan tillhandahållas på en webbsida dit man kan söka sig genom de kontaktuppgifter till den som bedriver bevakningen som det ska upplysas om. Denna reglering får anses såväl lämplig som förenlig med EU-regleringen.

För att upplysningar om kamerabevakning från rörliga objekt ska vara verksamma kan de givetvis lämnas genom skyltning, t.ex. vid vägar eller stigar som leder in till det område som ska bevakas eller i form av klisterlappar på fordon i vägtrafik. I de fall det är ett särskilt evenemang som ska bevakas, t.ex. en festival i ett parkområde, kan skyltning kombineras med upplysningar som lämnas i programblad eller liknande material.

När ska upplysningskravet inträda?

Upplysningsplikten enligt kameraövervakningslagen inträder när övervakningsutrustningen sätts upp. Att upplysningsplikten börjar gälla vid denna tidpunkt är en följd av hur kameraövervakningslagens generella tillämpningsområde har utformats. Lagen gäller när utrustningen är uppsatt så att den kan användas för personövervakning.

I avsnitt 10.2 har föreslagits att kamerabevakningslagens tillämpningsområde ska utformas så att lagen gäller när kamerabevakning sker, dvs. när den utrustning som omfattas av lagen används. I linje med det förslaget ska upplysningskravet inträda när kamerabevakningen sker. I praktiken innebär det att upplysningarna och informationen måste lämnas innan kameran eller utrustningen används.

En skillnad jämfört med nuvarande reglering blir alltså att upplysningskravet inte gäller när en kamera inte används. För att tillsynsåtgärder ska kunna vidtas mot någon som inte uppfyller upplysningskravet kommer det därmed att krävas bevisning om att kameran har använts. Skillnaden kan dock inte förutses leda till några ohanterliga praktiska problem vid sådan kamerabevakning som ska omfattas av kamerabevakningslagen. Samma tidpunkt för informationsskyldighetens inträde gäller för övrigt för annan kameraanvändning och för övrig personuppgiftsbehandling som helt regleras av förordningen eller brottsdatalagen.

Vem ska omfattas av upplysningskravet?

Upplysningskravet ska gälla för den som bedriver kamerabevakning. Detta är en skillnad mot vad som gäller enligt kameraövervakningslagen där upplysningsplikten riktar sig mot såväl den som bedriver kamerabevakning som den som har en övervakningskamera uppsatt (prop. 1989/90:119 s. 41 f.). Skillnaden är en naturlig följd av att kamerabevakningslagen föreslås gälla först när kamerabevakning sker och inte redan när utrustningen sätts upp. Upplysningskravet i kamerabevakningslagen kan då inte rikta sig mot någon annan än den som bedriver kamerabevakning.

12.2 Undantag från upplysningskravet

Förslag: Upplysning om kamerabevakning ska inte behöva lämnas vid

1. bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning,
2. bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet som innebär fara för liv eller hälsa eller för omfattande förstörelse av egendom på en viss plats och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott,
3. bevakning som sker för att skydda en byggnad, en annan anläggning eller ett område som enligt 4 § 4, 5 § 1–4 eller 6 § första stycket skyddslagen (2010:305) har förklarats vara skyddsobjekt, om bevakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet,

4. bevakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning,
5. bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller den som är räddningsledare enligt lagen (2003:778) om skydd mot olyckor, om bevakningen är av vikt för att avvärja en hotande olycka eller begränsa verkningarna av en inträffad olycka, och
6. bevakning som bedrivs av den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att efterforska en försvunnen person.

Undantaget i punkten 3 ska inte gälla för sådana byggnader, andra anläggningar eller områden som används för eller är avsedda för fredstida krishantering enligt 4 § 4 skyddslagen.

Undantagen ska inte gälla, om ljud ska avlyssnas eller tas upp vid kamerabevakningen.

Om det finns synnerliga skäl, ska tillsynsmyndigheten få besluta om undantag från upplysningskravet i enskilda fall. En ansökan om undantag ska vara skriftlig. Den kommun där kamerabevakningen ska ske ska få tillfälle att yttra sig före ett beslut om undantag, om bevakningen ska avse en plats dit allmänheten har tillträde och det behövs ett yttrande. Ett beslut om undantag ska förenas med de villkor som behövs. Om förutsättningarna för ett beslut om undantag ändras, får beslutet ändras eller, om förutsättningarna för ett sådant beslut inte längre är uppfyllda, detta återkallas.

Skälen för förslaget

Inledning

Kameraövervakningslagen innehåller bestämmelser om undantag från lagens upplysningsplikt i vissa fall. Undantagen gäller vid automatisk hastighetsövervakning som Polismyndigheten bedriver, övervakning av vissa skyddsobjekt, viss övervakning som Försvarsmakten bedriver och viss övervakning för att efterforska försvunna

personer. Om det finns synnerliga skäl, får länsstyrelsen i andra fall besluta om undantag från upplysningsplikten.

Som utgångspunkt ska gälla att undantagen bör behållas. De skäl som en gång motiverat att undantagen införts måste fortfarande antas göra sig gällande. Som framgått av föregående avsnitt finns det ett visst utrymme att i nationell rätt avvika från EU-regleringens bestämmelser om rätten till information. Nedan prövas också om det är möjligt att utan åberopande av detta utrymme behålla undantagen. Det görs där en bedömning för vart och ett av dagens undantag om undantaget är förenligt med EU-regleringen och lämnas förslag till om det ska tas in i kamerabevakningslagen och, i så fall, i vilken form.

Dessutom diskuteras om det bör införas ytterligare undantag från upplysningskravet dels vid kamerabevakning som är av vikt för att avvärja en hotande olycka eller för att begränsa verkningarna av en inträffad olycka, dels vid kamerabevakning som Polismyndigheten eller Säkerhetspolisen bedriver när det finns risk för viss allvarlig brottslighet.

Bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning

Kamerabevakning som bedrivs av Polismyndigheten vid automatisk hastighetsövervakning utförs i en verksamhet som består i brottsbekämpning och lagföring. Direktivet gäller därför när personuppgifter behandlas som en del av bevakningen.

Vid sådan kamerabevakning samlas det endast in uppgifter när ett fordon har överskridit gällande hastighetsbegränsning. Uppgifterna används i en påföljande brottsutredning. I en sådan utredning gäller bestämmelserna om förundersökning i rättegångsbalken. Dessa bestämmelser innehåller krav på att den som skäligen misstänks för brottet ska underrättas om misstanken och, i den mån det kan ske utan men för utredningen, få ta del av det som har förekommit vid undersökningen.

Vid den kamerabevakning som sker vid automatisk hastighetsövervakning är det alltså fråga om behandling av personuppgifter som ingår i ett ärende i samband med brottsutredning. För sådan behandling får enligt direktivet föreskrivas att rätten till information ska utövas i enlighet med medlemsstatens nationella rätt. Som

framgått kommer information om kamerabevakningen att ges till den som blivit föremål för sådan bevakning genom de bestämmelser som reglerar förundersökningen. Undantaget från upplysningskravet vid bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning bedöms med hänsyn härtill vara förenligt med EU-regleringen. Vidare framstår undantaget som lämpligt att behålla. Det ska därför införas i kamerabevakningslagen.

Bevakning av skyddsobjekt

Kameraövervakning som sker för att skydda vissa byggnader, andra anläggningar eller områden som enligt skyddslagen (2010:305) har förklarats vara skyddsobjekt är i kameraövervakningslagen undantagen från upplysningsplikten. De skyddsobjekt som omfattas av undantaget är av olika karaktär. Det är i stor utsträckning fråga om objekt som är av betydelse för försvarets verksamhet men även anläggningar och områden som är avsedda för civila ändamål, t.ex. energiförsörjning, vattenförsörjning, elektroniska kommunikationer och transporter, omfattas.

Avsikten med skyddslagen är att ge skydd mot säkerhetshotande verksamhet (prop. 2009/10:87 s. 25). Ursprungligen avsåg regleringen om skyddsobjekt främst militär verksamhet men med tiden har allt fler civila samhällsfunktioner kommit att omfattas. Det är övergripande fråga om att skydda samhället mot risker och påfrestningar på grundläggande samhällsfunktioner. Syftet med ett beslut om att en byggnad eller annan anläggning eller ett område eller annat objekt ska utgöra ett skyddsobjekt är att förstärka skyddet mot sabotage, terroristbrott, spionerі eller röjande i andra fall av hemliga uppgifter som rör totalförsvaret och grovt rån. Syftet kan också vara att skydda allmänheten mot skada som kan uppkomma till följd av militär verksamhet.

Förordningen och direktivet omfattar inte behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten. Enligt skälen till förordningen och direktivet innebär detta att verksamhet som avser *nationell säkerhet* faller utanför regleringen.

Begreppet förekommer inte i den svenska versionen av 1995 års dataskyddsdirektiv; däremot förekommer begreppet *national security*

i den engelska versionen av direktivet. I den svenska versionen används i stället *statens säkerhet* medan *rikets säkerhet* används i personuppgiftslagen. Av kommissionens förklaring till 1995 års direktiv framgår att begreppet national security är avsett att omfatta skydd av den nationella suveräniteten mot såväl interna som externa hot (jfr SOU 1993:10, bil. s. 184). I den svenska versionen av dataskyddsrambeslutet, som nu ersätts av det nya direktivet, förekommer begreppet *nationell säkerhet*. I den engelska versionen används *national security*. Vid genomförandet av rambeslutet uttalade regeringen att begreppet *rikets säkerhet* torde vara snävare än begreppet *nationell säkerhet* (prop. 2012/13:73 s. 68 ff.). I det betänkande som föregick propositionen angavs att en central och allmän utgångspunkt vid bedömningen av om en verksamhet påverkar den nationella säkerheten eller inte är huruvida det i en viss situation finns en otillåten påverkan på det demokratiska statsskicket eller en kapacitet att hota en viktig samhällsfunktion (SOU 2011:20 s. 221 ff.).

När det gäller begreppet nationell säkerhet i den nya förordningen har Dataskyddsutredningen inte närmare analyserat innebörden av detta men uttalat att det är rimligt att anta att det inom offentlig sektor finns även annan verksamhet än den som avser nationell säkerhet som kan falla utanför unionsrätten. Utredningen har också diskuterat förordningens undantag för behandling av personuppgifter i verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken. Utredningen har föreslagit att förordningen genom dataskyddslagen – i de delar där det är möjligt – ska utsträckas till att gälla även personuppgiftsbehandling i verksamheter inom dessa områden. På direktivets område har Utredningen om 2016 års dataskyddsdirektiv uttalat att till nationell säkerhet hör Säkerhetspolisens uppgifter att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet och terroristbrott och att utreda och beivra sådana brott samt att ansvara för personskyddet av den centrala statsledningen.

Begreppet nationell säkerhet måste alltså anses vara vidare än begreppet rikets säkerhet. Den exakta gränsen mellan vad som avser nationell säkerhet och vad som inte gör det är dock svår att dra. Vad gäller just skyddsobjekt skulle å ena sidan kunna hävdas att all verksamhet i eller vid sådana objekt har att göra med nationell säkerhet, eftersom syftet med att göra dem till skyddsobjekt är att skydda grundläggande samhällsfunktioner. Å andra sidan måste invändas

att det är tveksamt att anlägga ett sådant strikt svenskt synsätt i detta sammanhang; det har knappast varit avsikten med förordningen att personuppgiftsbehandling som sker i verksamheter som avser t.ex. transporter ska falla utanför förordningens tillämpningsområde. Alla objekt som avser transporter utgör inte heller skyddsobjekt, vilket ytterligare illustrerar gränsdragningssvårigheterna.

Såvitt avser kamerabevakning innebär det sagda att undantag från kravet på upplysning om sådan bevakning kan föreskrivas i kamerabevakningslagen utan hinder av EU-regleringen så länge det handlar om bevakning i verksamhet som avser nationell säkerhet. Personuppgiftsbehandling i sådan verksamhet faller utanför EU-regleringen och kan regleras fritt i svensk rätt, även om Dataskyddsutredningen har föreslagit att förordningen ska göras tillämplig även på sådan behandling. Många av de situationer av kamerabevakning där upplysning om bevakningen i dag inte behöver lämnas därför att bevakningen avser skyddsobjekt måste – även med beaktande av den osäkerhet som råder om innebörden av begreppet nationell säkerhet – anses vara sådana som faller utanför unionsrätten. De övriga situationerna får under alla förhållanden anses rymmas inom den möjlighet till nationella undantag från rätten till information som finns enligt EU-regleringen. Dagens undantag från upplysningsplikten är alltså förenliga med EU-regleringen och är också lämpliga att behålla framöver. Det föreslås därför att undantagen införs i kamerabevakningslagen.

Bevakning som Försvarsmakten bedriver i vissa fall

Från upplysningsplikten i kameraövervakningslagen undantas i dag också övervakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan övervakning.

Som framgått ovan faller personuppgiftsbehandling och kamerabevakning i Försvarsmaktens verksamhet i regel utanför EU-regleringen, eftersom verksamheten avser nationell säkerhet. EU-regleringen hindrar därför inte att undantaget från upplysningskravet behålls. Vidare framstår undantaget fortfarande som motiverat.

Det föreslås därför att ett sådant undantag tas in i kamerabevakningslagen.

Bevakning för efterforskning av försvunna personer

Undantaget från upplysningsplikten i kameraövervakningslagen för övervakning som är av vikt för att efterforska en försvunnen person har motiverats av att det sällan är möjligt att på ett verksamt sätt upplysa om övervakningen. Det beror dels på den skyndsamhet som måste iakttas vid insatser av detta slag, dels att övervakningen kan omfatta stora geografiska områden (prop. 2012/13:115 s. 57).

Detta undantag från upplysningskravet avser alltså en speciell situation av kamerabevakning med i normalfallet begränsade risker för integriteten som står mot intresset av att finna en saknad person. Med hänsyn härtill och med åberopande av det utrymme till undantag från EU-regleringen som tidigare konstaterats finnas görs bedömningen att ett fortsatt undantag kan förenas med den regleringen. Ett sådant föreslås därför i kamerabevakningslagen.

Bevakning vid en hotande eller inträffad olycka

I avsnitt 11 har föreslagits att kamerabevakning ska få ske under högst en månad utan att en ansökan om tillstånd har gjorts vid bevakning som bedrivs av Polismyndigheten eller den som är räddningsledare enligt lagen (2003:778) om skydd mot olyckor, om bevakningen är av vikt för att avvärja en hotande olycka eller begränsa verkningarna av en inträffad olycka.

Bestämmelsen är främst avsedd att komma till användning i anslutning till att avspärrning har skett på grund av en olycka, en katastrof eller någon annan nödfallsliknande situation (prop. 1997/98:64 s. 56 och 2012/13:115 s. 56). När kameraövervakningslagen infördes diskuterades om bestämmelsen kunde omfatta situationer där det fanns behov av kameraövervakning för att efterforska försvunna personer. Slutsatsen blev att så ofta inte var fallet och därför infördes ett särskilt tillfälligt undantag från tillståndsplikten för den situationen. Som framgått ovan undantogs den situationen också från kameraövervakningslagens upplysningsplikt och ska den även vara undantagen från den nya lagens upplysningskrav.

Vid hotande eller inträffade olyckor finns det i regel behov av att snabbt kunna få en överblick av olycksområdet. Ibland kan detta vara förhållandevis enkelt att få, i andra fall svårare exempelvis p.g.a. omfattningen av den hotande eller inträffade olyckan och det sammanhang i vilket den riskerar att inträffa respektive har inträffat. Som exempel på det senare kan nämnas en inträffad olycka vid en större anläggning där den bedrivna verksamheten är sådan att olyckan kan orsaka allvarliga skador på många människor eller på miljön. I sådana sammanhang kan främst kamerautrustade drönare eller kameror på eller i andra luftfartyg utgöra användbara hjälpmedel. Det kan i de fallen med hänsyn till behovet av skyndsamhet och det olycksdrabbade områdets storlek vara svårt att åtminstone inledningsvis uppfylla upplysningskravet i kamerabevakningslagen, förutsatt att kameraanvändningen omfattas av lagen. Samtidigt får intresset hos de enskilda som kan bli föremål för bevakningen att bli upplysta om denna anses väga mindre tungt än annars. Det kan också antas att dylika situationer utgör en mindre del av samtliga de olyckssituationer där kamerabevakning kan behövas och dessutom avser ett avgränsat antal människor och en tid som är begränsad till ett akut inledningsskede. I dessa fall bör, förutsatt att kamerabevakningen behöver fortsätta, kunna ställas krav på att upplysningskravet iakttas så snart som möjligt. I den mån detta av praktiska skäl är omöjligt kan en möjlighet till undantag från upplysningskravet i det enskilda fallet finnas enligt vad som föreslås nedan. Som regel torde dock en fortsatt kamerabevakning efter det första akuta skedet kunna anordnas för mer avgränsade områden med upplysning om bevakningen alternativt torde det saknas behov av fortsatt bevakning. I normalfallen där en avspärrning kan ske direkt ska upplysningskravet liksom tidigare uppfyllas samtidigt. Följaktligen finns det ett visst behov av ett undantag från upplysningskravet vid sådan kamerabevakning som sker för att avvärja en hotande olycka eller begränsa verkningarna av en inträffad olycka.

Ett sådant undantag avser en speciell situation av kamerabevakning med relativt begränsade risker för integriteten som står mot intresset av att avvärja en hotande olycka eller begränsa verkningarna av en inträffad olycka. Med hänsyn härtill och med åberopande av det utrymme till undantag från EU-regleringen som ovan

konstaterats finnas görs bedömningen att ett undantag kan förenas med den regleringen.

Mot denna bakgrund föreslås ett begränsat undantag från upplysningskravet vid sådan kamerabevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att avvärja en hotande olycka eller begränsa verkningarna av en inträffad olycka.

Bevakning som Polismyndigheten eller Säkerhetspolisen bedriver vid risk för viss allvarlig brottslighet

I kameraövervakningslagen finns ett tillfälligt undantag från tillståndsplikten vad avser viss kameraövervakning i Polismyndighetens och Säkerhetspolisens brottsbekämpande verksamhet. Enligt detta undantag får kameraövervakning bedrivas av dessa myndigheter under högst en månad utan att tillstånd har sökts, om det av särskild anledning finns risk för att allvarlig brottslighet som innebär fara för liv eller hälsa eller för omfattande förstörelse av egendom kommer att utövas på en viss plats och syftet med övervakningen är att förebygga eller förhindra brott. Om en ansökan om tillstånd görs inom en månad från det att kameraövervakningen inleddes, får den bedrivas utan tillstånd till dess att ansökningen har prövats. I avsnitt 11 har föreslagits att i huvudsak samma undantag från tillståndskravet ska finnas i kamerabevakningslagen.

Kamerabevakning som enligt detta undantag får bedrivas utan tillstånd omfattas i dag inte av ett motsvarande undantag från upplysningsplikten i kameraövervakningslagen. Med hänsyn till förändringar i brottsligheten och den teknikutveckling som skett, framför allt när det gäller möjligheten att bedriva kamerabevakning från drönare, finns det situationer där det framstår som motiverat att polisen ska kunna använda kameror som manövreras på avstånd utan att upplysning om användningen lämnas. Det handlar främst om situationer där det är mycket brådskande att använda en kamera och upplysning inte hinner lämnas.

Frågan om kameraanvändning av polisen utan upplysning med stöd i den lagstiftning som är aktuell i detta lagstiftningsärende är komplicerad. Detta har berörts redan ovan. Frågan har också varit föremål för diskussion i tidigare lagstiftningssammanhang, senast

i samband med införandet av kameraövervakningslagen i anslutning till en diskussion om undantag i enskilda fall från den lagens upplysningsplikt (a. prop. s. 88 ff.). Regeringen redogjorde där för att möjligheterna att använda hemlig kameraövervakning utvidgats sedan kameraövervakningslagens föregångare, lagen om allmän kameraövervakning, tillkommit. Därefter underströk regeringen att möjligheten till undantag från upplysningsplikten enligt kameraövervakningslagen inte är avsedd att användas på ett sätt som innebär en utvidgning av reglerna om hemlig kameraövervakning i tvångsmedelslagstiftningen (jfr prop. 1997/98:64 s. 25). Enligt regeringen borde därför kravet på synnerliga skäl för att medge undantag från upplysningsplikten inte kunna anses uppfyllt vid sådan övervakning som en polismyndighet bedriver utan tillstånd när det av särskild anledning finns risk för viss allvarlig brottslighet. Dessutom uttalade regeringen att det inte fanns skäl att inom ramen för kameraövervakningslagstiftningen införa en utvidgad möjlighet för de brottsbekämpande myndigheterna att använda dold övervakning utan prövning i det enskilda fallet.

Den lagstiftning om hemlig kameraövervakning som regeringen redogjorde för har därefter ändrats ytterligare.

Enligt rättegångsbalken får sådan övervakning användas vid förundersökning om 1) brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, 2) bl.a. sabotage, grovt sabotage, mordbrand, grov mordbrand, allmänfarlig ödeläggelse, uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet, högförräderi, krigsanstiftan, spionerі, grovt spionerі, olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person samt terroristbrott, brott enligt 3 eller 3 a § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller brott enligt lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet, 3) försök, förberedelse eller stämpling till de brott som avses i 1) eller 2), om en sådan gärning är belagd med straff och 4) annat brott när det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år. Hemlig kameraövervakning får användas när någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Åtgärden får då avse en sådan plats där den misstänkte kan antas komma att uppehålla sig. Om det inte finns någon som är skäligen

misstänkt för brottet, får hemlig kameraövervakning även användas för att övervaka den plats där brottet har begåtts eller en nära omgivning till denna plats. Sådan övervakning får ske, om syftet är att fastställa vem som skäligen kan misstänkas för brottet och åtgärden är av synnerlig vikt för utredningen.

Enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott får hemlig kameraövervakning användas när det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva viss brottslig verksamhet. Det gäller bl.a. sabotage, grovt sabotage, mordbrand, grov mordbrand, allmänfarlig ödeläggelse, uppror, väpnat hot mot laglig ordning, brott mot medborgerlig frihet, högförräderi, krigsanstiftan, spionerі, grovt spionerі, grov olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person, terroristbrott, grovt brott enligt 3 § andra stycket lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller grovt brott enligt 6 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet samt mord, dråp, grov misshandel, människorov eller olaga frihetsberövande i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd. Övervakning kan också ske när det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas brottslig verksamhet av det uppräknade slaget och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet. Hemlig kameraövervakning får avse en plats där personen kan antas komma att uppehålla sig eller en plats där den brottsliga verksamheten kan antas komma att utövas eller en nära omgivning till denna plats. Åtgärden ska vara av synnerlig vikt för att förhindra den brottsliga verksamheten och skälen för åtgärden måste uppväga det intrång eller men i övrigt som åtgärden innebär för den berörde eller för något annat motstående intresse.

Allmän domstol prövar om hemlig kameraövervakning ska få ske. I brådskande fall får en åklagare besluta om övervakning i avvaktan på domstolens beslut. Förfarandet vid hemlig kameraövervakning är kringgärdat av vissa rättssäkerhetsgarantier som inte har

några motsvarigheter i kameraövervakningslagen och inte heller kommer att ha det i den nya lagen.

Det är självfallet så att polisen har berättigade behov av att i vissa situationer använda sig av kameror utan att upplysning om detta bör eller kan lämnas, behov som i sin tur tjänar det samhälleliga intresset av att brott kan bekämpas på ett effektivt sätt.

Den rätta vägen att tillgodose dessa behov är dock, med hänsyn till den nu beskrivna bakgrunden, inte i första hand att genom kamerabevakningslagen öka möjligheten att bedriva dold kamerabevakning. Därigenom skulle nämligen den särskilda lagstiftning som annars gäller för polisens dolda kameraövervakning frångås. Förfarandet vid hemlig kameraövervakning är kringgärdat av striktare rättssäkerhetsgarantier än övervakning utan upplysning enligt kameraövervakningslagen och än vad som blir fallet för kamerabevakning enligt kamerabevakningslagen.

Till detta kommer att polisens kameraanvändning i de situationer som nu diskuteras typiskt sett – och till skillnad mot de fall som diskuterats i avsnitten ovan – avser miljöer som är särskilt integritetskänsliga därför att många människor befinner sig där och dessutom har som direkt syfte att kontrollera vissa av dessa människors förehavanden.

En av grundpelarna i kameraövervakningslagen och dess föregångare liksom i den nya lagen är att den lagstiftningen reglerar användning av öppen kamerabevakning i samhället. Dold kamerabevakning enligt den lagen ska i princip inte förekomma. Stor restriktivitet ska därför råda när det gäller att göra undantag från denna grundläggande princip. Den nya EU-regleringen innebär också nya krav på information som gör det svårt att avstå från att åtminstone allmänt informera om kamerabevakning. Det gäller även för de brottsbekämpande myndigheterna. Detta hindrar inte att det på just det område som gäller brottsbekämpning noga övervägs och i annan lagstiftning regleras att användning av kameror får ske utan att det informeras om denna, såsom också skett genom bestämmelserna i rättegångsbalken och den nämnda lagen.

Det är vidare svårt att se att ett undantag från upplysningskravet i kamerabevakningslagen skulle ha något påtagligt praktiskt mervärde jämfört med vad som redan gäller enligt den lagstiftning som direkt reglerar dold övervakning. Den senare tar sikte på i huvudsak samma typer av brott som omfattas av undantaget från till-

ståndskravet enligt kamerabevakningslagen och kan användas både innan brottsligheten har begåtts och i förundersökningssituationer. Dessutom ger den lagstiftningen möjlighet till snabba beslut om tillstånd genom att åklagare, som alltid går att nå p.g.a. av jourtjänstgöring, kan fatta sådana i avvaktan på domstolsprövning av frågan.

Med detta sagt får det likväl anses finnas ett starkt behov för polisen av att utan upplysning kunna bedriva kamerabevakning i vissa i dag oreglerade fall som bör tillgodoses så snart som möjligt. Det bör kunna ske i kamerabevakningslagen förutsatt att undantaget begränsas till vissa situationer och att dessa ringas in så långt som möjligt. Polisens behov därutöver kan förtjäna att övervägas i annat sammanhang utifrån den särskilda reglering som gäller för hemlig kameraövervakning. Det ligger dock utanför detta utredningsuppdrag.

De situationer som avses gäller de mer akuta fall med risk för allvarlig brottslighet som är undantagna från kravet på tillstånd till kamerabevakning. Vidare gäller det när det i dessa situationer är brådskande att påbörja kamerabevakningen samtidigt som förhållandena är sådana att det inte är praktiskt möjligt att direkt uppfylla kravet på upplysning. Så är i regel fallet när bevakningen ska ske från drönare eller annars från luften, dvs. med luftfartyg.

Det gäller däremot inte när bevakningen ska ske från rörliga objekt på marken, t.ex. fordon. Då är en upplysning möjlig att lämna på objektet, exempelvis genom en klisterlapp. Det gäller inte heller kamerabevakning från fasta objekt, som ju avser en avgränsad geografisk plats. Vidare gäller det inte situationer som inte är brådskande.

I de brådskande situationerna torde efter den första akuta inledningsfasen – förutsatt att kamerabevakningen då behöver fortsätta – upplysningskravet många gånger gå att uppfylla antingen därför att en skyltning eller motsvarande kan åstadkommas med lite tid för detta eller därför att kamerabevakningen kan anordnas på annat sätt, t.ex. från ett fast objekt eller fortsatt från luften men avseende ett mer begränsat område än tidigare. För det fall bevakningen behöver fortsätta och det är praktiskt omöjligt att ens då uppfylla upplysningskravet ska, som föreslås nedan, det finnas en möjlighet att ansöka om undantag från kravet hos tillsynsmyndigheten. Undantagsmöjligheten ska visserligen tillämpas med särskilt stor restriktivitet när det gäller polisen men helt utesluter

den inte att undantag kan meddelas. Det får överlämnas åt rättstillämpningen att avgöra de eventuella sådana fall som kan uppkomma.

Ett sådant undantag från upplysningskravet får anses förenligt med dataskyddsdirektivet. Direktivet innebär ett krav på att viss allmän information ska göras tillgänglig för registrerade. Utredningen om 2016 års dataskyddsdirektiv har föreslagit att kravet genomförs genom en bestämmelse i brottsdatalagen. Information som lämnas generellt för personuppgiftsbehandling enligt den bestämmelsen kan då gälla även i den angivna undantagssituationen genom den i avsnitt 10.1 föreslagna bestämmelsen om hur kamerabevakningslagen förhåller sig till andra bestämmelser.

Sammanfattningsvis föreslås att ett begränsat undantag från upplysningskravet ska gälla för sådan kamerabevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet som innebär fara för liv eller hälsa eller för omfattande förstörelse av egendom på en viss plats och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott.

Undantag i enskilda fall

Bestämmelsen om undantag i enskilda fall från upplysningsplikten i kameraövervakningslagen när det föreligger synnerliga skäl är avsedd att tillämpas restriktivt. I förarbetena (prop. 2012/13:115 s. 89 ff.) har som exempel på när undantag kan beslutas angetts övervakning av rovdjurslyor i syfte att upptäcka och beivra tjuvskytte och plundring samt för att kartlägga rovdjurens bestånd. Det har alltså ansetts viktigt att kunna bedriva kamerabevakning för viltvårds- och artskyddsändamål utan att t.ex. rovdjurslyors lägen avslöjas, eftersom syftet med bevakningen då förfelas. I förarbetena har också uttalats att det kan förekomma angelägna behov av undantag även i andra fall. Det kan t.ex. röra sig om fall där det inte är möjligt att på ett verkningsfullt sätt upplysa om övervakningen. Enligt uppgift från Datainspektionen har undantag medgetts, förutom vid bevakning av utrotningshotade djurarter, i fall där varor i butiker utsatts för hälsofarligt sabotage.

Undantaget från upplysningsplikten när det föreligger synnerliga skäl bedöms fylla en viktig funktion. En motsvarande möjlighet till undantag från kamerabevakningslagens upplysningskrav är alltså sakligt motiverad. Det är dessutom så att det numera kan vara rimligt att göra avsteg från upplysningskravet i en något högre utsträckning än vad som hittills varit möjligt, eftersom kravet kan vara praktiskt omöjligt att uppfylla. Inte minst den tekniska utvecklingen har bidragit till detta. Exempelvis kan kamerabevakning från rörliga objekt, t.ex. drönare, avse stora områden som skiftar från gång till annan. När sådan bevakning sker för ett berättigat och starkt intresse, exempelvis i räddningsverksamhet som bedrivs av en frivilligorganisation, samtidigt som de motstående integritetsaspekterna inte gör sig gällande med någon större tyngd får en något mer tillåtande praxis i fråga om undantag från upplysningskravet anses befogad. Det skulle kunna åstadkommas genom att det i stället för synnerliga skäl uppställs ett krav på särskilda skäl för att undantag ska medges. Emellertid har i praxis synnerliga skäl ansetts föreligga i just en sådan situation. Den eftersträvade praxisförskjutningen torde alltså kunna uppnås utan en ändring av bestämmelsen. Det får anses gälla även för de begränsade situationer som berörts i de två närmast föregående avsnitten och där ett undantag eventuellt kan komma i fråga. Med hänsyn härtill och eftersom en sådan ändrad bestämmelse kan riskera att öppna upp för en alltför generös tillämpning, bör ett krav på synnerliga skäl gälla.

Frågan är då om en undantagsmöjlighet av detta slag är förenlig med EU-regleringen. Möjligheten skulle visserligen vara generellt utformad. Emellertid skulle möjligheten vara begränsad på de sätten att det krävs ett beslut om undantag i det enskilda fallet och att det krävs synnerliga skäl för att undantag ska medges. Det innebär att en restriktivitet ska prägla prövningen. Till detta kommer att tillsynen nedan föreslås samlas hos en enda tillsynsmyndighet, Datainspektionen, vilket innebär garantier för såväl en restriktiv och enhetlig tillämpning av undantagsmöjligheten som en prövning där myndigheten beaktar de begränsningar som följer av EU-regleringen. Det bedöms därför vara förenligt med EU-regleringen att införa en bestämmelse i kamerabevakningslagen som ger tillsynsmyndigheten möjlighet att besluta om undantag från upplysningskravet i enskilda fall, om det finns synnerliga skäl. Följaktligen föreslås att en sådan bestämmelse införs.

Ska undantagen gälla även då ljud ska avlyssnas eller tas upp?

Kamerabevakning som innefattar avlyssning och upptagning av ljud innebär i regel särskilt påtagliga integritetsrisker, eftersom det normalt inte finns anledning att förvänta sig att utomstående ska ta del av vad man säger även om man befinner sig i en offentlig miljö. I kamerabevakningslagen ska det därför på samma sätt som i kameraövervakningslagen föreskrivas att de generella undantag från upplysningskravet som föreslagits ovan inte ska gälla, om ljud ska avlyssnas eller tas upp vid kamerabevakningen.

I kameraövervakningslagen gäller inte heller undantaget från upplysningsplikten i enskilda fall vid synnerliga skäl, om ljud ska avlyssnas eller tas upp vid bevakningen. Det har framkommit att detta försvårar bevakning som sker för att kartlägga bestånd av hotade rovdjur. Vid sådana kartläggningar görs bl.a. undersökningar av föryngringen av rovdjursstammen och en möjlighet att registrera ljudet från rovdjursungarna är då ofta en förutsättning för att en bedömning av föryngringen ska vara möjlig. Det förekommer alltså situationer där kamerabevakning för ett starkt berättigat intresse måste ske med avlyssning eller upptagning av ljud utan upplysning för att bevakningen ska kunna fylla sitt syfte.

En undantagsmöjlighet för sådana och liknande fall skulle innebära ett frångående av den princip som hittills gällt och som innebär att upplysningskravet bör vara ovillkorligt när det gäller avlyssning eller upptagning av ljud. Det är emellertid fråga om situationer där riskerna för integriteten är mycket begränsade. Vidare skulle tillsynsmyndigheten råda över en sådan möjlighet; ett undantag från upplysningskravet skulle kräva ett beslut av tillsynsmyndigheten. Ett sådant beslut skulle, med hänsyn till kravet på synnerliga skäl, endast komma i fråga i undantagsfall där intresset av avlyssning eller upptagning av ljud utan upplysning är berättigat och väger tungt samtidigt som intresset av integritetsskydd är marginellt.

Mot denna bakgrund föreslås att undantag från upplysningskravet i enskilda fall ska få göras också när ljud ska avlyssnas eller tas upp vid kamerabevakningen.

Förfarandet för undantag i enskilda fall

När det gäller förfarandet i ärenden om undantag från upplysningskravet i enskilda fall finns naturligen inte några bestämmelser om detta i förordningen eller direktivet. Bestämmelser om förfarandet måste tas in i kamerabevakningslagen. Dessa måste utformas så att de övergripande sett är förenliga med EU-regleringen. Som framgått lämnar både förordningen och direktivet utrymme bl.a. för att sanktioner föreskrivs i nationell rätt. En form av sanktion är återkallelse av ett positivt beslut.

I dag föreskrivs i kameraövervakningslagen att en ansökan om undantag från upplysningsplikten ska vara skriftlig. Vidare anges att vissa bestämmelser som gäller ärenden om tillstånd till kamerabevakning ska tillämpas även i ärenden om undantag. Det gäller bestämmelser om att ett yttrande från en organisation som företräder de anställda på arbetsplatsen ska avges och om att en berörd kommun ska ges tillfälle att yttra sig när övervakningsutrustningen ska kunna riktas mot en plats dit allmänheten har tillträde. Den senare frågan är dock otydligt reglerad i kameraövervakningslagen på grund av en missvisande hänvisning. Att detta gäller står dock klart. En sådan möjlighet fanns i den lag som föregick kameraövervakningslagen – lagen (1998:150) om allmän kameraövervakning – och inget tyder på annat än att avsikten varit att föra över denna till den nya lagen. Därutöver följer av kameraövervakningslagen att ett beslut om undantag ska förenas med de villkor som behövs. Sådana villkor kan skräddarsys och avse t.ex. under vilken tid undantaget gäller. Slutligen föreskrivs att ett beslut om undantag får ändras eller återkallas i motsvarande fall som ett tillstånd till kamerabevakning får ändras eller återkallas. Så är fallet om förutsättningarna för ett sådant beslut ändras eller inte längre alls föreligger.

Motsvarande bestämmelser ska införas i kamerabevakningslagen. Frågan om ett yttrande från en arbetstagarorganisation ska krävas behandlas dock för sig i avsnitt 13 nedan. Vad gäller möjligheten för en berörd kommun att yttra sig har i avsnitt 11.10 föreslagits att motsvarande möjlighet i ett ärende om tillstånd till kamerabevakning snävas in något jämfört med vad som gäller enligt kameraövervakningslagen till att så ska ske endast om det behövs.

Skälen för det har redovisats i det avsnittet. Detsamma föreslås gälla i fråga om ett ärende om undantag från upplysningskravet.

Dessutom föreslås vissa ytterligare bestämmelser för att uppnå en överensstämmelse med vad som föreslagits för ansökningar och beslut om tillstånd till kamerabevakning. En ansökan om undantag ska göras hos tillsynsmyndigheten och innehålla uppgift om den som ska bedriva bevakningen och i förekommande fall den som ska ha hand om bevakningen för hans eller hennes räkning. Skälen för ansökningen ska också framgå. Ett beslut om undantag ska ange vem som ska bedriva kamerabevakningen och i förekommande fall vem som ska ha hand om bevakningen för hans eller hennes räkning.

Dessa bestämmelser för förfarandet i ärenden om undantag från upplysningskravet är förenliga med EU-regleringen. Av tydlighetsskäl – och till skillnad mot vad som gäller enligt kameraövervakningslagen – föreslås att de samlas och anges uttryckligen för just dessa ärenden i stället för genom delvisa hänvisningar till vad som gäller i ärenden om tillstånd till kamerabevakning.

13 Ett förstärkt integritetsskydd vid kamerabevakning på arbetsplatser

Förslag: I fråga om kamerabevakning på arbetsplatser som omfattas av kravet på tillstånd till kamerabevakning ska ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med en ansökan om tillstånd. Detsamma ska gälla i fråga om en ansökan om undantag från kravet på upplysning om kamerabevakning vid bevakning på arbetsplatser.

I fråga om kamerabevakning på arbetsplatser som inte omfattas av tillståndskravet ska det införas en skyldighet för arbetsgivare att först förhandla om bevakningen med berörd arbetstagarorganisation på det sätt som anges i 11–14 §§ lagen (1976:580) om medbestämmande i arbetslivet. Från förhandlingsskyldigheten ska avvikelse få göras genom kollektivavtal.

En organisation som företräder arbetstagarna på arbetsplatsen ska ha rätt att överklaga beslut om tillstånd eller om undantag från upplysningskravet.

Skälen för förslaget

Utrymmet att förstärka integritetsskyddet vid kamerabevakning på arbetsplatser och vissa andra platser

Vid kamerabevakning av platser dit allmänheten har tillträde kommer det, som föreslagits i avsnitt 11, i vissa fall att gälla ett krav på tillstånd för att kamerabevakning ska få ske. Kravet innebär en

garanti för ett starkt skydd av enskildas integritet. Tillsynsmyndigheten ska som oberoende organ väga intresset av kamerabevakning mot intresset hos de enskilda som berörs av bevakningen att inte bli föremål för denna. När det gäller övrig kamerabevakning, såväl på platser dit allmänheten har tillträde men där tillståndskravet inte ska gälla som på platser dit allmänheten saknar tillträde, kommer det inte att finnas någon generell skyldighet att involvera tillsynsmyndigheten i bevakningen genom att anmäla den till myndigheten eller samråda med myndigheten om den. Som framgått tidigare kan en allmän skyldighet av det slaget inte införas, eftersom en sådan skulle vara oförenlig med den nya EU-regleringen. Därmed kan det bli svårt för tillsynsmyndigheten att få kännedom om vilken sådan bevakning som bedrivs och att vid behov tillsyna denna.

När det gäller viss kamerabevakning, nämligen sådan bevakning som sker i anställningsförhållanden, finns det dock en möjlighet att i kamerabevakningslagen ta in bestämmelser som ger ett förstärkt integritetsskydd jämfört med vad som annars gäller enligt dataskyddsförordningen eller följer av dataskyddsdirektivet.

Som framgått av avsnitt 7.1.12 får enligt en särskild bestämmelse i förordningen i nationell rätt eller i kollektivavtal fastställas mer specifika regler för att säkerställa skyddet av rättigheter och friheter vid behandling av personuppgifter i anställningsförhållanden. Det gäller särskilt t.ex. ledning, planering och organisering av arbetet, hälsa och säkerhet på arbetsplatsen och skydd av arbetsgivarens eller kundens egendom. Sådana nationella regler ska innehålla lämpliga och specifika åtgärder för att skydda den registrerades mänskliga värdighet, berättigade intressen och grundläggande rättigheter. Hänsyn ska särskilt tas till insyn i behandlingen, överföring av personuppgifter inom en koncern eller en grupp av företag som deltar i gemensam ekonomisk verksamhet samt övervakningssystem på arbetsplatsen. Eventuella sådana nationella bestämmelser ska anmälas till kommissionen. Bestämmelsen i förordningen ger alltså ett visst utrymme för att i kamerabevakningslagen särskilt reglera kamerabevakning i anställningsförhållanden.

I direktivet finns inte någon likalydande bestämmelse, eftersom motsvarande situation hos de myndigheter och andra som i och för sig avses i direktivet omfattas av förordningen. Detsamma gäller myndigheter och andra aktörer som annars inte faller in under förordningens och direktivets tillämpningsområden. I direktivet finns

för övrigt en bestämmelse om att det är tillåtet att i nationell rätt föreskriva starkare skyddsåtgärder än de som följer av direktivet och vad gäller kamerabevakning i sådan verksamhet som faller utanför EU-regleringen kan den annars regleras utan beaktande av denna reglering.

Frågan är då om det ska införas specifika bestämmelser i kamerabevakningslagen som ger ett särskilt starkt integritetsskydd vid kamerabevakning i anställningsförhållanden och, i så fall, vilken typ av bestämmelser som kan införas och hur långtgående dessa kan vara utan att de kommer i konflikt med den särskilda bestämmelsen i förordningen och förordningen i sin helhet. Som slagits fast i avsnitt 9.2.1 bör lagen endast innehålla de bestämmelser som särskilt behövs för kamerabevakning till skillnad mot annan personuppgiftsbehandling; bestämmelserna måste kunna motiveras av principiella skäl och av ett påtagligt praktiskt behov. Samtidigt har i avsnitt 9.2.2 som utgångspunkt lagts fast att integritetsskyddet vid kamerabevakning på arbetsplatser bör förstärkas. Eventuella bestämmelser bör vidare vara desamma för all kamerabevakning när en sådan utformning är ändamålsenlig och inte hindras av EU-regleringen. I den utsträckning det är lämpligt bör bestämmelserna dessutom utformas med förebild i kameraövervakningslagens regler. Nedan diskuteras dessa frågor först i ett avsnitt som gäller kamerabevakning på arbetsplatser dit allmänheten har tillträde och där kravet på tillstånd ska gälla och därefter i ett eget avsnitt vad gäller kamerabevakning på övriga arbetsplatser. I det första avsnittet diskuteras även vad som bör gälla i ärenden om undantag från det i avsnitt 12 föreslagna kravet på upplysning om kamerabevakning, oavsett om bevakningen avser en arbetsplats till vilken allmänheten har tillträde eller en annan arbetsplats. Att en sådan undantagsmöjlighet ska finnas i enskilda fall har föreslagits där.

Avslutningsvis förtjänar påpekas att bestämmelserna i EU-regleringen utgör en ”miniminivå”. Någon möjlighet att generellt göra bestämmelserna dispositiva och ge arbetsmarknadens parter utrymme att själva reglera olika frågor om personuppgiftsbehandling och kamerabevakning finns inte.

Ett extra integritetsskydd vid kamerabevakning på arbetsplatser där tillstånd till kamerabevakning krävs, m.m.

Vad först gäller kamerabevakning på arbetsplatser dit allmänheten har tillträde och där det ska krävas tillstånd för att sådan bevakning ska få ske innebär tillståndsförfarandet, som framgått ovan, i sig en garanti för ett starkt integritetsskydd. Vid tillståndsprövningen, som görs av en oberoende tillsynsmyndighet, ska intresset av kamerabevakning vägas mot intresset hos enskilda av att inte bli bevakade. Vid kamerabevakning på arbetsplatser innebär det att prövningen kommer att innefatta en bedömning av arbetsgivarens intresse i förhållande till arbetstagarnas intresse. Som underlag för den bedömningen har alltsedan den första svenska lagstiftningen på området 1977 arbetstagare genom sina fackliga organisationer haft en rätt att yttra sig i ärenden om tillståndspliktig kameraanvändning på arbetsplatser. Enligt kameraövervakningslagen ska ett sådant yttrande lämnas av ett skyddsombud, en skyddskommitté eller en organisation som företräder de anställda på arbetsplatsen. Ett motsvarande yttrande ska lämnas även i ett ärende om undantag från upplysningsplikten. I kameraövervakningslagen är det något oklart om detta gäller endast arbetsplatser dit allmänheten har tillträde. I föregångare till den lagen synes frågan ha reglerats på olika sätt utan att skillnaden närmare har diskuterats i förarbetena. Som framgått ska ett upplysningskrav gälla också enligt den nya kamerabevakningslagen. Vidare har sådana organisationer i dag en rätt att överklaga beslut om tillstånd och beslut om undantag från upplysningsskyldigheten såvitt gäller arbetsplatser.

Behovet av sådant inflytande för arbetstagare har knappast minskat utan snarare ökat med hänsyn till de tekniska möjligheter till kamerabevakning som finns i dag. Det finns därför inte anledning att nu se annorlunda på betydelsen av arbetstagares uppfattning i tillståndsärenden eller att göra någon ändring när det gäller möjligheten att överklaga beslut om tillstånd. Samma bedömning görs vad gäller yttranden i ärenden om undantag från upplysningskravet. Det gäller oavsett om allmänheten har tillträde till arbetsplatsen eller inte, även om yttranden i tillståndsärenden av naturliga skäl måste knytas till platser av det förra slaget. Vidare görs samma bedömning vad avser möjligheten att överklaga beslut i ärenden om undantag från upplysningskravet. Sådana svenska bestämmelser om

yttrande och överklagandemöjlighet är också förenliga med EU-regleringen.

Det föreslås därför följande. I fråga om kamerabevakning på arbetsplatser som omfattas av kravet på tillstånd till kamerabevakning ska ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med en ansökan om tillstånd. Detsamma ska gälla i fråga om en ansökan om undantag från kravet på upplysning om kamerabevakning vid bevakning på arbetsplatser. Dessutom ska en sådan organisation ha rätt att överklaga beslut om tillstånd eller om undantag från lagens upplysningskrav.

Behovet av ett förstärkt integritetsskydd på övriga arbetsplatser

Kravet på tillstånd till kamerabevakning ska inte gälla arbetsplatser dit allmänheten helt saknar tillträde. Det ska inte heller gälla på alla utan endast vissa arbetsplatser dit allmänheten har tillträde. På sådana arbetsplatser som i och för sig omfattas av tillståndskravet kan det vidare finnas utrymmen dit allmänheten saknar tillträde och kamerabevakning av sådana utrymmen träffas inte av kravet. Som framgått tidigare finns det flera skäl som talar för att det behövs ett särskilt integritetsskydd på dessa arbetsplatser.

Arbetsplatserna är platser där människor vistas regelbundet och under längre stunder. Kamerabevakning kan därför, beroende på hur den anordnas, vara särskilt integritetskänslig. Samtidigt är det arbetsgivaren själv som bedömer behovet av sådan bevakning och väger detta mot det motstående integritetsintresset. Någon överblick över på vilka arbetsplatser som det förekommer kamerabevakning och hur denna utförs finns inte. Därmed är det svårt för tillsynsmyndigheten att ingripa mot kamerabevakning som kan befaras vara helt otillåten eller alltför omfattande. Endast stickprovskontroller är möjliga. Den tillsyn som gjorts visar på allvarliga brister i tillämpningen av kameraövervakningslagens integritetsskyddande regler.

Vidare kan enligt förordningen kamerabevakning av arbetsplatser ske exempelvis med samtycke från den som ska bevakas. Det gäller såväl hos myndigheter som hos privaträttsliga arbetsgivare. Ett samtycke enligt förordningen måste inhämtas från var

och en av de anställda som kan bli föremål för kamerabevakning och ska bl.a. vara frivilligt och informerat samt utgöra en otvetydig viljeyttring. Även om det av ett skäl i ingressen till förordningen följer att samtycke inte bör utgöra en grund för personuppgiftsbehandling när det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet, utesluter förordningen alltså inte samtycke som grund för kamerabevakning på arbetsplatser. Ofta befinner sig emellertid arbetstagare i ett beroendeförhållande till arbetsgivaren. Det kan därför ifrågasättas om inhämtade samtycken alltid verkligen är frivilliga.

Som framgått av avsnitt 7.1.7 är det inte möjligt att i kamerabevakningslagen föreskriva att samtycke inte ska få användas som grund för att bedriva kamerabevakning på arbetsplatser. Vidare är det inte möjligt att ställa ytterligare krav på hur ett samtycke ska lämnas utöver de som gäller enligt förordningen.

Samtidigt ger förordningen ett starkt skydd för integriteten på arbetsplatser. Enligt förordningen ska en bedömning av en planerad kamerabevaknings konsekvenser för skyddet av personuppgifter göras när typen av kamerabevakning – särskilt med användning av ny teknik och med hänsyn till bevakningens art, omfattning, sammanhang och ändamål – sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. En konsekvensbedömning ska särskilt göras när det gäller systematisk övervakning av en allmän plats i stor omfattning. Att övervakning på allmän plats pekas ut innebär inte att liknande övervakning som i stället sker på andra platser inte ska konsekvensbedömas. Utpekandet är ett exempel på ett fall där det är angeläget att en sådan bedömning kommer till stånd. Eftersom kamerabevakning på arbetsplatser många gånger kan sägas vara av systematisk natur och av stor omfattning och därmed liknar den utpekade situationen, innebär det att kamerabevakning på arbetsplatser normalt ska föregås av en konsekvensbedömning. Ibland kan också kamerabevakningen avse arbetsplatser dit allmänheten har tillträde och där tillståndskravet inte gäller. Tillsynsmyndigheten ska enligt förordningen upprätta och offentliggöra en förteckning över vad som omfattas av kravet på konsekvensbedömning och möjligen kan myndigheten komma att ange arbetsplatser, antingen generellt eller ett urval baserat på

kriterier som myndigheten bedömer som lämpliga för att avgränsa detta.

När en konsekvensbedömning visar att kamerabevakningen skulle leda till en hög risk för fysiska personers rättigheter och friheter, om inte åtgärder vidtas för att minska risken, ska den som vill bedriva bevakningen samråda med tillsynsmyndigheten. Om tillsynsmyndigheten anser att kamerabevakningen skulle strida mot förordningen, ska myndigheten komma med skriftliga råd. Myndigheten kan också t.ex. utfärda varning eller tillfälligt eller definitivt förbjuda bevakningen. Det kan antas att samråd avseende arbetsplatser ofta kommer att behöva ske. Tillsynsmyndigheten kommer då att få kännedom om den planerade kamerabevakningen på arbetsplatsen och kan ingripa mot den om det behövs eller senare utöva tillsyn över denna.

Vidare förutsätter förordningen att det inom olika branscher utarbetas och används uppförandekoder. Utarbetandet av sådana ska uppmuntras av bl.a. tillsynsmyndigheten. Utkast till en sådan kod ska ges in till tillsynsmyndigheten, som ska yttra sig över om koden överensstämmer med förordningen. Myndigheten ska också godkänna koden, om förutsättningar för det finns, och i så fall offentliggöra denna. Myndigheten kan också ackreditera ett särskilt organ som ska övervaka efterlevnaden av en sådan uppförandekod. En ackreditering förutsätter bl.a. att organet har strukturer för att hantera klagomål om överträdelser av förordningen. Om koden överträds, ska organet vidta lämpliga åtgärder och informera tillsynsmyndigheten.

I förordningen finns vidare bestämmelser om rättsmedel, ansvar och sanktioner. Dessa innebär bl.a. att en enskild som blir föremål för kamerabevakning ska ha rätt att framföra klagomål hos tillsynsmyndigheten och under vissa förutsättningar ha rätt till ersättning av den personuppgiftsansvarige eller personuppgiftsbiträdet när förordningen överträtts. Vidare ska överträdelser av förordningen kunna medföra att arbetsgivare åläggs administrativa sanktionsavgifter.

Förordningens bestämmelser ger alltså ett starkt skydd för arbetstagares integritet vad gäller kamerabevakning och ett starkare skydd än det som hittills gällt enligt kameraövervakningslagen. Vidare kommer en skyldighet att upplysa om kamerabevakning på arbetsplatser att gälla enligt kamerabevakningslagen. Trots detta måste kamerabevakning på arbetsplatser av de skäl som anförts

inledningsvis anses vara så integritetskänslig att det är motiverat att stärka integritetsskyddet ytterligare genom någon form av särskild reglering i kamerabevakningslagen. Ett sådant förslag har ovan också lämnats såvitt gäller kamerabevakning på arbetsplatser som omfattas av tillståndskravet. Behovet av integritetsskydd kan sägas vara ännu påtagligare för de nu diskuterade fallen av kamerabevakning.

En förhandlingsskyldighet införs för kamerabevakning på övriga arbetsplatser

Frågan är då hur en bestämmelse i kamerabevakningslagen som stärker integritetsskyddet vid kamerabevakning på arbetsplatser som inte omfattas av tillståndskravet kan och bör utformas. Vad särskilt gäller undantag från kravet på upplysning om kamerabevakning har ovan lämnats vissa förslag som gäller alla arbetsplatser, dvs. även sådana som behandlas i detta avsnitt.

Ett alternativ kan vara att föreskriva en skyldighet för den som avser att bedriva kamerabevakning på en sådan arbetsplats att anmäla bevakningen till eller att registrera sig hos tillsynsmyndigheten. Ett sådant alternativ torde dock inte vara förenligt med förordningen. Skyldigheten skulle träffa kamerabevakning i en mängd olika verksamheter. Dessa verksamheter kan enligt förordningen annars inte regleras i nationell rätt på det sättet att det ställs upp ett krav på tillstånd eller anmälan för att kamerabevakning överhuvudtaget ska få ske, vilket utförligt har beskrivits i avsnitt 11. Ett krav av det slaget kan inte gälla för juridiska personer eller fysiska personer som bedriver kamerabevakning i verksamheter som inte kan betecknas vara av allmänt intresse. Det innebär att ett stort antal verksamheter som träffas av förordningens reglering inte kan omfattas av ett svenskt krav på tillstånd eller anmälan för att de ska få bedriva kamerabevakning. Många av dessa utgör samtidigt arbetsplatser. Om förordningens särskilda bestämmelse om utrymme för nationell reglering avseende anställningsförhållanden då skulle tolkas så att den ändå på dessa platser tillåter ett svenskt krav på anmälan eller registrering, skulle det i praktiken innebära att förordningens övriga reglering sätts ur spel i ett stort antal fall.

Vidare skulle det möjligen kunna uppstå svårigheter med att förena ett sådant krav med förordningens bestämmelser om skyl-

dighet att göra en konsekvensbedömning och, beroende på hur denna utfaller, samråda med tillsynsmyndigheten. Under alla förhållanden innebär dessa bestämmelser i förordningen att tillsynsmyndigheten många gånger torde få kännedom om kamerabevakning på arbetsplatser. Det praktiska behovet av en nationellt föreskriven anmälnings- eller registreringsskyldighet är därför litet. Ur ett rent inhemskt perspektiv skulle dessutom ett sådant krav medföra att en ny administrativ börda läggs på ett stort antal arbetsgivare med ökade kostnader som följd.

Mot den bakgrunden kan eller bör det inte i kamerabevakningslagen ställas upp ett krav på anmälan eller registrering för att kamerabevakning på de nu diskuterade arbetsplatserna ska få ske, inte heller ett anmälningskrav som är begränsat till vissa av arbetsplatserna. Av samma skäl ska inte tillsynsmyndigheten ges en rätt att föreskriva en hel eller partiell anmälnings- eller registreringsskyldighet för arbetsplatser.

Ett annat alternativ är att införa ett krav på att det ska finnas en skriftlig överenskommelse med skyddsombudet, skyddskommittén eller den organisation som företräder arbetstagarna för att kamerabevakning ska få ske på arbetsplatsen. Ett sådant krav finns i dag för att kamerabevakning ska få ske i butiker efter enbart en anmälan, även om vissa ytterligare krav också gäller. Kravet tillkom då kamerabevakning i butiker gick från att vara tillståndspliktig till att kunna ske efter anmälan (prop. 1997/98:64). Tillståndsplikten hade inneburit att fackliga organisationer haft en rätt att yttra sig över kamerabevakningen i tillståndsärenden och en rätt att överklaga beslut om tillstånd till kamerabevakning.

Ett krav på en sådan överenskommelse för att kamerabevakning ska få ske kan säkerställa ett gott skydd för arbetstagarnas integritet. Om ett sådant krav utformas mer generellt, kan integritetsskyddet förbättras avsevärt jämfört med vad som gäller enligt dagens lagstiftning. Ett allmänt krav på överenskommelse skulle delvis korrespondera med det generella krav på yttrande från fackliga organisationer som ska utgöra underlag för tillsynsmyndighetens bedömning i tillståndsfallen.

Det är dock knappast möjligt att lagstifta om att en sådan överenskommelse ska finnas i samtliga fall av kamerabevakning på arbetsplatser som inte omfattas av tillståndskravet. Ett krav på att det ska finnas en överenskommelse innebär i praktiken ett förbud

mot kamerabevakning, om en överenskommelse inte kan nås och detta även i situationer där kamerabevakning är laglig och annars förenlig med förordningen. Det är tveksamt om ett sådant allmänt krav går att förena med förordningen. Det utrymme som förordningen ger för nationella bestämmelser avser *mer specifika regler* än de som följer direkt av förordningen snarare än artskilda regler.

Vidare är det så att intresset av kamerabevakning väger olika tungt på olika arbetsplatser samtidigt som skilda arbetsplatser ser olika ut vad gäller vad som ska kamerabevakas, hur många personer som kan fångas av kamerabevakningen och under hur lång tid m.m. Det innebär att det på vissa arbetsplatser inte är motiverat att ställa upp ett sådant krav. Så har inte heller – med undantag för de nämnda fallen med butiker – skett i dagens kameraövervakningslag för andra platser som är tillståndsbefriade och som samtidigt kan utgöra arbetsplatser, t.ex. tunnelbanestationer och kasinon. Vad gäller tunnelbanestationer har lagstiftaren tidigare uttryckligen uttalat att med hänsyn till det starka intresset av kamerabevakning bör bevakningen inte vara beroende av att en överenskommelse träffats med de anställda (prop. 2012/13:115 s. 67). I sammanhanget ska också påpekas att när kravet på överenskommelse avseende butiker tillkom infördes det inte något motsvarande krav för kamerabevakning i banklokaler och kamerabevakning på postkontor som vid samma tillfälle blev anmälningspliktiga i stället för tillståndspliktiga. Ett krav på överenskommelse är alltså inte rimligt för alla arbetsplatser.

Av i huvudsak samma skäl går det inte att i kamerabevakningslagen peka ut särskilda arbetsplatser där ett krav på överenskommelse ska gälla. Att på förhand i lag ringa in de arbetsplatser där kamerabevakning kan behövas och där bevakningen är av det slaget att ett sådant tillkommande krav bör gälla, utöver de krav som följer av förordningen, är inte möjligt. Det framstår då också som olämpligt att behålla dagens reglering för just butiker. En föreskriftsrätt för tillsynsmyndigheten i frågan skulle vara lämpligare. Den myndigheten kommer att få en god bild av kamerabevakning på arbetsplatser genom de skyldigheter som följer av förordningen för den som vill bedriva kamerabevakning på en sådan plats. Som framgått ovan är det dock tveksamt om det är förenligt med förordningen att införa en svensk bestämmelse som i de enskilda fallen kan få som effekt att kamerabevakning helt förbjuds.

Ett ytterligare alternativ kan vara att i kamerabevakningslagen föreskriva en skyldighet för arbetsgivare att inför beslut om kamerabevakning förhandla med en organisation som företräder arbetstagarna.

I lagen (1976:580) om medbestämmande i arbetslivet (MBL) finns i 10–14 §§ bestämmelser om förhandlingsrätt och förhandlingsskyldighet. Vidare följer det av arbetsmiljölagen (1977:1160) att ett skyddsombud och en skyddskommitté ska informeras om viktigare förändringar av arbetsförhållandena på en arbetsplats.

Enligt 10 § MBL har en arbetstagarorganisation rätt till förhandling med en arbetsgivare i en fråga rörande förhållandet mellan arbetsgivaren och en sådan medlem i organisationen som är eller har varit arbetstagare hos arbetsgivaren. En arbetsgivare har motsvarande rätt att förhandla med en arbetstagarorganisation. Förhandlingsrätten tillkommer arbetstagarorganisationen även i förhållande till en organisation som arbetsgivaren tillhör och arbetsgivarens organisation i förhållande till arbetstagarorganisationen.

Vidare ska enligt 11 § en arbetsgivare innan denne beslutar om en viktigare förändring av sin verksamhet på eget initiativ förhandla med en arbetstagarorganisation i förhållande till vilken arbetsgivaren är bunden av kollektivavtal. Detsamma ska iakttas innan en arbetsgivare beslutar om en viktigare förändring av arbets- eller anställningsförhållandena för arbetstagare som tillhör organisationen. Om synnerliga skäl föranleder det, får arbetsgivaren dock fatta och verkställa beslut innan han eller hon har fullgjort denna förhandlingsskyldighet. Detta kallas primär förhandlingsrätt.

Även i annat fall ska enligt 12 § en arbetsgivare förhandla med kollektivavtalsbärande arbetstagarorganisation innan han eller hon fattar eller verkställer beslut som rör en medlem i denna, om organisationen påkallar detta. Om särskilda skäl föranleder det, får arbetsgivaren dock fatta och verkställa beslutet innan han eller hon har fullgjort denna förhandlingsskyldighet. Om en fråga särskilt angår arbets- eller anställningsförhållandena för arbetstagare som tillhör en arbetstagarorganisation i förhållande till vilken arbetsgivaren inte är bunden av kollektivavtal, är arbetsgivaren skyldig att förhandla enligt 11 och 12 §§ med den organisationen. Det framgår av 13 §.

Av 14 § följer att förhandlingsskyldigheten enligt 11–13 §§ i första hand ska fullgöras genom förhandling med en lokal arbets-

tagarorganisation förutsatt att en sådan finns. Om enighet vid förhandlingen inte uppnås, ska arbetsgivaren på begäran förhandla även med en central arbetstagarorganisation.

Bestämmelserna i MBL har tidigare bedömts vara förenliga med unionsrätten och måste också anses förenliga med den nya dataskyddsregleringen. Bestämmelserna är generellt utformade. Det torde saknas exempel på att det i särskild lagstiftning har införts specifika bestämmelser om att förhandlingsskyldighet ska gälla i en viss utpekad fråga. Något hinder mot en sådan specialreglering kan dock inte anses finnas. Utredningen om integritetsskydd i arbetslivet har i sitt betänkande med samma namn (SOU 2009:44) föreslagit en särskild lag om integritet i arbetslivet med bl.a. en bestämmelse om förhandlingsskyldighet. Enligt den bestämmelsen ska en arbetsgivare som avser att besluta om en övervaknings- eller kontrollåtgärd som är ägnad att på ett påtagligt sätt påverka en eller flera arbetstagares personliga integritet först förhandla med berörd arbetstagarorganisation på det sätt som anges i 11–14 §§ MBL. Förslaget har ännu inte lett till lagstiftning.

När en arbetsgivare överväger att besluta om kamerabevakning kan – beroende på syftet med bevakningen, hur denna ska utföras m.m. – förhandlingsskyldighet gälla enligt den bestämmelse i MBL som anger att en arbetsgivare ska förhandla innan han eller hon beslutar om en viktigare förändring av arbets- eller anställningsförhållandena. Det är dock osäkert i vilken utsträckning detta gäller inför en planerad kamerabevakning och därmed i vilken omfattning parterna faktiskt förhandlar om detta. För att stärka integritetsskyddet för arbetstagare bör det i kamerabevakningslagen införas en generell skyldighet för arbetsgivaren att på eget initiativ förhandla med berörd arbetstagarorganisation inför beslut om kamerabevakning. Det kan åstadkommas genom att bestämmelserna i 11–14 §§ MBL ska tillämpas i sådana fall.

Det bör dock vara tillåtet att genom kollektivavtal, ett centralt eller lokalt sådant, avvika från förhandlingsskyldigheten. Det är rimligt att berörda förhandlande parter på samma sätt som gäller för förhandlingsskyldigheten enligt MBL kan reglera denna efter vad de finner vara lämpligt. Ett sådant undantag föreslogs också av den nämnda utredningen.

Någon motsvarande reglering i arbetsmiljölagen om att ett skyddsombud och en skyddskommitté ska informeras om en planerad

kamerabevakning föreslås däremot inte. En reglering behövs inte i de fall ombudet eller företrädare för de anställda i kommittén har utsetts av en arbetstagarorganisation. Om det inte finns någon sådan organisation, skulle en reglering visserligen kunna fylla ett praktiskt behov. För närvarande får dock den nya förhandlingsskyldigheten med berörd arbetstagarorganisation anses vara tillräcklig. Den ovan nämnda utredningen stannade också för ett sådant förslag och kombinerade inte detta med en skyldighet i förhållande till skyddsombud eller skyddskommitté.

En särskild fråga är om den myndighet som ska ansvara för tillsynen enligt kamerabevakningslagen bör ges rätt att föreskriva undantag från förhandlingsskyldigheten. Det kan finnas vissa typsituationer av kamerabevakning där arbetsgivarens beslut om sådan bevakning inte nödvändigtvis måste föregås av en förhandlingsskyldighet för honom eller henne. Å andra sidan kan en sådan föreskriftsrätt synas vara onödig med hänsyn till möjligheten för arbetsmarknadens parter att avtala bort förhandlingsskyldigheten. I vart fall kan en föreskriftsrätt riskera att medföra att tillsynsmyndigheten och parterna har olika syn på om förhandling bör ske vid en viss typ av kamerabevakning. Av sistnämnda skäl bör en sådan föreskriftsrätt inte införas.

Följaktligen föreslås att det i fråga om kamerabevakning på arbetsplatser som inte omfattas av tillståndskravet ska införas en skyldighet för arbetsgivare att först förhandla om bevakningen med berörd arbetstagarorganisation på det sätt som anges i 11–14 §§ MBL. Från förhandlingsskyldigheten ska avvikelse få göras genom kollektivavtal.

14 Ett förstärkt integritetsskydd i övrigt

Förslag: Vid kamerabevakning ska i tillämpliga delar gälla bestämmelser i dataskyddsförordningen och dataskyddslagen med föreskrifter eller i brottsdatalagen med föreskrifter om principer för behandling av personuppgifter, rättigheter för enskilda, skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden och överföring av personuppgifter till tredjeland eller internationella organisationer.

Den som tar befattning med en uppgift som har inhämtats genom kamerabevakning ska inte obehörigen få röja eller utnyttja det som han eller hon på detta sätt har fått veta om någon enskilds personliga förhållanden. I det allmännas verksamhet ska i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400) tillämpas.

Bedömning: Några sakliga ändringar av bestämmelserna i offentlighets- och sekretesslagen om sekretess vid kamerabevakning och sekretess hos tillsynsmyndigheten behövs inte.

Skälen för förslaget och bedömningen

Ett förstärkt integritetsskydd

Dataskyddsförordningen och dataskyddsdirektivet innehåller, utöver vad som redan framgått av tidigare avsnitt, bestämmelser om bl.a. principer för personuppgiftsbehandling, rättigheter för enskilda, skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden samt överföring av personuppgifter till tredjeland eller internationella organisationer.

Förordningens bestämmelser och bestämmelserna i dataskyddslagen, som kompletterar förordningen, kommer att gälla direkt för kamerabevakning som avses i kamerabevakningslagen och samtidigt utgör personuppgiftsbehandling som omfattas av förordningens tillämpningsområde i den mån det inte införs särskilda bestämmelser i lagen. Detsamma gäller kamerabevakning i sådan verksamhet som inte omfattas av förordningen eller direktivet, t.ex. verksamhet som avser nationell säkerhet, om inte annat särskilt föreskrivs. Enligt dataskyddslagen ska nämligen förordningen och den lagen gälla även för personuppgiftsbehandling i sådan verksamhet. På samma sätt kommer brottsdatalagens och den tillhörande förordningens bestämmelser att gälla för kamerabevakning som utgör personuppgiftsbehandling som avses i direktivet och därmed omfattas av de författningarna. Om det i registerförfattningar finns särskilda bestämmelser om behandling av personuppgifter som kan tillämpas vid kamerabevakning, kommer dessa att gälla i stället för de nämnda regleringarna.

Av avsnitt 7.1.9 har framgått att bestämmelser om principer som enbart upprepar eller som avviker från innehållet i förordningen inte kan införas i svensk lagstiftning som kompletterar förordningen. I viss utsträckning kan dock principerna för behandling av personuppgifter begränsas. I avsnitt 7.1.10 har vidare gjorts bedömningen att vissa bestämmelser som innebär undantag från rättigheterna i förordningen för de registrerade kan införas i svensk lagstiftning. På direktivets område har i avsnitt 7.2.4 och 7.2.5 gjorts bedömningen att en svensk lagstiftning som omfattar kamerabevakning måste innehålla bestämmelser om principer och rättigheter för registrerade eller om undantag från dessa som uppfyller kraven i direktivet. Dessutom har i avsnitt 7.1.11 och 7.1.13 såvitt gäller förordningens tillämpningsområde gjorts bedömningen att bestämmelser om skyldigheter och överföring som enbart upprepar eller som avviker från innehållet i förordningen inte kan införas i svensk lagstiftning. Vad gäller direktivet har i avsnitt 7.2.6 och 7.2.7 framgått att en svensk lagstiftning som omfattar kamerabevakning måste innehålla bestämmelser om skyldigheter och överföring som uppfyller direktivets krav.

En utgångspunkt för kamerabevakningslagen, som slagits fast i avsnitt 9.2.1, är att den endast bör innehålla de bestämmelser som särskilt behövs för kamerabevakning på grund av de specifika för-

hållanden som gäller för sådan bevakning till skillnad mot annan personuppgiftsbehandling. Lagen bör inte innehålla bestämmelser som i princip skulle utgöra upprepningar av bestämmelser som annars gäller för sådan behandling. Vidare bör lagen inte innehålla bestämmelser som avviker från förordningen och dataskyddslagen eller brottsdatalagen annat än om det kan motiveras av principiella skäl och det finns ett påtagligt praktiskt behov av det.

Vad som ytterligare talar för att undvika särskilda bestämmelser i kamerabevakningslagen i fråga om förordningens och direktivets bestämmelser om principer, rättigheter, skyldigheter m.m. är att EU-regleringens bestämmelser i dessa delar ger ett starkt skydd för den personliga integriteten. Som framgått av avsnitt 7 är bestämmelserna i förordningen och direktivet fler än vad som följer av dagens kameraövervakningslag. Att låta dessa bestämmelser gälla kan därmed ge ett förstärkt integritetsskydd vid kamerabevakning jämfört med vad som gäller i dag. De förslag som lämnats i tidigare avsnitt innebär att möjligheterna att bedriva kamerabevakning kommer att öka. För att skapa en godtagbar balans mellan intresset av kamerabevakning och intresset av skydd för den personliga integriteten bör dessa ökade möjligheter att bedriva kamerabevakning åtföljas av ett förstärkt integritetsskydd i olika avseenden.

Nedan behandlas vissa för kamerabevakning särskilt intressanta bestämmelser i förordningen och i brottsdatalagen, som genomför direktivet. Det övervägs om dessa bestämmelser ska gälla i enlighet med utgångspunkten ovan eller om det är möjligt och bör införas avvikande bestämmelser i kamerabevakningslagen. Bestämmelser i EU-regleringen som saknar relevans för kamerabevakning, eftersom de avser situationer som inte förekommer vid sådan bevakning, behandlas inte. Inte heller behandlas sådana bestämmelser som är av mindre relevans på kamerabevakningsområdet. Dessa framstår övergripande sett som lämpliga även på detta område och ska därför gälla också vid kamerabevakning.

Principerna ska gälla vid kamerabevakning

Både förordningen och direktivet innehåller bestämmelser om principer. Dessa avser bl.a. principer för behandling av personuppgifter och rättsliga grunder för behandling, som tillsammans utgör de

allmänna förutsättningarna för att en personuppgiftsbehandling ska vara tillåten. Bland principerna för behandling kan särskilt nämnas de som avser krav på laglighet och korrekthet, ändamålsbegränsning, uppgiftsminimering, lagringsminimering samt integritet och konfidentialitet.

Som framgått ovan kan det på förordningens tillämpningsområde inte införas svenska bestämmelser för kamerabevakning som enbart upprepar eller som avviker från principerna enligt förordningen. I viss utsträckning kan dock principerna begränsas. Vidare måste en svensk lagstiftning som omfattar kamerabevakning uppfylla direktivets krav. När det gäller direktivet har Utredningen om 2016 års dataskyddsdirektiv föreslagit att principerna genomförs i brottsdatalagen och dess förordning. Det saknas skäl att på kamerabevakningsområdet avvika från vad som följer av förordningen eller föreskrivs i brottsdatalagen med föreskrifter.

Det finns anledning att särskilt beröra principen om lagringsminimering, som finns i både förordningen och direktivet. Principen innebär att personuppgifter inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. I direktivet anges därutöver att det ska föreskrivas lämpliga tidsgränser för radering av personuppgifter eller för periodisk översyn av behovet av att lagra personuppgifter. Utredningen om 2016 års dataskyddsdirektiv har föreslagit att dessa krav i direktivet genomförs genom att det i brottsdatalagen införs bestämmelser om att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen och att den personuppgiftsansvarige, om inte annat är föreskrivet, årligen ska se över behovet av att fortsatt behandla personuppgifterna.

Enligt kameraövervakningslagen får bild- eller ljudmaterial från kameraövervakning av en plats dit allmänheten har tillträde bevaras under högst två månader, om inte länsstyrelsen beslutar om en längre bevarandetid. Material från övervakning av en plats dit allmänheten inte har tillträde får inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med övervakningen. I förarbetena till kameraövervakningslagen framhölls att det är en förutsättning för en effektiv kamerabevakning att materialet kan sparas under tillräckligt lång tid för att kunna komma till avsedd

användning. Eftersom övervakning enligt kameraövervakningslagen i stor utsträckning syftar till att förebygga och utreda brott, är den särskilt angivna bevarandetiden anpassad för övervakning som sker för sådana syften (prop. 2012/13:115 s. 123 f.).

Framöver kommer möjligheterna att bedriva kamerabevakning att öka. Vid kameraanvändning som inte omfattas av kamerabevakningslagen kommer förordningens och brottsdatalagens bestämmelser att reglera användningen. Dessa regleringar innehåller inte någon särskilt angiven tid för hur länge bild- och ljudmaterial från sådan kameraanvändning får lagras. Vid kamerabevakning enligt kamerabevakningslagen som omfattas av tillståndskravet är det på direktivets område i och för sig möjligt att föreskriva en närmare angiven lagringstid. Detsamma gäller på förordningens område där tillståndskravet vilar på artikel 6.1 e, som i sin tur hänger samman med artikel 6.3 enligt vilken nationella bestämmelser om lagringstid är tillåtna. Det finns också en viss möjlighet enligt förordningen att ange en längsta lagringstid vid kamerabevakning som inte omfattas av tillståndskravet. Dock kommer kamerabevakning, både sådan som omfattas av tillståndskravet och sådan som inte gör det, att kunna ske för en mängd olika berättigade ändamål. Detsamma gäller för annan kameraanvändning. Med hänsyn härtill är det knappast möjligt att fastställa en enhetlig lagringstid. Vid bevakning som sker med tillstånd kan tillsynsmyndigheten förena tillståndet med villkor om att materialet endast får lagras under en viss angiven tid. Ett sådant villkor gäller dock endast så länge materialet inte kommer till användning i någon annan verksamhet än kamerabevakning hos den som bedriver bevakningen, t.ex. polisens användning av material från egen bevakning. I andra fall kan tillsynsmyndigheten i samband med konsekvensbedömningar och samråd med myndigheten använda sig av sina tillsynsbefogenheter om den planerade bevarandetiden anses medföra alltför höga risker. Mot denna bakgrund bör det inte införas någon särskild bestämmelse i kamerabevakningslagen om längsta tid för behandling av bild- och ljudmaterial från kamerabevakning. Den redovisade regleringen bedöms ge ett tillräckligt skydd för integriteten även utan en sådan tidsgräns för behandling av material från kamerabevakning.

Sammanfattningsvis föreslås att bestämmelserna om principer i förordningen och brottsdatalagen med förordning ska gälla i tillämpliga delar vid kamerabevakning. Det kan åstadkommas genom den

i avsnitt 10.1 föreslagna bestämmelsen om kamerabevakningslagens förhållande till andra bestämmelser. Den bestämmelsen innebär att förordningen, dataskyddslagen, föreskrifter som meddelats med stöd av den lagen eller annan författning som kompletterar förordningen gäller för kamerabevakning som omfattas av förordningen eller dataskyddslagen. Vidare innebär den att brottsdatalagen, föreskrifter som meddelats med stöd av den lagen eller annan författning som genomför direktivet gäller vid kamerabevakning som omfattas av brottsdatalagen. Det ska framhållas att dessa bestämmelser ska gälla i den mån kamerabevakningslagens tillståndsreglering inte tillämpas vad avser t.ex. villkor om längsta tid för behandling.

Rätten till tillgång ska gälla vid kamerabevakning

Enligt såväl förordningen som direktivet ska den registrerade ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne behandlas och i så fall få tillgång till uppgifterna och viss information, bl.a. om ändamålen med behandlingen, hur länge personuppgifterna kommer att lagras, rätten till rättelse eller radering av personuppgifterna och rätten att lämna in klagomål till tillsynsmyndigheten.

Utredningen om 2016 års dataskyddsdirektiv har föreslagit att direktivets bestämmelse genomförs i en bestämmelse i brottsdatalagen som innebär att den personuppgiftsansvarige till den som begär det ska lämna skriftligt besked om huruvida personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas, ska vidare sökanden få del av dem och få viss skriftlig information om behandlingen. Enligt förslaget behöver sökanden inte få del av personuppgifter som han eller hon redan har tagit del av, om det inte begärs, men det ska framgå av informationen att personuppgifterna i fråga behandlas.

Rätten till tillgång till personuppgifter är av central betydelse för att enskilda ska kunna ta till vara sina rättigheter. Exempelvis torde det väsentligen försvåra möjligheten för en enskild att få sina personuppgifter raderade, om det inte finns en möjlighet att först få bekräftelse på att behandling av uppgifterna sker.

En bestämmelse om rätt till tillgång till personuppgifter finns i dag i personuppgiftslagen, som bygger på 1995 års dataskyddsdirektiv. I tidigare lagstiftningssammanhang har med hänvisning till den s.k. missbruksregeln i den lagen gjorts bedömningen att en rätt till tillgång inte behövs vid sådan ostrukturerad behandling av personuppgifter som det i de allra flesta fall är fråga om vid kamerabevakning (SOU 2009:87 s. 205).

Dessa skäl väger nu lättare än tidigare. Möjligheterna att bedriva kamerabevakning kommer att öka, eftersom bevakning ska få ske för fler ändamål. Vidare ska det, som framgått ovan, inte finnas fasta tider för hur länge material från kamerabevakning får lagras. Detta talar för att rätten till tillgång enligt förordningen eller brottsdatalagen bör gälla vid kamerabevakning. En sådan rätt kan stärka skyddet för enskildas integritet. De föreslås därför att förordningens och brottsdatalagens bestämmelser om rätten till tillgång ska gälla vid kamerabevakning som avses i kamerabevakningslagen.

Det ska framhållas att behandling av personuppgifter vid kamerabevakning är speciell på det sättet att uppgifterna kan användas, men ofta inte används, för att identifiera personer genom att ett namn eller ett personnummer kopplas ihop med den som fångats på bild. Identifiering kan visserligen i vissa fall ske genom program för ansiktsigenkänning eller liknande men detta är generellt sett inte det vanliga vid kamerabevakning. Lagrat material är i normalfallet inte strukturerat så att det går att söka efter personuppgifter på annat sätt än manuellt. Om rätten till tillgång till personuppgifter skulle innebära att den som bedriver kamerabevakning på begäran av en enskild skulle behöva gå igenom materialet manuellt och med hjälp av jämförelsebilder och annan information försöka identifiera den enskilde, skulle regelverket riskera att skapa en orimlig administrativ börda för den som bedriver kamerabevakning.

Sådana farhågor fördes fram i förarbetena till polisdatalagen (2010:361). Frågan gällde då insamling av personuppgifter genom bild och ljud i polisens brottsbekämpande verksamhet. Regeringen anförde följande (prop. 2009/10:85 s. 85 f.).

> Ett grundläggande krav i den nya lagen bör vara att polisen alltid ska veta för vilket ändamål en uppgift bevaras. För att kunna uppfylla detta krav måste polisen känna till det huvudsakliga innehållet av en bild- eller ljudsekvens som bevaras, t.ex. vilken person som spaningen eller brottsutredningen avsåg. Det ligger i sakens natur att polisen inte kan förväntas känna till och dokumentera identiteten på samtliga personer

som förekommer i en filmsekvens t.ex. från en allmän plats. Och det faller på sin egen orimlighet att polisen skulle behöva informera samtliga dessa personer om behandlingen. Det bör framhållas – som uttalas i förarbetena till personuppgiftslagen (prop. 1997/98:44 s. 82 f.) – att den personuppgiftsansvarige bara är skyldig att utnyttja de sök- och sammanställningsmöjligheter som han eller hon har tillgång till för att få fram information att lämna till den registrerade. I sammanhanget kan erinras om att regeringen i nyssnämnda proposition hänvisade till Datalagskommitténs uttalande att ”inte ens EG-rätten kan tvinga någon att göra det som i praktiken är omöjligt” (SOU 1997:39 s. 392).

Rätten till tillgång till personuppgifter enligt förordningen och direktivet motsvarar i stort vad som gällt enligt 1995 års dataskyddsdirektiv. Det saknas därför anledning att göra någon annan bedömning av förordningens och direktivets bestämmelser i denna del än vad regeringen gjort i förhållande till motsvarande bestämmelse i 1995 års direktiv. Samma bedömning har gjorts av Utredningen om 2016 års dataskyddsdirektiv. EU-regleringen kan därför inte anses innebära att den som bedriver kamerabevakning är skyldig att vidta andra åtgärder än att utnyttja de sök- och sammanställningsmöjligheter som han eller hon har tillgång till.

Det ska slutligen framhållas att bestämmelser om sekretess och tystnadsplikt kan begränsa rätten till tillgång till material från kamerabevakning. Dessa frågor behandlas nedan.

Sekretess och tystnadsplikt vid kamerabevakning

Enligt offentlighets- och sekretesslagen (2009:400) gäller sekretess för uppgift om en enskilds personliga förhållanden som har inhämtats genom kameraövervakning som avses i kameraövervakningslagen, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men (32 kap. 3 §). Hos en domstol i dess rättskipande eller rättsvårdande verksamhet gäller sekretessen endast om det kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs. Sekretessen hindrar inte att uppgift lämnas till brottsbekämpande myndigheter i vissa fall eller till en kommun eller en myndighet för att förebygga en hotande olycka eller för att begränsa verkningarna av en redan inträffad olycka (32 kap. 3 a §). Sekretess till skydd för en enskild gäller normalt inte i förhållande till den enskilde

själv (12 kap. 1 §). Det innebär att sekretessen normalt inte hindrar att enskilda kan få tillgång till material från kamerabevakning som avser dem själva i det allmännas verksamhet. Om materialet omfattar även andra personer, kan den enskilde få tillgång till materialet förutsatt att ett utlämnande inte är till men för någon sådan annan person eller dennes närstående.

Kameraövervakningslagen innehåller en särskild bestämmelse om tystnadsplikt. Av bestämmelsen följer att den som tar befattning med en uppgift som har inhämtats genom kameraövervakning inte obehörigen får röja eller utnyttja det som han eller hon på detta sätt har fått veta om någon enskilds personliga förhållanden. Bestämmelsen gäller för privata aktörer. I bestämmelsen upplyses om att i det allmännas verksamhet ska i stället bestämmelserna i offentlighets- och sekretesslagen tillämpas. Vid tolkning av bestämmelsen i kameraövervakningslagen ska ledning sökas i regleringen i offentlighets- och sekretesslagen.

Ovan har föreslagits att rätten till tillgång enligt förordningen och brottsdatalagen ska gälla vid kamerabevakning. Bestämmelserna om sekretess och tystnadsplikt kan begränsa möjligheten för enskilda att få information om och tillgång till material från kamerabevakning som avser dem själva. Frågan är då om bestämmelserna kan behållas i sin nuvarande form.

Förhållandet mellan, å ena sidan, bestämmelser om sekretess och tystnadsplikt och, å andra sidan, EU-regleringen har analyserats av såväl Dataskyddsutredningen som Utredningen om 2016 års dataskyddsdirektiv.

Dataskyddsutredningen har föreslagit en bestämmelse i dataskyddslagen som innebär att skyldigheten att ge den registrerade information om och tillgång till personuppgifter inte ska gälla uppgifter som den personuppgiftsansvarige inte får lämna ut till den registrerade enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning. Om den personuppgiftsansvarige inte är en myndighet, får denne enligt den föreslagna bestämmelsen i motsvarande fall vägra att lämna ut uppgifter till den registrerade. Dataskyddsutredningen har gjort bedömningen att detta förslag är förenligt med förordningen. Bedömningen har bl.a. grundats på det utrymme till undantag från förordningens rättigheter för registrerade som finns enligt en särskild bestämmelse. Denna bestämmelse har behandlats närmare i avsnitt 12.

Utredningen om 2016 års dataskyddsdirektiv har i brottsdatalagen föreslagit begränsningar av rätten till personrelaterad information, bl.a. information om vilka personuppgifter som behandlas, som bygger på ett utrymme för sådana begränsningar som lämnas i direktivet. Begränsningarna innebär att rätten inte ska gälla i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att personuppgifter inte får lämnas ut av hänsyn till bl.a. intresset av att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet eller intresset av att annans fri- och rättigheter skyddas. Detta ska gälla även för en personuppgiftsansvarig som inte är en myndighet i motsvarande fall som avses i offentlighets- och sekretesslagen. Utredningen har bedömt att förslaget är förenligt med direktivet.

Utredningarnas förslag medför alltså att vissa rättigheter i förordningen respektive direktivet och brottsdatalagen inte ska gälla när personuppgifter omfattas av i dag gällande bestämmelser om sekretess eller tystnadsplikt. Det saknas anledning att ur ett kamerabevakningsperspektiv göra någon annan bedömning än vad de utredningarna gjort. Bestämmelserna om sekretess och tystnadsplikt vid kamerabevakning måste också, med hänsyn till deras innebörd och hur de ska förstås, anses rymmas inom de utrymmen för nationella inskränkningar som finns i förordningen och direktivet. Även andra sekretessbestämmelser kan vara relevanta vid kamerabevakning och kan begränsa rätten till tillgång till material från kamerabevakning i enlighet med vad de nämna utredningarna föreslagit.

Det ska påpekas att bestämmelsen om tystnadsplikt i kameraövervakningslagen delvis kan sägas ha ett vidare tillämpningsområde än de begränsningar som föreslagits i dataskyddslagen och brottsdatalagen. Kameraövervakningslagens bestämmelse innebär nämligen ett allmänt förbud mot att obehörigen röja eller utnyttja uppgifter om enskilds personliga förhållanden. Obehörighetsrekvisitet är avsett att tolkas så att ett uppgiftslämnande av en enskild aktör som motsvarar ett uppgiftslämnande som är tillåtet enligt sekretessregleringen inte är att betrakta som obehörigt. Det innebär att en behandling som innefattar att bild- och ljudmaterial från kamerabevakning sprids eller lämnas ut till någon annan endast får ske om

det står klart att personer som förekommer i materialet eller deras närstående inte lider men. Det är förutsatt på flera håll i förordningen att medlemsstaterna kan anta bestämmelser om yrkesmässig eller annan bindande tystnadsplikt (se t.ex. artikel 9 och 90). Förordningen kan därför inte anses hindra en sådan bestämmelse om tystnadsplikt i kamerabevakningslagen. Något hinder mot detta bedöms inte heller finnas i direktivet, som tillåter att medlemsstaterna föreskriver starkare skyddsåtgärder än de som fastställs i direktivet. Detta gäller särskilt som bestämmelsen ska tolkas på samma sätt som sker i motsvarande situationer enligt offentlighets- och sekretesslagen.

De sekretess- och tystnadspliktsbestämmelser som gäller i dag på kamerabevakningsområdet är alltså förenliga med EU-regleringen. De skäl som en gång motiverat att bestämmelserna införts – att skydda integriteten hos personer som förekommer i bild- och ljudmaterial – gör sig fortfarande gällande. Bestämmelserna ska därför behållas. Det finns emellertid anledning att överväga om de övriga förslag som lämnats bör föranleda några ändringar av bestämmelserna.

En följd av förslaget om kamerabevakningslagens tillämpningsområde är att kameror som har monterats på drönare även fortsättningsvis omfattas av kamerabevakningslagstiftningen. Det material som tas upp med sådana kameror har ofta ett vidare användningsområde än material som tas upp vid traditionell kamerabevakning. Detta talar å ena sidan för att behovet av att kunna sprida materialet kan vara större än vid andra former av kamerabevakning. Å andra sidan kan behovet av skydd för den personliga integriteten göra sig lika starkt gällande som vid annan kamerabevakning. Många gånger torde det dock inte vara fråga om material som innebär sådant men för en enskild som gör att det inte får röjas. Sammantaget bedöms det inte finnas tillräckliga skäl att till följd av det nu diskuterade ändra innehållet i sekretess- och tystnadspliktsbestämmelserna. Inte heller de övriga förslag som lämnats i tidigare avsnitt kan anses medföra något behov av att ändra bestämmelserna.

I sammanhanget ska också nämnas några ytterligare bestämmelser. För att enskilda ska kunna ta till vara sina rättigheter när information inte har lämnats ut eller när information har begränsats anges i direktivet att tillsynsmyndigheten på den enskildes vägnar ska kontrollera om personuppgifter om den enskilde behandlas

författningsenligt. Förordningen saknar en motsvarande bestämmelse. Utredningen om 2016 års dataskyddsdirektiv har föreslagit att direktivets bestämmelse genomförs i brottsdatalagen. Denna rätt enligt brottsdatalagen ska gälla även vid behandling av personuppgifter som sker vid kamerabevakning.

När det gäller dataskyddsombud har Dataskyddsutredningen på förordningens område förutsatt att det i verksamheter där känsliga uppgifter förekommer redan gäller sekretess enligt offentlighets- och sekretesslagen i den utsträckning som är motiverad i just den verksamheten. För dataskyddsombud i den privata sektorn har utredningen föreslagit en bestämmelse om tystnadsplikt, som innebär att den som fullgör uppgift som sådant ombud inte obehörigen får röja eller utnyttja det som han eller hon då har fått veta om en enskilds personliga eller ekonomiska förhållanden. Utredningen om 2016 års dataskyddsdirektiv har förutsett att det även på brottsdatalagens tillämpningsområde kommer att krävas en regel om tystnadsplikt för dataskyddsombud och kommer att återkomma till frågan i sitt slutbetänkande. Det har inte framkommit något behov av att vid kamerabevakning avvika från vad som annars ska gälla i fråga om tystnadsplikt för dataskyddsombud. Dataskyddslagens och brottsdatalagens bestämmelser om tystnadsplikt för dataskyddsombud ska därför gälla vid kamerabevakning.

Avslutningsvis finns det anledning att beröra vissa sekretessbrytande bestämmelser. Som framgått ovan hindrar sekretessen vid kamerabevakning inte att en uppgift i vissa fall lämnas till brottsbekämpande myndigheter eller till en kommun eller en myndighet för att förebygga en hotande olycka eller för att begränsa verkningarna av en redan inträffad olycka. Någon ändring i detta avseende är inte motiverad. Vidare har tillsynsmyndigheterna rätt att få tillgång till och granska bevarat bild- eller ljudmaterial. Enligt bestämmelser i förordningen och brottsdatalagen ska tillsynsmyndigheten få tillgång till personuppgifter och information som myndigheten behöver för att kunna fullgöra sina uppgifter. Offentlighets- och sekretesslagen hindrar inte att tillsynsmyndigheten får sådan tillgång. Frågor om tillsyn på kamerabevakningsområdet behandlas i avsnitt 15.

Sammanfattningsvis görs bedömningen att några sakliga ändringar av de nuvarande bestämmelserna i offentlighets- och sekretesslagen om sekretess vid kameraövervakning inte behövs. Det föreslås den

justeringen att det ska hänvisas till den nya kamerabevakningslagen. Vidare föreslås att en bestämmelse som motsvarar bestämmelsen om tystnadsplikt i kameraövervakningslagen införs i kamerabevakningslagen. Slutligen ska dataskyddslagens och brottsdatalagens bestämmelser om begränsningar av rätten till tillgång till personuppgifter och bestämmelser som knyter an till dessa gälla vid kamerabevakning.

Särskilt om sekretess hos tillsynsmyndigheten

Nedan föreslås att tillsynen över kamerabevakning enligt kamerabevakningslagen ska samlas hos en enda tillsynsmyndighet, Datainspektionen. Hos Datainspektionen gäller sekretess bl.a. för uppgift om en enskilds personliga eller ekonomiska förhållanden i ärende om tillstånd eller tillsyn som enligt lag eller annan författning ska handläggas av inspektionen, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs (32 kap. 1 § offentlighets- och sekretesslagen). När det är fråga om t.ex. granskning av upptaget bildmaterial i tillsynsverksamheten gäller dock den i avsnittet ovan nämnda bestämmelsen (32 kap. 3 § offentlighets- och sekretesslagen).

Enligt förordningen ska varje tillsynsmyndighets ledamöter och personal i enlighet med unionsrätten eller medlemsstaternas nationella rätt omfattas av tystnadsplikt både under och efter sin mandattid vad avser konfidentiell information som de fått kunskap om vid utförandet av sina uppgifter eller utövandet av sina befogenheter. Under mandatperioden ska denna tystnadsplikt i synnerhet gälla rapportering från fysiska personer om överträdelser av förordningen.

Dataskyddsutredningen har bedömt att denna bestämmelse i förordningen inte kräver någon ändring av den gällande sekretessbestämmelsen avseende Datainspektionens verksamhet. Enligt utredningen har det inte framkommit något som talar för att bestämmelsen orsakat tillämpningssvårigheter eller att sekretessen är otillräcklig ur ett integritetsperspektiv. Inte heller Utredningen om 2016 års dataskyddsdirektiv har föreslagit någon ändring av bestämmelsen.

Det saknas anledning att göra någon annan bedömning i fråga om sekretess hos Datainspektionen i ärenden enligt kamerabevak-

ningslagen eller vad gäller tillsyn över kamerabevakning i övrigt. Som framgått gäller en starkare sekretess vid granskning av upptaget bildmaterial i tillsynsverksamheten. Någon ändring behövs alltså inte.

Övriga relevanta rättigheter ska också gälla vid kamerabevakning

Förordningen och direktivet innehåller vidare ett antal ytterligare rättigheter för registrerade, som är mer eller mindre relevanta vid kamerabevakning. I det följande övervägs om rättigheterna, i enlighet med den inledningsvis fastslagna utgångspunkten, ska gälla för sådan kamerabevakning som avses i kamerabevakningslagen eller om det kan och bör göras undantag från dessa på detta område.

I såväl förordningen som direktivet finns en *rätt till rättelse och komplettering*. Denna innebär att en registrerad utan onödigt dröjsmål ska få felaktiga personuppgifter som rör honom eller henne rättade av den personuppgiftsansvarige. Vidare ska den registrerade med beaktande av ändamålet med behandlingen kunna få ofullständiga personuppgifter kompletterade. Utredningen om 2016 års dataskyddsdirektiv har föreslagit att direktivets bestämmelse genomförs i brottsdatalagen.

Denna rätt till rättelse och komplettering kan visserligen endast undantagsvis aktualiseras i fråga om bild- och ljudmaterial från kamerabevakning, eftersom en kamera registrerar det som faktiskt sker. Det kan dock inte helt uteslutas att materialet någon gång kan vara felaktigt. Exempelvis skulle en felaktig tidsangivelse i bilderna kunna förekomma. I en sådan situation framstår det som rimligt att det finns en möjlighet att få den felaktiga informationen rättad eller kompletterad.

Förordningen och direktivet innehåller vidare en *rätt till radering*. Denna innebär att den registrerade i vissa fall har rätt att begära att den personuppgiftsansvarige utan onödigt dröjsmål raderar personuppgifter som rör den registrerade. Det gäller t.ex. när personuppgifterna inte längre är nödvändiga för de ändamål för vilka de samlats in eller på annat sätt behandlats och när personuppgifterna har behandlats på ett olagligt sätt. Utredningen om 2016 års dataskyddsdirektiv har föreslagit att direktivets bestämmelse genomförs i brottsdatalagen.

Förordningen ger också den registrerade en rätt att i vissa situationer kräva av den personuppgiftsansvarige att *behandlingen begränsas*. Det gäller bl.a. när den registrerade bestrider personuppgifternas korrekthet, när behandlingen är olaglig och den registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning eller när den personuppgiftsansvarige inte längre behöver personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk. Uttrycket begränsning av behandling definieras som en markering av lagrade personuppgifter med syftet att begränsa behandlingen av dem i framtiden. Även direktivet innehåller en bestämmelse om begränsning av behandling. Enligt den ska den personuppgiftsansvarige, i stället för att radera personuppgifter, kunna begränsa behandlingen av dem dels om den registrerade bestrider att uppgifterna är korrekta och det rätta förhållandet inte kan fastställas, dels om uppgifterna ska sparas som bevisning. Utredningen om 2016 års dataskyddsdirektiv har föreslagit att denna bestämmelse genomförs i brottsdatalagen.

De situationer som avses med dessa rättigheter kan aktualiseras vid kamerabevakning. Det framstår som befogat att en enskild då ska ha den rätt som är knuten till situationen, t.ex. en möjlighet att få material som avser honom eller henne raderat när materialet inte längre är nödvändigt för det ändamål för vilket det samlats in eller på annat sätt behandlats. Det ska påpekas att vid sådan kamerabevakning som omfattas av tillståndskrav kommer villkoren för bevakningen att framgå av tillståndet. Så länge den som bedriver bevakningen uppfyller tillståndsvillkoren kan radering eller begränsning av behandling inte komma i fråga.

Slutligen innehåller förordningen, men inte direktivet, en *rätt för en registrerad att göra invändningar* mot en behandling av personuppgifter som avser honom eller henne och som grundar sig på artikel 6.1 e eller f, dvs. en behandling som är nödvändig som ett led i myndighetsutövning eller för att utföra en uppgift av allmänt intresse respektive en behandling som är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen när inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre. Den personuppgiftsansvarige får vid en invändning inte längre behandla personuppgifterna såvida

inte denne kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk.

En sådan rätt att invända bedöms kunna vara relevant och befogad vid kamerabevakning. Det ska dock framhållas att den endast gäller i de fall då bevakningen grundar sig på artikel 6.1 e eller f i förordningen och att bevakning som grundar sig på artikel 6.1 e omfattas av det föreslagna kravet på tillstånd till kamerabevakning. När tillstånd har meddelats har tillsynsmyndigheten redan vägt kamerabevakarens intresse av att bedriva bevakningen mot enskildas intresse av att inte bli bevakade. Så länge bevakningen håller sig inom villkoren för tillståndet väger kamerabevakarens intresse tyngre.

Sammanfattningsvis bedöms de diskuterade rättigheterna i olika grad kunna aktualiseras vid kamerabevakning men likväl ha ett berättigande. För att stärka integritetsskyddet bör rättigheterna gälla vid kamerabevakning, även om utrymmet för att göra rättigheterna gällande på detta område är begränsat jämfört med vad som gäller för personuppgiftsbehandling generellt sett. Följaktligen föreslås att förordningens och brottsdatalagens bestämmelser om rättigheter för enskilda ska gälla i tillämpliga delar vid kamerabevakning.

Bestämmelser om skyldigheter och om överföring av material ska gälla vid kamerabevakning

Både förordningen och direktivet innehåller långtgående bestämmelser om skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden. Dessa avser bl.a. allmänna skyldigheter, säkerhet för personuppgifter, konsekvensbedömning och samråd med tillsynsmyndigheten samt dataskyddsombud.

Förordningen innehåller också en reglering av under vilka förutsättningar personuppgifter får överföras till tredjeland eller till internationella organisationer. Huvudregeln är att en överföring är tillåten, om det mottagande tredjelandet eller den mottagande organisationen kan säkerställa en adekvat skyddsnivå för uppgifterna. Även direktivet innehåller bestämmelser som reglerar denna fråga. Dessa motsvarar i stort bestämmelserna i förordningen.

När det gäller kamerabevakning som avses i direktivet har Utredningen om 2016 års dataskyddsdirektiv föreslagit att direktivets

skyldigheter genomförs i brottsdatalagen och dess förordning. Exempelvis ska gälla att den personuppgiftsansvarige – genom lämpliga tekniska och organisatoriska åtgärder – dels ska säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att registrerades rättigheter skyddas, dels ska se till att dataskyddsprinciper säkerställs på ett effektivt sätt och att nödvändiga skyddsåtgärder integreras i behandlingen. Utredningen har vidare föreslagit att direktivets bestämmelser om överföring ska genomföras i brottsdatalagen.

Som framgått inledningsvis kan det ge ett förstärkt integritetsskydd att låta bestämmelserna i förordningen och, på direktivets område, i brottsdatalagen med förordning gälla vid kamerabevakning. Några skäl att på kamerabevakningsområdet – i den mån det är möjligt – avvika från förordningen eller brottsdatalagen vad gäller skyldigheter för personuppgiftsansvariga och överföring av personuppgifter till tredjeland eller internationella organisationer finns inte. Det föreslås därför att dessa bestämmelser i tillämpliga delar ska gälla vid kamerabevakning. Det ska framhållas att bestämmelserna endast ska gälla i den mån tillståndsregleringen i kamerabevakningslagen inte tillämpas vad avser t.ex. villkor i sådana avseenden.

15 Tillsyn, sanktioner och rättsmedel

15.1 Tillsynsmyndighet enligt kamerabevakningslagen

Förslag: Datainspektionen ska vara tillsynsmyndighet enligt kamerabevakningslagen. Detta ska regleras genom en bestämmelse i lagen om att den myndighet som regeringen bestämmer utövar tillsyn över kamerabevakning.

Skälen för förslaget

Inledning

I dataskyddsförordningen finns ett stort antal bestämmelser om tillsyn. Enligt dessa ska varje medlemsstat utse en eller flera självständiga tillsynsmyndigheter, som ska ansvara för att övervaka tillämpningen av förordningen. Tillsynsmyndigheten ska inta en oberoende ställning och ha vissa i förordningen uppräknade uppgifter och befogenheter.

Även i dataskyddsdirektivet finns ett flertal bestämmelser om tillsyn. I stora delar överensstämmer dessa med eller liknar dessa bestämmelserna i förordningen. Enligt direktivet får det i nationell rätt föreskrivas att en tillsynsmyndighet som har inrättats i enlighet med förordningen ska vara tillsynsmyndighet även enligt direktivet.

Av kameraövervakningslagen och dess föreskrifter följer att Datainspektionen har det centrala ansvaret för tillsynen över kameraövervakning och utövar den operativa tillsynen över kameraövervakning av platser dit allmänheten inte har tillträde medan den operativa tillsynen över kameraövervakning av platser dit allmänheten har tillträde utövas av länsstyrelserna. Som framgått av avsnitt 7

överensstämmer kameraövervakningslagens bestämmelser om tillsyn endast delvis med förordningens och direktivets bestämmelser.

Flertalet av förordningens bestämmelser om tillsyn kommer att gälla direkt i Sverige. Inom vissa ramar måste det i svensk rätt införas kompletterande regler, bl.a. om tillsynsmyndighetens organisation och om utnämning och avsättande av myndighetens medlemmar. På direktivets område måste det finnas svenska bestämmelser om tillsynsmyndigheten.

Som utgångspunkter för de överväganden som görs nedan om tillsynsmyndighet på kamerabevakningsområdet gäller att förslaget måste vara förenligt med bestämmelserna i EU-regleringen, att det bör vara gemensamt för all kamerabevakning och att det inte bör avvika från förslag som lagts av andra utredningar i motsvarande fråga.

Datainspektionen ska vara enda tillsynsmyndighet enligt kamerabevakningslagen

Vad gäller vilken eller vilka myndigheter som ska utöva tillsyn enligt kamerabevakningslagen, inklusive pröva ansökningar om tillstånd till kamerabevakning och om undantag från upplysningskravet, ska inledningsvis redogöras för vad andra utredningar har föreslagit i fråga om tillsynsansvaret för behandling av personuppgifter generellt sett.

Den i avsnitt 2 nämnda Utredningen om tillsynen över den personliga integriteten har föreslagit att Datainspektionen ska utses till svensk tillsynsmyndighet enligt förordningen och direktivet samt att detta ska regleras på förordningsnivå i myndighetens instruktion. Utredningen har vidare föreslagit att det inte längre ska ingå i Säkerhets- och integritetskyddsnämndens (SIN) uppdrag att utöva tillsyn över Polismyndighetens personuppgiftsbehandling i allmänhet. Den tillsynen ska i fortsättningen endast utföras av Datainspektionen. Vad gäller Säkerhetspolisens personuppgiftsbehandling i brottsbekämpande verksamhet ska enligt utredningen Datainspektionen ha behörighet att utöva tillsyn för att EU-regleringens krav ska uppfyllas samtidigt som SIN:s uppdrag ska omfatta all sådan behandling. Detta överensstämmer med vad som gäller på försvarsunderrättelseområdet där Statens inspektion för försvarsunderrättelseverksamhet utövar tillsyn parallellt med Datainspektionen. Utredningen har gjort bedömningen att Datainspektionen uppfyller

de krav på oberoende och befogenheter som gäller för tillsynsmyndigheten enligt förordningen och direktivet. Enligt utredningen saknar däremot SIN flera befogenheter som krävs enligt direktivet. Vidare har utredningen bedömt att Datainspektionen i allt väsentligt motsvarar EU-regleringens krav på tillsynsmyndighetens organisation och på utnämning respektive avsättande av myndighetens chef.

Dataskyddsutredningen och Utredningen om 2016 års dataskyddsdirektiv har utgått från att förslaget om att samla tillsynsansvaret enligt förordningen och direktivet hos Datainspektionen kommer att genomföras. Utredningen om 2016 års dataskyddsdirektiv har i brottsdatalagen, som genomför direktivet, föreslagit att tillsynsmyndigheten ska utöva tillsyn över tillämpningen av den lagen och andra svenska författningar som reglerar behandling av personuppgifter inom direktivets område. Dataskyddsutredningen har i den generella lag som ska komplettera förordningen, dataskyddslagen, föreslagit att förordningen och den lagen ska gälla även vid personuppgiftsbehandling i verksamheter som inte omfattas av unionsrätten och i verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken.

På kamerabevakningsområdet har länsstyrelserna sedan länge utövat operativ tillsyn, inte minst vad gäller frågor om tillstånd till kamerabevakning av platser dit allmänheten har tillträde. Som framgått av den i avsnitt 5 redovisade utvärderingen av kameraövervakningslagen har länsstyrelsernas rättstillämpning blivit allt mer enhetlig, särskilt sedan Datainspektionen fick det centrala tillsynsansvaret på området i samband med införandet av lagen sommaren 2013. Länsstyrelserna har en upparbetad kompetens på området och även en god lokalkännedom som många gånger är till nytta i ärendena.

Samtidigt innebär den nya förordningen, den nya kamerabevakningslagen med en delvis annorlunda reglering än den hittills gällande lagen och den nya generella svenska lagstiftning som ska gälla även för kamerabevakning en helt ny situation. Den ökade rättsliga komplexiteten ställer nya, höga krav i fråga om bl.a. resurser, kompetens och kvalitet. Även den snabba teknikutvecklingen på området kräver att en hög teknisk kompetens kan upprätthållas kontinuerligt. Vidare innebär i sig det förhållandet att länsstyrelserna är 21 stycken en viss risk för oenhetlighet i tillämpningen. Om tillämpningen inte är enhetlig, blir det svårare för den som

avser att bedriva kamerabevakning att tolka praxis och förutse om den planerade bevakningen är tillåten eller inte. Detta kan bli särskilt problematiskt för den som bedriver verksamhet i flera län och vill använda kamerabevakning i denna i olika delar av landet. Att förutsättningarna för kamerabevakning är tydliga är givetvis angeläget även för de enskilda som kan bli föremål för bevakningen.

Datainspektionen har i dag det mest omfattande tillsynsansvaret över personuppgiftsbehandling generellt sett i såväl privat som offentlig verksamhet. Vidare har Datainspektionen både det centrala ansvaret för tillsyn enligt kameraövervakningslagen och det operativa tillsynsansvaret för kameraövervakning av platser dit allmänheten inte har tillträde. I det centrala ansvaret ingår bl.a. att sammanställa rättspraxis, samla in fakta och erfarenheter om teknikutvecklingen och den internationella utvecklingen och utbilda och ge råd åt länsstyrelserna om lagstiftning, praxis och teknik på området. Den operativa tillsynen kräver bedömningar som mycket liknar dem som länsstyrelserna gör i dag. Datainspektionen har följaktligen en samlad och väl upparbetad kompetens och erfarenhet inte bara när det gäller personuppgifts- och integritetsfrågor allmänt sett utan även vad gäller kamerabevakningsfrågor.

Enligt de ovan nämnda utredningarna ska Datainspektionen vara svensk tillsynsmyndighet för personuppgiftsbehandling både enligt EU-regleringen – såväl förordningen som direktivet – och på det område som faller utanför den regleringen, låt vara att några andra myndigheter ska utöva viss parallell tillsyn. Datainspektionen kommer alltså att ha tillsynsansvaret över personuppgiftsbehandling generellt sett och sådan kameraanvändning som inte ska omfattas av kamerabevakningslagen.

Att låta Datainspektionen helt ansvara även för tillsynen enligt kamerabevakningslagen ligger i linje med detta och kan ge stora fördelar. Datainspektionen kan upprätthålla en god överblick över den kamerabevakning som förekommer och över rättsutvecklingen och tekniken inom området. Det kan säkerställa en hög kvalitet, enhetlighet och effektivitet i frågor om tillstånd till kamerabevakning och övriga frågor om kamerabevakning. Det gäller särskilt som EU-regleringen i stora delar är ny och det därför är angeläget med en enhetlig tolkning av förordningen, dataskyddslagen och dess föreskrifter, av brottsdatalagen med föreskrifter och av andra svenska författningar på området. Detsamma gäller delvis för de prövningar

som ska göras enligt den nya kamerabevakningslagen. Att överföra den uppgiften till Datainspektionen kan inte heller anses vara alltför betungande för myndigheten. Antalet tillståndsansökningar enligt dagens lag uppgår till 900–1 000 per år. Antalet ansökningar enligt den nya lagen kan antas bli lägre, eftersom det nya tillståndskravet är snävare utformat än dagens tillståndsplikt. Att samla tillsynen hos Datainspektionen skulle också göra det tydligare vilken myndighet som bär tillsynsansvaret enligt lagen. Till detta kommer att det är tveksamt om länsstyrelserna i alla delar uppfyller de mycket höga krav som i olika avseenden ställs i EU-regleringen på tillsynsmyndighetens roll, organisation och uppgifter.

Det finns följaktligen tungt vägande skäl för att tillsynsansvaret över kamerabevakning helt ska ligga hos Datainspektionen. Skälen för att behålla dagens ordning eller en liknande ordning där länsstyrelsernas operativa tillsyn koncentreras till vissa länsstyrelser är få. Det föreslås därför att Datainspektion ska vara tillsynsmyndighet enligt kamerabevakningslagen och att detta ska regleras genom en bestämmelse i lagen om att den myndighet som regeringen bestämmer utövar tillsyn över kamerabevakning.

Det kan diskuteras om länsstyrelserna fortsatt bör ha någon form av roll i frågor om tillstånd till kamerabevakning eller om undantag från upplysningskravet. Exempelvis skulle yttrande kunna inhämtas från berörd länsstyrelse i ett ärende om tillstånd. En sådan remissordning torde dock vara ovanlig i dylika tillståndsärenden enligt annan lagstiftning. Vidare skulle ordningen kräva just den kompetens och de resurser m.m. som ovan har motiverat att tillsynen flyttas från länsstyrelserna till Datainspektionen. Lokalkännedom i sådana ärenden kan i stället vid behov säkerställas genom att, som föreslagits i tidigare avsnitt, den kommun där kamerabevakningen ska ske ges tillfälle att yttra sig. Det kan också övervägas om länsstyrelserna bör kunna bistå Datainspektionen med mer praktiskt inriktad hjälp på de olika platser runtom i landet där kamerabevakning ska ske. En liknande ordning finns exempelvis i lagen (1974:191) om bevakningsföretag där det föreskrivs att andra myndigheter på begäran ska lämna länsstyrelsen den hjälp som behövs för tillsynen. En sådan ordning ska dock inte gälla för tillsynen över personuppgiftsbehandling enligt förordningen och dataskyddslagen eller enligt brottsdatalagen och bör därför inte heller gälla på kamerabevakningsområdet.

15.2 Tillsynsmyndighetens befogenheter, sanktioner, rättsmedel och skadestånd

Förslag: I ett ärende enligt kamerabevakningslagen hos tillsynsmyndigheten, vid underlåtenhet att bistå den myndigheten i ett sådant ärende och vid överträdelse av bestämmelserna i lagen eller av beslut som meddelats med stöd av lagen ska tillämpas bestämmelser om undersökningsbefogenheter för tillsynsmyndigheten, sanktionsavgifter och skadestånd i

1. dataskyddsförordningen, dataskyddslagen och föreskrifter som meddelats med stöd av den lagen när det gäller kamerabevakning som omfattas av förordningen eller den lagen, eller
2. brottsdatalagen och föreskrifter som meddelats med stöd av den lagen när det gäller kamerabevakning som omfattas av den lagen.

Vid tillämpning av bestämmelser om sanktionsavgifter ska för myndigheter gälla den högre avgiftsnivå som föreskrivs i dataskyddslagen respektive brottsdatalagen.

Tillsynsmyndighetens beslut enligt kamerabevakningslagen, t.ex. i frågor om tillstånd till kamerabevakning och undantag från kravet på upplysning om kamerabevakning samt sanktionsavgift, ska få överklagas till allmän förvaltningsdomstol. Beslut om tillstånd till kamerabevakning och om undantag från kravet på upplysning ska få överklagas även av den kommun där bevakningen ska ske. Som framgått av avsnitt 13 ska sådana beslut också, om kamerabevakningen ska avse en arbetsplats, få överklagas av en organisation som företräder arbetstagarna på arbetsplatsen. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Vid kamerabevakning ska i övrigt i de frågor som inte regleras direkt i kamerabevakningslagen utan i förordningen eller de generella författningarna bestämmelserna där om tillsynsmyndighetens befogenheter, sanktioner, överklagande m.m. gälla i tillämpliga delar.

Bedömning: Något straffansvar för den som bryter mot kamerabevakningslagens bestämmelser eller beslut som meddelats med stöd av lagen bör inte kunna följa. Inte heller bör det finnas någon möjlighet för tillsynsmyndigheten att förena ett föreläggande med vite.

Skälen för förslaget och bedömningen

Utgångspunkter för befogenheter och sanktioner

I dataskyddsförordningen finns bestämmelser om vilka uppgifter och befogenheter som tillsynsmyndigheten har. Myndigheten är behörig att utföra uppgifterna och utöva befogenheterna inom sin egen medlemsstats territorium. Vid gränsöverskridande personuppgiftsbehandling, då det finns flera behöriga tillsynsmyndigheter, är ansvarig myndighet tillsynsmyndigheten för den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga eller enda verksamhetsställe. I förordningen finns vidare bestämmelser om sanktioner vid överträdelser av förordningens bestämmelser.

Även i dataskyddsdirektivet finns bestämmelser om tillsyn och sanktioner, som till stora delar har samma eller liknande innehåll som bestämmelserna i förordningen.

Enligt kameraövervakningslagen har länsstyrelserna och Datainspektionen vissa befogenheter, exempelvis en möjlighet att meddela förelägganden och att förena dessa med vite samt en rätt att få tillträde till övervakningsanläggningar. Några bestämmelser om samarbete med andra länders tillsynsmyndigheter finns inte. I lagen finns bestämmelser om straffansvar för den som bryter mot t.ex. tillstånds- eller upplysningsplikten.

Som framgått av avsnitt 7 överensstämmer bestämmelserna i kameraövervakningslagen endast delvis med förordningens och direktivets bestämmelser, som är mer omfattande än lagens. Flertalet av förordningens bestämmelser kommer att gälla direkt i Sverige och kräver inte några kompletterande svenska bestämmelser. Vidare får kamerabevakningslagen inte innehålla bestämmelser som enbart upprepar eller avviker från innehållet i förordningen. I några avseenden tillåter dock förordningen kompletterande nationell reglering, t.ex. i fråga om befogenheter för tillsynsmyndigheten. På direktivets område krävs svenska bestämmelser om tillsyn och sanktioner som

uppfyller direktivets krav. Direktivet tillåter vidare att det i nationell rätt föreskrivs starkare skyddsåtgärder än de som fastställs i direktivet.

Som utgångspunkter för de analyser som görs nedan gäller att kamerabevakningslagens bestämmelser ska vara förenliga med bestämmelserna i förordningen och direktivet och även i övrigt bör anpassas till den regleringen. Vidare bör lagen endast innehålla de bestämmelser som särskilt behövs och dessa bör – så långt det är förenligt med EU-regleringen och ändamålsenligt – vara desamma för all kamerabevakning. Som en ytterligare utgångspunkt ska gälla att det inte bör införas bestämmelser som avviker från förslag som lagts av andra utredningar i samma eller närliggande frågor. I avsnitt 10.1 har föreslagits att kamerabevakningslagen ska innehålla en generell bestämmelse som reglerar förhållandet till andra bestämmelser om behandling av personuppgifter.

Tillsynsmyndighetens befogenheter och sanktioner vid personuppgiftsbehandling i allmänhet

Tillsynsmyndighetens – Datainspektionens – uppgifter och befogenheter vid personuppgiftsbehandling i allmänhet samt möjlighet att tillgripa sanktioner kommer att följa direkt av förordningen för personuppgiftsbehandling på det område som omfattas av förordningen.

Tillsynsmyndigheten ska ha vissa utredningsbefogenheter, t.ex. en befogenhet att från den personuppgiftsansvarige eller personuppgiftsbiträdet få tillgång till alla personuppgifter och all information som myndigheten behöver för att kunna fullgöra sina uppgifter och rätt att få tillträde till lokaler som tillhör en personuppgiftsansvarig eller ett personuppgiftsbiträde, inklusive tillgång till utrustning och andra medel för personuppgiftsbehandling. Tillsynsmyndigheten ska vidare ha vissa korrigerande befogenheter. Exempelvis ska myndigheten kunna utfärda varning, utfärda förelägganden som knyter an till bestämmelser i förordningen och tillfälligt eller definitivt kunna begränsa, inklusive förbjuda, en behandling av personuppgifter. Tillsynsmyndigheten ska även samarbeta med och assistera tillsynsmyndigheterna i de andra medlemsstaterna.

Vidare ska tillsynsmyndigheten vid överträdelser av förordningens bestämmelser besluta om administrativa sanktionsavgifter mot privat-

rättsliga subjekt. Detsamma gäller vid underlåtenhet att rätta sig efter tillsynsmyndighetens instruktioner, förelägganden eller beslut. Vid beslut om sanktionsavgift och dess storlek ska bl.a. beaktas överträdelsens karaktär, svårighetsgrad och varaktighet samt om överträdelsen skett med uppsåt eller av oaktsamhet, även om det inte krävs att överträdelsen har skett uppsåtligen eller av oaktsamhet. Andra faktorer som ska beaktas är antalet berörda, vilken skada de har lidit, om den ansvarige har försökt förebygga eller i efterhand komma till rätta med överträdelsen och eventuell ekonomisk vinst som görs eller ekonomisk förlust som undviks genom överträdelsen. När en sanktionsavgift fastställs mot en fysisk person torde den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation kunna beaktas. Om en sådan avgift skulle innebära en oproportionell börda för en fysisk person, får en reprimand utfärdas i stället. För något mindre allvarliga överträdelser, såsom överträdelse av kravet på konsekvensbedömning, är maxbeloppet tio miljoner euro eller två procent av den globala årsomsättningen när det gäller företag beroende på vilket belopp som är högst. För allvarligare överträdelser, t.ex. överträdelse av de grundläggande principerna för behandling, överträdelse av rätten till information, rättelse eller radering eller underlåtenhet att rätta sig efter tillsynsmyndighetens instruktioner, förelägganden eller beslut, är maxbeloppet 20 miljoner euro eller fyra procent av den globala årsomsättningen.

Utredningen om tillsynen över den personliga integriteten har ansett att det saknas behov av att föreskriva ytterligare befogenheter för tillsynsmyndigheten utöver vad som följer av förordningen, en bedömning som Dataskyddsutredningen och Utredningen om 2016 års dataskyddsdirektiv inte har ifrågasatt.

Dataskyddsutredningen har däremot föreslagit att det i dataskyddslagen föreskrivs att tillsynsmyndighetens befogenheter enligt förordningen även ska gälla vid myndighetens tillsyn över bestämmelser i den lagen och i andra författningar som kompletterar förordningen. Några bestämmelser som ger myndigheten möjlighet att tillgripa tvångsåtgärder, t.ex. med polishjälp, för att få tillträde till lokaler har inte ansetts behövas och inte heller ansetts lämpliga.

Vidare har utredningen föreslagit att sanktionsavgifter enligt förordningen även ska få riktas mot statliga och kommunala myndigheter. Som skäl för det har anförts bl.a. att dataskyddsregleringen syftar till att skydda enskildas integritet och att detta intresse väger

lika tungt när personuppgifter behandlas i det allmännas verksamhet, att själva personuppgiftsbehandlingen sker på i stort sett samma villkor och enligt samma regelverk som i privat sektor samt att behovet av avskräckande sanktioner inte torde vara mindre när det gäller myndigheters behandling.

Utredningen har föreslagit att sanktionsavgiften för myndigheter ska kunna uppgå till högst tio miljoner kronor för mindre allvarliga överträdelser och högst 20 miljoner kronor för allvarliga överträdelser. När det gäller avgifternas storlek har utredningen uttalat att det inte finns något utrymme att i svensk författning bestämma fasta belopp för vissa överträdelser men att förordningens möjlighet för en medlemsstat att bestämma i vilken utsträckning myndigheter ska kunna påföras avgifter innebär att medlemsstaterna har utrymme att bestämma ett tak för de belopp som kan påföras myndigheter. Utredningen har ansett att sanktionsavgifter som påförs myndigheter beloppsmässigt bör ligga i paritet med andra sanktionsavgifter i svensk rätt och även anfört bl.a. att skillnader mellan sanktionsavgifternas storlek utanför respektive innanför myndighetssfären kan motiveras av att personuppgiftsansvariga i den privata sektorn kan vara multinationella företag där det krävs synnerligen höga sanktionsbelopp för att de ska vara kännbara medan för myndigheter även en något lägre avgift kan förväntas påverka agerandet i önskad riktning. Utredningen har också föreslagit bestämmelser om förfarandet vid beslut om sanktionsavgifter och om verkställighet av avgifterna.

Dataskyddsutredningen har vidare gjort bedömningen att något straff inte ska kunna ådömas den som bryter mot förordningen. Utredningen har redogjort för de kriterier som måste vara uppfyllda för att en kriminalisering ska vara godtagbar (se bl.a. SOU 2013:38) och ansett att eftersom ansvaret för överträdelser av förordningen i huvudsak kommer att läggas på personuppgiftsansvariga och personuppgiftsbiträden – vilka i flertalet fall är juridiska personer –, bör de mycket kännbara avgifter som kan påföras enligt förordningen vara väsentligt mer effektiva i den meningen att de har en mer avhållande effekt än straffrättsliga sanktioner. Utredningen har vidare ansett att det från resurssynpunkt är mer effektivt att låta tillsynsmyndigheten sanktionera överträdelser, eftersom sådana sannolikt i stor utsträckning kommer att upptäckas och utredas av den myndigheten. Utredningen har även pekat på att ett straffansvar kan

aktualisera det s.k. dubbelbestraffningsförbudet, som finns både i den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna och i Europeiska unionens stadga om de grundläggande rättigheterna.

Utredningen har därutöver ansett att tillsynsmyndigheten inte bör ha en möjlighet att förena sina förelägganden med vite. Som skäl har anförts att sanktionsavgifterna kan användas framåtsyftande, dvs. för att säkerställa ett agerande i enlighet med tillsynsmyndighetens pålagor, genom att det erinras om att sådana avgifter kan utgå om ett föreläggande eller beslut inte följs. Utredningen har också pekat på det skadeståndsansvar som kan följa enligt förordningen och även uttalat att ett vite kan aktualisera dubbelbestraffningsförbudet.

Utredningen har föreslagit att bestämmelserna i förordningen och dataskyddslagen och dess föreskrifter om uppgifter, befogenheter och sanktioner ska tillämpas även vid personuppgiftsbehandling i verksamheter som inte omfattas av unionsrätten och i verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken.

På direktivets område har Utredningen om 2016 års dataskyddsdirektiv föreslagit bl.a. följande i brottsdatalagen och den tillhörande förordningen.

Tillsynsmyndigheten ska utöva allmän tillsyn över personuppgiftsbehandling. På begäran ska myndigheten lämna bistånd till en tillsynsmyndighet i en annan medlemsstat. Tillsynsmyndigheten ska ha vissa undersökningsbefogenheter, nämligen rätt att få tillgång till personuppgifter som behandlas, upplysningar om och dokumentation av behandling av personuppgifter och säkerhetsåtgärder, tillträde till lokaler som den personuppgiftsansvarige eller personuppgiftsbiträdet disponerar och tillgång till utrustning och andra medel för behandling av personuppgifter samt det biträde och annan information som behövs för tillsynen. Myndigheten ska inte ha rätt att med tvång skaffa sig tillträde till lokaler. Att göra lokaler tillgängliga ingår i den personuppgiftsansvariges samarbetsskyldighet i förhållande till tillsynsmyndigheten.

Tillsynsmyndigheten ska vidare ha dels vissa förebyggande befogenheter, dels vissa korrigerande befogenheter. Om tillsynsmyndigheten bedömer att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer och påpekanden förmå den personuppgifts-

ansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig. Myndigheten får även utfärda en skriftlig varning. Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning eller att den personuppgiftsansvarige eller personuppgiftsbiträdet annars inte fullgör sina skyldigheter, får myndigheten förelägga denne att vidta åtgärder för att behandlingen ska bli författningsenlig eller uppfylla andra skyldigheter, förbjuda fortsatt behandling när bristen är allvarlig eller besluta om sanktionsavgift. Det ska inte vara möjligt att förena ett föreläggande med vite.

Överträdelser av bestämmelser om personuppgiftsbehandling ska inte vara straffsanktionerade utöver vad som följer enligt brottsbalken, t.ex. genom bestämmelserna om brott mot tystnadsplikt och tjänstefel. Enligt utredningen skulle ett särskilt straffansvar inte utgöra en tillräckligt effektiv sanktion. I stället ska tillsynsmyndigheten kunna ta ut sanktionsavgifter av personuppgiftsansvariga och i några fall av personuppgiftsbiträden vid överträdelser av vissa bestämmelser i brottsdatalagen. Sanktionsavgift ska också få tas ut vid underlåtenhet att bistå tillsynsmyndigheten eller att rätta sig efter förelägganden eller beslut som myndigheten meddelat. Sanktionsavgift ska kunna påföras både myndigheter, såväl statliga som kommunala, och andra. För mindre allvarliga överträdelser, t.ex. överträdelse av skyldigheten att göra en konsekvensbedömning och samråda med tillsynsmyndigheten, ska avgiften uppgå till minst 25 000 kronor och högst tio miljoner kronor. För allvarliga överträdelser ska avgiften uppgå till minst 50 000 kronor och högst 20 miljoner kronor. Skälen till att sanktionsavgifterna bestämts på detta sätt har angetts vara att de i första hand kan komma i fråga för myndigheter och att de bör ligga i linje med de sanktionsavgifter som finns på andra områden och med storleken på företagsbot.

Vid bedömningen av om en avgift ska tas ut och till vilket belopp ska särskild hänsyn tas till om överträdelsen varit uppsåtlig eller berott på oaktsamhet, vilken skada, fara eller kränkning som överträdelsen inneburit, överträdelsens karaktär, svårhetsgrad och varaktighet, vad den personuppgiftsansvarige eller personuppgiftsbiträdet gjort för att begränsa skadan och om denne tidigare ålagts att betala sanktionsavgift. Sanktionsavgiften får sättas ned helt eller delvis, om överträdelsen är ringa eller ursäktlig eller om det annars

med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Därutöver ska gälla vissa bestämmelser om förfarandet vid beslut om sanktionsavgifter och om verkställighet av avgifterna.

Befogenheter och sanktioner vid kamerabevakning

De ovan beskrivna uppgifterna, befogenheterna och sanktionerna, som kommer att gälla för personuppgiftsbehandling i allmänhet enligt bestämmelserna i förordningen och dataskyddslagen med föreskrifter eller enligt bestämmelserna i brottsdatalagen och dess föreskrifter, måste – till följd av förordningens direkta tillämplighet respektive kraven i direktivet – eller bör gälla även för kamerabevakning som avses i kamerabevakningslagen i de frågor som inte regleras direkt i lagen. De skäl som anförts för dessa bestämmelser har fog för sig även på kamerabevakningsområdet. Bestämmelserna ska därför gälla för kamerabevakning. Det kan åstadkommas genom den i avsnitt 10.1 föreslagna bestämmelsen om kamerabevakningslagens förhållande till andra bestämmelser. Till skillnad mot vad som gäller enligt dagens kameraövervakningslag innebär det bl.a. att vite, handräckning av Polismyndigheten och straffansvar inte kan komma i fråga vid tillsyn av eller överträdelser vid kamerabevakning enligt sådana bestämmelser.

Vad gäller de frågor som regleras särskilt i kamerabevakningslagen – kravet på tillstånd till kamerabevakning, kravet på upplysning om bevakning och förhandlingsskyldigheten för arbetsgivare – måste också gälla vissa bestämmelser om tillsynsmyndighetens uppgifter och befogenheter samt om sanktioner vid överträdelser. Bestämmelserna i förordningen och de generella författningarna kan inte – om inte annat anges i dessa – gälla direkt, eftersom de är kopplade till de materiella bestämmelser som finns där. Enligt förordningen är det möjligt att i nationell rätt, såsom kamerabevakningslagen, föreskriva ytterligare befogenheter för tillsynsmyndigheten och enligt direktivet får det i nationell rätt föreskrivas starkare skyddsåtgärder än de som följer av direktivet. Det kan vidare konstateras att ett svenskt tillståndskrav, som ju är tillåtet enligt EU-regleringen, av naturliga skäl kräver kompletterande svenska bestämmelser för att tillsynsmyndigheten ska ha nödvändiga verk-

tyg i tillståndsförfarandet och vid överträdelser. Följaktligen kan relevanta bestämmelser i förordningen, dataskyddslagen och dess föreskrifter respektive brottsdatalagen och dess föreskrifter i och för sig göras tillämpliga även i fråga om de nämnda bestämmelserna i kamerabevakningslagen.

När det gäller upplysningar, tillträde till lokaler och dylikt, dvs. sådana befogenheter som i förordningen kallas utredningsbefogenheter och i brottsdatalagen kallas undersökningsbefogenheter, skulle det visserligen många gånger kunna vara tillräckligt att tillämpa bestämmelser i förvaltningslagen (1986:233), som troligen kommer att ersättas av en ny förvaltningslag (se prop. 2016/17:180). De krav som kamerabevakningslagen ska innehålla är sådana att den som vill bedriva kamerabevakning ska vända sig till tillsynsmyndigheten och har ett intresse i saken som gör att behovet av att införa särskilda bestämmelser om upplysningar m.m. i lagen eller av att låta bestämmelserna i förordningen och de generella författningarna gälla framstår som litet.

Emellertid kan det inte uteslutas att det någon gång behövs särskilda sådana krav, t.ex. i ett ärende om återkallelse av tillstånd. Att då låta förordningens och de generella författningarnas bestämmelser gälla är lämpligast. Dessa är, i de delar de kan tillämpas, ändamålsenliga även i ärenden enligt kamerabevakningslagen. En fördel med en sådan lösning är att regleringen då blir densamma som för andra situationer som avser kamerabevakning men som inte regleras direkt i kamerabevakningslagen. Det stämmer väl överens med den angivna utgångspunkten att bestämmelserna bör anpassas till EU-regleringen även i delar där de i och för sig skulle kunna utformas annorlunda. Onödiga olikheter i fråga om kamerabevakning beroende på om en viss skyldighet eller liknande finns direkt i kamerabevakningslagen eller följer av förordningen eller brottsdatalagen kan undvikas. Dessutom uppstår det inte några skillnader jämfört med regleringen och hanteringen av liknande frågor avseende annan personuppgiftsbehandling. Det kan underlätta för såväl tillsynsmyndigheten som enskilda.

Även om det delvis följer redan av den föreslagna generella regleringen, föreslås det därför att bestämmelserna i förordningen, dataskyddslagen och lagens föreskrifter eller brottsdatalagen och den lagens föreskrifter om befogenheter för tillsynsmyndigheten avseende upplysningar etc. ska tillämpas också i ett ärende hos den

myndigheten enligt kamerabevakningslagen, dvs. i en fråga om tillstånd till kamerabevakning, om undantag från upplysningskravet vid kamerabevakning eller om återkallelse eller ändring av ett tillståndsbeslut eller beslut om undantag. Det förra regelverket ska tillämpas vad gäller kamerabevakning som utgör personuppgiftsbehandling som omfattas av förordningens egentliga tillämpningsområde eller av förordningen och dataskyddslagen genom den bestämmelse om detta som finns i den lagen. Det senare regelverket ska tillämpas vad gäller kamerabevakning som utgör personuppgiftsbehandling som omfattas av brottsdatalagen. Det föreslås att ordet undersökningsbefogenheter används som gemensamt begrepp i kamerabevakningslagen för det som i brottsdatalagen benämns undersökningsbefogenheter och i förordningen benämns utredningsbefogenheter. Till skillnad mot vad som gäller enligt kameraövervakningslagen kan handräckning inte komma i fråga i ärenden om kamerabevakning. Vite behandlas nedan.

När det gäller sanktioner för underlåtenhet att bistå tillsynsmyndigheten i ett ärende enligt kamerabevakningslagen eller vid överträdelse av lagens materiella bestämmelser eller av beslut som meddelats med stöd av lagen saknas det skäl att se annorlunda på frågan om vilka sanktioner som kan eller bör gälla än vad Dataskyddsutredningen och Utredningen om 2016 års dataskyddsdirektiv gjort. Det innebär att ett system med en administrativ sanktion – sanktionsavgift – ska införas. Det innebär samtidigt att något straffansvar för den som bryter mot kamerabevakningslagens bestämmelser eller beslut som meddelats med stöd av lagen inte bör kunna följa, vilket skiljer sig mot vad som gäller enligt dagens reglering. Av avsnitt 14 har framgått att ett straffansvar enligt brottsbalken för brott mot tystnadsplikt dock fortsatt ska gälla. Vidare bör det inte finnas någon möjlighet för tillsynsmyndigheten att förena ett föreläggande med vite. Vad gäller vite kan tilläggas att den hittillsvarande användningen av vite enligt kameraövervakningslagen torde ha varit sparsam, särskilt mot sådana subjekt som ska omfattas av den nya lagens tillståndskrav. Något större behov av en särskild vitesbestämmelse i kamerabevakningslagen finns därför inte.

Sanktionssystemet enligt förordningen och dataskyddslagen överensstämmer i stort med sanktionssystemet i brottsdatalagen. Vissa skillnader finns dock. Det skulle därför kunna övervägas att låta enbart det ena gälla för all kamerabevakning för att därigenom

förenkla regleringen på kamerabevakningsområdet. Emellertid skulle det i vissa fall ändå leda till att olika regelsystem ska tillämpas på överträdelser vid kamerabevakning beroende på om det är en överträdelse av en materiell bestämmelse i kamerabevakningslagen eller en överträdelse av en bestämmelse på annat håll som gäller även för kamerabevakning. Om t.ex. enbart förordningens och dataskyddslagens bestämmelser skulle gälla vid överträdelse av de materiella bestämmelserna i kamerabevakningslagen, skulle det innebära att en överträdelse av en bestämmelse i brottsdatalagen – som gäller för kamerabevakning – ska åtföljas av en sanktion enligt brottsdatalagens system medan en överträdelse av en bestämmelse i kamerabevakningslagen ska åtföljas av en sanktion enligt det förstnämnda systemet.

Detta talar för att sanktionssystemet enligt förordningen och dataskyddslagen med föreskrifter ska gälla för sådan kamerabevakning som utgör personuppgiftsbehandling som omfattas av den regleringen medan sanktionssystemet enligt brottsdatalagen och dess föreskrifter ska gälla för sådan kamerabevakning som utgör personuppgiftsbehandling som omfattas av den regleringen. En motsvarande ordning har också föreslagits i avsnitt 14 för ett flertal bestämmelser som ska gälla vid kamerabevakning men som inte finns i kamerabevakningslagen liksom ovan i fråga om befogenheter och sanktioner vid överträdelser av sådana bestämmelser. Vidare är skillnaderna i sanktionssystemen inte så stora att det kan antas medföra några större svårigheter i tillämpningen eller andra konsekvenser som talar mot en sådan ordning. Exempelvis torde den skillnaden som består i att en sanktionsavgift enligt förordningen *ska* påföras medan en sanktionsavgift enligt brottsdatalagen *får* tas ut inte bli särskilt stor i praktiken. Om t.ex. någon bedriver kamerabevakning utan erforderligt tillstånd, ska i regel en sanktionsavgift komma i fråga. Till detta kommer att även för de myndigheter som normalt omfattas av brottsdatalagen kommer ibland förordningen och dataskyddslagen i stället att gälla. Samma skillnader kommer då att gälla vid personuppgiftsbehandling av dessa myndigheter.

Det föreslås därför att sanktionssystemet enligt förordningen och dataskyddslagen eller sanktionssystemet enligt brottsdatalagen ska tillämpas vid underlåtenhet att bistå tillsynsmyndigheten i ett ärende enligt kamerabevakningslagen och vid överträdelse av bestämmelserna i lagen eller av beslut som meddelats med stöd av lagen.

I övrigt ska följande gälla. Som föreslagits i tidigare avsnitt ska tillsynsmyndigheten kunna återkalla ett tillstånd till kamerabevakning eller besluta om nya villkor vid ändrade förhållanden. Vidare ska myndigheten kunna återkalla eller ändra ett beslut om undantag från kravet på upplysning. Sanktionsavgift ska kunna tas ut också när en återkallelse eller en ändring av villkor eller beslut om undantag sker efter överträdelse. Detta är förutsatt i förordningen och direktivet. Inom ramen för bedömningen av om en sanktionsavgift ska utgå och till vilket belopp kan hänsyn tas till ett sådant beslut.

Den högre avgiftsnivå som föreslagits i dataskyddslagen respektive brottsdatalagen för myndigheter – högst 20 miljoner kronor – föreslås gälla vid en myndighets överträdelse av bestämmelserna i kamerabevakningslagen eller av beslut som meddelats med stöd av lagen och vid underlåtenhet att bistå tillsynsmyndigheten i ett ärende enligt lagen. Detta eftersom den nivån kommer att gälla för andra jämförbara överträdelser vid kamerabevakning enligt förordningen eller brottsdatalagen och därför att kraven enligt kamerabevakningslagen syftar till att säkerställa ett starkt integritetsskydd. Vad gäller förhandlingsskyldigheten för arbetsgivare enligt lagen är det dessutom fråga om en s.k. särskild behandlingssituation enligt förordningen där förordningens utrymme att ställa upp specifika nationella krav i syfte att säkerställa skyddet av anställdas rättigheter och friheter vid personuppgiftsbehandling har nyttjats.

Vad särskilt gäller överträdelse av kravet på upplysning om kamerabevakning ska påpekas att det inte i brottsdatalagen men däremot i förordningen medges att sanktionsavgift tas ut när en liknande skyldighet där att lämna information har överträtts. Vid kamerabevakning är upplysning om bevakningen av sådan vikt att det måste kunna utgå en sanktionsavgift vid överträdelse av upplysningskravet. Detta krav i kamerabevakningslagen och i dess föregångare är grundläggande i lagstiftningen på området och syftar till att förhindra att människor bevakas i hemlighet.

Sammanfattningsvis föreslås följande. I ett ärende enligt kamerabevakningslagen hos tillsynsmyndigheten, vid underlåtenhet att bistå den myndigheten i ett sådant ärende och vid överträdelse av bestämmelserna i lagen eller av beslut som meddelats med stöd av lagen ska tillämpas bestämmelser om undersökningsbefogenheter för tillsynsmyndigheten och sanktionsavgifter i dataskyddsförordningen, dataskyddslagen och föreskrifter som meddelats med stöd av den

lagen när det gäller kamerabevakning som omfattas av förordningen eller den lagen eller i brottsdatalagen och föreskrifter som meddelats med stöd av den lagen när det gäller kamerabevakning som omfattas av den lagen. Vid tillämpning av bestämmelser om sanktionsavgifter ska för myndigheter gälla den högre avgiftsnivå som föreskrivs i dataskyddslagen respektive brottsdatalagen. Det innebär att sanktionsavgiften kan bestämmas till upp till 20 miljoner kronor för en myndighet.

Enligt dataskyddslagen ska förordningen och den lagen samt dess föreskrifter tillämpas också vid personuppgiftsbehandling, och därmed vid kamerabevakning, som faller utanför förordningens egentliga tillämpningsområde och utanför direktivets tillämpningsområde, om inte annat föreskrivs i annan författning.

Rättsmedel och skadestånd

Förordningen och direktivet innehåller också bestämmelser om rättsmedel och skadestånd. Som framgått av avsnitt 7 kommer förordningens bestämmelser att gälla direkt. Vissa svenska processuella bestämmelser kan finnas men annars kan svenska bestämmelser som enbart upprepar eller avviker från förordningen inte införas. Vidare har framgått att det på direktivets område måste finnas bestämmelser i svensk lagstiftning som uppfyller direktivets krav.

Samma utgångpunkter som angetts i avsnittet ovan gäller vid de överväganden som görs nedan i fråga om rättsmedel och skadestånd.

På förordningens område gäller att varje registrerad som anser att hans eller hennes rättigheter har åsidosatts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med förordningen har rätt till ett effektivt rättsmedel. Vidare har en person som har lidit materiell eller immateriell skada till följd av en överträdelse av förordningen rätt till ersättning från den personuppgiftsansvarige för den uppkomna skadan. Även ett personuppgiftsbiträde kan bli skadeståndsskyldigt under vissa förutsättningar. Dessutom ska varje fysisk eller juridisk person ha rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut rörande denne som meddelats av en tillsynsmyndighet.

Dataskyddsutredningen har på förordningens område föreslagit att dataskyddslagen ska innehålla en bestämmelse om att vissa beslut enligt förordningen som en personuppgiftsansvarig myndighet meddelar med anledning av att en registrerad utövar sina rättigheter ska få överklagas till allmän förvaltningsdomstol. Bestämmelsen har sin grund i allmänna förvaltningsrättsliga principer. Utredningen har vidare gjort bedömningen att rätten till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde tillgodoses genom möjligheten enligt gällande svensk rätt att föra talan om skadestånd i allmän domstol. När det gäller tillsynsmyndighetens beslut enligt förordningen och dess beslut i enskilda fall, bl.a. beslut om sanktionsavgifter enligt dataskyddslagen, ska dessa få överklagas till allmän förvaltningsdomstol. Utredningen har dessutom föreslagit en bestämmelse i dataskyddslagen med innebörd att förordningens rätt till ersättning även ska gälla vid överträdelser av bestämmelser i den lagen och i andra författningar som kompletterar förordningen. Enligt dataskyddslagen ska dessa bestämmelser i förordningen och lagen tillämpas även vid behandling av personuppgifter i verksamheter som inte omfattas av unionsrätten och i verksamhet som avser den gemensamma utrikes- och säkerhetspolitiken.

Utredningen om 2016 års dataskyddsdirektiv har på direktivets område ansett att rätten att föra talan mot en personuppgiftsansvarig eller ett personuppgiftsbiträde om den registrerades rättigheter har kränkts genom personuppgiftsbehandlingen inte kräver några lagstiftningsåtgärder. Däremot har utredningen föreslagit att när den personuppgiftsansvarige är en myndighet ska vissa beslut som gäller registrerades rättigheter kunna överklagas till allmän förvaltningsdomstol. Vidare har föreslagits att tillsynsmyndighetens beslut enligt brottsdatalagen eller föreskrifter som meddelats i anslutning till den får överklagas till allmän förvaltningsdomstol. När det gäller skadestånd har utredningen föreslagit bestämmelser i brottsdatalagen om att den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandling av personuppgifter i strid med den lagen eller föreskrifter som meddelats i anslutning till den har orsakat.

I förordningen liksom i direktivet finns dessutom bestämmelser om att en registrerad, som anser att behandlingen av personuppgifter avseende honom eller henne strider mot förordningen respek-

tive direktivet, ska ha rätt att lämna in ett klagomål till tillsynsmyndigheten. Dataskyddsutredningen har ansett att det inte behövs några svenska bestämmelser om rätten att lämna in klagomål men däremot föreslagit bestämmelser om att den registrerade kunna begära besked i frågan om tillsynsmyndigheten avser att utöva tillsyn, om myndigheten inte inom tre månader behandlar hans eller hennes klagomål. Myndigheten ska då inom två veckor antingen lämna ett sådant besked eller i ett särskilt beslut avslå begäran. Ett avslagsbeslut ska kunna överklagas till allmän förvaltningsdomstol. Om domstolen bifaller överklagandet, ska den förelägga tillsynsmyndigheten att inom en bestämd tid lämna besked till den registrerade i frågan om tillsyn kommer att utövas. Domstolens beslut ska inte kunna överklagas. Utredningen om 2016 års dataskyddsdirektiv har också gjort bedömningen att en registrerads rätt att lämna in klagomål till en tillsynsmyndighet enligt direktivet inte kräver några lagstiftningsåtgärder, annat än en bestämmelse om att tillsynsmyndigheten ska handlägga sådana klagomål. En särskild reglering om dröjsmålstalan, som motsvarar den som föreslagits i dataskyddslagen, har föreslagits i brottsdatalagen.

Samma bedömningar som dessa utredningar gjort i de nu redovisade frågorna görs såvitt gäller kamerabevakning som avses i kamerabevakningslagen. Vidare ska de bestämmelser som föreslagits av utredningarna i de generella lagarna gälla även för kamerabevakning i fråga om de materiella bestämmelser som inte finns i kamerabevakningslagen utan i förordningen och dataskyddslagen eller i brottsdatalagen och som också ska gälla för kamerabevakning. Det kan åstadkommas genom den i avsnitt 10.1 föreslagna bestämmelsen om kamerabevakningslagens förhållande till andra bestämmelser.

I sådana frågor som regleras direkt i kamerabevakningslagen, t.ex. frågor om tillstånd till kamerabevakning och undantag från kravet på upplysning om kamerabevakning, föreslås att det ska vara möjligt att överklaga tillsynsmyndighetens beslut till allmän förvaltningsdomstol och att det ska krävas prövningstillstånd vid överklagande till kammarrätten. Detta överensstämmer med vad som gäller enligt förvaltningslagen och kameraövervakningslagen. Eftersom beslut i ärenden enligt kamerabevakningslagen kommer att meddelas endast av Datainspektionen och inte som tidigare även av olika länsstyrelser, kommer – om inte annat föreskrivs – handläggningen att koncentreras till en enda förvaltningsrätt och en kammar-

rätt. Olika skäl kan visserligen anföras mot en sådan koncentration. Emellertid kan de skäl som anförts för att samla tillsynen hos Datainspektionen åberopas också för att koncentrera prövningen hos domstol. För det talar dessutom att överklaganden av Datainspektionens beslut i andra frågor enligt förordningen och dataskyddslagen eller enligt brottsdatalagen kommer att koncentreras till samma instanser. Det föreslås därför inte någon särskild reglering som fortsatt innebär behörighet för flera domstolar.

I avsnitt 13 har föreslagits att när ett beslut om tillstånd till kamerabevakning eller om undantag från upplysningskravet avser en arbetsplats ska beslutet få överklagas även av en organisation som företräder arbetstagarna på arbetsplatsen.

I dag gäller enligt kameraövervakningslagen att ett beslut om tillstånd till kameraövervakning eller om undantag från upplysningsplikten får överklagas av den kommun där övervakningen ska ske. I tidigare avsnitt har föreslagits att kommuner fortfarande ska ha en roll, om än mer begränsad än enligt dagens lag, i ärenden om tillstånd till kamerabevakning och om undantag från upplysningskravet enligt kamerabevakningslagen. I linje med det föreslås att beslut om tillstånd och om undantag ska få överklagas av den kommun där kamerabevakningen ska ske.

Enligt kameraövervakningslagen gäller vidare att den myndighet som regeringen bestämmer får överklaga ett beslut om kameraövervakning av en plats dit allmänheten har tillträde för att ta till vara allmänna intressen. Datainspektionen är i dag den myndighet som kan överklaga i den angivna situationen. Som framgått ska Datainspektionen vara ensam tillsynsmyndighet enligt kamerabevakningslagen och, till skillnad mot vad som gäller i dag, därmed vara den myndighet som beslutar i frågor om tillstånd och om undantag från kravet på upplysning. Det innebär att när någon överklagar ett beslut av Datainspektionen till förvaltningsdomstol blir inspektionen dennes motpart. Datainspektionen får då också en rätt att överklaga domstolens avgörande förutsatt att avgörandet har gått emot inspektionen. Någon särskild ordning för överklagande när den enskilde inte överklagar Datainspektionens beslut, t.ex. en möjlighet för Justitiekanslern att överklaga, bör inte införas. En motsvarande ordning enligt annan lagstiftning är relativt ovanlig. En sådan skulle också kräva särskilda resurser i viss omfattning. Dessutom framstår det praktiska behovet av en sådan ordning som

begränsat. Beslut enligt kamerabevakningslagen kommer till följd av utformningen av det nya tillståndskravet många gånger att avse myndigheter. I ett fall där en myndighet anser ett överklagande vara befogat kan myndigheten förutsättas ha egna resurser att överklaga. Följaktligen behövs inte någon motsvarighet till bestämmelsen i kameraövervakningslagen i den nya lagen.

I fråga om formerna för överklagande av tillsynsmyndighetens beslut, vilken överklagandefrist som ska gälla m.m. bör inte avvikas från förvaltningslagens bestämmelser. Några särskilda bestämmelser i sådana frågor föreslås därför inte.

Vad sedan gäller skadestånd bör sådant kunna utgå vid överträdelse av de materiella bestämmelserna i kamerabevakningslagen, inklusive vid överträdelse av förhandlingsskyldigheten för arbetsgivare, eller av beslut som meddelats med stöd av lagen. Syftet med regleringen i lagen är att säkerställa ett starkt integritetsskydd. En skadeståndsskyldighet är därför rimlig. I dataskyddslagen har föreslagits en skadeståndsbestämmelse som gäller även vid överträdelser av andra lagar som kompletterar förordningen. Någon särskild bestämmelse skulle därför inte krävas i kamerabevakningslagen. Motsvarande bestämmelse har dock inte föreslagits i databrottslagen. Utredningen om 2016 års dataskyddsdirektiv avser att återvända till frågan i sitt kommande slutbetänkande. Av såväl tydlighetsskäl som sakliga skäl föreslås därför att det i kamerabevakningslagen föreskrivs att bestämmelserna om skadestånd i förordningen eller brottsdatalagen ska tillämpas.

En särskild fråga är om tillsynsmyndigheten ska kunna bestämma att myndighetens beslut enligt kamerabevakningslagen, t.ex. beslut om tillstånd, ska gälla omedelbart. En sådan bestämmelse finns i kameraövervakningslagen. Någon motsvarande möjlighet har inte föreslagits i dataskyddslagen eller brottsdatalagen. I regeringens förslag till ny förvaltningslag har det tagits in generella bestämmelser om i vilka fall beslut får verkställas. Huvudregeln är att ett överklagbart beslut får verkställas när överklagandetiden har gått ut förutsatt att det inte har överklagats. Från denna huvudregel görs vissa undantag. Ett beslut får verkställas omedelbart bl.a. om beslutet gäller endast tillfälligt eller om ett väsentligt allmänt eller enskilt intresse kräver det. Myndigheten ska då först noga överväga om det finns skäl att avvakta med att verkställa beslutet på grund av

att det medför mycket ingripande verkningar för någon enskild eller någon annan omständighet.

Beslut enligt kamerabevakningslagen kan vara antingen positiva eller negativa för den som bedriver kamerabevakning. Exempelvis kan ett beslut innebära att tillstånd till kamerabevakning meddelas i ett fall där behovet av bevakningen är trängande. I en sådan situation är det fullt rimligt att bevakningen kan komma i gång så snart som möjligt. Även när ett beslut har gått emot en kommun eller en arbetstagarorganisation som yttrat sig i ett ärende enligt kamerabevakningslagen – men varit positivt för den bedriver kamerabevakning – bör det finnas en viss möjlighet för att beslutet ska få verkställas omedelbart. En avvägning får då ske mellan motstående intressen i det enskilda fallet. Vad gäller beslut som är negativa för den som bedriver kamerabevakning, t.ex. beslut om återkallelse av tillstånd eller återkallelse av beslut om undantag från upplysningskravet, finns det däremot i regel inte anledning att avvika från vad som är huvudregeln enligt annan lagstiftning. En möjlighet för tillsynsmyndigheten att bestämma att dess beslut ska gälla omedelbart bör alltså finnas. Den reglering som föreslagits i den nya förvaltningslagen kan tillgodose det nu beskrivna. Någon särskild bestämmelse i kamerabevakningslagen föreslås därför inte.

Hos domstol kommer efter överklagande bestämmelserna i förvaltningsprocesslagen (1971:291) att gälla. Det innebär bl.a. att domstolen kan besluta att det överklagade beslutet tills vidare inte ska gälla.

Sammanfattningsvis föreslås följande. Tillsynsmyndighetens beslut enligt kamerabevakningslagen, t.ex. i frågor om tillstånd till kamerabevakning och undantag från kravet på upplysning om kamerabevakning samt sanktionsavgift, ska få överklagas till allmän förvaltningsdomstol. Beslut om tillstånd till kamerabevakning och om undantag från kravet på upplysning ska få överklagas även av den kommun där bevakningen ska ske. Som framgått av avsnitt 13 ska sådana beslut också, om kamerabevakningen ska avse en arbetsplats, få överklagas av en organisation som företräder arbetstagarna på arbetsplatsen. Prövningstillstånd ska krävas vid överklagande till kammarrätten. Vid överträdelse av bestämmelserna i lagen eller av beslut som meddelats med stöd av lagen ska bestämmelser om skadestånd i antingen förordningen, dataskyddslagen och föreskrifter som meddelats med stöd av den lagen eller brottsdatalagen

och föreskrifter som meddelats med stöd av den lagen tillämpas. Det förra regelverket ska tillämpas vad gäller kamerabevakning som omfattas av förordningen eller dataskyddslagen och det senare vad gäller kamerabevakning som omfattas av brottsdatalagen.

15.3 En föreskriftsrätt?

Förslag: I kamerabevakningslagen ska införas en föreskriftsrätt som avser avgifter för ansökningar enligt lagen.

Bedömning: Någon rätt för tillsynsmyndigheten att meddela föreskrifter för tillämpningen av kamerabevakningslagen behövs inte.

Skälen för förslaget och bedömningen

En föreskriftsrätt för tillsynsmyndigheten?

I det lagstiftningsärende som ledde till införandet av kameraövervakningslagen väckte flera remissinstanser frågan om den centrala tillsynsmyndigheten på kamerabevakningsområdet, Datainspektionen, borde ges en rätt att meddela föreskrifter för tillämpningen av lagen (prop. 2012:13/115 s. 132). En sådan föreskriftsrätt ansågs kunna leda till en enhetlig rättstillämpning och vara till värdefull hjälp för myndigheter och enskilda, vilket i sin tur kunde leda till ett förstärkt integritetsskydd. Någon föreskriftsrätt infördes dock inte.

Dataskyddsutredningen och Utredningen om 2016 års dataskyddsdirektiv har i sina generella lagar som kompletterar förordningen respektive genomför direktivet föreslagit en relativt omfattande föreskriftsrätt för Datainspektionen på dataskyddsområdet. Denna föreskriftsrätt kommer att gälla även för kamerabevakning i de frågor som inte regleras direkt i kamerabevakningslagen utan i förordningen och de generella lagarna.

Frågan är om det därutöver bör införas en föreskriftsrätt i kamerabevakningslagen som särskilt ska gälla bestämmelserna i den lagen. Det är tveksamt om detta behövs eller ens är lämpligt. De materiella bestämmelserna i lagen är relativt få. De ska vidare tillämpas av Datainspektionen som enda tillsynsmyndighet på kamerabevakningsområdet och av få domstolar. Att tillämpningen är koncen-

trerad på detta sätt kan säkerställa en enhetlig rättstillämpning. Det finns visserligen bestämmelser som kräver tolkningar. Det gäller främst begreppet ”uppgift av allmänt intresse” i bestämmelsen om i vilka fall tillståndskravet gäller och vad som ska förstås med ”berättigade ändamål” i bestämmelsen om hur tillståndsprövningen ska gå till. Begrepp av sådana slag i en lagstiftning bör normalt, i den mån de behöver tolkas, ges sin närmare innebörd i rättstillämpningen av en eventuell tillsynsmyndighet och av domstolar. Det förstnämnda begreppet är dessutom ett unionsrättsligt begrepp och kan därmed inte fritt ges ett helt bestämt och detaljerat innehåll i svenska föreskrifter. Begreppet kommer troligen att belysas inom ramen för det unionsrättsliga samarbetet om den nya dataskyddsregleringen. Vidare kommer domstolspraxis, både i Sverige och i andra medlemsstater, att utvecklas kring begreppet. Ytterst är det EU-domstolen som avgör begreppets innebörd. Även begreppet berättigade ändamål knyter an till dataskyddsregleringen. Med hänsyn härtill görs bedömningen att det inte behövs någon rätt för tillsynsmyndigheten att meddela föreskrifter för tillämpningen av kamerabevakningslagen. Det hindrar inte tillsynsmyndigheten från att på annat sätt informera om hur myndigheten eller hur man inom EU ser på exempelvis dessa begrepp.

Avgifter

Enligt kameraövervakningslagen får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om avgift för en ansökan enligt lagen.

Förordningen och direktivet innehåller i princip ett förbud mot avgiftsbeläggning för tillsynsmyndighetens handläggning av frågor enligt EU-regleringen. Det krav på tillstånd till kamerabevakning som ska gälla enligt kamerabevakningslagen utgör dock en specifik svensk reglering, som är tillåten enligt förordningen och direktivet. Något hinder mot att ta ut avgifter för ansökningar om tillstånd enligt lagen föreligger därför inte. Detsamma får anses gälla ansökningar om undantag från upplysningskravet enligt kamerabevakningslagen. Å andra sidan bör som utgångspunkt gälla detsamma som gäller enligt EU-regleringen. Vidare kommer tillståndskravet i första hand att träffa myndigheter, vilket innebär – om ansökningar

ska vara avgiftsbelagda – att en avgiftsbeläggning främst kommer att träffa statliga medel. Dagens avgiftssystem torde också vara relativt komplicerat och under alla förhållanden kräva förenklingar.

Mot denna bakgrund bör det i kamerabevakningslagen öppnas för att på lägre normgivningsnivå avgiftsbelägga ansökningar. Det föreslås alltså att det i kamerabevakningslagen ska införas en föreskriftsrätt som avser avgifter för ansökningar enligt lagen.

16 Ikraftträdande- och övergångsbestämmelser

Förslag: Kamerabevakningslagen och ändringen i offentlighets- och sekretesslagen (2009:400) ska träda i kraft den 25 maj 2018 samtidigt som kameraövervakningslagen ska upphöra att gälla.

Tillstånd till kameraövervakning som har beslutats enligt den äldre lagen och som avser kamerabevakning som omfattas av kravet på tillstånd i den nya lagen ska fortfarande gälla. Övriga tillstånd som har beslutats enligt den äldre lagen ska inte längre gälla.

Undantag från upplysningsplikten som har beslutats enligt den äldre lagen ska fortfarande gälla.

Anmälningar som har gjorts enligt den äldre lagen ska inte längre gälla.

Ärenden som har inletts hos länsstyrelserna enligt den äldre lagen men ännu inte har avgjorts ska överlämnas till den myndighet som ska utöva tillsyn över kamerabevakning enligt den nya lagen.

Mål som har överklagats till annan förvaltningsrätt än Förvaltningsrätten i Stockholm eller till annan kammarrätt än Kammarrätten i Stockholm enligt den äldre lagen men ännu inte har avgjorts ska överlämnas till Förvaltningsrätten i Stockholm respektive Kammarrätten i Stockholm. Om ett mål har överklagats av en enskild, ska den myndighet som ska utöva tillsyn över kamerabevakning enligt den nya lagen vara motpart.

Äldre föreskrifter om skadestånd ska fortfarande gälla för skada som har orsakats före ikraftträdandet.

Äldre föreskrifter ska fortfarande gälla för överträdelser som har skett före ikraftträdandet.

Vad gäller ändringen i offentlighets- och sekretesslagen ska äldre föreskrifter fortfarande gälla för uppgift som har inhämtats före ikraftträdandet.

Skälen för förslaget

Ikraftträdande

Av dataskyddsförordningens artikel 99 följer att förordningen ska tillämpas från och med den 25 maj 2018. Dataskyddsutredningen har föreslagit att dataskyddslagen, som innehåller kompletterande bestämmelser till förordningen, och föreskrifter som meddelats med stöd av den lagen ska träda i kraft den dagen och att personuppgiftslagen samtidigt ska upphöra att gälla.

Enligt artikel 63 i dataskyddsdirektivet ska medlemsstaterna senast den 6 maj 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att genomföra direktivet. Bestämmelserna ska tillämpas av medlemsstaterna från och med samma dag. Utredningen om 2016 års dataskyddsdirektiv har föreslagit att brottsdatalagen och dess föreskrifter ska träda i kraft den 1 maj 2018.

Kamerabevakningslagen innehåller bestämmelser som både kompletterar förordningen och genomför direktivet samtidigt som den innehåller hänvisningar till såväl förordningen och dataskyddslagen med föreskrifter som brottsdatalagen med föreskrifter. Kamerabevakningslagen kan därför inte träda i kraft förrän samtliga dessa regleringar börjar gälla, dvs. tidigast den 25 maj 2018. Det innebär att direktivet inte kommer att genomföras på kamerabevakningsområdet genom kamerabevakningslagen inom den föreskrivna tiden. Emellertid kommer den nuvarande kameraövervakningslagen och den nya brottsdatalagen att gälla under den tiden och därigenom genomföra direktivet på detta område. Kamerabevakningslagen bör träda i kraft så snart som möjligt. Det föreslås därför att lagen ska träda i kraft den 25 maj 2018. Samtidigt ska kameraövervakningslagen upphöra att gälla. Samma ikraftträdande föreslås i fråga om ändringen i offentlighets- och sekretesslagen (2009:400).

Övergångsbestämmelser

Dataskyddsutredningen har på det område som omfattas av förordningen eller dataskyddslagen föreslagit bl.a. att äldre föreskrifter fortfarande ska gälla för ärenden som har inletts hos Datainspektionen men inte avgjorts före ikraftträdandet, för överklagande av beslut som har meddelats med stöd av dessa föreskrifter och för överträdelser som har skett före ikraftträdandet. Utredningen har dessutom föreslagit att äldre föreskrifter om skadestånd fortfarande ska gälla för skada som har orsakats före upphävandet.

Utredningen om 2016 års dataskyddsdirektiv har på det område som omfattas av direktivet föreslagit bl.a. följande övergångsbestämmelser till brottsdatalagen.

- Sanktionsavgift ska få beslutas endast för överträdelser som har begåtts efter ikraftträdandet. För överträdelser som begåtts före ikraftträdandet ska fortfarande äldre föreskrifter gälla.
- Ärenden om tillsyn över personuppgiftsbehandling och som Datainspektionen eller Säkerhets- och integritetsskyddsnämnden inte har avgjort före ikraftträdandet ska handläggas enligt äldre föreskrifter.
- Äldre föreskrifter ska fortfarande gälla för överklagande av beslut som meddelats före ikraftträdandet.
- Bestämmelser om skadestånd i personuppgiftslagen ska fortfarande gälla för skada som har orsakats före ikraftträdandet.

De nu redovisade övergångsbestämmelserna kommer att gälla, i de delar de är relevanta, i fråga om bestämmelser i de angivna regleringarna som ska gälla även för kamerabevakning som avses i kamerabevakningslagen.

I fråga om de materiella bestämmelser för kamerabevakning som finns i kamerabevakningslagen gäller enligt allmänna principer att bestämmelserna gäller från och med att de träder i kraft, om något annat inte föreskrivs i övergångsbestämmelser. Frågan är då om det behövs några sådana bestämmelser.

När lagen träder i kraft kommer det att finnas tillstånd till kamerabevakning som har beslutats enligt kameraövervakningslagen och som avser sådan kamerabevakning som även omfattas av tillståndskravet enligt den nya lagen. Motsvarande gäller beslut om undantag

från den äldre lagens upplysningsplikt. De förra uppgår till ett stort antal. Den prövning som ska göras enligt den nya lagen i fråga om tillstånd till kamerabevakning och om undantag från upplysningskravet kommer inte att vara strängare än enligt den äldre lagen. Visserligen kan prövningen indirekt sägas innefatta en bedömning av om kamerabevakningen är laglig i den mening som krävs enligt förordningen och dataskyddslagen eller enligt brottsdatalagen, vartill kamerabevakningslagen hänvisar. Emellertid måste detta ha gällt även tidigare, eftersom ett sådant krav funnits i 1995 års dataskyddsdirektiv och personuppgiftslagen. Något behov av att ompröva befintliga beslut finns följaktligen inte. En övergångsbestämmelse om att sådana tillstånd fortfarande ska gälla föreslås därför liksom en övergångsbestämmelse om att beslut om undantag från upplysningsplikten fortfarande ska gälla.

När det gäller tillstånd som har beslutats enligt kameraövervakningslagen och som avser kamerabevakning som inte längre ska omfattas av något krav på tillstånd enligt den nya kamerabevakningslagen ska dessa upphöra att gälla. Sådana tillstånd avser kamerabevakning på förordningens tillämpningsområde och bevakningen ska i stället stå i överenstämmelse med bestämmelserna i förordningen och dataskyddslagen och dess föreskrifter. En utgångspunkt i förordningen är att personuppgiftsbehandling som pågår den 25 maj 2018 då förordningen ska börja tillämpas ska ha bringats i överensstämmelse med förordningen till den dagen. Dataskyddsutredningen har inte föreslagit någon övergångsbestämmelse som ger personuppgiftsansvariga och personuppgiftsbiträden viss tid att efter ikraftträdandet ordna sin behandling så att den blir förenlig med förordningen. Även vad gäller kamerabevakning som inte längre ska vara tillståndsskyldig kan förutsättas att bevakningen kan vara förenlig med förordningen redan från den dag då denna ska börja tillämpas. Av tydlighetsskäl föreslås det därför en övergångsbestämmelse av innebörd att sådana tillstånd inte längre ska gälla när kamerabevakningslagen trätt i kraft, dvs. den 25 maj 2018.

Motsvarande föreslås av tydlighetsskäl i fråga om anmälningar. Även kamerabevakning som tidigare kunnat ske efter endast en anmälan men som framöver inte omfattas av vare sig krav på tillstånd eller krav på anmälan förutsätts alltså kunna bringas i överensstämmelse med förordningen.

Vad gäller ansökningar om tillstånd till kamerabevakning eller om undantag från kravet på upplysning som gjorts enligt den gamla lagen men inte hunnit avgöras före den nya lagens ikraftträdande är det rimligt att de prövas enligt den nya lagen. Det gäller även för prövning av överklaganden i sådana frågor som skett före ikraftträdandet men ännu inte avgjorts. Detsamma gäller andra frågor enligt kameraövervakningslagen som vid ikraftträdandet av lagen är anhängiggjorda i ärenden hos länsstyrelserna eller i mål hos domstolarna. Prövningarna och besluten måste vara förenliga med den nya EU-regleringen från ikraftträdandet och de nya bestämmelserna i kamerabevakningslagen bör därför tillämpas. Särskilt tillståndsbeslut kan dessutom komma att meddelas att gälla för lång tid framöver och det är då inte lämpligt att sådana fattas efter en prövning enligt den gamla lagen. Vidare är prövningen enligt den nya lagen helt ny i vissa avseenden, t.ex. i fråga om vilken kamerabevakning som omfattas av kravet på tillstånd. Lagen är även mer generös för den som vill bedriva kamerabevakning i fråga om bl.a. möjligheterna att få tillstånd till bevakning. I enlighet med de ovan angivna allmänna principerna att nya bestämmelser gäller från och med att de träder i kraft – och att en avvikelse från detta kräver en övergångsbestämmelse – ska alltså ärenden och mål som är anhängiga vid ikraftträdandet handläggas och prövas enligt kamerabevakningslagen.

Vidare är det rimligt att dessa ärenden hos länsstyrelserna överlämnas till den myndighet som ska utöva tillsyn över kamerabevakning enligt den nya lagen, dvs. Datainspektionen. Detsamma gäller mål som enligt den äldre lagen har överklagats till annan förvaltningsrätt än Förvaltningsrätten i Stockholm men inte har hunnit avgöras före ikraftträdandet. Motsvarande gäller mål som har överklagats till annan kammarrätt än Kammarrätten i Stockholm. Förvaltningsrätten i Stockholm respektive Kammarrätten i Stockholm kommer – genom att Datainspektionen blir tillsynsmyndighet – att vara ensam behörig domstol. I ett mål hos domstol som överklagats av en enskild bör den nya tillsynsmyndigheten, inte den tidigare behöriga länsstyrelsen, vara motpart.

Att prövningen av ärendena och målen – som ska ske enligt den nya lagen – redan från början koncentreras hos Datainspektionen respektive de nämnda domstolarna kan bäst säkerställa att tillämpningen håller en hög kvalitet och blir enhetlig samt sker på ett

effektivt sätt. Det gäller särskilt med hänsyn till att den kommer att inrymma frågor som är helt nya enligt kamerabevakningslagen och ibland kan vara komplicerade. Det gäller t.ex. frågor om omfattningen av kravet på tillstånd och de nya eller vidgade intressen av kamerabevakning som ska beaktas särskilt vid tillståndsprövningen. Att de andra förvaltningsrätterna och kammarrätterna under en övergångsperiod skulle behöva sätta sig in i och tillämpa den nya reglering som ska gälla för kamerabevakning skulle inte heller utgöra ett effektivt resursutnyttjande.

Följaktligen ska länsstyrelserna överlämna ärendena till den nya tillsynsmyndigheten. Vidare ska målen överlämnas till de angivna domstolarna. Den nya tillsynsmyndigheten ska vara motpart i ett mål som har överklagats av en enskild. Såvitt gäller målen krävs övergångsbestämmelser om detta, eftersom en domstol inte förlorar sin behörighet till följd av ändrade bestämmelser under handläggningen av ett mål. En övergångsbestämmelse behövs i och för sig inte vad gäller länsstyrelsernas ärenden men bör av tydlighetsskäl ändå finnas.

Vissa kompletteringar i ärendena eller målen kan bli nödvändiga. Föreläggande om det kommer att kunna utfärdas enligt de nya bestämmelserna om undersökningsbefogenheter för tillsynsmyndigheten respektive med stöd av förvaltningsprocesslagen (1971:291). Några övergångsbestämmelser om detta behövs inte.

I prövningarna hos tillsynsmyndigheten och domstolarna kan det komma att uppstå vissa situationer som kan vara svårhanterliga. Det gäller t.ex. ett överklagat beslut om avslag på en ansökan om tillstånd till kamerabevakning där domstolen gör bedömningen att bevakningen inte längre är tillståndsskyldig. I en sådan situation torde ändamålet med överklagandet kunna anses ha förfallit och målet kunna avskrivas. Exakt vilka situationer som är tänkbara och huruvida de kommer att uppkomma och i så fall i vilken omfattning är svårt att säga. De kan i vart fall inte antas bli särskilt många och kommer dessutom bara att uppkomma under en övergångsperiod. Det kan därför överlämnas åt rättstillämpningen att hantera dessa. Några övergångsbestämmelser behövs alltså inte.

Den nya förhandlingsskyldigheten för arbetsgivare enligt kamerabevakningslagen ska gälla inför arbetsgivarens beslut om kamerabevakning. Kamerabevakning som redan pågår vid ikraftträdandet träffas inte av skyldigheten. Lagens bestämmelse om denna skyldig-

het ska enligt huvudprincipen gälla från och med att lagen träder i kraft.

I fråga om skadestånd finns vissa bestämmelser i kameraövervakningslagen. Enligt den nya kamerabevakningslagen ska bestämmelser om skadestånd i förordningen och dataskyddslagen eller brottsdatalagen tillämpas. Även om nya skadeståndsbestämmelser anses bli tillämpliga i fråga om skadestånd till följd av skadefall som inträffar först efter ikraftträdandet föreslås av tydlighetsskäl att det i en övergångsbestämmelse anges att de äldre föreskrifterna om skadestånd fortfarande ska gälla för skada som har orsakats före ikraftträdandet.

Slutligen innebär kamerabevakningslagen att den straffrättsliga regleringen och vitesmöjligheten i kameraövervakningslagen ersätts med ett system som innebär att överträdelser av den nya lagen eller av beslut som meddelats med stöd av lagen ska kunna föranleda sanktionsavgift, som är en administrativ sanktion men som har straffliknande inslag.

Enligt artikel 7 i Europakonventionen får ingen fällas till ansvar för en gärning eller underlåtenhet som vid den tidpunkt då den begicks inte utgjorde ett brott enligt nationell eller internationell rätt. Inte heller får ett strängare straff utmätas än det som var tillämpligt vid den tidpunkt då brottet begicks. Vidare finns i 2 kap. 10 § regeringsformen ett förbud mot retroaktiv straff- och skattelagstiftning. Förbudet mot retroaktiv skattelag anses vara analogt tillämpligt på straffliknande administrativa påföljder (prop. 1975/76:209, s. 125). Av 5 § andra stycket lagen om införande av brottsbalken framgår att straff ska bestämmas enligt den lag som gällde när gärningen företogs utom i fall där annan lag gäller när dom meddelas och den nya lagen leder till frihet från straff eller lindrigare straff. Bestämmelsen har enligt förarbetena generell räckvidd, dvs. den gäller även utanför brottsbalken (prop. 1964:10, s. 99). Den ger uttryck för det som brukar kallas den lindrigaste lagens princip.

Ett sanktionssystem med en sanktionsavgift får formellt sett anses lindrigare än ett straffansvar. Emellertid är huvudsyftet med att överträdelser av kamerabevakningslagen eller av beslut som har meddelats med stöd av lagen inte längre ska vara kriminaliserade att skapa ett effektivare sanktionssystem. Vidare kan en sanktionsavgift i ett enskilt fall vara svårare än ett bötesstraff. Den lindrigaste

lagens princip gör sig då inte gällande. Till detta kommer att ett upphävande av äldre straffbestämmelser utan en övergångsbestämmelse kan innebära att straffansvaret i vissa situationer bortfaller, vilket i vissa fall framstår som svårmotiverat. Dessutom innehåller den nya lagen vissa nya krav, bl.a. ett skärpt upplysningskrav. I praktiken torde det emellertid vara ytterst ovanligt med lagföring av brott mot kameraövervakningslagen. Även användningen av vite enligt den lagen är sparsam. För att undvika tolkningsproblem föreslås att äldre föreskrifter fortfarande ska gälla för överträdelser som har skett före ikraftträdandet.

En särskild fråga är hur man bör se på överträdelser som börjat före men fortsatt efter kamerabevakningslagens ikraftträdande. Situationen kan närmast jämföras med brott som består i pågående handlande, s.k. perdurerande brott. När det gäller sådana anses det att den nya lagen ska tillämpas på hela förfarandet. Motsvarande synsätt bör anläggas på överträdelser av kamerabevakningslagens bestämmelser.

Vad slutligen gäller ändringen i offentlighets- och sekretesslagen behövs och föreslås därför en övergångsbestämmelse om att äldre föreskrifter fortfarande ska gälla för uppgift som har inhämtats före ikraftträdandet.

17 Konsekvenser

17.1 Förslagen

Förslaget till kamerabevakningslag kompletterar dataskyddsförordningen och genomför dataskyddsdirektivet på kamerabevakningsområdet samt avser sådan kamerabevakning som inte omfattas av förordningens egentliga tillämpningsområde eller direktivets tillämpningsområde. En allmän utgångspunkt har varit att anpassa lagen till EU-regleringen även i de delar lagen i och för sig hade kunnat utformas annorlunda. Två anknytande utgångspunkter har varit att lagen endast bör innehålla de bestämmelser som särskilt behövs för kamerabevakning till skillnad mot annan personuppgiftsbehandling och att bestämmelserna, så långt det är förenligt med EU-regleringen och ändamålsenligt, bör vara desamma för all kamerabevakning. Andra utgångspunkter har varit att lagen bör ge ökade möjligheter till kamerabevakning samtidigt som den bör ge ett förstärkt skydd för den personliga integriteten, däribland vid kamerabevakning på arbetsplatser.

Kamerabevakningslagen innehåller få helt nya krav men i vissa avseenden skärps kraven och i andra mildras de.

Förslagen i avsnitt 11 har motsvarigheter i dagens lagstiftning. Förslagen innebär dock att färre aktörer än tidigare kommer att omfattas av ett krav på tillstånd för att få bedriva kamerabevakning – i första hand myndigheter kommer fortsatt att omfattas av ett tillståndskrav medan de flesta privata rättssubjekt inte kommer att göra det.

Också förslagen i avsnitt 12 har motsvarigheter i dagens lagstiftning. Det ställs dock i vissa avseenden högre krav på den som bedriver kamerabevakning, eftersom fler upplysningar än tidigare ska lämnas vid kamerabevakning och viss ytterligare information ska göras tillgänglig för dem som kan bli kamerabevakade. I andra

avseenden ställs det lägre krav än tidigare, eftersom möjligheterna till undantag från kravet på upplysning vidgas något.

Många av kraven i avsnitt 13 följer redan av dagens lagstiftning. Däremot är kravet på att en arbetsgivare i vissa fall ska förhandla med berörd arbetstagarorganisation innan denne beslutar om kamerabevakning generellt sett nytt. En förhandlingsskyldighet kan dock gälla redan i dag enligt lagen (1976:580) om medbestämmande i arbetslivet. Det är emellertid osäkert i vilken utsträckning detta gäller.

Förslagen i avsnitt 14 innebär att EU-regleringens och anknytande generell svensk lagstiftnings bestämmelser om principer, rättigheter, skyldigheter och överföring ska gälla i tillämpliga delar vid kamerabevakning. Dessa bestämmelser har vissa motsvarigheter i dagens kameraövervakningslag.

Förslagen i avsnitt 15 har vissa motsvarigheter i dagens lagstiftning. En förändring är att länsstyrelsernas tillsynsansvar flyttas till Datainspektionen. En annan förändring är att straffansvar inte längre ska kunna följa för den som bryter mot kamerabevakningslagstiftningen. I övrigt innebär förslagen att frågor som avser tillsynsmyndighetens befogenheter, sanktioner, rättsmedel och skadestånd anpassas till vad som enligt förordningen och direktivet gäller för personuppgiftsbehandling i övrigt.

Det förtjänar framhållas att det pågår ett omfattande arbete inom Regeringskansliet, bl.a. i form av ett stort antal utredningar, som på olika sätt rör EU:s nya dataskyddsreglering. Exempelvis har konsekvenserna av de anpassningar och kompletterande svenska författningsbestämmelser på generell nivå som förordningen ger anledning till analyserats av Dataskyddsutredningen (SOU 2017:39). På motsvarande sätt har en bedömning av konsekvenserna av det generella genomförandet av direktivets bestämmelser gjorts av Utredningen om 2016 års dataskyddsdirektiv (SOU 2017:29). Vidare har förordningens och direktivets konsekvenser för tillsynsmyndigheten tidigare övervägts av Utredningen om tillsynen över den personliga integriteten (SOU 2016:65), som föreslagit att Datainspektionen ska vara tillsynsmyndighet enligt förordningen och direktivet. Konsekvenser i dessa avseenden berörs inte närmare här. Övriga utredningars förslag kan dock komma att påverka hur Datainspektionen behöver arbeta och vara organiserad vad gäller tillsynen på kamerabevakningsområdet. Detta innebär att det är svårt att i nuläget säkert bedöma vilka ekonomiska konsekvenser de förslag som lämnats

i de föregående avsnitten kommer att få för den myndigheten. Genomförandet av förslagen och de förslag som lämnats av de övriga utredningarna måste också rimligen ske samordnat. Bedömningarna när det gäller konsekvenserna av förevarande förslag får därför bli preliminära uppskattningar.

17.2 Ekonomiska konsekvenser

17.2.1 Konsekvenser för staten

Förslag: Förslagen väntas leda till ökade kostnader för Datainspektionen, Förvaltningsrätten i Stockholm och Kammarrätten i Stockholm. De ökade kostnaderna för Datainspektionen ska finansieras genom att anslagen till länsstyrelserna minskas. De ökade kostnaderna för Förvaltningsrätten i Stockholm och Kammarrätten i Stockholm kan finanseras genom att anslagen till övriga förvaltningsrätter och kammarrätter minskas i motsvarande mån.

Bedömning: Förslagen väntas inte leda till några andra kostnadsökningar för staten som inte ryms inom befintliga ekonomiska ramar.

Skälen för förslaget och bedömningen: Förslaget att Datainspektionen ska vara ensam tillsynsmyndighet enligt kamerabevakningslagen innebär att länsstyrelserna inte längre ska ha något tillsynsansvar på kamerabevakningsområdet. Datainspektionen, som i dag har operativ tillsyn över platser som allmänheten saknar tillträde till och det centrala tillsynsansvaret på området, har alltså föreslagits ansvara även för den operativa tillsynen av platser till vilka allmänheten har tillträde. Förslaget innebär att ansökningar om tillstånd till kamerabevakning och om undantag från kravet på upplysning om kamerabevakning ska prövas av inspektionen. För att kunna hantera sina nya uppgifter måste myndigheten tillföras ekonomiska resurser.

Enligt uppgift från länsstyrelserna i den enkätundersökning som gjorts och redovisats i avsnitt 5 avgjordes drygt 900 ärenden om tillstånd under 2015. Utifrån det totala antalet anmälningar om

kameraövervakning den 1 januari 2016 jämfört med den 1 januari 2013 kan antalet årliga nytillkomna anmälningar uppskattas till drygt 1 000 stycken. Under år 2015 gjordes vidare omkring 200 inspektioner av samtliga länsstyrelser runt om i landet. Den totala resursåtgången för länsstyrelserna avseende kameraövervakning under det året uppgick till omkring tolv årsarbetskrafter. Mot bakgrund av de uppgifter som länsstyrelserna lämnat i enkätsvaren kan uppskattningsvis 10–15 procent av den totala arbetsinsatsen anses avse inspektion. Antalet ansökningar om undantag från upplysningskravet berördes inte i enkätundersökningen men kan antas uppgå till ett mycket litet antal. Dessa uppgifter får tjäna som utgångspunkt för en uppskattning av hur stora resurser Datainspektionen ska tillföras.

Resursbehovet för tillsynen enligt kamerabevakningslagen påverkas av förslaget att kamerabevakning i större utsträckning än tidigare kommer att få ske utan tillstånd, eftersom tillståndskravet har föreslagits omfatta färre aktörer. Vidare har föreslagits att det nuvarande anmälningskravet tas bort. Förslagen kommer därför att leda till färre tillståndsansökningar och att hanteringen av anmälningar helt försvinner. Detta kommer i sin tur att leda till en motsvarande minskning av resursbehovet. Samtidigt är avsikten att möjligheterna till kamerabevakning för de som ska omfattas av tillståndskravet ska öka. Antalet årliga tillståndsärenden kan grovt uppskattas till omkring hälften av de ärenden som avgjordes under år 2015 eller 400–600 stycken. Till detta kommer ett mindre antal ärenden om undantag från upplysningskravet. Förslaget som avser undantag från upplysningskravet bedöms inte leda till någon påtaglig ökning av sådana ärenden. Däremot ska den generella tillsynen över kamerabevakning förstärkas.

Mot den här bakgrunden bedöms det totala personella resursbehovet minska något. Någon mer exakt uppskattning av behovet är i nuläget inte möjlig, eftersom den skulle vara förenad med alltför stora osäkerhetsmoment. Detta beror bl.a. på att resursbehovet är avhängigt hur Datainspektionen väljer att organisera sin tillsynsverksamhet på kamerabevakningsområdet; en centraliserad myndighet som Datainspektionen har helt andra förutsättningar att bedriva tillsyn än regionala myndigheter som länsstyrelserna. Vidare har Datainspektionen i dag både det centrala ansvaret för tillsyn enligt kameraövervakningslagen och det operativa tillsynsansvaret för

kameraövervakning av platser dit allmänheten inte har tillträde. I det centrala ansvaret ingår bl.a. att sammanställa rättspraxis, samla in fakta och erfarenheter om teknikutvecklingen och den internationella utvecklingen och utbilda och ge råd åt länsstyrelserna om lagstiftning, praxis och teknik på området. Den operativa tillsynen kräver bedömningar som mycket liknar dem som länsstyrelserna gör i dag. För att ta till vara allmänna intressen har Datainspektionen också en rätt att överklaga beslut om kameraövervakning av en plats dit allmänheten har tillträde. Resursbehovet påverkas också av att en förhållandevis stor del av regelverket för kamerabevakning har föreslagits motsvara vad som ska gälla generellt för behandling av personuppgifter. Tillsynen av kamerabevakning kan därför i viss utsträckning samordnas med Datainspektionens tillsyn av personuppgifter i stort. Allt detta kan väntas medföra effektivitetsvinster för tillsynsmyndigheten.

Enligt Datainspektionens årsredovisning för år 2015 var myndighetens driftskostnad per arbetskraft det året omkring en miljon kronor. Om samtliga ovan uppskattade tolv årsarbetskrafter som i dag avser kameraövervakning vid länsstyrelserna skulle överföras till Datainspektionen, skulle alltså myndigheten behöva tillföras omkring tolv miljoner kronor. Som framgått ovan bedöms dock Datainspektionens personella behov bli mindre än vad länsstyrelserna har i dag till följd av en minskad hantering av ärenden om tillstånd och anmälningar om kamerabevakning och till följd av de nämnda väntade effektivitetsvinsterna. Även den omständigheten att Datainspektionen inte längre ska samordna den operativa tillsynen på vissa platser och ge råd och stöd till länsstyrelserna innebär att resurser kommer att frigöras inom myndigheten. Det innebär att resurstillskottet till Datainspektionen bör vara lägre än det angivna beloppet.

Länsstyrelsernas resursbehov för att hantera ansökningar och anmälningar har vidare delvis finansierats genom avgifter. Även Datainspektionens resursbehov kan framöver, om det bedöms lämpligt, delvis finansieras genom ansökningsavgifter. Avgifterna för år 2015 kan, utifrån de ovan redovisade siffrorna avseende inkomna ansökningar och anmälningar, uppskattas ha gett en inkomst motsvarande omkring fyra miljoner kronor till länsstyrelserna, varav drygt en halv miljon hänfört sig till anmälningar. Om antalet årliga tillståndsansökningar, i enlighet med den ovan redovisade uppskattningen, kommer att uppgå till 400–600, skulle en oförändrad ansök-

ningsavgift inbringa 1,5–2,2 miljoner kronor. De ökade kostnaderna för Datainspektionen ska i övrigt eller annars finansieras genom att anslagen till länsstyrelserna minskas.

När det gäller rättsväsendet kan det inledningsvis konstateras att de lämnade förslagen innebär att straffansvar inte ska kunna följa för den som bryter mot kamerabevakningslagens bestämmelser eller beslut som meddelats med stöd av lagen. Ett undantag gäller dock för brott mot tystnadsplikt, som emellertid redan i dag är straffbelagt. Det är fråga om ett mycket litet antal mål som försvinner till följd av avkriminaliseringen och de frigjorda resurserna bedöms som försumbara.

Att Datainspektionen blir ensam tillsynsmyndighet innebär att Förvaltningsrätten i Stockholm och Kammarrätten i Stockholm kommer att bli de enda domstolar som prövar överklagade beslut enligt kamerabevakningslagen. Det kommer att ske en viss ökning av antalet mål i dessa domstolar samtidigt som en minskning sker hos de domstolar som fram till nu prövat mål om kameraövervakning. Enligt uppgifter som lämnats i enkätundersökningen överklagades under år 2015 knappt 130 beslut om tillstånd till kameraövervakning. Med hänsyn till att tillståndskravet i lagen ska omfatta färre aktörer kan andelen överklagande beslut i fråga om tillstånd väntas minska. Vidare kommer andra beslut enligt kamerabevakningslagen att kunna överklagas, främst beslut om sanktionsavgift. Det är svårt att uppskatta hur många sådana mål som överklagandemöjligheten kommer att generera men någon avsevärd ökning av antalet mål jämfört med i dag kan i dagsläget inte förutses. Även vissa beslut som avser kamerabevakning som meddelas med stöd av förordningen eller de generella svenska lagarna, dataskyddslagen och brottsdatalagen, kommer att kunna överklagas. Sådana konsekvenser har analyserats i de konsekvensbedömningar som de inledningsvis nämnda utredningarna gjort. Den ökade måltillströmningen till Förvaltningsrätten i Stockholm och, i mindre mån, till Kammarrätten i Stockholm – där ett krav på prövningstillstånd ska gälla – innebär att dessa domstolar bör tillföras resurser. En grov uppskattning är att Förvaltningsrätten i Stockholm behöver tillföras en årsarbetskraft och att Kammarrätten i Stockholm behöver tillföras 0,2 årsarbetskrafter. De ökade kostnaderna, som för förvaltningsrättens del uppskattas till en och en halv miljon kronor och för kammarrättens del till 300 000 kronor, kan finansieras genom

en motsvarande minskning av anslagen till övriga förvaltningsrätter och kammarrätter.

De föreslagna ändringarna i fråga om kravet på upplysning bedöms leda till mindre kostnader av engångskaraktär för de statliga myndigheter som bedriver kamerabevakning för att uppdatera befintliga upplysningar. Förslagen om ett förstärkt integritetsskydd på arbetsplatser, däribland införandet av en förhandlingsskyldighet, bedöms inte leda till annat än en marginell ökning av kostnaderna för de myndigheter som vill bedriva kamerabevakning av arbetsplatsen.

Förslagen om ett förstärkt integritetsskydd i övrigt innebär att regleringen i förordningen eller brottsdatalagen ska gälla vid kamerabevakning. I kostnadshänseende medför förslagen inte någon skillnad i förhållande till vad som annars hade gällt.

Förslagen väntas inte leda till några andra kostnadsökningar för staten som inte ryms inom befintliga ekonomiska ramar.

17.2.2 Konsekvenser för kommuner och landsting

Bedömning: Förslagen väntas medföra endast mindre kostnader av engångskaraktär för kommuner och landsting. Kostnaderna ryms inom befintliga ekonomiska ramar.

Skälen för bedömningen: De lämnade förslagen innebär inte några större ändringar för kommunernas del. Det förhållandet att tillståndskravet har föreslagits omfatta färre aktörer innebär som redovisats ovan att antalet tillståndsärenden kommer att minska. Det innebär att kommunerna kommer att behöva avsätta mindre resurser för att yttra sig i sådana ärenden. Även det förhållandet att tillsynsmyndigheten endast ska behöva inhämta ett sådant yttrande om det behövs, kan väntas minska resursbehovet något. Uppskattningsvis är det emellertid fråga om marginella kostnadsbesparingar.

På motsvarande sätt som beskrivits ovan för de statliga myndigheterna kommer förslagen i fråga om kravet på upplysning att medföra mindre engångskostnader för de kommuner som bedriver bevakning när de ska uppdatera befintliga upplysningar. Även förslagen om ett förstärkt integritetsskydd på arbetsplatser, t.ex. införandet av en förhandlingsskyldighet, bedöms inte leda till annat än en margi-

nell ökning av kostnaderna för de kommuner som vill bedriva kamerabevakning av arbetsplatsen.

Förslagen om ett förstärkt integritetsskydd i övrigt innebär att regleringen i förordningen eller brottsdatalagen ska gälla vid kamerabevakning. I kostnadshänseende medför förslagen inte någon skillnad i förhållande till vad som annars hade gällt.

Vid en sammantagen bedömning väntas förslagen medföra endast mindre kostnader av engångskaraktär för kommuner och landsting. Kostnaderna ryms inom befintliga ekonomiska ramar.

17.2.3 Konsekvenser för enskilda

Bedömning: Bortsett från vissa mindre kostnader av engångskaraktär väntas förslagen inte leda till några nya kostnader eller någon ökad administrativ börda för enskilda. Förslagen väntas tvärtom leda till minskade kostnader och en minskad administrativ börda för den stora merparten av de enskilda som vill bedriva kamerabevakning.

Skälen för bedömningen: Förslagen innebär att det i stor utsträckning inte längre kommer att krävas tillstånd eller anmälan för att enskilda ska få bedriva kamerabevakning. I dessa fall kommer förslagen att medföra en kostnadsminskning för de enskilda, eftersom de inte behöver betala avgifter för att få bedriva bevakningen. Att tillstånd inte krävs kan vidare medföra fördelar från konkurrenssynpunkt för svenska rättssubjekt jämfört med om ett svenskt tillståndskrav gällt. De enskilda som inte längre omfattas av krav på tillstånd eller anmälan kan i stället behöva göra en konsekvensbedömning och, beroende på hur den utfaller, samråda med tillsynsmyndigheten. Detta kommer att orsaka en viss administrativ börda och vissa kostnader men eftersom kraven följer av EU-regleringen hade detta blivit följden även utan de förslag som har lämnats här. Det förhållandet att upplysningskravet är något mer detaljerat än tidigare kommer att orsaka mindre engångskostnader för enskilda som bedriver kamerabevakning när de ska uppdatera upplysningarnas innehåll.

Förslagen om ett förstärkt integritetsskydd på arbetsplatser, t.ex. införandet av en förhandlingsskyldighet, bedöms inte leda till

annat än en marginell ökning av kostnaderna för enskilda som vill bedriva kamerabevakning av arbetsplatsen.

Förslagen om ett förstärkt integritetsskydd i övrigt innebär att regleringen i förordningen eller brottsdatalagen ska gälla vid kamerabevakning. I kostnadshänseende medför förslagen inte någon skillnad i förhållande till vad som annars hade gällt.

Sammanfattningsvis görs bedömningen att förslagen, bortsett från vissa mindre kostnader av engångskaraktär, inte väntas leda till några nya kostnader eller någon ökad administrativ börda för enskilda. Förslagen väntas tvärtom leda till minskade kostnader och en minskad administrativ börda för den stora merparten av de enskilda som vill bedriva kamerabevakning.

17.3 Konsekvenser för det brottsförebyggande arbetet och brottsligheten

Bedömning: Förslagen kan ge positiva effekter för det brottsförebyggande arbetet och även för motverkandet av brottslighet i övrigt.

Skälen för bedömningen: Som närmare redovisats i avsnitt 9.2.2 är kamerabevakning ett verktyg bland flera som kan förebygga, förhindra eller upptäcka brottslighet eller bidra till att begångna brott kan utredas och lagföras. Undersökningar, både svenska och utländska, visar att kamerabevakning har vissa brottsförebyggande effekter. Vidare kan realtidstillgång till material från kamerabevakning vara av stort värde för Polismyndighetens planlagda operativa brottsförebyggande insatser. Bild- och ljudmaterial från kamerabevakning, både från Polismyndighetens egen bevakning och från andra aktörers bevakning, används dessutom i brottsutredningar. Materialet kan ofta föra brottsutredningarna framåt och bidra till att lagföring sker.

De lämnade förslagen innebär som helhet att möjligheterna att bedriva kamerabevakning ökar, inte minst när bevakningen ska ske för brottsbekämpande ändamål. Kamerabevakning kommer i större utsträckning att få ske utan tillstånd och i de fall tillstånd krävs kommer det att bli lättare att få tillstånd. Dessa ökade möjligheter att bedriva kamerabevakning kan ge positiva effekter för det brotts-

förebyggande arbetet. De kan också ge positiva effekter för motverkandet av brottslighet i övrigt, eftersom material från kamerabevakning i större utsträckning kommer att användas för utredning och lagföring av brott. Att begångna brott utreds och lagförs kan vidare bidra till att straffsystemet får avsedd generell brottsavhållande verkan.

17.4 Konsekvenser för skyddet av den personliga integriteten

Bedömning: Förslagen innebär ett förstärkt skydd för enskildas personliga integritet.

Skälen för bedömningen: Kamerabevakning innebär ett intrång i enskildas intresse av att inte bli föremål för kamerabevakning. Ökade möjligheter att bedriva kamerabevakning kan därför medföra högre risker för den personliga integriteten. Att bli utsatt för brott kan emellertid också utgöra en kränkning av den personliga integriteten. I den mån de ökade möjligheterna att bedriva kamerabevakning leder till minskad brottslighet kan därför en förbättring av integritetsskyddet uppnås.

Dessutom har flera förstärkningar av integritetsskyddet vid kamerabevakning föreslagits. En av dessa är att det införs en skyldighet för arbetsgivare att, innan han eller hon beslutar om kamerabevakning av arbetsplatsen, i vissa fall först förhandla med en organisation som företräder arbetstagarna på arbetsplatsen på det sätt som anges i lagen (1976:580) om medbestämmande i arbetslivet. Andra förstärkningar är att EU-regleringens detaljerade bestämmelser om bl.a. rättigheter för registrerade och skyldigheter för personuppgiftsansvariga ska gälla även vid kamerabevakning. Också delar av förslagen om kravet på upplysning och om rättsmedel m.m. stärker enskildas rättigheter.

Sammantaget görs bedömningen att förslagen innebär ett förstärkt skydd för enskildas personliga integritet.

17.5 Konsekvenser i övrigt

Bedömning: Förslagen väntas inte få några andra konsekvenser.

Skälen för bedömningen: Förslagen väntas inte få några konsekvenser för den kommunala självstyrelsen eller för jämställdheten och inte heller andra sådana konsekvenser – som inte redan berörts – som avses i 14 eller 15 §§ kommittéförordningen (1998:1474) eller 7 § förordningen (2007:1244) om konsekvensutredning vid regelgivning.

18 Författningskommentar

18.1 Förslaget till kamerabevakningslag

Allmänna bestämmelser

Inledande bestämmelse

1 § I denna lag finns bestämmelser om kamerabevakning som

– kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), nedan kallad dataskyddsförordningen,

– genomför Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, nedan kallat dataskyddsdirektivet, eller

– avser sådan kamerabevakning som inte omfattas av dataskyddsförordningen eller dataskyddsdirektivet.

I denna inledande paragraf anges att det i lagen finns bestämmelser om kamerabevakning som kompletterar dataskyddsförordningen och genomför dataskyddsdirektivet. Av tydlighetsskäl anges också att lagen innehåller bestämmelser som avser sådan kamerabevakning som inte omfattas av förordningen eller direktivet. Bestämmelserna i lagen är gemensamma för all kamerabevakning. Vad som förstås med kamerabevakning anges i 3 §. Med stöd i förordningen och direktivet går bestämmelserna utöver eller avviker de i vissa avseenden från vad som annars följer av den regleringen. Av 6 § framgår att utöver vad som föreskrivs i lagen gäller i tillämpliga delar antingen dataskyddsförordningen, lagen (2018:000) med komplet-

terande bestämmelser till EU:s dataskyddsförordning, föreskrifter som meddelats med stöd av den lagen eller annan författning som kompletterar dataskyddsförordningen vid kamerabevakning som omfattas av förordningen eller den angivna lagen eller brottsdatalagen (2018:000), föreskrifter som meddelats med stöd av den lagen eller annan författning som genomför dataskyddsdirektivet vid kamerabevakning som omfattas av brottsdatalagen. Förevarande paragraf har behandlats i avsnitt 10.1.

Lagens syfte

2 § Syftet med denna lag är att tillgodose behovet av kamerabevakning för berättigade ändamål och att skydda enskilda mot otillbörliga intrång i den personliga integriteten vid sådan bevakning.

I paragrafen anges lagens syfte, som är tudelat. Paragrafen har behandlats i avsnitt 10.1.

Det ena syftet med lagen är att tillgodose behovet av kamerabevakning för berättigade ändamål. Det andra är att skydda enskilda, dvs. fysiska personer, mot otillbörliga intrång i den personliga integriteten vid kamerabevakning. Bestämmelserna om kamerabevakning ska säkerställa en lämplig balans mellan nyttan med kamerabevakning och skyddet av den personliga integriteten. Med berättigade ändamål avses både de i 9 § särskilt uppräknade ändamålen som ska beaktas vid prövning av om tillstånd till kamerabevakning ska ges och ändamål som annars är berättigade enligt de regleringar som avses i 6 §. De regleringar som det hänvisas till i 6 § och som gäller även för kamerabevakning innehåller också bestämmelser med ett liknande tudelat syfte.

Lagens tillämpningsområde

3 § Denna lag gäller vid kamerabevakning. Med kamerabevakning förstås

1. att en TV-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning, utan att manövreras på platsen, används varaktigt eller regelbundet upprepat för personbevakning,

2. att en separat teknisk anordning för avlyssning eller upptagning av ljud används för personbevakning i samband med användning av sådan utrustning som avses i 1, och

3. att en separat teknisk anordning för att behandla upptaget bild- och ljudmaterial används.

Av denna paragraf framgår lagens materiella tillämpningsområde. Detta har behandlats i avsnitt 10.2.

I paragrafen anges att lagen gäller vid kamerabevakning och definieras sedan i tre punkter vad som förstås med sådan bevakning. Gemensamt för punkterna är att tillämpningsområdet knyter an till *användning* av viss utrustning.

Med kamerabevakning förstås enligt *punkten 1* att en TV-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning, utan att manövreras på platsen, används varaktigt eller regelbundet upprepat för personbevakning.

Den utrustning som omfattas – TV-kameror, andra optisk-elektroniska instrument och därmed jämförbara utrustningar – är densamma som tidigare omfattats av kameraövervakningslagen (2013:460). Med *optisk* avses alla registreringar som kan ske med instrument inom det elektromagnetiska våglängdsspektrat för optisk strålning. Med *elektronisk* förstås att förmedling av bilder, visning av bilder eller lagring av bilder sker genom elektronisk påverkan. Däremot saknar det betydelse om andra funktioner styrs på elektronisk väg. Det innebär exempelvis att fiberoptiska kikare liksom stillbilds- och filmkameror är att anse som optisk-elektroniska instrument, om bildupptagningen direkt förmedlas vidare till en elektronisk bildskärm eller lagras på ett elektroniskt medium. Även t.ex. värmekameror omfattas. Med *därmed jämförbar utrustning* avses instrument som kan nyttja sådan elektromagnetisk strålning som röntgen och radiofrekvent strålning.

Begreppet *utan att manövreras på platsen* har samma innebörd som i den tidigare kameraövervakningslagen och praxis avseende den lagen. Med platsen menas den plats där TV-kameran, det optisk-elektroniska instrumentet eller den därmed jämförbara utrustningen finns. Utrustningen kan finnas antingen på en ”fast plats”, t.ex. på en fasad, på en inomhusvägg, i ett tak eller på en stolpe, eller på en ”rörlig plats”, t.ex. på eller i ett fordon, ett fartyg eller en drönare eller ett annat luftfartyg. Med att utrustningen används utan att manövreras på platsen avses att den fortlöpande hanteringen av utrustningen sker på ett ställe som är klart åtskilt från den plats där utrustningen finns. Endast det förhållandet att utrustningen

sätts igång på stället eller fungerar med inbyggd automatik innebär inte att den manövreras på platsen. Utrustning som finns i användarens omedelbara närhet och som fortlöpande styrs av användaren är manövrerad på platsen.

Lagen omfattar inte en kamera eller annan därmed jämförbar utrustning som är handhållen och inte heller en kamera eller därmed jämförbar utrustning som på annat sätt är kroppsburen, t.ex. en kamera som är fäst i en persons kläder eller monterad på en hjälm. Lagen omfattar vidare inte exempelvis användning av en webbkamera eller någon annan utrustning för videokonferens, en kamera placerad på vindrutan i en bil eller en kamera fäst på ett cykelstyre förutsatt att användaren är i kamerans eller utrustningens omedelbara närhet och fortlöpande styr över denna, dvs. avgör att den ska användas och vad som ska fotograferas eller filmas. Detsamma bör gälla när en passagerare i en bil är den som använder kameran även om han eller hon inte genom att styra fordonet avgör vad som ska fotograferas eller filmas. I undantagsfall kan dock omständigheterna vara sådana att manövreringen i de nämnda situationerna inte kan anses ske på platsen. Detta har utvecklats i avsnitt 10.2. Fordons inbyggda backkameror eller andra kameror som är helt integrerade i fordon är inte manövrerade på platsen.

För att det ska vara fråga om kamerabevakning enligt punkten 1 krävs dessutom att utrustningen *används varaktigt eller regelbundet upprepat*. Detta krav tar, till följd av den avgränsning av lagens tillämpningsområde som följer av kravet på att utrustningen inte ska manövreras på platsen, i första hand sikte på hur användningen sker på en viss geografisk plats. När kameraanvändning avser ”rörliga platser” är kravet på ”utan att manövreras på platsen” endast uppfyllt i vissa fall. Så kan t.ex. vara fallet när kamerabevakning sker från en drönare. I ett sådant fall får kravet på varaktighet eller regelbunden upprepning prövas mot den användningen.

Användning som är *varaktig* omfattas även om den endast sker vid ett enda tillfälle. Som kortvarig användning bör anses användning som sker under högst runt någon halvtimme. Sådan kortvarig användning vid ett enstaka tillfälle omfattas inte.

Med *regelbundet upprepad* användning menas att utrustningen används vid ett flertal tillfällen som ligger nära eller relativt nära varandra i tiden eller som är mer utspridda men ändå infaller på ett planmässigt sätt. Även användning som annars följer ett särskilt möns-

ter innefattas i begreppet. Exempelvis omfattas användning vid återkommande särskilda evenemang eller andra händelser och användning efter aktivering genom att en människa kommer in i kamerans upptagningsområde. Det saknar betydelse om användningen är kortvarig vid tillfällena. Om utrustningen används endast med långa och oregelbundna mellanrum, är det inte fråga om regelbunden upprepning. Om användningen vid något eller flera av dessa tillfällen inte är kortvarig, omfattas den dock av vad som menas med varaktig.

Med *personbevakning* avses att personer kan identifieras genom bevakningen. Det krävs att sådana kännetecken kan iakttas som gör att man utan större osäkerhet kan skilja de personer som iakttas från andra personer. Så är fallet om hela personen eller personens ansikte syns tydligt. Även sådant som utmärkande klädsel, speciella kroppsrörelser eller särskild kroppskonstitution kan möjliggöra identifiering. I att utrustningen *används för personbevakning* ligger både användning som sker i det direkta syftet att kontrollera människors förehavanden och användning i situationer där detta direkta syfte saknas men där människor normalt kan komma in i kamerans upptagningsområde. Om en människa endast av en tillfällighet kan hamna i en kameras blickfång, är det inte fråga om personbevakning. Så kan t.ex. vara fallet vid kameraanvändning som är avsedd enbart för kontroll av en tillverkningsmaskin i vars närhet människor normalt inte ska befinna sig, även om någon vid ett enstaka tillfälle kan råka göra det. Däremot är det fråga om personbevakning också då en kamera är placerad i naturen eller på någon annan enslig plats och människor därför sällan kommer in i kamerans upptagningsområde.

Vidare framgår av *punkten 2* att med kamerabevakning förstås även att en separat teknisk anordning för avlyssning eller upptagning av ljud används för personbevakning i samband med användning av sådan utrustning som avses i punkten 1. Exempel på sådana anordningar är mikrofoner och radiosändare som inte är inbyggda i utrustning som omfattas av punkten 1.

Slutligen följer av *punkten 3* att med kamerabevakning förstås också att en separat teknisk anordning för att behandla upptaget bild- och ljudmaterial används. Exempelvis avses användning av separata anordningar för att lagra inspelad film. Av 7 § framgår att uttryck som används i lagen har samma betydelse som i dataskyddsförordningen när det gäller kamerabevakning som omfattas av för-

ordningen eller lagen med kompletterande bestämmelser till EU:s dataskyddsförordning eller som i brottsdatalagen när det gäller kamerabevakning som omfattas av den lagen. Uttrycket behandling definieras i förordningen respektive brottsdatalagen.

4 § Lagen gäller endast om

1. kamerabevakning enligt 3 § 1 eller 2 sker med utrustning som finns i Sverige och den som bedriver bevakningen är etablerad i Sverige eller i tredjeland, eller

2. kamerabevakning enligt 3 § 3 avser behandling av bild- och ljudmaterial som tagits upp vid bevakning som avses i 1 och behandlingen utförs av den som bedriver bevakningen eller för hans eller hennes räkning.

I paragrafen anges lagens territoriella tillämpningsområde. Detta har behandlats i avsnitt 10.3.

Av *punkten 1* följer att sådan kamerabevakning som avses i 3 § 1 eller 2 endast omfattas av lagen om den använda utrustningen finns i Sverige och den som bedriver bevakningen är etablerad i Sverige eller i tredjeland. Vidare följer av *punkten 2* att i fråga om sådan kamerabevakning som avses i 3 § 3 gäller lagen endast om behandlingen avser bild- och ljudmaterial som tagits upp vid bevakning enligt punkten 1 och behandlingen utförs av den som bedriver bevakningen, dvs. av densamme som i punkten 1, eller för hans eller hennes räkning.

Med Sverige avses svenskt landterritorium och sjöterritorium samt luftrummet ovanför land- och sjöterritorierna. Av 7 § framgår att uttryck som används i lagen har samma betydelse som i dataskyddsförordningen när det gäller kamerabevakning som omfattas av förordningen eller lagen med kompletterande bestämmelser till EU:s dataskyddsförordning eller som i brottsdatalagen när det gäller kamerabevakning som omfattas av den lagen. Någon definition av tredjeland finns inte i dataskyddsförordningen men med ett sådant land avses en stat som inte är skyldig att tillämpa förordningen. På det område som omfattas av brottsdatalagen finns en särskild definition av tredjeland.

För sådan kamerabevakning som utgör personuppgiftsbehandling som omfattas av dataskyddsförordningen gäller enligt förordningen att när den som bedriver bevakningen inte är etablerad inom EU ska han eller hon skriftligen utse en företrädare för sig i unionen.

Om den som bedriver bevakningen utför personuppgiftsbehandling i flera EU-stater, ska enligt förordningen företrädaren vara etablerad i en av dessa. Detsamma gäller för sådan kamerabevakning på vilken förordningens bestämmelser ska tillämpas enligt vad som föreskrivs i lagen med kompletterande bestämmelser till EU:s dataskyddsförordning, om inte annat anges i annan författning. Det följer av 6 § 1 i förevarande lag.

Om den som bedriver kamerabevakningen lämnar över inspelat material till någon annan som därigenom blir ansvarig för behandlingen av detta, upphör kamerabevakningslagen att vara tillämplig såvitt avser det materialet. Bestämmelsen i 26 § gäller dock fortsatt för den som lämnat över materialet.

5 § Lagen gäller inte vid

1. kamerabevakning som en fysisk person utför som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,
2. hemlig kameraövervakning enligt 27 kap. rättegångsbalken eller lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott,
3. kamerabevakning som sker i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, och
4. kamerabevakning som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

I paragrafen anges vissa undantag från lagens tillämpningsområde. Undantagen har behandlats i avsnitt 10.4.

Enligt *punkten 1* gäller lagen inte vid kamerabevakning som en fysisk person utför som ett led i en verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll. Undantagets lydelse är densamma som i dataskyddsförordningen. Undantaget omfattar endast kamerabevakning som bedrivs av fysiska personer, inte bevakning som utförs av juridiska personer. Kamerabevakning som bedrivs på uppdrag av en fysisk person, t.ex. av ett bevakningsbolag, omfattas av undantaget. Den viktigaste faktorn för att avgöra om undantaget är tillämpligt är platsen för kamerabevakningen. Bevakning som sker i en privatbostad av den som bor där omfattas normalt av undantaget. Detsamma kan gälla t.ex. bevakning av personens tomtmark, garage och förråd. Undantaget bör inte anses omfatta kamerabevakning i offentliga miljöer eller av

områden som är privatägda men allemansrättsligt tillgängliga, dvs. platser dit allmänheten har tillträde. Detsamma gäller kamerabevakning som bedrivs inom ramen för näringsverksamhet, oavsett platsen för bevakningen.

I *punkten 2* undantas hemlig kameraövervakning enligt 27 kap. rättegångsbalken eller lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

Av *punkterna 3 och 4* följer att lagen inte omfattar kamerabevakning som sker i en verksamhet som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen och kamerabevakning som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande. Bestämmelserna i lagen gäller alltså inte för kamerabevakning i sådana verksamheter. I lagen med kompletterande bestämmelser till EU:s dataskyddsförordning anges att bestämmelserna i den lagen och i dataskyddsförordningen inte ska tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Vidare anges att vissa bestämmelser i den kompletterande lagen och i dataskyddsförordningen inte ska tillämpas på behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande. Dessa bestämmelser i lagen med kompletterande bestämmelser till EU:s dataskyddsförordning gäller sådan kamerabevakning som enligt punkterna 3 och 4 undantas från denna lags tillämpningsområde förutsatt att bevakningen omfattas av dataskyddsförordningen eller lagen med kompletterande bestämmelser till EU:s dataskyddsförordning.

Lagens förhållande till andra bestämmelser

6 § Utöver vad som föreskrivs i denna lag gäller i tillämpliga delar

1. dataskyddsförordningen, lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning, föreskrifter som meddelats med stöd av den lagen eller annan författning som kompletterar dataskyddsförordningen vid kamerabevakning som omfattas av förordningen eller den angivna lagen, eller

2. brottsdatalagen (2018:000), föreskrifter som meddelats med stöd av den lagen eller annan författning som genomför dataskyddsdirektivet vid kamerabevakning som omfattas av brottsdatalagen.

I paragrafen anges hur lagens bestämmelser förhåller sig till andra bestämmelser. Frågan har behandlats i avsnitt 10.1, 14 och 15.

Av paragrafen framgår att utöver vad som föreskrivs i förevarande lag gäller i tillämpliga delar andra bestämmelser vid kamerabevakning som avses i lagen.

Om det är fråga om sådan kamerabevakning som utgör personuppgiftsbehandling som omfattas av dataskyddsförordningen, gäller enligt *punkten 1* förordningen, lagen med kompletterande bestämmelser till EU:s dataskyddsförordning, föreskrifter som meddelats med stöd av den lagen eller annan författning som kompletterar dataskyddsförordningen. Att förordningens bestämmelser gäller följer direkt av unionsrätten men har angetts för att göra paragrafen fullständig och begriplig. Normalt är det dataskyddsförordningen och den generella kompletterande regleringen som gäller. I den mån det i annan författning finns särskilda bestämmelser som kan tillämpas på kamerabevakning har dessa dock företräde. Av lagen med kompletterande bestämmelser till EU:s dataskyddsförordning framgår att bestämmelserna i förordningen, i den ursprungliga lydelsen, och i den lagen även gäller – i tillämpliga delar – vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten och i verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget, dvs. som omfattas av den gemensamma utrikes- och säkerhetspolitiken. Detta gäller även kamerabevakning som utgör personuppgiftsbehandling i sådan verksamhet förutsatt att det inte i annan författning anges annat.

Om det är fråga om sådan kamerabevakning som utgör personuppgiftsbehandling som avses i dataskyddsdirektivet, gäller enligt *punkten 2* brottsdatalagen, föreskrifter som meddelats med stöd av den lagen eller annan författning som genomför direktivet. Normalt är det brottsdatalagen och föreskrifter som meddelats med stöd av den som gäller. I den mån det i annan författning finns särskilda bestämmelser som kan tillämpas på kamerabevakning har dessa dock företräde.

Regleringarna gäller ”i tillämpliga delar”, eftersom inte alla bestämmelser är av relevans för kamerabevakning. De bestämmelser som gäller vid kamerabevakning enligt denna paragraf avser exempelvis principer för behandling av personuppgifter, längsta tid som personuppgifter får behandlas, skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden samt rättigheter för registrerade utom

i de delar som förevarande lags bestämmelser gäller i stället. Det som anges om behandling av personuppgifter, personuppgiftsansvarig och registrerade ska tillämpas i fråga om kamerabevakning, den som bedriver kamerabevakning och de som blir föremål för kamerabevakning. Det får bedömas från fall till fall om en viss bestämmelse i dataskyddsförordningen, brottsdatalagen eller annan författning kan tillämpas.

Uttryck i lagen

7 § Uttryck som används i denna lag har samma betydelse som i dataskyddsförordningen när det gäller kamerabevakning som omfattas av förordningen eller lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning eller som i brottsdatalagen (2018:000) när det gäller kamerabevakning som omfattas av den lagen.

Av paragrafen framgår att uttryck som används i lagen har samma betydelse som i dataskyddsförordningen när det gäller kamerabevakning som omfattas av förordningen eller lagen med kompletterande bestämmelser till EU:s dataskyddsförordning eller som i brottsdatalagen när det gäller kamerabevakning som omfattas av den lagen. Det gäller t.ex. uttrycket behandling. Paragrafen har behandlats i avsnitt 10.2.

Tillstånd till kamerabevakning

Krav på tillstånd

8 § Tillstånd krävs till kamerabevakning av en plats dit allmänheten har tillträde, om bevakningen ska bedrivas av en myndighet. Detsamma gäller om kamerabevakning av en sådan plats ska bedrivas av en annan juridisk person eller en fysisk person vid utförande av en uppgift som följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning och

1. avser brottsbekämpning, lagföring eller straffverkställighet eller upprätthållande av allmän ordning och säkerhet,
2. avser nationell säkerhet, eller
3. annars är av allmänt intresse.

I paragrafen anges i vilka fall det krävs tillstånd till kamerabevakning enligt lagen. Tillståndskravet har behandlats i avsnitt 11.1–11.7. I 10 och 11 §§ finns bestämmelser om undantag från tillståndskravet.

Av paragrafen följer att tillstånd krävs till kamerabevakning av en plats dit allmänheten har tillträde i fall då bevakningen ska bedrivas av antingen en myndighet eller ett annat rättssubjekt i viss verksamhet. Enligt 16 § gäller som huvudregel ett krav på upplysning om kamerabevakning, oavsett om bevakningen avser en plats dit allmänheten har tillträde eller en annan plats.

Med plats dit allmänheten har tillträde menas detsamma som enligt tidigare praxis på området. Exempelvis avses gator, torg och parker samt transportmedel för allmänna kommunikationer och ankomst- och avgångshallar för passagerare som använder sådana transportmedel. Ytterligare exempel kan vara utrymmen för allmänheten hos myndigheter, på vårdinrättningar och i simhallar.

Att tillståndskravet gäller vid kamerabevakning, dvs. vid användning av sådan utrustning som omfattas av lagen, innebär i praktiken att tillstånd måste sökas och beviljas innan bevakningen får påbörjas.

Tillståndskravet gäller enligt *första meningen* för alla myndigheter, både statliga och kommunala.

Enligt *andra meningen* gäller tillståndskravet också för andra juridiska personer än myndigheter och för fysiska personer vid utförande av vissa uppgifter förutsatt att uppgiften följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning. Uppgiften ska alltså vara fastställd i gällande rätt på ett konstitutionellt korrekt sätt. Formuleringen omfattar även uppgifter som följer av direkt tillämpliga unionsrättsakter, eftersom sådana gäller i Sverige med den verkan som följer av EU-fördragen. Vad uppgifterna kan avse räknas upp i tre punkter. Endast vissa av uppgifterna kan ha stöd i kollektivavtal.

Enligt *punkten 1* gäller tillståndskravet om uppgiften avser brottsbekämpning, lagföring eller straffverkställighet eller upprätthållande av allmän ordning och säkerhet. Kravet gäller alltså för privaträttsliga subjekt som, genom författning etc., har anförtrotts uppgifter som avser brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet. Det gäller exempelvis ordningsvakter som upprätthåller allmän ordning och säkerhet eller väktare som genom särskilt förordnande har fått i uppdrag att utöva myndighet t.ex. i Polismyndigheten vad gäller någon av de angivna

uppgifterna. Avser förordnandet någon annan uppgift gäller i stället punkten 3.

Av *punkten 2* följer att tillståndskravet även gäller kamerabevakning vid utförande av en uppgift som avser nationell säkerhet, dvs. Sveriges nationella säkerhet. Punkten omfattar t.ex. ett subjekt som i författning eller beslut som meddelats med författningsstöd har anförtrotts en uppgift som avser verksamhet på försvarsområdet. Som exempel kan nämnas sådan särskilt utsedd personal som anlitas som skyddsvakter enligt skyddslagen (2010:305).

Enligt *punkten 3* omfattar tillståndskravet slutligen en uppgift som annars är av allmänt intresse. Begreppet är unionsrättsligt men vid tolkningen kan ledning sökas i hur begreppet ska förstås enligt inhemsk svensk lagstiftning. En sådan uppgift som avses i punkten kan ha tilldelats ett statligt bolag med ett särskilt samhällsintresse genom regeringsbeslut. Det kan också vara en uppgift som med stöd av kommunallagen (1991:900) har getts till ett kommunalt bolag genom beslut i fullmäktige. Även helt privat bedriven verksamhet av allmänt intresse omfattas förutsatt att verksamheten följer av lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning. Oreglerad verksamhet av allmänt intresse omfattas inte liksom inte heller verksamhet som i och för sig är reglerad men inte är av allmänt intresse. I avsnitt 11.5 har närmare beskrivits begreppets innebörd och lämnats exempel på när tillståndskravet gäller respektive inte gäller.

9 § Tillstånd till kamerabevakning ska ges om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad.

Vid bedömningen av intresset av kamerabevakning ska det särskilt beaktas om bevakningen behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats eller på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet till person eller på egendom,
2. förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller begränsa verkningarna av sådana störningar,
3. utöva kontrollverksamhet,
4. förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor, eller
5. tillgodose andra därmed jämförliga ändamål.

Vid bedömningen av den enskildes intresse av att inte bli kamerabevakad ska det särskilt beaktas

1. hur bevakningen ska utföras,
2. om teknik som främjar skyddet av den enskildes personliga integritet ska användas, och
3. vilket område som ska bevakas.

I paragrafen regleras förutsättningarna för att tillstånd till kamerabevakning ska ges. Dessa har behandlats i avsnitt 11.9 och 9.2.2.

För att tillstånd ska kunna ges till en planerad kamerabevakning måste den i grunden vara laglig i den mening som krävs enligt dataskyddsförordningen eller brottsdatalagen, som genomför dataskyddsdirektivet. Huruvida förordningens eller brottsdatalagens krav på laglighet gäller beror på om bevakningen omfattas av förordningens tillämpningsområde eller annars av förordningen genom en bestämmelse i lagen med kompletterande bestämmelser till EU:s dataskyddsförordning, som gäller enligt 6 § 1 i förevarande lag, eller av brottsdatalagens tillämpningsområde. Denna fråga har behandlats bl.a. i avsnitt 10.1. Kravet på tillstånd gäller därutöver. Ett tillstånd till kamerabevakning innebär inte att tillstånd som kan krävas enligt annan lagstiftning inte behövs.

Tillståndsprövningen ska ske i form av en avvägning mellan intresset av kamerabevakning och den enskildes intresse av att inte bli bevakad. En helhetsbedömning av omständigheterna i det enskilda fallet ska göras. I denna ingår att pröva om tillståndet även ska avse tillstånd till efterföljande behandling av bilder eller till avlyssning eller upptagning av ljud.

De intressen av kamerabevakning som ska tillmätas särskild betydelse har utökats eller förtydligats jämfört med den tidigare kameraövervakningslagen. De uttryckligt angivna ändamål som kan åberopas som berättigade för kamerabevakning är alltså fler eller vidare än tidigare. Syftet är att ge ökade möjligheter till tillstånd jämfört med kameraövervakningslagen, särskilt för brottsbekämpande och lagförande ändamål men även för andra ändamål. Det gäller oavsett vem som vill bedriva kamerabevakning. Detta kan dock få betydelse vid bedömningen av hur tungt dennes intresse av bevakning väger. Huruvida ett visst subjekt med fog kan åberopa ett visst intresse och hur tungt det intresset väger får avgöras i det enskilda fallet.

Det förhållandet att kamerabevakning som omfattas av förordningen i vissa sammanhang inte längre är tillstånds- eller anmälningspliktig bör också som utgångspunkt, förutsatt att en sådan bevakning i det enskilda fallet kan antas vara förenlig med förordningen oavsett om den faktiskt sker, medföra att tillstånd kan ges i högre utsträckning till tillståndsskyldig kamerabevakning i närheten. Som exempel kan nämnas tillståndsfri kamerabevakning på en snabbmatsrestaurang inrymd i ankomst- och avgångshallen på en järnvägsstation. Kamerabevakning av hallen i närheten av restaurangen bör då normalt inte anses lika integritetskänslig som tidigare.

De ökade möjligheterna till tillstånd gäller också tillstånd till efterföljande behandling av bilder, inklusive inspelning, även om ett sådant tillstånd generellt sett inte regelmässigt bör följa. Ett tillstånd till kamerabevakning för brottsbekämpande ändamål bör dock i regel innefatta en sådan rätt. En sådan bör också kunna ges i större utsträckning i andra fall än vad som varit möjligt tidigare.

Tillståndsgivningen vad gäller avlyssning eller upptagning av ljud bör präglas av restriktivitet. Endast om ett starkt behov av en avlyssning- eller upptagningsmöjlighet kan påvisas i det enskilda fallet bör tillstånd till detta ges.

Vad gäller kamerabevakning som ska ske från rörliga objekt, t.ex. drönare, behövs inte ett tillstånd för varje enskild flygning eller varje uppdrag utan ett mer generellt tillstånd kan meddelas.

Enligt *första stycket* ska tillstånd till kamerabevakning ges om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad. En proportionalitetsbedömning med en överviktsprincip gäller. Det räcker att intresset av kamerabevakning väger över det motstående intresset för att tillstånd ska ges. Kamerabevakning bör inte ses som ett hjälpmedel som ska användas i stället för andra åtgärder i samma syfte utan som ett komplement till sådana åtgärder, särskilt när det gäller brottsförebyggande åtgärder.

I *andra stycket* anges vad som särskilt ska beaktas vid bedömningen av intresset av kamerabevakning.

Enligt *punkten 1* ska det särskilt beaktas om bevakning behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på en brottsutsatt plats eller på en annan plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet till person eller på egendom.

Punkten är delvis helt ny, delvis vidare än kameraövervakningslagens motsvarande bestämmelse.

Vad gäller en brottsutsatt plats tar punkten sikte på brott i allmänhet, t.ex. våldsbrott, stöldbrott och narkotikabrott. Med en sådan plats menas inte varje plats där det någon gång har inträffat enstaka brott. Det krävs att människor eller egendom på platsen eller platsen i övrigt drabbats av brott i viss omfattning.

Punkten omfattar även vissa typer av brottslighet på annan plats. Med en plats där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet till person eller på egendom avses en plats som inte är, eller kan visas vara, utsatt för sådana brott i den mening som avses med brottsutsatt plats men där det finns en särskild risk för angrepp av de angivna slagen jämfört med andra platser i samhället dit allmänheten har tillträde. Det är en plats där sådana angrepp inträffat med viss upprepning utan att platsen kan anses brottsutsatt eller där det finns en generell hotbild avseende de typerna av angrepp mot människor som bor, arbetar eller annars vistas regelmässigt på platsen eller mot egendom som finns där, t.ex. en viss byggnad eller fordon med anknytning till platsen. Ett exempel kan vara en förläggning för asylsökande såvitt gäller delar dit allmänheten har tillträde och ett annat en myndighets lokaler för anställda och myndighetens fordon. Med angrepp på någons liv, hälsa eller trygghet till person avses bl.a. misshandelsbrott, olaga tvång, olaga hot, våld eller hot mot tjänsteman, ofredande och sexualbrott. Också t.ex. våldsamt upplopp omfattas. Detsamma gäller terroristbrott. Med angrepp på egendom avses brott som innebär förstörelse av egendom, t.ex. skadegörelse och mordbrand, däremot inte andra brott som avser egendom, t.ex. fickstölder. Även bl.a. terroristbrott och sabotage innefattas i begreppet angrepp på egendom.

Intresset av att utreda och lagföra brott bör ges stor tyngd oavsett om kamerabevakningen samtidigt kan antas förebygga brottslighet på platsen eller inte. Med behov av bevakning för att utreda och lagföra brott avses behov av teknisk bevisning för att utreda framtida brott som kan komma att begås på platsen. Ett behov av kameraanvändning som aktualiseras först efter det att ett brott har begåtts och där kameraanvändningen enbart syftar till att utreda detta brott inom ramen för en förundersökning kan inte tillgodoses genom tillstånd enligt denna lag. Däremot medger givetvis ett till-

stånd som meddelats enligt denna punkt att en pågående kamerabevakning får fortsätta för att säkra utredning om brott som inträffar under bevakningen.

Tillstånd enligt punkten 1 bör många gånger kunna ges för att motverka terrorangrepp, angrepp på polismän, brandkårs- och ambulanspersonal och liknande yrkeskategorier, övergrepp – exempelvis sexuella ofredanden eller ofredanden – i samband med stora folksamlingar, t.ex. på konserter, eller på särskilt integritetskänsliga platser såsom simhallar. Detsamma gäller för att motverka brott i särskilt utsatta bostadsområden, på förläggningar för asylsökande, på inrättningar för hälso- och sjukvård samt på bussar, tåg, spårvagnar och andra färdmedel avsedda för allmän personbefordran och platser för ankommande och avresande passagerare med sådana färdmedel.

Av *punkten 2* följer vidare att det särskilt ska beaktas om kamerabevakning behövs för att förebygga, förhindra eller upptäcka störningar av allmän ordning och säkerhet eller begränsa verkningarna av sådana störningar. Denna punkt är ny jämfört med kameraövervakningslagen och överlappar delvis punkten 1. Intresset av allmän ordning och säkerhet kan vara berättigat att åberopa för såväl myndigheter som andra som har ett ansvar för ordning och säkerhet som följer av författning, t.ex. av ordningslagen (1993:1617). Exempel på sådana aktörer är Polismyndigheten och kommunala myndigheter och subjekt som bedriver kollektivtrafik. Begreppet allmän ordning och säkerhet bör tolkas på det sätt som görs enligt de andra relevanta författningar i vilka det förekommer.

Enligt *punkten 3* ska det särskilt beaktas om kamerabevakning behövs för att utöva kontrollverksamhet. Som exempel kan nämnas gränskontroll och tullkontroll. Andra exempel är kontroll av vattenskyddsområden, dammsäkerhet och miljöfarliga verksamheter. Punkten är ny jämfört med kameraövervakningslagen.

Vidare ska det enligt *punkten 4* särskilt beaktas om kamerabevakning behövs för att förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor. Punkten omfattar såväl olyckor som kan drabba människors liv och hälsa som olyckor som kan drabba egendom och miljön. Detta intresse av bevakning har vidgats jämfört med kameraövervakningslagen.

Slutligen följer av *punkten 5* att det särskilt ska beaktas om kamerabevakning behövs för att tillgodose andra därmed jämförliga ändamål, dvs. ändamål som är jämförbara med ändamålen i punk-

terna 1–4. Till följd av att punkterna 1–4 är delvis nya, delvis vidgade jämfört med kameraövervakningslagen innebär punkten 5 en utvidgning jämfört med den lagen. Exempel på kamerabevakning för därmed jämförliga ändamål är kamerabevakning för utförande av en uppgift som avser Sveriges säkerhet och som inte omfattas av de tidigare punkterna, kamerabevakning i samband med forskning som avser hur olyckor kan undvikas, t.ex. i trafiken, och kamerabevakning för inventering av djur eller någon annan viltvård. Ytterligare ett exempel är kamerabevakning som sker genom flygning av kamerautrustade drönare i övningssyfte hos en myndighet när myndighetens verksamhet är sådan som omfattas av någon av punkterna 1–4.

Även andra ändamål än de som anges i punkterna 1–5 kan vara berättigade och innebära att intresset av kamerabevakning väger över den enskildes intresse av att inte bli kamerabevakad. Normalt krävs då att integritetsriskerna är försumbara. Ibland kan riskerna vara större och intresset av kamerabevakning ändå väga över. Så kan vara fallet, om tillsynsmyndigheten kan förena ett tillstånd till kamerabevakning med villkor som begränsar integritetsintrånget. Ett exempel på ett berättigat intresse av kamerabevakning som kan väga över det motstående intresset är kamerabevakning från en drönare som sker för att dokumentera landskap i samband med byggprojekt eller översikts- och detaljplaner.

I *punkterna 1–3 i tredje stycket* anges vad som särskilt ska beaktas vid bedömningen av den enskildes intresse av att inte bli kamerabevakad. Det ska beaktas hur bevakningen ska utföras, om teknik som främjar skyddet av den enskildes personliga integritet ska användas och vilket område som ska bevakas.

Som exempel på integritetsfrämjande teknik kan nämnas teknik som innebär att personer i bild maskeras så att det inte går att identifiera dem, teknik som krypterar upptaget bild- och ljudmaterial och kameror som aktiveras först efter olika typer av larm, såsom larm som reagerar på onormala rörelsemönster, inbrottslarm, överfallslarm, evakueringslarm och larm som aktiveras av skottlossning, glaskross eller människoskrik. Integritetsfrämjande teknik kan många gånger ha stor betydelse för hur tungt intresset av att inte bli kamerabevakad väger och medföra att intresset av kamerabevakningen väger över.

Vad gäller det område som ska bevakas är det av betydelse om det är ett område där många människor normalt rör sig. Det gäller oavsett om bevakningen ska ske från ett fast placerat objekt eller från ett rörligt objekt. Områdets karaktär är också av betydelse. Exempelvis är enskildas intresse av att inte bli kamerabevakade särskilt starkt i omklädningsrum och på liknande platser.

När intresset av brottsbekämpning åberopas till stöd för kamerabevakning bör integritetsintresset anses vara mindre starkt när de enskilda som kan bli föremål för kamerabevakningen samtidigt är de som riskerar att drabbas av den brottslighet som bevakningen syftar till att motverka. Motsvarande bör gälla i fråga om intressen som avser allmän ordning och säkerhet samt olyckor.

Undantag från tillståndskravet

10 § Tillstånd till kamerabevakning krävs inte vid

1. bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning,

2. bevakning som sker för att skydda en byggnad, en annan anläggning eller ett område som enligt 4 § 4, 5 § 1–4 eller 6 § första stycket skyddslagen (2010:305) har förklarats vara skyddsobjekt, om bevakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet,

3. bevakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning,

4. bevakning som Trafikverket bedriver

a) av vägtrafik eller av sjötrafik vid en rörlig bro,

b) vid en betalstation som avses i bilagorna till lagen (2004:629) om trängselskatt och som sker för att samla in endast uppgifter som behövs för att beslut om trängselskatt ska kunna fattas och för att kontrollera att sådan skatt betalas, och

c) vid en betalstation på allmän väg som används vid uttag av infrastrukturavgifter enligt lagen (2014:52) om infrastrukturavgifter på väg och som sker för att samla in endast uppgifter som behövs för att beslut om infrastrukturavgift ska kunna fattas och för att kontrollera att sådan avgift betalas,

5. sådan trafikbevakning i en vägtunnel som avses i lagen (2006:418) om säkerhet i vägtunnlar och som bedrivs av någon annan tunnelhållare än Trafikverket,

6. bevakning i en tunnelbanevagn eller av en tunnelbanestation, om bevakningen har till enda syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott eller förebygga, förhindra eller upptäcka olyckor eller begränsa verkningarna av inträffade olyckor,

7. bevakning i en lokal där det bedrivs postverksamhet eller av området omedelbart utanför in- och utgångar till en sådan lokal eller av en yta i en butikslokal på vilken det bedrivs postverksamhet, om bevakningen har till enda syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott,

8. bevakning i ett parkeringshus, om bevakningen har till enda syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott, och

9. bevakning som sker för säkerheten i trafiken eller arbetsmiljön från ett fordon, en maskin eller liknande för att förbättra sikten för föraren eller användaren.

Undantaget från tillståndskravet i första stycket 2 gäller inte för sådana byggnader, andra anläggningar och områden som används för eller är avsedda för fredstida krishantering enligt 4 § 4 skyddslagen.

Paragrafen reglerar i nio punkter undantag från kravet på tillstånd till kamerabevakning. Övervägandena finns i avsnitt 11.8. Paragrafen motsvarar i stora delar vad som gällt tidigare enligt kameraövervakningslagen.

Undantaget i *punkten 4* är delvis förändrat jämfört med vad som gällt tidigare. Undantaget i a) omfattar numera också bevakning som bedrivs av Trafikverket av sjötrafik vid en rörlig – öppningsbar – bro i anslutning till väg.

Undantagen i *punkterna 6–8* är nya jämfört med kameraövervakningslagen. De motsvarar i huvudsak kamerabevakning i vissa situationer som varit anmälningsskyldiga enligt den lagen. I punkten 6, som avser kamerabevakning i en tunnelbanevagn eller av en tunnelbanestation, är syftena förhindra och lagföra brott nya. Syftet upptäcka brott har ersatt det tidigare avslöja brott. Vidare har syftena förebygga och upptäcka olyckor lagts till. Med tunnelbanestation avses ett område där det bedrivs tunnelbaneverksamhet och krävs färdbevis för att vistas. I punkten 7, som avser kamerabevakning på platser där det bedrivs postverksamhet, är syftena förhindra brottslig verksamhet och lagföra brott nya medan syftet upptäcka brott har ersatt det tidigare avslöja brott. Med en lokal där det bedrivs postverksamhet avses en lokal där det huvudsakligen bedrivs verk-

samhet i vilken det ingår postverksamhet. Med en yta i en butikslokal på vilken det bedrivs postverksamhet menas ett visst område avsett för sådan verksamhet i en lokal där konsumenter kan köpa varor och tjänster eller hyra varor, dock inte restauranger och andra näringsställen. Postverksamhet definieras i postlagen (2010:1045). Även i punkten 8, som avser kamerabevakning i parkeringshus, har syftena utökats eller ändrats på samma sätt som i punkten 7. Undantagen från tillståndskravet i punkterna gäller kamerabevakning i sin helhet, dvs. användning av utrustning eller anordning som avses i 3 § 1–3, och omfattar därmed också avlyssning och upptagning av ljud.

Tillfälliga undantag från tillståndskravet

11 § Kamerabevakning får ske under högst en månad utan att en ansökan om tillstånd har gjorts vid

1. bevakning som bedrivs av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet som innebär fara för liv eller hälsa eller för omfattande förstörelse av egendom på en viss plats och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott,

2. bevakning som bedrivs av Polismyndigheten eller den som är räddningsledare enligt lagen (2003:778) om skydd mot olyckor, om bevakningen är av vikt för att avvärja en hotande olycka eller begränsa verkningarna av en inträffad olycka, och

3. bevakning som bedrivs av den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att efterforska en försvunnen person.

Om en ansökan om tillstånd görs inom en månad från det att kamerabevakningen inleddes, får bevakningen bedrivas utan tillstånd till dess att ansökningen har prövats.

Paragrafen reglerar i punkterna 1–3 tillfälliga undantag från kravet på tillstånd till kamerabevakning. Paragrafen motsvarar vad som gällt tidigare enligt kameraövervakningslagen utom vad avser *punkten 1* där syftena upptäcka brottslig verksamhet, utreda brott och lagföra brott är nya och där det förtydligats att syftena i punkten avser sådan brottslighet och sådana brott som anges i denna. Med syftena utreda och lagföra avses ett behov av teknisk bevisning för att utreda och lagföra de framtida brott av de i punkten angivna typerna

som det av särskild anledning finns risk för. De brottstyper som avses är delvis samma som de som särskilt räknas upp i en del av 9 § andra stycket 1. Punkten 1 i förevarande paragraf är snävare. Den avser något färre brottstyper och innehåller krav på att dessa ska vara av kvalificerat slag. Paragrafen har behandlats i avsnitt 11.8.

Ansökan om tillstånd

12 § En ansökan om tillstånd till kamerabevakning ska göras skriftligen hos tillsynsmyndigheten.

Ansökningen ska innehålla

1. uppgift om den som ska bedriva bevakningen och i förekommande fall den som ska ha hand om bevakningen för tillståndshavarens räkning,
2. uppgift om bevakningens ändamål,
3. en beskrivning av bevakningen, särskilt den utrustning som ska användas, var utrustningen ska placeras, det område som ska bevakas och de tider då bevakning ska ske,
4. en bedömning av behovet av och proportionaliteten i bevakningen i förhållande till ändamålet,
5. en bedömning av riskerna för intrång i den personliga integriteten och en beskrivning av de åtgärder som planeras för att hantera riskerna, och
6. uppgift om de omständigheter i övrigt som är av betydelse för prövningen av ärendet.

Om bevakningen avser en arbetsplats, ska ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med ansökningen.

I paragrafen finns bestämmelser om ansökningar om tillstånd till kamerabevakning. Innehållet i bestämmelsen har behandlats dels i avsnitt 11.10, dels i avsnitt 13.

Av *första stycket* följer att en ansökan om tillstånd ska vara skriftlig och göras hos tillsynsmyndigheten. Av föreskrifter följer att Datainspektionen är tillsynsmyndighet.

I *andra stycket* anges vad ansökningen ska innehålla. I de uppgifter som ska lämnas ligger också att sökanden bör beskriva varför ändamålet med bevakningen inte kan tillgodoses genom något annat medel, särskilt när det gäller brottsförebyggande åtgärder.

Om kamerabevakningen avser en arbetsplats, ska enligt *tredje stycket* sökanden tillsammans med ansökningen lämna in ett yttrande från ett skyddsombud, en skyddskommitté eller en orga-

nisation som företräder arbetstagarna på arbetsplatsen. I yttrandet bör anges om bevakningen godtas eller inte. Om den inte godtas, bör skälen för det framgå. Inställningen i ett sådant yttrande bör tillmätas särskild betydelse i tillståndsprövningen. Bestämmelsen gäller när den som vill bedriva kamerabevakning är arbetsgivare och kamerabevakningen avser dennes arbetsplats där han eller hon bedriver verksamhet. Flera yttranden kan krävas, om det finns olika arbetstagargrupper på arbetsplatsen.

Yttrande av kommunen

13 § Innan tillsynsmyndigheten beslutar om tillstånd till kamerabevakning ska den kommun där bevakningen ska ske få tillfälle att yttra sig, om det behövs.

Av paragrafen följer att tillsynsmyndigheten i ett ärende om tillstånd till kamerabevakning ska ge den kommun där bevakningen ska ske tillfälle att yttra sig, om det behövs. Syftet med bestämmelsen är att säkerställa att lokala synpunkter beaktas i ärendet när sådana kan vara av betydelse. Det bör i det enskilda ärendet stå klart att det finns ett behov av att höra kommunen för att ett yttrande ska inhämtas. Tillsynsmyndigheten avgör om ett yttrande ska inhämtas och på vilket stadium av handläggningen det ska ske. Frågan om yttrande har behandlats i avsnitt 11.10.

Beslut om tillstånd

14 § Ett beslut om tillstånd till kamerabevakning ska ange vem som ska bedriva bevakningen och i förekommande fall vem som ska ha hand om bevakningen för tillståndshavarens räkning.

Beslutet ska förenas med villkor om hur kamerabevakningen får anordnas. Villkoren ska avse

1. bevakningens ändamål,
2. den utrustning som får användas och var utrustningen får placeras,
3. det område som får bevakas och de tider då bevakning får ske, och
4. upplysning om bevakningen, behandling av bilder eller ljud och andra förhållanden som har betydelse för att skydda enskildas personliga integritet, om sådana villkor behövs för tillståndet.

Ett tillstånds giltighet får begränsas till en viss tid.

15 § Om förutsättningarna för ett tillstånd ändras, får tillsynsmyndigheten besluta om nya villkor eller, om förutsättningarna för tillstånd inte längre är uppfyllda, återkalla tillståndet.

I paragraferna regleras innehåll i tillsynsmyndighetens beslut om tillstånd till kamerabevakning och myndighetens möjlighet att vid ändrade förutsättningar besluta om nya tillståndsvillkor eller återkalla tillståndet. Tillsynsmyndigheten ska förena ett tillstånd med vissa villkor och kan förena det med ytterligare villkor. Ett tillstånd kan tidsbegränsas t.ex. när kamerabevakningen är planerad att pågå endast under en viss tidsperiod eller när bevakningen är så integritetskänslig att det finns skäl att efter en viss tid göra en förnyad prövning. Om förutsättningarna för ett tillstånd ändras, bör tillståndshavaren anmäla det till tillsynsmyndigheten. I första hand bör tillsynsmyndigheten besluta om nya villkor. Endast om det inte ter sig meningsfullt bör tillståndet återkallas. Frågorna har behandlats i avsnitt 11.10.

Upplysning om kamerabevakning

Krav på upplysning

16 § Vid kamerabevakning ska genom tydlig skyltning eller på något annat liknande verksamt sätt lämnas upplysning om

1. kamerabevakningen,
2. identiteten hos och kontaktuppgifterna till den som ska bedriva bevakningen, och
3. kontaktuppgifter till ett eventuellt dataskyddsombud.

Om ljud kan avlyssnas eller tas upp vid bevakningen, ska en särskild upplysning lämnas om detta.

Information ska även göras tillgänglig för dem som kan bli kamerabevakade om

1. ändamålet med och den rättsliga grunden för kamerabevakningen,
2. hur länge upptaget bild- och ljudmaterial får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa detta, och
3. möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifterna till den.

I paragrafen finns bestämmelser om krav på upplysning vid kamerabevakning. Bestämmelsen har behandlats i avsnitt 12.1. I 17 och 19 §§ finns bestämmelser om undantag från upplysningskravet.

Enligt paragrafen ska vid kamerabevakning genom tydlig skyltning eller på något annat liknande verksamt sätt lämnas vissa upplysningar. Dessutom ska viss ytterligare information göras tillgänglig för dem som kan bli kamerabevakade. Kravet i paragrafen riktar sig mot den som ska bedriva kamerabevakning. Det gäller för all kamerabevakning som omfattas av lagen oavsett om tillstånd till kamerabevakningen krävs eller inte och oberoende av om bevakningen avser en plats dit allmänheten har tillträde eller en annan plats. I vissa fall används en kamera av flera aktörer. I de fallen ska upplysningar enligt bestämmelsen lämnas beträffande varje aktör.

Upplysningskravet inträder när kamerabevakningen sker. Det innebär i praktiken att upplysningar måste lämnas innan bevakningen får påbörjas. Genom upplysningarna ska en enskild få möjlighet att undvika kamerabevakningen eller att anpassa sitt uppträdande till att bevakning sker och få möjlighet att ta till vara sina rättigheter enligt dataskyddsförordningen eller brottsdatalagen i enlighet med vad som följer av 6 §. Kravet på upplysning gäller i stället för förordningens och den lagens bestämmelser om rätten till information.

Att upplysningar enligt *första stycket* ska lämnas genom tydlig skyltning eller på något annat liknande verksamt sätt innebär att människor som kan bli föremål för kamerabevakning ska kunna få kännedom om innehållet i upplysningarna. Det krävs inte att varje individ som kan beröras av bevakningen faktiskt har tagit del av upplysningarna. Det är tillräckligt att åtgärderna varit ägnade att underrätta honom eller henne om bevakningen. Vad som kan anses vara en verksam upplysning varierar beroende på vilket område som ska bevakas och vilka personer som kan komma att bevakas.

Skyltning är ofta ändamålsenlig när kamerabevakningen avser inomhusmiljöer. Om bevakningen avser en begränsad krets av personer, kan det ibland vara lämpligare att lämna skriftlig information direkt till de berörda. Flera informationssätt kan kombineras.

Också när kamerabevakning sker utomhus, från utrustning på såväl fast placerade objekt som rörliga objekt såsom fordon eller drönare, kan i många fall verksamma upplysningar lämnas genom skyltning. Skyltning kan t.ex. ske på den plats som ska kamerabevakas, vid vägar eller stigar som leder in i det område som ska be-

vakas eller genom klisterlappar på fordon i vägtrafik. Vad särskilt gäller kamerabevakning som sker från drönare kan det finnas situationer då verksamma upplysningar inte alls eller inte enbart kan lämnas genom skyltning på platsen. Så kan t.ex. vara fallet när bevakningen avser ett större område. Det kan då krävas en kombination av åtgärder, t.ex. information i programblad eller liknande, på en webbplats eller i annonser, för att upplysningarna ska vara verksamma. Operatören av drönaren bör även bära varselväst för att informera om bevakningen.

Vid kamerabevakning som sker med stöd av tillstånd enligt 8 § ska enligt 14 § andra stycket 4 tillsynsmyndigheten, om det behövs, i tillståndsbeslutet meddela villkor som avser upplysning om bevakningen och kan därigenom anpassa kravet på upplysning till förhållandena i det enskilda fallet.

Enligt första stycket *punkten 1* ska upplysning lämnas om kamerabevakningen, dvs. att platsen är kamerabevakad. En text som upplyser om detta kan förses med en kamerasymbol för att göra informationen lättare att upptäcka och förstå. Vidare ska enligt *punkten 2* upplysning lämnas om identiteten hos och kontaktuppgifterna till den som ska bedriva bevakningen. Namnet på den fysiska eller juridiska person som ska bedriva kamerabevakningen och uppgift om dennes postadress, telefonnummer, webbadress, e-postadress eller motsvarande ska lämnas. Upplysning ska enligt *punkten 3* också lämnas om kontaktuppgifter till ett eventuellt dataskyddsombud. Det kan men behöver inte vara en kontaktuppgift direkt till ombudet. Det är tillräckligt att ombudet går att nå med hjälp av uppgifterna. I verksamheter som omfattas av brottsdatalagen ska ett eller flera dataskyddsombud utses. I verksamheter som omfattas av dataskyddsförordningen behöver ett dataskyddsombud endast utses i vissa fall.

Om ljud kan avlyssnas eller tas upp vid bevakningen, ska enligt *andra stycket* en särskild upplysning lämnas om detta. En sådan upplysning ska lämnas på det sätt som anges i första stycket.

Av *tredje stycket* följer att den som ska bedriva kamerabevakning även ska göra viss annan information tillgänglig för dem som kan bli kamerabevakade. Att informationen ska göras tillgänglig innebär att den antingen kan lämnas på samma sätt som upplysningarna enligt första och andra styckena eller kan tillhandahållas på annat sätt,

t.ex. på en webbsida dit man kan söka sig genom de kontaktuppgifter som det enligt första stycket ska upplysas om.

Enligt *punkten 1* ska information om ändamålet med och den rättsliga grunden för kamerabevakningen tillgängliggöras. Om det finns flera ändamål, ska samtliga dessa anges. Det är typen av ändamål som kamerabevakningen sker för och den konkreta rättsliga grunden för bevakningen, t.ex. ett visst författningsstöd, som ska anges. Om kamerabevakningen kan ske utan krav på tillstånd och efter en intresseavvägning enligt förordningen, får även anges vilket intresse som motiverar kamerabevakningen i det enskilda fallet. Enligt *punkten 2* ska information göras tillgänglig om hur länge upptaget bild- och ljudmaterial får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa detta. För det fall bild och ljud endast förmedlas direkt utan att spelas in ska detta anges. Slutligen ska enligt *punkten 3* informeras om möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifterna till den.

Undantag från upplysningskravet

17 § Upplysning om kamerabevakning behöver inte lämnas vid

1. bevakning som Polismyndigheten bedriver vid automatisk hastighetsövervakning,

2. bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller Säkerhetspolisen, om det av särskild anledning finns risk för allvarlig brottslighet som innebär fara för liv eller hälsa eller för omfattande förstörelse av egendom på en viss plats och syftet med bevakningen är att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda eller lagföra sådana brott,

3. bevakning som sker för att skydda en byggnad, en annan anläggning eller ett område som enligt 4 § 4, 5 § 1–4 eller 6 § första stycket skyddslagen (2010:305) har förklarats vara skyddsobjekt, om bevakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet,

4. bevakning som Försvarsmakten bedriver från ett fordon, fartyg eller luftfartyg som ett led i en militär insats eller militär övning eller som behövs för att prova utrustning för sådan bevakning,

5. bevakning som bedrivs i brådskande fall från ett luftfartyg av Polismyndigheten eller den som är räddningsledare enligt lagen (2003:778) om skydd mot olyckor, om bevakningen är av vikt för att avvärja en hotande olycka eller begränsa verkningarna av en inträffad olycka, och

6. bevakning som bedrivs av den som är räddningsledare enligt lagen om skydd mot olyckor, om bevakningen är av vikt för att efterforska en försvunnen person.

Undantaget från upplysningskravet i första stycket 3 gäller inte för sådana byggnader, andra anläggningar eller områden som används för eller är avsedda för fredstida krishantering enligt 4 § 4 skyddslagen.

I paragrafen regleras i sex punkter generella undantag från kravet på upplysning om kamerabevakning. Bestämmelsen har behandlats i avsnitt 12.2.

Paragrafen motsvarar i punkterna 1, 3, 4 och 6 vad som gällt tidigare enligt kameraövervakningslagen. Punkterna 2 och 5 är nya. Undantagen i paragrafen motsvarar undantagen från tillståndskravet i 10 § första stycket 1–3 och motsvarar delar av undantagen från det kravet i 11 §.

Undantaget i *punkten 2* motsvarar det tillfälliga undantaget från tillståndskravet i 11 § första stycket 1 med de tillkommande kraven att det är fråga om ett brådskande fall och att kamerabevakningen sker från ett luftfartyg, t.ex. en drönare. Undantaget innebär att kamerabevakning får ske utan att upplysning om den lämnas när det är brådskande att påbörja bevakningen samtidigt som förhållandena är sådana i det enskilda fallet att det inte är praktiskt möjligt att direkt uppfylla upplysningskravet.

Undantaget i *punkten 5* motsvarar det tillfälliga undantaget från tillståndskravet i 11 § första stycket 2 med de tillkommande kraven att det är fråga om ett brådskande fall och att kamerabevakningen sker från ett luftfartyg, t.ex. en drönare. Undantaget innebär att kamerabevakning får ske utan att upplysning om den lämnas när det finns ett behov av att skyndsamt påbörja bevakningen samtidigt som förhållandena är sådana i det enskilda fallet att det inte är praktiskt möjligt att direkt uppfylla upplysningskravet. Så kan t.ex. vara fallet när en olycka inträffat vid en större anläggning där den bedrivna verksamheten är sådan att olyckan kan orsaka allvarliga skador på många människor eller på miljön.

Efter den första akuta inledningsfasen i de fall som avses i punkterna 2 och 5 får – förutsatt att kamerabevakningen behöver fortsätta – antingen upplysningskravet uppfyllas, om det då är praktiskt möjligt exempelvis genom att bevakningen anordnas för ett mer avgränsat område, eller ett undantag från kravet sökas enligt 19 §.

Av 18 § framgår att undantagen inte gäller, om ljud ska avlyssnas eller tas upp vid kamerabevakningen.

18 § Undantagen från upplysningskravet gäller inte, om ljud ska avlyssnas eller tas upp vid kamerabevakningen.

Av paragrafen följer att undantagen i 17 § från kravet på upplysning inte gäller, om ljud ska avlyssnas eller tas upp vid kamerabevakningen. Undantag från upplysningskravet i enskilda fall enligt 19 § träffas inte av förevarande paragraf. Paragrafen har behandlats i avsnitt 12.2.

Undantag från upplysningskravet i enskilda fall

19 § Om det finns synnerliga skäl, får tillsynsmyndigheten i enskilda fall besluta om undantag från upplysningskravet.

I paragrafen finns en bestämmelse om undantag i enskilda fall från kravet på upplysning om kamerabevakning. Bestämmelsen har behandlats i avsnitt 12.2.

Av paragrafen framgår att tillsynsmyndigheten får besluta om undantag från upplysningskravet, om det finns synnerliga skäl. Undantagsmöjligheten ska tillämpas restriktivt.

Undantag kan beslutas i fall där syftet med kamerabevakningen skulle gå förlorat, om upplysning skulle lämnas om bevakningen. Exempel på när ett sådant undantag kan komma i fråga är kamerabevakning av rovdjurslyor i syfte att upptäcka och beivra tjuvskytte eller plundring eller i syfte att kartlägga rovdjursbeståndet.

Undantag kan också beslutas när upplysningskravet är praktiskt omöjligt att uppfylla, t.ex. därför att kamerabevakningen ska ske från ett luftfartyg, såsom en drönare, vid olika tillfällen och avse stora områden som skiftar från gång till annan samtidigt som behovet av bevakning kommer att uppkomma hastigt vid de enskilda tillfällena. När sådan kamerabevakning ska ske för ett berättigat och starkt intresse och de motstående integritetsaspekterna inte gör sig gällande med någon större tyngd bör undantag medges. Som exempel kan nämnas kamerabevakning i räddningsverksamhet som bedrivs av en frivilligorganisation.

Undantag kan vidare komma i fråga när kamerabevakning i ett brådskande fall bedrivs utan upplysning med stöd av något av de generella undantagen i 17 § första stycket 2 och 5 och behovet av att kamerabevaka kvarstår efter det inledande, akuta skedet och upplysningskravet inte heller då kan uppfyllas.

Ett undantag från upplysningskravet får omfatta avlyssning eller upptagning av ljud. Ett sådant undantag bör dock endast komma i fråga i undantagsfall där intresset av kamerabevakning utan upplysning är berättigat och väger tungt samtidigt som intresset av integritetsskydd är marginellt. Ett exempel är kamerabevakning som syftar till att kartlägga föryngringen av rovdjursstammen.

Ansökan om undantag

20 § En ansökan om undantag från upplysningskravet ska göras skriftligen hos tillsynsmyndigheten.

Ansökningen ska innehålla uppgift om den som ska bedriva kamerabevakningen och i förekommande fall den som ska ha hand om bevakningen för hans eller hennes räkning samt skälen för ansökningen.

Om bevakningen avser en arbetsplats, ska ett yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen lämnas in tillsammans med ansökningen.

I paragrafen finns bestämmelser om ansökningar om undantag i enskilda fall från kravet på upplysning om kamerabevakning. Innehållet i bestämmelsen har behandlats dels i avsnitt 12.2, dels i avsnitt 13.

Av *första stycket* följer att en ansökan om undantag ska vara skriftlig och göras hos tillsynsmyndigheten. Av föreskrifter följer att Datainspektionen är tillsynsmyndighet.

Enligt *andra stycket* ska ansökningen innehålla uppgift om den som ska bedriva kamerabevakningen och i förekommande fall den som ska ha hand om bevakningen för hans eller hennes räkning samt skälen för ansökningen. Sökanden bör i regel ange ändamålet med kamerabevakningen och lämna en beskrivning av bevakningen, t.ex. genom att uppge vilken utrustning som ska användas, var utrustningen ska placeras, vilket område som ska bevakas och vilka tider som bevakningen ska ske.

Om kamerabevakningen avser en arbetsplats, ska enligt *tredje stycket* sökanden tillsammans med ansökningen lämna in ett

yttrande från ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen. I yttrandet bör anges om ett undantag från upplysningskravet godtas eller inte. Om det inte godtas, bör skälen för det framgå. Inställningen i ett sådant yttrande bör tillmätas särskild betydelse i prövningen av om undantag ska beslutas. Bestämmelsen gäller när den som vill bedriva kamerabevakning är arbetsgivare och kamerabevakningen avser dennes arbetsplats där han eller hon bedriver verksamhet. Flera yttranden kan krävas, om det finns olika arbetstagargrupper på arbetsplatsen.

Yttrande av kommunen

21 § Innan tillsynsmyndigheten beslutar om undantag från upplysningskravet ska den kommun där kamerabevakningen ska ske få tillfälle att yttra sig, om bevakningen ska avse en plats dit allmänheten har tillträde och det behövs ett yttrande.

Av paragrafen följer att tillsynsmyndigheten i ett ärende om undantag från upplysningskravet ska ge den kommun där bevakningen ska ske tillfälle att yttra sig, om bevakningen ska avse en plats dit allmänheten har tillträde och det behövs ett yttrande. Syftet med bestämmelsen är att säkerställa att lokala synpunkter beaktas i ärendet när sådana kan vara av betydelse. Det bör i det enskilda fallet stå klart att det finns ett behov av att höra kommunen för att ett yttrande ska inhämtas. Om tillsynsmyndighetens prövning brådskar och undantaget är avsett att gälla endast för en begränsad tid, kan det tala för att ett yttrande inte bör inhämtas. Tillsynsmyndigheten avgör om ett yttrande ska inhämtas och på vilket stadium av handläggningen det ska ske. Frågan om yttrande har behandlats i avsnitt 12.2.

Beslut om undantag

22 § Ett beslut om undantag från upplysningskravet ska ange vem som ska bedriva kamerabevakningen och i förekommande fall vem som ska ha hand om bevakningen för hans eller hennes räkning.

Beslutet ska förenas med de villkor som behövs.

23 § Om förutsättningarna för ett beslut om undantag ändras, får tillsynsmyndigheten ändra beslutet eller, om förutsättningarna för ett sådant beslut inte längre är uppfyllda, återkalla detta.

I paragraferna regleras innehåll i tillsynsmyndighetens beslut om undantag från upplysningskravet och myndighetens möjlighet att vid ändrade förutsättningar besluta om ändring eller återkallelse av beslutet. Tillsynsmyndigheten ska förena ett beslut om undantag med de villkor som behövs. Ett beslut kan behöva förenas med villkor som motsvarar ett eller flera av de villkor som ett beslut om tillstånd till kamerabevakning enligt 14 § andra stycket ska förenas med. Undantaget får också begränsas till att gälla en viss tid. Om förutsättningarna för ett beslut om undantag ändras, bör den som bedriver kamerabevakningen anmäla det till tillsynsmyndigheten. I första hand bör tillsynsmyndigheten besluta om ändring av beslutet. Endast om det inte ter sig meningsfullt bör beslutet om undantag återkallas. Frågorna har behandlats i avsnitt 12.2.

Förhandlingsskyldighet för arbetsgivare

Förhandlingsskyldighet

24 § Innan en arbetsgivare beslutar om kamerabevakning som avser arbetsplatsen och som inte omfattas av kravet på tillstånd ska arbetsgivaren förhandla med berörd arbetstagarorganisation på det sätt som anges i 11–14 §§ lagen (1976:580) om medbestämmande i arbetslivet.

I paragrafen finns en bestämmelse om förhandlingsskyldighet för en arbetsgivare som avser att besluta om kamerabevakning av den egna arbetsplatsen. Förhandlingsskyldigheten har behandlats i avsnitt 13.

Av paragrafen följer att innan en arbetsgivare beslutar om kamerabevakning som avser arbetsplatsen, dvs. den plats där han eller hon bedriver verksamhet, och som inte omfattas av kravet på tillstånd till kamerabevakning ska arbetsgivaren förhandla med berörd arbetstagarorganisation på det sätt som anges i 11–14 §§ lagen (1976:580) om medbestämmande i arbetslivet. Av 5 § andra stycket den lagen framgår att 11 och 12 §§ i lagen ska tillämpas även när kollektivavtal tillfälligt inte gäller.

Skyldigheten att förhandla gäller oavsett om allmänheten har eller saknar tillträde till den plats som kamerabevakningen ska avse förutsatt att bevakningen inte är tillståndsskyldig. På vissa arbetsplatser kan det finnas såväl områden dit allmänheten har tillträde och där kravet på tillstånd till kamerabevakning gäller som områden där förhandlingsskyldigheten gäller för kamerabevakning.

Förhandlingsskyldigheten gäller inte för kamerabevakning som faller utanför lagens tillämpningsområde. Exempelvis gäller den inte vid kamerabevakning som en fysisk person bedriver i sin bostad där någon har anlitats för att utföra visst arbete för den boendes privata räkning.

Mot vem och hur förhandlingsskyldigheten ska fullgöras framgår av 11–14 §§ lagen om medbestämmande i arbetslivet. Frågor om med vem förhandling ska ske m.m. får avgöras på samma sätt som när dessa bestämmelser tillämpas direkt i andra situationer än de som regleras i förvarande paragraf. Också frågan om den som vill bedriva kamerabevakning är att anse som arbetsgivare får avgöras i enlighet med vad som gäller inom arbetsrätten.

Om en arbetsgivare vill låta bli att upplysa om kamerabevakning på arbetsplatsen, ska arbetsgivaren enligt 20 § ansöka hos tillsynsmyndigheten om ett undantag från lagens upplysningskrav. I ett sådant ärende ska enligt samma paragraf ett yttrande avges av ett skyddsombud, en skyddskommitté eller en organisation som företräder arbetstagarna på arbetsplatsen. Yttrandet ska lämnas in tillsammans med ansökningen.

Undantag från förhandlingsskyldigheten

25 § Från förhandlingsskyldigheten för arbetsgivare får avvikelse göras genom kollektivavtal.

Paragrafen innehåller en bestämmelse om undantag från förhandlingsskyldigheten för arbetsgivare. Detta har behandlats i avsnitt 13.

Av paragrafen framgår att avvikelse från förhandlingsskyldigheten får göras genom kollektivavtal. En avvikelse kan göras antingen i ett lokalt avtal eller i ett centralt avtal.

Tystnadsplikt och utlämnande av uppgifter

26 § Den som tar befattning med en uppgift som har inhämtats genom kamerabevakning får inte obehörigen röja eller utnyttja det som han eller hon på detta sätt har fått veta om någon enskilds personliga förhållanden. I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400).

I paragrafen finns en bestämmelse om tystnadsplikt och en upplysning om att bestämmelserna i offentlighets- och sekretesslagen (2009:400) om utlämnande av uppgifter gäller i det allmännas verksamhet. Bestämmelsen har behandlats i avsnitt 14.

Av *första meningen* framgår att den som tar befattning med en uppgift som har inhämtats genom kamerabevakning inte obehörigen får röja eller utnyttja det som han eller hon på detta sätt har fått veta om någon enskilds personliga förhållanden. Bestämmelsen gäller för enskilda som bedriver kamerabevakning och omfattar både uppgifter som inhämtas i realtid och uppgifter som har inhämtats ur inspelat bild- och ljudmaterial. Det är inte bara spridning av själva materialet som omfattas utan även röjande eller utnyttjande av uppgifter ur materialet.

Obehörighetsrekvisitet är avsett att tolkas på så sätt att ett uppgiftslämnande av en enskild aktör som motsvarar ett uppgiftslämnande som är tillåtet enligt offentlighets- och sekretesslagen inte är att betrakta som obehörigt. Den bestämmelse i offentlighets- och sekretesslagen som särskilt tar sikte på uppgifter som har inhämtats genom kamerabevakning, 32 kap. 3 §, har ett omvänt skaderekvisit. Det innebär att sekretess gäller, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider men. I enlighet med detta är det inte fråga om ett obehörigt utlämnande enligt förevarande paragraf, om det står klart att den uppgift det gäller kan lämnas ut utan att den enskilde eller någon närstående till den enskilde lider men. Frågan om en uppgift omfattas av tystnadsplikt beror alltså på vad materialet innehåller. Om den som uppgiften avser samtycker till ett utlämnande, är det inte fråga om ett obehörigt utlämnande.

Exempelvis omfattar bestämmelsen den situationen att bilder från kamerabevakning via en bildskärm i anslutning till kameran visas för förbipasserande. Röjandet bör då inte anses vara obehörigt, eftersom bilderna endast visar det som de förbipasserande även utan

tillgång till dessa kan se från den plats där bildskärmen finns. Sådana kameror och bildskärmar förekommer bl.a. i vissa butiker. Bestämmelsen omfattar också t.ex. tillgängliggörande av bilder via en webbkamera oavsett om tillgängliggörandet sker i realtid eller inte under förutsättning att användningen av kameran faller inom kamerabevakningslagens tillämpningsområde. Huruvida ett sådant tillgängliggörande innebär ett obehörigt utlämnande får avgöras i det enskilda fallet.

Ett utlämnande som är tillåtet enligt den sekretessbrytande bestämmelsen i 32 kap. 3 a § offentlighets- och sekretesslagen är tillåtet också enligt förevarande paragraf. Enskilda som bedriver kamerabevakning får alltså lämna ut inspelat material till en åklagarmyndighet, Polismyndigheten, Tullverket, Kustbevakningen eller Skatteverket, om uppgiften behövs för att utreda ett begånget brott för vilket fängelse är föreskrivet eller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket fängelse är föreskrivet. Ett utlämnande får vidare ske till en kommun eller en myndighet som ansvarar för räddningstjänst enligt lagen (2003:778) om skydd mot olyckor, om uppgiften behövs för att förebygga en hotande olycka eller för att begränsa verkningarna av en redan inträffad olycka.

Den som bryter mot förevarande paragraf kan dömas för brott mot tystnadsplikt enligt 20 kap. 3 § brottsbalken.

Såvitt avser myndigheters möjligheter att lämna ut uppgifter om enskildas personliga förhållanden som inhämtats genom kamerabevakning tillämpas enligt *andra meningen* bestämmelserna i offentlighets- och sekretesslagen.

Tillsyn, sanktionsavgifter och skadestånd

Tillsynsmyndighet

27 § Den myndighet som regeringen bestämmer (tillsynsmyndigheten) utövar tillsyn över kamerabevakning enligt denna lag.

Enligt paragrafen utövar den myndighet som regeringen bestämmer tillsyn över kamerabevakning enligt lagen. Myndigheten kallas tillsynsmyndigheten i lagen. Till skillnad mot vad som gällt enligt kameraövervakningslagen är tillsynen samlad hos en enda myndig-

het. Av föreskrifter följer att Datainspektionen är tillsynsmyndighet. Tillsynen avser både efterlevnaden av bestämmelserna i lagen och beslut som meddelats med stöd av lagen och efterlevnaden av andra bestämmelser som enligt 6 § gäller för kamerabevakning. Övervägandena finns i avsnitt 15.1. Av 6 och 28 §§ följer vilka uppgifter och befogenheter som tillsynsmyndigheten har.

Undersökningsbefogenheter, sanktionsavgifter och skadestånd

28 § I ett ärende enligt denna lag hos tillsynsmyndigheten och vid underlåtenhet att bistå den myndigheten i ett sådant ärende tillämpas bestämmelser om undersökningsbefogenheter för tillsynsmyndigheten och sanktionsavgifter i

1. dataskyddsförordningen, lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som meddelats med stöd av den lagen när det gäller kamerabevakning som omfattas av förordningen eller den lagen, eller

2. brottsdatalagen (2018:000) och föreskrifter som meddelats med stöd av den lagen när det gäller kamerabevakning som omfattas av den lagen.

Bestämmelser i första stycket 1 eller 2 tillämpas på motsvarande sätt i fråga om sanktionsavgifter och skadestånd vid överträdelse av bestämmelserna i denna lag eller av beslut som meddelats med stöd av lagen.

Vid tillämpning av bestämmelser om sanktionsavgifter gäller för myndigheter den högre avgiftsnivå som föreskrivs i lagen med kompletterande bestämmelser till EU:s dataskyddsförordning respektive brottsdatalagen.

Av paragrafen framgår att vissa bestämmelser i antingen dataskyddsförordningen, lagen med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som meddelats med stöd av den lagen eller brottsdatalagen och föreskrifter som meddelats med stöd av den lagen ska tillämpas i vissa situationer som regleras i kamerabevakningslagen. Vilket regelverk som ska tillämpas beror på om kamerabevakningen i det enskilda fallet utgör personuppgiftsbehandling som faller in under den förra eller den senare regleringen. Av 6 § framgår att bestämmelser om tillsynsmyndighetens befogenheter, sanktionsavgifter m.m. i dessa regelverk gäller direkt för kamerabevakning som avses i kamerabevakningslagen i de frågor som inte regleras i lagen.

Enligt *första stycket* tillämpas bestämmelser om tillsynsmyndighetens undersökningsbefogenheter – i dataskyddsförordningen kallade

utredningsbefogenheter och i brottsdatalagen kallade undersökningsbefogenheter – i ärenden enligt kamerabevakningslagen hos tillsynsmyndigheten, t.ex. i ärenden om tillstånd till kamerabevakning och om undantag från kravet på upplysning om kamerabevakning. Vid underlåtenhet att bistå tillsynsmyndigheten i ett sådant ärende tillämpas bestämmelser om sanktionsavgifter.

Av *andra stycket* framgår att bestämmelser om sanktionsavgifter och skadestånd tillämpas vid överträdelse av bestämmelserna i kamerabevakningslagen eller av beslut som meddelats med stöd av lagen. Med beslut avses även villkor i beslutet. Exempelvis kan sanktionsavgift eller skadestånd aktualiseras i fall där tillståndsskyldig kamerabevakning bedrivs utan tillstånd eller i strid med villkoren i ett meddelat tillstånd. Även överträdelse av kravet på upplysning eller av ett beslut om undantag från det kravet kan medföra sanktionsavgift eller skadestånd. Detsamma gäller överträdelse av förhandlingsskyldigheten för arbetsgivare. En överträdelse av den skyldigheten kan samtidigt innebära att bestämmelser i lagen (1976:580) om medbestämmande i arbetslivet överträds i samband med en fråga om sådan förhandlingsskyldighet. Skadestånd enligt den lagen kan då komma i fråga.

Vid tillämpning av bestämmelser om sanktionsavgifter enligt första eller andra stycket gäller för myndigheter enligt *tredje stycket* den högre avgiftsnivå som föreskrivs i lagen med kompletterande bestämmelser till EU:s dataskyddsförordning respektive brottsdatalagen.

Paragrafen har behandlats i avsnitt 15.2.

Överklagande m.m.

Överklagande

29 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol.

Beslut om tillstånd till kamerabevakning och om undantag från kravet på upplysning om kamerabevakning får överklagas även av den kommun där bevakningen ska ske och, om kamerabevakningen ska avse en arbetsplats, av en organisation som företräder arbetstagarna på arbetsplatsen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

I paragrafen finns vissa bestämmelser om överklagande. Av 6 § följer att andra bestämmelser om rättsmedel också gäller vid kamerabevakning som avses i lagen. Övervägandena bakom förevarande paragraf finns i avsnitt 13 och 15.2.

Enligt *första stycket* får tillsynsmyndighetens beslut enligt kamerabevakningslagen överklagas till allmän förvaltningsdomstol. Överklaganderätten gäller bl.a. beslut i frågor om tillstånd till kamerabevakning och undantag från kravet på upplysning om kamerabevakning samt beslut om sanktionsavgift som har fattats med stöd av 28 §.

Enligt *andra stycket* får beslut om tillstånd till kamerabevakning och om undantag från kravet på upplysning om kamerabevakning överklagas även av den kommun där bevakningen ska ske och, om kamerabevakningen ska avse en arbetsplats, av en organisation som företräder arbetstagarna på arbetsplatsen. Överklaganderätten är kopplad till de fall som avses i 12 § tredje stycket, 13 §, 20 § tredje stycket och 21 §.

Enligt *tredje stycket* krävs prövningstillstånd vid överklagande till kammarrätten. Det gäller samtliga beslut som avses i paragrafen.

Föreskrifter

30 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om avgifter för ansökningar enligt denna lag.

I paragrafen bemyndigas regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om avgifter för ansökningar enligt kamerabevakningslagen. Ansökningar enligt lagen handläggs av tillsynsmyndigheten som första instans. Frågan har behandlats i avsnitt 15.3.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 25 maj 2018.
2. Genom lagen upphävs kameraövervakningslagen (2013:460).
3. Tillstånd till kameraövervakning som har beslutats enligt den äldre lagen och som avser kamerabevakning som omfattas av kravet på tillstånd i den nya lagen gäller fortfarande. Övriga tillstånd som har beslutats enligt den äldre lagen gäller inte längre.

4. Undantag från upplysningsplikten som har beslutats enligt den äldre lagen gäller fortfarande.

5. Anmälningar som har gjorts enligt den äldre lagen gäller inte längre.

6. Ärenden som har inletts hos länsstyrelserna enligt den äldre lagen men ännu inte har avgjorts överlämnas till den myndighet som utövar tillsyn över kamerabevakning enligt den nya lagen.

7. Mål som har överklagats till annan förvaltningsrätt än Förvaltningsrätten i Stockholm eller till annan kammarrätt än Kammarrätten i Stockholm enligt den äldre lagen men ännu inte har avgjorts överlämnas till Förvaltningsrätten i Stockholm respektive Kammarrätten i Stockholm. Om ett mål har överklagats av en enskild, är den myndighet som utövar tillsyn över kamerabevakning enligt den nya lagen motpart.

8. Äldre föreskrifter om skadestånd gäller fortfarande för skada som har orsakats före ikraftträdandet.

9. Äldre föreskrifter gäller fortfarande för överträdelser som har skett före ikraftträdandet.

Frågor om ikraftträdande- och övergångsbestämmelser har behandlats i avsnitt 16.

Av *punkterna 1 och 2* följer att den nya lagen, kamerabevakningslagen, träder i kraft den 25 maj 2018 och att den äldre lagen, kameraövervakningslagen, då upphör att gälla. Dataskyddsdirektivet ska vara genomfört i svensk rätt den 6 maj 2018. Under tiden från det datumet fram till att den nya lagen träder i kraft gäller den äldre lagen och brottsdatalagen.

Bestämmelserna i *punkterna 3–7* innebär följande. Ett tillstånd till kameraövervakning som har beslutats med stöd av den äldre lagen gäller även när den nya lagen har trätt i kraft, om tillståndet avser kamerabevakning som omfattas av kravet på tillstånd i den nya lagen. Övriga tillstånd som har beslutats enligt den äldre lagen gäller däremot inte längre. Vidare gäller ett beslut om undantag från upplysningsplikten som har beslutats med stöd av den äldre lagen även efter att den nya lagen har trätt i kraft. Däremot gäller inte längre en anmälan som har gjorts enligt den äldre lagen. Ärenden om tillstånd till kameraövervakning eller om undantag från upplysningsplikten som har inletts hos länsstyrelserna före ikraftträdandet av kamerabevakningslagen men ännu inte har avgjorts vid ikraftträdandet handläggs enligt den nya lagen. Detsamma gäller för då pågående mål hos domstol som avser överklagade beslut som har meddelats med stöd av den äldre lagen. Länsstyrelserna ska

överlämna ärendena till den nya tillsynsmyndigheten Datainspektionen. De domstolar som har pågående mål men som efter ikraftträdandet inte längre ska pröva sådana ska överlämna målen till behörig domstol. I målen ska Datainspektionen inträda som motpart i stället för länsstyrelsen när det är en enskild som har överklagat.

I p*unkten 8* anges att äldre föreskrifter om skadestånd fortfarande gäller för skada som har orsakats före ikraftträdandet. Enligt *punkten 9* gäller också äldre föreskrifter fortfarande för överträdelser som har skett före ikraftträdandet.

18.2 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

32 kap.

Kamerabevakning

Enskilds personliga förhållanden

3 § Sekretess gäller för sådan uppgift om en enskilds personliga förhållanden som har inhämtats genom kamerabevakning som avses i kamerabevakningslagen (2018:000), om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.

Sekretessen enligt första stycket gäller hos en domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

I paragrafen regleras sekretess till skydd för uppgift om enskilds personliga förhållanden som har inhämtats genom kamerabevakning. Ändringen innebär dels att uttrycket kamerabevakning har ersatt uttrycket kameraövervakning, dels att en hänvisning till kameraövervakningslagen har ersatts med en hänvisning till kamerabevakningslagen. Frågan har behandlats i avsnitt 14.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 25 maj 2018.
2. Äldre föreskrifter gäller fortfarande för uppgift som har inhämtats före ikraftträdandet.

Frågor om ikraftträdande- och övergångsbestämmelser har behandlats i avsnitt 16.

Enligt *punkten 1* träder ändringen i kraft den 25 maj 2018. Av *punkten 2* följer att sekretessen enligt den tidigare lydelsen av paragrafen fortfarande gäller för uppgift som har inhämtats före ikraftträdandet.

Särskilda yttranden

Särskilt yttrande av experten juristen Sara Markstedt

Jag ställer mig bakom utredningens bedömning att den nya dataskyddsförordningen, som kommer att gälla direkt i Sverige, innebär att många av kameraövervakningslagens nuvarande bestämmelser inte kan behållas och att en reglering av kamerabevakning inte kan innehålla något generellt krav på tillstånd eller anmälan. Även jag menar alltså att regler om kamerabevakning måste betraktas som en dataskyddsreglering.

Utredningens bedömning och förslag innebär att det generellt sett inte längre kommer att gälla något krav på tillstånd inför en kamerabevakning. När privata aktörer utför kamerabevakning utan att det faller inom ramen för en uppgift av allmänt intresse kommer det i stället att vara den nya gemensamma EU-rätten om skydd för personuppgifter som ska tillämpas till skydd för enskildas integritet. Den regleringen sätter gränser för när och hur kamerabevakning får ske och hur inspelat material får hanteras. Det finns anledning att framhålla att regleringen i både dataskyddsförordningen och det nya direktivet om personuppgiftsbehandling på det brottsbekämpande området innebär ett stärkt integritetsskydd jämfört med nuvarande lagstiftning om skydd för personuppgifter. EU-regleringen innehåller däremot inte några krav på formella tillståndsförfaranden inför kamerabevakning.

I frågan om ett tillståndskrav för myndigheters kamerabevakning, i synnerhet Polisens, gör jag en annan bedömning än utredningen. Det finns enligt mig inte längre några vägande skäl för att i nationell rätt ställa upp tillkommande krav på förhandstillstånd från tillsynsmyndigheten inför polisens kamerabevakning, utöver det stärkta skydd för den personliga integriteten som den nya EU-rätten innebär. Tillit bör i stället sättas till att en rättsvårdande myndighet

som Polisen, lika väl som privata aktörer, på eget ansvar kan tillämpa gällande regler om integritetsskydd och hantera bland annat nödvändighets- och proportionalitetsavvägningar inför en kameraanvändning. För andra typer av personuppgiftsbehandling gäller redan den ordningen att myndigheten själv ansvarar för att följa skyddsregleringen utan några förhandstillstånd. Intern tillsyn och kontroll äger också rum inom Polisen, som utöver internrevisionen nyligen beslutat att inrätta en särskild tillsynsfunktion direkt under myndighetsledningen. Jag menar därför att tillståndskravet kan avskaffas även för polisens kamerabevakning utan att det riskerar att leda till otillbörliga integritetsintrång. Ett fortsatt formellt förfarande med ansökan om tillstånd och ändringsanmälningar så snart behoven av kamerabevakning förändras innebär att polismän behöver ägna sig åt tidsödande administration på ett sätt som enligt min bedömning inte längre vägs upp av integritetshänsyn. I det sammanhanget bör framhållas att den nya dataskyddsregleringen också innebär ökade dokumentationskrav.

På det brottsbekämpande området syftar den nya dataskyddsregleringen inte enbart till att stärka integritetsskyddet utan också till att säkerställa att sådant informationsutbyte mellan behöriga myndigheter som är nödvändigt enligt unionsrätten eller nationell rätt inte begränsas. Det är även ur denna synvinkel angeläget att svensk polis inte ges sämre förutsättningar än polis i övriga europeiska länder att inhämta uppgifter genom användning av kameror och att utbyta sådana uppgifter i syfte att bekämpa brott och upprätthålla allmän ordning och säkerhet. Trots de justeringar i tillståndsbedömningen som utredningen föreslår kommer ett förfarande i Sverige där polisens kamerabevakning som huvudregel kräver förhandstillstånd från den tillsynsmyndighet som är satt att värna integritetsintresset att leda till en inskränkning avseende vilken kameraanvändning som medges. Tillståndsprövningen sträcker sig nämligen utöver en prövning av om en kamerabevakning annars vore laglig eller inte. Jag drar slutsatsen att det måste vara avsikten att begränsa polisens kamerabevakning om ett sådant extra tillståndskrav fortsatt ska gälla och ställer mig frågande till om det finns skäl för detta.

Den föreslagna regleringen är inte heller teknikneutral. Det skapar fortsatt svåra avgränsningsfrågor avseende vilken kameraanvändning som faller in under tillståndskravet, bl.a. vilka kameror som

anses manövrerade på platsen eller inte. Sådana avgränsningsproblem riskerar att hämma önskvärd utveckling på kameraområdet. Inte bara det privata näringslivet utan även polisen behöver emellertid kunna dra nytta av den tekniska utvecklingen i takt med dess framsteg. T.ex. kommer användande av kameraförsedda drönare i flera avseenden att vara till mycket stor nytta i den framtida polisverksamheten.

För att säkerställa ett gott integritetsskydd är det enligt mig, i vart fall när det gäller kameror som används i eller på fordon, fartyg eller luftfartyg eller liknande rörliga objekt, lämpligare med ett förhandssamråd med tillsynsmyndigheten på systemnivå än med ett formellt tillståndskrav. Vid tillfället för en tillståndsprövning avseende den typen av kameror kommer nämligen inte någon given plats eller några reella intressen att vara kända. Beslut om att använda sådana kameror bör i stället förbehållas polis som i varje given situation ansvarar för att regler om integritetsskydd följs men även tar ansvar för vad en kameraanvändning, eller val att avstå från sådan användning, i den givna situationen får för konsekvenser för brottsbekämpningen och förutsättningarna att upprätthålla allmän ordning och säkerhet. Enligt min uppfattning bör därför i vart fall inte andra polisiära kameror än dem som omfattas av det skisserade minimalistiska alternativet i avsnitt 10.2 träffas av ett krav på förhandstillstånd från tillsynsmyndigheten. De potentiella svårigheter som det alternativet innebär är enligt min bedömning av mindre omfattning än de nackdelar som följer av det tillämpningsområde som utredningen föreslår.

Till skillnad från vad som anförs i utredningen bedömer jag inte att det är nödvändigt att dra en skarp gräns i dataskyddsregleringen när det gäller användning av kameror som inte anses manövrerade på platsen (t.ex. kameraförsedda drönare) i situationer där ett konkret brott utreds. Bestämmelser i dataskyddsregleringen bör nämligen som utgångspunkt utgöra tillräckligt lagstöd för det intrång i enskildas integritet i ideell bemärkelse som en sådan kameraanvändning kan medföra, oavsett om förundersökning i en viss situation har hunnit inledas eller inte. Enligt min bedömning torde det endast vara när användningen av kamera därtill skulle medföra ett intrång i t.ex. den kroppsliga integriteten, enskilds hus, rum eller slutet förvaringsställe eller i förtrolig försändelse som en annan typ av lagstöd behövs för åtgärden (jfr 27 och 28 kap. rättegångsbalken). Om

det ändå skulle anses önskvärt med ytterligare reglering av polisens kameraanvändning, bör syftet vara att genom regleringen åstadkomma ett tydligt stöd snarare än en begränsning av den kameraanvändning som vore tillåten även utan tillkommande lagstiftning.

Det polisiära behovet av kamerabevakning kan vidare inte alltid förutses i sådan god tid att en tillståndsansökan hinner upprättas och prövas i förväg. Polisens möjligheter att tillfälligt kamerabevaka med undantag från tillståndskravet föreslås emellertid även framöver vara begränsade. Om en tillståndsplikt alls ska gälla, menar jag att den undantagsbestämmelsen borde omfatta varje kamerabevakning som är nödvändig och annars vore laglig enligt dataskyddsregleringen. Utredningens förslag i denna del hämmar enligt mig i onödan möjligheten för svensk polis att med kort varsel använda kameror när det behövs, där det behövs.

Ett stort antal författningar kommer att reglera polisens personuppgiftsbehandling efter EU:s dataskyddsreform, vilket blir komplext för tillämparen. Enligt min uppfattning bör polisens kamerabevakning inte längre regleras i en särskild lag, eftersom tillståndskravet bör utgå. Anpassade regler om sätt för fullgörande av upplysningskrav gentemot enskilda vid kamerabevakning och undantag från det upplysningskravet, liksom regler om förhandlingsskyldighet för arbetsgivare, skulle i stället efter behov kunna införlivas i den generella svenska lag som kommer att komplettera dataskyddsförordningen (eller annan författning som reglerar personuppgiftsbehandling på förordningens område) respektive i den föreslagna brottsdatalagen (se SOU 2017:29) eller polisdatalagen.

Särskilt yttrande av experten rådmannen Ronny Idstrand

Jag ställer mig bakom utredningens förslag i dess huvudsakliga delar men har följande synpunkter gällande forum för prövning av de ärenden som kan komma att överklagas eller på annat sätt bli föremål för en domstolsprocess.

Enligt nuvarande ordning prövas mål enligt kameraövervakningslagen vid landets samtliga länsstyrelser, vilket i sin tur innebär att överklaganden kan komma att prövas även vid samtliga förvaltningsrätter och kammarrätter. Jag har i och för sig inte någon invändning mot att det sker en specialisering på så sätt att Datainspektionen blir ensam tillsynsmyndighet. Mina invändningar gäller att den framtida prövningen av ärendetypen enbart kommer att ske vid en förvaltningsrätt och en kammarrätt. I grunden avser lagstiftningen att tillgodose behovet av bevakning och övervakning med hjälp av kameror m.m. för berättigade ändamål men samtidigt ska man vid prövningen ta hänsyn till den personliga integriteten. Denna intresseavvägning ställer på så sätt frågor kring skyddet för fysiska personers grundläggande rättigheter och friheter.

Frågor av denna karaktär berör även andra rättsområden och är av fundamentalt intresse för varje domstolsprövning, eftersom de har starka beröringspunkter med grundlagen och liknande författningstexter, såväl i Sverige som inom den Europeiska Unionen och i den Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Det rör sig således om frågor som varje domstol måste förhålla sig till och beakta vid de prövningar som görs. I förlängningen, om andra likartade måltyper också i framtiden endast kan prövas av en eller ett fåtal domstolar, löper det en risk att förminska övriga domstolars kompetens och erfarenhet av likartade frågor. Det kan även leda till att vissa domstolar blir mindre attraktiva än andra, vilket försvårar rekryteringen av domare. Det är därför enligt min mening olyckligt att denna typ av ärenden lyfts bort från merparten av de allmänna förvaltningsdomstolarna.

Mot denna bakgrund hade jag önskat en annan utformning av 29 § kamerabevakningslagen.

Kommittédirektiv 2015:125

Kameraövervakning – brottsbekämpning och integritetsskydd

Beslut vid regeringssammanträde den 26 november 2015

Sammanfattning

En särskild utredare ska utreda vissa frågor om kameraövervakning. Syftet är att säkerställa att kameraövervakning kan användas där det behövs för att bekämpa brott och samtidigt garantera ett starkt skydd för den personliga integriteten.

Utredaren ska bl.a.

- kartlägga och utvärdera vad kameraövervakningslagen (2013:460) har inneburit för möjligheterna till kameraövervakning och skyddet för den personliga integriteten,
- analysera om möjligheterna till kameraövervakning på särskilt brottsutsatta platser och andra platser med förhöjt skyddsbehov, t.ex. asylboenden, medieredaktioner och lokaler som används av religiösa samfund, behöver förbättras,
- undersöka hur lagens tillämpningsområde förhåller sig till användning av ny teknik, såsom t.ex. kamerautrustade drönare, och bl.a. ta ställning till om det behövs integritetsstärkande eller teknikfrämjande åtgärder,
- ta ställning till om integritetsskyddet på vissa platser dit allmänheten inte har tillträde, t.ex. arbetsplatser och skolor, behöver förbättras,

- analysera om integritetsskyddet kan förstärkas genom att Datainspektionen ges föreskriftsrätt när det gäller tillämpningen av kameraövervakningslagen, och
- lämna de författningsförslag som bedöms lämpliga.

Uppdraget ska redovisas senast den 28 februari 2017.

Uppdraget

Kameraövervakningslagen trädde i kraft den 1 juli 2013. Tidigare reglerades kameraövervakning i två lagar: lagen (1998:150) om allmän kameraövervakning och personuppgiftslagen (1998:204). Genom kameraövervakningslagen samlades reglerna om kameraövervakning på ett och samma ställe. Syftet med lagen var att modernisera regleringen av kameraövervakning på ett sätt som skulle säkerställa balansen mellan intresset av att använda kameraövervakning för berättigade ändamål och intresset av att skydda den enskildes integritet (proposition En ny kameraövervakningslag, prop. 2012/13:115).

Vad har kameraövervakningslagen inneburit i praktiken?

Enligt kameraövervakningslagen krävs tillstånd från länsstyrelsen vid övervakning av platser dit allmänheten har tillträde, t.ex. gator och torg. Tillstånd ska ges om övervakningsintresset väger tyngre än integritetsintresset. I dessa avseenden innebar införandet av kameraövervakningslagen inte någon förändring jämfört med vad som gällde tidigare. Lagen innebar dock vissa förändringar när det gäller vilka omständigheter som ska beaktas särskilt vid tillståndsprövningen. En förändring var att behovet av kameraövervakning för att avslöja eller utreda brott numera uttryckligen anges som något som ska beaktas vid bedömningen av övervakningsintresset. Tidigare angavs endast förebyggande av brott. En annan förändring var att användandet av teknik som främjar skyddet av den enskildes personliga integritet ska beaktas särskilt vid bedömningen av integritetsintresset. I förarbetena angavs att denna ändring skulle kunna utöka möjligheterna att meddela tillstånd i vissa situationer (prop. 2012/13:115 s. 49).

Vidare innebar införandet av lagen lättnader för viss kameraövervakning genom att tillståndsplikt ersattes med anmälningsplikt. Detta gäller bl.a. övervakning i parkeringshus och tunnelbanan samt viss övervakning i butiker. Integritetsskyddet förstärktes samtidigt genom införandet av bl.a. starkare sekretesskydd, ökade krav på säkerhetsåtgärder och en skadeståndsbestämmelse som ger enskilda rätt till ersättning för skada och kränkning vid överträdelser av kameraövervakningslagen. Vidare gavs Datainspektionen ett centralt tillsynsansvar i syfte att bl.a. göra länsstyrelsernas praxis mer enhetlig.

Det finns nu anledning att kartlägga tillämpningen av kameraövervakningslagen och bedöma om den fungerar tillfredsställande. Av särskilt intresse i detta sammanhang är vad de förändringar som infördes genom kameraövervakningslagen har inneburit i praktiken. Det är också av intresse att undersöka hur lagens tillämpningsområde förhåller sig till användningen av ny teknik. Ett exempel är användningen av kamerautrustade drönare som har blivit allt vanligare på senare tid. Tekniken används redan i dag och har många potentiella användningsområden inom både offentlig och kommersiell verksamhet. Några exempel är inom skogs- och jordbruk, räddningsarbete och för inspektioner och tillsynsarbete, men också inom tjänsteindustrin. Kamerautrustade drönare kan samtidigt användas på ett sätt som innebär att enskilda skulle kunna utsättas för integritetskränkande övervakning. Det finns i dag viss reglering som kan omfatta fotografering eller spridning av bildmaterial från kamerautrustade drönare, t.ex. förbudet i brottsbalken mot kränkande fotografering och lagen om skydd av landskapsinformation. Rättsläget får i dagsläget dock anses oklart i vilken mån kamerautrustade drönare eller motsvarande annan ny teknik också omfattas av kameraövervakningslagens tillämpningsområde.

Utredaren ska därför

- kartlägga tillämpningen av kameraövervakningslagen,
- analysera vilka konsekvenser lagen har haft för möjligheten att få tillstånd till kameraövervakning,
- bedöma vad de förändringar som infördes genom kameraövervakningslagen har haft för konsekvenser för skyddet av den personliga integriteten,

- utvärdera Datainspektionens centrala tillsynsansvar genom att bl.a. undersöka om länsstyrelsernas rättstillämpning har blivit mer enhetlig,
- undersöka hur lagens tillämpningsområde förhåller sig till användningen av ny teknik, såsom t.ex. kamerautrustade drönare, och ta ställning till om det behöver vidtas åtgärder för att stärka skyddet för den personliga integriteten eller främja ändamålsenlig användning av ny teknik, och
- lämna de författningsförslag som bedöms lämpliga.

Hur kan möjligheten till kameraövervakning på särskilt brottsutsatta platser och andra platser med ett förhöjt skyddsbehov säkerställas?

På särskilt brottsutsatta platser kan kameraövervakning fungera som ett komplement till andra brottsförebyggande åtgärder. Tekniken kan också underlätta avslöjandet av pågående brott och vara av betydelse i efterföljande utredningar. En effektiv brottsbekämpning kan i sin tur bidra till ett tryggare samhälle. Det är därför angeläget att kameraövervakningslagen inte ställer upp för höga krav för Polismyndighetens eller andra relevanta aktörers möjligheter att få tillstånd till övervakning på särskilt brottsutsatta platser. Det är också viktigt att en ändamålsenlig användning av tekniken inte försvåras genom att tillstånd att övervaka förenas med alltför begränsande villkor. En rätt att inte bara övervaka utan också spela in och bevara material innebär generellt sett ett större integritetsintrång men kan också vara en förutsättning för att kunna utreda vissa brott och lägga fram tillräcklig bevisning i domstol.

I dagens samhälle finns också platser och byggnader som, även om de inte är frekvent utsatta för brott, har en generell hotbild riktad mot sig. Det kan exempelvis handla om asylboenden, medieredaktioner och lokaler som används av religiösa samfund. Kameraövervakning kan utgöra en del i skyddet av sådana platser och byggnader. Det behöver därför säkerställas att det inte finns onödiga hinder för en sådan användning av tekniken.

Det finns alltså anledning att utreda om det finns tillräckliga möjligheter till kameraövervakning på särskilt brottsutsatta platser och andra platser med ett förhöjt skyddsbehov. Det är ur integritetssynpunkt samtidigt viktigt att säkerställa att kameraövervakning

inte sker slentrianmässigt. En given utgångspunkt är därför att kameraövervakning endast ska användas om övervakningsintresset väger tyngre än integritetsintresset.

Utredaren ska därför

- bedöma om möjligheterna till kameraövervakning på särskilt brottsutsatta platser behöver förbättras,
- analysera om andra relevanta aktörer än brottsbekämpande myndigheter har ändamålsenliga möjligheter till sådan kameraövervakning,
- bedöma om det finns tillräckliga möjligheter att ta hänsyn till hotbilder av mer generellt slag vid tillståndsprövningen, och
- lämna de författningsförslag som bedöms lämpliga.

Kameraövervakning av bl.a. skogs- och lantbruksmaskiner kan behöva underlättas

Behov av en ändamålsenlig kameraövervakning finns även i andra slags miljöer. Jaktlagsutredningen har i ett delbetänkande (SOU 2014:54) föreslagit att kameraövervakning under vissa förutsättningar ska få ske av s.k. vildsvinsåtlar utan individuell tillståndsprövning. Enligt förslaget ska det i syfte att underlätta en effektiv jakt i stället vara tillräckligt med en anmälan till länsstyrelsen. Betänkandet bereds för närvarande i Regeringskansliet.

I skogs- och lantbruksverksamhet finns det ofta behov av att tillfälligt lämna kvar maskiner, arbetsbodar m.m. ute i skog och mark. Den utrustning som används är ofta mycket stöldbegärlig och stölder sker inte sällan i organiserad form. Det har ifrågasatts om det finns tillräckliga möjligheter att kameraövervaka utrustning av detta slag. En särskild fråga som väckts är i vilken utsträckning det finns förutsättningar enligt kameraövervakningslagen att ge tillstånd till kameraövervakning av utrustning som tillfälligt placeras på platser som är svåra att precisera i förväg. Denna fråga kan också uppkomma vid andra typer av kameraöverövervakning, t.ex. övervakning med kameror som är uppsatta på fordon.

Utredaren ska därför

- ta ställning till om kameraövervakning av maskiner och annan utrustning som används i skogs- och lantbruket behöver underlättas,
- analysera om det finns tillräckliga förutsättningar enligt kameraövervakningslagen att ge tillstånd till övervakning av platser som är svåra att precisera i förväg, och
- lämna de författningsförslag som bedöms lämpliga.

Behöver integritetsskyddet vid kameraövervakning på exempelvis arbetsplatser och skolor förbättras?

Vid kameraövervakning av platser dit allmänheten har tillträde garanteras integritetsskyddet bl.a. genom tillstånds- och anmälningsplikt. När det gäller platser dit allmänheten inte har tillträde gäller dock i dag varken krav på tillstånd eller anmälan. Det är Datainspektionen som utövar tillsyn över sådan kameraövervakning men eftersom det saknas krav på anmälan kan det vara svårt för Datainspektionen att få kännedom om vilken övervakning som bedrivs.

I samband med kameraövervakningslagens tillkomst förespråkade flera remissinstanser att det skulle införas en anmälningsplikt för vissa platser dit allmänheten inte har tillträde (prop. 2012/13:115 s. 82). En sådan anmälningsplikt skulle kunna bidra till en bättre bild av kameraövervakningen i samhället, underlätta Datainspektionens tillsynsarbete samt förstärka integritetsskyddet. Enligt regeringen finns det därför anledning att analysera om anmälningsplikt bör införas för kameraövervakning av exempelvis arbetsplatser och skolors inomhusmiljöer. I analysen bör det ingå en bedömning av om det i så fall finns anledning till undantag från anmälningsplikten i vissa fall. Det bör i detta sammanhang även analyseras vilka fördelar respektive nackdelar det skulle innebära att överlåta till Datainspektionen att föreskriva om vilken typ av platser som ska omfattas av en anmälningsplikt.

Kameraövervakning av platser dit allmänheten inte har tillträde får ske antingen med samtycke från den som ska övervakas eller om det bedöms att övervakningsintresset väger tyngre än integritetsintresset. När det gäller kameraövervakning av anställda kan det

förekomma att ett samtycke visserligen inhämtas men att det inte är givet att detta är giltigt. Det beror på att den anställde ofta befinner sig i ett sådant beroendeförhållande till arbetsgivaren att det kan ifrågasättas om samtycket är frivilligt. Det finns bl.a. med anledning av detta beroendeförhållande skäl att överväga ett förstärkt inflytande för arbetstagarorganisationer i frågor som rör kameraövervakning på arbetsplatser. I kameraövervakningslagen finns redan bestämmelser vars syfte är att särskilt tillvarata arbetstagares integritetsintressen (13 § första stycket 3 och 17 § andra stycket). De aktuella bestämmelserna gäller dock bara för platser dit allmänheten har tillträde. Flera remissinstanser förespråkade att regler som garanterade någon form av inflytande för arbetstagarorganisationer skulle införas också för arbetsplatser dit allmänheten inte har tillträde (prop. 2012/13:115 s. 78–84.). Några sådana regler infördes dock inte. I syfte att garantera ett starkt integritetsskydd för arbetstagare bör frågan nu utredas närmare.

Utredaren ska därför

- analysera om det finns skäl att låta kameraövervakning på vissa platser dit allmänheten inte har tillträde, exempelvis arbetsplatser och skolors inomhusmiljöer, omfattas av anmälningsplikt,
- bedöma om en eventuell reglering av vilka platser som ska omfattas av anmälningsplikt ska tas in i kameraövervakningslagen eller om det bör överlåtas till Datainspektionen att meddela föreskrifter om detta,
- utreda om det finns skäl att förstärka inflytandet för arbetstagarorganisationer i frågor som rör kameraövervakning på arbetsplatser dit allmänheten inte har tillträde, och
- lämna de författningsförslag som bedöms lämpliga.

En föreskriftsrätt för Datainspektionen skulle kunna stärka integritetsskyddet

Av förarbetena till kameraövervakningslagen framgår att flera remissinstanser föreslog en föreskriftsrätt för Datainspektionen när det gäller tillämpningen av lagen (prop. 2012:13/115 s. 132). Någon sådan modell infördes dock inte. En föreskriftsrätt för Datainspektionen skulle kunna leda till en mer enhetlig tillämpning av lagen

och vara till värdefull hjälp för myndigheter och enskilda som i dag måste göra relativt svåra egna bedömningar för att följa lagstiftningen. Detta skulle i sin tur kunna leda till ett förstärkt integritetsskydd. Regeringen anser därför att frågan bör analyseras närmare.

Utredaren ska därför

- analysera om Datainspektionen bör ges en föreskriftsrätt när det gäller tillämpningen av kameraövervakningslagen, och
- lämna de författningsförslag som bedöms lämpliga.

Övriga frågor

Utredaren är oförhindrad att ta upp och lämna författningsförslag i frågor som har samband med de frågeställningar som ska utredas särskilt.

Reformen av EU:s dataskyddsreglering och annat pågående EU-arbete

Den 25 januari 2012 lade kommissionen fram förslag till en genomgripande reform av EU:s dataskyddsreglering. Förslaget består dels av en allmän dataskyddsförordning (KOM2012 11) som ska ersätta det s.k. dataskyddsdirektivet (95/46/EG), dels av ett särskilt dataskyddsdirektiv för de brottsbekämpande myndigheterna (KOM2012 10) som ska ersätta det s.k. dataskyddsrambeslutet (2008/977/RIF). Förhandlingar pågår fortfarande på EU-nivå men när reformen är avslutad kommer det att finnas ett behov av en översyn av kameraövervakningslagen. En sådan översyn förutsågs redan i förarbetena till lagen (prop. 2012/13:115 s. 142). När förhandlingarna är avslutade kommer regeringen därför att ge utredaren tilläggsdirektiv om frågor som rör anpassningen till den nya EU-rättsliga dataskyddsregleringen.

EU-kommissionen har också påbörjat ett arbete med att ta fram ett EU-gemensamt regelverk för drönare. I den s.k. Rigadeklarationen framhålls att europeiska och nationella dataskyddsmyndigheter ska ta fram riktlinjer och övervakningsmekanismer om befintligt dataskyddsregelverk i relation till drönare. Utredaren bör bevaka och beakta detta arbete.

Konsekvensbeskrivningar

Utredaren ska redovisa de ekonomiska konsekvenserna av de förslag som läggs fram. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. Utredaren ska också redovisa förslagens konsekvenser för den personliga integriteten samt förslagens betydelse för brottsligheten och det brottsförebyggande arbetet.

Samråd och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete som bedrivs inom Regeringskansliet, utredningsväsendet och inom EU. Under genomförandet av uppdraget ska utredaren ha en dialog med och inhämta upplysningar från de myndigheter och andra organisationer som kan vara berörda av aktuella frågor.

Uppdraget ska redovisas senast den 28 februari 2017.

(Justitiedepartementet)

Kommittédirektiv 2016:54

Tilläggsdirektiv till Utredningen om kameraövervakning – brottsbekämpning och integritetsskydd (Ju 2015:14)

Beslut vid regeringssammanträde den 16 juni 2016.

Utvidgning av och förlängd tid för uppdraget

Regeringen beslutade den 26 november 2015 att ge en särskild utredare i uppdrag att utreda vissa frågor om kameraövervakning (dir. 2015:125).

Uppdraget utvidgas så att utredaren även ska analysera hur regleringen i kameraövervakningslagen (2013:460) bör anpassas till den nya EU-rättsliga dataskyddsregleringen samt lämna de författningsförslag med anledning av detta som behövs och är lämpliga.

Enligt utredningens direktiv skulle uppdraget redovisas senast den 28 februari 2017. Utredningstiden förlängs. Uppdraget ska i stället redovisas senast den 15 juni 2017.

Den nya EU-rättsliga dataskyddsregleringen

Om kameraövervakning sker på ett sätt som innebär att personer direkt eller indirekt kan identifieras, innebär det en behandling av personuppgifter. Personuppgiftsbehandling som sker helt eller delvis på automatisk väg eller med uppgifter som ska ingå i ett register omfattas av den EU-rättsliga dataskyddsregleringens tillämpningsområde. En svensk reglering av kameraövervakning måste därför vara förenlig med denna EU-reglering.

Den allmänna regleringen om behandling av personuppgifter inom EU finns i dag i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om behandling av det fria flödet av sådana uppgifter (dataskyddsdirektivet). Dataskyddsdirektivet har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen (1998:204). Tidigare reglerades också viss kameraövervakning i personuppgiftslagen men genom införandet av kameraövervakningslagen samlades reglerna om kameraövervakning på ett och samma ställe.

Den 27 april 2016 antog Europaparlamentet och rådet förordningen (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), nedan dataskyddsförordningen. Förordningen utgör en ny generell reglering för personuppgiftsbehandling inom EU och kommer att ersätta det nuvarande dataskyddsdirektivet. Förordningen ska börja tillämpas två år räknat från den tjugonde dagen efter publicering i Europeiska unionens officiella tidning. Det huvudsakliga syftet med förordningen är att ytterligare harmonisera och effektivisera skyddet för personuppgifter för att förbättra den inre marknadens funktion och öka enskildas kontroll över sina personuppgifter.

Från dataskyddsförordningens tillämpningsområde undantas behandling av personuppgifter som a) utgör ett led i en verksamhet som inte omfattas av unionsrätten, b) medlemsstaterna utför när de bedriver verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken, c) en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll, eller d) behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

Samtidigt med dataskyddsförordningen antog Europaparlamentet och rådet direktivet om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, nedan ”det

nya dataskyddsdirektivet". Direktivet innehåller särregler för sådan personuppgiftsbehandling som behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Direktivet ska ha genomförts i svensk rätt senast två år efter dess ikraftträdande.

Regeringen har tillsatt en utredning som ska föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som dataskyddsförordningen ger anledning till (Ju 2016:04, dir. 2016:15). Regeringen har också tillsatt en utredning som ska föreslå hur det nya dataskyddsdirektivet ska genomföras i svensk rätt (Ju 2016:06, dir. 2016:21).

Utredarens nuvarande uppdrag

Utredaren ska enligt sina nuvarande direktiv utreda vissa frågor om kameraövervakning. Det övergripande syftet är att säkerställa att kameraövervakning kan användas där det behövs för att bekämpa brott och samtidigt garantera ett starkt skydd för den personliga integriteten. Utredaren ska mot denna bakgrund bl.a. analysera om möjligheterna till kameraövervakning på särskilt brottsutsatta platser och andra platser med förhöjt skyddsbehov behöver förbättras. Utredaren ska också undersöka hur lagens tillämpningsområde förhåller sig till användningen av ny teknik, ta ställning till om integritetsskyddet på vissa platser dit allmänheten inte har tillträde behöver förbättras samt analysera om Datainspektionen ska ges föreskriftsrätt när det gäller tillämpningen av kameraövervakningslagen.

Av de nuvarande direktiven framgår också att utredaren kommer att ges tilläggsdirektiv om frågor som rör anpassningen till den nya EU-rättsliga dataskyddsregleringen.

Utvidgningen av uppdraget

Enligt artikel 288 i fördraget om Europeiska unionens funktionssätt ska en EU-förordning ha allmän giltighet och vara till alla delar bindande och direkt tillämplig i varje medlemsstat. Till skillnad från EU-direktiv ska förordningar inte genomföras i nationell rätt. Inom dataskyddsförordningens tillämpningsområde är utrymmet för natio-

nell särreglering av personuppgiftsbehandling således generellt sett begränsat.

Det finns dock flera bestämmelser i förordningen som ger medlemsstaterna rätt att införa eller behålla nationell reglering. Av artikel 6.2 framgår exempelvis att medlemsstaterna får behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen för sådan personuppgiftsbehandling som är nödvändig för att fullgöra en rättslig förpliktelse eller utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Medlemsstaterna får i fråga om sådan behandling närmare fastställa specifika krav och andra åtgärder för att säkerställa en laglig och rättvis behandling av uppgifterna. Enligt artikel 6.3 i förordningen ska i dessa fall grunden för behandlingen fastställas i enlighet med unionsrätten eller nationell rätt. Det kan i sammanhanget också framhållas att medlemsstaterna enligt artikel 88 i dataskyddsförordningen har möjlighet att i lag eller i kollektivavtal fastställa mer specifika regler för att säkerställa skyddet av rättigheter och friheter vid behandling av anställdas personuppgifter i anställningsförhållanden, särskilt när det t.ex. gäller säkerhet på arbetsplatsen eller skydd av arbetsgivarens eller kundens egendom.

Det nya dataskyddsdirektivet kräver ett nationellt genomförande vilket betyder att Sverige inom direktivets tillämpningsområde måste behålla eller införa bestämmelser om personuppgiftsbehandling som lever upp till direktivets krav. Enligt artikel 1.3 ska direktivet dessutom inte hindra medlemsstaterna från att föreskriva starkare skyddsåtgärder än de som fastställs i direktivet för skyddet av den registrerades rättigheter och friheter med avseende på behöriga myndigheters behandling av personuppgifter.

Mot denna bakgrund behöver det analyseras hur den nya EU-rättsliga dataskyddsregleringen påverkar utrymmet att i nationell rätt reglera personuppgiftsbehandling vid kameraövervakning. Med utgångspunkt i en sådan analys behöver det sedan utredas hur regleringen i kameraövervakningslagen bör anpassas till dataskyddsförordningen och det nya dataskyddsdirektivet. En fråga som därmed behöver belysas är hur kameraövervakningslagens krav på tillstånd respektive anmälan för viss kameraövervakning förhåller sig till dataskyddsregleringen. Det bör även ingå i uppdraget att analysera om regleringen i 32 kap. 3 och 3 a §§ offentlighets- och sekre-

tesslagen (2009:400) om sekretess för uppgifter som har inhämtats genom kameraövervakning behöver ses över med anledning av dataskyddsreformen.

En fråga som också behöver analyseras särskilt är hur den nya EU-rättsliga dataskyddsregleringens bestämmelser om tillsynsmyndigheter förhåller sig till organisationen av tillsynen över kameraövervakning i Sverige. Enligt kameraövervakningslagen ansvarar i dag länsstyrelserna för den operativa tillsynen över kameraövervakning av platser dit allmänheten har tillträde, medan Datainspektionen har ett motsvarande ansvar för platser dit allmänheten inte har tillträde. Därutöver har Datainspektionen ett centralt tillsynsansvar för all kameraövervakning och en rätt att överklaga länsstyrelsernas beslut för att tillvarata allmänhetens intressen. Både dataskyddsförordningen och det nya dataskyddsdirektivet innehåller detaljerade regler om tillsynsmyndigheternas roll, organisation och uppgifter. Det ställs bl.a. krav på hur tillsynsmyndighetens ledamöter ska utses samt vilka kvalifikationer, erfarenheter och komptens de ska ha. Vidare föreskrivs att de nationella tillsynsmyndigheterna på olika sätt ska samarbeta med och assistera andra medlemsstaters tillsynsmyndigheter. Vid genomförandet av uppdraget i denna del bör utredaren ta hänsyn till de förslag som lämnas av Utredningen om tillsynen över den personliga integriteten (Ju 2015:02) som ska redovisa sitt uppdrag senast den 30 september 2016.

Det är viktigt att regler om kameraövervakning är tydliga, förutsebara och enkla att tillämpa samtidigt som de skyddar enskilda från otillbörliga intrång i den personliga integriteten. Utgångspunkten bör därför vara att kameraövervakning i Sverige även fortsättningsvis ska regleras särskilt i den utsträckning som det bedöms vara förenligt med EU-rätten. Utredaren bör också eftersträva att huvuddragen i den nuvarande regleringen av kameraövervakning behålls, samtidigt som det är angeläget att de förbättringsbehov som uppmärksammas inom ramen för det ursprungliga uppdraget tillgodoses. Utredaren ska vidare under arbetet analysera hur en anpassning av kameraövervakningslagen förhåller sig till de förslag om kameraövervakning av vildsvinsåtlar som lämnats i Jaktlagsutredningens betänkande Vildsvin och viltskador (SOU 2014:54) samt i promemorian Kameraövervakning av vildsvinsåtlar (N2015/06665/RS).

Utredaren ska därför

- analysera hur regleringen i kameraövervakningslagen bör anpassas till den nya EU-rättsliga dataskyddsregleringen,
- analysera om regleringen om sekretess för uppgifter som har inhämtats genom kameraövervakning samt tillsynsansvaret på kameraövervakningsområdet behöver anpassas med anledning av den nya EU-rättsliga dataskyddsregleringen, och
- lämna de författningsförslag som behövs och är lämpliga.

Uppdragets genomförande och redovisning

Det som sägs om uppdragets genomförande och konsekvensbeskrivning i ursprungsdirektiven gäller också det utvidgade uppdraget. Här ingår bl.a. att redovisa de ekonomiska konsekvenserna av förslag som innebär förändringar av den nuvarande tillstånds- eller tillsynsverksamheten. Vid anpassningen av svensk rätt till den nya EU-regleringen bör en enhetlig tolkning av regelverket eftersträvas. Utredaren ska därför följa och i lämplig omfattning samråda med Dataskyddsutredningen (Ju 2016:04), Utredningen om genomförande av EU:s direktiv om skydd av personuppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet (Ju 2016:06) samt Utredningen om tillsynen över den personliga integriteten (Ju 2015:02).

Utredningstiden förlängs. Uppdraget ska redovisas senast den 15 juni 2017.

(Justitiedepartementet)

4.5.2016 SV Europeiska unionens officiella tidning L 119/1

I

(Lagstiftningsakter)

FÖRORDNINGAR

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679

av den 27 april 2016

om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ( ),

med beaktande av Regionkommitténs yttrande ( ),

i enlighet med det ordinarie lagstiftningsförfarandet ( ), och

av följande skäl:

(1) Skyddet för fysiska personer vid behandling av personuppgifter är en grundläggande rättighet. Artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) och artikel 16.1 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) föreskriver att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

(2) Principerna och reglerna för skyddet för fysiska personer vid behandling av deras personuppgifter bör, oavsett deras medborgarskap eller hemvist, respektera deras grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Avsikten med denna förordning är att bidra till att skapa ett område med frihet, säkerhet och rättvisa och en ekonomisk union, till ekonomiska och sociala framsteg, till förstärkning och konvergens av ekonomierna inom den inre marknaden samt till fysiska personers välbefinnande.

(3) Europaparlamentets och rådets direktiv 95/46/EG ( ) syftar till att harmonisera skyddet av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter och att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna.

( ) EUT C 229, 31.7.2012, s. 90.
( ) EUT C 391, 18.12.2012, s. 127.
( ) Europaparlamentets ståndpunkt av den 12 mars 2014 (ännu ej offentliggjord i EUT) och rådets ståndpunkt vid första behandlingen av den 8 april 2016 (ännu ej offentliggjord i EUT). Europaparlamentets ståndpunkt av den 14 april 2016.
( ) Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).

(4) Behandlingen av personuppgifter bör utformas så att den tjänar människor. Rätten till skydd av personuppgifter är inte en absolut rättighet; den måste förstås utifrån sin uppgift i samhället och vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen. Denna förordning respekterar alla grundläggande rättigheter och iakttar de friheter och principer som erkänns i stadgan, såsom de fastställts i fördragen, särskilt skydd för privat- och familjeliv, bostad och kommunikationer, skydd av personuppgifter, tankefrihet, samvetsfrihet och religionsfrihet, yttrande- och informationsfrihet, näringsfrihet, rätten till ett effektivt rättsmedel och en opartisk domstol samt kulturell, religiös och språklig mångfald.

(5) Den ekonomiska och sociala integration som uppstått tack vare den inre marknaden har lett till en betydande ökning av de gränsöverskridande flödena av personuppgifter. Utbytet av personuppgifter mellan offentliga och privata aktörer, inbegripet fysiska personer, sammanslutningar och företag, över hela unionen har ökat. Nationella myndigheter i medlemsstaterna uppmanas i unionsrätten att samarbeta och utbyta personuppgifter för att vara i stånd att fullgöra sina uppdrag eller utföra arbetsuppgifter för en myndighet som finns i en annan medlemsstat.

(6) Den snabba tekniska utvecklingen och globaliseringen har skapat nya utmaningar vad gäller skyddet av personuppgifter. Omfattningen av insamling och delning av personuppgifter har ökat avsevärt. Tekniken gör det möjligt för både privata företag och offentliga myndigheter att i sitt arbete använda sig av personuppgifter i en helt ny omfattning. Allt fler fysiska personer gör sina personliga uppgifter allmänt tillgängliga, världen över. Tekniken har omvandlat både ekonomin och det sociala livet, och bör ytterligare underlätta det fria flödet av personuppgifter inom unionen samt överföringar till tredjeländer och internationella organisationer, samtidigt som en hög skyddsnivå säkerställs för personuppgifter.

(7) Dessa förändringar kräver en stark och mer sammanhängande ram för dataskyddet inom unionen, uppbackad av kraftfullt tillsynsarbete, eftersom det är viktigt att skapa den tillit som behövs för att utveckla den digitala ekonomin över hela den inre marknaden. Fysiska personer bör ha kontroll över sina egna personuppgifter. Den rättsliga säkerheten och smidigheten för fysiska personer, ekonomiska operatörer och myndigheter bör stärkas.

(8) Om denna förordning föreskriver förtydliganden eller begränsningar av dess bestämmelser genom medlemsstaternas nationella rätt, kan medlemsstaterna, i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga för de personer som de tillämpas på, införliva delar av denna förordning i nationell rätt.

(9) Målen och principerna för direktiv 95/46/EG är fortfarande giltiga, men det har inte kunnat förhindra bristande enhetlighet i genomförandet av dataskyddet i olika delar av unionen, rättsosäkerhet eller allmänt spridda uppfattningar om att betydande risker kvarstår för fysiska personer, särskilt med avseende på användning av internet. Skillnader i nivån på skyddet av fysiska personers rättigheter och friheter, särskilt rätten till skydd av personuppgifter, vid behandling av personuppgifter i olika medlemsstater kan förhindra det fria flödet av personuppgifter över hela unionen. Dessa skillnader kan därför utgöra ett hinder för att bedriva ekonomisk verksamhet på unionsnivå, de kan snedvrida konkurrensen och hindra myndigheterna att fullgöra sina skyldigheter enligt unionsrätten. De varierande skyddsnivåerna beror på skillnader i genomförandet och tillämpningen av direktiv 95/46/EG.

(10) För att säkra en enhetlig och hög skyddsnivå för fysiska personer och för att undanröja hindren för flödena av personuppgifter inom unionen bör nivån på skyddet av fysiska personers rättigheter och friheter vid behandling av personuppgifter vara likvärdig i alla medlemsstater. En konsekvent och enhetlig tillämpning av bestämmelserna om skydd av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter bör säkerställas i hela unionen. Vad gäller behandlingen av personuppgifter för att fullgöra en rättslig förpliktelse, för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som utförs av den personuppgiftsansvarige, bör medlemsstaterna tillåtas att behålla eller införa nationella bestämmelser för att närmare fastställa hur bestämmelserna i denna förordning ska tillämpas. Jämte den allmänna och övergripande lagstiftning om dataskydd varigenom direktiv 95/46/EG genomförs har medlemsstaterna flera sektorsspecifika lagar på områden som kräver mer specifika bestämmelser. Denna förordning ger dessutom medlemsstaterna handlingsutrymme att specificera sina bestämmelser, även för behandlingen av särskilda kategorier av personuppgifter (nedan kallade *känsliga uppgifter*). Denna förordning utesluter inte att det i medlemsstaternas nationella rätt fastställs närmare omständigheter för specifika situationer där uppgifter behandlas, inbegripet mer exakta villkor för laglig behandling av personuppgifter.

(11) Ett effektivt skydd av personuppgifter över hela unionen förutsätter att de registrerades rättigheter förstärks och specificeras och att de personuppgiftsansvarigas och personuppgiftsbiträdenas skyldigheter vid behandling av personuppgifter klargörs, samt att det finns likvärdiga befogenheter för övervakning och att det säkerställs att reglerna för skyddet av personuppgifter efterlevs och att sanktionerna för överträdelser är likvärdiga i medlemsstaterna.

(12) I artikel 16.2 i EUF-fördraget bemyndigas Europaparlamentet och rådet att fastställa bestämmelser om skydd för fysiska personer när det gäller behandling av personuppgifter och bestämmelser om den fria rörligheten för personuppgifter.

(13) För att säkerställa en enhetlig nivå för skyddet av fysiska personer över hela unionen och undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden behövs en förordning som skapar rättslig säkerhet och öppenhet för ekonomiska aktörer, däribland mikroföretag samt små och medelstora företag, och som ger fysiska personer i alla medlemsstater samma rättsligt verkställbara rättigheter och skyldigheter samt ålägger personuppgiftsansvariga och personuppgiftsbiträden samma ansvar, så att övervakningen av behandling av personuppgifter blir enhetlig, sanktionerna i alla medlemsstater likvärdiga och samarbetet mellan tillsynsmyndigheterna i olika medlemsstater effektivt. För att den inre marknaden ska fungera väl krävs att det fria flödet av personuppgifter inom unionen inte begränsas eller förbjuds av skäl som har anknytning till skydd för fysiska personer med avseende på behandling av personuppgifter. För att ta hänsyn till mikroföretagens samt de små och medelstora företagens särskilda situation innehåller denna förordning ett undantag för organisationer som sysselsätter färre än 250 personer med avseende på registerföring. Dessutom uppmanas unionens institutioner och organ samt medlemsstaterna och deras tillsynsmyndigheter att vid tillämpningen av denna förordning ta hänsyn till mikroföretagens samt de små och medelstora företagens särskilda behov. Begreppen mikroföretag samt små och medelstora företag bör bygga på artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG ( ).

(14) Det skydd som ska tillhandahållas enligt denna förordning bör tillämpas på fysiska personer, oavsett medborgarskap eller hemvist, med avseende på behandling av deras personuppgifter. Denna förordning omfattar inte behandling av personuppgifter rörande juridiska personer, särskilt företag som bildats som juridiska personer, exempelvis uppgifter om namn på och typ av juridisk person samt kontaktuppgifter.

(15) För att förhindra att det uppstår en allvarlig risk för att reglerna kringgås bör skyddet för fysiska personer vara teknikneutralt och inte vara beroende av den teknik som används. Skyddet för fysiska personer bör vara tillämpligt på både automatiserad och manuell behandling av personuppgifter, om personuppgifterna ingår i eller är avsedda att ingå i ett register. Akter eller grupper av akter samt omslag till dessa, som inte är ordnade enligt särskilda kriterier, bör inte omfattas av denna förordning.

(16) Denna förordning är inte tillämplig på frågor som rör skyddet av grundläggande rättigheter och friheter eller det fria flödet av personuppgifter på områden som inte omfattas av unionsrätten, såsom verksamhet rörande nationell säkerhet. Denna förordning är inte tillämplig på medlemsstaternas behandling av personuppgifter när de agerar inom ramen för unionens gemensamma utrikes- och säkerhetspolitik.

(17) Europaparlamentets och rådets förordning (EG) nr 45/2001 ( ) är tillämplig på den behandling av personuppgifter som sker i unionens institutioner, organ och byråer. Förordning (EG) nr 45/2001 och de av unionens övriga rättsakter som är tillämpliga på sådan behandling av personuppgifter bör anpassas till principerna och bestämmelserna i den här förordningen och tillämpas mot bakgrund av den här förordningen. För att tillhandahålla en stark och sammanhängande ram för dataskyddet inom unionen bör nödvändiga anpassningar av förordning (EG) nr 45/2001 göras när den här förordningen har antagits, så att de båda förordningarna kan tillämpas samtidigt.

(18) Denna förordning är inte tillämplig på fysiska personers behandling av personuppgifter som ett led i verksamhet som är helt och hållet privat eller har samband med personens hushåll och därmed saknar koppling till yrkes- eller affärsmässig verksamhet. Privat verksamhet eller verksamhet som har samband med hushållet kan omfatta

( ) Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (K(2003) 1422) (EUT L 124, 20.5.2003, s. 36).

( ) Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

korrespondens och innehav av adresser, aktivitet i sociala nätverk och internetverksamhet i samband med sådan verksamhet. Denna förordning är dock tillämplig på personuppgiftsansvariga eller personuppgiftsbiträden som tillhandahåller utrustning för behandling av personuppgifter för sådan privat verksamhet eller hushållsverksamhet.

(19) Skyddet för fysiska personer när det gäller behöriga myndigheters behandling av personuppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten och det fria flödet av sådana uppgifter, säkerställs på unionsnivå av en särskild unionsrättsakt. Därför bör denna förordning inte vara tillämplig på behandling av personuppgifter för dessa ändamål. Personuppgifter som myndigheter behandlar enligt denna förordning och som används för de ändamålen bör emellertid regleras genom en mer specifik unionsrättsakt, nämligen Europaparlamentets och rådets direktiv (EU) 2016/680 ( ). Medlemsstaterna får anförtro behöriga myndigheter i den mening som avses i direktiv (EU) 2016/680 uppgifter som inte nödvändigtvis utförs för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, så att behandlingen av personuppgifter för dessa andra ändamål, i den mån den omfattas av unionsrätten, omfattas av tillämpningsområdet för denna förordning.

Vad gäller dessa behöriga myndigheters behandling av personuppgifter för ändamål som omfattas av tillämpningsområdet för denna förordning, bör medlemsstaterna kunna bibehålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning. I sådana bestämmelser får det fastställas mer specifika krav för dessa behöriga myndigheters behandling av personuppgifter för dessa andra ändamål, med beaktande av respektive medlemsstats konstitutionella, organisatoriska och administrativa struktur. När privata organs behandling av personuppgifter omfattas av tillämpningsområdet för denna förordning, bör denna förordning ge medlemsstaterna möjlighet att, under särskilda villkor, i lag begränsa vissa skyldigheter och rättigheter, om en sådan begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda särskilda viktiga intressen, däribland allmän säkerhet samt förebyggande, förhindrande, utredning, avslöjande och lagföring av brott eller verkställande av straffrättsliga påföljder eller skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten. Detta är exempelvis relevant i samband med bekämpning av penningtvätt eller verksamhet vid kriminaltekniska laboratorier.

(20) Eftersom denna förordning bland annat gäller för verksamhet inom domstolar och andra rättsliga myndigheter, skulle det i unionsrätt eller medlemsstaternas nationella rätt kunna anges vilken behandling och vilka förfaranden för behandling som berörs när det gäller domstolars och andra rättsliga myndigheters behandling av personuppgifter. Tillsynsmyndigheternas behörighet bör inte omfatta domstolars behandling av personuppgifter när detta sker inom ramen för domstolarnas dömande verksamhet, i syfte att säkerställa domstolsväsendets oberoende när det utför sin rättsskipande verksamhet, inbegripet när det fattar beslut. Det bör vara möjligt att anförtro tillsynen över sådan behandling av uppgifter till särskilda organ inom medlemsstaternas rättsväsen, vilka framför allt bör säkerställa efterlevnaden av bestämmelserna i denna förordning, främja domstolsväsendets medvetenhet om sina skyldigheter enligt denna förordning och hantera klagomål relaterade till sådan behandling av uppgifter.

(21) Denna förordning påverkar inte tillämpningen av Europaparlamentets och rådets direktiv 2000/31/EG ( ), särskilt bestämmelserna om tjänstelevererande mellanhänders ansvar i artiklarna 12–15 i det direktivet. Syftet med det direktivet är att bidra till att den inre marknaden fungerar väl genom att säkerställa fri rörlighet för informationssamhällets tjänster mellan medlemsstaterna.

(22) All behandling av personuppgifter som sker inom ramen för arbetet på personuppgiftsansvarigas eller personuppgiftsbiträdens verksamhetsställen inom unionen bör ske i överensstämmelse med denna förordning, oavsett om behandlingen i sig äger rum inom unionen. Verksamhetsställe innebär det faktiska och reella utförandet av verksamhet med hjälp av en stabil struktur. Den rättsliga formen för en sådan struktur, oavsett om det är en filial eller ett dotterföretag med status som juridisk person, bör inte vara den avgörande faktorn i detta avseende.

( ) Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (se sidan 89 i detta nummer av EUT).

( ) Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden ("Direktiv om elektronisk handel") (EGT L 178, 17.7.2000, s. 1).

(23) För att fysiska personer inte ska fråntas det skydd som denna förordning ger dem bör sådan behandling av personuppgifter om registrerade personer som befinner sig i unionen vilken utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad inom unionen omfattas av denna förordning, om behandlingen avser utbjudande av varor eller tjänster inom unionen till de registrerade, oavsett om detta är kopplat till en betalning. I syfte att avgöra om en personuppgiftsansvarig eller ett personuppgiftsbiträde erbjuder varor eller tjänster till registrerade som befinner sig i unionen bör man fastställa om det är uppenbart att den personuppgiftsansvarige eller personuppgiftsbiträdet avser att erbjuda tjänster till registrerade i en eller flera av unionens medlemsstater. Medan enbart åtkomlighet till den personuppgiftsansvariges, personuppgiftsbiträdets eller en mellanhands webbplats i unionen, till en e-postadress eller andra kontaktuppgifter eller användning av ett språk som allmänt används i det tredjeland där den personuppgiftsansvarige är etablerad inte är tillräckligt för att fastställa en sådan avsikt, kan faktorer som användning av ett språk eller en valuta som allmänt används i en eller flera medlemsstater med möjlighet att beställa varor och tjänster på detta andra språk, eller omnämnande av kunder eller användare som befinner sig i unionen, göra det uppenbart att den personuppgiftsansvarige avser att erbjuda varor eller tjänster till registrerade inom unionen.

(24) Den behandling av personuppgifter som avser registrerade som befinner sig i unionen som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen bör också omfattas av denna förordning, om den hör samman med övervakningen av de registrerade personernas beteende när de befinner sig i unionen. För att avgöra huruvida en viss behandling kan anses övervaka beteendet hos registrerade, bör det fastställas om fysiska personer spåras på internet, och om personuppgifterna därefter behandlas med hjälp av teknik som profilerar fysiska personer, i synnerhet för att fatta beslut rörande honom eller henne eller för att analysera eller förutsäga hans eller hennes personliga preferenser, beteende och attityder.

(25) Om medlemsstaternas nationella rätt är tillämplig i kraft av folkrätten, bör denna förordning också vara tillämplig på personuppgiftsansvariga som inte är etablerade inom unionen, exempelvis i en medlemsstats diplomatiska beskickning eller konsulat.

(26) Principerna för dataskyddet bör gälla all information som rör en identifierad eller identifierbar fysisk person. Personuppgifter som har pseudonymiserats och som skulle kunna tillskrivas en fysisk person genom att kompletterande uppgifter används bör anses som uppgifter om en identifierbar fysisk person. För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel, som t.ex. utgallring, som, antingen av den personuppgiftsansvarige eller av en annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen. Principerna för dataskyddet bör därför inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar. Denna förordning berör därför inte behandling av sådan anonym information, vilket inbegriper information för statistiska ändamål eller forskningsändamål.

(27) Denna förordning gäller inte behandling av personuppgifter rörande avlidna personer. Medlemsstaterna får fastställa bestämmelser för behandlingen av personuppgifter rörande avlidna personer.

(28) Tillämpningen av pseudonymisering av personuppgifter kan minska riskerna för de registrerade som berörs och hjälpa personuppgiftsansvariga och personuppgiftsbiträden att fullgöra sina skyldigheter i fråga om dataskydd. Ett uttryckligt införande av *pseudonymisering* i denna förordning är inte avsett att utesluta andra åtgärder för dataskydd.

(29) För att skapa incitament för tillämpning av pseudonymisering vid behandling av personuppgifter bör åtgärder för pseudonymisering som samtidigt medger en allmän analys vara möjliga inom samma personuppgiftsansvarigs verksamhet, när den personuppgiftsansvarige har vidtagit de tekniska och organisatoriska åtgärder som är nödvändiga för att se till att denna förordning genomförs för berörd uppgiftsbehandling och att kompletterande uppgifter för tillskrivning av personuppgifterna till en specifik registrerad person förvaras separat. Den personuppgiftsansvarige som behandlar personuppgifterna bör ange behöriga personer inom samma personuppgiftsansvarigs verksamhet.

(30) Fysiska personer kan knytas till nätidentifierare som lämnas av deras utrustning, applikationer, verktyg och protokoll, t.ex. ip-adresser, kakor eller andra identifierare, som radiofrekvensetiketter. Detta kan efterlämna spår som, särskilt i kombination med unika identifierare och andra uppgifter som tas emot av servrarna, kan användas för att skapa profiler för fysiska personer och identifiera dem.

(31) Offentliga myndigheter som för sin myndighetsutövning mottar personuppgifter i enlighet med en rättslig förpliktelse, t.ex. skatte- och tullmyndigheter, finansutredningsgrupper, oberoende administrativa myndigheter eller finansmarknadsmyndigheter med ansvar för reglering och övervakning av värdepappersmarknader, bör inte betraktas som mottagare om de tar emot personuppgifter som är nödvändiga för utförandet av en särskild utredning av allmänt intresse, i enlighet med unionsrätten eller medlemstaternas nationella rätt. Offentliga myndigheters begäranden om att uppgifter ska lämnas ut ska alltid vara skriftliga och motiverade, läggas fram i enskilda fall och inte gälla hela register eller leda till att register kopplas samman. Dessa offentliga myndigheters behandling av personuppgifter bör ske i överensstämmelse med de bestämmelser för dataskydd som är tillämpliga på behandlingens ändamål.

(32) Samtycke bör lämnas genom en entydig bekräftande handling som innebär ett frivilligt, specifikt, informerat och otvetydigt medgivande från den registrerades sida om att denne godkänner behandling av personuppgifter rörande honom eller henne, som t.ex. genom en skriftlig, inklusive elektronisk, eller muntlig förklaring. Detta kan inbegripa att en ruta kryssas i vid besök på en internetsida, genom val av inställningsalternativ för tjänster på informationssamhällets område eller genom någon annan förklaring eller något annat beteende som i sammanhanget tydligt visar att den registrerade godtar den avsedda behandlingen av sina personuppgifter. Tystnad, på förhand ikryssade rutor eller inaktivitet bör därför inte utgöra samtycke. Samtycket bör gälla all behandling som utförs för samma ändamål. Om behandlingen tjänar flera olika syften, bör samtycke ges för samtliga syften. Om den registrerade ska lämna sitt samtycke efter en elektronisk begäran, måste denna vara tydlig och koncis och får inte onödigtvis störa användningen av den tjänst som den avser.

(33) Det är ofta inte möjligt att fullt ut identifiera syftet med en behandling av personuppgifter för vetenskapliga forskningsändamål i samband med insamlingen av uppgifter. Därför bör registrerade kunna ge sitt samtycke till vissa områden för vetenskaplig forskning, när vedertagna etiska standarder för vetenskaplig forskning iakttas. Registrerade bör ha möjlighet att endast lämna sitt samtycke till vissa forskningsområden eller delar av forskningsprojekt i den utsträckning det avsedda syftet medger detta.

(34) Genetiska uppgifter bör definieras som personuppgifter som rör en fysisk persons nedärvda eller förvärvade genetiska kännetecken, vilka framgår av en analys av ett biologiskt prov från den fysiska personen i fråga, framför allt kromosom-, DNA- eller RNA-analys eller av en annan form av analys som gör det möjligt att inhämta motsvarande information.

(35) Personuppgifter om hälsa bör innefatta alla de uppgifter som hänför sig till en registrerad persons hälsotillstånd som ger information om den registrerades tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd. Detta inbegriper uppgifter om den fysiska personen som insamlats i samband med registrering för eller tillhandahållande av hälso- och sjukvårdstjänster till den fysiska personen enligt Europaparlamentets och rådets direktiv 2011/24/EU ( ), ett nummer, en symbol eller ett kännetecken som den fysiska personen tilldelats för att identifiera denne för hälso- och sjukvårdsändamål, uppgifter som härrör från tester eller undersökning av en kroppsdel eller kroppssubstans, däribland genetiska uppgifter och biologiska prov, och andra uppgifter om exempelvis sjukdom, funktionshinder, sjukdomsrisk, sjukdomshistoria, klinisk behandling eller den registrerades fysiologiska eller biomedicinska tillstånd, oberoende av källan, exempelvis från en läkare eller från annan sjukvårdspersonal, ett sjukhus, en medicinteknisk produkt eller ett diagnostiskt in vitro-test.

(36) Den personuppgiftsansvariges huvudsakliga verksamhetsställe i unionen bör vara den plats i unionen där den personuppgiftsansvarige har sin centrala förvaltning, såvida inte beslut om ändamålen och medlen för behandling av personuppgifter fattas vid ett annat av den personuppgiftsansvariges verksamhetsställen i unionen; i sådant fall

( ) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).

bör det andra verksamhetsstället anses vara det huvudsakliga verksamhetsstället. En personuppgiftsansvarigs huvudsakliga verksamhetsställe inom unionen bör avgöras med beaktande av objektiva kriterier och bör inbegripa den faktiska och reella ledning som fattar de huvudsakliga besluten vad avser ändamål och medel för behandlingen med hjälp av en stabil struktur. Detta kriterium bör inte vara avhängigt av om behandlingen av personuppgifter utförs på detta ställe. Att tekniska medel och teknik för behandling av personuppgifter eller behandlingsverksamhet finns och används visar i sig inte att det rör sig om ett huvudsakligt verksamhetsställe och utgör därför inte avgörande kriterier för ett huvudsakligt verksamhetsställe. Personuppgiftsbiträdets huvudsakliga verksamhetsställe bör vara den plats i unionen där denne har sin centrala förvaltning eller, om denne inte har någon central förvaltning inom unionen, den plats inom unionen där den huvudsakliga behandlingen sker. I fall som omfattar både en personuppgiftsansvarig och ett personuppgiftsbiträde bör den behöriga ansvariga tillsynsmyndigheten fortfarande vara tillsynsmyndigheten i den medlemsstat där den personuppgiftsansvarige har sitt huvudsakliga verksamhetsställe, men den tillsynsmyndighet som gäller för personuppgiftsbiträdet bör betraktas som en berörd tillsynsmyndighet och den tillsynsmyndigheten bör delta i det samarbetsförfarande som föreskrivs i denna förordning. Om utkastet till beslut endast gäller den personuppgiftsansvarige, bör tillsynsmyndigheterna i den eller de medlemsstater där personuppgiftsbiträdet har ett eller flera verksamhetsställen inte under några omständigheter betraktas som berörda tillsynsmyndigheter. Om behandlingen utförs av en koncern bör det kontrollerande företagets huvudsakliga verksamhetsställe betraktas som koncernens huvudsakliga verksamhetsställe, utom då behandlingens ändamål och de medel med vilka den utförs fastställs av ett annat företag.

(37) En koncern bör innefatta ett kontrollerande företag och de företag som detta företag kontrollerar (kontrollerade företag), varvid det kontrollerande företaget bör vara det företag som kan utöva ett dominerande inflytande på de övriga företagen i kraft av exempelvis ägarskap, finansiellt deltagande eller de bestämmelser som det regleras av eller befogenheten att införa regler som rör personuppgiftsskyddet. Ett företag med kontroll över behandlingen av personuppgifter vid företag som är underställda detta företag bör, tillsammans med dessa företag, anses utgöra en koncern.

(38) Barns personuppgifter förtjänar särskilt skydd, eftersom barn kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder samt om sina rättigheter när det gäller behandling av personuppgifter. Sådant särskilt skydd bör i synnerhet gälla användningen av barns personuppgifter i marknadsföringssyfte eller för att skapa personlighets- eller användarprofiler samt insamling av personuppgifter med avseende på barn när tjänster som erbjuds direkt till barn utnyttjas. Samtycke från den person som har föräldraansvar över ett barn bör inte krävas för förebyggande eller rådgivande tjänster som erbjuds direkt till barn.

(39) Varje behandling av personuppgifter måste vara laglig och rättvis. Det bör vara klart och tydligt för fysiska personer hur personuppgifter som rör dem insamlas, används, konsulteras eller på annat sätt behandlas samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas. Öppenhetsprincipen kräver att all information och kommunikation i samband med behandlingen av dessa personuppgifter är lättillgänglig och lättbegriplig samt att ett klart och tydligt språk används. Den principen gäller framför allt informationen till registrerade om den personuppgiftsansvariges identitet och syftet med behandlingen samt ytterligare information för att sörja för en rättvis och öppen behandling för berörda fysiska personer och deras rätt att erhålla bekräftelse på och meddelande om vilka personuppgifter rörande dem som behandlas. Fysiska personer bör göras medvetna om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter och om hur de kan utöva sina rättigheter med avseende på behandlingen. De specifika ändamål som personuppgifterna behandlas för bör vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in. Personuppgifterna bör vara adekvata, relevanta och begränsade till vad som är nödvändigt för de ändamål som de behandlas för. Detta kräver i synnerhet att det tillses att den period under vilken personuppgifterna lagras är begränsad till ett strikt minimum. Personuppgifter bör endast behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel. För att säkerställa att personuppgifter inte sparas längre än nödvändigt bör den personuppgiftsansvarige införa tidsfrister för radering eller för regelbunden kontroll. Alla rimliga åtgärder bör vidtas för att rätta eller radera felaktiga uppgifter. Personuppgifter bör behandlas på ett sätt som säkerställer lämplig säkerhet och konfidentialitet för personuppgifterna samt förhindrar obehörigt tillträde till och obehörig användning av personuppgifter och den utrustning som används för behandlingen.

(40) För att behandling ska vara laglig bör personuppgifterna behandlas efter samtycke från den berörda registrerade eller på någon annan legitim grund som fastställts i lag, antingen i denna förordning eller i annan unionsrätt eller

medlemsstaternas nationella rätt enligt denna förordning, vilket inbegriper att de rättsliga skyldigheter som åligger den personuppgiftsansvarige måste fullgöras eller att ett avtal i vilket den registrerade är part måste genomföras eller att åtgärder på begäran av den registrerade måste vidtas innan avtalet ingås.

(41) När det i denna förordning hänvisas till en rättslig grund eller lagstiftningsåtgärd, innebär detta inte nödvändigtvis en lagstiftningsakt antagen av ett parlament, utan att detta påverkar krav som uppställs i den konstitutionella ordningen i den berörda medlemsstaten. En sådan rättslig grund eller lagstiftningsåtgärd bör dock vara tydlig och precis och dess tillämpning bör vara förutsägbar för personer som omfattas av den, i enlighet med rättspraxis vid Europeiska unionens domstol (nedan kallad *domstolen*) och Europeiska domstolen för de mänskliga rättigheterna.

(42) När behandling sker efter samtycke från registrerade, bör personuppgiftsansvariga kunna visa att de registrerade har lämnat sitt samtycke till behandlingen. I synnerhet vid skriftliga förklaringar som rör andra frågor bör det finnas skyddsåtgärder som säkerställer att de registrerade är medvetna om att samtycke ges och om hur långt samtycket sträcker sig. I enlighet med rådets direktiv 93/13/EEG ( ) bör en förklaring om samtycke som den personuppgiftsansvarige i förväg formulerat tillhandahållas i en begriplig och lätt tillgänglig form, med användning av ett klart och tydligt språk och utan oskäliga villkor. För att samtycket ska vara informerat bör den registrerade känna till åtminstone den personuppgiftsansvariges identitet och syftet med den behandling för vilken personuppgifterna är avsedda. Samtycke bör inte betraktas som frivilligt om den registrerade inte har någon genuin eller fri valmöjlighet eller inte utan problem kan vägra eller ta tillbaka sitt samtycke.

(43) För att säkerställa att samtycket lämnas frivilligt bör det inte utgöra giltig rättslig grund för behandling av personuppgifter i ett särskilt fall där det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet och det därför är osannolikt att samtycket har lämnats frivilligt när det gäller alla förhållanden som denna särskilda situation omfattar. Samtycke antas inte vara frivilligt om det inte medger att separata samtycken lämnas för olika behandlingar av personuppgifter, trots att detta är lämpligt i det enskilda fallet, eller om genomförandet av ett avtal – inbegripet tillhandahållandet av en tjänst – är avhängigt av samtycket, trots att samtycket inte är nödvändigt för ett sådant genomförande.

(44) Behandling bör vara laglig när den är nödvändig i samband med avtal eller när det finns en avsikt att ingå ett avtal.

(45) Behandling som grundar sig på en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller behandling som krävs för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning, bör ha en grund i unionsrätten eller i en medlemsstats nationella rätt. Denna förordning medför inte något krav på en särskild lag för varje enskild behandling. Det kan räcka med en lag som grund för flera behandlingar som bygger på en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller om behandlingen krävs för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Behandlingens syfte bör också fastställas i unionsrätten eller i medlemsstaternas nationella rätt. Därtill skulle man genom denna grund kunna ange denna förordnings allmänna villkor för laglig personuppgiftsbehandling och precisera kraven för att fastställa vem den personuppgiftsansvarige är, vilken typ av personuppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut, ändamålsbegränsningar, lagringstid samt andra åtgärder för att tillförsäkra en laglig och rättvis behandling. Unionsrätten eller medlemsstaternas nationella rätt bör också reglera frågan huruvida en personuppgiftsansvarig som utför en uppgift av allmänt intresse eller som ett led i myndighetsutövning ska vara en offentlig myndighet eller någon annan fysisk eller juridisk person som omfattas av offentligrättslig lagstiftning eller, om detta motiveras av allmänintresset, vilket inbegriper hälso- och sjukvårdsändamål, såsom folkhälsa och socialt skydd och förvaltning av hälso- och sjukvårdstjänster, av civilrättslig lagstiftning, exempelvis en yrkesorganisation.

(46) Behandling av personuppgifter bör även anses laglig när den är nödvändig för att skydda ett intresse som är av avgörande betydelse för den registrerades eller en annan fysisk persons liv. Behandling av personuppgifter på

( ) Rådets direktiv 93/13/EEG av den 5 april 1993 om oskäliga villkor i konsumentavtal (EGT L 95, 21.4.1993, s. 29).

grundval av en annan fysisk persons grundläggande intressen bör i princip endast äga rum om behandlingen inte uppenbart kan ha en annan rättslig grund. Vissa typer av behandling kan tjäna både viktiga allmänintressen och intressen som är av grundläggande betydelse för den registrerade, till exempel när behandlingen är nödvändig av humanitära skäl, bland annat för att övervaka epidemier och deras spridning eller i humanitära nödsituationer, särskilt vid naturkatastrofer eller katastrofer orsakade av människan.

(47) En personuppgiftsansvarigs berättigade intressen, inklusive intressena för en personuppgiftsansvarig till vilken personuppgifter får lämnas ut, eller för en tredje part, kan utgöra rättslig grund för behandling, på villkor att de registrerades intressen eller grundläggande rättigheter och friheter inte väger tyngre, med beaktande av de registrerades rimliga förväntningar till följd av förhållandet till den personuppgiftsansvarige. Ett sådant berättigat intresse kan till exempel finnas när det föreligger ett relevant och lämpligt förhållande mellan den registrerade och den personuppgiftsansvarige i sådana situationer som att den registrerade är kund hos eller arbetar för den personuppgiftsansvarige. Ett berättigat intresse kräver under alla omständigheter en noggrann bedömning, som inbegriper huruvida den registrerade vid tidpunkten för inhämtandet av personuppgifter och i samband med detta rimligen kan förvänta sig att en uppgiftsbehandling för detta ändamål kan komma att ske. Den registrerades intressen och grundläggande rättigheter skulle i synnerhet kunna väga tyngre än den personuppgiftsansvariges intressen, om personuppgifter behandlas under omständigheter där den registrerade inte rimligen kan förvänta sig någon ytterligare behandling. Med tanke på att det är lagstiftarens sak att genom lagstiftning tillhandahålla den rättsliga grunden för de offentliga myndigheternas behandling av personuppgifter, bör den rättsliga grunden inte gälla den behandling de utför som ett led i fullgörandet av sina uppgifter. Sådan behandling av personuppgifter som är absolut nödvändig för att förhindra bedrägerier utgör också ett berättigat intresse för berörd personuppgiftsansvarig. Behandling av personuppgifter för direktmarknadsföring kan betraktas som ett berättigat intresse.

(48) Personuppgiftsansvariga som ingår i en koncern eller institutioner som är underställda ett centralt organ kan ha ett berättigat intresse att överföra personuppgifter inom koncernen för interna administrativa ändamål, bland annat för behandling av kunders eller anställdas personuppgifter. De allmänna principerna för överföring av personuppgifter, inom en koncern, till företag i tredjeland påverkas inte.

(49) Behandling av personuppgifter utgör ett berättigat intresse för berörd personuppgiftsansvarig i den mån den är absolut nödvändig och proportionell för att säkerställa nät- och informationssäkerhet, dvs. förmågan hos ett nät eller ett informationssystem att vid en viss tillförlitlighetsnivå tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande som äventyrar tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda personuppgifter och säkerheten hos besläktade tjänster som tillhandahålls av – eller är tillgängliga via – dessa nät och system, av myndigheter, incidenthanteringsorganisationer (Cert), enheter för hantering av datasäkerhetsincidenter, tillhandahållare av elektroniska kommunikationsnät och kommunikationstjänster och tillhandahållare av säkerhetsteknik och säkerhetstjänster. Detta skulle t.ex. kunna innefatta att förhindra obehörigt tillträde till elektroniska kommunikationsnät och felaktig kodfördelning och att sätta stopp för överbelastningsattacker och skador på datasystem och elektroniska kommunikationssystem.

(50) Behandling av personuppgifter för andra ändamål än de för vilka de ursprungligen samlades in bör endast vara tillåten, när detta är förenligt med de ändamål för vilka personuppgifterna ursprungligen samlades in. I dessa fall krävs det inte någon annan separat rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs. Om behandlingen är nödvändig för att fullgöra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som den personuppgiftsansvarige har fått i uppgift att utföra, kan unionsrätten eller medlemsstaternas nationella rätt fastställa och närmare ange för vilka uppgifter och syften ytterligare behandling bör betraktas som förenlig och laglig. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör betraktas som förenlig och laglig behandling av uppgifter. Den rättsliga grund för behandling av personuppgifter som återfinns i unionsrätten eller i medlemsstaternas nationella rätt kan också utgöra en rättslig grund för ytterligare behandling. För att fastställa om ett ändamål med den ytterligare behandlingen är förenligt med det ändamål för vilket personuppgifterna ursprungligen insamlades bör den personuppgiftsansvarige, efter att ha uppfyllt alla krav vad beträffar den ursprungliga behandlingens lagenlighet, bland annat beakta alla kopplingar mellan dessa ändamål och ändamålen med den avsedda ytterligare behandlingen, det sammanhang inom vilket personuppgifterna insamlats, särskilt de registrerades rimliga förväntningar till följd av förhållandet till den personuppgiftsansvarige i fråga om den

art, den planerade ytterligare behandlingens konsekvenser för de registrerade samt förekomsten av lämpliga skyddsåtgärder för både den ursprungliga och den planerade ytterligare behandlingen.

Om den registrerade har gett sitt medgivande eller behandlingen grundar sig på unionsrätten eller på medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa i synnerhet viktiga mål av allmänt intresse, bör den personuppgiftsansvarige tillåtas att behandla personuppgifterna ytterligare, oavsett om detta är förenligt med ändamålen eller inte. Under alla omständigheter bör tillämpningen av principerna i denna förordning, särskilt informationen till den registrerade om dessa andra ändamål och om dennes rättigheter, inbegripet rätten att göra invändningar, säkerställas. Om den personuppgiftsansvarige anmäler möjliga brott eller hot mot den allmänna säkerheten och i enskilda fall eller i flera fall som rör samma brott eller hot mot den allmänna säkerheten överför dessa personuppgifter till en behörig myndighet, ska detta betraktas som att den personuppgiftsansvarige agerar i ett berättigat intresse. Sådan överföring i den personuppgiftsansvariges berättigade intresse eller ytterligare behandling av personuppgifter bör emellertid vara förbjuden, om behandlingen inte är förenlig med lagstadgad eller yrkesmässig tystnadsplikt eller annan bindande tystnadsplikt.

(51) Personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheterna och friheter bör åtnjuta särskilt skydd, eftersom behandling av sådana uppgifter kan innebära betydande risker för de grundläggande rättigheterna och friheterna. Dessa personuppgifter bör även inbegripa personuppgifter som avslöjar ras eller etniskt ursprung, varvid användningen av termen *ras* i denna förordning inte innebär att unionen godtar teorier som söker fastställa förekomsten av skilda människoraser. Behandling av foton bör inte systematiskt anses utgöra behandling av särskilda kategorier av personuppgifter, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person. Sådana personuppgifter bör inte behandlas, såvida inte behandling medges i särskilda fall som fastställs i denna förordning, med beaktande av att det i medlemsstaternas lagstiftning får införas särskilda bestämmelser om dataskydd för att anpassa tillämpningen av bestämmelserna i denna förordning i syfte att fullgöra en rättslig skyldighet eller en uppgift av allmänt intresse eller som ett led i myndighetsutövning som den personuppgiftsansvarige har fått i uppgift att utföra. Utöver de särskilda kraven för sådan behandling, bör de allmänna principerna och andra bestämmelser i denna förordning tillämpas, särskilt när det gäller villkoren för laglig behandling. Undantag från det allmänna förbudet att behandla sådana särskilda kategorier av personuppgifter bör uttryckligen fastställas, bland annat om den registrerade lämnar sitt uttryckliga samtycke eller för att tillgodose specifika behov, i synnerhet när behandlingen utförs inom ramen för legitima verksamheter som bedrivs av vissa sammanslutningar eller stiftelser i syfte att göra det möjligt att utöva grundläggande friheter.

(52) Undantag från förbudet att behandla särskilda kategorier av personuppgifter bör även tillåtas om de föreskrivs i unionsrätten eller i medlemsstaternas nationella rätt och underkastas lämpliga skyddsåtgärder för att skydda personuppgifter och övriga grundläggande rättigheter, när allmänintresset motiverar detta, i synnerhet i fråga om behandling av personuppgifter inom ramen för arbetsrätt och sociallagstiftning, däribland pensioner, och för hälsosäkerhetsändamål, övervaknings- och varningssyften, förebyggande eller kontroll av smittsamma sjukdomar och andra allvarliga hot mot hälsan. Detta undantag får göras för hälsoändamål, inbegripet folkhälsa och förvaltningen av hälso- och sjukvårdstjänster, särskilt för att säkerställa kvalitet och kostnadseffektivitet i de förfaranden som används vid prövningen av ansökningar om förmåner och tjänster inom sjukförsäkringssystemet, eller för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Genom undantag bör man även tillåta behandling av sådana personuppgifter där så krävs för fastställande, utövande eller försvar av rättsliga anspråk, oavsett om detta sker inom ett domstolsförfarande eller inom ett administrativt eller ett utomrättsligt förfarande.

(53) Särskilda kategorier av personuppgifter som förtjänar ett mer omfattande skydd bör endast behandlas i hälsorelaterade syften om detta krävs för att uppnå dessa syften och gagnar fysiska personer och samhället i stort, särskilt inom ramen för förvaltningen av tjänster för hälso- och sjukvård och social omsorg och deras system, inbegripet behandling som utförs av förvaltningen och centrala nationella hälsovårdsmyndigheter av sådana uppgifter för syften som hör samman med kvalitetskontroll, information om förvaltningen samt allmän nationell och lokal tillsyn över hälso- och sjukvårdssystemet och systemet för social omsorg och säkerställande av kontinuitet inom hälso- och sjukvård och social omsorg samt gränsöverskridande hälso- och sjukvård eller hälsosäkerhet, syften som hör samman med övervakning samt varningssyften eller för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål som baseras på unionsrätten eller på medlemsstaternas nationella rätt, vilka måste ha ett syfte av allmänt intresse, samt studier som genomförs av allmänt intresse på folkhälsoområdet. Denna förordning bör därför innehålla harmoniserade villkor för behandling av särskilda kategorier av personuppgifter om hälsa, vad gäller särskilda behov, i synnerhet när behandlingen av uppgifterna utförs för vissa hälsorelaterade syften av personer som enligt lag är underkastade

yrkesmässig tystnadsplikt. Unionsrätten eller medlemsstaternas nationella rätt bör föreskriva särskilda och lämpliga åtgärder som skyddar fysiska personers grundläggande rättigheter och personuppgifter. Medlemsstaterna bör få behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om hälsa. Detta bör emellertid inte hindra det fria flödet av personuppgifter inom unionen, när villkoren tillämpas på gränsöverskridande behandling av sådana uppgifter.

(54) På folkhälsoområdet kan det bli nödvändigt att med hänsyn till ett allmänt intresse behandla särskilda kategorier av personuppgifter utan att den registrerades samtycke inhämtas. Sådan behandling bör förutsätta lämpliga och särskilda åtgärder för att skydda fysiska personers rättigheter och friheter. I detta sammanhang bör *folkhälsa* tolkas enligt definitionen i Europaparlamentets och rådets förordning (EG) nr 1338/2008 ( ), nämligen alla aspekter som rör hälsosituationen, dvs. allmänhetens hälsotillstånd, inbegripet sjuklighet och funktionshinder, hälsans bestämningsfaktorer, hälso- och sjukvårdsbehov, resurser inom hälso- och sjukvården, tillhandahållande av och allmän tillgång till hälso- och sjukvård, utgifter för och finansiering av hälso- och sjukvården samt dödsorsaker. Sådan behandling av uppgifter om hälsa av allmänt intresse bör inte innebära att personuppgifter behandlas för andra ändamål av tredje part, exempelvis arbetsgivare eller försäkrings- och bankföretag.

(55) Myndigheters behandling av personuppgifter på officiellt erkända religiösa sammanslutningars vägnar i syften som fastställs i grundlag eller i folkrätten anses också grunda sig på ett allmänt intresse.

(56) Om det för att det demokratiska systemet ska fungera i samband med allmänna val är nödvändigt att politiska partier i vissa medlemsstater samlar in personuppgifter om fysiska personers politiska uppfattningar, får behandling av sådana uppgifter tillåtas med hänsyn till ett allmänt intresse, på villkor att lämpliga skyddsåtgärder fastställs.

(57) Om de personuppgifter som behandlas av en personuppgiftsansvarig inte gör det möjligt för denne att identifiera en fysisk person, bör den personuppgiftsansvarige inte vara tvungen att skaffa ytterligare information för att kunna identifiera den registrerade, om ändamålet endast är att följa någon av bestämmelserna i denna förordning. Den personuppgiftsansvarige bör dock inte vägra att ta emot kompletterande uppgifter som den registrerade lämnat som stöd för utövandet av sina rättigheter. Identifiering bör omfatta digital identifiering av en registrerad, till exempel genom en autentiseringsmekanism, exempelvis samma identifieringsinformation som används av den registrerade för att logga in på den nättjänst som tillhandahålls av den personuppgiftsansvarige.

(58) Öppenhetsprincipen kräver att all information som riktar sig till allmänheten eller till registrerade är kortfattad, lättåtkomlig och lättbegriplig samt utformad på ett tydligt och enkelt språk samt att man vid behov använder visualisering. Denna information kan ges elektroniskt, exempelvis på en webbplats, när den riktas till allmänheten. Detta är särskilt relevant i situationer där mängden olika aktörer och den tekniska komplexiteten gör det svårt för den registrerade att veta och förstå om personuppgifter som rör honom eller henne samlas in, vem som gör det och för vilket syfte, exempelvis i fråga om reklam på nätet. Eftersom barn förtjänar särskilt skydd, bör all information och kommunikation som riktar sig till barn utformas på ett tydligt och enkelt språk som barnet lätt kan förstå.

(59) Förfaranden bör fastställas som gör det lättare för registrerade att utöva sina rättigheter enligt denna förordning, inklusive mekanismer för att begära och i förekommande fall kostnadsfritt få tillgång till och erhålla rättelse eller radering av personuppgifter samt för att utöva rätten att göra invändningar. Den personuppgiftsansvarige bör också tillhandahålla hjälpmedel för elektroniskt ingivna framställningar, särskilt i fall då personuppgifter behandlas elektroniskt. Personuppgiftsansvariga bör utan onödigt dröjsmål och senast inom en månad vara skyldiga att besvara registrerades önskemål och lämna en motivering, om de inte avser att uppfylla sådana önskemål.

( ) Europaparlamentets och rådets förordning (EG) nr 1338/2008 av den 16 december 2008 om gemenskapsstatistik om folkhälsa och hälsa och säkerhet i arbetet (EUT L 354, 31.12.2008, s. 70).

(60) Principerna om rättvis och öppen behandling fordrar att den registrerade informeras om att behandling sker och syftet med den. Den personuppgiftsansvarige bör till den registrerade lämna all ytterligare information som krävs för att säkerställa en rättvis och öppen behandling, med beaktande av personuppgiftsbehandlingens specifika omständigheter och sammanhang. Dessutom bör den registrerade informeras om förekomsten av profilering samt om konsekvenserna av sådan profilering. Om personuppgifterna samlas in från den registrerade, bör denne även informeras om huruvida han eller hon är skyldig att tillhandahålla personuppgifterna och om konsekvenserna om han eller hon inte lämnar dem. Denna information får tillhandahållas kombinerad med standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över den planerade behandlingen. Om sådana symboler visas elektroniskt bör de vara maskinläsbara.

(61) Information om behandling av personuppgifter som rör den registrerade bör lämnas till honom eller henne vid den tidpunkt då personuppgifterna samlas in från den registrerade eller, om personuppgifterna erhålls direkt från en annan källa, inom en rimlig period, beroende på omständigheterna i fallet. Om personuppgifter legitimt kan lämnas ut till en annan mottagare, bör de registrerade informeras första gången personuppgifterna lämnas ut till denna mottagare. Om den personuppgiftsansvarige avser att behandla personuppgifter för ett annat ändamål än det för vilket uppgifterna insamlades, bör denne före ytterligare behandling informera den registrerade om detta andra syfte och lämna annan nödvändig information. Om personuppgifternas ursprung inte kan meddelas den registrerade på grund av att olika källor har använts, bör allmän information ges.

(62) Det är dock inte nödvändigt att införa någon skyldighet att tillhandahålla information, om den registrerade redan innehar denna information, om registreringen eller utlämnandet av personuppgifterna uttryckligen föreskrivs i lag eller om det visar sig vara omöjligt eller skulle medföra orimliga ansträngningar att tillhandahålla den registrerade informationen. Det sistnämnda skulle särskilt kunna vara fallet om behandlingen sker för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. I detta avseende bör antalet registrerade, uppgifternas ålder och lämpliga skyddsåtgärder beaktas.

(63) Den registrerade bör ha rätt att få tillgång till personuppgifter som insamlats om denne samt på enkelt sätt och med rimliga intervall kunna utöva denna rätt, för att vara medveten om att behandling sker och kunna kontrollera att den är laglig. Detta innefattar rätten för registrerade att få tillgång till uppgifter om sin hälsa, exempelvis uppgifter i läkarjournaler med t.ex. diagnoser, undersökningsresultat, bedömningar av behandlande läkare och eventuella vårdbehandlingar eller interventioner. Alla registrerade bör därför ha rätt att få kännedom och underrättelse om framför allt orsaken till att personuppgifterna behandlas, om möjligt vilken tidsperiod behandlingen pågår, vilka som mottar personuppgifterna, bakomliggande logik i samband med automatisk behandling av personuppgifter och, åtminstone när behandlingen bygger på profilering, konsekvenserna av sådan behandling. Om möjligt bör den personuppgiftsansvarige kunna ge fjärråtkomst till ett säkert system genom vilket den registrerade kan få direkt åtkomst till sina personuppgifter. Denna rätt bör inte inverka menligt på andras rättigheter eller friheter, t.ex. affärshemligheter eller immateriell äganderätt och särskilt inte på upphovsrätt som skyddar programvaran. Resultatet av dessa överväganden bör dock inte bli att den registrerade förvägras all information. Om den personuppgiftsansvarige behandlar en stor mängd uppgifter om den registrerade, bör den personuppgiftsansvarige kunna begära att den registrerade lämnar uppgift om vilken information eller vilken behandling en framställan avser, innan informationen lämnas ut.

(64) Personuppgiftsansvariga bör vidta alla rimliga åtgärder för att kontrollera identiteten på en registrerad som begär tillgång, särskilt inom ramen för nättjänster och i fråga om nätidentifierare. Personuppgiftsansvariga bör inte behålla personuppgifter enbart för att kunna agera vid en potentiell begäran.

(65) Den registrerade bör ha rätt att få sina personuppgifter rättade och en *rätt att bli bortglömd*, om lagringen av uppgifterna strider mot denna förordning eller unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av. En registrerad bör särskilt ha rätt att få sina personuppgifter raderade och kunna begära att dessa personuppgifter inte behandlas, om de inte längre behövs med tanke på de ändamål för vilka de samlats in eller på annat sätt behandlats, om en registrerad har återtagit sitt samtycke till behandling eller invänder mot behandling av personuppgifter som rör honom eller henne, eller om behandlingen av hans eller

hennes personuppgifter på annat sätt inte överensstämmer med denna förordning. Denna rättighet är särskilt relevant när den registrerade har gett sitt samtycke som barn, utan att vara fullständigt medveten om riskerna med behandlingen, och senare vill ta bort dessa personuppgifter, särskilt på internet. Den registrerade bör kunna utöva denna rätt även när han eller hon inte längre är barn. Ytterligare lagring av personuppgifterna bör dock vara laglig, om detta krävs för att utöva yttrandefrihet och informationsfrihet, för att uppfylla en rättslig förpliktelse, för att utföra en uppgift i av allmänt intresse eller som ett led i myndighetsutövning som anförtrotts den personuppgiftsansvarige, med anledning av ett allmänt intresse inom folkhälsoområdet, för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål eller för fastställande, utövande eller försvar av rättsliga anspråk.

(66) För att stärka ”rätten att bli bortglömd” i nätmiljön bör rätten till radering utvidgas genom att personuppgiftsansvariga som offentliggjort personuppgifter är förpliktigade att vidta rimliga åtgärder, däribland tekniska åtgärder, för att informera de personuppgiftsansvariga som behandlar dessa personuppgifter om att den registrerade har begärt radering av alla länkar till och kopior eller reproduktioner av dessa personuppgifter. I samband med detta bör den personuppgiftsansvarige vidta rimliga åtgärder, med beaktande av tillgänglig teknik och de hjälpmedel som står den personuppgiftsansvarige till buds, däribland tekniska åtgärder, för att informera de personuppgiftsansvariga som behandlar personuppgifterna om den registrerades begäran.

(67) Sätten att begränsa behandlingen av personuppgifter kan bland annat inbegripa att man tillfälligt flyttar de valda personuppgifterna till ett annat databehandlingssystem, gör de valda uppgifterna otillgängliga för användare eller tillfälligt avlägsnar offentliggjorda uppgifter från en webbplats. I automatiserade register bör begränsningen av behandlingen i princip ske med tekniska medel på ett sådant sätt att personuppgifterna inte blir föremål för ytterligare behandling och inte kan ändras. Det förhållandet att behandlingen av personuppgifter är begränsad bör klart anges inom systemet.

(68) För att ytterligare förbättra kontrollen över sina egna uppgifter bör den registrerade, om personuppgifterna behandlas automatiskt, också tillåtas att motta de personuppgifter som rör honom eller henne, som han eller hon har tillhandahållit den personuppgiftsansvarige, i ett strukturerat, allmänt använt, maskinläsbart och kompatibelt format och överföra dessa till en annan personuppgiftsansvarig. Personuppgiftsansvariga bör uppmuntras att utveckla kompatibla format som möjliggör dataportabilitet. Denna rättighet bör vara tillämplig om den registrerade har tillhandahållit uppgifterna efter att ha lämnat sitt samtycke eller om behandlingen är nödvändig för att ett avtal ska kunna genomföras. Den bör inte vara tillämplig om behandlingen utgår från en annan rättslig grund än samtycke eller avtal. På grund av sin art bör denna rättighet inte utövas mot personuppgiftsansvariga som behandlar personuppgifter som ett led i myndighetsutövning. Därför bör den inte vara tillämplig när behandlingen av personuppgifterna är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som utförs av den personuppgiftsansvarige. Den registrerades rätt att överföra eller motta personuppgifter som rör honom eller henne innebär inte någon skyldighet för de personuppgiftsansvariga att införa eller upprätthålla behandlingssystem som är tekniskt kompatibla. Om mer än en registrerad berörs inom en viss uppsättning personuppgifter, bör rätten att motta personuppgifterna inte inverka på andra registrerades rättigheter och friheter enligt denna förordning. Denna rättighet bör inte heller påverka den registrerades rätt att få till stånd radering av personuppgifter och de inskränkningar av denna rättighet vilka anges i denna förordning och bör i synnerhet inte medföra radering av personuppgifter om den registrerade som denne har lämnat för genomförande av ett avtal, i den utsträckning och så länge som personuppgifterna krävs för genomförande av avtalet. Om det är tekniskt möjligt, bör den registrerade ha rätt till direkt överföring av personuppgifterna från en personuppgiftsansvarig till en annan.

(69) När personuppgifter lagligen får behandlas, eftersom behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i en myndighetsutövning som utförs av den personuppgiftsansvarige, eller på grund av en personuppgiftsansvarigs eller en tredje parts berättigade intressen, bör alla registrerade ändå ha rätt att göra invändningar mot behandling av personuppgifter som rör de registrerades särskilda situation. Det bör ankomma på den personuppgiftsansvarige att visa att dennes tvingande berättigade intressen väger tyngre än den registrerades intressen eller grundläggande rättigheter och friheter.

(70) Om personuppgifter behandlas för direktmarknadsföring, bör den registrerade, oavsett om det handlar om inledande eller ytterligare behandling, ha rätt att när som helst kostnadsfritt invända mot sådan behandling, inbegripet profilering, i den mån denna är kopplad till direktmarknadsföring. Denna rättighet bör uttryckligen meddelas den registrerade och redovisas tydligt, klart och åtskilt från annan information.

(71) Den registrerade bör ha rätt att inte bli föremål för ett beslut, vilket kan inbegripa en åtgärd, med bedömning av personliga aspekter rörande honom eller henne, vilket enbart grundas på automatiserad behandling och medför rättsverkan för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne, såsom ett automatiserat avslag på en kreditansökan online eller e-rekrytering utan personlig kontakt. Sådan behandling omfattar "profilering" i form av automatisk behandling av personuppgifter med bedömning av personliga aspekter rörande en fysisk person, särskilt för att analysera eller förutse aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar, i den mån dessa har rättsverkan rörande honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. Beslutsfattande grundat på sådan behandling, inbegripet profilering, bör dock tillåtas när det uttryckligen beviljas genom unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av, inbegripet för sådan övervakning och sådant förebyggande av bedrägerier och skatteundandragande som genomförs i enlighet med unionsinstitutionernas eller de nationella tillsynsorganens bestämmelser, standarder och rekommendationer samt för att säkra för tillförlitlighet hos en tjänst som tillhandahålls av den personuppgiftsansvarige, eller när det krävs för ingående eller genomförande av ett avtal mellan den registrerade och en personuppgiftsansvarig eller den registrerade har gett sitt uttryckliga samtycke. Denna form av uppgiftsbehandling bör under alla omständigheter omgärdas av lämpliga skyddsåtgärder, som bör inkludera specifik information till den registrerade och rätt till mänskligt ingripande, att framföra sina synpunkter, att erhålla en förklaring till det beslut som fattas efter sådan bedömning och att överklaga beslutet. Sådana åtgärder bör inte gälla barn.

I syfte att säkra för rättvis och transparent behandling med avseende på den registrerade, med beaktande av omständigheterna och det sammanhang i vilket personuppgifterna behandlas, bör den personuppgiftsansvarige använda adekvata matematiska eller statistiska förfaranden för profilering, genomföra tekniska och organisatoriska åtgärder som framför allt säkerställer att faktorer som kan medföra felaktigheter i personuppgifter korrigeras och att risken för fel minimeras samt säkra personuppgifterna på sådant sätt att man beaktar potentiella risker för den registrerades intressen och rättigheter och förhindrar bland annat diskriminerande effekter för fysiska personer, på grund av ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse, medlemskap i fackföreningar, genetisk status eller hälsostatus eller sexuell läggning, eller som leder till åtgärder som får sådana effekter. Automatiserat beslutsfattande och profilering baserat på särskilda kategorier av personuppgifter bör endast tillåtas på särskilda villkor.

(72) Profilering omfattas av denna förordnings bestämmelser om behandling av personuppgifter, såsom de rättsliga grunderna för behandlingen och principer för dataskydd. Europeiska dataskyddsstyrelsen som inrättas genom denna förordning (nedan kallad *styrelsen*) bör kunna utfärda riktlinjer i detta avseende.

(73) Begränsningar med avseende på specifika principer och rätten till information, tillgång till och rättelse eller radering av personuppgifter, rätten till dataportabilitet, rätten att göra invändningar, profileringsbaserade beslut samt information till den registrerade om personuppgiftsincidenter och vissa av den personuppgiftsansvariges relaterade skyldigheter kan införas genom unionsrätten eller medlemsstaternas nationella rätt, i den mån de är nödvändiga och proportionella i ett demokratiskt samhälle för att upprätthålla den allmänna säkerheten, exempelvis för att skydda människoliv, särskilt vid naturkatastrofer eller katastrofer framkallade av människan, vid förebyggande, förhindrande, utredning och lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten eller överträdelser av etiska principer för reglerade yrken, vad gäller unionens eller en medlemsstats övriga viktiga mål av allmänt intresse, särskilt om de är av stort ekonomiskt eller finansiellt intresse för unionen eller en medlemsstat, förande av offentliga register som förs av hänsyn till ett allmänt intresse, ytterligare behandling av arkiverade personuppgifter för att tillhandahålla specifik information om politiskt beteende under tidigare totalitära regimer eller skydd av den registrerade eller andras rättigheter och friheter, inklusive socialt skydd, folkhälsa och humanitära skäl. Dessa begränsningar bör överensstämma med kraven i stadgan och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

(74) Personuppgiftsansvariga bör åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar. Personuppgiftsansvariga bör särskilt vara skyldiga att vidta lämpliga och effektiva åtgärder och kunna visa att behandlingen är förenlig med denna förordning, även vad gäller åtgärdernas effektivitet. Man bör inom dessa åtgärder beakta behandlingens art, omfattning, sammanhang och ändamål samt risken för fysiska personers rättigheter och friheter.

(75) Risken för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av personuppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering eller annan betydande ekonomisk eller social nackdel, om registrerade kan berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter, om personuppgifter behandlas som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i fackförening, om genetiska uppgifter, uppgifter om hälsa eller sexualliv eller fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder behandlas, om personliga aspekter bedöms, framför allt analyser eller förutsägelser beträffande sådant som rör arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlitlighet eller beteende, vistelseort eller förflyttningar, i syfte att skapa eller använda personliga profiler, om det sker behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

(76) Hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen inbegriper en risk eller en hög risk.

(77) Vägledning för den personuppgiftsansvariges eller personuppgiftsbiträdets genomförande av lämpliga åtgärder och för påvisande av att behandlingen är förenlig med denna förordning, särskilt när det gäller att kartlägga den risk som är förknippad med behandlingen och bedöma dess ursprung, art, sannolikhetsgrad och allvar samt fastställa bästa praxis för att minska risken, kan framför allt ges genom godkända uppförandekoder, godkänd certifiering, riktlinjer från styrelsen eller genom anvisningar från ett dataskyddsombud. Styrelsen kan också utfärda riktlinjer för uppgiftsbehandling som inte bedöms medföra någon hög risk för fysiska personers rättigheter och friheter samt ange vilka åtgärder som i sådana fall kan vara tillräckliga för att bemöta en sådan risk.

(78) Skyddet av fysiska personers rättigheter och friheter i samband med behandling av personuppgifter förutsätter att lämpliga tekniska och organisatoriska åtgärder vidtas, så att kraven i denna förordning uppfylls. För att kunna visa att denna förordning följs bör den personuppgiftsansvarige anta interna strategier och vidta åtgärder, särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard. Sådana åtgärder kan bland annat bestå av att uppgiftsbehandlingen minimeras, att personuppgifter snarast möjligt pseudonymiseras, att öppenhet om personuppgifternas syfte och behandling iakttas, att den registrerade får möjlighet att övervaka uppgiftsbehandlingen och att den personuppgiftsansvarige får möjlighet att skapa och förbättra säkerhetsanordningar. Vid utveckling, utformning, urval och användning av applikationer, tjänster och produkter som är baserade på behandling av personuppgifter eller behandlar personuppgifter för att uppfylla sitt syfte bör producenterna av dessa produkter, tjänster och applikationer uppmanas att beakta rätten till dataskydd när sådana produkter, tjänster och applikationer utvecklas och utformas och att, med tillbörlig hänsyn till den tekniska utvecklingen, säkerställa att personuppgiftsansvariga och personuppgiftsbiträden kan fullgöra sina skyldigheter avseende dataskydd. Principerna om inbyggt dataskydd och dataskydd som standard bör också beaktas vid offentliga upphandlingar.

(79) Skyddet av de registrerades rättigheter och friheter samt de personuppgiftsansvarigas och personuppgiftsbiträdenas ansvar, även i förhållande till tillsynsmyndigheternas övervakning och åtgärder, kräver ett tydligt fastställande av vem som bär ansvaret enligt denna förordning, bl.a. när personuppgiftsansvariga gemensamt fastställer ändamål och medel för en behandling tillsammans med andra personuppgiftsansvariga eller när en behandling utförs på en personuppgiftsansvarigs vägnar.

(80) När personuppgiftsansvariga eller personuppgiftsbiträden som inte är etablerade inom unionen behandlar personuppgifter om registrerade som befinner sig inom unionen och det bakomliggande syftet med uppgiftsbehandlingen är att erbjuda de registrerade personerna i unionen varor eller tjänster, oberoende av om de registrerade personerna måste betala för dem, eller att övervaka deras beteende i den mån beteendet äger rum i unionen, bör de personuppgiftsansvariga eller personuppgiftsbiträdena utnämna en företrädare, såvida inte behandlingen endast är tillfällig, inte omfattar behandling i stor omfattning av särskilda kategorier av personuppgifter eller behandling av personuppgifter om fällande domar i brottmål samt överträdelser och det är

osannolikt att den inbegriper en risk för fysiska personers rättigheter och friheter, med beaktande av behandlingens art, sammanhang, omfattning och ändamål eller om den personuppgiftsansvarige är en myndighet eller ett organ. Företrädaren bör agera på den personuppgiftsansvariges eller på personuppgiftsbiträdets vägnar och kan kontaktas av samtliga tillsynsmyndigheter. Företrädaren bör uttryckligen utses genom en skriftlig fullmakt från den personuppgiftsansvarige eller från personuppgiftsbiträdet att agera på dennes vägnar med avseende på dennes skyldigheter enligt denna förordning. Utnämningen av företrädaren inverkar inte på den personuppgiftsansvariges eller på personuppgiftsbiträdets ansvar enligt denna förordning. Företrädaren bör utföra sina uppgifter i enlighet med erhållen fullmakt från den personuppgiftsansvarige eller från personuppgiftsbiträdet, vilket inbegriper samarbete med de behöriga tillsynsmyndigheterna i fråga om alla åtgärder som vidtas för att säkra efterlevnad av denna förordning. Den utsedda företrädaren bör underkastas verkställighetsförfaranden i händelse den personuppgiftsansvarige eller personuppgiftsbiträdet inte uppfyller sina skyldigheter.

(81) För att se till att kraven i denna förordning uppfylls vad gäller behandling som av ett personuppgiftsbiträde ska utföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige, när denne anförtror behandling åt ett personuppgiftsbiträde, endast använda personuppgiftsbiträden som ger tillräckliga garantier, i synnerhet i fråga om sakkunskap, tillförlitlighet och resurser, för att genomföra tekniska och organisatoriska åtgärder som uppfyller kraven i denna förordning, bl.a. vad gäller säkerhet i samband med behandlingen av uppgifter. Personuppgiftsbiträdets anslutning till en godkänd uppförandekod eller en godkänd certifieringsmekanism kan användas som ett sätt att påvisa att den personuppgiftsansvarige fullgör sina skyldigheter. När uppgifter behandlas av ett personuppgiftsbiträde, bör hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt mellan personuppgiftsbiträdet och den personuppgiftsansvarige, där föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade anges, med beaktande av personuppgiftsbiträdets specifika arbets- och ansvarsuppgifter inom ramen för den behandling som ska utföras och risken med avseende på den registrerades rättigheter och friheter. Den personuppgiftsansvarige och personuppgiftsbiträdet får välja att använda sig av ett enskilt avtal eller standardavtalsklausuler som antingen antas direkt av kommissionen eller av en tillsynsmyndighet i enlighet med mekanismen för enhetlighet och därefter antas av kommissionen. Efter det att behandlingen på den personuppgiftsansvariges vägnar har avslutats, bör personuppgiftsbiträdet återlämna eller radera personuppgifterna, beroende på vad den personuppgiftsansvarige väljer, såvida inte lagring av personuppgifterna krävs enligt den unionsrätt eller medlemsstaternas nationella rätt som personuppgiftsbiträdet omfattas av.

(82) För att påvisa att denna förordning följs bör de personuppgiftsansvariga eller personuppgiftsbiträdena föra register över behandling som sker under deras ansvar. Alla personuppgiftsansvariga och personuppgiftsbiträden bör vara skyldiga att samarbeta med tillsynsmyndigheten och på dennas begäran göra detta register tillgängligt, så att det kan tjäna som grund för övervakningen av behandlingen.

(83) För att upprätthålla säkerheten och förhindra behandling som bryter mot denna förordning bör personuppgiftsansvariga eller personuppgiftsbiträden utvärdera riskerna med behandlingen och vidta åtgärder, såsom kryptering, för att minska dem. Åtgärderna bör säkerställa en lämplig säkerhetsnivå, inbegripet konfidentialitet, med beaktande av den senaste utvecklingen och genomförandekostnader i förhållande till riskerna och vilken typ av personuppgifter som ska skyddas. Vid bedömningen av datasäkerhetsrisken bör man även beakta de risker som personuppgiftsbehandling medför, såsom förstöring, förlust eller ändringar genom olyckshändelse eller otillåtna handlingar eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, framför allt när denna kan medföra fysisk, materiell eller immateriell skada.

(84) I syfte att säkra för bättre efterlevnad av denna förordning när behandlingen sannolikt kan innebära en hög risk för fysiska personers rättigheter och friheter, bör den personuppgiftsansvarige vara ansvarig för att en konsekvensbedömning utförs avseende datasskydd för att bedöma framför allt riskens ursprung, art, särdrag och allvar. Resultatet av denna bedömning bör beaktas vid fastställandet av de lämpliga åtgärder som ska vidtas för att visa att behandlingen av personuppgifter är förenlig med denna förordning. I de fall en konsekvensbedömning avseende dataskydd ger vid handen att uppgiftsbehandlingen medför en hög risk, som den personuppgiftsansvarige inte kan begränsa genom lämpliga åtgärder med avseende på tillgänglig teknik och genomförandekostnader, bör ett samråd med tillsynsmyndigheten ske före behandlingen.

(85) En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan för fysiska personer leda till fysisk, materiell eller immateriell skada, såsom förlust av kontrollen över de egna personuppgifterna eller till begränsning av deras rättigheter, diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, obehörigt hävande av pseudonymisering, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, eller till annan ekonomisk eller social nackdel för den berörda fysiska personen. Så

snart en personuppgiftsansvarig blir medveten om att en personuppgiftsincident har inträffat, bör den personuppgiftsansvarige därför anmäla personuppgiftsincidenten till tillsynsmyndigheten utan onödigt dröjsmål och, om så är möjligt, inom 72 timmar efter att ha blivit medveten om denna, om inte den personuppgiftsansvarige, i enlighet med ansvarsprincipen, kan påvisa att det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter. Om en sådan anmälan inte kan ske inom 72 timmar, bör skälen till fördröjningen åtfölja anmälan och information får lämnas i omgångar utan otillbörligt vidare dröjsmål.

(86) Den personuppgiftsansvarige bör utan onödigt dröjsmål underrätta den registrerade om en personuppgiftsincident, om personuppgiftsincidenten sannolikt kommer att medföra en hög risk för den fysiska personens rättigheter och friheter, så att denne kan vidta nödvändiga försiktighetsåtgärder. Denna underrättelse bör beskriva personuppgiftsincidentens art samt innehålla rekommendationer för den berörda fysiska personen om hur de potentiella negativa effekterna kan mildras. De registrerade bör underrättas så snart detta rimligtvis är möjligt, i nära samarbete med tillsynsmyndigheten och i enlighet med den vägledning som lämnats av den eller andra relevanta myndigheter, exempelvis brottsbekämpande myndigheter. Till exempel kräver behovet av att mildra en omedelbar skaderisk att de registrerade underrättas omedelbart, medan behovet av att vidta lämpliga åtgärder vid fortlöpande eller likartade personuppgiftsincidenter däremot kan motivera längre tid för underrättelsen.

(87) Det bör undersökas huruvida alla lämpliga tekniska skyddsåtgärder och alla lämpliga organisatoriska åtgärder har vidtagits för att omedelbart fastställa om en personuppgiftsincident har ägt rum och skyndsamt informera tillsynsmyndigheten och den registrerade. Att en anmälan gjordes utan onödigt dröjsmål bör fastställas med hänsyn tagen bl.a. till personuppgiftsincidentens art och svårighetsgrad och dess följder och negativa effekter för den registrerade. En sådan anmälan kan leda till ett ingripande från tillsynsmyndighetens sida i enlighet med dess uppgifter och befogenheter enligt denna förordning.

(88) När ingående regler fastställs för format och förfaranden för anmälan av personuppgiftsincidenter, bör vederbörlig hänsyn tas till omständigheterna kring incidenten, däribland om personuppgifterna var skyddade av lämpliga tekniska skyddsåtgärder, som betydligt begränsar sannolikheten för identitetsbedrägeri eller andra former av missbruk. Dessutom bör sådana regler och förfaranden beakta brottsbekämpande myndigheters berättigade intressen, där en för tidig redovisning kan riskera att i onödan hämma utredning av omständigheterna kring en personuppgiftsincident.

(89) Direktiv 95/46/EG föreskrev en allmän skyldighet att anmäla behandling av personuppgifter till tillsynsmyndigheterna. Denna skyldighet medförde administrativa och ekonomiska bördor, men förbättrade inte alltid personuppgiftsskyddet. Sådana övergripande och allmänna anmälningsskyldigheter bör därför avskaffas och ersättas av effektiva förfaranden och mekanismer som i stället inriktas på de typer av behandlingar som sannolikt innebär en hög risk för fysiska personers rättigheter och friheter, i kraft av deras art, omfattning, sammanhang och ändamål. Dessa behandlingar kan vara sådana som särskilt inbegriper användning av ny teknik eller är av en ny typ, för vilken konsekvensbedömning avseende uppgiftsskydd inte tidigare har genomförts av den personuppgiftsansvarige, eller som blir nödvändiga på grund av den tid som har förflutit sedan den ursprungliga behandlingen.

(90) I sådana fall bör den personuppgiftsansvarige före behandlingen, med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt upphovet till risken, göra en konsekvensbedömning avseende dataskydd i syfte att bedöma den höga riskens specifika sannolikhetsgrad och allvar samt dess ursprung. Konsekvensbedömningen bör främst innefatta de planerade åtgärder, skyddsåtgärder och mekanismer som ska minska denna risk, säkerställa personuppgiftskyddet och visa att denna förordning efterlevs.

(91) Detta bör särskilt vara tillämpligt på storskalig uppgiftsbehandling med syftet att behandla betydande mängder personuppgifter på regional, nationell eller övernationell nivå, vilket skulle kunna påverka ett stort antal registrerade och sannolikt kommer att innebära en hög risk, exempelvis till följd av uppgifternas känsliga natur, där i enlighet med den uppnådda nivån av teknisk kunskap en ny teknik används storskaligt, samt på annan behandling som innebär en hög risk för registrerades rättigheter och friheter, framför allt när denna behandling gör det svårare för de registrerade att utöva sina rättigheter. En konsekvensbedömning avseende dataskydd bör

också göras, där personuppgifter behandlas i syfte att fatta beslut om specifika fysiska personer efter en systematisk och omfattande bedömning av fysiska personers personliga aspekter på grundval av profilering av dessa uppgifter eller efter behandling av särskilda kategorier av personuppgifter, biometriska uppgifter eller uppgifter om fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder. Likaså krävs en konsekvensbedömning avseende dataskydd för övervakning av allmän plats i stor omfattning, särskilt vid användning av optisk-elektroniska anordningar, eller för all annan behandling där den behöriga tillsynsmyndigheten anser att behandlingen sannolikt kommer att innebära en hög risk för de registrerades rättigheter och friheter, framför allt på grund av att den hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal eller på grund av att den systematiskt genomförs i stor omfattning. Behandling av personuppgifter bör inte anses vara storskalig, om det är fråga om personuppgifter från patienter eller klienter som behandlas av enskilda läkare, andra yrkesverksamma på hälsoområdet eller juridiska ombud. I dessa fall bör en konsekvensbedömning avseende dataskydd inte vara obligatorisk.

(92) Ibland kan det vara förnuftigt och ekonomiskt att en konsekvensbedömning avseende dataskydd inriktar sig på ett vidare område än ett enda projekt, exempelvis när myndigheter eller organ avser att skapa en gemensam tillämpnings- eller behandlingsplattform eller när flera personuppgiftsansvariga planerar att införa en gemensam tillämpnings- eller behandlingsmiljö för en hel bransch eller ett helt segment eller för en allmänt utnyttjad horisontell verksamhet.

(93) Medlemsstaterna kan anse det nödvändigt att genomföra en sådan bedömning före behandlingen i samband med antagandet av medlemsstaters nationella rätt som ligger till grund för utförandet av myndighetens eller det offentliga organets uppgifter och reglerar den aktuella specifika behandlingsåtgärden eller serien av åtgärder.

(94) Om det av en konsekvensbedömning avseende dataskydd framgår att behandlingen utan skyddsåtgärder, säkerhetsåtgärder och mekanismer för att minska risken kommer att innebära en hög risk för fysiska personers rättigheter och friheter, och den personuppgiftsansvarige anser att risken inte kan begränsas genom åtgärder som är rimliga med avseende på tillgänglig teknik och genomförandekostnader, bör samråd hållas med tillsynsmyndigheten innan behandlingen inleds. En sådan hög risk kommer sannolikt att orsakas av vissa typer av behandling samt av en viss omfattning och frekvens för behandlingen, vilket även kan leda till skador för eller kränkningar av fysiska personers rättigheter och friheter. Tillsynsmyndigheten bör inom en fastställd tid svara på en begäran om samråd. Ett uteblivet svar från tillsynsmyndigheten inom denna tid bör dock inte hindra ett eventuellt ingripande från tillsynsmyndighetens sida i enlighet med dess uppgifter och befogenheter enligt denna förordning, inbegripet befogenheten att förbjuda behandling. Som en del av denna samrådsprocess får resultatet av en konsekvensbedömning avseende dataskydd som utförs med avseende på behandlingen i fråga överlämnas till tillsynsmyndigheten, framför allt de åtgärder som planeras för att minska risken för fysiska personers rättigheter och friheter.

(95) Personuppgiftsbiträdet bör vid behov och på begäran bistå den personuppgiftsansvarige med fullgörande av de skyldigheter som härrör från utförandet av konsekvensbedömningar avseende dataskydd och förhandssamråd med tillsynsmyndigheten.

(96) Ett samråd med tillsynsmyndigheten bör även ske som ett led i det förberedande arbetet med en lagstiftningsåtgärd som stadgar om behandling av personuppgifter i syfte att säkerställa att den avsedda behandlingen överensstämmer med denna förordning och framför allt för att minska den risk den medför för den registrerade.

(97) När en behandling utförs av en myndighet, med undantag av domstolar eller oberoende rättsliga myndigheter som en del av deras dömande verksamhet, eller när en behandling utförs i den privata sektorn av en personuppgiftsansvarig vars kärnverksamhet består av behandlingsverksamhet som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller när den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av personuppgifter och uppgifter som rör fällande domar i brottmål och överträdelser, bör en person med sakkunskap i fråga om dataskyddslagstiftning och -förfaranden bistå den personuppgiftsansvarige eller personuppgiftsbiträdet för att övervaka den interna efterlevnaden av denna förordning. I den privata sektorn avser personuppgiftsansvarigas kärnverksamhet deras primära verksamhet och inte behandling av personuppgifter som kompletterande verksamhet. Den nödvändiga nivån på sakkunskapen bör fastställas särskilt i enlighet med den uppgiftsbehandling

som utförs och det skydd som krävs för de personuppgifter som behandlas av den personuppgiftsansvarige eller personuppgiftsbiträdet. Denna typ av dataskyddsombud bör, oavsett om de är anställda av den personuppgiftsansvarige eller ej, kunna fullgöra sitt uppdrag och utföra sina uppgifter på ett oberoende sätt.

(98) Sammanslutningar eller andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden bör uppmuntras att utarbeta uppförandekoder inom gränserna för denna förordning, så att tillämpningen av denna förordning effektiviseras, med beaktande av särdragen hos den behandling som sker inom vissa sektorer och de särskilda behov som finns inom mikroföretag samt inom små och medelstora företag. I synnerhet skulle man genom sådana uppförandekoder kunna anpassa personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter, med beaktande av den risk som behandlingen sannolikt innebär för fysiska personers rättigheter och friheter.

(99) Vid utformningen av en uppförandekod eller vid ändring eller utvidgning av en befintlig sådan kod bör sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden samråda med berörda intressenter, i möjligaste mån inbegripet registrerade, och beakta de inlagor som mottas och de åsikter som framförs som svar på samråden.

(100) För att förbättra öppenheten och efterlevnaden av denna förordning bör införandet av certifieringsmekanismer och dataskyddsförsegling och dataskyddsmärkning uppmuntras, så att registrerade snabbt kan bedöma nivån på relevanta produkters och tjänsters dataskydd.

(101) Flöden av personuppgifter till och från länder utanför unionen och till och från internationella organisationer är nödvändiga för utvecklingen av internationell handel och internationellt samarbete. Ökningen av dessa flöden har medfört nya utmaningar och nya farhågor när det gäller skyddet av personuppgifter. Det är viktigt att den skyddsnivå som fysiska personer säkerställs inom unionen genom denna förordning inte undergrävs när personuppgifter överförs från unionen till personuppgiftsansvariga, personuppgiftsbiträden eller andra mottagare i tredjeland eller till internationella organisationer, vilket inbegriper vidarebefordran av personuppgifter från tredjelandet eller den internationella organisationen till personuppgiftsansvariga, personuppgiftsbiträden i samma eller ett annat tredjeland eller en annan internationell organisation. Överföringar till tredjeländer och internationella organisationer får under alla omständigheter endast utföras i full överensstämmelse med denna förordning. En överföring kan endast ske, om de villkor som fastställs i bestämmelserna i denna förordning om överföring av personuppgifter till tredjeländer eller internationella organisationer har uppfyllts av den personuppgiftsansvarige eller personuppgiftsbiträdet, med förbehåll för de övriga bestämmelserna i denna förordning.

(102) Denna förordning påverkar inte internationella avtal mellan unionen och tredjeländer som reglerar överföring av personuppgifter, däribland lämpliga skyddsåtgärder för de registrerade. Medlemsstaterna får ingå internationella avtal som innefattar överföring av personuppgifter till tredjeländer eller internationella organisationer i den mån sådana avtal inte påverkar denna förordning eller andra bestämmelser i unionsrätten och innehåller en skälig nivå av skydd för de registrerades grundläggande rättigheter.

(103) Kommissionen kan med verkan för hela unionen fastställa att ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation erbjuder en adekvat dataskyddsnivå och på så sätt skapa rättslig säkerhet och enhetlighet i hela unionen vad gäller tredjelandet eller den internationella organisationen som anses tillhandahålla en sådan skyddsnivå. I dessa fall får överföringar av personuppgifter till det tredjelandet eller den internationella organisationen ske utan ytterligare tillstånd. Kommissionen kan också, efter att ha underrättat tredjelandet eller den internationella organisationen och lämnat en fullständig motivering, besluta att ett sådant beslut ska återkallas.

(104) I enlighet med de grundläggande värderingar som unionen bygger på, bl.a. skyddet av mänskliga rättigheter, bör kommissionen i sin bedömning av tredjelandet eller ett territorium eller en specificerad sektor i ett tredjeland beakta hur ett visst tredjeland respekterar rättsstatsprincipen, tillgången till rättslig prövning samt internationella människorättsnormer och -standarder samt landets allmänna lagstiftning och sektorslagstiftning, inklusive lagstiftning om allmän säkerhet, försvar och nationell säkerhet samt allmän ordning och straffrätt. Vid antagandet av ett beslut om adekvat skyddsnivå avseende ett territorium eller en specificerad sektor i ett tredjeland bör hänsyn tas till tydliga och objektiva kriterier, t.ex. specifik behandling och tillämpningsområdet för tillämpliga rättsliga standarder och gällande lagstiftning i tredjelandet. Tredjelandet bör erbjuda garantier som säkerställer en

tillfredsställande skyddsnivå som i huvudsak motsvarar den som säkerställs i unionen, i synnerhet när personuppgifter behandlas inom en eller flera specifika sektorer. Tredjelandet bör framför allt säkerställa en effektiv oberoende dataskyddsövervakning och sörja för samarbetsmekanismer med medlemsstaternas dataskyddsmyndigheter, och de registrerade bör tillförsäkras effektiva och lagstadgade rättigheter samt effektiv administrativ och rättslig prövning.

(105) Utöver de internationella åtaganden som tredjelandet eller den internationella organisationen har gjort bör kommissionen beakta de skyldigheter som följer av tredjelandets eller den internationella organisationens deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter och genomförandet av dessa skyldigheter. Framför allt bör tredjelandets anslutning till Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk behandling av personuppgifter och dess tilläggsprotokoll beaktas. Kommissionen bör samråda med styrelsen vid bedömningen av skyddsnivån i tredjeländer eller internationella organisationer.

(106) Kommissionen bör övervaka hur beslut om skyddsnivå i ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation fungerar, och övervaka hur beslut som antas på grundval av artikel 25.6 eller 26.4 i direktiv 95/46/EG fungerar. Kommissionen bör i sina beslut om adekvat skyddsnivå föreskriva en mekanism för periodisk översyn av hur de fungerar. Denna periodiska översyn bör genomföras i samråd med det berörda tredjelandet eller den berörda internationella organisationen, med beaktande av all relevant utveckling i tredjelandet eller den internationella organisationen. Vid övervakningen och genomförandet av den periodiska översynen bör kommissionen ta hänsyn till synpunkter och resultat från Europaparlamentet och rådet samt andra relevanta organ och källor. Kommissionen bör inom rimlig tid utvärdera hur de sistnämnda besluten fungerar och rapportera alla relevanta resultat till den kommitté, i den mening som avses i Europaparlamentets och rådets förordning (EU) nr 182/2011 ( ), som inrättats enligt denna förordning och till Europaparlamentet och rådet.

(107) Kommissionen kan konstatera att ett tredjeland, ett territorium eller en viss specificerad sektor i ett tredjeland eller en internationell organisation inte längre säkerställer en adekvat dataskyddsnivå. Överföring av personuppgifter till detta tredjeland eller till denna internationella organisation bör då förbjudas, såvida inte kraven i denna förordning avseende överföring med stöd av lämpliga skyddsåtgärder, inbegripet bindande företagsbestämmelser och undantag för särskilda situationer, är uppfyllda. I så fall bör det finnas möjlighet till samråd mellan kommissionen och dessa tredjeländer eller internationella organisationer. Kommissionen bör i god tid informera tredjelandet eller den internationella organisationen om skälen och inleda samråd med tredjelandet eller organisationen för att avhjälpa situationen.

(108) Saknas beslut om adekvat skyddsnivå bör den personuppgiftsansvarige eller personuppgiftsbiträdet vidta åtgärder för att kompensera för det bristande dataskyddet i ett tredjeland med hjälp av lämpliga skyddsåtgärder för den registrerade. Sådana lämpliga skyddsåtgärder kan bestå i tillämpning av bindande företagsbestämmelser, standardbestämmelser om dataskydd som antagits av kommissionen, standardbestämmelser om dataskydd som antagits av en tillsynsmyndighet eller avtalsbestämmelser som godkänts av en tillsynsmyndighet. Dessa skyddsåtgärder bör säkerställa iakttagande av de krav i fråga om dataskydd och registrerades rättigheter som är lämpliga för behandling inom unionen, inbegripet huruvida bindande rättigheter för de registrerade och effektiva rättsmedel är tillgängliga, inbegripet en faktisk rätt att föra talan på administrativ väg eller inför domstol och att kräva kompensation i unionen eller i ett tredjeland. De bör särskilt gälla överensstämmelse med allmänna principer för behandling av personuppgifter samt principerna om inbyggt dataskydd och dataskydd som standard. Överföring av uppgifter kan också utföras av offentliga myndigheter eller organ till offentliga myndigheter eller organ i tredjeländer eller internationella organisationer med motsvarande skyldigheter eller uppgifter, inbegripet på grundval av bestämmelser som ska införas i administrativa överenskommelser, t.ex. samförståndsavtal, som föreskriver verkställbara och faktiska rättigheter för de registrerade. Tillstånd från den behöriga tillsynsmyndigheten bör erhållas när skyddsåtgärder föreskrivs i icke rättsligt bindande administrativa arrangemang.

(109) Personuppgiftsansvarigas eller personuppgiftsbiträdens möjlighet att använda standardiserade dataskyddsbestämmelser som antagits av kommissionen eller av en tillsynsmyndighet bör inte hindra att de infogar

( ) Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

standardiserade dataskyddsbestämmelser i ett vidare avtal, såsom ett avtal mellan personuppgiftsbiträdet och ett annat personuppgiftsbiträde, eller lägger till andra bestämmelser eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt står i strid med standardavtalsklausuler som antagits av kommissionen eller av en tillsynsmyndighet eller påverkar de registrerades grundläggande rättigheter eller friheter. Personuppgiftsansvariga och personuppgiftsbiträden bör uppmuntras att tillhandahålla ytterligare skyddsåtgärder via avtalsmässiga åtaganden som kompletterar de standardiserade skyddsbestämmelserna.

(110) En koncern eller en grupp av företag som deltar i en gemensam ekonomisk verksamhet bör kunna använda sig av godkända bindande företagsbestämmelser för sina internationella överföringar från unionen till organisationer inom samma koncern eller grupp av företag som deltar i en gemensam ekonomisk verksamhet, under förutsättning att företagsbestämmelserna inbegriper alla nödvändiga principer och bindande rättigheter som säkerställer lämpliga skyddsåtgärder för överföringar eller kategorier av överföringar av personuppgifter.

(111) Det bör införas bestämmelser som ger möjlighet att under vissa omständigheter göra överföringar, om den registrerade har lämnat sitt uttryckliga samtycke, när överföringen är tillfällig och nödvändig med hänsyn till ett avtal eller ett rättsligt anspråk, oavsett om detta sker inom ett rättsligt förfarande eller i ett administrativt eller utomrättsligt förfarande, inbegripet förfaranden inför tillsynsorgan. Det bör också införas bestämmelser som ger möjlighet till överföringar om viktiga allmänintressen fastställda genom unionsrätten eller medlemsstaternas nationella rätt så kräver eller när överföringen görs från ett register som inrättats genom lag och är avsett att konsulteras av allmänheten eller av personer med ett berättigat intresse. I sistnämnda fall bör en sådan överföring inte omfatta alla personuppgifter eller hela kategorier av uppgifter i registret, och överföringen bör endast göras när registret är avsett att vara tillgängligt för personer med ett berättigat intresse, på begäran av dessa personer eller om de själva är mottagarna, med full hänsyn till de registrerades intressen och grundläggande rättigheter.

(112) Dessa undantag bör främst vara tillämpliga på uppgiftsöverföringar som krävs och är nödvändiga med hänsyn till viktiga allmänintressen, exempelvis vid internationella utbyten av uppgifter mellan konkurrensmyndigheter, skatte- eller tullmyndigheter, finanstillsynsmyndigheter, socialförsäkringsmyndigheter eller hälsovårdsmyndigheter, till exempel vid kontaktspårning för smittsamma sjukdomar eller för att minska och/eller undanröja dopning inom idrott. En överföring av personuppgifter bör också betraktas som laglig, om den är nödvändig för att skydda ett intresse som är väsentligt för den registrerades eller en annan persons vitala intressen, inklusive dennes fysiska integritet och liv, om den registrerade är oförmögen att ge sitt samtycke. Saknas beslut om adekvat skyddsnivå får unionsrätten eller medlemsstaternas nationella rätt med hänsyn till viktiga allmänintressen uttryckligen fastställa gränser för överföringen av särskilda kategorier av uppgifter till ett tredjeland eller en internationell organisation. Medlemsstaterna bör underrätta kommissionen om sådana bestämmelser. Varje överföring till en internationell humanitär organisation av personuppgifter rörande en registrerad som är fysiskt eller rättsligt förhindrad att ge sitt samtycke, i syfte att utföra en uppgift inom ramen för Genèvekonventionerna eller vara förenlig med internationell humanitär rätt, vilken är tillämplig vid väpnade konflikter, skulle kunna anses vara nödvändig för ett betydande allmänintresse eller för att den är av vitalt intresse för den registrerade.

(113) Överföringar som kan anses vara icke återkommande och endast gäller ett begränsat antal registrerade kan också vara möjliga när personuppgiftsansvarigas tvingande berättigade intressen motiverar detta, om inte den registrerades intressen eller rättigheter och friheter väger tyngre än dessa intressen, och den personuppgiftsansvarige har bedömt alla omständigheter kring uppgiftsöverföringen. Den personuppgiftsansvarige bör ta särskild hänsyn till personuppgifternas art, den eller de avsedda behandlingarnas ändamål och varaktighet samt situationen i ursprungslandet, tredjelandet och det slutliga bestämmelselandet och bör tillhandahålla lämpliga åtgärder för att skydda fysiska personers grundläggande rättigheter och friheter vid behandlingen av deras personuppgifter. Sådana överföringar bör endast vara möjliga i vissa fall där inget av de andra skälen till överföring är tillämpligt. För vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör hänsyn tas till samhällets legitima förväntningar i fråga om ökad kunskap. Den personuppgiftsansvarige bör informera tillsynsmyndigheten och den registrerade om överföringen.

(114) Om kommissionen inte har fattat beslut om adekvat dataskyddsnivå i ett tredjeland, bör den personuppgiftsansvarige eller personuppgiftsbiträdet i alla fall använda sig av lösningar som ger de registrerade verkställbara och effektiva rättigheter vad gäller behandlingen av deras personuppgifter inom unionen när dessa uppgifter väl har överförts, så att de fortsatt kan utöva sina grundläggande rättigheter och att skyddsåtgärder fortsatt gäller i förhållande till dem.

(115) Vissa tredjeländer antar lagar och andra författningar som syftar till att direkt reglera behandling som genomförs av fysiska och juridiska personer under medlemsstaternas jurisdiktion. Detta kan inkludera rättsliga avgöranden eller beslut av administrativa myndigheter i tredjeländer med krav på att personuppgiftsansvariga eller personuppgiftsbiträden överför eller överlämnar personuppgifter, vilka inte grundar sig på något gällande internationellt avtal, såsom ett fördrag om ömsesidig rättshjälp, mellan det begärande tredjelandet och unionen eller en medlemsstat. Extraterritoriell tillämpning av dessa lagar och andra författningar kan strida mot internationell rätt och inverka menligt på det skydd av fysiska personer som säkerställs inom unionen genom denna förordning. Överföringar bör endast tillåtas om villkoren i denna förordning för en överföring till tredjeländer är uppfyllda. Detta kan vara fallet bl.a. när utlämnande är nödvändigt på grund av ett viktigt allmänintresse som erkänns i unionsrätten eller i medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av.

(116) När personuppgifter förs över gränser utanför unionen kan detta öka risken för att fysiska personer inte kan utöva sina dataskyddsrättigheter, i synnerhet för att skydda sig från otillåten användning eller otillåtet utlämnande av denna information. Samtidigt kan tillsynsmyndigheter finna att de inte är i stånd att handlägga klagomål eller göra utredningar som gäller verksamheter utanför gränserna för deras land. Deras strävan att arbeta tillsammans över gränserna kan också hindras av otillräckliga preventiva eller korrigerande befogenheter, oenhetliga rättsliga regelverk och praktiska hinder, som exempelvis bristande resurser. Närmare samarbete mellan dataskyddstillsynsmyndigheter bör därför främjas för att hjälpa dem att utbyta information och utföra utredningar med sina internationella motparter. I syfte att bygga upp internationella samarbetsmekanismer för att underlätta och tillhandahålla ömsesidig internationell hjälp med att kontrollera efterlevnaden av lagstiftningen till skydd för personuppgifter, bör kommissionen och tillsynsmyndigheterna utbyta information och samarbeta, inom verksamhet som rör utövandet av deras befogenheter, med behöriga myndigheter i tredjeländer, på grundval av ömsesidighet och i överensstämmelse med denna förordning.

(117) Ett väsentligt inslag i skyddet av fysiska personer vid behandlingen av personuppgifter är att medlemsstaterna inrättar tillsynsmyndigheter med behörighet att utföra sina uppgifter och utöva sina befogenheter under fullständigt oberoende. Medlemsstaterna bör kunna inrätta fler än en tillsynsmyndighet om det behövs för att ta hänsyn till den egna konstitutionella, organisatoriska och administrativa strukturen.

(118) Tillsynsmyndigheternas oberoende bör dock inte innebära att deras utgifter inte kan underkastas kontroll- eller övervakningsmekanismer eller bli föremål för domstolsprövning.

(119) Om en medlemsstat inrättar flera tillsynsmyndigheter, bör den genom lagstiftning säkerställa att dessa tillsynsmyndigheter effektivt deltar i mekanismen för enhetlighet. Medlemsstaten bör i synnerhet utnämna en tillsynsmyndighet som fungerar som samlande kontaktpunkt för dessa myndigheters effektiva deltagande i mekanismen för att säkra ett snabbt och smidigt samarbete med övriga tillsynsmyndigheter, styrelsen och kommissionen.

(120) Varje tillsynsmyndighet bör tilldelas de ekonomiska och personella resurser och lokalutrymmen samt den infrastruktur som är nödvändig för att den effektivt ska kunna utföra sina uppgifter, däribland de uppgifter som är knutna till ömsesidigt bistånd och samarbete med övriga tillsynsmyndigheter i hela unionen. Varje tillsynsmyndighet bör ha en separat offentlig årlig budget, som kan ingå i den övergripande statsbudgeten eller nationella budgeten.

(121) De allmänna villkoren för tillsynsmyndighetens ledamot eller ledamöter bör fastställas genom varje medlemsstats lagstiftning och där bör i synnerhet föreskrivas att ledamöterna ska utnämnas genom ett öppet förfarande antingen av medlemsstatens parlament, regering eller statschef, på grundval av ett förslag från regeringen, en ledamot av regeringen, parlamentet eller en av parlamentets kammare eller av ett oberoende organ som enligt medlemsstaternas nationella rätt har anförtrotts utnämningen. I syfte att säkerställa tillsynsmyndighetens oberoende bör ledamoten eller ledamöterna handla med integritet, avstå från alla handlingar som står i strid med deras tjänsteutövning och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet som står i strid med deras uppdrag. Tillsynsmyndigheten bör ha egen personal, som valts ut av tillsynsmyndigheten eller ett oberoende organ som fastställs i medlemsstaternas nationella rätt, vilken uteslutande bör vara underställd tillsynsmyndighetens ledamot eller ledamöter.

(122) Varje tillsynsmyndighet bör ha behörighet att inom sin medlemsstats territorium utöva de befogenheter och utföra de uppgifter som den tilldelats i enlighet med denna förordning. Detta bör framför allt omfatta behandling

inom ramen för verksamhet vid den personuppgiftsansvariges eller personuppgiftsbiträdets verksamhetsställen inom den egna medlemsstatens territorium, behandling av personuppgifter som utförs av myndigheter eller privata organ som agerar i ett allmänt intresse, behandling som påverkar registrerade på dess territorium eller behandling som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen när den rör registrerade som är bosatta på dess territorium. Detta bör inbegripa att hantera klagomål som lämnas in av en registrerad, genomföra undersökningar om tillämpningen av denna förordning samt främja allmänhetens medvetenhet om risker, bestämmelser, skyddsåtgärder och rättigheter när det gäller behandlingen av personuppgifter.

(123) Tillsynsmyndigheterna bör övervaka tillämpningen av bestämmelserna i denna förordning och bidra till att tillämpningen blir enhetlig över hela unionen, för att skydda fysiska personer vid behandling av deras personuppgifter och för att underlätta det fria flödet av personuppgifter inom den inre marknaden. För detta ändamål bör tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen, utan att det behövs något avtal mellan medlemsstaterna om tillhandahållande av ömsesidigt bistånd eller om sådant samarbete.

(124) Om behandlingen av personuppgifter sker inom ramen för verksamhet vid en personuppgiftsansvarigs eller ett personuppgiftsbiträdes verksamhetsställe i unionen och den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat, eller om behandling som sker inom ramen för verksamhet vid ett enda verksamhetsställe tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka registrerade i mer än en medlemsstat, bör tillsynsmyndigheten för den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga verksamhetsställe eller för detta enda verksamhetsställe tillhörande den personuppgiftsansvarige eller personuppgiftsbiträdet agera som ansvarig myndighet. Denna bör samarbeta med de övriga myndigheter som berörs, eftersom den personuppgiftsansvarige eller personuppgiftsbiträdet har ett verksamhetsställe inom deras medlemsstats territorium, eftersom registrerade som är bosatta på deras territorium i väsentlig grad påverkas eller eftersom ett klagomål har lämnats in till dem. Även när en registrerad som inte är bosatt i medlemsstaten har lämnat in ett klagomål, bör den tillsynsmyndighet som klagomålet har lämnats in till också vara en berörd tillsynsmyndighet. Styrelsen bör inom ramen för sina uppgifter kunna utfärda riktlinjer för alla frågor som rör tillämpningen av denna förordning, framför allt för vilka kriterier som ska beaktas för att konstatera om behandlingen i fråga i väsentlig grad påverkar registrerade i mer än en medlemsstat och för vad som utgör en relevant och motiverad invändning.

(125) Den ansvariga myndigheten bör ha behörighet att anta bindande beslut om åtgärder inom ramen för de befogenheter som den tilldelats i enlighet med denna förordning. I egenskap av ansvarig myndighet bör tillsynsmyndigheten nära involvera och samordna de berörda tillsynsmyndigheterna i beslutsfattandet. Om man beslutar att helt eller delvis avslå den registrerades klagomål, bör detta beslut antas av den tillsynsmyndighet som klagomålet har lämnats in till.

(126) Den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna bör gemensamt enas om beslutet, som bör rikta sig till den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga eller enda verksamhetsställe och vara bindande för den personuppgiftsansvarige och personuppgiftsbiträdet. Den personuppgiftsansvarige eller personuppgiftsbiträdet bör vidta de åtgärder som krävs för att säkerställa efterlevnad av denna förordning och genomförande av det beslut som den ansvariga tillsynsmyndigheten har anmält till den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga verksamhetsställe vad gäller behandling i unionen.

(127) Varje tillsynsmyndighet som inte agerar som ansvarig tillsynsmyndighet bör vara behörig att behandla lokala fall, om den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat men ärendet för den specifika behandlingen endast avser behandling som utförs i en enda medlemsstat och endast omfattar registrerade i denna enda medlemsstat, till exempel om ärendet avser behandling av anställdas personuppgifter inom ramen för en medlemsstats specifika anställningsförhållanden. I sådana fall bör tillsynsmyndigheten utan dröjsmål underrätta den ansvariga tillsynsmyndigheten om detta ärende. Efter att ha underrättats bör den ansvariga tillsynsmyndigheten besluta huruvida den kommer att hantera ärendet i enlighet med bestämmelsen om samarbete mellan den ansvariga tillsynsmyndigheten och andra berörda tillsynsmyndigheter (nedan kallad *mekanismen för en enda kontaktpunkt*), eller om den tillsynsmyndighet som underrättade den bör behandla ärendet på lokal nivå. När den ansvariga tillsynsmyndigheten beslutar huruvida den kommer att behandla ärendet, bör den ta hänsyn till om den personuppgiftsansvarige eller personuppgiftsbiträdet har ett verksamhetsställe i den medlemsstat där den tillsynsmyndighet som underrättade den ansvariga myndigheten är belägen för att säkerställa ett effektivt genomförande av ett beslut gentemot den personuppgiftsansvarige eller personuppgiftsbiträdet. När den ansvariga tillsynsmyndigheten beslutar att behandla ärendet, bör den tillsynsmyndighet som underrättade den

ha möjlighet att lämna in ett förslag till beslut, som den ansvariga tillsynsmyndigheten bör ta största möjliga hänsyn till när den utarbetar utkastet till beslut inom ramen för mekanismen för en enda kontaktpunkt.

(128) Bestämmelserna om den ansvariga tillsynsmyndigheten och mekanismen för en enda kontaktpunkt bör inte tillämpas om behandlingen utförs av myndigheter eller privata organ i ett allmänt intresse. I sådana fall bör den enda tillsynsmyndighet som är behörig att utöva de befogenheter som den tilldelas i enlighet med denna förordning vara tillsynsmyndigheten i den medlemsstat där myndigheten eller det privata organet är etablerat.

(129) För att denna förordning ska övervakas och verkställas på ett enhetligt sätt i hela unionen bör tillsynsmyndigheterna i alla medlemsstater ha samma uppgifter och effektiva befogenheter, bl.a. undersökningsbefogenheter, korrigerande befogenheter och befogenheter att ålägga sanktioner samt befogenheter att utfärda tillstånd och ge råd, särskilt vid klagomål från fysiska personer och, utan att det påverkar åklagarmyndigheternas befogenheter enligt medlemsstaternas nationella rätt, att upplysa de rättsliga myndigheterna om överträdelser av denna förordning och delta i rättsliga förfaranden. Dessa befogenheter bör även omfatta en befogenhet att införa en tillfällig eller definitiv begränsning av, inklusive förbud mot, behandling. Medlemsstaterna får fastställa andra uppgifter med anknytning till skyddet av personuppgifter enligt denna förordning. Tillsynsmyndigheternas befogenheter bör utövas opartiskt, rättvist och inom rimlig tid i överensstämmelse med lämpliga rättssäkerhetsgarantier i unionsrätten och i medlemsstaternas nationella rätt. Framför allt bör varje åtgärd vara lämplig, nödvändig och proportionell för att säkerställa efterlevnad av denna förordning, med beaktande av omständigheterna i varje enskilt fall, samt respektera varje persons rätt att bli hörd innan några enskilda åtgärder som påverkar honom eller henne negativt vidtas och vara utformad så att onödiga kostnader och alltför stora olägenheter för de berörda personerna undviks. Undersökningsbefogenheten när det gäller tillträde till lokaler bör utövas i enlighet med särskilda krav i medlemsstaternas nationella processrätt, såsom kravet på att inhämta förhandstillstånd från rättsliga myndigheter. Varje rättsligt bindande åtgärd som vidtas av tillsynsmyndigheten bör vara skriftlig, klar och entydig, innehålla information om vilken tillsynsmyndighet som har utfärdat åtgärden och datum för utfärdandet, vara undertecknad av tillsynsmyndighetens chef eller en av dess ledamöter efter dennes bemyndigande samt innehålla en motivering till åtgärden och en hänvisning till rätten till ett effektivt rättsmedel. Detta bör inte utesluta ytterligare krav enligt medlemsstaternas nationella processrätt. Antagande av ett rättsligt bindande beslut innebär att det kan bli föremål för domstolsprövning i den medlemsstat till vilken den tillsynsmyndighet som antog beslutet hör.

(130) Om den tillsynsmyndighet till vilken klagomålet har ingetts inte är den ansvariga tillsynsmyndigheten, bör den ansvariga tillsynsmyndigheten nära samarbeta med den tillsynsmyndighet till vilken klagomålet har ingetts i enlighet med de bestämmelser om samarbete och enhetlighet som fastställs i denna förordning. I sådana fall bör den ansvariga tillsynsmyndigheten när den vidtar åtgärder avsedda att ha rättsverkan, inbegripet utdömandet av administrativa sanktionsavgifter, ta största hänsyn till synpunkter från den tillsynsmyndighet till vilken klagomålet har ingetts, vilken bör kvarstå som behörig för genomförande av utredningar på den egna medlemsstatens territorium i samverkan med den behöriga tillsynsmyndigheten.

(131) Om en annan tillsynsmyndighet bör agera som ansvarig tillsynsmyndighet för den personuppgiftsansvariges eller personuppgiftsbiträdets behandling men den sakfråga som klagomålet gäller eller den möjliga överträdelsen endast rör den personuppgiftsansvariges eller personuppgiftsbiträdets behandling i den medlemsstat där klagomålet har ingetts eller den eventuella överträdelsen har upptäckts, och frågan inte i väsentlig grad påverkar eller inte sannolikt i väsentlig grad kommer att påverka registrerade i andra medlemsstater, bör den tillsynsmyndighet som mottar ett klagomål eller upptäcker eller på annat sätt informeras om situationer som innebär eventuella överträdelser av denna förordning försöka få till stånd en uppgörelse i godo med den personuppgiftsansvarige och, om detta inte lyckas, utöva sina befogenheter fullt ut. Detta bör omfatta särskild behandling som utförs inom tillsynsmyndighetens medlemsstats territorium eller med avseende på registrerade inom denna medlemsstats territorium, behandling som utförs inom ramen för ett erbjudande om varor eller tjänster som särskilt riktar sig till registrerade inom tillsynsmyndighetens medlemsstats territorium eller behandling som måste bedömas med beaktande av relevanta rättsliga skyldigheter enligt medlemsstaternas nationella rätt.

(132) Medvetandehöjande kampanjer från tillsynsmyndigheters sida riktade till allmänheten bör innefatta särskilda åtgärder riktade dels till personuppgiftsansvariga och personuppgiftsbiträden, inbegripet mikroföretag samt små och medelstora företag, dels till fysiska personer, särskilt i utbildningssammanhang.

(133) Tillsynsmyndigheterna bör hjälpa varandra att utföra sina uppgifter och ge ömsesidigt bistånd så att denna förordning tillämpas och verkställs enhetligt på den inre marknaden. En tillsynsmyndighet som begärt ömsesidigt bistånd får anta en provisorisk åtgärd, om den inte har fått något svar på en begäran om ömsesidigt bistånd inom en månad från det att begäran mottogs av den andra tillsynsmyndigheten.

(134) Alla tillsynsmyndigheter bör om lämpligt delta i gemensamma insatser med andra tillsynsmyndigheter. Den anmodade tillsynsmyndigheten bör vara skyldig att besvara en begäran inom en fastställd tidsperiod.

(135) För att denna förordning ska tillämpas enhetligt i hela unionen bör en mekanism för enhetlighet när det gäller samarbete mellan tillsynsmyndigheterna skapas. Denna mekanism bör främst tillämpas när en tillsynsmyndighet avser att anta en åtgärd som är avsedd att ha rättsverkan gällande behandlingar som i väsentlig grad påverkar ett betydande antal registrerade i flera medlemsstater. Den bör också tillämpas när en berörd tillsynsmyndighet eller kommissionen begär att ett sådant ärende ska hanteras inom ramen för mekanismen för enhetlighet. Mekanismen bör inte påverka åtgärder som kommissionen kan komma att vidta när den utövar sina befogenheter enligt fördragen.

(136) Vid tillämpningen av mekanismen för enhetlighet bör styrelsen inom en fastställd tidsperiod avge ett yttrande, om en majoritet av dess ledamöter så beslutar eller om någon berörd tillsynsmyndighet eller kommissionen begär detta. Styrelsen bör också ges befogenhet att anta rättsligt bindande beslut vid tvister mellan tillsynsmyndigheter. För detta ändamål bör den, normalt med två tredjedelars majoritet av sina ledamöter, utfärda rättsligt bindande beslut i tydligt fastställda fall då tillsynsmyndigheter har olika uppfattningar, framför allt när det gäller mekanismen för samarbete mellan den ansvariga tillsynsmyndigheten och berörda tillsynsmyndigheter om sakförhållandena, i synnerhet om huruvida denna förordning har överträtts.

(137) Det kan uppstå brådskande behov att agera för att skydda registrerades rättigheter och friheter, särskilt när fara föreligger att säkerställandet av en registrerad persons rättighet kan komma att försvåras avsevärt. En tillsynsmyndighet bör därför kunna vidta vederbörligen motiverade provisoriska åtgärder inom sitt territorium med en viss giltighetsperiod, som inte bör överskrida tre månader.

(138) Tillämpningen av en sådan mekanism bör vara ett villkor för lagligheten av en åtgärd som är avsedd att ha rättsverkan och som vidtas av tillsynsmyndigheten i de fall där denna tillämpning är obligatorisk. I andra ärenden som inbegriper flera länder bör samarbetsmekanismen mellan den ansvariga tillsynsmyndigheten och berörda tillsynsmyndigheter tillämpas, och ömsesidigt bistånd och gemensamma insatser kan utföras mellan de berörda tillsynsmyndigheterna på bilateral eller multilateral basis utan att mekanismen för enhetlighet utlöses.

(139) I syfte att främja en enhetlig tillämpning av denna förordning bör styrelsen inrättas som ett oberoende unionsorgan. För att styrelsen ska kunna uppfylla sina mål bör den vara en juridisk person. Styrelsen bör företrädas av sin ordförande. Den bör ersätta arbetsgruppen för skydd av fysiska personer med avseende på behandlingen av personuppgifter, som inrättades genom direktiv 95/46/EG. Den bör bestå av chefen för en tillsynsmyndighet i varje medlemsstat och Europeiska datatillsynsmannen eller deras respektive företrädare. Kommissionen bör delta i styrelsens verksamhet utan att ha rösträtt, och Europeiska datatillsynsmannen bör ha specifik rösträtt. Styrelsen bör bidra till denna förordnings enhetliga tillämpning i hela unionen, bl.a. genom att lämna råd till kommissionen, särskilt vad gäller skyddsnivån i tredjeländer eller internationella organisationer, och främja samarbetet mellan tillsynsmyndigheterna i hela unionen. Styrelsen bör agera oberoende när den utför sina uppgifter.

(140) Styrelsen bör biträdas av ett sekretariat som tillhandahålls av Europeiska datatillsynsmannen. Den personal vid Europeiska datatillsynsmannen som medverkar i utförandet av de uppgifter som enligt denna förordning anförtros styrelsen bör för sina uppgifter uteslutande ta emot instruktioner från styrelsens ordförande och rapportera till denne.

(141) Alla registrerade bör ha rätt att lämna in ett klagomål till en enda tillsynsmyndighet, särskilt i den medlemsstat där den registrerade har sin hemvist, och ha rätt till ett effektivt rättsmedel i enlighet med artikel 47 i stadgan,

om den registrerade anser att hans eller hennes rättigheter enligt denna förordning har kränkts eller om tillsynsmyndigheten inte reagerar på ett klagomål, helt eller delvis avslår eller avvisar ett klagomål eller inte agerar när så är nödvändigt för att skydda den registrerades rättigheter. Utredningen av ett klagomål bör, med förbehåll för eventuell domstolsprövning, ske i den utsträckning som är lämplig i det enskilda fallet. Tillsynsmyndigheten bör inom rimlig tid informera den registrerade om hur arbetet med klagomålet fortskrider och vad resultatet blir. Om ärendet fordrar ytterligare utredning eller samordning med en annan tillsynsmyndighet, bör den registrerade underrättas även om detta. För att förenkla inlämningen av klagomål bör varje tillsynsmyndighet vidta åtgärder, såsom att tillhandahålla ett formulär för inlämnande av klagomål som även kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.

(142) Om en registrerad anser att hans eller hennes rättigheter enligt denna förordning har kränkts, bör han eller hon ha rätt att ge mandat till ett organ, en organisation eller en sammanslutning som drivs utan vinstsyfte och som har inrättats i enlighet med en medlemsstats nationella rätt, som har stadgeenliga mål av allmänt intresse och bedriver verksamhet på området skydd av personuppgifter, att på hans eller hennes vägnar lämna in ett klagomål till en tillsynsmyndighet, om detta föreskrivs i medlemsstatens nationella rätt, att på den registrerades vägnar utöva rätten till domstolsprövning eller att på den registrerades vägnar utöva rätten att ta emot ersättning. En medlemsstat får föreskriva att ett sådant organ, en sådan organisation eller en sådan sammanslutning ska ha rätt att lämna in ett klagomål i den medlemsstaten, oberoende av en registrerad persons mandat, och ha rätt till ett effektivt rättsmedel, om det eller den har skäl att anse att en registrerad persons rättigheter har kränkts till följd av behandling av personuppgifter som strider mot denna förordning. Detta organ, denna organisation eller denna sammanslutning får inte ges rätt att kräva ersättning på en registrerad persons vägnar oberoende av den registrerades mandat.

(143) Varje fysisk eller juridisk person har rätt att väcka ogiltighetstalan mot styrelsens beslut vid domstolen enligt de villkor som föreskrivs i artikel 263 i EUF-fördraget. I sin egenskap av adressater för sådana beslut måste, i enlighet med artikel 263 i EUF-fördraget, de berörda tillsynsmyndigheter som önskar överklaga dessa väcka talan inom två månader efter det att beslutet meddelats dem. Om styrelsens beslut direkt och personligen berör en personuppgiftsansvarig, ett personuppgiftsbiträde eller en enskild, kan den enskilde väcka ogiltighetstalan mot besluten inom två månader efter det att de har offentliggjorts på styrelsens webbplats, i enlighet med artikel 263 i EUF-fördraget. Utan att det påverkar denna rätt inom ramen för artikel 263 i EUF-fördraget bör varje fysisk eller juridisk person ha rätt till ett effektivt rättsmedel vid den behöriga nationella domstolen mot ett beslut av en tillsynsmyndighet som har rättsliga följder för denna person. Sådana beslut avser särskilt tillsynsmyndighetens utövande av utrednings-, korrigerings- och godkännandebefogenheter eller avvisande av eller avslag på klagomål. Rätten till ett effektivt rättsmedel inbegriper dock inte åtgärder som vidtagits av tillsynsmyndigheter när dessa inte är rättsligt bindande, såsom yttranden som avgivits eller rådgivning som tillhandahållits av tillsynsmyndigheten. Talan mot beslut som har fattats av en tillsynsmyndighet bör väckas vid domstolarna i den medlemsstat där tillsynsmyndigheten har sitt säte och bör genomföras i enlighet med den medlemsstatens nationella processrätt. Dessa domstolar bör ha fullständig behörighet, vilket bör omfatta behörighet att pröva alla fakta och rättsliga frågor som rör den tvist som anhängiggjorts vid dem.

Om talan avslås eller avvisas av en tillsynsmyndighet, kan den enskilde väcka talan vid domstolarna i samma medlemsstat. I samband med rättsmedel som avser tillämpningen av denna förordning kan eller, i det fall som anges i artikel 267 i EUF-fördraget, måste nationella domstolar som anser att ett beslut om ett förhandsavgörande är nödvändigt för att de ska kunna döma begära att domstolen meddelar ett förhandsavgörande om tolkningen av unionsrätten, inbegripet denna förordning. Om dessutom ett beslut av en tillsynsmyndighet om genomförande av ett beslut av styrelsen överklagas till en nationell domstol och giltigheten av styrelsens beslut ifrågasätts, har inte den nationella domstolen befogenhet att förklara styrelsens beslut ogiltigt utan måste hänskjuta frågan om giltighet till domstolen i enlighet med artikel 267 i EUF-fördraget såsom den tolkats av domstolen, närhelst den anser att beslutet är ogiltigt. En nationell domstol får dock inte hänskjuta en fråga om giltigheten av styrelsens beslut på begäran av en fysisk eller juridisk person som haft tillfälle att väcka ogiltighetstalan mot beslutet, i synnerhet inte om denna person direkt och personligen berördes av beslutet men inte gjorde detta inom den frist som anges i artikel 263 i EUF-fördraget.

(144) Om en domstol där ett förfarande inletts mot beslut som har fattats av en tillsynsmyndighet har skäl att tro att ett förfarande rörande samma behandling, såsom samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller samma personuppgiftsbiträde, eller samma händelseförlopp, har inletts vid en annan behörig domstol i en annan medlemsstat, bör den kontakta denna domstol i syfte att bekräfta förekomsten av sådana relaterade förfaranden. Om relaterade förfaranden pågår vid en domstol i en annan medlemsstat får alla andra

domstolar än den domstol där förfarandet först inleddes låta förfarandena vila eller på en av parternas begäran förklara sig obehöriga till förmån för den domstol där förfarandet först inleddes, om den domstolen har behörighet i förfarandet i fråga och dess lagstiftning tillåter förening av sådana relaterade förfaranden. Förfarandena anses vara relaterade, om de är så nära förenade att en gemensam handläggning och dom är påkallad för att undvika att oförenliga domar meddelas som en följd av att förfarandena prövas i olika rättegångar.

(145) När det gäller ett rättsligt förfarande mot en personuppgiftsansvarig eller ett personuppgiftsbiträde bör käranden kunna välja att väcka talan antingen vid domstolarna i de medlemsstater där den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad eller där den registrerade är bosatt, såvida inte den personuppgiftsansvarige är en myndighet i en medlemsstat som agerar inom ramen för sin myndighetsutövning.

(146) Den personuppgiftsansvarige eller personuppgiftsbiträdet bör ersätta all skada som en person kan komma att lida till följd av behandling som strider mot denna förordning. Den personuppgiftsansvarige eller personuppgiftsbiträdet bör dock befrias från skadeståndsskyldighet om den kan visa att den inte på något sätt är ansvarig för skadan. Begreppet skada bör tolkas brett mot bakgrund av domstolens rättspraxis på ett sätt som fullt ut återspeglar denna förordnings mål. Detta påverkar inte skadeståndsanspråk till följd av överträdelser av andra bestämmelser i unionsrätten eller i medlemsstaternas nationella rätt. Behandling som strider mot denna förordning omfattar även behandling som strider mot delegerade akter och genomförandeakter som antagits i enlighet med denna förordning och medlemsstaternas nationella rätt med närmare specifikation av denna förordnings bestämmelser. Registrerade bör få full och effektiv ersättning för den skada de lidit. Om personuppgiftsansvariga eller personuppgiftsbiträden medverkat vid samma behandling, bör varje personuppgiftsansvarig eller personuppgiftsbiträde hållas ansvarig för hela skadan. Om de är förenade i samma rättsliga förfarande i enlighet med medlemsstaternas nationella rätt, kan ersättningen dock fördelas i enlighet med varje personuppgiftsansvarigs eller personuppgiftsbiträdes ansvar för den genom behandlingen uppkomna skadan, förutsatt att den registrerade som lidit skada tillförsäkras full och effektiv ersättning. Varje personuppgiftsansvarig eller personuppgiftsbiträde som har betalat full ersättning får därefter inleda förfaranden för återkrav mot andra personuppgiftsansvariga eller personuppgiftsbiträden som medverkat vid samma behandling.

(147) Om särskilda bestämmelser om behörighet fastställs i denna förordning, framför allt vad gäller förfaranden för att begära rättslig prövning som inbegriper ersättning mot en personuppgiftsansvarig eller ett personuppgiftsbiträde, bör inte allmänna bestämmelser om behörighet, såsom bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 1215/2012 ( ), påverka tillämpningen av sådana särskilda bestämmelser.

(148) För att stärka verkställigheten av denna förordning bör det utdömas sanktioner, inbegripet administrativa sanktionsavgifter, för överträdelser av denna förordning utöver eller i stället för de lämpliga åtgärder som tillsynsmyndigheten vidtar i enlighet med denna förordning. Vid en mindre överträdelse eller om den sanktionsavgift som sannolikt skulle utdömas skulle innebära en oproportionell börda för en fysisk person får en reprimand utfärdas i stället för sanktionsavgifter. Vederbörlig hänsyn bör dock tas till överträdelsens karaktär, svårighetsgrad och varaktighet och huruvida den har skett uppsåtligen, vilka åtgärder som vidtagits för att lindra skadan, graden av ansvar eller eventuella tidigare överträdelser av relevans, det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, efterlevnad av åtgärder som förordnats mot den personuppgiftsansvarige eller personuppgiftsbiträdet, tillämpning av en uppförandekod och eventuella andra försvårande eller förmildrande faktorer. Utdömandet av sanktioner, inbegripet administrativa sanktionsavgifter, bör underkastas adekvata rättssäkerhetsgarantier i överensstämmelse med allmänna principer inom unionsrätten och stadgan, vilket inbegriper ett effektivt rättsligt skydd och korrekt rättsligt förfarande.

(149) Medlemsstaterna bör kunna fastställa bestämmelser om straffrättsliga påföljder för överträdelser av denna förordning, inbegripet för överträdelser av nationella bestämmelser som antagits i enlighet med och inom ramen för denna förordning. Dessa straffrättsliga påföljder kan även inbegripa en möjlighet att förverka den vinning som gjorts genom överträdelser av denna förordning. Utdömandet av straffrättsliga påföljder för överträdelser av sådana nationella bestämmelser och administrativa sanktioner bör dock inte medföra ett åsidosättande av principen ne bis in idem enligt domstolens tolkning.

(150) För att förstärka och harmonisera de administrativa sanktionerna för överträdelser av denna förordning bör samtliga tillsynsmyndigheter ha befogenhet att utfärda administrativa sanktionsavgifter. Det bör i denna

( ) Europaparlamentets och rådets förordning (EU) nr 1215/2012 av den 12 december 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttens område (EUT L 351, 20.12.2012, s. 1).

förordning anges vilka överträdelserna är, den övre gränsen för och kriterierna för fastställande av de administrativa sanktionsavgifterna, som i varje enskilt fall bör bestämmas av den behöriga tillsynsmyndigheten med beaktande av alla relevanta omständigheter i det särskilda fallet, med vederbörlig hänsyn bl.a. till överträdelsens karaktär, svårighetsgrad och varaktighet samt till dess följder och till de åtgärder som vidtas för att sörja för fullgörandet av skyldigheterna enligt denna förordning och för att förebygga eller lindra konsekvenserna av överträdelsen. Om de administrativa sanktionsavgifterna åläggs ett företag, bör ett företag i detta syfte anses vara ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget. Om de administrativa sanktionsavgifterna åläggs personer som inte är ett företag, bör tillsynsmyndigheten ta hänsyn till den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation, när den överväger lämplig sanktionsavgift. Mekanismen för enhetlighet kan också tillämpas för att främja en enhetlig tillämpning av administrativa sanktionsavgifter. Medlemsstaterna bör fastställa om och i vilken utsträckning myndigheter ska omfattas av administrativa sanktionsavgifter. Utfärdande av administrativa sanktionsavgifter eller utdelning av en varning påverkar inte tillämpningen av tillsynsmyndigheternas övriga befogenheter eller av andra sanktioner enligt denna förordning.

(151) Danmarks och Estlands rättssystem tillåter inte administrativa sanktionsavgifter i enlighet med denna förordning. Bestämmelserna om administrativa sanktionsavgifter kan tillämpas så att sanktionsavgiften i Danmark utdöms som en straffrättslig påföljd av en behörig nationell domstol och att den i Estland utdöms av tillsynsmyndigheten inom ramen för ett förseelseförfarande, under förutsättning att en sådan tillämpning av bestämmelserna i dessa medlemsstater har en effekt som är likvärdig med administrativa sanktionsavgifter som utdöms av tillsynsmyndigheter. De behöriga nationella domstolarna bör därför beakta rekommendationen från den tillsynsmyndighet som initierar sanktionsavgiften. De sanktionsavgifter som utdöms bör i alla händelser vara effektiva, proportionella och avskräckande.

(152) Om denna förordning inte harmoniserar administrativa sanktioner eller om nödvändigt i andra fall, till exempel vid fall av allvarliga överträdelser av denna förordning, bör medlemsstaterna genomföra ett system med effektiva, proportionella och avskräckande sanktioner. Dessa sanktioners art, straffrättsliga eller administrativa, bör fastställas i medlemsstaternas nationella rätt.

(153) Medlemsstaterna bör i sin lagstiftning sammanjämka bestämmelserna om yttrandefrihet och informationsfrihet, vilket inbegriper journalistiska, akademiska, konstnärliga och/eller litterära uttrycksformer, med rätten till skydd av personuppgifter i enlighet med denna förordning. Behandling av personuppgifter enbart för journalistiska, akademiska, konstnärliga eller litterära ändamål bör undantas från vissa av kraven i denna förordning, så att rätten till skydd av personuppgifter vid behov kan förenas med rätten till yttrandefrihet och informationsfrihet, som följer av artikel 11 i stadgan. Detta bör särskilt gälla vid behandling av personuppgifter inom det audiovisuella området och i nyhetsarkiv och pressbibliotek. Medlemsstaterna bör därför anta lagstiftningsåtgärder som fastställer de olika undantag som behövs för att skapa en balans mellan dessa grundläggande rättigheter. Medlemsstaterna bör fastställa sådana undantag med avseende på allmänna principer, de registrerades rättigheter, personuppgiftsansvariga och personuppgiftsbiträden, överföring av uppgifter till tredjeländer eller internationella organisationer, de oberoende tillsynsmyndigheterna, samarbete och enhetlighet samt specifika situationer där personuppgifter behandlas. Om sådana undantag varierar från en medlemsstat till en annan, ska den nationella rätten i den medlemsstat vars lag den personuppgiftsansvarige omfattas av tillämpas. För att beakta vikten av rätten till yttrandefrihet i varje demokratiskt samhälle måste det göras en bred tolkning av vad som innefattas i denna frihet, som till exempel journalistik.

(154) Denna förordning gör det möjligt att vid tillämpningen av den ta hänsyn till principen om allmänhetens rätt att få tillgång till allmänna handlingar. Allmänhetens rätt att få tillgång till allmänna handlingar kan betraktas som ett allmänt intresse. Personuppgifter i handlingar som innehas av en myndighet eller ett offentligt organ bör kunna lämnas ut offentligt av denna myndighet eller detta organ, om utlämning stadgas i unionsrätten eller i medlemsstatens nationella rätt som är tillämplig på myndigheten eller det offentliga organet. Denna rätt bör sammanjämka allmänhetens rätt att få tillgång till allmänna handlingar och vidareutnyttjande av information från den offentliga sektorn med rätten till skydd av personuppgifter och får därför innehålla föreskrifter om den nödvändiga sammanjämkningen med rätten till skydd av personuppgifter enligt denna förordning. Hänvisningen till offentliga myndigheter och organ bör i detta sammanhang omfatta samtliga myndigheter eller andra organ som omfattas av medlemsstaternas nationella rätt om allmänhetens tillgång till handlingar. Europaparlamentets och rådets direktiv 2003/98/EG ( ) ska inte på något sätt påverka skyddsnivån för fysiska personer med avseende

( ) Europaparlamentets och rådets direktiv 2003/98/EG av den 17 november 2003 om vidareutnyttjande av information från den offentliga sektorn (EUT L 345, 31.12.2003, s. 90).

på behandling av personuppgifter enligt bestämmelserna i unionsrätten och i medlemsstaternas nationella rätt och i synnerhet ändras inte de skyldigheter och rättigheter som anges i denna förordning genom det direktivet. I synnerhet ska direktivet inte vara tillämpligt på handlingar till vilka, med hänsyn till skyddet av personuppgifter, tillgång enligt tillgångsbestämmelserna är utesluten eller begränsad eller på delar av handlingar som är tillgängliga enligt dessa bestämmelser men som innehåller personuppgifter vilkas vidareutnyttjande i lag har fastställts som oförenligt med lagstiftningen om skydd för fysiska personer vid behandling av personuppgifter.

(155) En medlemsstatsnationella rätt eller kollektivavtal, inbegripet ”verksamhetsöverenskommelser”, får föreskriva särskilda bestämmelser om behandling av anställdas personuppgifter i anställningsförhållanden, särskilt när det gäller villkoren för hur personuppgifter i anställningsförhållanden får behandlas på grundval av samtycke från den anställde, rekrytering, genomförande av anställningsavtalet, inklusive befrielse från i lag eller kollektivavtal stadgade skyldigheter, ledning, planering och organisering av arbetet samt hälsa och säkerhet på arbetsplatsen, men också när det gäller att såväl kollektivt som individuellt utöva och komma i åtnjutande av rättigheter och förmåner som är knutna till anställningen samt att avsluta anställningsförhållandet.

(156) Behandlingen av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör omfattas av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt denna förordning. Skyddsåtgärderna bör säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt principen om uppgiftsminimering iakttas. Ytterligare behandling av personuppgifter för arkivändamål av allmänintresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör genomföras, när den personuppgiftsansvarige har bedömt möjligheten att uppnå dessa ändamål genom behandling av personuppgifter som inte medger eller inte längre medger identifiering av de registrerade, förutsatt att det finns lämpliga skyddsåtgärder (t. ex. pseudonymisering av personuppgifter). Medlemsstaterna bör införa lämpliga skyddsåtgärder för behandlingen av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Medlemsstaterna bör på särskilda villkor med förbehåll för lämpliga skyddsåtgärder för de registrerade ha rätt att specificera och göra undantag från kraven på information, rätten till rättelse eller radering av personuppgifter, rätten att bli bortglömd, rätten till begränsning av behandlingen, rätten till dataportabilitet och rätten att göra invändning i samband med behandling av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Villkoren och säkerhetsåtgärderna i fråga kan medföra att de registrerade måste följa särskilda förfaranden för att utöva dessa rättigheter, om det är lämpligt med hänsyn till den särskilda behandlingens syfte tillsammans med tekniska och organisatoriska åtgärder som syftar till att minimera behandlingen av personuppgifter i enlighet med principerna om proportionalitet och nödvändighet. Behandling av personuppgifter för vetenskapliga ändamål bör även vara förenlig med annan relevant lagstiftning, exempelvis om kliniska prövningar.

(157) Genom att koppla samman information från olika register kan forskare erhålla ny kunskap av stort värde med avseende på medicinska tillstånd som exempelvis hjärt-kärlsjukdomar, cancer och depression. På grundval av registren kan forskningsresultaten förbättras, eftersom de bygger på en större befolkningsgrupp. Forskning inom samhällsvetenskap som bedrivs på grundval av register gör det möjligt för forskare att få grundläggande kunskaper om sambandet på lång sikt mellan ett antal sociala villkor, exempelvis arbetslöshet och utbildning, och andra livsförhållanden. Forskningsresultat som erhållits på grundval av register utgör en stabil, högkvalitativ kunskap, som kan ligga till grund för utformningen och genomförandet av kunskapsbaserad politik, förbättra livskvaliteten för ett antal personer och förbättra de sociala tjänsternas effektivitet. För att underlätta vetenskaplig forskning får personuppgifter behandlas för vetenskapliga forskningsändamål, med förbehåll för lämpliga villkor och skyddsåtgärder i unionsrätten eller i medlemsstaternas nationella rätt.

(158) Om personuppgifter behandlas för arkivändamål, bör denna förordning också gälla denna behandling, med beaktande av att denna förordning inte bör gälla för avlidna personer. Offentliga myndigheter eller offentliga eller privata organ som innehar uppgifter av allmänt intresse bör vara tillhandahållare som, i enlighet med unionsrätten eller medlemsstaternas nationella rätt, har en rättslig skyldighet att förvärva, bevara, bedöma, organisera, beskriva, kommunicera, främja, sprida och ge tillgång till uppgifter av bestående värde för allmänintresset. Medlemsstaterna bör också ha rätt att föreskriva att personuppgifter får vidarebehandlas för arkivering, exempelvis i syfte att tillhandahålla specifik information om politiskt beteende under tidigare totalitära regimer, folkmord, brott mot mänskligheten, särskilt Förintelsen, eller krigsförbrytelser.

(159) Om personuppgifter behandlas för vetenskapliga forskningsändamål, bör denna förordning också gälla denna behandling. Behandling av personuppgifter för vetenskapliga forskningsändamål bör i denna förordning ges en vid tolkning och omfatta till exempel teknisk utveckling och demonstration, grundforskning, tillämpad forskning och privatfinansierad forskning. Behandlingen av personuppgifter bör dessutom ta hänsyn till unionens mål enligt artikel 179.1 i EUF-fördraget angående åstadkommandet av ett europeiskt forskningsområde. Vetenskapliga forskningsändamål bör också omfatta studier som utförs av ett allmänt intresse inom folkhälsoområdet. För att tillgodose de särskilda kraven i samband med behandling av personuppgifter för vetenskapliga forskningsändamål bör särskilda villkor gälla, särskilt vad avser offentliggörande eller annat utlämnande av personuppgifter inom ramen för vetenskapliga forskningsändamål. Om resultatet av vetenskaplig forskning, särskilt för hälso- och sjukvårdsändamål, ger anledning till ytterligare åtgärder i den registrerades intresse, bör de allmänna reglerna i denna förordning tillämpas på dessa åtgärder.

(160) Om personuppgifter behandlas för historiska forskningsändamål, bör denna förordning också gälla denna behandling. Detta bör även omfatta forskning för historiska och genealogiska ändamål, med beaktande av att denna förordning inte bör gälla för avlidna personer.

(161) När det gäller samtycke till deltagande i vetenskaplig forskning inom ramen för kliniska prövningar, bör de relevanta bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 536/2014 ( ) tillämpas.

(162) Om personuppgifter behandlas för statistiska ändamål, bör denna förordning gälla denna behandling. Unionsrätten eller medlemsstaternas nationella rätt bör, inom ramen för denna förordning, fastställa statistiskt innehåll, kontroll av tillgång, specifikationer för behandling av personuppgifter för statistiska ändamål och lämpliga åtgärder till skydd för den registrerades rättigheter och friheter och för att säkerställa insynsskydd för statistiska uppgifter. Med statistiska ändamål avses varje åtgärd som vidtas för den insamling och behandling av personuppgifter som är nödvändig för statistiska undersökningar eller för framställning av statistiska resultat. Dessa statistiska resultat kan vidare användas för olika ändamål, inbegripet vetenskapliga forskningsändamål. Ett statistiskt ändamål innebär att resultatet av behandlingen för statistiska ändamål inte består av personuppgifter, utan av aggregerade personuppgifter, och att resultatet eller uppgifterna inte används till stöd för åtgärder eller beslut som avser en särskild fysiskperson.

(163) De konfidentiella uppgifter som unionens myndigheter och nationella statistikansvariga myndigheter samlar in för att framställa officiell europeisk och officiell nationell statistik bör skyddas. Europeisk statistik bör utvecklas, framställas och spridas i enlighet med de statistiska principerna i artikel 338.2 i EUF-fördraget, medan hanteringen av nationell statistik även bör överensstämma med medlemsstaternas nationella rätt. Europaparlamentets och rådets förordning (EG) nr 223/2009 ( ) innehåller ytterligare preciseringar om statistisk konfidentialitet för europeisk statistik.

(164) Vad beträffar tillsynsmyndigheternas befogenheter att från personuppgiftsansvariga eller personuppgiftsbiträden få tillgång till personuppgifter och tillträde till lokaler, får medlemsstaterna, inom gränserna för denna förordning, genom lagstiftning anta särskilda regler för att skydda yrkesmässig eller annan motsvarande tystnadsplikt, i den mån detta är nödvändigt för att jämka samman rätten till skydd av personuppgifter med tystnadsplikten. Detta påverkar inte tillämpningen av medlemsstaternas befintliga skyldigheter att anta bestämmelser om tystnadsplikt, där detta krävs enligt unionsrätten.

(165) Denna förordning är förenlig med kravet på att respektera och inte påverka den ställning som kyrkor och religiösa sammanslutningar eller samfund har i medlemsstaterna enligt gällande grundlag i enlighet med artikel 17 i EUF-fördraget.

(166) I syfte att uppnå målen för denna förordning, nämligen att skydda fysiska personers grundläggande rättigheter och friheter och i synnerhet deras rätt till skydd av personuppgifter och för att säkra det fria flödet av

( ) Europaparlamentets och rådets förordning (EU) nr 536/2014 av den 16 april 2014 om kliniska prövningar av humanläkemedel och om upphävande av direktiv 2001/20/EG (EUT L 158, 27.5.2014, s. 1).

( ) Europaparlamentets och rådets förordning (EG) nr 223/2009 av den 11 mars 2009 om europeisk statistik och om upphävande av Europaparlamentets och rådets förordning (EG, Euratom) nr 1101/2008 om utlämnande av insynsskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor, rådets förordning (EG) nr 322/97 om gemenskapsstatistik och rådets beslut 89/382/EEG, Euratom om inrättande av en kommitté för Europeiska gemenskapernas statistiska program (EUT L 87, 31.3.2009, s. 164).

personuppgifter inom unionen, bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen. Delegerade akter bör framför allt antas när det gäller kriterier och krav vad gäller certifieringsmekanismer, information som ska ges med användning av standardiserade symboler och förfaranden för att tillhandahålla sådana symboler. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå. När kommissionen förbereder och utarbetar delegerade akter bör den se till att relevanta handlingar översänds samtidigt till Europaparlamentet och rådet och att detta sker så snabbt som möjligt och på lämpligt sätt.

(167) För att säkerställa enhetliga villkor för tillämpningen av denna förordning bör kommissionen ges genomförandebefogenheter i enlighet med denna förordning. Dessa befogenheter bör utövas i enlighet med förordning (EU) nr 182/2011. Kommissionen bör därvid överväga särskilda åtgärder för mikroföretag och små och medelstora företag.

(168) Granskningsförfarandet bör användas vid antagande av genomförandeakter om standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden och mellan personuppgiftsbiträden, uppförandekoder, tekniska standarder och mekanismer för certifiering, adekvat nivå på det skydd som lämnas av ett tredjeland, ett territorium eller av en specificerad sektor inom det tredjelandet eller en internationell organisation, standardiserade skyddsbestämmelser, format och förfaranden för elektroniskt utbyte av information mellan personuppgiftsansvariga, personuppgiftsbiträden och tillsynsmyndigheter för bindande företagsbestämmelser, ömsesidigt bistånd och tillvägagångssätt för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen.

(169) Kommissionen bör när det föreligger tvingande skäl till skyndsamhet anta omedelbart tillämpliga genomförandeakter, när tillgängliga bevis visar att ett tredjeland, ett territorium eller en specificerad sektor inom det tredjelandet eller en internationell organisation inte upprätthåller en adekvat skyddsnivå.

(170) Eftersom målet för denna förordning, nämligen att säkerställa en likvärdig nivå för skyddet av fysiska personer och det fria flödet av personuppgifter inom hela unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning eller verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen (EU-fördraget). I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

(171) Direktiv 95/46/EG bör upphävas genom denna förordning. Behandling som redan pågår den dag då denna förordning börjar tillämpas bör bringas i överensstämmelse med denna förordning inom en period av två år från det att denna förordning träder i kraft. Om behandlingen grundar sig på samtycke enligt direktiv 95/46/EG, är det inte nödvändigt att den registrerade på nytt ger sitt samtycke för att den personuppgiftsansvarige ska kunna fortsätta med behandlingen i fråga efter det att denna förordning börjar tillämpas, om det sätt på vilket samtycket gavs överensstämmer med villkoren i denna förordning. Beslut av kommissionen som antagits och tillstånd från tillsynsmyndigheterna som utfärdats på grundval av direktiv 95/46/EG ska fortsatt vara giltiga tills de ändras, ersätts eller upphävs.

(172) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 och avgav ett yttrande den 7 mars 2012 ( ).

(173) Denna förordning bör vara tillämplig på alla frågor som gäller skyddet av grundläggande rättigheter och friheter i förhållande till behandlingen av personuppgifter, vilka inte omfattas av särskilda skyldigheter med samma mål som anges i Europaparlamentets och rådets direktiv 2002/58/EG ( ), däribland den personuppgiftsansvariges skyldigheter och fysiska personers rättigheter. För att klargöra förhållandet mellan denna förordning och direktiv 2002/58/EG bör det direktivet ändras. När denna förordning har antagits, bör direktiv 2002/58/EG ses över, framför allt för att säkerställa konsekvens med denna förordning.

( ) EUT C 192, 30.6.2012, s. 7.
( ) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Syfte

1. I denna förordning fastställs bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och om det fria flödet av personuppgifter.

2. Denna förordning skyddar fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.

3. Det fria flödet av personuppgifter inom unionen får varken begränsas eller förbjudas av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter.

Artikel 2

Materiellt tillämpningsområde

1. Denna förordning ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

2. Denna förordning ska inte tillämpas på behandling av personuppgifter som

a) utgör ett led i en verksamhet som inte omfattas av unionsrätten,

b) medlemsstaterna utför när de bedriver verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget,

c) en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,

d) behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

3. Förordning (EG) nr 45/2001 är tillämplig på den behandling av personuppgifter som sker i EU:s institutioner, organ och byråer. Förordning (EG) nr 45/2001 och de av unionens övriga rättsakter som är tillämpliga på sådan behandling av personuppgifter ska anpassas till principerna och bestämmelserna i denna förordning i enlighet med artikel 98.

4. Denna förordning påverkar inte tillämpningen av direktiv 2000/31/EG, särskilt bestämmelserna om tjänsteleverera nde mellanhänders ansvar i artiklarna 12–15 i det direktivet.

Artikel 3

Territoriellt tillämpningsområde

1. Denna förordning ska tillämpas på behandlingen av personuppgifter inom ramen för den verksamhet som bedrivs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i unionen, oavsett om behandlingen utförs i unionen eller inte.

2. Denna förordning ska tillämpas på behandling av personuppgifter som avser registrerade som befinner sig i unionen och som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen, om behandlingen har anknytning till

a) utbjudande av varor eller tjänster till sådana registrerade i unionen, oavsett om dessa varor eller tjänster erbjuds kostnadsfritt eller inte, eller

b) övervakning av deras beteende så länge beteendet sker inom unionen.

3. Denna förordning ska tillämpas på behandling av personuppgifter som utförs av en personuppgiftsansvarig som inte är etablerad i unionen, men på en plats där en medlemsstats nationella rätt gäller enligt folkrätten.

Artikel 4

Definitioner

I denna förordning avses med

1. *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad *en registrerad*), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,

2. *behandling*: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,

3. *begränsning av behandling*: markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden,

4. *profilering*: varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar,

5. *pseudonymisering*: behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person,

6. *register*: en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,

7. *personuppgiftsansvarig*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt,

8. *personuppgiftsbiträde*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

9. *mottagare*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte; offentliga myndigheter som kan komma att motta

personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare; offentliga myndigheters behandling av dessa uppgifter ska vara förenlig med tillämpliga bestämmelser för dataskydd beroende på behandlingens syfte,

10. *tredje part*: en fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar är behöriga att behandla personuppgifterna,

11. *samtycke* av den registrerade: varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne,

12. *personuppgiftsincident*: en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,

13. *genetiska uppgifter*: alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om denna fysiska persons fysiologi eller hälsa och vilka framför allt härrör från en analys av ett biologiskt prov från den fysiska personen i fråga,

14. *biometriska uppgifter*: personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter,

15. *uppgifter om hälsa*: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus,

16. *huvudsakligt verksamhetsställe*:

    a) när det gäller en personuppgiftsansvarig med verksamhetsställen i mer än en medlemsstat, den plats i unionen där vederbörande har sin centrala förvaltning, om inte besluten om ändamålen och medlen för behandlingen av personuppgifter fattas vid ett annat av den personuppgiftsansvariges verksamhetsställen i unionen och det sistnämnda verksamhetsstället har befogenhet att få sådana beslut genomförda, i vilket fall det verksamhetsställe som har fattat sådana beslut ska betraktas som det huvudsakliga verksamhetsstället,

    b) när det gäller ett personuppgiftsbiträde med verksamhetsställen i mer än en medlemsstat, den plats i unionen där vederbörande har sin centrala förvaltning eller, om personuppgiftsbiträdet inte har någon central förvaltning i unionen, det av personuppgiftsbiträdets verksamhetsställen i unionen där den huvudsakliga behandlingen inom ramen för verksamheten vid ett av personuppgiftsbiträdets verksamhetsställen sker, i den utsträckning som personuppgiftsbiträdet omfattas av särskilda skyldigheter enligt denna förordning,

17. *företrädare*: en i unionen etablerad fysisk eller juridisk person som skriftligen har utsetts av den personuppgiftsansvarige eller personuppgiftsbiträdet i enlighet med artikel 27 och företräder denne i frågor som gäller dennes skyldigheter enligt denna förordning,

18. *företag*: en fysisk eller juridisk person som bedriver ekonomisk verksamhet, oavsett dess juridiska form, vilket inbegriper partnerskap eller föreningar som regelbundet bedriver ekonomisk verksamhet,

19. *koncern*: ett kontrollerande företag och dess kontrollerade företag,

20. *bindande företagsbestämmelser*: strategier för skydd av personuppgifter som en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad på en medlemsstats territorium använder sig av vid överföringar eller en uppsättning av överföringar av personuppgifter till en personuppgiftsansvarig eller ett personuppgiftsbiträde i ett eller flera tredjeländer inom en koncern eller en grupp av företag som deltar i gemensam ekonomisk verksamhet,

21. *tillsynsmyndighet*: en oberoende offentlig myndighet som är utsedd av en medlemsstat i enlighet med artikel 51,

22. *berörd tillsynsmyndighet*: en tillsynsmyndighet som berörs av behandlingen av personuppgifter på grund av att

a) den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad på tillsynsmyndighetens medlemsstats territorium,

b) registrerade som är bosatta i den tillsynsmyndighetens medlemsstat i väsentlig grad påverkas eller sannolikt i väsentlig grad kommer att påverkas av behandlingen, eller

c) ett klagomål har lämnats in till denna tillsynsmyndighet,

23. *gränsöverskridande behandling*:

a) behandling av personuppgifter som äger rum inom ramen för verksamhet vid verksamhetsställen i mer än en medlemsstat tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen, när den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat, eller

b) behandling av personuppgifter som äger rum inom ramen för verksamhet vid ett enda verksamhetsställe tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen men som i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka registrerade i mer än en medlemsstat,

24. *relevant och motiverad invändning*: en invändning mot ett förslag till beslut avseende frågan huruvida det föreligger en överträdelse av denna förordning eller huruvida den planerade åtgärden i förhållande till den personuppgiftsansvarige eller personuppgiftsbiträdet är förenlig med denna förordning, av vilken invändning det tydligt framgår hur stora risker utkastet till beslut medför när det gäller registrerades grundläggande rättigheter och friheter samt i tillämpliga fall det fria flödet av personuppgifter inom unionen,

25. *informationssamhällets tjänster*: alla tjänster enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 ( ),

26. *internationell organisation*: en organisation och dess underställda organ som lyder under folkrätten, eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera länder.

KAPITEL II

Principer

Artikel 5

Principer för behandling av personuppgifter

1. Vid behandling av personuppgifter ska följande gälla:

a) Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (*laglighet, korrekthet och öppenhet*).

b) De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenlig med de ursprungliga ändamålen (*ändamålsbegränsning*).

c) De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (*uppgiftsminimering*).

d) De ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (*korrekthet*).

( ) Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

e) De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (*lagringsminimering*).

f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (*integritet och konfidentialitet*).

2. Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs (*ansvarsskyldighet*).

Artikel 6

Laglig behandling av personuppgifter

1. Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.

b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Led f i första stycket ska inte gälla för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

2. Medlemsstaterna får behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning med hänsyn till behandling för att efterleva punkt 1 c och e genom att närmare fastställa specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling, inbegripet för andra specifika situationer då uppgifter behandlas i enlighet med kapitel IX.

3. Den grund för behandlingen som avses i punkt 1 c och e ska fastställas i enlighet med

a) unionsrätten, eller

b) en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av.

Syftet med behandlingen ska fastställas i den rättsliga grunden eller, i fråga om behandling enligt punkt 1 e, ska vara nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Den rättsliga grunden kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning, bland annat: de allmänna villkor som ska gälla för den personuppgiftsansvariges behandling, vilken typ av uppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål, ändamålsbegränsningar, lagringstid samt typer av behandling och förfaranden för behandling, inbegripet åtgärder för att tillförsäkra en laglig och rättvis behandling, däribland för behandling i andra särskilda

situationer enligt kapitel IX. Unionsrätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas.

4. Om en behandling för andra ändamål än det ändamål för vilket personuppgifterna samlades in inte grundar sig på den registrerades samtycke eller på unionsrätten eller medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda de mål som avses i artikel 23.1, ska den personuppgiftsansvarige för att fastställa huruvida behandling för andra ändamål är förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in bland annat beakta följande:

a) Kopplingar mellan de ändamål för vilka personuppgifterna har samlats in och ändamålen med den avsedda ytterligare behandlingen.

b) Det sammanhang inom vilket personuppgifterna har samlats in, särskilt förhållandet mellan de registrerade och den personuppgiftsansvarige.

c) Personuppgifternas art, särskilt huruvida särskilda kategorier av personuppgifter behandlas i enlighet med artikel 9 eller huruvida personuppgifter om fällande domar i brottmål och överträdelser behandlas i enlighet med artikel 10.

d) Eventuella konsekvenser för registrerade av den planerade fortsatta behandlingen.

e) Förekomsten av lämpliga skyddsåtgärder, vilket kan inbegripa kryptering eller pseudonymisering.

Artikel 7

Villkor för samtycke

1. Om behandlingen grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter.

2. Om den registrerades samtycke lämnas i en skriftlig förklaring som också rör andra frågor, ska begäran om samtycke läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Om en del av förklaringen innebär en överträdelse av denna förordning, ska denna del inte vara bindande.

3. De registrerade ska ha rätt att när som helst återkalla sitt samtycke. Återkallandet av samtycket ska inte påverka lagligheten av behandling som grundar sig på samtycke, innan detta återkallas. Innan samtycke lämnas ska den registrerade informeras om detta. Det ska vara lika lätt att återkalla som att ge sitt samtycke.

4. Vid bedömning av huruvida samtycke är frivilligt ska största hänsyn bland annat tas till huruvida genomförandet av ett avtal, inbegripet tillhandahållandet av en tjänst, har gjorts beroende av samtycke till sådan behandling av personuppgifter som inte är nödvändig för genomförandet av det avtalet.

Artikel 8

Villkor som gäller barns samtycke avseende informationssamhällets tjänster

1. Vid erbjudande av informationssamhällets tjänster direkt till ett barn, ska vid tillämpningen av artikel 6.1 a behandling av personuppgifter som rör ett barn vara tillåten om barnet är minst 16 år. Om barnet är under 16 år ska sådan behandling vara tillåten endast om och i den mån samtycke ges eller godkänns av den person som har föräldraansvar för barnet.

Medlemsstaterna får i sin nationella rätt föreskriva en lägre ålder i detta syfte, under förutsättning att denna lägre ålder inte är under 13 år.

2. Den personuppgiftsansvarige ska göra rimliga ansträngningar för att i sådana fall kontrollera att samtycke ges eller godkänns av den person som har föräldraansvar för barnet, med hänsyn tagen till tillgänglig teknik.

3. Punkt 1 ska inte påverka tillämpningen av allmän avtalsrätt i medlemsstaterna, såsom bestämmelser om giltigheten, upprättandet eller effekten av ett avtal som gäller ett barn.

Artikel 9

Behandling av särskilda kategorier av personuppgifter

1. Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden.

2. Punkt 1 ska inte tillämpas om något av följande gäller:

a) Den registrerade har uttryckligen lämnat sitt samtycke till behandlingen av dessa personuppgifter för ett eller flera specifika ändamål, utom då unionsrätten eller medlemsstaternas nationella rätt föreskriver att förbudet i punkt 1 inte kan upphävas av den registrerade.

b) Behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd, i den omfattning detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt eller ett kollektivavtal som antagits med stöd av medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställs.

c) Behandlingen är nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.

d) Behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att behandlingen enbart rör sådana organs medlemmar eller tidigare medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta och personuppgifterna inte lämnas ut utanför det organet utan den registrerades samtycke.

e) Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

f) Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet.

g) Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

h) Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system, på grundval av unionsrätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet och under förutsättning att de villkor och skyddsåtgärder som avses i punkt 3 är uppfyllda.

i) Behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter, på grundval av unionsrätten eller medlemsstaternas nationella rätt, där lämpliga och specifika åtgärder för att skydda den registrerades rättigheter och friheter fastställs, särskilt tystnadsplikt.

j) Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

3. Personuppgifter som avses i punkt 1 får behandlas för de ändamål som avses i punkt 2 h, när uppgifterna behandlas av eller under ansvar av en yrkesutövare som omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ eller av en annan person som också omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ.

4. Medlemsstaterna får behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om hälsa.

Artikel 10

Behandling av personuppgifter som rör fällande domar i brottmål samt överträdelser

Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder enligt artikel 6.1 får endast utföras under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet.

Artikel 11

Behandling som inte kräver identifiering

1. Om de ändamål för vilka den personuppgiftsansvarige behandlar personuppgifter inte kräver eller inte längre kräver att den registrerade identifieras av den personuppgiftsansvarige, ska den personuppgiftsansvarige inte vara tvungen att bevara, förvärva eller behandla ytterligare information för att identifiera den registrerade endast i syfte att följa denna förordning.

2. Om den personuppgiftsansvarige, i de fall som avses i punkt 1 i denna artikel, kan visa att denne inte är i stånd att identifiera den registrerade, ska den personuppgiftsansvarige om möjligt informera den registrerade om detta. I sådana fall ska artiklarna 15–20 inte gälla, förutom när den registrerade för utövande av sina rättigheter i enlighet med dessa artiklar tillhandahåller ytterligare information som gör identifieringen möjlig.

KAPITEL III

Den registrerades rättigheter

Avsnitt 1

Insyn och villkor

Artikel 12

Klar och tydlig information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter

1. Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att till den registrerade tillhandahålla all information som avses i artiklarna 13 och 14 och all kommunikation enligt artiklarna 15–22 och 34 vilken avser behandling i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn. Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt.

2. Den personuppgiftsansvarige ska underlätta utövandet av den registrerades rättigheter i enlighet med artiklarna 15–22. I de fall som avses i artikel 11.2 får den personuppgiftsansvarige inte vägra att tillmötesgå den registrerades begäran om att utöva sina rättigheter enligt artiklarna 15–22, om inte den personuppgiftsansvarige visar att han eller hon inte är i stånd att identifiera den registrerade.

3. Den personuppgiftsansvarige ska på begäran utan onödigt dröjsmål och under alla omständigheter senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits enligt artiklarna 15–22. Denna period får vid behov förlängas med ytterligare två månader, med beaktande av hur komplicerad begäran är och antalet inkomna begäranden. Den personuppgiftsansvarige ska underrätta den registrerade om en sådan förlängning inom en månad från det att begäran mottagits samt ange orsakerna till förseningen. Om den registrerade lämnar begäran i elektronisk form, ska informationen om möjligt tillhandahållas i elektronisk form, om den registrerade inte begär något annat.

4. Om den personuppgiftsansvarige inte vidtar åtgärder på den registrerades begäran, ska den personuppgiftsansvarige utan dröjsmål och senast en månad efter att ha mottagit begäran informera den registrerade om orsaken till att åtgärder inte vidtagits och om möjligheten att lämna in ett klagomål till en tillsynsmyndighet och begära rättslig prövning.

5. Information som tillhandahållits enligt artiklarna 13 och 14, all kommunikation och samtliga åtgärder som vidtas enligt artiklarna 15–22 och 34 ska tillhandahållas kostnadsfritt. Om begäranden från en registrerad är uppenbart ogrundade eller orimliga, särskilt på grund av deras repetitiva art, får den personuppgiftsansvarige antingen

a) ta ut en rimlig avgift som täcker de administrativa kostnaderna för att tillhandahålla den information eller vidta den åtgärd som begärts, eller

b) vägra att tillmötesgå begäran.

Det åligger den personuppgiftsansvarige att visa att begäran är uppenbart ogrundad eller orimlig.

6. Utan att det påverkar tillämpningen av artikel 11 får den personuppgiftsansvarige, om denne har rimliga skäl att betvivla identiteten hos den fysiska person som lämnar in en begäran enligt artiklarna 15–21, begära att ytterligare information som är nödvändig för att bekräfta den registrerades identitet tillhandahålls.

7. Den information som ska tillhandahållas de registrerade i enlighet med artiklarna 13 och 14 får tillhandahållas kombinerad med standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över den planerade behandlingen. Om sådana symboler visas elektroniskt ska de vara maskinläsbara.

8. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 92 för att fastställa vilken information som ska visas med hjälp av symboler och förfaranden för att tillhandahålla sådana symboler.

Avsnitt 2

Information och tillgång till personuppgifter

Artikel 13

Information som ska tillhandahållas om personuppgifterna samlas in från den registrerade

1. Om personuppgifter som rör en registrerad person samlas in från den registrerade, ska den personuppgiftsansvarige, när personuppgifterna erhålls, till den registrerade lämna information om följande:

a) Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.

b) Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall.

c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.

d) Om behandlingen är baserad på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen.

e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.

f) I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artikel 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

2. Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige vid insamlingen av personuppgifterna lämna den registrerade följande ytterligare information, vilken krävs för att säkerställa rättvis och transparent behandling:

a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

b) Att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.

c) Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, att det föreligger en rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.

d) Rätten att inge klagomål till en tillsynsmyndighet.

e) Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav eller ett krav som är nödvändigt för att ingå ett avtal samt huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att sådana uppgifter inte lämnas.

f) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

3. Om den personuppgiftsansvarige avser att ytterligare behandla personuppgifterna för ett annat syfte än det för vilket de insamlades, ska den personuppgiftsansvarige före denna ytterligare behandling ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt punkt 2.

4. Punkterna 1, 2 och 3 ska inte tillämpas om och i den mån den registrerade redan förfogar över informationen.

Artikel 14

Information som ska tillhandahållas om personuppgifterna inte har erhållits från den registrerade

1. Om personuppgifterna inte har erhållits från den registrerade, ska den personuppgiftsansvarige förse den registrerade med följande information:

a) Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.

b) Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall.

c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.

d) De kategorier av personuppgifter som behandlingen gäller.

e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.

f) I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till en mottagare i ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artiklarna 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

2. Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige lämna den registrerade följande information, vilken krävs för att säkerställa rättvis och transparent behandling när det gäller den registrerade:

a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

b) Om behandlingen grundar sig på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen.

c) Förekomsten av rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade och att invända mot behandling samt rätten till dataportabilitet.

d) Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, rätten att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.

e) Rätten att inge klagomål till en tillsynsmyndighet.

f) Varifrån personuppgifterna kommer och i förekommande fall huruvida de har sitt ursprung i allmänt tillgängliga källor.

g) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

3. Den personuppgiftsansvarige ska lämna den information som anges i punkterna 1 och 2

a) inom en rimlig period efter det att personuppgifterna har erhållits, dock senast inom en månad, med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas,

b) om personuppgifterna ska användas för kommunikation med den registrerade, senast vid tidpunkten för den första kommunikationen med den registrerade, eller

c) om ett utlämnande till en annan mottagare förutses, senast när personuppgifterna lämnas ut för första gången.

4. Om den personuppgiftsansvarige avser att ytterligare behandla personuppgifterna för ett annat syfte än det för vilket de insamlades, ska den personuppgiftsansvarige före denna ytterligare behandling ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt punkt 2.

5. Punkterna 1–4 ska inte tillämpas i följande fall och i den mån

a) den registrerade redan förfogar över informationen,

b) tillhandahållandet av sådan information visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning, särskilt för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, eller i den mån den skyldighet som avses i punkt 1 i den här artikeln sannolikt kommer att göra det omöjligt eller avsevärt försvårar uppfyllandet av målen med den behandlingen; i sådana fall ska den personuppgiftsansvarige vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen, inbegripet göra uppgifterna tillgängliga för allmänheten,

c) erhållande eller utlämnande av uppgifter uttryckligen föreskrivs genom unionsrätten eller genom en medlemsstats nationella rätt som den registrerade omfattas av och som fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen, eller

d) personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt, inbegripet andra lagstadgade sekretessförpliktelser.

Artikel 15

Den registrerades rätt till tillgång

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna och följande information:

a) Ändamålen med behandlingen.

b) De kategorier av personuppgifter som behandlingen gäller.

c) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer.

d) Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

e) Förekomsten av rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifterna eller begränsningar av behandling av personuppgifter som rör den registrerade eller att invända mot sådan behandling.

f) Rätten att inge klagomål till en tillsynsmyndighet.

g) Om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån dessa uppgifter kommer.

h) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

2. Om personuppgifterna överförs till ett tredjeland eller till en internationell organisation, ska den registrerade ha rätt till information om de lämpliga skyddsåtgärder som i enlighet med artikel 46 har vidtagits vid överföringen.

3. Den personuppgiftsansvarige ska förse den registrerade med en kopia av de personuppgifter som är under behandling. För eventuella ytterligare kopior som den registrerade begär får den personuppgiftsansvarige ta ut en rimlig avgift på grundval av de administrativa kostnaderna. Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat.

4. Den rätt till en kopia som avses i punkt 3 ska inte inverka menligt på andras rättigheter och friheter.

Avsnitt 3

Rättelse och radering

Artikel 16

Rätt till rättelse

Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få felaktiga personuppgifter som rör honom eller henne rättade. Med beaktande av ändamålet med behandlingen, ska den registrerade ha rätt att komplettera ofullständiga personuppgifter, bland annat genom att tillhandahålla ett kompletterande utlåtande.

Artikel 17

Rätt till radering (”rätten att bli bortglömd”)

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få sina personuppgifter raderade och den personuppgiftsansvarige ska vara skyldig att utan onödigt dröjsmål radera personuppgifter om något av följande gäller:

a) Personuppgifterna är inte längre nödvändiga för de ändamål för vilka de samlats in eller på annat sätt behandlats.

b) Den registrerade återkallar det samtycke på vilket behandlingen grundar sig enligt artikel 6.1 a eller artikel 9.2 a och det finns inte någon annan rättslig grund för behandlingen.

c) Den registrerade invänder mot behandlingen i enlighet med artikel 21.1 och det saknas berättigade skäl för behandlingen som väger tyngre, eller den registrerade invänder mot behandlingen i enlighet med artikel 21.2.

d) Personuppgifterna har behandlats på olagligt sätt.

e) Personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse i unionsrätten eller i medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av.

f) Personuppgifterna har samlats in i samband med erbjudande av informationssamhällets tjänster, i de fall som avses i artikel 8.1.

2. Om den personuppgiftsansvarige har offentliggjort personuppgifterna och enligt punkt 1 är skyldig att radera personuppgifterna, ska den personuppgiftsansvarige med beaktande av tillgänglig teknik och kostnaden för genomförandet vidta rimliga åtgärder, inbegripet tekniska åtgärder, för att underrätta personuppgiftsansvariga som behandlar personuppgifterna om att den registrerade har begärt att de ska radera eventuella länkar till, eller kopior eller reproduktioner av dessa personuppgifter.

3. Punkterna 1 och 2 ska inte gälla i den utsträckning som behandlingen är nödvändig av följande skäl:

a) För att utöva rätten till yttrande- och informationsfrihet.

b) För att uppfylla en rättslig förpliktelse som kräver behandling enligt unionsrätten eller enligt en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av eller för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige.

c) För skäl som rör ett viktigt allmänt intresse på folkhälsoområdet enligt artikel 9.2 h och i samt artikel 9.3.

d) För arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål enligt artikel 89.1, i den utsträckning som den rätt som avses i punkt 1 sannolikt omöjliggör eller avsevärt försvårar uppnåendet av syftet med den behandlingen.

e) För att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

Artikel 18

Rätt till begränsning av behandling

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige kräva att behandlingen begränsas om något av följande alternativ är tillämpligt:

a) Den registrerade bestrider personuppgifternas korrekthet, under en tid som ger den personuppgiftsansvarige möjlighet att kontrollera om personuppgifterna är korrekta.

b) Behandlingen är olaglig och den registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning.

c) Den personuppgiftsansvarige behöver inte längre personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

d) Den registrerade har invänt mot behandling i enlighet med artikel 21.1 i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.

2. Om behandlingen har begränsats i enlighet med punkt 1 får sådana personuppgifter, med undantag för lagring, endast behandlas med den registrerades samtycke eller för att fastställa, göra gällande eller försvara rättsliga anspråk eller för att skydda någon annan fysisk eller juridisk persons rättigheter eller för skäl som rör ett viktigt allmänintresse för unionen eller för en medlemsstat.

3. En registrerad som har fått behandling begränsad i enlighet med punkt 1 ska underrättas av den personuppgiftsansvarige innan begränsningen av behandlingen upphör.

Artikel 19

Anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling

Den personuppgiftsansvarige ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling som skett i enlighet med artiklarna 16, 17.1 och 18, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Artikel 20

Rätt till dataportabilitet

1. Den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits personuppgifterna hindrar detta, om

a) behandlingen grundar sig på samtycke enligt artikel 6.1 a eller artikel 9.2 a eller på ett avtal enligt artikel 6.1 b, och

b) behandlingen sker automatiserat.

2 Vid utövandet av sin rätt till dataportabilitet i enlighet med punkt 1 ska den registrerade ha rätt till överföring av personuppgifterna direkt från en personuppgiftsansvarig till en annan, när detta är tekniskt möjligt.

3. Utövandet av den rätt som avses i punkt 1 i den här artikeln ska inte påverka tillämpningen av artikel 17. Den rätten ska inte gälla i fråga om en behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige.

4. Den rätt som avses i punkt 1 får inte påverka andras rättigheter och friheter på ett ogynnsamt sätt.

Avsnitt 4

Rätt att göra invändningar och automatiserat individuellt beslutsfattande

Artikel 21

Rätt att göra invändningar

1. Den registrerade ska, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på artikel 6.1 e eller f, inbegripet profilering som grundar sig på dessa bestämmelser. Den personuppgiftsansvarige får inte längre behandla personuppgifterna såvida denne inte kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.

2. Om personuppgifterna behandlas för direkt marknadsföring ska den registrerade ha rätt att när som helst invända mot behandling av personuppgifter som avser honom eller henne för sådan marknadsföring, vilket inkluderar profilering i den utsträckning som denna har ett samband med sådan direkt marknadsföring.

3. Om den registrerade invänder mot behandling för direkt marknadsföring ska personuppgifterna inte längre behandlas för sådana ändamål.

4. Senast vid den första kommunikationen med den registrerade ska den rätt som avses i punkterna 1 och 2 uttryckligen meddelas den registrerade och redovisas tydligt, klart och åtskilt från eventuell annan information.

5. När det gäller användningen av informationssamhällets tjänster, och trots vad som sägs i direktiv 2002/58/EG, får den registrerade utöva sin rätt att göra invändningar på automatiserat sätt med användning av tekniska specifikationer.

6. Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska den registrerade, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att göra invändningar mot behandling av personuppgifter avseende honom eller henne om inte behandlingen är nödvändig för att utföra en uppgift av allmänt intresse.

Artikel 22

Automatiserat individuellt beslutsfattande, inbegripet profilering

1. Den registrerade ska ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne.

2. Punkt 1 ska inte tillämpas om beslutet

a) är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige,

b) tillåts enligt unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av och som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen, eller

c) grundar sig på den registrerades uttryckliga samtycke.

3. I fall som avses i punkt 2 a och c ska den personuppgiftsansvarige genomföra lämpliga åtgärder för att säkerställa den registrerades rättigheter, friheter och rättsliga intressen, åtminstone rätten till personlig kontakt med den personuppgiftsansvarige för att kunna utrycka sin åsikt och bestrida beslutet.

4. Beslut enligt punkt 2 får inte grunda sig på de särskilda kategorier av personuppgifter som avses i artikel 9.1, såvida inte artikel 9.2 a eller g gäller och lämpliga åtgärder som ska skydda den registrerades berättigade intressen har vidtagits.

Avsnitt 5

Begränsningar

Artikel 23

Begränsningar

1. Det ska vara möjligt att i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige eller personuppgiftsbiträdet omfattas av införa en lagstiftningsåtgärd som begränsar tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i artiklarna 12–22 och 34, samt artikel 5 i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 12–22, om en sådan begränsning sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa

a) den nationella säkerheten,

b) försvaret,

c) den allmänna säkerheten,

d) förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten,

e) andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet,

f) skydd av rättsväsendets oberoende och rättsliga åtgärder,

g) förebyggande, förhindrande, utredning, avslöjande och lagföring av överträdelser av etiska regler som gäller för lagreglerade yrken,

h) en tillsyns-, inspektions- eller regleringsfunktion som, även i enstaka fall, har samband med myndighetsutövning i fall som nämns i a–e och g,

i) skydd av den registrerade eller andras rättigheter och friheter,

j) verkställighet av civilrättsliga krav.

2. Framför allt ska alla lagstiftningsåtgärder som avses i punkt 1 innehålla specifika bestämmelser åtminstone, när så är relevant, avseende

a) ändamålen med behandlingen eller kategorierna av behandling,

b) kategorierna av personuppgifter,

c) omfattningen av de införda begränsningarna,

d) skyddsåtgärder för att förhindra missbruk eller olaglig tillgång eller överföring,

e) specificeringen av den personuppgiftsansvarige eller kategorierna av personuppgiftsansvariga,

f) lagringstiden samt tillämpliga skyddsåtgärder med beaktande av behandlingens art, omfattning och ändamål eller kategorierna av behandling,

g) riskerna för de registrerades rättigheter och friheter, och

h) de registrerades rätt att bli informerade om begränsningen, såvida detta inte kan inverka menligt på begränsningen.

KAPITEL IV

Personuppgiftsansvarig och personuppgiftsbiträde

Avsnitt 1

Allmänna skyldigheter

Artikel 24

Den personuppgiftsansvariges ansvar

1. Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.

2. Om det står i proportion till behandlingen, ska de åtgärder som avses i punkt 1 omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.

3. Tillämpningen av godkända uppförandekoder som avses i artikel 40 eller godkända certifieringsmekanismer som avses i artikel 42 får användas för att visa att den personuppgiftsansvarige fullgör sina skyldigheter.

Artikel 25

Inbyggt dataskydd och dataskydd som standard

1. Med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder – såsom pseudonymisering – vilka är utformade för ett effektivt genomförande av dataskyddsprinciper – såsom uppgiftsminimering – och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i denna förordning uppfylls och den registrerades rättigheter skyddas.

2. Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

3. En godkänd certifieringsmekanism i enlighet med artikel 42 får användas för att visa att kraven i punkterna 1 och 2 i den här artikeln följs.

Artikel 26

Gemensamt personuppgiftsansvariga

1. Om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. Gemensamt personuppgiftsansvariga ska under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt denna förordning, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artiklarna 13 och 14, genom ett inbördes arrangemang, såvida inte de personuppgiftsansvarigas respektive skyldigheter fastställs genom unionsrätten eller en medlemsstats nationella rätt som de personuppgiftsansvariga omfattas av. Inom ramen för arrangemanget får en gemensam kontaktpunkt för de personuppgiftsansvariga utses.

2. Det arrangemang som avses i punkt 1 ska på lämpligt sätt återspegla de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade. Det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade.

3. Oavsett formerna för det arrangemang som avses i punkt 1 får den registrerade utöva sina rättigheter enligt denna förordning med avseende på och emot var och en av de personuppgiftsansvariga.

Artikel 27

Företrädare för personuppgiftsansvariga eller personuppgiftsbiträden som inte är etablerade i unionen

1. Om artikel 3.2 tillämpas ska den personuppgiftsansvarige eller personuppgiftsbiträdet skriftligen utse en företrädare i unionen.

2. Skyldigheten enligt punkt 1 i denna artikel ska inte gälla

a) tillfällig behandling som inte omfattar behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller behandling av personuppgifter avseende fällande domar i brottmål samt överträdelser, som avses i artikel 10, och som sannolikt inte kommer att medföra en risk för fysiska personers rättigheter och friheter, med hänsyn till behandlingens art, sammanhang, omfattning och ändamål, eller

b) en offentlig myndighet eller ett offentligt organ.

3. Företrädaren ska vara etablerad i en av de medlemsstater där de registrerade, vars personuppgifter behandlas i samband med att de erbjuds varor eller tjänster, eller vars beteende övervakas, befinner sig.

4. Företrädaren ska på den personuppgiftsansvariges eller personuppgiftsbiträdets uppdrag, utöver eller i stället för den personuppgiftsansvarige eller personuppgiftsbiträdet, fungera som kontaktperson för i synnerhet tillsynsmyndigheter och registrerade, i alla frågor som har anknytning till behandlingen, i syfte att säkerställa efterlevnad av denna förordning.

5. Att den personuppgiftsansvarige eller personuppgiftsbiträdet utser en företrädare ska inte påverka de rättsliga åtgärder som skulle kunna inledas mot den personuppgiftsansvarige eller personuppgiftsbiträdet.

Artikel 28

Personuppgiftsbiträden

1. Om en behandling ska genomföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas.

2. Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.

3. När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige och i vilken föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges. I det avtalet eller den rättsakten ska det särskilt föreskrivas att personuppgiftsbiträdet

a) endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av, och i så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt,

b) säkerställer att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt,

c) ska vidta alla åtgärder som krävs enligt artikel 32,

d) ska respektera de villkor som avses i punkterna 2 och 4 för anlitandet av ett annat personuppgiftsbiträde,

e) med tanke på behandlingens art, ska hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter i enlighet med kapitel III,

f) ska bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå,

g) beroende på vad den personuppgiftsansvarige väljer, ska radera eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av behandlingstjänster har avslutats, och radera befintliga kopior såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt, och

h) ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i denna artikel har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige.

Med avseende på led h i första stycket ska personuppgiftsbiträdet omedelbart informera den personuppgiftsansvarige om han anser att en instruktion strider mot denna förordning eller mot andra av unionens eller medlemsstaternas dataskyddsbestämmelser.

4. I de fall där ett personuppgiftsbiträde anlitar ett annat personuppgiftsbiträde för utförande av specifik behandling på den personuppgiftsansvariges vägnar ska det andra personuppgiftsbiträdet, genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt, åläggas samma skyldigheter i fråga om dataskydd som de som fastställs i avtalet eller den andra rättsakten mellan den personuppgiftsansvarige och personuppgiftsbiträdet enligt punkt 3, och framför allt att ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning. Om det andra personuppgiftsbiträdet inte fullgör sina skyldigheter i fråga om dataskydd ska det ursprungliga personuppgiftsbiträdet vara fullt ansvarig gentemot den personuppgiftsansvarige för utförandet av det andra personuppgiftsbiträdets skyldigheter.

5. Ett personuppgiftsbiträdes anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att tillräckliga garantier tillhandahålls, så som avses punkterna 1 och 4 i den här artikeln.

6. Det avtal eller den andra rättsakt som avses i punkterna 3 och 4 i den här artikeln får, utan att det påverkar tillämpningen av ett enskilt avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet, helt eller delvis baseras på sådana standardavtalsklausuler som avses i punkterna 7 och 8 i den här artikeln, inbegripet när de ingår i en certifiering som i enlighet med artiklarna 42 och 43 beviljats den personuppgiftsansvarige eller personuppgiftsbiträdet.

7. Kommissionen får fastställa standardavtalsklausuler för de frågor som avses i punkterna 3 och 4 i den här artikeln, i enlighet med det granskningsförfarande som avses i artikel 93.2.

8. En tillsynsmyndighet får fastställa standardavtalsklausuler för de frågor som avses i punkterna 3 och 4 i den här artikeln, i enlighet med den mekanism för enhetlighet som avses i artikel 63.

9. Det avtal eller den andra rättsakt som avses i punkterna 3 och 4 ska upprättas skriftligen, inbegripet i ett elektroniskt format.

10. Om ett personuppgiftsbiträde överträder denna förordning genom att fastställa ändamålen med och medlen för behandlingen, ska personuppgiftsbiträdet anses vara personuppgiftsansvarig med avseende på den behandlingen, utan att det påverkar tillämpningen av artiklarna 82, 83 och 84.

Artikel 29

Behandling under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende

Personuppgiftsbiträdet och personer som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, får endast behandla dessa på instruktion från den personuppgiftsansvarige, såvida han eller hon inte är skyldig att göra det enligt unionsrätten eller medlemsstaternas nationella rätt.

Artikel 30

Register över behandling

1. Varje personuppgiftsansvarig och, i tillämpliga fall, dennes företrädare ska föra ett register över behandling som utförts under dess ansvar. Detta register ska innehålla samtliga följande uppgifter:

a) Namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet.

b) Ändamålen med behandlingen.

c) En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.

d) De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer.

e) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentationen av lämpliga skyddsåtgärder.

f) Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.

g) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1.

2. Varje personuppgiftsbiträde och, i tillämpliga fall, dennes företrädare ska föra ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning, som omfattar följande:

a) Namn och kontaktuppgifter för personuppgiftsbiträdet eller personuppgiftsbiträdena och för varje personuppgiftsansvarig för vars räkning personuppgiftsbiträdet agerar, och, i tillämpliga fall, för den personuppgiftsansvariges eller personuppgiftsbiträdets företrädare samt dataskyddsombudet.

b) De kategorier av behandling som har utförts för varje personuppgiftsansvariges räkning.

c) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentationen av lämpliga skyddsåtgärder.

d) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1.

3. De register som avses i punkterna 1 och 2 ska upprättas skriftligen, inbegripet i elektronisk form.

4. På begäran ska den personuppgiftsansvarige eller personuppgiftsbiträdet samt, i tillämpliga fall, den personuppgiftsansvariges eller personuppgiftsbiträdets företrädare göra registret tillgängligt för tillsynsmyndigheten.

5. De skyldigheter som anges i punkterna 1 och 2 ska inte gälla för ett företag eller en organisation som sysselsätter färre än 250 personer såvida inte den behandling som utförs sannolikt kommer att medföra en risk för registrerades rättigheter och friheter, behandlingen inte är tillfällig eller behandlingen omfattar särskilda kategorier av uppgifter som avses i artikel 9.1 eller personuppgifter om fällande domar i brottmål samt överträdelser som avses i artikel 10.

Artikel 31

Samarbete med tillsynsmyndigheten

Den personuppgiftsansvarige och personuppgiftsbiträdet samt, i tillämpliga fall, deras företrädare ska på begäran samarbeta med tillsynsmyndigheten vid utförandet av dennes uppgifter.

Avsnitt 2

Säkerhet för personuppgifter

Artikel 32

Säkerhet i samband med behandlingen

1. Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt

a) pseudonymisering och kryptering av personuppgifter,

b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,

c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,

d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

2. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

3. Anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att kraven i punkt 1 i den här artikeln följs.

4. Den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det.

Artikel 33

Anmälan av en personuppgiftsincident till tillsynsmyndigheten

1. Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig i enlighet med artikel 55, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.

2. Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident.

3. Den anmälan som avses i punkt 1 ska åtminstone

a) beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,

b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,

c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och

d) beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

4. Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

5. Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av denna artikel.

Artikel 34

Information till den registrerade om en personuppgiftsincident

1. Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.

2. Den information till den registrerade som avses i punkt 1 i denna artikel ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone de upplysningar och åtgärder som avses i artikel 33.3 b, c och d.

3. Information till den registrerade i enlighet med punkt 1 krävs inte om något av följande villkor är uppfyllt:

a) Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som ska göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna, såsom kryptering.

b) Den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter som avses i punkt 1 sannolikt inte längre kommer att uppstå.

c) Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.

4. Om den personuppgiftsansvarige inte redan har informerat den registrerade om personuppgiftsincidenten får tillsynsmyndigheten, efter att ha bedömt sannolikheten för att personuppgiftsincidenten medför en hög risk, kräva att personuppgiftsbiträdet gör det eller får besluta att något av de villkor som avses i punkt 3 uppfylls.

Avsnitt 3

Konsekvensbedömning avseende dataskydd samt föregående samråd

Artikel 35

Konsekvensbedömning avseende dataskydd

1. Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.

2. Den personuppgiftsansvarige ska rådfråga dataskyddsombudet, om ett sådant utsetts, vid genomförande av en konsekvensbedömning avseende dataskydd.

3. En konsekvensbedömning avseende dataskydd som avses i punkt 1 ska särskilt krävas i följande fall:

a) En systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer.

b) Behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller av personuppgifter som rör fällande domar i brottmål och överträdelser som avses i artikel 10.

c) Systematisk övervakning av en allmän plats i stor omfattning.

4. Tillsynsmyndigheten ska upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd i enlighet med punkt 1. Tillsynsmyndigheten ska översända dessa förteckningar till den styrelse som avses i artikel 68.

5. Tillsynsmyndigheten får också upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som inte kräver någon konsekvensbedömning avseende dataskydd. Tillsynsmyndigheten ska översända dessa förteckningar till styrelsen.

6. Innan de förteckningar som avses i punkterna 4 och 5 antas ska den behöriga tillsynsmyndigheten tillämpa den mekanism för enhetlighet som avses i artikel 63 om en sådan förteckning inbegriper behandling som rör erbjudandet av varor eller tjänster till registrerade, eller övervakning av deras beteende i flera medlemsstater, eller som väsentligt kan påverka den fria rörligheten för personuppgifter i unionen.

7. Bedömningen ska innehålla åtminstone

a) en systematisk beskrivning av den planerade behandlingen och behandlingens syften, inbegripet, när det är lämpligt, den personuppgiftsansvariges berättigade intresse,

b) en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,

c) en bedömning av de risker för de registrerades rättigheter och friheter som avses i punkt 1, och

d) de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att denna förordning efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

8. De berörda personuppgiftsansvarigas eller personuppgiftsbiträdenas efterlevnad av godkända uppförandekoder enligt artikel 40 ska på lämpligt sätt beaktas vid bedömningen av konsekvenserna av de behandlingar som utförs av dessa personuppgiftsansvariga eller personuppgiftsbiträden, framför allt när det gäller att ta fram en konsekvensbedömning avseende dataskydd.

9. Den personuppgiftsansvarige ska, när det är lämpligt, inhämta synpunkter från de registrerade eller deras företrädare om den avsedda behandlingen, utan att det påverkar skyddet av kommersiella eller allmänna intressen eller behandlingens säkerhet.

10. Om behandling enligt artikel 6.1 c eller e har en rättslig grund i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av, reglerar den rätten den aktuella specifika behandlingsåtgärden eller serien av åtgärder i fråga och en konsekvensbedömning avseende dataskydd redan har genomförts som en del av en allmän konsekvensbedömning i samband med antagandet av denna rättsliga grund, ska punkterna 1–7 inte gälla, om inte medlemsstaterna anser det nödvändigt att utföra en sådan bedömning före behandlingen.

11. Den personuppgiftsansvarige ska vid behov genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen avseende dataskydd åtminstone när den risk som behandlingen medför förändras.

Artikel 36

Förhandssamråd

1. Den personuppgiftsansvarige ska samråda med tillsynsmyndigheten före behandling om en konsekvensbedömning avseende dataskydd enligt artikel 35 visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken.

2. Om tillsynsmyndigheten anser att den planerade behandling som avses i punkt 1 skulle strida mot denna förordning, särskilt om den personuppgiftsansvarige inte i tillräcklig mån har fastställt eller reducerat risken, ska tillsynsmyndigheten inom en period på högst åtta veckor från det att begäran om samråd mottagits, ge den personuppgiftsansvarige och i tillämpliga fall personuppgiftsbiträdet skriftliga råd och får utnyttja alla de befogenheter som den har enligt artikel 58. Denna period får förlängas med sex veckor beroende på hur komplicerad den planerade behandlingen är. Tillsynsmyndigheten ska informera den personuppgiftsansvarige och, i tillämpliga fall, personuppgiftsbiträdet om en sådan förlängning inom en månad från det att begäran om samråd mottagits, tillsammans med orsakerna till förseningen. Dessa perioder får tillfälligt upphöra att löpa i avvaktan på att tillsynsmyndigheten erhåller den information som den har begärt med tanke på samrådet.

3. Vid samråd med tillsynsmyndigheten enligt punkt 1 ska den personuppgiftsansvarige till tillsynsmyndigheten lämna

a) i tillämpliga fall de respektive ansvarsområdena för de personuppgiftsansvariga, gemensamt personuppgiftsansvariga och personuppgiftsbiträden som medverkar vid behandlingen, framför allt vid behandling inom en koncern,

b) ändamålen med och medlen för den avsedda behandlingen,

c) de åtgärder som vidtas och de garantier som lämnas för att skydda de registrerades rättigheter och friheter enligt denna förordning,

d) i tillämpliga fall kontaktuppgifter till dataskyddsombudet,

e) konsekvensbedömningen avseende dataskydd enligt artikel 35, och

f) all annan information som begärs av tillsynsmyndigheten.

4. Medlemsstaterna ska samråda med tillsynsmyndigheten vid utarbetandet av ett förslag till lagstiftningsåtgärd som ska antas av ett nationellt parlament eller av en regleringsåtgärd som grundar sig på en sådan lagstiftningsåtgärd som rör behandling.

5. Trots vad som sägs i punkt 1 får det i medlemsstaternas nationella rätt krävas att personuppgiftsansvariga ska samråda med, och erhålla förhandstillstånd av, tillsynsmyndigheten när det gäller en personuppgiftsansvarigs behandling för utförandet av en uppgift som den personuppgiftsansvarige utför av allmänt intresse, inbegripet behandling avseende social trygghet och folkhälsa.

Avsnitt 4

Dataskyddsombud

Artikel 37

Utnämning av dataskyddsombudet

1. Den personuppgiftsansvarige och personuppgiftsbiträdet ska under alla omständigheter utnämna ett dataskyddsombud om

a) behandlingen genomförs av en myndighet eller ett offentligt organ, förutom när detta sker som en del av domstolarnas dömande verksamhet,

b) den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling som, på grund av sin karaktär, sin omfattning och/eller sina ändamål, kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller

c) den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter i enlighet med artikel 9 och personuppgifter som rör fällande domar i brottmål och överträdelser, som avses i artikel 10.

2. En koncern får utnämna ett enda dataskyddsombud om det på varje etableringsort är lätt att nå ett dataskyddsombud.

3. Om den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet eller ett offentligt organ, får ett enda dataskyddsombud utnämnas för flera sådana myndigheter eller organ, med hänsyn till deras organisationsstruktur och storlek.

4. I andra fall än de som avses i punkt 1 får eller, om så krävs enligt unionsrätten eller medlemsstaternas nationella rätt, ska den personuppgiftsansvarige eller personuppgiftsbiträdet eller sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden utnämna ett dataskyddsombud. Dataskyddsombudet får agera för sådana sammanslutningar och andra organ som företräder personuppgiftsansvariga eller personuppgiftsbiträden.

5. Dataskyddsombudet ska utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i artikel 39.

6. Dataskyddsombudet får ingå i den personuppgiftsansvariges eller personuppgiftsbiträdets personal, eller utföra uppgifterna på grundval av ett tjänsteavtal.

7. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.

Artikel 38

Dataskyddsombudets ställning

1. Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

2. Den personuppgiftsansvarige och personuppgiftsbiträdet ska stödja dataskyddsombudet i utförandet av de uppgifter som avses i artikel 39 genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap.

3. Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att uppgiftskyddsombudet inte tar emot instruktioner som gäller utförandet av dessa uppgifter. Han eller hon får inte avsättas eller bli föremål för sanktioner av den personuppgiftsansvarige eller personuppgiftsbiträdet för att ha utfört sina uppgifter. Dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå.

4. Den registrerade får kontakta dataskyddsombudet med avseende på alla frågor som rör behandlingen av dennes personuppgifter och utövandet av dennes rättigheter enligt denna förordning.

5. Dataskyddsombudet ska, när det gäller dennes genomförande av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt.

6. Dataskyddsombudet får fullgöra andra uppgifter och uppdrag. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska se till att sådana uppgifter och uppdrag inte leder till en intressekonflikt.

Artikel 39

Dataskyddsombudets uppgifter

1. Dataskyddsombudet ska ha minst följande uppgifter:

a) Att informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar om deras skyldigheter enligt denna förordning och andra av unionens eller medlemsstaternas dataskyddsbestämmelser.

b) Att övervaka efterlevnaden av denna förordning, av andra av unionens eller medlemsstaternas dataskyddsbestämmelser och av den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.

c) Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den enligt artikel 35.

d) Att samarbeta med tillsynsmyndigheten.

e) Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, inbegripet det förhandssamråd som avses i artikel 36, och vid behov samråda i alla andra frågor.

2. Dataskyddsombudet ska vid utförandet av sina uppgifter ta vederbörlig hänsyn till de risker som är förknippade med behandling, med beaktande av behandlingens art, omfattning, sammanhang och syften.

Avsnitt 5

Uppförandekod och certifiering

Artikel 40

Uppförandekoder

1. Medlemsstaterna, tillsynsmyndigheterna, styrelsen och kommissionen ska uppmuntra utarbetandet av uppförandekoder avsedda att bidra till att denna förordning genomförs korrekt, med hänsyn till särdragen hos de olika sektorer där behandling sker, och de särskilda behoven hos mikroföretag samt små och medelstora företag.

2. Sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden får utarbeta uppförandekoder, eller ändra eller utöka sådana koder, i syfte att specificera tillämpningen av denna förordning, till exempel när det gäller

a) rättvis och öppen behandling,

b) personuppgiftsansvarigas berättigade intressen i särskilda sammanhang,

c) insamling av personuppgifter,

d) pseudonymisering av personuppgifter,

e) information till allmänheten och de registrerade,

f) utövande av registrerades rättigheter,

g) information till och skydd av barn samt metoderna för att erhålla samtycke från de personer som har föräldraansvar för barn,

h) åtgärder och förfaranden som avses i artiklarna 24 och 25 samt åtgärder för att säkerställa säkerhet vid behandling i enlighet med artikel 32,

i) anmälan av personuppgiftsincidenter till tillsynsmyndigheter och meddelande av sådana personuppgiftsincidenter till registrerade,

j) överföring av personuppgifter till tredjeländer eller internationella organisationer,

k) utomrättsliga förfaranden och andra tvistlösningsförfaranden för lösande av tvister mellan personuppgiftsansvariga och registrerade när det gäller behandling, utan att detta påverkar registrerades rättigheter enligt artiklarna 77 och 79.

3. Uppförandekoder som är godkända i enlighet med punkt 5 i denna artikel och som har allmän giltighet enligt punkt 9 i denna artikel får, förutom att de iakttas av personuppgiftsansvariga eller personuppgiftsbiträden som omfattas av denna förordning, även iakttas av personuppgiftsansvariga eller personuppgiftsbiträden som inte omfattas av denna förordning enligt artikel 3, för att tillhandahålla lämpliga garantier inom ramen för överföringar av personuppgifter till tredjeländer eller internationella organisationer enligt villkoren i artikel 46.2 e. Sådana personuppgiftsansvariga eller personuppgiftsbiträden ska göra bindande och verkställbara åtaganden, genom avtal eller andra rättsligt bindande instrument, att tillämpa dessa lämpliga garantier inbegripet när det gäller registrerades rättigheter.

4. Den uppförandekod som avses i punkt 2 i den här artikeln ska innehålla mekanismer som gör det möjligt för det organ som avses i artikel 41.1 att utföra den obligatoriska övervakningen av att dess bestämmelser efterlevs av personuppgiftsansvariga och personuppgiftsbiträden som tillämpar den, utan att det påverkar uppgifter eller befogenheter för de tillsynsmyndigheter som är behöriga enligt artikel 55 eller 56.

5. Sammanslutningar och andra organ som avses i punkt 2 i den här artikeln som avser att utarbeta en uppförandekod eller ändra eller utöka befintliga uppförandekoder ska inge utkastet till uppförandekod, ändringen eller utökningen till den tillsynsmyndighet som är behörig enligt artikel 55. Tillsynsmyndigheten ska yttra sig om huruvida utkastet till uppförandekod, ändring eller utökning överensstämmer med denna förordning och ska godkänna ett det utkastet till kod, ändring eller utökning om den finner att tillräckliga garantier tillhandahålls.

6. Om utkastet till kod, eller en ändring eller utökning, godkänns i enlighet med punkt 5, och om den berörda uppförandekoden inte avser behandling i flera medlemsstater, ska tillsynsmyndigheten registrera och offentliggöra uppförandekoden.

7. Om ett utkast till uppförandekod avser behandling i flera medlemsstater ska den tillsynsmyndighet som är behörig enligt artikel 55 innan den godkänner utkastet till kod, ändring eller utökning, inom ramen för det förfarande som avses i artikel 63 överlämna det till styrelsen som ska avge ett yttrande om huruvida utkastet till kod, ändring eller utökning är förenlig med denna förordning eller, i de fall som avses i punkt 3 i den här artikeln, tillhandahåller lämpliga garantier.

8. Om det i det yttrande som avses i punkt 7 bekräftas att utkastet till kod, ändring eller utökning är förenligt med denna förordning, eller, i de fall som avses i punkt 3, tillhandahåller lämpliga garantier, ska styrelsen inlämna sitt yttrande till kommissionen.

9. Kommissionen får, genom genomförandeakter, besluta att den godkända koden, ändringen eller utökningen som getts in till den enligt punkt 8 i den här artikeln har allmän giltighet inom unionen. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

10. Kommissionen ska se till att de godkända koder om vilka det har beslutats att de har allmän giltighet enligt punkt 9 offentliggörs på lämpligt sätt.

11. Styrelsen ska samla alla godkända uppförandekoder, ändringar och utökningar i ett register och offentliggöra dem på lämpligt sätt.

Artikel 41

Övervakning av godkända uppförandekoder

1. Utan att det påverkar den berörda tillsynsmyndighetens uppgifter och befogenheter enligt artiklarna 57 och 58 får övervakningen av efterlevnaden av en uppförandekod i enlighet med artikel 40 utföras av ett organ som har en lämplig expertnivå i förhållande till kodens syfte och som ackrediteras för detta ändamål av den behöriga tillsynsmyndigheten.

2. Ett organ som avses i punkt 1 får ackrediteras för att övervaka efterlevnaden av en uppförandekod om detta organ har

a) visat sitt oberoende och sin expertis i förhållande till uppförandekodens syfte på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande,

b) upprättat förfaranden varigenom det kan bedöma de berörda personuppgiftsansvarigas och personuppgiftsbiträdenas lämplighet för att tillämpa uppförandekoden, övervaka att de efterlever dess bestämmelser och regelbundet se över hur den fungerar,

c) upprättat förfaranden och strukturer för att hantera klagomål om överträdelser av uppförandekoden eller det sätt på vilket uppförandekoden har tillämpats, eller tillämpas, av en personuppgiftsansvarig eller ett personuppgiftsbiträde, och för att göra dessa förfaranden och strukturer synliga för registrerade och för allmänheten, och

d) på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande visat att dess uppgifter och uppdrag inte leder till en intressekonflikt.

3. Den behöriga tillsynsmyndigheten ska inlämna utkastet till kriterier för ackreditering av ett organ som avses i punkt 1 i den här artikeln till styrelsen i enlighet med den mekanism för enhetlighet som avses i artikel 63.

4. Utan att det påverkar den behöriga tillsynsmyndighetens uppgifter och befogenheter och tillämpningen av bestämmelserna i kapitel VIII ska ett organ som avses i punkt 1 i denna artikel, med förbehåll för tillräckliga skyddsåtgärder, vidta lämpliga åtgärder i fall av en personuppgiftsansvarigs eller ett personuppgiftsbiträdes överträdelse av uppförandekoden, inbegripet avstängning eller uteslutande av den personuppgiftsansvarige eller personuppgiftsbiträdet från uppförandekoden. Det ska informera den behöriga tillsynsmyndigheten om sådana åtgärder och skälen för att de vidtagits.

5. Den behöriga tillsynsmyndigheten ska återkalla ackrediteringen av ett organ som avses i punkt 1 om villkoren för ackrediteringen inte, eller inte längre, uppfylls eller om åtgärder som vidtagits av organet strider mot denna förordning.

6. Denna artikel ska inte gälla behandling som utförs av offentliga myndigheter och organ.

Artikel 42

Certifiering

1. Medlemsstaterna, tillsynsmyndigheterna, styrelsen och kommissionen ska uppmuntra, särskilt på unionsnivå, införandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som syftar till att visa att personuppgiftsansvarigas eller personuppgiftsbiträdens behandling är förenlig med denna förordning. De särskilda behoven hos mikroföretag samt små och medelstora företag ska beaktas.

2. Certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som är godkända enligt punkt 5 i denna artikel får, förutom att de iakttas av personuppgiftsansvariga eller personuppgiftsbiträden som omfattas av denna förordning, inrättas för att visa att det föreligger lämpliga garantier som tillhandahålls av personuppgiftsansvariga och personuppgiftsbiträden som inte omfattas av denna förordning enligt artikel 3, inom ramen för överföringar av personuppgifter till tredjeländer eller internationella organisationer enligt villkoren i artikel 46.2 f. Sådana personuppgiftsansvariga eller personuppgiftsbiträden ska göra bindande och verkställbara åtaganden, genom avtal eller andra rättsligt bindande instrument, att tillämpa dessa lämpliga garantier, inbegripet när det gäller registrerades rättigheter.

3. Certifieringen ska vara frivillig och tillgänglig via ett öppet förfarande.

4. En certifiering i enlighet med denna artikel minskar inte den personuppgiftsansvariges eller personuppgiftsbiträdets ansvar för att denna förordning efterlevs och påverkar inte uppgifter och befogenheter för de tillsynsmyndigheter som är behöriga enligt artikel 55 eller 56.

5. En certifiering i enlighet med denna artikel ska utfärdas av de certifieringsorgan som avses i artikel 43 eller av den behöriga tillsynsmyndigheten på grundval av kriterier som godkänts av den behöriga myndigheten enligt artikel 58.3 eller av styrelsen enligt artikel 63. Om kriterierna har godkänts av styrelsen får detta leda till en gemensam certifiering, det europeiska sigillet för dataskydd.

6. Den personuppgiftsansvarige eller det personuppgiftsbiträde som låter sin behandling av uppgifter omfattas av certifieringsmekanismen ska förse det certifieringsorgan som avses i artikel 43 eller, i tillämpliga fall, den behöriga tillsynsmyndigheten, med all information och tillgång till behandlingsförfaranden som krävs för att genomföra certifieringsförfarandet.

7. Certifiering ska utfärdas till en personuppgiftsansvarig eller ett personuppgiftsbiträde för en period på högst tre år och får förnyas på samma villkor under förutsättning att kraven fortsätter att vara uppfyllda. Certifiering ska, i tillämpliga fall, återkallas av de certifieringsorgan som avses i artikel 43 eller av den behöriga tillsynsmyndigheten om kraven för certifieringen inte eller inte längre uppfylls.

8. Styrelsen ska samla alla certifieringsmekanismer och sigill och märkningar för dataskydd i ett register och offentliggöra dem på lämpligt sätt.

Artikel 43

Certifieringsorgan

1. Utan att det påverkar den behöriga tillsynsmyndighetens uppgifter och befogenheter enligt artiklarna 57 och 58 ska certifieringsorgan som har lämplig nivå av expertis i fråga om dataskydd, efter att ha informerat tillsynsmyndigheten för att den ska kunna utöva sina befogenheter enligt artikel 58.2 h när så är nödvändigt, utfärda och förnya certifiering. Medlemsstat ska säkerställa att dessa certifieringsorgan är ackrediterade av en av eller båda följande:

a) Den tillsynsmyndighet som är behörig enligt artikel 55 eller 56,

b) det nationella ackrediteringsorgan som utsetts i enlighet med Europaparlamentets och rådets förordning (EG) nr 765/2008 ( ) i enlighet med EN-ISO/IEC 17065/2012 och med de ytterligare krav som fastställts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56.

2. Certifieringsorgan som avses i punkt 1 får ackrediteras i enlighet med den punkten endast om de har

a) visat oberoende och expertis i förhållande till certifieringens syfte på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande,

( ) Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

b) förbundit sig att respektera de kriterier som avses i artikel 42.5 och godkänts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56, eller av styrelsen enligt artikel 63,

c) upprättat förfaranden för utfärdande, periodisk översyn och återkallande av certifiering, sigill och märkningar för dataskydd,

d) upprättat förfaranden och strukturer för att hantera klagomål om överträdelser av certifieringen eller det sätt på vilket certifieringen har tillämpats, eller tillämpas, av en personuppgiftsansvarig eller ett personuppgiftsbiträde, och för att göra dessa förfaranden och strukturer synliga för registrerade och för allmänheten, och

e) på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande visat att deras uppgifter och uppdrag inte leder till en intressekonflikt.

3. Ackrediteringen av certifieringsorgan som avses i punkterna 1 och 2 i denna artikel ska ske på grundval av kriterier som godkänts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56, eller av styrelsen enligt artikel 63. I händelse av ackreditering enligt punkt 1 b i den här artikeln ska dessa krav komplettera dem som föreskrivs i förordning (EG) nr 765/2008 och de tekniska regler som beskriver certifieringsorganens metoder och förfaranden.

4. De certifieringsorgan som avses i punkt 1 ska ansvara för den korrekta bedömning som leder till certifieringen eller återkallelsen av certifieringen, utan att det påverkar den personuppgiftsansvariges eller personuppgiftsbiträdets ansvar att efterleva denna förordning. Ackrediteringen ska utfärdas för en period på högst fem år och får förnyas på samma villkor under förutsättning att certifieringsorganet uppfyller de krav som anges i denna artikel.

5. De certifieringsorgan som avses i punkt 1 ska informera de behöriga tillsynsmyndigheterna om orsakerna till beviljandet eller återkallelsen av den begärda certifieringen.

6. De krav som avses i punkt 3 i den här artikeln och de kriterier som avses i artikel 42.5 ska offentliggöras av tillsynsmyndigheten i ett lättillgängligt format. Tillsynsmyndigheterna ska också översända dessa krav och kriterier till styrelsen. Styrelsen ska samla alla certifieringsmekanismer och sigill för dataskydd i ett register och offentliggöra dem på lämpligt sätt.

7. Utan att det påverkar tillämpningen av kapitel VIII ska den behöriga tillsynsmyndigheten eller det nationella ackrediteringsorganet återkalla ett certifieringsorgans ackreditering enligt punkt 1 i denna artikel om villkoren för ackrediteringen inte, eller inte längre, uppfylls eller om åtgärder som vidtagits av certifieringsorganet strider mot denna förordning.

8. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 92 i syfte att närmare ange de krav som ska tas i beaktande för de certifieringsmekanismer för dataskydd som avses i artikel 42.1.

9. Kommissionen får anta genomförandeakter för att fastställa tekniska standarder för certifieringsmekanismer och sigill och märkningar för dataskydd samt rutiner för att främja och erkänna dessa certifieringsmekanismer, sigill och märkningar. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

KAPITEL V

Överföring av personuppgifter till tredjeländer eller internationella organisationer

Artikel 44

Allmän princip för överföring av uppgifter

Överföring av personuppgifter som är under behandling eller är avsedda att behandlas efter det att de överförts till ett tredjeland eller en internationell organisation får bara ske under förutsättning att den personuppgiftsansvarige och personuppgiftsbiträdet, med förbehåll för övriga bestämmelser i denna förordning, uppfyller villkoren i detta kapitel, inklusive för vidare överföring av personuppgifter från tredjelandet eller den internationella organisationen till ett annat tredjeland eller en annan internationell organisation. Alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den nivå på skyddet av fysiska personer som säkerställs genom denna förordning inte undergrävs.

Artikel 45

Överföring på grundval av ett beslut om adekvat skyddsnivå

1. Personuppgifter får överföras till ett tredjeland eller en internationell organisation om kommissionen har beslutat att tredjelandet, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå. En sådan överföring ska inte kräva något särskilt tillstånd.

2. När kommissionen bedömer om en adekvat skyddsnivå föreligger ska den särskilt beakta

a) rättsstatsprincipen, respekten för de mänskliga rättigheterna och de grundläggande friheterna, relevant lagstiftning, både allmän lagstiftning och sektorslagstiftning, inklusive avseende allmän säkerhet, försvar, nationell säkerhet och straffrätt och offentliga myndigheters tillgång till personuppgifter samt tillämpningen av sådan lagstiftning, dataskyddsregler, yrkesregler och säkerhetsbestämmelser, inbegripet regler för vidare överföring av personuppgifter till ett annat tredjeland eller en annan internationell organisation, som ska följas i det landet eller den internationella organisationen, rättspraxis samt faktiska och verkställbara rättigheter för registrerade och effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs,

b) huruvida det finns en eller flera effektivt fungerande oberoende tillsynsmyndigheter i tredjelandet, eller som utövar tillsyn över den internationella organisationen, som har ansvar för att säkerställa och kontrollera att dataskyddsregler följs, inklusive lämpliga verkställighetsbefogenheter, ge de registrerade råd och assistans när det gäller utövandet av deras rättigheter och samarbeta med medlemsstaternas tillsynsmyndigheter, och

c) vilka internationella åtaganden det berörda tredjelandet eller den berörda internationella organisationen har gjort, eller andra skyldigheter som följer av rättsligt bindande konventioner eller instrument samt av dess deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter.

3. Kommissionen får, efter att ha bedömt om det föreligger en adekvat skyddsnivå, genom en genomförandeakt besluta att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland, eller en internationell organisation säkerställer en adekvat skyddsnivå i den mening som avses i punkt 2 i den här artikeln. Genomförandeakten ska inrätta en mekanism för regelbunden översyn, minst vart fjärde år, som ska beakta all relevant utveckling i det tredjelandet eller den internationella organisationen. Beslutets territoriella och sektorsmässiga tillämpning ska regleras i genomförandeakten, där det också i förekommande fall ska anges vilken eller vilka myndigheter som är tillsynsmyndighet(er) enligt punkt 2 b i den här artikeln. Genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

4. Kommissionen ska fortlöpande övervaka utveckling i tredjeländer och internationella organisationer vilken kan påverka hur beslut som antagits enligt punkt 3 i den här artikeln och beslut som antagits på grundval av artikel 25.6 i direktiv 95/46/EG fungerar.

5. Kommissionen ska, när tillgänglig information visar, i synnerhet efter den översyn som avses i punkt 3 i den här artikeln, att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom tredjelandet i fråga eller en internationell organisation inte längre säkerställer adekvat skydd i den mening som avses i punkt 2 i den här artikeln och, i den mån det behövs, genom genomförandeakter återkalla, ändra eller upphäva det beslut som avses i punkt 3 i den här artikeln utan retroaktiv verkan. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

När det föreligger vederbörligen motiverade och tvingande skäl till skyndsamhet ska kommissionen anta omedelbart tillämpliga genomförandeakter i enlighet med det förfarande som avses i artikel 93.3.

6. Kommissionen ska samråda med tredjelandet eller den internationella organisationen i fråga för att lösa den situation som lett till beslutet enligt punkt 5.

7. Beslut enligt punkt 5 i den här artikeln ska inte påverka överföring av personuppgifter till tredjelandet, ett territorium eller en eller flera specificerade sektorer inom tredjelandet, eller den internationella organisationen i fråga enligt artiklarna 46–49.

8. Kommissionen ska i *Europeiska unionens officiella tidning* och på sin webbplats offentliggöra en förteckning över de tredjeländer och de territorier och specificerade sektorer i ett givet tredjeland samt de internationella organisationer för vilka den har fastställt att en adekvat skyddsnivå inte eller inte längre säkerställs.

9. De beslut som antas av kommissionen på grundval av artikel 25.6 i direktiv 95/46/EG ska förbli i kraft tills de ändrats, ersatts eller upphävts av ett kommissionsbeslut som antagits i enlighet med punkt 3 eller 5 i den här artikeln.

Artikel 46

Överföring som omfattas av lämpliga skyddsåtgärder

1. I avsaknad av ett beslut i enlighet med artikel 45.3, får en personuppgiftsansvarig eller ett personuppgiftsbiträde endast överföra personuppgifter till ett tredjeland eller en internationell organisation efter att ha vidtagit lämpliga skyddsåtgärder, och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga.

2. Lämpliga skyddsåtgärder enligt punkt 1 får, utan att det krävs särskilt tillstånd från en övervakningsmyndighet, ta formen av

a) ett rättsligt bindande och verkställbart instrument mellan offentliga myndigheter eller organ,

b) bindande företagsbestämmelser i enlighet med artikel 47,

c) standardiserade dataskyddsbestämmelser som antas av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2,

d) standardiserade dataskyddsbestämmelser som antagits av en tillsynsmyndighet och godkänts av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2,

e) en godkänd uppförandekod enlig artikel 40 tillsammans med rättsligt bindande och verkställbara åtaganden för den personuppgiftsansvarige eller personuppgiftsbiträdet i tredjelandet att tillämpa lämpliga skyddsåtgärder, även när det gäller registrerades rättigheter, eller

f) en godkänd certifieringsmekanism enlig artikel 42 tillsammans med rättsligt bindande och verkställbara åtaganden för den personuppgiftsansvarige, personuppgiftsbiträdet i tredjelandet att tillämpa lämpliga skyddsåtgärder, även när det gäller de registrerades rättigheter.

3. Med förbehåll för tillstånd från den behöriga tillsynsmyndigheten, får lämpliga skyddsåtgärder enligt punkt 1 också i synnerhet ta formen av

a) avtalsklausuler mellan den personuppgiftsansvarige eller personuppgiftsbiträdet och den personuppgiftsansvarige, personuppgiftsbiträdet eller mottagaren av personuppgifterna i tredjelandet eller den internationella organisationen, eller

b) bestämmelser som ska införas i administrativa överenskommelser mellan offentliga myndigheter eller organ vilka inbegriper verkställbara och faktiska rättigheter för registrerade.

4. Tillsynsmyndigheten ska tillämpa den mekanism för enhetlighet som avses i artikel 63 i de fall som avses i punkt 3 i den här artikeln.

5. Tillstånd från en medlemsstat eller tillsynsmyndighet på grundval av artikel 26.2 i direktiv 95/46/EG ska förbli giltigt tills det, vid behov, ändrats, ersatts eller upphävts av den tillsynsmyndigheten. De beslut som fattas av kommissionen på grundval av artikel 26.4 i direktiv 95/46/EG ska förbli i kraft tills de, vid behov, ändrats, ersatts eller upphävts av ett kommissionsbeslut som antagits i enlighet med punkt 2 i den här artikeln.

Artikel 47

Bindande företagsbestämmelser

1. Den behöriga tillsynsmyndigheten ska godkänna bindande företagsbestämmelser i enlighet med den mekanism för enhetlighet som föreskrivs i artikel 63 under förutsättning att de

a) är rättslig bindande, tillämpas på, och verkställs av alla delar som berörs inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet, inklusive deras anställda,

b) innehåller uttryckliga bestämmelser om de registrerades lagstadgade rättigheter när det gäller behandlingen av deras personuppgifter, och

c) uppfyller villkoren i punkt 2.

2. De bindande företagsbestämmelser som avses i punkt 1 ska närmare ange åtminstone följande:

a) struktur och kontaktuppgifter för den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet och för var och en av dess medlemmar,

b) vilka överföringar eller uppsättningar av överföringar av uppgifter som omfattas, inklusive kategorierna av personuppgifter, typen av behandling och dess ändamål, den typ av registrerade som berörs samt vilket eller vilka tredjeländer som avses,

c) bestämmelsernas rättsligt bindande natur, såväl internt som externt,

d) tillämpningen av allmänna principer för dataskydd, särskilt avgränsning av syften, uppgiftsminimering, begränsade lagringsperioder, datakvalitet, inbyggt dataskydd och dataskydd som standard, rättslig grund för behandling, behandling av särskilda kategorier av personuppgifter, åtgärder för att säkerställa datasäkerhet och villkoren när det gäller vidare överföring av uppgifter till organ som inte är bundna av bindande företagsbestämmelser,

e) de registrerades rättigheter avseende behandling och medlen för att utöva dessa rättigheter, inklusive rätten att inte bli föremål för beslut grundade enbart på automatisk behandling, inklusive profilering, enligt artikel 22, rätten att inge klagomål till den behöriga tillsynsmyndigheten och till behöriga domstolar i medlemsstaterna enligt artikel 79, rätten till prövning samt i förekommande fall rätten till kompensation för överträdelse av de bindande företagsbestämmelserna,

f) att den personuppgiftsansvarige eller personuppgiftsbiträdet som är etablerad inom en medlemsstats territorium tar på sig ansvaret om en berörd enhet som inte är etablerad inom unionen bryter mot de bindande företagsbestämmelserna; den personuppgiftsansvarige eller personuppgiftsbiträdet får helt eller delvis undantas från denna skyldighet endast på villkor att det kan visas att den berörda enheten i företagsgruppen inte kan hållas ansvarig för den skada som har uppkommit,

g) hur de registrerade ska informeras om innehållet i de bindande företagsbestämmelserna, särskilt de bestämmelser som avses i leden d, e och f i denna punkt utöver den information som avses i artiklarna 13 och 14,

h) uppgifterna för varje dataskyddsombud som utsetts i enlighet med artikel 37, eller varje annan person eller enhet med ansvar för kontrollen av att de bindande företagsbestämmelserna följs inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet, samt i fråga om utbildning och hantering av klagomål,

i) förfaranden för klagomål,

j) rutinerna inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet för att kontrollera att de bindande företagsreglerna följs; sådana rutiner ska inbegripa dataskyddstillsyn och metoder för att säkerställa korrigerande åtgärder för att skydda de registrerades rättigheter; resultaten av sådana kontroller bör meddelas den person eller enhet som avses i led h och styrelsen i det kontrollerande företaget i koncernen eller gruppen av företag som deltar i gemensam ekonomisk verksamhet, och bör på begäran vara tillgänglig för den behöriga tillsynsmyndigheten,

k) rutinerna för att rapportera och dokumentera ändringar i bestämmelserna, samt rutinerna för att rapportera dessa ändringar till tillsynsmyndigheten,

l) rutinerna för att samarbeta med tillsynsmyndigheten i syfte att se till att alla medlemmar i den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet följer reglerna, särskilt genom att meddela tillsynsmyndigheten resultaten av kontroller av de åtgärder som avses i led j,

m) rutinerna för att till den behöriga tillsynsmyndigheten rapportera alla rättsliga krav som en medlem i koncernen eller gruppen av företag som deltar i gemensam ekonomisk verksamhet är underkastad i ett tredjeland och som sannolikt kommer att ha en avsevärd negativ inverkan på de garantier som ges genom de bindande företagsbestämmelserna, och

n) lämplig utbildning om dataskydd för personal som har ständig eller regelbunden tillgång till personuppgifter.

3. Kommissionen får närmare ange vilket format och vilka rutiner som ska användas för de personuppgiftsansvarigas, personuppgiftsbiträdenas och tillsynsmyndigheternas utbyte av information om bindande företagsbestämmelser i den mening som avses i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

Artikel 48

Överföringar och utlämnanden som inte är tillåtna enligt unionsrätten

Domstolsbeslut eller beslut från myndigheter i tredjeland där det krävs att en personuppgiftsansvarig eller ett personuppgiftsbiträde överför eller lämnar ut personuppgifter får erkännas eller genomföras på något som helst sätt endast om det grundar sig på en internationell överenskommelse, såsom ett avtal om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen eller en medlemsstat, utan att detta påverkar andra grunder för överföring enligt detta kapitel.

Artikel 49

Undantag i särskilda situationer

1. Om det inte föreligger något beslut om adekvat skyddsnivå enligt artikel 45.3, eller om lämpliga skyddsåtgärder enligt artikel 46, inbegripet bindande företagsbestämmelser, får en överföring eller uppsättning av överföringar av personuppgifter till ett tredjeland eller en internationell organisation endast ske om något av följande villkor är uppfyllt:

a) Den registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med sådana överföringar för den registrerade när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder.

b) Överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den personuppgiftsansvarige eller för att genomföra åtgärder som föregår ett sådant avtal på den registrerades begäran.

c) Överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den personuppgiftsansvarige och en annan fysisk eller juridisk person i den registrerades intresse.

d) Överföringen är nödvändig av viktiga skäl som rör allmänintresset.

e) Överföringen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

f) Överföringen är nödvändig för att skydda den registrerades eller andra personers grundläggande intressen, när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.

g) Överföringen görs från ett register som enligt unionsrätten eller medlemsstaternas nationella rätt är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse, men endast i den utsträckning som de i unionsrätten eller i medlemsstaternas nationella rätt angivna villkoren för tillgänglighet uppfylls i det enskilda fallet.

När en överföring inte skulle kunna grundas på en bestämmelse i artikel 45 eller 46, inklusive bestämmelserna om bindande företagsbestämmelser, och inget av undantagen för en särskild situation som avses i första stycket i den här punkten är tillämpligt, får en överföring till ett tredjeland eller en internationell organisation äga rum endast omöverföringen inte är repetitiv, endast gäller ett begränsat antal registrerade, är nödvändig för ändamål som rör den personuppgiftsansvariges tvingande berättigade intressen och den registrerades intressen eller rättigheter och friheter inte väger tyngre, och den personuppgiftsansvarige har bedömt samtliga omständigheter kring överföringen av uppgifter och på grundval av denna bedömning vidtagit lämpliga skyddsåtgärder för att skydda personuppgifter. Den personuppgiftsansvarige ska informera tillsynsmyndigheten om överföringen. Den personuppgiftsansvarige ska utöver tillhandahållande av den information som avses i artiklarna 13 och 14 informera den registrerade om överföringen och om de tvingande berättigade intressen som eftersträvas.

2. En överföring enligt led g i punkt 1 första stycket får inte omfatta alla personuppgifter eller hela kategorier av personuppgifter som finns i registret. Om registret är avsett att vara tillgängligt för personer med ett berättigat intresse ska överföringen göras endast på begäran av dessa personer eller om de själva är mottagarna.

3. Leden a, b och c i punkt 1 första stycket samt andra stycket i samma punkt ska inte gälla åtgärder som vidtas av offentliga myndigheter som ett led i myndighetsutövning.

4. Det allmänintresse som avses i led d i punkt 1 första stycket ska vara erkänt i unionsrätten eller i den nationella rätt som den personuppgiftsansvarige omfattas av.

5. Saknas beslut om adekvat skyddsnivå, får unionsrätten eller medlemsstaternas nationella rätt med hänsyn till viktiga allmänintressen uttryckligen fastställa gränser för överföringen av specifika kategorier av personuppgifter till ett tredjeland eller en internationell organisation. Medlemsstaterna ska underrätta kommissionen om sådana bestämmelser.

6. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska bevara uppgifter både om bedömningen och om de lämpliga skyddsåtgärder som avses i punkt 1 andra stycket i den här artikeln i det register som avses i artikel 30.

Artikel 50

Internationellt samarbete för skydd av personuppgifter

När det gäller tredjeländer och internationella organisationer ska kommissionen och tillsynsmyndigheterna vidta lämpliga åtgärder för att

a) utveckla rutiner för det internationella samarbetet för att underlätta en effektiv tillämpning av lagstiftningen om skydd av personuppgifter,

b) på internationell nivå erbjuda ömsesidigt bistånd för en effektiv tillämpning av lagstiftningen om skydd av personuppgifter, bland annat genom underrättelse, hänskjutande av klagomål, bistånd vid utredningar samt informationsutbyte, med iakttagande av lämpliga skyddsåtgärder för personuppgifter samt skyddet av andra grundläggande rättigheter och friheter,

c) involvera berörda aktörer i diskussioner och åtgärder som syftar till att öka det internationella samarbetet när det gäller tillämpningen av lagstiftningen om skydd av personuppgifter,

d) främja utbyte och dokumentation om lagstiftning och praxis för skydd av personuppgifter, inklusive avseende behörighetskonflikter med tredjeländer.

KAPITEL VI

Oberoende tillsynsmyndigheter

Avsnitt 1

Oberoende ställning

Artikel 51

Tillsynsmyndighet

1. Varje medlemsstat ska föreskriva att en eller flera offentliga myndigheter ska vara ansvariga för att övervaka tillämpningen av denna förordning, i syfte att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling samt att underlätta det fria flödet av sådana uppgifter inom unionen (nedan kallad *tillsynsmyndighet*).

2. Varje tillsynsmyndighet ska bidra till en enhetlig tillämpning av denna förordning i hela unionen. För detta ändamål ska tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen i enlighet med kapitel VII.

3. Om det finns fler än en tillsynsmyndighet i en medlemsstat ska medlemsstaten utse den tillsynsmyndighet som ska företräda dessa myndigheter i styrelsen; medlemsstaten ska också upprätta en rutin för att se till att övriga myndigheter följer reglerna för den mekanism för enhetlighet som avses i artikel 63.

4. Varje medlemsstat ska senast den 25 maj 2018 anmäla till kommissionen vilka nationella bestämmelser den antar i enlighet med detta kapitel, och alla framtida ändringar som rör dessa bestämmelser ska anmälas utan dröjsmål.

Artikel 52

Oberoende

1. Varje tillsynsmyndighet ska vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med denna förordning.

2. Varje tillsynsmyndighets ledamot eller ledamöter ska i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med denna förordning stå fria från utomstående påverkan, direkt såväl som indirekt, och får varken begära eller ta emot instruktioner av någon.

3. Tillsynsmyndighetens ledamöter ska avhålla sig från alla handlingar som är oförenliga med deras skyldigheter och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet som står i strid med deras tjänsteutövning.

4. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet förfogar över de personella, tekniska och finansiella resurser samt de lokaler och den infrastruktur som behövs för att myndigheten ska kunna utföra sina uppgifter och utöva sina befogenheter, inklusive inom ramen för det ömsesidiga biståndet, samarbetet och deltagandet i styrelsens verksamhet.

5. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet väljer och förfogar över egen personal, som ska ta instruktioner uteslutande från den berörda tillsynsmyndighetens ledamot eller ledamöter.

6. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet blir föremål för finansiell kontroll, utan att detta påverkar tillsynsmyndighetens oberoende och att de förfogar över en separat, offentlig årsbudget som kan ingå i den övergripande statsbudgeten eller nationella budgeten.

Artikel 53

Allmänna villkor för tillsynsmyndighetens ledamöter

1. Medlemsstaterna ska föreskriva att varje ledamot av deras tillsynsmyndigheter ska utnämnas genom ett genom ett öppet förfarande med insyn av

— deras parlament,

— deras regering,

— deras statschef, eller

— ett oberoende organ som genom medlemsstatens nationella rätt anförtrotts utnämningen.

2. Varje ledamot ska ha de kvalifikationer, den erfarenhet och den kompetens, särskilt på området skydd av personuppgifter, som krävs för att ledamoten ska kunna utföra sitt uppdrag och utöva sina befogenheter.

3. En ledamots uppdrag ska upphöra då mandattiden löper ut eller om ledamoten avgår eller avsätts från sin tjänst i enlighet med den berörda medlemsstatens nationella rätt.

4. En ledamot får avsättas endast på grund av grov försummelse eller när ledamoten inte längre uppfyller de villkor som krävs för att utföra uppdraget.

Artikel 54

Regler för inrättandet av en tillsynsmyndighet

1. Varje medlemsstat ska fastställa följande i lag:

a) Varje tillsynsmyndighets inrättande.

b) De kvalifikationer och de villkor för lämplighet som krävs för att någon ska kunna utnämnas till ledamot av en tillsynsmyndighet.

c) Regler och förfaranden för att utse varje tillsynsmyndighets ledamot eller ledamöter.

d) Mandattiden för varje tillsynsmyndighets ledamot eller ledamöter, vilken inte får understiga fyra år, utom vid tillsättandet av de första ledamöterna efter den 24 maj 2016, då ett stegvis tillsättningsförfarande med kortare perioder för några av ledamöterna får tillämpas om detta är nödvändigt för att säkerställa myndighetens oberoende.

e) Huruvida varje tillsynsmyndighets ledamot eller ledamöter får ges förnyat mandat, och om så är fallet, för hur många perioder.

f) Vilka villkor som gäller för de skyldigheter som varje tillsynsmyndighets ledamot eller ledamöter och personal har, förbud mot handlingar, yrkesverksamhet och förmåner som står i strid därmed under och efter mandattiden och vilka bestämmelser som gäller för anställningens upphörande.

2. Varje tillsynsmyndighets ledamot eller ledamöter och personal ska i enlighet med unionsrätten eller medlemsstaternas nationella rätt omfattas av tystnadsplikt både under och efter sin mandattid vad avser konfidentiell information som de fått kunskap om under utförandet av deras uppgifter eller utövandet av deras befogenheter. Under mandatperioden ska denna tystnadsplikt i synnerhet gälla rapportering från fysiska personer om överträdelser av denna förordning.

Avsnitt 2

Behörighet, uppgifter och befogenheter

Artikel 55

Behörighet

1. Varje tillsynsmyndighet ska vara behörig att utföra de uppgifter och utöva de befogenheter som tilldelas den enligt denna förordning inom sin egen medlemsstats territorium.

2. Om behandling utförs av myndigheter eller privata organ som agerar på grundval av artikel 6.1 c eller e ska tillsynsmyndigheten i den berörda medlemsstaten vara behörig. I sådana fall ska artikel 56 inte tillämpas.

3. Tillsynsmyndigheterna ska inte vara behöriga att utöva tillsyn över domstolar som behandlar personuppgifter i sin dömande verksamhet.

Artikel 56

Den ansvariga tillsynsmyndighetens behörighet

1. Utan att det påverkar tillämpningen av artikel 55 ska tillsynsmyndigheten för den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga verksamhetsställe eller enda verksamhetsställe vara behörig att agera som ansvarig tillsynsmyndighet för den personuppgiftsansvariges eller personuppgiftsbiträdets gränsöverskridande behandling i enlighet med det förfarande som föreskrivs i artikel 60.

2. Genom undantag från punkt 1 ska varje tillsynsmyndighet vara behörig att behandla ett klagomål som lämnats in till denna eller en eventuell överträdelse av denna förordning, om sakfrågan i ärendet endast rör ett verksamhetsställe i medlemsstaten eller i väsentlig grad påverkar registrerade endast i medlemsstaten.

3. I de fall som avses i punkt 2 i den här artikeln ska tillsynsmyndigheten utan dröjsmål informera den ansvariga tillsynsmyndigheten om detta ärende. Inom tre veckor från det att den underrättats ska den ansvariga tillsynsmyndigheten besluta huruvida den kommer att behandla ärendet i enlighet med det förfarande som föreskrivs i artikel 60, med hänsyn till huruvida den personuppgiftsansvarige eller personuppgiftsbiträdet har eller inte har ett verksamhetsställe som är beläget i den medlemsstat där den tillsynsmyndighet som lämnat informationen är belägen.

4. Om den ansvariga tillsynsmyndigheten beslutar att behandla ärendet ska det ske i enlighet med det förfarande som föreskrivs i artikel 60. Den tillsynsmyndighet som underrättade den ansvariga tillsynsmyndigheten får lämna in ett utkast till beslut till den ansvariga tillsynsmyndigheten. Den ansvariga tillsynsmyndigheten ska ta största möjliga hänsyn till detta utkast till beslut när det utarbetar det utkast till beslut som avses i artikel 60.3.

5. Om den ansvariga tillsynsmyndigheten beslutar att inte behandla ärendet ska den tillsynsmyndighet som underrättade den ansvariga tillsynsmyndigheten behandla ärendet i enlighet med artiklarna 61 och 62.

6. Den ansvariga tillsynsmyndigheten ska vara den personuppgiftsansvariges eller personuppgiftsbiträdets enda motpart när det gäller den registreringsansvariges eller den personuppgiftsbiträdets gränsöverskridande behandling.

Artikel 57

Uppgifter

1. Utan att det påverkar de andra uppgifter som föreskrivs i denna förordning ska varje tillsynsmyndighet på sitt territorium ansvara för följande:

a) Övervaka och verkställa tillämpningen av denna förordning.

b) Öka allmänhetens medvetenhet om och förståelse för risker, regler, skyddsåtgärder och rättigheter i fråga om behandling. Särskild uppmärksamhet ska ägnas åt insatser som riktar sig till barn.

c) I enlighet med medlemsstatens nationella rätt ge rådgivning åt det nationella parlamentet, regeringen och andra institutioner och organ om lagstiftningsåtgärder och administrativa åtgärder rörande skyddet av fysiska personers rättigheter och friheter när det gäller behandling.

d) Öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter enligt denna förordning.

e) På begäran tillhandahålla information till registrerade om hur de ska utöva sina rättigheter enligt denna förordning, och om så krävs samarbeta med tillsynsmyndigheter i andra medlemsstater för detta ändamål.

f) Behandla klagomål från en registrerad eller från ett organ, en organisation eller en sammanslutning enligt artikel 80, och där så är lämpligt undersöka den sakfråga som klagomålet gäller och inom rimlig tid underrätta den enskilde om hur undersökningen fortskrider och om resultatet, i synnerhet om det krävs ytterligare undersökningar eller samordning med en annan tillsynsmyndighet.

g) Samarbeta, inbegripet utbyta information, med och ge ömsesidigt bistånd till andra tillsynsmyndigheter för att se till att denna förordning tillämpas och verkställs på ett enhetligt sätt.

h) Utföra undersökningar om tillämpningen av denna förordning, inbegripet på grundval av information som erhålls från en annan tillsynsmyndighet eller annan myndighet.

i) Följa sådan utveckling som påverkar skyddet av personuppgifter, bland annat inom informations- och kommunikationsteknik och affärspraxis.

j) Anta sådana standardavtalsklausuler som avses i artiklarna 28.8 och 46.2 d.

k) Upprätta och föra en förteckning när det gäller kravet på en konsekvensbedömning avseende dataskydd enligt artikel 35.4.

l) Ge råd om behandling av personuppgifter enligt artikel 36.2.

m) Främja framtagande av uppförandekoder enligt artikel 40.1 samt yttra sig över och godkänna sådana uppförandekoder som tillhandahåller tillräckliga garantier, i enlighet med artikel 40.5.

n) Uppmuntra till inrättandet av certifieringsmekanismer för dataskydd och av sigill och märkningar för dataskydd i enlighet med artikel 42.1 samt godkänna certifieringskriterierna i enlighet med artikel 42.5.

o) I tillämpliga fall genomföra en periodisk översyn av certifieringar som utfärdats i enlighet med artikel 42.7.

p) Utarbeta och offentliggöra kriterier för ackreditering av ett organ för övervakning av uppförandekoder enligt artikel 41 och ett certifieringsorgan enligt artikel 43.

q) Ackreditera ett organ för övervakning av uppförandekoder enligt artikel 41 och ett certifieringsorgan enligt artikel 43.

r) Godkänna sådana avtalsklausuler och bestämmelser som avses i artikel 46.3.

s) Godkänna sådana bindande företagsbestämmelser som avses i artikel 47.

t) Bidra till styrelsens verksamhet.

u) Hålla arkiv över överträdelser av denna förordning och åtgärder som vidtagits i enlighet med artikel 58.2.

v) Utföra eventuella andra uppgifter som rör skyddet av personuppgifter.

2. Varje tillsynsmyndighet ska underlätta inlämningen av klagomål enligt punkt 1 f genom åtgärder såsom ett särskilt formulär för ändamålet, vilket också kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.

3. Utförandet av alla tillsynsmyndigheters uppgifter ska vara avgiftsfritt för den registrerade och, i tillämpliga fall, för dataskyddsombudet.

4. Om en begäran är uppenbart ogrundad eller orimlig, särskilt på grund av dess repetitiva karaktär, får tillsynsmyndigheten ta ut en rimlig avgift grundad på de administrativa kostnaderna eller vägra att tillmötesgå begäran. Det åligger tillsynsmyndigheten att visa att begäran är uppenbart ogrundad eller orimlig.

Artikel 58

Befogenheter

1. Varje tillsynsmyndighet ska ha samtliga följande utredningsbefogenheter

a) Beordra den personuppgiftsansvarige eller personuppgiftsbiträdet, och i tillämpliga fall den personuppgiftsansvariges eller personuppgiftsbiträdets företrädare, att lämna all information som myndigheten behöver för att kunna fullgöra sina uppgifter.

b) Genomföra undersökningar i form av dataskyddstillsyn.

c) Genomföra en översyn av certifieringar som utfärdats i enlighet med artikel 42.7.

d) Meddela den personuppgiftsansvarige eller personuppgiftsbiträdet om en påstådd överträdelse av denna förordning.

e) Från den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter och all information som tillsynsmyndigheten behöver för att kunna fullgöra sina uppgifter.

f) Få tillträde till alla lokaler som tillhör den personuppgiftsansvarige och personuppgiftsbiträdet, inbegripet tillgång till all utrustning och alla andra medel för behandling av personuppgifter i överensstämmelse med unionens processrätt eller medlemsstaternas nationella processrätt.

2. Varje tillsynsmyndighet ska ha samtliga följande korrigerande befogenheter

a) Utfärda varningar till en personuppgiftsansvarig eller personuppgiftsbiträdet om att planerade behandlingar sannolikt kommer att bryta mot bestämmelserna i denna förordning.

b) Utfärda reprimander till en personuppgiftsansvarig eller personuppgiftsbiträdet om behandling bryter mot bestämmelserna i denna förordning.

c) Förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att tillmötesgå den registrerades begäran att få utöva sina rättigheter enligt denna förordning.

d) Förelägga en personuppgiftsansvarig eller ett personuppgiftsbiträde att se till att behandlingen sker i enlighet med bestämmelserna i denna förordning och om så krävs på ett specifikt sätt och inom en specifik period,

e) Förelägga den personuppgiftsansvarige att meddela den registrerade att en personuppgiftsincident har inträffat.

f) Införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, behandling.

g) Förelägga om rättelse eller radering av personuppgifter samt begränsning av behandling enligt artiklarna 16, 17 och 18 och underrätta mottagare till vilka personuppgifterna har lämnats ut om dessa åtgärder enligt artiklarna 17.2 och 19.

h) Återkalla en certifiering eller beordra certifieringsorganet att återkalla en certifiering som utfärdats enligt artikel 42 eller 43, eller beordra certifieringsorganet att inte utfärda certifiering om kraven för certifiering inte eller inte längre uppfylls.

i) Påföra administrativa sanktionsavgifter i enlighet med artikel 83 utöver eller i stället för de åtgärder som avses i detta stycke, beroende på omständigheterna i varje enskilt fall.

j) Förelägga om att flödet av uppgifter till en mottagare i tredje land eller en internationell organisation ska avbrytas.

3. Varje tillsynsmyndighet ska ha samtliga följande befogenheter att utfärda tillstånd och att ge råd:

a) Ge råd till den personuppgiftsansvarige i enlighet med det förfarande för förhandssamråd som avses i artikel 36.

b) På eget initiativ eller på begäran avge yttranden till det nationella parlamentet, medlemsstatens regering eller, i enlighet med medlemsstatens nationella rätt, till andra institutioner och organ samt till allmänheten, i frågor som rör skydd av personuppgifter.

c) Ge tillstånd till behandling enligt artikel 36.5 om medlemsstatens rätt kräver ett sådant förhandstillstånd.

d) Avge ett yttrande om och godkänna utkast till uppförandekoder enligt artikel 40.5.

e) Ackreditera certifieringsorgan i enlighet med artikel 43.

f) Utfärda certifieringar och godkänna kriterier för certifiering i enlighet med artikel 42.5.

g) Anta standardiserade dataskyddsbestämmelser enligt artiklarna 28.8 och 46.2 d.

h) Godkänna avtalsklausuler enligt artikel 46.3 a.

i) Godkänna administrativa överenskommelser enligt artikel 46.3 b.

j) Godkänna bindande företagsbestämmelser enligt artikel 47.

4. Utövandet av de befogenheter som tillsynsmyndigheten tilldelas enligt denna artikel ska omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel och rättssäkerhet, som fastställs i unionsrätten och i medlemsstaternas nationella rätt i enlighet med stadgan.

5. Varje medlemsstat ska i lagstiftning fastställa att dess tillsynsmyndighet ska ha befogenhet att upplysa de rättsliga myndigheterna om överträdelser av denna förordning och vid behov att inleda eller på övrigt vis delta i rättsliga förfaranden, för att verkställa bestämmelserna i denna förordning.

6. Varje medlemsstat får i lagstiftning föreskriva att dess tillsynsmyndighet ska ha ytterligare befogenheter utöver dem som avses i punkterna 1, 2 och 3. Utövandet av dessa befogenheter ska inte påverka den effektiva tillämpningen av kapitel VII.

Artikel 59

Verksamhetsrapporter

Varje tillsynsmyndighet ska upprätta en årlig rapport om sin verksamhet, vilken kan omfatta en förteckning över typer av anmälda överträdelser och typer av åtgärder som vidtagits i enlighet med artikel 58.2. Rapporterna ska översändas till det nationella parlamentet, regeringen och andra myndigheter som utsetts genom medlemsstatens nationella rätt. De ska göras tillgängliga för allmänheten, kommissionen och styrelsen.

KAPITEL VII

Samarbete och enhetlighet

Avsnitt 1

Samarbete

Artikel 60

Samarbete mellan den ansvariga tillsynsmyndigheten och de andra berörda tillsynsmyndigheterna

1. Den ansvariga tillsynsmyndigheten ska samarbeta med de andra berörda tillsynsmyndigheterna i enlighet med denna artikel i en strävan att uppnå samförstånd. Den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna ska utbyta all relevant information med varandra.

2. Den ansvariga tillsynsmyndigheten får när som helst begära att andra berörda tillsynsmyndigheter ger ömsesidigt bistånd i enlighet med artikel 61 och får genomföra gemensamma insatser i enlighet med artikel 62, i synnerhet för att utföra utredningar eller övervaka genomförandet av en åtgärd som avser en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i en annan medlemsstat.

3. Den ansvariga tillsynsmyndigheten ska utan dröjsmål meddela de andra berörda tillsynsmyndigheterna den relevanta informationen i ärendet. Den ska utan dröjsmål lägga fram ett utkast till beslut för de andra berörda tillsynsmyndigheterna så att de kan avge ett yttrande och ta vederbörlig hänsyn till deras synpunkter.

4. Om någon av de andra berörda tillsynsmyndigheterna inom en period av fyra veckor efter att de har rådfrågats i enlighet med punkt 3 i den här artikeln uttrycker en relevant och motiverad invändning mot utkastet till beslut ska den ansvariga tillsynsmyndigheten, om den inte instämmer i den relevanta och motiverade invändningen eller anser att invändningen inte är relevant eller motiverad, överlämna ärendet till den mekanism för enhetlighet som avses i artikel 63.

5. Om den ansvariga tillsynsmyndigheten avser att följa den relevanta och motiverade invändningen ska den till de andra berörda tillsynsmyndigheterna överlämna ett reviderat utkast till beslut så att de kan avge ett yttrande. Detta reviderade utkast till beslut ska omfattas av det förfarande som avses i punkt 4 inom en period av två veckor.

6. Om ingen av de andra berörda tillsynsmyndigheterna har gjort invändningar mot det utkast till beslut som den ansvariga tillsynsmyndigheten har lagt fram inom den period som avses i punkterna 4 och 5 ska den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna anses samtycka till detta utkast till beslut och ska vara bundna av det.

7. Den ansvariga tillsynsmyndigheten ska anta och meddela beslutet till den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga eller enda verksamhetsställe, allt efter omständigheterna, och underrätta de andra berörda tillsynsmyndigheterna och styrelsen om beslutet i fråga, inbegripet en sammanfattning av relevanta fakta och en relevant motivering. Den tillsynsmyndighet till vilken ett klagomål har lämnats in ska underrätta den enskilde om beslutet.

8. Om ett klagomål avvisas eller avslås ska den tillsynsmyndighet till vilken klagomålet lämnades in, genom undantag från punkt 7, anta beslutet och meddela den enskilde samt informera den personuppgiftsansvarige.

9. Om den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna är överens om att avvisa eller avslå delar av ett klagomål och att vidta åtgärder beträffande andra delar av klagomålet ska ett separat beslut antas för var och en av dessa delar av frågan. Den ansvariga tillsynsmyndigheten ska anta beslutet om den del som gäller åtgärder som avser den personuppgiftsansvarige och meddela det till den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga eller enda verksamhetsställe på medlemsstatens territorium och underrätta den enskilde om detta, medan den enskildes tillsynsmyndighet ska anta beslutet för den del som gäller avvisande av eller avslag på klagomålet och meddela det till den enskilde och underrätta den personuppgiftsansvarige eller personuppgiftsbiträdet om detta.

10. Efter att den personuppgiftsansvarige eller personuppgiftsbiträdet har meddelats om den ansvariga myndighetens beslut i enlighet med punkterna 7 och 9 ska den personuppgiftsansvarige eller personuppgiftsbiträdet vidta nödvändiga åtgärder för att se till att beslutet efterlevs vad gäller behandling med koppling till alla deras verksamhetsställen i unionen. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska meddela den ansvariga tillsynsmyndigheten vilka åtgärder som har vidtagits för att efterleva beslutet, och den ansvariga tillsynsmyndigheten ska informera de andra berörda tillsynsmyndigheterna.

11. Om en berörd tillsynsmyndighet under exceptionella omständigheter har skäl att anse att det finns ett brådskande behov av att agera för att skydda registrerades intressen ska det skyndsamma förfarande som avses i artikel 66 tillämpas.

12. Den ansvariga tillsynsmyndigheten och de andra berörda tillsynsmyndigheterna ska förse varandra med den information som krävs enligt denna artikel på elektronisk väg med användning av ett standardiserat format.

Artikel 61

Ömsesidigt bistånd

1. Tillsynsmyndigheterna ska utbyta relevant information och ge ömsesidigt bistånd i arbetet för att genomföra och tillämpa denna förordning på ett enhetligt sätt, och ska införa åtgärder som bidrar till ett verkningsfullt samarbete. Det ömsesidiga biståndet ska i synnerhet omfatta begäranden om information och tillsynsåtgärder, till exempel begäranden om utförande av förhandstillstånd och förhandssamråd, inspektioner och utredningar.

2. Varje tillsynsmyndighet ska vidta lämpliga åtgärder som krävs för att besvara en begäran från en annan tillsynsmyndighet utan onödigt dröjsmål och inte senare än en månad efter det att den tagit emot begäran. Till sådana åtgärder hör bland annat att översända relevant information om genomförandet av en pågående utredning.

3. En begäran om bistånd ska innehålla all nödvändig information, inklusive syftet med begäran och skälen till denna. Information som utbytts får endast användas för det syfte för vilket den har begärts.

4. Den tillsynsmyndighet som tar emot en begäran får endast vägra att tillmötesgå begäran om

a) den inte är behörig att behandla den sakfråga som begäran avser eller de åtgärder som det begärs att den ska utföra, eller

b) det skulle stå i strid med denna förordning eller unionsrätten eller den nationella rätt i en medlemsstat som tillsynsmyndigheten omfattas av att tillmötesgå begäran.

5. Den tillsynsmyndighet som tagit emot begäran ska meddela den myndighet som begäran kommer ifrån om resultatet eller, allt efter omständigheterna, om hur de åtgärder som vidtagits för att tillmötesgå begäran fortskrider. Den tillsynsmyndighet som tagit emot begäran ska redogöra för sina skäl för att vägra tillmötesgå begäran i enlighet med punkt 4.

6. Den tillsynsmyndighet som tar emot en begäran ska som regel tillhandahålla den information som begärts av andra tillsynsmyndigheter på elektronisk väg med användning av ett standardiserat format.

7. Tillsynsmyndigheter som tar emot en begäran får inte ta ut någon avgift för åtgärder som vidtagits av dem till följd av en begäran om ömsesidigt bistånd. Tillsynsmyndigheter får i undantagsfall komma överens med andra tillsynsmyndigheter om regler för ersättning från varandra för vissa utgifter i samband med tillhandahållande av ömsesidigt bistånd.

8. Om en tillsynsmyndighet inte tillhandahåller den information som avses i punkt 5 i denna artikel inom en månad efter det att den erhållit begäran från en annan tillsynsmyndighet får den begärande myndigheten anta en provisorisk åtgärd på sin medlemsstats territorium i enlighet med artikel 55.1. I detta fall ska det brådskande behov av att agera enligt artikel 66.1 anses vara uppfyllt och kräva ett brådskande bindande beslut från styrelsen i enlighet med artikel 66.2.

9. Kommissionen får genom genomförandeakter närmare ange format och förfaranden för sådant ömsesidigt bistånd som avses i denna artikel samt formerna för elektronisk överföring av information tillsynsmyndigheter emellan, samt mellan tillsynsmyndigheter och styrelsen, i synnerhet det standardiserade format som avses i punkt 6 i den här artikeln. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

Artikel 62

Tillsynsmyndigheters gemensamma insatser

1. Tillsynsmyndigheter ska vid behov genomföra gemensamma insatser, inbegripet gemensamma utredningar och gemensamma verkställighetsåtgärder i vilka ledamöter eller personal från andra medlemsstaters tillsynsmyndigheter deltar.

2. Om den personuppgiftsansvarige eller personuppgiftsbiträdet har verksamhetsställen i flera medlemsstater eller om ett betydande antal registrerade personer i mer än en medlemsstat sannolikt kommer att påverkas i väsentlig grad av att uppgifter behandlas, ska tillsynsmyndigheterna i var och en av dessa medlemsstater ha rätt att delta i de gemensamma insatserna. Den tillsynsmyndighet som är behörig enligt artikel 56.1 eller 56.4 ska bjuda in tillsynsmyndigheterna i var och en av de berörda medlemsstaterna att delta i de gemensamma insatserna och ska utan dröjsmål svara på en annan tillsynsmyndighets begäran att få delta.

3. En tillsynsmyndighet får, i enlighet med medlemsstatens nationella rätt och efter godkännande från ursprungslandets tillsynsmyndighet, tilldela befogenheter, inklusive utredningsbefogenheter, till ledamöter eller personal från ursprungslandets tillsynsmyndighet som deltar i gemensamma insatser eller, i den mån lagstiftningen i den medlemsstat som är värdland för tillsynsmyndigheten tillåter detta, medge att ursprungslandets tillsynsmyndighets ledamöter eller personal utövar utredningsbefogenheter enligt lagstiftningen i ursprungslandets tillsynsmyndighets medlemsstat. Sådana utredningsbefogenheter får endast utövas under vägledning och i närvaro av ledamöter eller personal från värdlandets tillsynsmyndighet. Ledamöter och personal från ursprungslandets tillsynsmyndighet ska omfattas av den medlemsstats nationella rätt som gäller för värdlandets tillsynsmyndighet.

4. Om personal från ursprungslandets tillsynsmyndighet verkar i en annan medlemsstat i enlighet med punkt 1 ska värdtillsynsmyndighetens medlemsstat ansvara för deras handlingar, vilket inbegriper ansvar för skador som personalen vållar i samband med insatserna, i enlighet med rätten i den medlemsstat på vars territorium personalen verkar.

5. Den medlemsstat på vars territorium skadorna förorsakades ska ersätta sådana skador enligt de villkor som gäller för skador som förorsakas av dess egen personal. Den medlemsstat vars tillsynsmyndighets tjänstemän har orsakat en person skada på någon annan medlemsstats territorium ska fullt ut ersätta den andra medlemsstaten för det belopp som denna har betalat ut till den personens rättsinnehavare.

6. Utan att det påverkar rättigheterna gentemot tredje man och tillämpningen av punkt 5, ska varje medlemsstat i de fall som nämns i punkt 1 avstå från att kräva ersättning från en annan medlemsstat för skador som avses i punkt 4.

7. Om en gemensam insats planeras och en tillsynsmyndighet inte inom en månad har uppfyllt sin skyldighet enligt punkt 2 i den här artikeln, andra meningen får övriga tillsynsmyndigheter anta provisoriska åtgärder på sina respektive medlemsstaters territorium i enlighet med artikel 55. I detta fall ska det brådskande behov av att agera enligt artikel 66.1 anses vara uppfyllt och kräva ett yttrande eller ett brådskande bindande beslut från styrelsen i enlighet med artikel 66.2.

Avsnitt 2

Enhetlighet

Artikel 63

Mekanism för enhetlighet

För att bidra till en enhetlig tillämpning av denna förordning i hela unionen ska tillsynsmyndigheterna samarbeta med varandra och, i förekommande fall, med kommissionen, genom den mekanism för enhetlighet som föreskrivs i detta avsnitt.

Artikel 64

Yttrande från Styrelsen

1. Styrelsen ska avge ett yttrande när en behörig tillsynsmyndighet avser att anta någon av åtgärderna nedan. I detta syfte ska den behöriga tillsynsmyndigheten skicka utkastet till beslut till styrelsen när det

a) syftar till att anta en förteckning över behandling som omfattas av kravet på en konsekvensbedömning avseende dataskydd enligt artikel 35.4,

b) rör ett ärende i enlighet med artikel 40.7 om huruvida ett utkast till uppförandekoder eller en ändring eller förlängning av en uppförandekod är förenlig med denna förordning,

c) syftar till att godkänna kriterierna för ackreditering av ett organ enligt artikel 41.3 eller ett certifieringsorgan enligt artikel 43.3,

d) syftar till att fastställa standardiserade dataskyddsbestämmelser enligt artiklarna 46.2 d och 28.8,

e) syftar till att godkänna sådana avtalsklausuler som avses i artikel 46.3 a, eller

f) syftar till att godkänna bindande företagsbestämmelser enligt artikel 47.

2. Varje tillsynsmyndighet, styrelsens ordförande eller kommissionen får i syfte att erhålla ett yttrande begära att styrelsen granskar en fråga med allmän räckvidd eller som har följder i mer än en medlemsstat, i synnerhet om en behörig myndighet inte uppfyller sina skyldigheter i fråga om ömsesidigt bistånd i enlighet med artikel 61 eller i fråga om gemensamma insatser i enlighet med artikel 62.

3. I de fall som avses i punkterna 1 och 2 ska styrelsen avge ett yttrande i den fråga som ingivits till den, förutsatt att den inte redan har avgett ett yttrande i samma fråga. Detta yttrande ska antas med enkel majoritet av styrelsens ledamöter inom åtta veckor. Denna period får förlängas med ytterligare sex veckor med hänsyn till sakfrågans komplexitet. Vad gäller det utkast till beslut som avses i punkt 1 som spridits till styrelsens ledamöter i enlighet med punkt 5, ska en ledamot som inte har gjort invändningar inom en rimlig period som ordföranden angett anses samtycka till utkastet till beslut.

4. Tillsynsmyndigheterna och kommissionen ska utan onödigt dröjsmål i ett standardiserat elektroniskt format till styrelsen översända all relevant information, som allt efter omständigheterna får utgöras av en sammanfattning av sakförhållanden, utkastet till beslut, grunden till att en sådan åtgärd är nödvändig och synpunkter från övriga berörda tillsynsmyndigheter.

5. Styrelsens ordförande ska utan onödigt dröjsmål och på elektronisk väg upplysa

a) styrelsens ledamöter samt kommissionen om all relevant information som meddelats styrelsen i ett standardiserat format; styrelsens sekretariat ska vid behov tillhandahålla översättningar av relevant information; och

b) den tillsynsmyndighet som, allt efter omständigheterna, avses i punkterna 1 och 2 samt kommissionen om yttrandet, och ska också offentliggöra det.

6. Den behöriga tillsynsmyndigheten får inte anta sitt utkast till beslut enligt punkt 1 inom den period som avses i punkt 3.

7. Den tillsynsmyndighet som avses i punkt 1 ska ta största möjliga hänsyn till styrelsens yttrande och ska, inom två veckor efter att yttrandet inkommit, i ett standardiserat elektroniskt format meddela styrelsens ordförande om huruvida den kommer att hålla fast vid eller ändra sitt utkast till beslut, och i förekommande fall översända det ändrade utkastet till beslut.

8. Om den berörda tillsynsmyndigheten underrättar styrelsens ordförande inom den period som avses i punkt 7 i den här artikeln om att den inte avser att följa styrelsens yttrande, helt eller delvis, och tillhandahåller en relevant motivering, ska artikel 65.1 tillämpas.

Artikel 65

Tvistlösning genom styrelsen

1. För att säkerställa en korrekt och enhetlig tillämpning av denna förordning i enskilda fall ska styrelsen anta ett bindande beslut i följande fall:

a) Om en berörd tillsynsmyndighet i ett fall som avses i artikel 60.4 har gjort en relevant och motiverad invändning mot ett utkast till beslut av den ansvariga myndigheten, eller om den ansvariga myndigheten har avslagit denna invändning med motiveringen att den inte var relevant eller motiverad. Det bindande beslutet ska avse alla ärenden som är föremål för den relevanta och motiverade invändningen, särskilt frågan om huruvida det föreligger en överträdelse av denna förordning.

b) Om det finns motstridiga åsikter om vilken av de berörda tillsynsmyndigheterna som är behörig för det huvudsakliga verksamhetsstället.

c) Om en behörig tillsynsmyndighet inte begär ett yttrande från styrelsen i de fall som avses i artikel 64.1, eller inte följer ett yttrande som styrelsen avger enligt artikel 64. I detta fall får varje berörd tillsynsmyndighet eller kommissionen översända ärendet till styrelsen.

2. Det beslut som avses i punkt 1 ska antas inom en månad efter det att sakfrågan hänskjutits med två tredjedels majoritet av styrelsens ledamöter. Denna period får förlängas med ytterligare en månad med hänsyn till sakfrågans komplexitet. Det beslut som avses i punkt 1 ska vara motiverat och riktat till den ansvariga tillsynsmyndigheten och alla berörda tillsynsmyndigheter och ska vara bindande för dem.

3. Om styrelsen inte har kunnat anta något beslut inom de perioder som avses i punkt 2 ska den anta sitt beslut inom två veckor efter utgången av den andra månad som avses i punkt 2 med enkel majoritet av styrelsens ledamöter. Om styrelsens ledamöter är delade i frågan ska beslutet antas i enlighet med ordförandens röst.

4. De berörda tillsynsmyndigheterna ska inte anta något beslut om den sakfråga som ingivits till styrelsen i enlighet med punkt 1 under de perioder som avses i punkterna 2 och 3.

5. Styrelsens ordförande ska utan onödigt dröjsmål meddela de berörda tillsynsmyndigheterna det beslut som avses i punkt 1. Kommissionen ska informeras om detta. Beslutet ska utan dröjsmål offentliggöras på styrelsens webbplats efter att tillsynsmyndigheten har meddelat det slutliga beslut som avses i punkt 6.

6. Den ansvariga tillsynsmyndigheten eller, allt efter omständigheterna, den tillsynsmyndighet till vilken klagomålet har ingetts ska anta sitt slutliga beslut på grundval av det beslut som avses i punkt 1 i den här artikeln, utan onödigt dröjsmål och senast en månad efter det att styrelsen har meddelat sitt beslut. Den ansvariga tillsynsmyndigheten eller, allt efter omständigheterna, den tillsynsmyndighet till vilken klagomålet har ingetts ska underrätta styrelsen om vilken dag dess slutliga beslut meddelas till den personuppgiftsansvarige respektive personuppgiftsbiträdet och den registrerade. De berörda tillsynsmyndigheternas slutliga beslut ska antas i enlighet med bestämmelserna i artikel 60.7, 60.8 och 60.9. Det slutliga beslutet ska hänvisa till det beslut som avses i punkt 1 i den här artikeln och ska precisera att det beslut som avses i punkt 1 kommer att offentliggöras på styrelsens webbplats i enlighet med punkt 5 i den här artikeln. Det beslut som avses i punkt 1 i den här artikeln ska fogas till det slutliga beslutet.

Artikel 66

Skyndsamt förfarande

1. Under exceptionella omständigheter får en berörd tillsynsmyndighet med avvikelse från den mekanism för enhetlighet som avses i artiklarna 63, 64 och 65 eller det förfarande som avses i artikel 60 omedelbart vidta provisoriska åtgärder avsedda att ha rättsverkan på det egna territoriet och med förutbestämd varaktighet som inte överskrider tre månader, om den anser att det finns ett brådskande behov av att agera för att skydda registrerades rättigheter och friheter. Tillsynsmyndigheten ska utan dröjsmål underrätta de andra berörda tillsynsmyndigheterna, styrelsen och kommissionen om dessa åtgärder och om skälen till att de vidtas.

2. Om en tillsynsmyndighet har vidtagit en åtgärd enligt punkt 1 och anser att definitiva åtgärder skyndsamt måste antas, får den begära ett brådskande yttrande eller ett brådskande bindande beslut från styrelsen; den ska då motivera varför den begär ett sådant yttrande eller beslut.

3. Om en behörig tillsynsmyndighet inte har vidtagit någon lämplig åtgärd i en situation som kräver skyndsam handling för att skydda registrerades rättigheter och friheter, får vilken tillsynsmyndighet som helst begära ett brådskande yttrande eller, i tillämpliga fall, ett brådskande bindande beslut från styrelsen, varvid den ska motivera varför den begär ett sådant yttrande eller beslut och varför åtgärden måste vidtas skyndsamt.

4. Genom undantag från artiklarna 64.3 och 65.2 ska ett brådskande yttrande eller ett brådskande beslut enligt punkterna 2 och 3 i den här artikeln antas inom två veckor med enkel majoritet av styrelsens ledamöter.

Artikel 67

Utbyte av information

Kommissionen får anta genomförandeakter med allmän räckvidd i syfte att närmare ange tillvägagångssätten för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen, särskilt det standardiserade format som avses i artikel 64.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

Avsnitt 3

Europeiska dataskyddsstyrelsen

Artikel 68

Europeiska dataskyddsstyrelsen

1. Europeiska dataskyddsstyrelsen (nedan kallad *styrelsen*) inrättas härmed som ett unionsorgan och ska ha ställning som juridisk person.

2. Styrelsen ska företrädas av sin ordförande.

3. Styrelsen ska bestå av chefen för en tillsynsmyndighet per medlemsstat och av Europeiska datatillsynsmannen eller deras respektive företrädare.

4. Om en medlemsstat har mer än en tillsynsmyndighet som ansvarar för att övervaka tillämpningen av bestämmelserna i denna förordning ska en gemensam företrädare utses i enlighet med den medlemsstatens nationella rätt.

5. Kommissionen ska ha rätt att delta i styrelsens verksamhet och möten utan rösträtt. Kommissionen ska utse en egen företrädare. Styrelsens ordförande ska underrätta kommissionen om styrelsens verksamhet.

6. I de fall som avses i artikel 65 ska Europeiska datatillsynsmannen endast ha rösträtt i fråga om beslut som rör principer och regler som är tillämpliga på unionens institutioner, organ och byråer, och som i allt väsentligt motsvarar dem i denna förordning.

Artikel 69

Oberoende

1. Styrelsen ska vara oberoende när den fullgör sina uppgifter eller utövar sina befogenheter i enlighet med artiklarna 70 och 71.

2. Utan att detta påverkar kommissionens rätt att lämna en begäran enligt artikel 70.1 b och 70.2 ska styrelsen när den fullgör sina uppgifter eller utövar sina befogenheter varken begära eller ta emot instruktioner av någon.

Artikel 70

Styrelsens uppgifter

1. Styrelsen ska se till att denna förordning tillämpas enhetligt. För detta ändamål ska styrelsen, på eget initiativ eller i förekommande fall på begäran av kommissionen, i synnerhet

a) övervaka och säkerställa korrekt tillämpning av denna förordning i de fall som avses i artiklarna 64 och 65 utan att det påverkar de nationella tillsynsmyndigheternas uppgifter,

b) ge kommissionen råd i alla frågor som gäller skydd av personuppgifter inom unionen, inklusive om eventuella förslag till ändring av denna förordning,

c) ge kommissionen råd om format och förfaranden för informationsutbyte mellan personuppgiftsansvariga, personuppgiftsbiträden och tillsynsmyndigheter för bindande företagsbestämmelser,

d) utfärda riktlinjer, rekommendationer och bästa praxis beträffande förfaranden för att radera länkar, kopior eller reproduktioner av personuppgifter från allmänt tillgängliga kommunikationstjänster enligt artikel 17.2,

e) på eget initiativ eller på begäran av en av sina ledamöter eller av kommissionen behandla frågor om tillämpningen av denna förordning och utfärda riktlinjer, rekommendationer och bästa praxis i syfte att främja en enhetlig tillämpning av denna förordning,

f) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och villkoren för profileringsbaserade beslut enligt artikel 22.2,

g) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att konstatera sådana personuppgiftsincidenter och fastställa sådant onödigt dröjsmål som avses i artikel 33.1 och 33.2 och för de särskilda omständigheter under vilka en personuppgiftsansvarig eller ett personuppgiftsbiträde är skyldig att anmäla personuppgiftsincidenten,

h) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt angående de omständigheter under vilka en personuppgiftsincident sannolikt kommer att leda till hög risk för rättigheterna och friheterna för de fysiska personer som avses i artikel 34.1,

i) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och kraven för överföringar av personuppgifter på grundval av bindande företagsbestämmelser som personuppgiftsansvariga eller personuppgiftsbiträden följer samt ytterligare nödvändiga krav för att säkerställa skyddet för personuppgifter för berörda registrerade enligt artikel 47,

j) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och villkoren för överföring av personuppgifter på grundval av artikel 49.1,

k) utforma riktlinjer för tillsynsmyndigheterna i fråga om tillämpningen av de åtgärder som avses i artikel 58.1, 58.2 och 58.3 och fastställandet av administrativa sanktionsavgifter i enlighet med artikel 83,

l) se över den praktiska tillämpningen av de riktlinjer och rekommendationer samt den bästa praxis som avses i leden e och f,

m) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att fastställa gemensamma förfaranden för fysiska personers rapportering av överträdelser av denna förordning enligt artikel 54.2,

n) främja utarbetandet av uppförandekoder och införandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd i enlighet med artiklarna 40 och 42,

o) ackreditera certifieringsorgan och utföra sin periodiska översyn i enlighet med artikel 43 och föra ett offentligt register över ackrediterade organ i enlighet med artikel 43.6 och över de ackrediterade personuppgiftsansvariga eller personuppgiftsbiträdena som är etablerade i tredjeländer i enlighet med artikel 42.7,

p) närmare ange de krav som avses i artikel 43.3 i syfte att ackreditera certifieringsorgan enligt artikel 42,

q) avge ett yttrande till kommissionen om de certifieringskrav som avses i artikel 43.8,

r) avge ett yttrande till kommissionen om de symboler som avses i artikel 12.7,

s) avge ett yttrande till kommissionen för bedömningen av adekvat skyddsnivå i ett tredjeland eller en internationell organisation, inklusive för bedömningen av huruvida ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom det tredjelandet, eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå; i detta syfte ska kommissionen lämna all nödvändig dokumentation till styrelsen, inklusive korrespondens med regeringen i tredjelandet, med avseende på tredjelandet, territoriet eller den specificerade sektorn, eller till databehandlingssektorn i tredjelandet eller den internationella organisationen,

t) avge yttranden om utkast till beslut som läggs fram av tillsynsmyndigheter inom den mekanism för enhetlighet som avses i artikel 64.1, i ärenden som ingivits i enlighet med artikel 64.2 och anta bindande beslut i enlighet med artikel 65, inbegripet de fall som avses i artikel 66,

u) främja samarbete och effektivt bilateralt och multilateralt utbyte av bästa praxis och information mellan tillsynsmyndigheterna,

v) främja gemensamma utbildningsprogram och underlätta personalutbyte mellan tillsynsmyndigheterna och där så är lämpligt även med tillsynsmyndigheter i tredjeländer eller internationella organisationer,

w) främja utbyte av kunskap och dokumentation om lagstiftning om och praxis för dataskydd med tillsynsmyndigheter för dataskydd i hela världen.

x) avge yttranden över de uppförandekoder som utarbetas på unionsnivå i enlighet med artikel 40.9, och

y) föra ett offentligt elektroniskt register över tillsynsmyndigheters beslut och domstolars avgöranden i frågor som hanteras inom mekanismen för enhetlighet.

2. När kommissionen begär rådgivning från styrelsen får den ange en tidsfrist med hänsyn till hur brådskande ärendet är.

3. Styrelsen ska vidarebefordra sina yttranden, riktlinjer, rekommendationer och bästa praxis till kommissionen och till den kommitté som avses i artikel 93, samt offentliggöra dem.

4. När så är lämpligt ska styrelsen samråda med berörda parter och ge dem möjlighet att yttra sig inom rimlig tid. styrelsen ska, utan att det påverkar tillämpningen av artikel 76, offentliggöra resultatet av samrådsförfarandet.

Artikel 71

Rapporter

1. Styrelsen ska sammanställa en årsrapport om skydd av fysiska personer vid behandling inom unionen och, i förekommande fall, i tredjeländer och internationella organisationer. Rapporten ska offentliggöras och översändas till Europaparlamentet, rådet och kommissionen.

2. Årsrapporten ska också innehålla en översikt över den praktiska tillämpningen av de riktlinjer och rekommendationer och den bästa praxis som avses i artikel 70.1 l liksom de bindande beslut som avses i artikel 65.

Artikel 72

Förfarande

1. Styrelsen ska fatta beslut med enkel majoritet av dess ledamöter, om inte annat anges i denna förordning.

2. Styrelsen ska själv anta sin arbetsordning med två tredjedels majoritet av sina ledamöter och fastställa sina arbetsformer.

Artikel 73

Ordförande

1. Styrelsen ska med enkel majoritet välja en ordförande och två vice ordförande bland sina ledamöter.

2. Ordförandens och de vice ordförandenas mandattid ska vara fem år och kunna förnyas en gång.

Artikel 74

Ordförandens uppgifter

1. Ordföranden ska ha i uppgift att

a) sammankalla till styrelsens möten och planera dagordningen,

b) meddela beslut som antas av styrelsen i enlighet med artikel 65 till den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna,

c) se till att styrelsens uppgifter fullgörs i tid, särskilt i fråga om den mekanism för enhetlighet som avses i artikel 63.

2. Fördelningen av uppgifter mellan ordföranden och de vice ordförandena ska fastställas i styrelsens arbetsordning.

Artikel 75

Sekretariatet

1. Styrelsen ska förfoga över ett sekretariat som ska tillhandahållas av Europeiska datatillsynsmannen.

2. Sekretariatet ska utföra sina uppgifter enbart under ledning av ordföranden för styrelsen.

3. Den personal vid Europeiska datatillsynsmannen som utför de uppgifter som styrelsen tilldelas genom denna förordning ska följa separata rapporteringsvägar från den personal som utför de uppgifter som Europeiska datatillsynsmannen tilldelas.

4. När så är lämpligt ska styrelsen och Europeiska datatillsynsmannen fastställa och offentliggöra ett samförståndsavtal för genomförande av denna artikel, som fastställer villkoren för deras samarbete, och som ska tillämpas på den personal vid Europeiska datatillsynsmannen som utför de uppgifter som styrelsen tilldelas genom denna förordning.

5. Sekretariatet ska förse styrelsen med analysstöd samt administrativt och logistiskt stöd.

6. Sekretariatet ska särskilt ansvara för

a) styrelsens löpande arbete,

b) kommunikationen mellan styrelsens ledamöter, dess ordförande och kommissionen,

c) kommunikationen med andra institutioner och med allmänheten,

d) användningen av elektroniska medel för intern och extern kommunikation,

e) översättning av relevant information,

f) förberedelser och uppföljning av styrelsens möten,

g) förberedelse, sammanställning och offentliggörande av yttranden, beslut om lösning av tvister mellan tillsynsmyndigheter och andra texter som antas av styrelsen.

Artikel 76

Konfidentialitet

1. Styrelsens överläggningar ska vara konfidentiella i de fall som styrelsen bedömer detta vara nödvändigt, i enlighet med vad som anges i dess arbetsordning.

2. Tillgången till handlingar som skickas till styrelsens ledamöter, till experter eller till företrädare för tredje part ska regleras av Europaparlamentets och rådets förordning (EG) nr 1049/2001 ( ).

KAPITEL VIII

Rättsmedel, ansvar och sanktioner

Artikel 77

Rätt att lämna in klagomål till en tillsynsmyndighet

1. Utan att det påverkar något annat administrativt prövningsförfarande eller rättsmedel, ska varje registrerad som anser att behandlingen av personuppgifter som avser henne eller honom strider mot denna förordning ha rätt att lämna in ett klagomål till en tillsynsmyndighet, särskilt i den medlemsstat där han eller hon har sin hemvist eller sin arbetsplats eller där det påstådda intrånget begicks.

2. Den tillsynsmyndighet till vilken klagomålet har ingetts ska underrätta den enskilde om hur arbetet med klagomålet fortskrider och vad resultatet blir, inbegripet möjligheten till rättslig prövning enligt artikel 78.

Artikel 78

Rätt till ett effektivt rättsmedel mot tillsynsmyndighetens beslut

1. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol ska varje fysisk eller juridisk person ha rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut rörande dem som meddelats av en tillsynsmyndighet.

2. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol, ska varje registrerad person ha rätt till ett effektivt rättsmedel om den tillsynsmyndighet som är behörig i enlighet med artiklarna 55 och 56 underlåter att behandla ett klagomål eller att informera den registrerade inom tre månader om hur det fortskrider med det klagomål som ingetts med stöd av artikel 77 eller vilket beslut som har fattats med anledning av det.

3. Talan mot en tillsynsmyndighet ska väckas vid domstolarna i den medlemsstat där tillsynsmyndigheten har sitt säte.

4. Om talan väcks mot ett beslut som fattats av en tillsynsmyndighet och som föregicks av ett yttrande från eller beslut av styrelsen inom ramen för mekanismen för enhetlighet ska tillsynsmyndigheten vidarebefordra detta yttrande eller beslut till domstolen.

Artikel 79

Rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde

1. Utan att det påverkar tillgängliga administrativa prövningsförfaranden eller prövningsförfaranden utanför domstol, inbegripet rätten att lämna in ett klagomål till en tillsynsmyndighet i enlighet med artikel 77, ska varje registrerad som anser att hans eller hennes rättigheter enligt denna förordning har åsidosatts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med denna förordning ha rätt till ett effektivt rättsmedel.

2. Talan mot en personuppgiftsansvarig eller ett personuppgiftsbiträde ska väckas vid domstolarna i den medlemsstat där den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad. Alternativt får sådan talan väckas vid domstolarna i den medlemsstat där den registrerade har sin hemvist, såvida inte den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet i en medlemsstat som agerar inom ramen för sin myndighetsutövning.

( ) Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43).

Artikel 80

Företrädande av registrerade

1. Den registrerade ska ha rätt att ge ett organ, en organisation eller sammanslutning utan vinstsyfte, som har inrättats på lämpligt sätt i enlighet med lagen i en medlemsstat, vars stadgeenliga mål är av allmänt intresse och som är verksam inom området skydd av registrerades rättigheter och friheter när det gäller skyddet av deras personuppgifter, i uppdrag att lämna in ett klagomål för hans eller hennes räkning, att utöva de rättigheter som avses i artiklarna 77, 78 och 79 för hans eller hennes räkning samt att för hans eller hennes räkning utöva den rätt till ersättning som avses i artikel 82 om så föreskrivs i medlemsstatens nationella rätt.

2. Medlemsstaterna får föreskriva att ett organ, en organisation eller en sammanslutning enligt punkt 1 i den här artikeln, oberoende av en registrerads mandat, har rätt att i den medlemsstaten inge klagomål till den tillsynsmyndighet som är behörig enligt artikel 77 och utöva de rättigheter som avses i artiklarna 78 och 79 om organet, organisationen eller sammanslutningen anser att den registrerades rättigheter enligt den här förordningen har kränkts som en följd av behandlingen.

Artikel 81

Vilandeförklaring av förfaranden

1. Om en behörig domstol i en medlemsstat har information om att förfaranden som rör samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller personuppgiftsbiträde pågår i en domstol i en annan medlemsstat ska den kontakta denna domstol i den andra medlemsstaten för att bekräfta förekomsten av sådana förfaranden.

2. Om förfaranden som rör samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller personuppgiftsbiträde pågår i en domstol i en annan medlemstat får alla andra behöriga domstolar än den där förfarandena först inleddes vilandeförklara förfarandena.

3. Om dessa förfaranden prövas i första instans får varje domstol, utom den vid vilken förfarandena först inleddes, också förklara sig obehörig på begäran av en av parterna, om den domstol vid vilken förfarandena först inleddes är behörig att pröva de berörda förfarandena och dess lagstiftning tillåter förening av dessa.

Artikel 82

Ansvar och rätt till ersättning

1. Varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av denna förordning ska ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan.

2. Varje personuppgiftsansvarig som medverkat vid behandlingen ska ansvara för skada som orsakats av behandling som strider mot denna förordning. Ett personuppgiftsbiträde ska ansvara för skada uppkommen till följd av behandlingen endast om denne inte har fullgjort de skyldigheter i denna förordning som specifikt riktar sig till personuppgiftsbiträden eller agerat utanför eller i strid med den personuppgiftsansvariges lagenliga anvisningar.

3. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska undgå ansvar enligt punkt 2 om den visar att den inte på något sätt är ansvarig för den händelse som orsakade skadan.

4. Om mer än en personuppgiftsansvarig eller ett personuppgiftsbiträde, eller både en personuppgiftsansvarig och ett personuppgiftsbiträde, har medverkat vid samma behandling, och om de enligt punkterna 2 och 3 är ansvariga för eventuell skada som behandlingen orsakat ska varje personuppgiftsansvarig eller personuppgiftsbiträde hållas ansvarig för hela skadan för att säkerställa att den registrerade får effektiv ersättning.

5. Om en personuppgiftsansvarig eller ett personuppgiftsbiträde, i enlighet med punkt 4, har betalat full ersättning för den skada som orsakats ska den personuppgiftsansvarige eller personuppgiftsbiträdet ha rätt att från de andra personuppgiftsansvariga eller personuppgiftsbiträdena som medverkat vid samma behandling återkräva den del av ersättningen som motsvarar deras del av ansvaret för skadan i enlighet med de villkor som fastställs i punkt 2.

6. Domstolsförfaranden för utövande av rätten till ersättning ska tas upp vid de domstolar som är behöriga enligt den nationella rätten i den medlemsstat som avses i artikel 79.2.

Artikel 83

Allmänna villkor för påförande av administrativa sanktionsavgifter

1. Varje tillsynsmyndighet ska säkerställa att påförande av administrativa sanktionsavgifter i enlighet med denna artikel för sådana överträdelser av denna förordning som avses i punkterna 4, 5 och 6 i varje enskilt fall är effektivt, proportionellt och avskräckande.

2. Administrativa sanktionsavgifter ska, beroende på omständigheterna i det enskilda fallet, påföras utöver eller i stället för de åtgärder som avses i artikel 58.2 a–h och j. Vid beslut om huruvida administrativa sanktionsavgifter ska påföras och om beloppet för de administrativa sanktionsavgifterna i varje enskilt fall ska vederbörlig hänsyn tas till följande:

a) Överträdelsens karaktär, svårighetsgrad och varaktighet med beaktande av den aktuella uppgiftsbehandlingens karaktär, omfattning eller syfte samt antalet berörda registrerade och den skada som de har lidit.

b) Om överträdelsen skett med uppsåt eller genom oaktsamhet.

c) De åtgärder som den personuppgiftsansvarige eller personuppgiftsbiträdet har vidtagit för att lindra den skada som de registrerade har lidit.

d) Graden av ansvar hos den personuppgiftsansvarige eller personuppgiftsbiträdet med beaktande av de tekniska och organisatoriska åtgärder som genomförts av dem i enlighet med artiklarna 25 och 32.

e) Eventuella relevanta tidigare överträdelser som den personuppgiftsansvarige eller personuppgiftsbiträdet gjort sig skyldig till.

f) Graden av samarbete med tillsynsmyndigheten för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter.

g) De kategorier av personuppgifter som påverkas av överträdelsen.

h) Det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, särskilt huruvida och i vilken omfattning den personuppgiftsansvarige eller personuppgiftsbiträdet anmälde överträdelsen.

i) När åtgärder enligt artikel 58.2 tidigare har förordnats mot den berörda personuppgiftsansvarige eller personuppgiftsbiträdet vad gäller samma sakfråga, efterlevnad av dessa åtgärder.

j) Tillämpandet av godkända uppförandekoder i enlighet med artikel 40 eller godkända certifieringsmekanismer i enlighet med artikel 42.

k) Eventuell annan försvårande eller förmildrande faktor som är tillämplig på omständigheterna i fallet, såsom ekonomisk vinst som görs eller förlust som undviks, direkt eller indirekt, genom överträdelsen.

3. Om en personuppgiftsansvarig eller ett personuppgiftsbiträde, med avseende på en och samma eller sammankopplade uppgiftsbehandlingar, uppsåtligen eller av oaktsamhet överträder flera av bestämmelserna i denna förordning får den administrativa sanktionsavgiftens totala belopp inte överstiga det belopp som fastställs för den allvarligaste överträdelsen.

4. Vid överträdelser av följande bestämmelser ska det i enlighet med punkt 2 påföras administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om det gäller ett företag, på upp till 2 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

a) Personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter enligt artiklarna 8, 11, 25–39, 42 och 43.

b) Certifieringsorganets skyldigheter enligt artiklarna 42 och 43.

c) Övervakningsorganets skyldigheter enligt artikel 41.4.

5. Vid överträdelser av följande bestämmelser ska det i enlighet med punkt 2 påföras administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

a) De grundläggande principerna för behandling, inklusive villkoren för samtycke, enligt artiklarna 5, 6, 7 och 9.

b) Registrerades rättigheter enligt artiklarna 12–22.

c) Överföring av personuppgifter till en mottagare i ett tredjeland eller en internationell organisation enligt artiklarna 44–49.

d) Alla skyldigheter som följer av medlemsstaternas lagstiftning som antagits på grundval av kapitel IX.

e) Underlåtenhet att rätta sig efter ett föreläggande eller en tillfällig eller permanent begränsning av behandling av uppgifter eller ett beslut om att avbryta uppgiftsflödena som meddelats av tillsynsmyndigheten i enlighet med artikel 58.2 eller underlåtelse att ge tillgång till uppgifter i strid med artikel 58.1.

6. Vid underlåtenhet att rätta sig efter ett föreläggande från tillsynsmyndigheten i enlighet med artikel 58.2 ska det i enlighet med punkt 2 i den här artikeln påföras administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

7. Utan att det påverkar tillsynsmyndigheternas korrigerande befogenheter enligt artikel 58.2 får varje medlemsstat fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och organ som är inrättade i medlemsstaten.

8. Tillsynsmyndighetens utövande av sina befogenheter enligt denna artikel ska omfattas av lämpliga rättssäkerhetsgarantier i enlighet med unionsrätten och medlemsstaternas nationella rätt, inbegripet effektiva rättsmedel och rättssäkerhet.

9. Om det i medlemsstatens rättssystem inte finns några föreskrifter om administrativa sanktionsavgifter får den här artikeln tillämpas så att förfarandet inleds av den behöriga tillsynsmyndigheten och sanktionsavgifterna sedan utdöms av behörig nationell domstol, varvid det säkerställs att rättsmedlen är effektiva och har motsvarande verkan som de administrativa sanktionsavgifter som påförs av tillsynsmyndigheter. De sanktionsavgifter som påförs ska i alla händelser vara effektiva, proportionella och avskräckande. Dessa medlemsstater ska till kommissionen anmäla de bestämmelser i deras lagstiftning som de antar i enlighet med denna punkt senast den 25 maj 2018, samt utan dröjsmål anmäla eventuell senare ändringslagstiftning eller ändringar som berör dem.

Artikel 84

Sanktioner

1. Medlemsstaterna ska fastställa regler om andra sanktioner för överträdelser av denna förordning, särskilt för överträdelser som inte är föremål för administrativa sanktionsavgifter enligt artikel 83, och vidta alla nödvändiga åtgärder för att säkerställa att de genomförs. Dessa sanktioner ska vara effektiva, proportionella och avskräckande.

2. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antar i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella senare ändringar som berör dem.

KAPITEL IX

Bestämmelser om särskilda behandlingssituationer

Artikel 85

Behandling och yttrande- och informationsfriheten

1. Medlemsstaterna ska i lag förena rätten till integritet i enlighet med denna förordning med yttrande- och informationsfriheten, inbegripet behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

2. Medlemsstaterna ska, för behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande, fastställa undantag eller avvikelser från kapitel II (principer), kapitel III (den registrerades rättigheter), kapitel IV (personuppgiftsansvarig och personuppgiftsbiträde), kapitel V (överföring av personuppgifter till tredjeländer eller internationella organisationer), kapitel VI (oberoende tillsynsmyndigheter), kapitel VII (samarbete och enhetlighet) och kapitel IX (särskilda situationer vid behandling av personuppgifter) om dessa är nödvändiga för att förena rätten till integritet med yttrande- och informationsfriheten.

3. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antagit i enlighet med punkt 2, samt utan dröjsmål anmäla eventuell senare ändringslagstiftning eller ändringar som berör dem.

Artikel 86

Behandling och allmänhetens tillgång till allmänna handlingar

Personuppgifter i allmänna handlingar som förvaras av en myndighet eller ett offentligt organ eller ett privat organ för utförande av en uppgift av allmänt intresse får lämnas ut av myndigheten eller organet i enlighet med den unionsrätt eller den medlemsstats nationella rätt som myndigheten eller det offentliga organet omfattas av, för att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd av personuppgifter i enlighet med denna förordning.

Artikel 87

Behandling av nationella identifikationsnummer

Medlemsstaterna får närmare bestämma på vilka särskilda villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas. Ett nationellt identifikationsnummer eller ett annat vedertaget sätt för identifiering ska i sådana fall endast användas med iakttagande av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt denna förordning.

Artikel 88

Behandling i anställningsförhållanden

1. Medlemsstaterna får i lag eller i kollektivavtal fastställa mer specifika regler för att säkerställa skyddet av rättigheter och friheter vid behandling av anställdas personuppgifter i anställningsförhållanden, särskilt när det gäller rekrytering, genomförande av anställningsavtalet inklusive befrielse från i lag eller kollektivavtal stadgade skyldigheter, ledning, planering och organisering av arbetet, jämställdhet och mångfald i arbetslivet, hälsa och säkerhet på arbetsplatsen samt skydd av arbetsgivarens eller kundens egendom men också när det gäller att såväl kollektivt som individuellt utöva och komma i åtnjutande av rättigheter och förmåner som är knutna till anställningen samt att avsluta anställningsförhållandet.

2. Dessa regler ska innehålla lämpliga och specifika åtgärder för att skydda den registrerades mänskliga värdighet, berättigade intressen och grundläggande rättigheter, varvid hänsyn särskilt ska tas till insyn i behandlingen, överföring av personuppgifter inom en koncern eller en grupp av företag som deltar i gemensam ekonomisk verksamhet samt övervakningssystem på arbetsplatsen.

3. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antar i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella senare ändringar som berör dem.

Artikel 89

Skyddsåtgärder och undantag för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål

1. Behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ska omfattas av lämpliga skyddsåtgärder i enlighet med denna förordning för den registrerades rättigheter och friheter. Skyddsåtgärderna ska säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt

principen om uppgiftsminimering iakttas. Dessa åtgärder får inbegripa pseudonymisering, under förutsättning att dessa ändamål kan uppfyllas på det sättet. När dessa ändamål kan uppfyllas genom vidare behandling av uppgifter som inte medger eller inte längre medger identifiering av de registrerade ska dessa ändamål uppfyllas på det sättet.

2. Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål får det i unionsrätten eller i medlemsstaternas nationella rätt föreskrivas undantag från de rättigheter som avses i artiklarna 15, 16, 18 och 21 med förbehåll för de villkor och skyddsåtgärder som avses i punkt 1 i den här artikeln i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla de särskilda ändamålen, och sådana undantag krävs för att uppnå dessa ändamål.

3. Om personuppgifter behandlas för arkivändamål av allmänt intresse får det i unionsrätten eller i medlemsstaternas nationella rätt föreskrivas om undantag från de rättigheter som avses i artiklarna 15, 16, 18, 19, 20 och 21 med förbehåll för de villkor och skyddsåtgärder som avses i punkt 1 i den här artikeln i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla de särskilda ändamålen, och sådana undantag krävs för att uppnå dessa ändamål.

4. Om behandling enligt punkterna 2 och 3 samtidigt har andra ändamål, ska undantagen endast tillämpas på behandling för de ändamål som avses i dessa punkter.

Artikel 90

Tystnadsplikt

1. Medlemsstaterna får anta särskilda bestämmelser för att fastställa tillsynsmyndigheternas befogenheter enligt artikel 58.1 e och f gentemot personuppgiftsansvariga eller personuppgiftsbiträden som enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställts av behöriga nationella organ omfattas av tystnadsplikt eller andra motsvarande former av förbud mot att lämna ut uppgifter, om det är nödvändigt och står i proportion till vad som behövs för att förena rätten till skydd för personuppgifter och tystnadsplikten. Dessa bestämmelser ska endast tillämpas med avseende på personuppgifter som den personuppgiftsansvarige eller personuppgiftsbiträdet har erhållit i samband med en verksamhet som omfattas av denna tystnadsplikt.

2. Varje medlemsstat ska till kommissionen anmäla de bestämmelser den har antagit i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella ändringar som berör dem.

Artikel 91

Befintliga bestämmelser om dataskydd inom kyrkor och religiösa samfund

1. Om kyrkor och religiösa samfund eller gemenskaper i en medlemsstat vid tidpunkten för ikraftträdandet av denna förordning tillämpar övergripande bestämmelser om skyddet av fysiska personer i samband med behandling, får sådana befintliga bestämmelser fortsätta att tillämpas under förutsättning att de görs förenliga med denna förordning.

2. Kyrkor och religiösa samfund som tillämpar övergripande bestämmelser i enlighet med punkt 1 i denna artikel ska vara föremål för kontroll av en oberoende tillsynsmyndighet som kan vara specifik, förutsatt att den uppfyller de villkor som fastställs i kapitel VI i denna förordning.

KAPITEL X

Delegerade akter och genomförandeakter

Artikel 92

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 12.8 och artikel 43.8 ska ges till kommissionen tills vidare från och med den 24 maj 2016.

3. Den delegering av befogenhet som avses i artikel 12.8 och artikel 43.8 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

5. En delegerad akt som antas enligt artikel 12.8 och artikel 43.8 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av tre månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med tre månader på Europaparlamentets eller rådets initiativ.

Artikel 93

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

3. När det hänvisas till denna punkt ska artikel 8 i förordning (EU) nr 182/2011, jämförd med artikel 5 i samma förordning, tillämpas.

KAPITEL XI

Slutbestämmelser

Artikel 94

Upphävande av direktiv 95/46/EG

1. Direktiv 95/46/EG ska upphöra att gälla med verkan från och med den 25 maj 2018.

2. Hänvisningar till det upphävda direktivet ska anses som hänvisningar till denna förordning. Hänvisningar till arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, som inrättades genom artikel 29 i direktiv 95/46/EG, ska anses som hänvisningar till Europeiska dataskyddsstyrelsen, som inrättas genom denna förordning.

Artikel 95

Förhållande till direktiv 2002/58/EG

Denna förordning ska inte innebära några ytterligare förpliktelser för fysiska eller juridiska personer som behandlar personuppgifter inom ramen för tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät i unionen, när det gäller områden inom vilka de redan omfattas av särskilda skyldigheter för samma ändamål i enlighet med direktiv 2002/58/EG.

Artikel 96

Förhållande till tidigare ingångna avtal

De internationella avtal som rör överföring av personuppgifter till tredjeländer eller internationella organisationer som ingicks av medlemsstaterna före den 24 maj 2016 och som är förenliga med unionsrätten i dess lydelse innan detta datum, ska fortsätta att gälla tills de ändras, ersätts eller återkallas.

Artikel 97

Kommissionsrapporter

1. Senast den 25 maj 2020 och därefter vart fjärde år ska kommissionen överlämna en rapport om tillämpningen och översynen av denna förordning till Europaparlamentet och rådet.

2. Inom ramen för de utvärderingar och översyner som avses i punkt 1 ska kommissionen särskilt undersöka hur följande bestämmelser tillämpas och fungerar:

a) Kapitel V om överföring av personuppgifter till tredjeländer och internationella organisationer, särskilt när det gäller beslut som antagits enligt artikel 45.3 i den här förordningen och beslut som antagits på grundval av artikel 25.6 i direktiv 95/46/EG.

b) Kapitel VII om samarbete och enhetlighet.

3. Med avseende på tillämpningen av punkt 1 får kommissionen begära information från medlemsstaterna och tillsynsmyndigheterna.

4. Kommissionen ska när den utför de utvärderingar och översyner som avses i punkterna 1 och 2 ta hänsyn till ståndpunkter och slutsatser från Europaparlamentet, rådet och andra relevanta organ och källor.

5. Kommissionen ska om nödvändigt överlämna lämpliga förslag om ändring av denna förordning, med särskild hänsyn till informationsteknikens utveckling och mot bakgrund av tendenserna inom informationssamhället.

Artikel 98

Översyn av andra unionsrättsakter om dataskydd

Kommissionen ska, om så är lämpligt, lägga fram lagstiftningsförslag i syfte att ändra andra unionsrättsakter om skydd av personuppgifter, för att säkerställa ett enhetligt och konsekvent skydd för fysiska personer med avseende på behandling. Detta gäller i synnerhet bestämmelserna om skyddet för fysiska personer i samband med behandling som utförs av unionens institutioner, organ och byråer samt om det fria flödet av sådana uppgifter.

Artikel 99

Ikraftträdande och tillämpning

1. Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

2. Den ska tillämpas från och med den 25 maj 2018.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 27 april 2016.

På Europaparlamentets vägnar	*På rådets vägnar*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT
Ordförande	*Ordförande*

4.5.2016 SV Europeiska unionens officiella tidning L 119/89

DIREKTIV

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2016/680

av den 27 april 2016

om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16.2,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Regionkommitténs yttrande ( ),

i enlighet med det ordinarie lagstiftningsförfarandet ( ), och

av följande skäl:

(1) Skyddet för fysiska personer med avseende på behandling av personuppgifter är en grundläggande rättighet. I artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) och artikel 16.1 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) föreskrivs att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

(2) Principerna och reglerna för skyddet för fysiska personer med avseende på behandling av deras personuppgifter bör, oavsett deras medborgarskap eller hemvist, respektera deras rättigheter och grundläggande friheter, särskilt deras rätt till skydd av personuppgifter. Detta direktiv är avsett att bidra till att skapa ett område med frihet, säkerhet och rättvisa.

(3) Den snabba tekniska utvecklingen och globaliseringen har skapat nya utmaningar vad gäller skyddet av personuppgifter. Omfattningen av insamlingen och delningen av personuppgifter har ökat avsevärt. Tekniken gör det möjligt att i en aldrig tidigare skådad omfattning behandla personuppgifter i verksamheter såsom förebyggande, förhindrande, utredning, avslöjande och lagföring av brott eller verkställighet av straffrättsliga påföljder.

(4) Det fria flödet av personuppgifter mellan behöriga myndigheter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten inom unionen, samt överföringar av sådana personuppgifter till tredjeländer och internationella organisationer, bör underlättas samtidigt som en hög skyddsnivå för personuppgifter säkerställs. Denna utveckling kräver en stark och mer sammanhängande ram för skyddet av personuppgifter inom unionen, uppbackad av kraftfullt tillsynsarbete.

(5) Europaparlamentets och rådets direktiv 95/46/EG ( ) är tillämpligt på all behandling av personuppgifter i medlemsstaterna, såväl inom den offentliga som inom den privata sektorn. Det är emellertid inte tillämpligt på behandling av personuppgifter ”som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten”, t.ex. verksamhet på områdena för straffrättsligt samarbete och polissamarbete.

( ) EUT C 391, 18.12.2012, s. 127.
( ) Europaparlamentets ståndpunkt av den 12 mars 2014 (ännu ej offentliggjord i EUT) och rådets ståndpunkt vid första behandlingen av den 8 april 2016 (ännu ej offentliggjord i EUT). Europaparlamentets ståndpunkt av den 14 april 2016.
( ) Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).

(6) Rådets rambeslut 2008/977/RIF ( ) är tillämpligt på områdena för straffrättsligt samarbete och polissamarbete. Tillämpningsområdet för det rambeslutet begränsas till behandling av sådana personuppgifter som överförs eller görs tillgängliga mellan medlemsstaterna.

(7) Att säkerställa en enhetlig och hög skyddsnivå för fysiska personers personuppgifter och underlätta utbytet av personuppgifter mellan behöriga myndigheter i medlemsstaterna är av avgörande betydelse för att säkerställa ett effektivt straffrättsligt samarbete och polissamarbete. Därför bör skyddet för fysiska personers rättigheter och friheter i samband med behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, vara likvärdigt i alla medlemsstater. Ett effektivt skydd av personuppgifter i hela unionen förutsätter att de registrerades rättigheter stärks och att skyldigheterna för dem som behandlar personuppgifter, ökar, samt likvärdiga befogenheter för att övervaka och säkerställa efterlevnaden av bestämmelserna om skydd av personuppgifter i medlemsstaterna.

(8) I artikel 16.2 i EUF-fördraget bemyndigas Europaparlamentet och rådet att fastställa bestämmelser om skydd för fysiska personer när det gäller behandling av personuppgifter samt om det fria flödet för personuppgifter.

(9) Med stöd av denna grund fastställs i Europaparlamentets och rådets förordning (EU) 2016/679 ( ) allmänna bestämmelser om skydd av fysiska personer i samband med behandling av personuppgifter och om det fria flödet för sådana uppgifter inom unionen.

(10) I förklaring nr 21 om skydd av personuppgifter på området för straffrättsligt samarbete och polissamarbete, fogad till slutakten från den regeringskonferens som antog Lissabonfördraget, bekräftade konferensen att det med hänsyn till dessa områdens särart kan komma att bli nödvändigt att anta särskilda regler om skydd av personuppgifter och om det fria flödet av personuppgifter på områdena för straffrättsligt samarbete och polissamarbete med stöd av artikel 16 i EUF-fördraget.

(11) Det är därför lämpligt att dessa områden behandlas i ett direktiv som fastställer särskilda regler om skydd för fysiska personer i samband med behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, med respekt för den särskilda karaktären hos denna verksamhet. Sådana behöriga myndigheter kan omfatta inte bara offentliga myndigheter såsom rättsliga myndigheter, polis eller andra brottsbekämpande myndigheter, utan också alla andra organ eller enheter som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning enligt detta direktiv. Förordning (EU) 2016/679 bör tillämpas när ett sådant organ eller en sådan enhet behandlar personuppgifter för andra ändamål än de som avses i detta direktiv. Förordning (EU) 2016/679 är därför tillämplig i fall då ett organ eller en enhet samlar in personuppgifter för andra ändamål och behandlar dessa personuppgifter ytterligare för att iaktta sina rättsliga skyldigheter. Exempelvis behåller finansinstitut vissa personuppgifter som de behandlar i syfte att utreda, avslöja eller lagföra brott, och tillhandahåller dessa personuppgifter för behöriga nationella myndigheter endast i särskilda fall och i enlighet med medlemsstaternas nationella rätt. Ett organ eller en enhet som behandlar personuppgifter för sådana myndigheters räkning inom detta direktivs tillämpningsområde bör vara bundet av ett avtal eller annan rättsakt och de bestämmelser som är tillämpliga på personuppgiftsbiträden enligt detta direktiv, medan tillämpningen av förordning (EU) 2016/679 förblir opåverkad när det gäller personuppgiftsbiträdets behandling av personuppgifter som inte omfattas av detta direktivs tillämpningsområde.

(12) Polisens och andra brottsbekämpande myndigheters verksamhet är främst inriktad på att förebygga, förhindra, utreda, avslöja och lagföra brott, inbegripet polisverksamhet där man inte på förhand vet om det inträffade utgör ett brott eller inte. Sådan verksamhet kan också innefatta myndighetsutövning genom vidtagande av tvångsåtgärder vid demonstrationer, större idrottsevenemang och upplopp. Denna verksamhet omfattar också upprätthållande av lag och ordning som en uppgift som anförtros åt polisen eller andra brottsbekämpande

( ) Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (EUT L 350, 30.12.2008, s. 60).

( ) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (se sidan 1 i detta nummer av EUT).

myndigheter när det är nödvändigt för att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten och mot i lag skyddade grundläggande allmänna intressen som kan leda till ett brott. Medlemsstaterna får åt behöriga myndigheter anförtro andra uppgifter som inte nödvändigtvis utförs för att förebygga, förhindra, utreda, avslöja eller lagföra brott, inklusive att skydda mot och förebygga hot mot den allmänna säkerheten, så att behandlingen av personuppgifter för dessa andra ändamål, i den mån den omfattas av unionsrätten, omfattas av tillämpningsområdet för förordning (EU) 2016/679.

(13) Ett brott i den mening som avses i detta direktiv bör utgöra ett självständigt begrepp i unionsrätten enligt Europeiska unionens domstols (nedan kallad *domstolen*) tolkning.

(14) Eftersom detta direktiv inte bör tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten, bör verksamhet som rör nationell säkerhet, verksamhet som utförs av byråer och organ som hanterar nationella säkerhetsfrågor och medlemsstaternas behandling av personuppgifter när de utför verksamhet som omfattas av del V kapitel 2 i fördraget om Europeiska unionen (EU-fördraget) inte betraktas som verksamhet som omfattas av detta direktivs tillämpningsområde.

(15) För att säkerställa en enhetlig skyddsnivå för fysiska personer genom rättsligt verkställbara rättigheter i hela unionen och undvika avvikelser som hämmar utbytet av personuppgifter mellan behöriga myndigheter, bör detta direktiv innehålla harmoniserade bestämmelser om skydd och fri rörlighet för personuppgifter som behandlas för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Tillnärmningen av medlemsstaternas nationella rätt bör inte leda till försämringar i det personuppgiftsskydd de tillhandahåller, utan i stället ha till syfte att säkerställa en hög skyddsnivå inom unionen. Inget ska hindra medlemsstaterna från att föreskriva starkare skyddsåtgärder än dem som fastställs i detta direktiv för skyddet av den registrerades rättigheter och friheter med avseende på behöriga myndigheters behandling av personuppgifter.

(16) Detta direktiv påverkar inte tillämpningen av principen om allmänhetens rätt att få tillgång till allmänna handlingar. Enligt förordning (EU) 2016/679 får personuppgifter i allmänna handlingar som förvaras av en offentlig myndighet eller ett offentligt eller privat organ för utförande av en uppgift av allmänt intresse lämnas ut av myndigheten eller organet i enlighet med unionsrätten eller medlemsstatens nationella lagstiftning som den offentliga myndigheten eller det offentliga organet omfattas av, för att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd av personuppgifter.

(17) Det skydd som ska tillhandahållas enligt detta direktiv bör tillämpas på fysiska personer, oavsett medborgarskap eller hemvist, med avseende på behandling av deras personuppgifter.

(18) För att förhindra att det uppstår en allvarlig risk för att reglerna kringgås bör skyddet för fysiska personer vara teknikneutralt och inte vara beroende av den teknik som används. Skyddet för fysiska personer bör vara tillämpligt på både automatiserad och manuell behandling av personuppgifter, om personuppgifterna ingår i eller är avsedda att ingå i ett register. Akter eller grupper av akter samt omslag till dessa, som inte är ordnade enligt särskilda kriterier, bör inte omfattas av detta direktiv.

(19) Europaparlamentets och rådets förordning (EG) nr 45/2001 ( ) är tillämplig på den behandling av personuppgifter som sker i unionens institutioner, organ och byråer. Förordning (EG) nr 45/2001 och de av unionens övriga rättsakter som är tillämpliga på sådan behandling av personuppgifter bör anpassas till principerna och bestämmelserna i förordning (EU) 2016/679.

(20) Detta direktiv bör inte hindra medlemsstaterna från att i nationell straffprocesslagstiftning ange vilken behandling och vilka förfaranden för behandling som berörs när det gäller domstolars och andra rättsliga myndigheters behandling av personuppgifter, särskilt när det gäller personuppgifter som ingår i ett domstolsbeslut eller i protokoll avseende straffrättsliga förfaranden.

( ) Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

(21) Principerna för dataskydd bör gälla all information som rör en identifierad eller identifierbar fysisk person. För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel, som t.ex. utgallring, som, antingen av den personuppgiftsansvarige eller av någon annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva faktorer som kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen. Principerna för dataskydd bör därför inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte längre är identifierbar.

(22) Offentliga myndigheter som för sin myndighetsutövning mottar personuppgifter i enlighet med en rättslig förpliktelse, t.ex. skatte- och tullmyndigheter, finansutredningsgrupper, oberoende administrativa myndigheter eller finansmarknadsmyndigheter med ansvar för reglering och övervakning av värdepappersmarknader, bör inte betraktas som mottagare om de tar emot personuppgifter som är nödvändiga för utförandet av en särskild utredning i allmänhetens intresse, i enlighet med unionsrätten eller medlemstaternas nationella rätt. Offentliga myndigheters begäranden om att uppgifter ska lämnas ut bör alltid vara skriftliga och motiverade, läggas fram i enskilda fall och inte gälla hela register eller leda till att register kopplas samman. Dessa offentliga myndigheters behandling av personuppgifter bör ske i överensstämmelse med de bestämmelser om dataskydd som är tillämpliga på behandlingens ändamål.

(23) Genetiska uppgifter bör definieras som personuppgifter som rör en fysisk persons nedärvda eller förvärvade genetiska kännetecken som ger unik information om denna enskilda persons fysiologi eller hälsa och vilka framgår av en analys av ett biologiskt prov från den fysiska personen i fråga, framför allt kromosom-, DNA- eller RNA-analys eller av en annan form av analys som gör det möjligt att inhämta motsvarande information. Eftersom genetiska uppgifter är komplexa och känsliga finns det en stor risk för att den personuppgiftsansvarige missbrukar och återanvänder dem för olika ändamål. All diskriminering på grundval av genetiska särdrag bör i princip vara förbjuden.

(24) Personuppgifter om hälsa bör innefatta alla uppgifter som hänför sig till en registrerad persons hälsotillstånd som ger information om den registrerades tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd. Detta inbegriper uppgifter om den enskilda personen som samlats in i samband med registrering för eller tillhandahållande av hälso- och sjukvårdstjänster till den fysiska personen enligt Europaparlamentets och rådets direktiv 2011/24/EU ( ), ett nummer, en symbol eller ett kännetecken som personen tilldelats för att unikt identifiera den fysiska personen för hälso- och sjukvårdsändamål, uppgifter som härrör från tester eller undersökningar av en kroppsdel eller kroppssubstans, däribland genetiska uppgifter och biologiska prover, och andra uppgifter om exempelvis sjukdom, funktionshinder, sjukdomsrisk, sjukdomshistoria, klinisk behandling, eller den registrerades fysiologiska eller biomedicinska tillstånd oberoende av källan, exempelvis från en läkare eller från annan sjukvårdspersonal, ett sjukhus, en medicinteknisk produkt eller ett diagnostiskt in vitro-test.

(25) Samtliga medlemsstater är anslutna till Internationella kriminalpolisorganisationen (Interpol). För att kunna fullgöra sitt uppdrag mottar, lagrar och cirkulerar Interpol personuppgifter i syfte att hjälpa behöriga myndigheter att förebygga, förhindra och bekämpa internationell brottslighet. Därför är det lämpligt att stärka samarbetet mellan unionen och Interpol genom att främja ett effektivt utbyte av personuppgifter med respekt för de grundläggande rättigheterna och friheterna vid automatiserad behandling av personuppgifter. När personuppgifter överförs från unionen till Interpol samt till länder som har delegerade medlemmar i Interpol bör detta direktiv, framför allt bestämmelserna om internationella överföringar, gälla. Detta direktiv bör inte påverka de särskilda bestämmelserna i rådets gemensamma ståndpunkt 2005/69/RIF ( ) och rådets beslut 2007/533/RIF ( ).

(26) Varje behandling av personuppgifter måste vara laglig, korrekt och öppen i förhållande till berörda fysiska personer och endast genomföras för särskilda lagstadgade ändamål. Detta hindrar i sig inte brottsbekämpande myndigheter från att genomföra verksamhet såsom hemliga utredningar eller videoövervakning. Sådan verksamhet kan genomföras i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa

( ) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).
( ) Rådets gemensamma ståndpunkt 2005/69/RIF av den 24 januari 2005 om utbyte av vissa uppgifter med Interpol (EUT L 27, 29.1.2005, s. 61).
( ) Rådets beslut 2007/533/RIF av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) (EUT L 205, 7.8.2007, s. 63).

straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, förutsatt att verksamheten har fastställts i lag och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den fysiska personens berättigade intressen. Dataskyddsprincipen om korrekt behandling är ett begrepp som är skilt från rätten till en opartisk domstol enligt artikel 47 i stadgan och rätten till en rättvis rättegång enligt artikel 6 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Fysiska personer bör göras medvetna om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter och om hur de kan utöva sina rättigheter med avseende på behandlingen. De specifika ändamål som personuppgifterna behandlas för bör vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in. Personuppgifterna bör vara adekvata och relevanta för de ändamål som de behandlas för. Det bör i synnerhet säkerställas att de uppgifter som insamlats inte är orimligt omfattande och att de inte sparas längre än vad som är nödvändigt för det ändamål för vilket uppgifterna behandlas. Personuppgifter bör endast behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel. För att säkerställa att uppgifter inte sparas längre än nödvändigt bör den personuppgiftsansvarige införa tidsfrister för radering eller för regelbunden kontroll. Medlemsstaterna bör inrätta lämpliga skyddsåtgärder för personuppgifter som lagras under längre perioder, för arkivändamål av allmänt intresse, för vetenskapliga, statistiska eller historiska ändamål.

(27) Om behöriga myndigheter ska kunna förebygga, förhindra, utreda och lagföra brott är det nödvändigt att de behandlar personuppgifter som insamlats inom ramen för förebyggande, förhindrande, utredning och lagföring av specifika brott i ett bredare sammanhang för att utveckla förståelsen för kriminell verksamhet och göra kopplingar mellan olika upptäckta brott.

(28) För att bibehålla behandlingens säkerhet och förhindra behandling som innebär en överträdelse av detta direktiv bör personuppgifter behandlas på ett sätt som säkerställer en lämplig säkerhets- och konfidentialitetsnivå samt förhindrar obehörigt tillträde till eller obehörig användning av personuppgifter och den utrustning som används för behandlingen, med beaktande av tillgänglig teknik och den tekniska utvecklingen samt genomförandekostnader i förhållande till riskerna och den typ av personuppgifter som ska skyddas.

(29) Personuppgifter bör samlas in för särskilda, uttryckligt angivna och berättigade ändamål som omfattas av detta direktivs tillämpningsområde och bör inte behandlas för andra ändamål än att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Om samma eller en annan personuppgiftsansvarig behandlar personuppgifter för ett ändamål som omfattas av detta direktiv men som inte är det ändamål som uppgifterna insamlades för, bör behandlingen vara tillåten, förutsatt att behandlingen har godkänts i enlighet med tillämpliga rättsliga bestämmelser och är nödvändig och står i proportion till det andra ändamålet.

(30) Principen om uppgifters korrekthet bör tillämpas med hänsyn till den typ av behandling det är fråga om och syftet med denna. Särskilt i domstolsförfaranden baseras utsagor som innehåller personuppgifter på fysiska personers subjektiva uppfattning, och kan inte alltid verifieras. Följaktligen bör inte korrekthetskravet röra korrektheten i en utsaga, utan endast det faktum att en viss utsaga har gjorts.

(31) Behandling av personuppgifter på områdena för straffrättsligt samarbete och polissamarbete innebär av naturliga skäl att personuppgifter om olika kategorier av registrerade behandlas. Därför är det viktigt att i tillämpliga fall och i möjligaste mån göra en klar åtskillnad mellan personuppgifter om olika kategorier av registrerade, t.ex. brottsmisstänkta, brottsdömda och brottsoffer samt andra som berörs av ett brottmål, t.ex. vittnen, personer med relevant information eller personer med kontakter eller band till brottsmisstänkta och brottsdömda. Detta bör inte hindra tillämpningen av rätten till oskuldspresumtion som garanteras i stadgan och i Europakonventionen, tolkade enligt rättspraxis från domstolen och Europeiska domstolen för de mänskliga rättigheterna.

(32) De behöriga myndigheterna bör säkerställa att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. För att säkerställa skydd för fysiska personer, korrekthet, fullständighet eller i vilken grad personuppgifterna är aktuella och tillförlitlighet i de personuppgifter som överförs eller görs tillgängliga, bör de behöriga myndigheterna i möjligaste mån föra in nödvändiga uppgifter vid all överföring av personuppgifter.

(33) När det i detta direktiv hänvisas till medlemsstaternas nationella rätt, en rättslig grund eller lagstiftningsåtgärd innebär detta inte nödvändigtvis en lagstiftningsakt antagen av ett parlament, med förbehåll för krav i den

berörda medlemsstatens konstitutionella ordning. Medlemsstaternas nationella rätt, den rättsliga grunden eller lagstiftningsåtgärden bör emellertid i dessa fall vara tydlig och precis, och dess tillämpning förutsägbar för dem som omfattas av den i enlighet med rättspraxis från domstolen och Europeiska domstolen för de mänskliga rättigheterna. Medlemsstaternas nationella rätt som reglerar behandlingen av personuppgifter inom tillämpningsområdet för detta direktiv bör åtminstone specificera målen, vilka personuppgifter som ska behandlas, behandlingens ändamål, förfarandena för att bevara personuppgifternas integritet och konfidentialitet samt förfarandena för förstöring av dem så att tillräckliga garantier mot risken för missbruk och godtycklighet ges.

(34) Behöriga myndigheters behandling av personuppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott, verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, bör omfatta varje åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter som utförs i dessa syften, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, justering eller sammanförande, begränsning av behandlingen, radering eller förstöring. Framför allt bör bestämmelserna i detta direktiv gälla personuppgifter som vid tillämpningen av detta direktiv överförs till en mottagare som inte omfattas av detta direktiv. Med sådana mottagare bör avses fysiska eller juridiska personer, myndigheter, institutioner eller andra organ som den behöriga myndigheten lagligen lämnar ut personuppgifterna till. Om personuppgifter ursprungligen samlats in av en behörig myndighet för något av detta direktivs ändamål, bör förordning (EU) 2016/679 vara tillämplig på behandlingen av dessa uppgifter för andra ändamål än de som anges i detta direktiv om behandlingen är godkänd enligt unionsrätten eller nationell rätt. Framför allt bör bestämmelserna i förordning (EU) 2016/679 gälla överföring av personuppgifter för ändamål som inte omfattas av detta direktiv. Förordning (EU) 2016/679 bör gälla när personuppgifter behandlas av en mottagare som varken är eller agerar i egenskap av behörig myndighet i den mening som avses i detta direktiv och som lagligen mottagit personuppgifter av en behörig myndighet. Vid tillämpningen av detta direktiv bör medlemsstaterna också närmare kunna ange tillämpningen av bestämmelserna i förordning (EU) 2016/679 på de villkor som anges i den förordningen.

(35) För att vara laglig bör behandlingen av personuppgifter enligt detta direktiv vara nödvändig för att utföra en uppgift av allmänt intresse som en behörig myndighet ansvarar för enligt unionsrätten eller medlemsstaternas nationella rätt för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Denna verksamhet bör omfatta skydd av intressen som är av grundläggande betydelse för den registrerade. Utförandet av uppgifterna att förebygga, förhindra, utreda, avslöja eller lagföra brott, som de behöriga myndigheterna institutionellt har tilldelats enligt lag, gör det möjligt för dem att kräva eller beordra att fysiska personer efterlever de begäranden som gjorts. I detta fall bör den registrerades samtycke, enligt definitionen i förordning (EU) 2016/679, inte utgöra en rättslig grund för behöriga myndigheters behandling av personuppgifter. Om den registrerade är skyldig att fullgöra en rättslig förpliktelse har den registrerade inte någon genuin och fri valmöjlighet, och således är det inte möjligt att betrakta den registrerades reaktion som en frivillig viljeyttring. Detta bör inte hindra medlemsstaterna från att i lag fastställa att den registrerade får tillåta behandling av sina personuppgifter vid tillämpning av detta direktiv, såsom DNA-testning inom ramen för brottsutredningar eller övervakning av var den registrerade befinner sig med elektronisk fotboja för verkställighet av straffrättsliga påföljder.

(36) Medlemsstaterna bör föreskriva att om det i den unionsrätt eller nationella rätt som är tillämplig på den överförande behöriga myndigheten fastställs särskilda villkor som under särskilda omständigheter är tillämpliga på behandlingen av personuppgifter, såsom användning av hanteringskoder, bör den överförande behöriga myndigheten informera den mottagare till vilken uppgifterna överförs om dessa villkor och om kravet att respektera dem. Sådana villkor kan till exempel innefatta ett förbud mot att överföra personuppgifter till andra mottagare eller använda dem i andra syften än de för vilka de överfördes till mottagaren eller att informera den registrerade vid en begränsning av rätten till information utan förhandsgodkännande från den överförande behöriga myndigheten. Dessa skyldigheter bör även gälla för överföringar från den överförande behöriga myndigheten till mottagare i tredjeländer eller internationella organisationer. Medlemsstaterna bör säkerställa att den överförande behöriga myndigheten inte tillämpar dessa villkor på mottagare i andra medlemsstater eller på byråer och organ som inrättats i enlighet med avdelning V kapitlen 4 och 5 i EUF-fördraget, med undantag för sådana villkor som är tillämpliga på motsvarande överföringar av uppgifter inom den medlemsstat där den behöriga myndigheten är belägen.

(37) Personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheter och friheter bör åtnjuta ett särskilt skydd eftersom behandling av sådana uppgifter kan innebära betydande risker för de grundläggande rättigheterna och friheterna. Dessa personuppgifter bör även inbegripa personuppgifter som avslöjar ras eller etniskt ursprung, varvid användningen av termen *ras* i detta direktiv inte innebär att unionen

godtar teorier som söker fastställa förekomsten av skilda människoraser. Dessa personuppgifter bör inte behandlas såvida inte behandlingen omfattas av lämpliga skyddsåtgärder för den registrerades lagstadgade rättigheter och friheter och medges i fall som är tillåtna enligt lag, eller behandlingen, om den ännu inte är tillåten enligt lag, är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan person, eller behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade. Lämpliga skyddsåtgärder för den registrerades rättigheter och friheter kan till exempel inbegripa möjligheten att samla in dessa uppgifter endast i samband med andra uppgifter om den berörda fysiska personen, möjligheten att säkra de insamlande uppgifterna, striktare regler om tillgång till uppgifterna för den behöriga myndighetens personal på lämpligt sätt, och förbud mot att översända sådana uppgifter. Behandling av sådana uppgifter bör även tillåtas enligt lag när den registrerade uttryckligen har gett sitt samtycke i fall där uppgiftsbehandlingen är särskilt inkräktande för honom eller henne. Den registrerades samtycke bör dock inte i sig utgöra någon rättslig grund för behöriga myndigheters behandling av sådana känsliga personuppgifter.

(38) Den registrerade bör ha rätt att inte bli föremål för ett beslut angående bedömning av personliga aspekter rörande honom eller henne som uteslutande grundas på automatiserad behandling och som har negativa rättsliga följder eller i betydande grad påverkar honom eller henne. Denna form av uppgiftsbehandling bör under alla omständigheter omfattas av lämpliga skyddsåtgärder, inbegripet skild information till den registrerade och rätt till personlig kontakt, särskilt för framförande av egna synpunkter, rätten att erhålla en förklaring för det beslut som fattats efter sådan bedömning och rätten att överklaga beslutet. Profilering som leder till diskriminering av fysiska personer på grundval av personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheter och friheter är förbjuden på de villkor som fastställs i artiklarna 21 och 52 i stadgan.

(39) För att den registrerade ska kunna utöva sina rättigheter bör all information till denne vara lättåtkomlig, t.ex. via den personuppgiftsansvariges webbplats, och lättbegriplig, på ett klart och tydligt språk. Denna information bör anpassas till de behov som sårbara människor, t.ex. barn, har.

(40) Det bör finnas arrangemang som underlättar för registrerade att utöva sina rättigheter enligt de bestämmelser som antas i enlighet med detta direktiv, bl.a. rutiner för att kostnadsfritt begära och i tillämpliga fall få, särskilt, kostnadsfri tillgång till och rättelse eller radering av personuppgifter och begränsning av behandlingen. Personuppgiftsansvariga bör vara skyldiga att besvara en begäran från den registrerade utan onödigt dröjsmål, om inte de personuppgiftsansvariga tillämpar begränsningar av den registrerades rättigheter i enlighet med detta direktiv. Om en begäran är uppenbart ogrundad eller orimlig, som i fall då en registrerad utan skäl och vid upprepade tillfällen begär uppgifter eller om denne missbrukar sin rätt till information genom att exempelvis i sin begäran tillhandahålla felaktig eller missvisande information, bör den personuppgiftsansvarige dessutom kunna ta ut en rimlig avgift eller vägra att tillmötesgå begäran.

(41) När den personuppgiftsansvarige begär att ytterligare information som är nödvändig för att bekräfta den registrerades identitet ska tillhandahållas bör denna information endast behandlas för detta specifika ändamål och bör inte lagras längre än vad som krävs för detta ändamål.

(42) Åtminstone följande information bör göras tillgänglig för den registrerade: Vem som är personuppgiftsansvarig, att behandling sker, syftena med behandlingen, rätten att lämna in klagomål och rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandlingen. Informationen kan anges på den behöriga myndighetens webbplats. Dessutom bör den registrerade, i specifika fall och för att göra det möjligt för honom eller henne att utöva sina rättigheter, informeras om behandlingens rättsliga grund och om hur länge uppgifterna kommer att lagras, i den utsträckning som den ytterligare informationen är nödvändig, med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas, för att garantera en korrekt behandling när det gäller den registrerade.

(43) Fysiska personer bör ha rätt att få tillgång till uppgifter som insamlats som rör dem samt att på enkelt sätt och med rimliga intervall kunna utöva denna rätt för att hålla sig underrättade om att behandling sker och kunna kontrollera att den är laglig. Därför bör varje registrerad ha rätt att känna till och underrättas om de ändamål för vilka uppgifterna behandlas, hur länge behandlingen kommer att pågå och vilka som kommer att få del av uppgifterna, inbegripet mottagare i tredjeländer. Om denna underrättelse omfattar information om personuppgifternas ursprung bör denna information inte avslöja fysiska personers identitet, framför allt konfidentiella källor. För att denna rättighet ska respekteras är det tillräckligt att den registrerade innehar en komplett sammanfattning av dessa uppgifter i begripligt format, det vill säga ett format som gör det möjligt för den registrerade att få kännedom om dessa uppgifter och kontrollera att de är korrekta och behandlade i enlighet med detta direktiv så

att den sökande kan utöva de rättigheter som han eller hon tilldelas enligt detta direktiv. En sådan sammanfattning skulle kunna tillhandahållas i form av en kopia av de personuppgifter som håller på att behandlas.

(44) Medlemsstaterna bör ha möjlighet att genom lagstiftning vidta åtgärder som innebär att informationen till de registrerade senareläggs, begränsas eller utelämnas eller att deras tillgång till sina personuppgifter helt eller delvis begränsas, i den utsträckning och så länge som en sådan åtgärd utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, och syftet är att undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden, undvika menlig inverkan på förebyggande, förhindrande, utredning, upptäckt eller lagföring av brott eller verkställighet av straffrättsliga påföljder, skydd för allmän eller nationell säkerhet eller skydd för andra personers rättigheter och friheter. Den personuppgiftsansvarige bör genom en konkret och individuell granskning i varje enskilt fall bedöma om rätten till tillgång delvis eller helt bör begränsas.

(45) En vägran eller begränsning av tillgång bör i princip meddelas den registrerade skriftligen och inkludera de faktiska eller rättsliga skäl som beslutet grundar sig på.

(46) All begränsning av den registrerades rättigheter måste vara förenlig med stadgan och med Europakonventionen, tolkade enligt rättspraxis från domstolen respektive Europeiska domstolen för de mänskliga rättigheterna, och i synnerhet respektera kärnan i dessa rättigheter och friheter.

(47) Fysiska personer bör ha rätt att få felaktiga personuppgifter som rör dem rättade, särskilt faktauppgifter, samt rätt att få dem raderade om behandlingen av uppgifterna utgör en överträdelse av detta direktiv. Rätten till rättelse bör emellertid inte påverka exempelvis innehållet i ett vittnesmål. En fysisk person bör också ha rätt till begränsning av behandlingen när han eller hon bestrider korrektheten av en personuppgift och det inte kan fastställas huruvida denna är korrekt eller när personuppgiften måste sparas som bevisning. Framför allt bör behandlingen av personuppgifter begränsas snarare än att uppgifterna raderas om det i ett visst fall finns rimliga skäl att anta att en radering skulle kunna påverka den registrerades legitima intressen. I ett sådant fall bör begränsade uppgifter endast behandlas för det ändamål som hindrade att de raderades. Behandling av personuppgifter kan exempelvis begränsas genom att man flyttar de valda uppgifterna till ett annat databehandlingssystem, till exempel för arkivering, eller gör de valda uppgifterna otillgängliga. I automatiserade register bör begränsningen av behandlingen i princip ske med tekniska medel. Att behandlingen av personuppgifter är begränsad bör anges inom systemet på sådant sätt att det tydligt framgår att behandlingen av personuppgifterna är begränsad. Sådan rättelse, radering av personuppgifter eller begränsning av behandlingen bör meddelas till de mottagare till vilka uppgifterna har lämnats ut och till de behöriga myndigheter från vilka de oriktiga uppgifterna härrörde. De personuppgiftsansvariga bör också avstå från vidare spridning av sådana uppgifter.

(48) Om en personuppgiftsansvarig nekar en registrerad dennes rätt till information, tillgång till, rättelse, eller radering av personuppgifter eller till begränsning av behandlingen bör den registrerade ha rätt att begära att den nationella tillsynsmyndigheten kontrollerar behandlingens laglighet. De registrerade bör informeras om denna rättighet. När en tillsynsmyndighet agerar för de registrerades räkning, bör tillsynsmyndigheten åtminstone informera dem om att tillsynsmyndigheten har utfört alla nödvändiga kontroller eller översyner. Tillsynsmyndigheten bör också informera de registrerade om rätten att begära rättslig prövning.

(49) När personuppgifter behandlas inom ramen för en brottsutredning eller domstolsförfaranden vid brottmål, bör medlemsstaterna kunna föreskriva att rätten till information, tillgång, rättelse och radering samt till begränsning av behandlingen utövas i enlighet med nationella bestämmelser om rättsliga förfaranden.

(50) Den personuppgiftsansvarige bör åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar. Personuppgiftsansvariga bör särskilt vara skyldiga att vidta lämpliga och effektiva åtgärder och bör kunna visa att behandlingen är förenlig med detta direktiv. I samband med dessa åtgärder bör behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter beaktas. De åtgärder som den personuppgiftsansvarige vidtar bör omfatta utarbetande och genomförande av särskilda skyddsåtgärder för behandling av personuppgifter om sårbara fysiska personer, t.ex. barn.

(51) Risker för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av uppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller identitetsbedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller uppgifter som omfattas av tystnadsplikt, obehörigt hävande av

pseudonymisering, eller annan betydande ekonomisk eller social nackdel; eller om registrerade kan komma att berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter; om personuppgifter behandlas som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i fackförening, om genetiska uppgifter eller biometriska uppgifter behandlas för att unikt identifiera en person eller om uppgifter om hälsa eller uppgifter om sexualliv och sexuell läggning eller fällande domar i brottmål samt brott eller därmed sammanhängande säkerhetsåtgärder behandlas; om det förekommer en bedömning av personliga aspekter, exempelvis analyser och förutsägelser beträffande sådant som rör arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlitlighet eller beteende, vistelseort eller förflyttningar, i syfte att skapa eller använda personliga profiler; eller om personuppgifter rörande sårbara fysiska personer, framför allt barn, behandlas; eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

(52) Riskens sannolikhetsgrad och allvar bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas enligt en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen medför hög risk. Med hög risk avses en särskild risk för menlig inverkan på registrerades rättigheter och friheter.

(53) Skyddet för fysiska personers rättigheter och friheter i samband med behandlingen av personuppgifter kräver lämpliga tekniska och organisatoriska åtgärder för att säkerställa att kraven i detta direktiv uppfylls. Genomförandet av sådana åtgärder bör inte enbart bero på ekonomiska hänsyn. För att kunna visa överensstämmelse med detta direktiv bör den personuppgiftsansvarige anta interna strategier och vidta åtgärder, som i synnerhet följer principerna om inbyggt dataskydd och dataskydd som standard. Om den personuppgiftsansvarige har genomfört en konsekvensbedömning avseende dataskydd i enlighet med detta direktiv bör resultatet beaktas vid utarbetandet av dessa åtgärder och förfaranden. Sådana åtgärder kan bland annat bestå av pseudonymisering snarast möjligt. Pseudonymisering vid tillämpning av detta direktiv kan utgöra ett verktyg som kan underlätta det fria flödet av personuppgifter inom området med frihet, säkerhet och rättvisa.

(54) Skyddet för de registrerades rättigheter och friheter samt de personuppgiftsansvarigas och registerförarnas ansvar, också i förhållande till tillsynsmyndigheternas övervakning och åtgärder, kräver ett tydligt fastställande av vem som bär ansvaret enligt detta direktiv, bl.a. när personuppgiftsansvariga gemensamt fastställer ändamål och medel för en behandling tillsammans med andra personuppgiftsansvariga eller när en behandling utförs på en personuppgiftsansvarigs vägnar.

(55) Ett personuppgiftsbiträdes behandling bör styras av en rättsakt som omfattar ett avtal som binder personuppgiftsbiträdet till den personuppgiftsansvarige och där det särskilt anges att personuppgiftsbiträdet endast bör agera på instruktion av den personuppgiftsansvarige. Personuppgiftsbiträdet bör beakta principen om inbyggt dataskydd och dataskydd som standard.

(56) För att visa överensstämmelse med detta direktiv bör de personuppgiftsansvariga eller registerförarna föra register över alla kategorier av behandling som sker under deras ansvar. Alla personuppgiftsansvariga och personuppgiftsbiträden bör vara skyldiga att samarbeta med tillsynsmyndigheten och på dennas begäran göra detta register tillgängligt för myndigheten så att det kan tjäna som grund för övervakningen av behandlingen. Personuppgiftsansvariga eller personuppgiftsbiträden som behandlar personuppgifter i icke-automatiserade behandlingssystem bör ha infört effektiva metoder, t.ex. loggar eller andra typer av register, för att visa att behandlingen är laglig, möjliggöra egenkontroll och säkerställa dataintegritet och datasäkerhet.

(57) Loggar bör åtminstone föras över behandlingar i automatiserade behandlingssystem såsom insamling, ändring, läsning, utlämning, inklusive överföringar, sammanförande eller radering. Identifieringen av den person som läst eller lämnat ut personuppgifter bör loggas och från denna identifiering skulle det kunna vara möjligt att fastställa motiveringen till behandlingen. Loggarna bör endast användas för att kontrollera om behandlingen av uppgifterna är tillåten, för egenkontroll, för att garantera dataintegritet och datasäkerhet samt för straffrättsliga förfaranden. Egenkontroll omfattar även behöriga myndigheters interna disciplinära förfaranden.

(58) En konsekvensbedömning avseende dataskydd bör genomföras av den personuppgiftsansvarige om det är sannolikt att uppgiftsbehandlingen, på grund av sin karaktär, sin omfattning eller sina ändamål, medför en hög risk för de registrerades rättigheter och friheter, vilken i synnerhet bör omfatta planerade åtgärder, skyddsåtgärder och mekanismer för att säkerställa skyddet av personuppgifter och för att styrka efterlevnaden av detta direktiv. Konsekvensbedömningarna bör omfatta relevanta system och processer för behandling men inte enskilda fall.

(59) I syfte att säkerställa ett effektivt skydd av de registrerades rättigheter och friheter bör den personuppgiftsansvarige eller personuppgiftsbiträdet i vissa fall samråda med tillsynsmyndigheten före behandlingen.

(60) För att upprätthålla säkerheten och förhindra behandling som bryter mot detta direktiv bör personuppgiftsansvariga eller personuppgiftsbiträden utvärdera de risker som behandlingen är förknippad med och bör vidta åtgärder, såsom kryptering, för att mildra dem. Åtgärderna bör leda till en lämplig säkerhetsnivå, inklusive konfidentialitetsnivå, med beaktande av den senaste utvecklingen och till genomförandekostnaderna med hänsyn till riskerna och vilken typ av personuppgifter som ska skyddas. Vid bedömningen av riskerna när det gäller datasäkerhet bör man beakta de risker som uppgiftsbehandling medför, såsom förstöring, förlust eller ändringar genom olyckshändelse eller olagliga handlingar eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, som framför allt kan leda till fysisk, materiell eller immateriell skada. Den personuppgiftsansvarige och personuppgiftsbiträdet bör säkerställa att behandlingen av personuppgifter inte utförs av obehöriga personer.

(61) En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan för fysiska personer leda till fysisk, materiell eller immateriell skada, såsom förlust av kontrollen över de egna personuppgifterna eller till begränsning av deras rättigheter, diskriminering, identitetsstöld eller identitetsbedrägeri, ekonomisk förlust, obehörigt hävande av pseudonymisering, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, eller till annan betydande ekonomisk eller social nackdel för den berörda fysiska personen. Så snart en personuppgiftsansvarig blir medveten om en personuppgiftsincident bör den personuppgiftsansvarige därför anmäla personuppgiftsincidenten till tillsynsmyndigheten utan onödigt dröjsmål och, om möjligt, inom 72 timmar efter att ha fått kännedom om denna, om inte den personuppgiftsansvarige, i enlighet med ansvarsprincipen, kan visa att det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter. Om anmälan inte kan göras inom 72 timmar bör skälen till fördröjningen åtfölja anmälan och informationen får lämnas i omgångar utan otillbörligt vidare dröjsmål.

(62) Fysiska personer bör utan onödigt dröjsmål underrättas om personuppgiftsincidenten sannolikt leder till en högre risk för deras rättigheter och friheter så att de kan vidta nödvändiga försiktighetsåtgärder. Underrättelsen bör innehålla en beskrivning av personuppgiftsincidentens art samt rekommendationer till den berörda fysiska personen om hur de potentiella negativa effekterna kan mildras. De registrerade bör underrättas så snart detta rimligtvis är möjligt, i nära samarbete med tillsynsmyndigheten och i enlighet med den vägledning som lämnats av den eller andra relevanta myndigheter. Exempelvis kräver behovet av att mildra en omedelbar skaderisk att de registrerade underrättas omgående medan behovet att vidta lämpliga åtgärder vid fortlöpande eller likartade uppgiftsincidenter kan motivera längre tid för underrättelsen. Om man inte kan undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden, undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder eller skydda allmän säkerhet, nationell säkerhet eller andra personers rättigheter och friheter genom att senarelägga eller begränsa informationen till den berörda fysiska personen om en personuppgiftsincident skulle denna information under exceptionella omständigheter kunna utelämnas.

(63) Den personuppgiftsansvarige bör utse en person att hjälpa denne att övervaka den interna efterlevnaden av de bestämmelser som antas i enlighet med detta direktiv, förutom om en medlemsstat beslutar att undanta domstolar och andra oberoende rättsliga myndigheter som behandlar personuppgifter inom ramen för sin dömande verksamhet. Denna person kan vara en av den personuppgiftsansvariges medarbetare som fått särskild utbildning inom dataskyddslagstiftning och praxis i fråga om dataskydd för att förvärva sakkunskap på detta område. Den nödvändiga nivån på sakkunskapen bör särskilt fastställas i enlighet med den uppgiftsbehandling som utförs och det skydd som krävs för de personuppgifter som behandlas av den personuppgiftsansvarige. Hans eller hennes uppgift kan utföras på deltid eller heltid. Flera personuppgiftsansvariga kan, med beaktande av organisationsstruktur och storlek, gemensamt utse ett dataskyddsombud, t.ex. vid gemensamma resurser i centralenheter. Denna person kan också utnämnas till olika befattningar inom de berörda personuppgiftsansvarigas struktur. Denna person bör hjälpa den personuppgiftsansvarige och de anställda som behandlar personuppgifter genom att ge information och råd till dem angående efterlevnaden av deras respektive skyldigheter i fråga om dataskydd. Dataskyddsombudet i fråga bör kunna utföra sina uppdrag och uppgifter på ett oberoende sätt i enlighet med medlemsstaternas nationella rätt.

(64) Medlemsstaterna bör säkerställa att överföringar till ett tredjeland eller en internationell organisation endast får äga rum om detta är nödvändigt för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller för att verkställa straffrättsliga påföljder, inklusive för att skydda mot samt förebygga och förhindra hot mot den

allmänna säkerheten, och den personuppgiftsansvarige i tredjelandet eller den internationella organisationen är en myndighet som är behörig i den mening som avses i detta direktiv. En överföring bör endast utföras av behöriga myndigheter som agerar som personuppgiftsansvariga, utom när personuppgiftsbiträden uttryckligen har getts i uppdrag att göra en överföring för personuppgiftsansvarigas räkning. En sådan överföring kan äga rum när kommissionen har beslutat att skyddsnivån i ett tredjeland eller en internationell organisation är adekvat eller när lämpliga skyddsåtgärder föreligger, eller när undantag för särskilda situationer gäller. Det är viktigt att den skyddsnivå som fysiska personer garanteras inom unionen genom detta direktiv inte undergrävs när personuppgifter överförs från unionen till personuppgiftsansvariga, personuppgiftsbiträden eller andra mottagare i tredjeländer eller internationella organisationer, vilket inbegriper fall av vidare överföring av personuppgifter från tredjelandet eller den internationella organisationen till personuppgiftsansvariga eller personuppgiftsbiträden i samma eller i ett annat tredjeland eller en annan internationell organisation.

(65) Om personuppgifter överförs från en medlemsstat till tredjeländer eller internationella organisationer bör en sådan överföring i princip ske först efter det att den medlemsstat från vilken uppgifterna insamlades har gett sitt tillstånd till överföringen. För ett effektivt samarbete i fråga om brottsbekämpning krävs att, om ett hot mot en medlemsstats eller ett tredjelands allmänna säkerhet eller en medlemsstats väsentliga intressen är så överhängande att det är omöjligt att i tid inhämta ett förhandstillstånd, den behöriga myndigheten bör få överföra de relevanta personuppgifterna till det berörda tredjelandet eller internationella organisationen utan sådant förhandstillstånd. Medlemsstaterna bör föreskriva att eventuella särskilda villkor som rör överföringen bör vidarebefordras till tredjeländer eller internationella organisationer. För vidare överföring av personuppgifter bör det krävas förhandstillstånd från den behöriga myndighet som utförde den ursprungliga överföringen. När den behöriga myndighet som utförde den ursprungliga överföringen fattar beslut om en begäran om tillstånd för vidare överföring bör den vederbörligen beakta alla relevanta faktorer, inklusive hur allvarligt brottet är, de särskilda villkor på vilka, och det ändamål för vilket, uppgifterna ursprungligen överfördes, arten och villkoren för verkställandet av den straffrättsliga påföljden, samt nivån på skyddet av personuppgifter i det tredjeland eller den internationella organisation som personuppgifterna vidare överförs till. Den behöriga myndighet som utförde den ursprungliga överföringen bör också ha möjlighet att tillämpa särskilda villkor för vidare överföring. Dessa särskilda villkor kan beskrivas, t.ex. i hanteringskoder.

(66) Kommissionen bör med verkan för hela unionen kunna fastställa att vissa tredjeländer, ett visst territorium eller en eller flera specificerade sektorer i ett tredjeland eller en internationell organisation kan erbjuda en adekvat dataskyddsnivå, och på så sätt skapa rättssäkerhet och enhetlighet i hela unionen vad gäller dessa tredjeländer eller internationella organisationer som anses erbjuda en sådan skyddsnivå. I dessa fall bör överföringar av personuppgifter till dessa länder kunna ske utan särskilt tillstånd, utom när en annan medlemsstat från vilken uppgifterna insamlades måste ge tillstånd till överföringen.

(67) I enlighet med de grundläggande värderingar som unionen vilar på, särskilt skyddet av de mänskliga rättigheterna, bör kommissionen i sin bedömning av ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland beakta i vilken omfattning ett visst tredjeland iakttar rättsstatsprincipen, möjligheten till rättslig prövning samt internationella människorättsliga normer och standarder samt landets allmänna lagstiftning och sektorslagstiftning, vilket inbegriper lagstiftning om allmän säkerhet, försvar och nationell säkerhet samt allmän ordning och straffrätt. Vid antagandet av ett beslut om adekvat skyddsnivå avseende ett territorium eller en specificerad sektor i ett tredjeland bör hänsyn tas till tydliga och objektiva kriterier, t.ex. specifik behandling och tillämpningsområdet för tillämpliga rättsliga standarder och gällande lagstiftning i det tredjelandet. Tredjelandet bör erbjuda garantier som säkerställer en tillfredsställande skyddsnivå, som i huvudsak motsvarar den som säkerställs inom unionen, i synnerhet när uppgifter behandlas inom en eller flera specifika sektorer. Tredjelandet bör framför allt säkerställa en effektiv oberoende dataskyddsövervakning samt sörja för mekanismer för samarbete med medlemsstaternas dataskyddsmyndigheter och de registrerade bör tillförsäkras effektiva och verkställbara rättigheter samt effektiva administrativa och rättsliga rättsmedel.

(68) Utöver de internationella åtaganden som tredjelandet eller den internationella organisationen har ingått bör kommissionen också beakta de skyldigheter som följer av tredjelandets eller den internationella organisationens deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter, samt genomförandet av dessa skyldigheter. Framför allt bör tredjelandets anslutning till Europarådets konvention av den 28 januari 1981 om skydd för fysiska personer vid automatiserad databehandling av personuppgifter och dess tilläggsprotokoll beaktas. Kommissionen bör samråda med Europeiska dataskyddsstyrelsen, inrättad genom förordning

(EU) 2016/679 (nedan kallad *styrelsen*) vid bedömningen av skyddsnivån i tredjeländer eller internationella organisationer. Kommissionen bör också beakta alla relevanta kommissionsbeslut om adekvat skyddsnivå som antagits i enlighet med artikel 45 i förordning (EU) 2016/679.

(69) Kommissionen bör övervaka hur beslut om skyddsnivå i ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation fungerar. I sina beslut om adekvat skyddsnivå bör kommissionen föreskriva en mekanism för periodisk översyn av hur de fungerar. Denna periodiska översyn bör göras i samråd med tredjelandet eller den internationella organisationen i fråga och bör beakta all relevant utveckling i tredjelandet eller den internationella organisationen.

(70) Kommissionen bör även kunna konstatera att ett tredjeland eller ett territorium eller en specificerad sektor inom ett tredjeland, eller en internationell organisation, inte längre säkerställer en adekvat dataskyddsnivå. Följaktligen bör överföringar av personuppgifter till det tredjelandet eller den internationella organisationen förbjudas om inte kraven i detta direktiv rörande överföring som är föremål för lämpliga skyddsåtgärder och undantag i särskilda situationer är uppfyllda. Bestämmelser bör fastställas för förfaranden för samråd mellan kommissionen och dessa tredjeländer eller internationella organisationer. Kommissionen bör i god tid informera tredjelandet eller den internationella organisationen om skälen och inleda samråd med tredjelandet eller organisationen för att avhjälpa situationen.

(71) Överföringar som inte grundar sig på ett sådant beslut om adekvat skyddsnivå bör endast tillåtas om lämpliga skyddsåtgärder garanteras i ett rättsligt bindande instrument, som säkerställer skyddet av personuppgifterna eller om den personuppgiftsansvarige har gjort en bedömning av alla omständigheter kring en uppgiftsöverföring och på grundval av denna bedömning anser att lämpliga skyddsåtgärder föreligger vad avser skyddet av personuppgifter. Sådana rättsligt bindande instrument kan t.ex. vara rättsligt bindande bilaterala avtal som har ingåtts av medlemsstaterna och genomförts inom deras rättsordning och som kan åberopas av registrerade som omfattas av denna och som sörjer för att kraven i fråga om dataskydd uppfylls och att registrerades rättigheter respekteras, inbegripet rätten till en effektiv administrativ eller rättslig prövning. Den personuppgiftsansvarige bör vid bedömningen av alla omständigheter kring uppgiftsöverföringen kunna beakta samarbetsavtal som ingåtts mellan Europol eller Eurojust och tredjeländer, som medger utbyte av personuppgifter. Den personuppgiftsansvarige bör också kunna beakta att överföringen av personuppgifter kommer att omfattas av tystnadplikt och principen om specificitet, vilket säkerställer att personuppgifterna inte kommer att behandlas i andra syften än för överföringen. Dessutom bör den personuppgiftsansvarige beakta att personuppgifterna inte kommer att användas för att göra framställningar om, meddela eller verkställa dödsstraff eller någon form av grym och omänsklig behandling. Även om dessa villkor kan betraktas som tillräckliga skyddsåtgärder för överföringen av uppgifter bör den personuppgiftsansvarige kunna begära ytterligare skyddsåtgärder.

(72) Om det inte finns något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder saknas kan en överföring eller en kategori av överföringar endast äga rum i särskilda situationer om överföringen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan person, eller för att skydda den registrerades berättigade intressen om lagstiftningen i den medlemsstat som överför personuppgifterna föreskriver detta, eller för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en medlemsstat eller i ett tredjeland, eller om det är nödvändigt i ett enskilt fall för att förebygga, förhindra, avslöja, utreda eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive för att skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten, eller i ett enskilt fall för att fastslå, göra gällande eller försvara rättsliga anspråk. Dessa undantag bör tolkas restriktivt och bör inte möjliggöra upprepade, omfattande eller strukturella överföringar av personuppgifter eller storskaliga överföringar av uppgifter, utan begränsas till uppgifter som är absolut nödvändiga. Sådana överföringar bör dokumenteras och på begäran göras tillgängliga för tillsynsmyndigheten så att man kan övervaka om överföringen är laglig.

(73) Medlemsstaternas behöriga myndigheter tillämpar gällande bilaterala eller multilaterala internationella avtal som ingåtts med tredjeländer på området för straffrättsligt samarbete och polissamarbete för utbyte av relevant information för att de ska kunna fullgöra de uppgifter som de anförtrotts enligt lag. Detta sker i princip genom eller åtminstone i samarbete med tredjeländernas berörda myndigheter, i vissa fall även i avsaknad av ett bilateralt eller multilateralt internationellt avtal. I specifika enskilda fall är emellertid de ordinarie förfaranden som kräver kontakt med myndigheten i tredjelandet ineffektiva eller olämpliga, framför allt för att överföringen inte skulle kunna utföras i tid eller för att myndigheten i tredjelandet inte respekterar rättsstatsprincipen eller internationella människorättsliga normer och standarder, så att medlemsstaternas behöriga myndigheter skulle kunna besluta att överföra personuppgifterna direkt till de mottagare som är etablerade i dessa tredjeländer. Detta kan till exempel vara fallet om det finns ett akut behov av att överföra personuppgifter för att rädda livet på en person som riskerar att utsättas för ett brott eller för att förhindra en överhängande fara för brottslighet, inbegripet terrorism. Även om denna överföring mellan behöriga myndigheter och mottagare som är etablerade i tredjeländer endast

äger rum i särskilda enskilda fall bör det i detta direktiv föreskrivas villkor för att reglera sådana fall. Dessa bestämmelser bör inte betraktas som undantag från något befintligt bilateralt eller multilateralt internationellt avtal på området för straffrättsligt samarbete och polissamarbete. Dessa bestämmelser bör vara tillämpliga utöver övriga bestämmelser i detta direktiv, särskilt bestämmelserna om när personuppgifter får behandlas och bestämmelserna i kapitel V.

(74) När personuppgifter förs över gränserna kan detta öka risken för att fysiska personer inte ska kunna utöva sina dataskyddsrättigheter för att skydda sig mot olaglig användning eller olagligt utlämnande av dessa uppgifter. Samtidigt kan tillsynsmyndigheter finna att de inte är i stånd att handlägga klagomål eller genomföra utredningar avseende verksamheter utanför sina egna gränser. Deras strävan att samarbeta i ett gränsöverskridande sammanhang kan också försvåras på grund av otillräckliga preventiva eller korrigerande befogenheter och oenhetliga rättsliga regelverk. Närmare samarbete mellan tillsynsmyndigheter bör därför främjas för att hjälpa dem att utbyta information med sina utländska motparter.

(75) För att skydda fysiska personer med avseende på behandling av personuppgifter är det av avgörande betydelse att medlemsstaterna inrättar tillsynsmyndigheter som kan utföra sitt uppdrag fullständigt oberoende. Tillsynsmyndigheterna bör övervaka tillämpningen av detta direktiv och bör bidra till enhetlig tillämpning av dessa i hela unionen, för att skydda fysiska personer när deras personuppgifter behandlas. För detta ändamål bör tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen.

(76) Medlemsstaterna får anförtro en tillsynsmyndighet som de redan har inrättat i enlighet med förordning (EU) 2016/679 ansvaret för de uppgifter som ska utföras av de nationella tillsynsmyndigheter som ska inrättas i enlighet med detta direktiv.

(77) Medlemsstaterna bör kunna inrätta mer än en tillsynsmyndighet för att återspegla sin konstitutionella, organisatoriska och administrativa struktur. Varje tillsynsmyndighet bör tilldelas de ekonomiska och personella resurser och lokalutrymmen samt den infrastruktur som krävs för att den effektivt ska kunna utföra sina uppgifter, däribland de uppgifter som är knutna till ömsesidigt bistånd och samarbete med övriga tillsynsmyndigheter i hela unionen. Varje tillsynsmyndighet bör ha en separat offentlig årlig budget, som kan ingå i den övergripande statsbudgeten eller nationella budgeten.

(78) Tillsynsmyndigheterna bör vara föremål för oberoende kontroll- eller övervakningsmekanismer i fråga om sina utgifter, förutsatt att denna finansiella kontroll inte påverkar deras oberoende.

(79) De allmänna villkoren för tillsynsmyndighetens ledamot eller ledamöter bör fastställas i medlemsstaternas nationella rätt och bör i synnerhet föreskriva att de ska utnämnas antingen av den berörda medlemsstatens parlament eller dess regering eller dess statschef på grundval av ett förslag från regeringen eller en minister eller parlamentet eller dess kammare eller av ett oberoende organ som enligt medlemsstaternas nationella rätt har anförtrotts utnämningen genom ett öppet förfarande. I syfte att säkerställa tillsynsmyndighetens oberoende bör ledamoten eller ledamöterna handla med integritet, bör avstå från alla handlingar som står i strid med deras tjänsteutövning och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet som står i strid med deras uppdrag. För att säkerställa tillsynsmyndighetens oberoende bör personalurvalet göras av tillsynsmyndigheten, och kunna innefatta ett ingripande från ett oberoende organ som enligt medlemsstaternas nationella rätt har anförtrotts uppgiften.

(80) Detta direktiv är visserligen tillämpligt på nationella domstolars och andra rättsliga myndigheters verksamheter, men tillsynsmyndigheterna bör inte ha behörighet att övervaka behandling av personuppgifter inom ramen för domstolars dömande verksamhet. Syftet är att garantera domarnas oberoende när de utför sina rättsliga uppgifter. Detta undantag bör vara inskränkt till rättsliga verksamheter i domstolsmål och inte vara tillämpligt på övriga verksamheter där domare i enlighet med medlemsstaternas nationella rätt kan medverka. Medlemsstaterna bör också kunna föreskriva att tillsynsmyndigheten inte ska vara behörig att övervaka andra oberoende rättsliga myndigheter som behandlar personuppgifter inom ramen för sin rättsliga verksamhet, exempelvis allmänna åklagarmyndigheter. Under alla omständigheter är domstolarnas och andra oberoende rättsliga myndigheters efterlevnad av bestämmelserna i detta direktiv alltid föremål för en oberoende kontroll i enlighet med artikel 8.3 i stadgan.

(81) Tillsynsmyndigheterna bör hantera klagomål som anförs av registrerade och utreda ärendena i fråga eller överföra dem till den behöriga övervakande myndigheten. Utredningen av ett klagomål bör, med förbehåll för eventuell domstolsprövning, ske i den utsträckning som är lämplig i det enskilda fallet. Tillsynsmyndigheten bör i rimlig tid informera den registrerade om hur arbetet med klagomålet fortskrider och vad resultatet blir. Om ärendet kräver ytterligare utredning eller samordning med en annan tillsynsmyndighet bör den registrerade underrättas även om detta.

(82) För att man ska kunna övervaka efterlevnaden av och verkställa detta direktiv på ett effektivt, tillförlitligt och enhetligt sätt i hela unionen enligt EUF-fördraget, i enlighet med den tolkning som domstolen gjort, bör tillsynsmyndigheterna i alla medlemsstater ha samma uppgifter och effektiva befogenheter, bl.a. undersökningsbefogenheter, korrigerande befogenheter och rådgivande befogenheter, som utgör nödvändiga medel för utförandet av deras uppgifter. Emellertid bör deras befogenheter inte inkräkta på särskilda regler för straffrättsliga förfaranden, inbegripet utredning och lagföring av brott, eller domstolsväsendets oberoende. Utan att det påverkar åklagarmyndigheternas befogenheter enligt medlemsstaternas nationella rätt bör tillsynsmyndigheterna också ha befogenhet att upplysa de rättsliga myndigheterna om överträdelser av detta direktiv eller delta i rättsliga förfaranden. Tillsynsmyndigheternas befogenheter bör utövas i överensstämmelse med lämpliga rättssäkerhetsgarantier som fastställs i unionsrätten och i medlemsstaternas nationella rätt samt opartiskt, korrekt och inom rimlig tid. Framför allt bör varje åtgärd vara lämplig, nödvändig och proportionell för att säkerställa efterlevnaden av detta direktiv, med beaktande av omständigheterna i varje enskilt fall, samt respektera varje persons rätt att bli hörd innan några enskilda åtgärder som påverkar den berörda personen negativt vidtas, och utformas så att onödiga kostnader och alltför stora olägenheter för denne undviks. Undersökningsbefogenheten när det gäller tillträde till lokaler bör utövas i enlighet med särskilda krav i medlemsstaternas nationella rätt, såsom kravet på att inhämta förhandstillstånd från rättsliga myndigheter. Antagande av ett rättsligt bindande beslut bör bli föremål för domstolsprövning i den medlemsstat där den tillsynsmyndighet som antog beslutet är belägen.

(83) Tillsynsmyndigheterna bör bistå varandra när de utför sina uppgifter och ge ömsesidigt bistånd för att säkerställa att de bestämmelser som antas i enlighet med detta direktiv efterlevs och tillämpas på ett enhetligt sätt.

(84) Styrelsen bör bidra till detta direktivs enhetliga tillämpning i hela unionen, bl.a. genom att lämna råd till kommissionen och främja samarbetet mellan tillsynsmyndigheterna i hela unionen.

(85) Alla registrerade bör ha rätt att lämna in ett klagomål till en enda tillsynsmyndighet och till ett effektivt rättsmedel i enlighet med artikel 47 i stadgan, om den registrerade anser att hans eller hennes rättigheter enligt de bestämmelser som antas i enlighet med detta direktiv har kränkts eller om tillsynsmyndigheten inte reagerar på ett klagomål, helt eller delvis avslår eller avvisar ett klagomål eller inte agerar när så är nödvändigt för att skydda den registrerades rättigheter. Utredningen av ett klagomål bör, med förbehåll för eventuell domstolsprövning, ske i den utsträckning som är lämplig i det enskilda fallet. Den behöriga tillsynsmyndigheten bör i rimlig tid informera den registrerade om hur arbetet med klagomålet fortskrider och vad resultatet blir. Om ärendet kräver ytterligare utredning eller samordning med en annan tillsynsmyndighet bör den registrerade underrättas även om detta. För att förenkla inlämnandet av klagomål bör varje tillsynsmyndighet vidta åtgärder, såsom att tillhandahålla ett formulär för inlämnande av klagomål som även kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.

(86) Varje fysisk eller juridisk person bör ha rätt till ett effektivt rättsmedel vid behörig nationell domstol mot en tillsynsmyndighets beslut som har rättsliga följder för denna person. Ett sådant beslut avser särskilt tillsynsmyndighetens utövande av utrednings-, korrigerings- och godkännandebefogenheter eller avvisande av eller avslag på klagomål. Denna rätt inbegriper dock inte tillsynsmyndigheters övriga åtgärder som inte är rättsligt bindande, såsom yttranden som avgetts eller rådgivning som tillhandahållits av tillsynsmyndigheten. Talan mot en tillsynsmyndighet bör väckas vid domstol i den medlemsstat där tillsynsmyndigheten är etablerad och bör prövas i enlighet med den nationella rätten i den medlemsstaten. Dessa domstolar bör ha fullständig behörighet, vilket bör omfatta behörighet att rättsligt eller faktiskt pröva alla frågor som rör de tvister som anhängiggjorts vid dem.

(87) Om en registrerad anser att hans eller hennes rättigheter enligt detta direktiv har kränkts bör han eller hon ha rätt att ge ett organ som syftar till att skydda registrerades rättigheter och intressen vad gäller skyddet av deras

personuppgifter, och som inrättats i enlighet med den nationella rätten i en medlemsstat, i uppdrag att på hans eller hennes vägnar lämna in ett klagomål till en tillsynsmyndighet och utöva rätten till rättsmedel. De registrerades rätt att bli företrädda bör inte påverka medlemsstatens nationella processrätt enligt vilken det kan vara obligatoriskt att registrerade företräds inför nationell domstol av en advokat enligt definitionen i rådets direktiv 77/249/EEG ( ).

(88) Personer som lider skada till följd av behandling som står i strid med de bestämmelser som antas i enlighet med detta direktiv bör få ersättning av den personuppgiftsansvarige eller av någon annan myndighet som är behörig enligt medlemsstaternas nationella rätt. Begreppet *skada* bör tolkas brett mot bakgrund av domstolens rättspraxis och på ett sätt som fullt ut återspeglar detta direktivs mål. Detta påverkar inte skadeståndsanspråk till följd av överträdelser av andra bestämmelser i unionsrätten eller i medlemsstaternas nationella rätt. Vid hänvisning till behandling som är olaglig eller står i strid med de bestämmelser som antas i enlighet med detta direktiv omfattas även behandling som inte är i överensstämmelse med de genomförandeakter som antagits i enlighet med detta direktiv. Registrerade bör få full och effektiv ersättning för den skada de lidit.

(89) Om någon fysisk eller juridisk person överträder detta direktiv bör detta leda till sanktioner, oavsett om personen i fråga omfattas av privaträtt eller offentlig rätt. Medlemsstaterna bör säkerställa att sanktioner är effektiva, proportionella och avskräckande och bör vidta alla åtgärder som krävs för att sanktionerna ska verkställas.

(90) För att säkerställa enhetliga villkor för genomförandet av detta direktiv bör kommissionen tilldelas genomförandebefogenheter vad gäller adekvata skyddsnivåer i ett tredjeland, ett territorium eller en specificerad sektor inom ett tredjeland eller en internationell organisation och för format och förfaranden för ömsesidigt bistånd samt tillvägagångssätten för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ( ).

(91) Mot bakgrund av att dessa rättsakter har allmän räckvidd bör granskningsförfarandet användas vid antagandet av genomförandeakter om adekvata skyddsnivåer i ett tredjeland, ett territorium eller en specificerad sektor inom detta tredjeland eller en internationell organisation och om format och förfaranden för ömsesidigt bistånd samt tillvägagångssätten för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen.

(92) Kommissionen bör när tvingande skäl till skyndsamhet föreligger i vederbörligen motiverade fall anta omedelbart tillämpliga genomförandeakter avseende ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation där en adekvat skyddsnivå inte längre kan säkerställas.

(93) Eftersom målen för detta direktiv, nämligen att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, och för att säkerställa ett fritt utbyte av personuppgifter mellan behöriga myndigheter inom unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare på grund av åtgärdens omfattning eller verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i EU-fördraget. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.

(94) Särskilda bestämmelser i unionsakter på området för straffrättsligt samarbete och polissamarbete som antagits före dagen för antagandet av detta direktiv, och som reglerar behandlingen av personuppgifter mellan medlemsstaterna eller tillträdet för utsedda myndigheter i medlemsstaterna till informationssystem som inrättats i

( ) Rådets direktiv 77/249/EEG av den 22 mars 1977 om underlättande för advokater att effektivt begagna sig av friheten att tillhandahålla tjänster (EGT L 78, 26.3.1977, s. 17).

( ) Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

enlighet med fördragen, bör kvarstå oförändrade, till exempel de särskilda bestämmelser om skydd av personuppgifter som tillämpas i enlighet med rådets beslut 2008/615/RIF ( ), eller artikel 23 i konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater ( ). Eftersom artikel 8 i stadgan och artikel 16 i EUF-fördraget kräver att den grundläggande rätten till skydd av personuppgifter bör säkerställas på ett enhetligt sätt i hela unionen bör kommissionen utvärdera situationen vad gäller förhållandet mellan detta direktiv och rättsakter, antagna före dagen för antagandet av detta direktiv, som reglerar behandling av personuppgifter mellan medlemsstaterna eller tillträde för utsedda myndigheter i medlemsstater till informationssystem som inrättats i enlighet med fördragen, i syfte att bedöma om dessa särskilda bestämmelser behöver anpassas till detta direktiv. Vid behov bör kommissionen lägga fram förslag i syfte att säkerställa enhetliga rättsregler angående behandlingen av personuppgifter.

(95) För att säkerställa ett övergripande och enhetligt skydd av personuppgifter i unionen bör internationella avtal som medlemsstaterna ingått före dagen för detta direktivs ikraftträdande, och som överensstämmer med relevant unionsrätt som var tillämplig före den dagen, fortsätta att gälla till dess att de ändras, ersätts eller upphävs.

(96) Medlemsstaterna bör medges en period på högst två år från dagen för ikraftträdandet av detta direktiv för att införliva det. Behandling som redan pågår den dagen bör bringas i överensstämmelse med detta direktiv inom en period av två år från det att detta direktiv träder i kraft. I fall där sådan behandling överensstämmer med unionsrätt som var tillämplig före dagen för ikraftträdandet av detta direktiv bör dock inte kraven i detta direktiv rörande förhandssamråd med tillsynsmyndigheten gälla för behandling som redan pågick vid den tidpunkten, eftersom dessa krav, p.g.a. sin natur, är sådana att de ska uppfyllas före själva behandlingen. Om medlemsstaterna tillämpar den längre genomförandeperioden som löper ut sju år efter detta direktivs ikraftträdande för fullgörandet av loggningsskyldigheterna för automatiserade behandlingssystem som inrättats före den dagen bör den personuppgiftsansvarige eller personuppgiftsbiträdet ha infört effektiva metoder, t.ex. loggar eller andra typer av register, för att visa att behandlingen av uppgifterna är laglig, möjliggöra egenkontroll samt säkerställa dataintegritet och datasäkerhet.

(97) Detta direktiv påverkar inte bestämmelserna om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi i Europaparlamentets och rådets direktiv 2011/93/EU ( ).

(98) Rambeslut 2008/977/RIF bör därför upphävas.

(99) I enlighet med artikel 6a i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till EU-fördraget och EUF-fördraget, är Förenade kungariket och Irland inte bundna av de bestämmelser i detta direktiv som avser medlemsstaternas behandling av personuppgifter när de bedriver verksamhet som omfattas av avdelning V kapitel 4 eller 5 i tredje delen av EUF-fördraget i det fall då Förenade kungariket och Irland inte är bundna av bestämmelserna om formerna för straffrättsligt samarbete eller polissamarbete inom ramen för vilka de bestämmelser måste iakttas som fastställs på grundval av artikel 16 i EUF-fördraget.

(100) I enlighet med artiklarna 2 och 2a i protokoll nr 22 om Danmarks ställning, fogat till EU-fördraget och EUF-fördraget, är Danmark inte bundet av reglerna i detta direktiv och omfattas inte av den tillämpning av regler som avser medlemsstaternas behandling av personuppgifter när dessa utövar verksamhet som omfattas av tillämpningsområdet för kapitlen 4 och 5 i avdelning V i tredje delen i EUF-fördraget. Eftersom detta direktiv bygger på av Schengenregelverket, som omfattas av avdelning V i tredje delen av EUF-fördraget, ska Danmark i enlighet med artikel 4 i protokollet inom en tid av sex månader efter antagandet av detta direktiv besluta huruvida landet ska genomföra det i sin nationella lagstiftning.

(101) När det gäller Island och Norge utgör detta direktiv en vidareutveckling av bestämmelserna i Schengenregelverket i enlighet med avtalet mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ( ).

( ) Rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (EUT L 210, 6.8.2008, s. 1).
( ) Rådets akt av den 29 maj 2000 om att i enlighet med artikel 34 i Fördraget om Europeiska unionen upprätta konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (EGT C 197, 12.7.2000, s. 1).
( ) Europaparlamentets och rådets direktiv 2011/93/EU av den 13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om ersättande av rådets rambeslut 2004/68/RIF (EUT L 335, 17.12.2011, s. 1).
( ) EGT L 176, 10.7.1999, s. 36.

(102) När det gäller Schweiz utgör detta direktiv, i enlighet med avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket, en utveckling av bestämmelserna i Schengenregelverket ( ).

(103) När det gäller Liechtenstein utgör detta direktiv en vidareutveckling av bestämmelserna i Schengenregelverket i enlighet med protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Liechtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ( ).

(104) Detta direktiv respekterar de grundläggande rättigheterna och iakttar de principer som erkänns i stadgan som erkänns i EUF-fördraget, särskilt rätten till respekt för privatlivet och familjelivet, rätten till skydd av personuppgifter, rätt till ett effektivt rättsmedel och till en opartisk domstol. De inskränkningar som gjorts av dessa rättigheter överensstämmer med artikel 52.1 i stadgan eftersom de är nödvändiga för att uppnå av unionen erkända mål av allmänt intresse eller för att skydda andras rättigheter och friheter.

(105) I enlighet med den gemensamma politiska förklaringen av den 28 september 2011 från medlemsstaterna och kommissionen om förklarande dokument, har medlemsstaterna åtagit sig att, i de fall detta är berättigat, låta anmälan av införlivandeåtgärder åtföljas av ett eller flera dokument som förklarar förhållandet mellan de olika delarna i direktivet och motsvarande delar i de nationella införlivandeåtgärderna. Med avseende på detta direktiv anser lagstiftaren att översändandet av sådana dokument är berättigat.

(106) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001 och avgav ett yttrande den 7 mars 2012 ( ).

(107) Detta direktiv bör inte hindra medlemsstaterna från att i nationell straffprocesslagstiftning genomföra bestämmelser om registrerades utövande av sina rättigheter vad gäller information, tillgång till och rättelse eller radering av personuppgifter och begränsning av behandling i samband med straffrättsliga förfaranden samt eventuella begränsningar av dessa rättigheter.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Syfte och mål

1. I detta direktiv fastställs bestämmelser om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

2. Enligt detta direktiv ska medlemsstaterna

a) skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, och

b) säkerställa att behöriga myndigheters utbyte av personuppgifter inom unionen, när sådant utbyte krävs enligt unionsrätten eller medlemsstaternas nationella rätt, varken begränsas eller förbjuds av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter.

( ) EUT L 53, 27.2.2008, s. 52.
( ) EUT L 160, 18.6.2011, s. 21.
( ) EGT C 192, 30.6.2012, s. 7.

3. Detta direktiv ska inte hindra medlemsstaterna från att föreskriva starkare skyddsåtgärder än de som fastställs i detta direktiv för skyddet av den registrerades rättigheter och friheter med avseende på behöriga myndigheters behandling av personuppgifter.

Artikel 2

Tillämpningsområde

1. Detta direktiv ska tillämpas på behandling av personuppgifter som utförs av behöriga myndigheter för de ändamål som anges i artikel 1.1.

2. Detta direktiv ska tillämpas på behandling av personuppgifter som helt eller delvis företas på automatiserad väg samt på annan behandling än automatiserad behandling av personuppgifter som ingår i eller kommer att ingå i ett register.

3. Detta direktiv tillämpas inte på behandling av personuppgifter

a) som utgör ett led i en verksamhet som inte omfattas av unionsrätten,

b) som utförs av unionens institutioner, organ och byråer.

Artikel 3

Definitioner

I detta direktiv avses med

1. *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar enskild person (nedan kallad *en registrerad*), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras, särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer, eller till en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,

2. *behandling*: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,

3. *begränsning av behandling*: markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden,

4. *profilering*: varje form av automatiserad behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga aspekter rörande denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar,

5. *pseudonymisering*: behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person,

6. *register*: en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,

7. *behörig myndighet*:

   a) en offentlig myndighet som har behörighet att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga hot mot den allmänna säkerheten, eller

   b) annat organ eller annan enhet som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten,

8. *personuppgiftsansvarig*: en behörig myndighet som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivs i unionsrätten eller medlemsstaternas nationella rätt,

9. *personuppgiftsbiträde*: en fysisk eller juridisk person, myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

10. *mottagare*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte; offentliga myndigheter som kan komma att motta personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare; offentliga myndigheters behandling av dessa uppgifter ska vara förenlig med tillämpliga bestämmelser för dataskydd beroende på behandlingens syfte,

11. *personuppgiftsincident*: en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,

12. *genetiska uppgifter*: alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om denna fysiska persons fysiologi eller hälsa och vilka framför allt härrör från en analys av ett biologiskt prov från den fysiska personen i fråga,

13. *biometriska uppgifter*: personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar unik identifiering av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter,

14. *uppgifter om hälsa*: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus,

15. *tillsynsmyndighet*: en oberoende offentlig myndighet som är utsedd av en medlemsstat i enlighet med artikel 41,

16. *internationell organisation*: en organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera länder,

KAPITEL II

Principer

Artikel 4

Principer för behandling av personuppgifter

1. Medlemsstaterna ska föreskriva att personuppgifter ska

a) behandlas på ett lagligt och korrekt sätt,

b) samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte behandlas på ett sätt som står i strid med dessa ändamål,

c) vara adekvata, relevanta och inte för omfattande i förhållande till de syften för vilka de behandlas,

d) vara korrekta och, om nödvändigt, uppdaterade; alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål,

e) inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas,

f) behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

2. Behandling som utförs av samma eller en annan personuppgiftsansvarig för något annat ändamål som anges i artikel 1.1 än det för vilket personuppgifterna samlas in ska tillåtas om

a) den personuppgiftsansvarige i enlighet med unionsrätten eller medlemsstaternas nationella rätt är bemyndigad att behandla sådana personuppgifter för ett sådant ändamål, och

b) behandlingen är nödvändig och står i proportion till detta andra ändamål i enlighet med unionsrätten eller medlemsstaternas nationella rätt.

3. Behandling som utförs av samma eller en annan personuppgiftsansvarig kan inbegripa arkivändamål av allmänt intresse och vetenskaplig, statistisk eller historisk användning för de ändamål som anges i artikel 1.1 under förutsättning att det finns lämpliga skyddsåtgärder för de registrerades rättigheter och friheter.

4. Den personuppgiftsansvarige ska ansvara för, och kunna visa efterlevnad av, punkterna 1, 2 och 3.

Artikel 5

Tidsgränser för lagring och översyn

Medlemsstaterna ska föreskriva att lämpliga tidsgränser fastställs för radering av personuppgifter eller för periodisk översyn av behovet av att lagra personuppgifter. Procedurrelaterade åtgärder ska säkerställa att tidsgränserna efterlevs.

Artikel 6

Åtskillnad mellan olika kategorier av registrerade

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, i tillämpliga fall och så långt det är möjligt, ska göra en klar åtskillnad mellan personuppgifter som rör olika kategorier av registrerade, såsom

a) personer avseende vilka det finns tungt vägande skäl att anta att de har begått eller är på väg att begå ett brott,

b) personer som dömts för brott,

c) brottsoffer eller personer avseende vilka det finns vissa omständigheter som ger anledning att anta att de kan vara brottsoffer, och

d) andra som berörs av ett brott, såsom personer som kan komma att kallas att vittna i samband med brottsutredningar eller senare straffrättsliga förfaranden, personer som kan ge information om brott eller personer med kontakter med eller band till någon av de personer som avses i a och b.

Artikel 7

Åtskillnad mellan personuppgifter och kontroll av kvaliteten på personuppgifterna

1. Medlemsstaterna ska föreskriva att personuppgifter som grundar sig på fakta så långt det är möjligt ska åtskiljas från personuppgifter som grundar sig på personliga bedömningar.

2. Medlemsstaterna ska föreskriva att de behöriga myndigheterna ska vidta alla rimliga åtgärder för att se till att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. Varje behörig myndighet ska därför i den mån det är praktiskt möjligt kontrollera kvaliteten på personuppgifterna innan dessa överförs eller görs tillgängliga. Vid all överföring av personuppgifter ska, så långt det är möjligt, sådan nödvändig information läggas till som gör det möjligt för den mottagande behöriga myndigheten att bedöma i vilken grad personuppgifterna är korrekta, fullständiga och tillförlitliga samt i vilken utsträckning de är aktuella.

3. Om det visar sig att felaktiga personuppgifter har överförts eller att personuppgifter olagligen har överförts ska mottagaren omedelbart underrättas om detta. I sådana fall ska personuppgifterna rättas eller raderas eller behandlingen begränsas i enlighet med artikel 16.

Artikel 8

Laglig behandling av personuppgifter

1. Medlemsstaterna ska föreskriva att behandling ska vara laglig endast om och i den mån behandlingen är nödvändig för att utföra en uppgift som utförs av en behörig myndighet för de ändamål som anges i artikel 1.1 och som sker på grundval av unionsrätt eller medlemsstaternas nationella rätt.

2. Medlemsstaternas nationella rätt som reglerar behandling inom tillämpningsområdet för detta direktiv ska åtminstone specificera syftet med behandlingen, vilka personuppgifter som ska behandlas och behandlingens ändamål.

Artikel 9

Särskilda villkor för uppgiftsbehandling

1. Personuppgifter som samlas in av behöriga myndigheter för de ändamål som anges i artikel 1.1. ska inte behandlas för andra ändamål än de som anges i artikel 1.1 såvida inte sådan behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt. När personuppgifter behandlas för andra ändamål ska förordning (EU) 2016/679 tillämpas, såvida inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten.

2. Om de behöriga myndigheterna enligt medlemsstaternas nationella rätt anförtros utförandet av andra uppgifter än de som utförs för de ändamål som anges i artikel 1.1, ska förordning (EU) 2016/679 vara tillämplig på behandlingen för dessa ändamål, inklusive för arkivändamål av allmänt intresse, för historiska eller vetenskapliga forskningsändamål eller för statistiska ändamål, såvida inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten.

3. Om den unionsrätt eller nationella rätt som är tillämplig på den överförande behöriga myndigheten fastställer särskilda villkor för behandling, ska medlemsstaten föreskriva att den överförande behöriga myndigheten ska informera mottagaren om dessa särskilda villkor och om kravet att respektera dem.

4. Medlemsstaterna ska föreskriva att den överförande behöriga myndigheten inte ska tillämpa villkor enligt punkt 3 på mottagare i andra medlemsstater eller på byråer och organ som inrättats i enlighet med avdelning V kapitlen 4 och 5 i EUF-fördraget, med undantag för de villkor som är tillämpliga på motsvarande överföringar av uppgifter inom den överförande behöriga myndighetens medlemsstat.

Artikel 10

Behandling av särskilda kategorier av personuppgifter

Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, samt behandling av genetiska uppgifter, biometriska uppgifter för att unikt identifiera en fysisk person eller uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara tillåten endast om det är absolut nödvändigt och under förutsättning att det finns lämpliga skyddsåtgärder för den registrerades rättigheter och friheter och endast

a) om behandlingen är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt,

b) för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan fysisk person, eller

c) om behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

Artikel 11

Automatiserat individuellt beslutsfattande

1. Medlemsstaterna ska föreskriva att beslut som enbart grundas på automatiserad behandling, inbegripet profilering, som har negativa rättsliga följder för den registrerade eller i betydande grad påverkar honom eller henne, ska förbjudas om de inte är tillåtna enligt unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige lyder under och som föreskriver lämpliga skyddsåtgärder för den registrerades rättigheter och friheter, åtminstone rätten till mänskligt ingripande från den personuppgiftsansvariges sida.

2. Beslut som avses i punkt 1 i den här artikeln får inte grundas på de särskilda kategorier av personuppgifter som avses i artikel 10, såvida inte lämpliga åtgärder för att skydda den registrerades rättigheter och friheter samt berättigade intressen har vidtagits.

3. Profilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter enligt artikel 10 ska förbjudas i enlighet med unionsrätten.

KAPITEL III

Den registrerades rättigheter

Artikel 12

Information om och villkor för utövandet av den registrerades rättigheter

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska vidta rimliga åtgärder för att tillhandahålla den registrerade all information som avses i artikel 13 och alla meddelanden enligt artiklarna 11, 14–18 och 31 som avser behandling i en koncis, begriplig och lättillgänglig form och på ett klart och tydligt språk. Informationen ska tillhandahållas på lämpligt sätt, t.ex. elektroniskt. Som en allmän regel ska den personuppgiftsansvarige tillhandahålla informationen i samma format som begäran.

2. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underlätta utövandet av den registrerades rättigheter enligt artiklarna 11 och 14–18.

3. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige utan onödigt dröjsmål skriftligen ska informera den registrerade om uppföljningen av hans eller hennes begäran.

4. Medlemsstaterna ska föreskriva att den information som tillhandahålls enligt artikel 13 och alla meddelanden eller åtgärder som vidtas enligt artiklarna 11, 14–18 och 31 ska tillhandahållas kostnadsfritt. Om en registrerads begäran är uppenbart ogrundad eller orimlig, särskilt på grund av att den är repetitiv, får den personuppgiftsansvarige antingen

a) ta ut en rimlig avgift med beaktande av de administrativa kostnaderna för tillhandahållandet av informationen eller meddelandet eller vidtagandet av den åtgärd som begärs, eller

b) vägra att tillmötesgå begäran.

Den personuppgiftsansvarige ska visa att begäran är uppenbart ogrundad eller orimlig.

5. Om den personuppgiftsansvarige har rimliga skäl att betvivla identiteten hos den fysiska person som lämnar in en begäran enligt artiklarna 14 eller 16, får den personuppgiftsansvarige begära att ytterligare information som är nödvändig för att bekräfta den registrerades identitet ska tillhandahållas.

Artikel 13

Information som ska göras tillgänglig för eller lämnas till den registrerade

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska göra åtminstone följande information tillgänglig för den registrerade:

a) Den personuppgiftsansvariges identitet och kontaktuppgifter.

b) Dataskyddsombudets kontaktuppgifter, i tillämpliga fall.

c) Ändamålen med den behandling för vilken personuppgifterna är avsedda.

d) Rätten att lämna in klagomål till en tillsynsmyndighet samt tillsynsmyndighetens kontaktuppgifter.

e) Rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter och begränsning av behandlingen av personuppgifter som rör den registrerade.

2. Utöver den information som avses i punkt 1, ska medlemsstaterna i lag föreskriva att den personuppgiftsansvarige i specifika fall ska lämna följande information till den registrerade, för att göra det möjligt för honom eller henne att utöva sina rättigheter:

a) Behandlingens rättsliga grund.

b) Den period under vilken personuppgifterna kommer att lagras eller, om det inte är möjligt, de kriterier som används för att fastställa denna period.

c) I tillämpliga fall, kategorierna av mottagare av personuppgifterna, inbegripet i tredjeländer eller internationella organisationer.

d) Vid behov ytterligare information, i synnerhet om personuppgifterna samlas in utan den registrerades vetskap.

3. Medlemsstaterna får anta lagstiftningsåtgärder som gör att informationen till den registrerade enligt punkt 2 senareläggs, begränsas eller utelämnas, i den utsträckning och så länge som en sådan åtgärd är nödvändig och proportionell i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att

a) undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden,

b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,

c) skydda den allmänna säkerheten,

d) skydda den nationella säkerheten,

e) skydda andra personers rättigheter och friheter.

4. Medlemsstaterna får anta lagstiftningsåtgärder för att fastställa kategorier av behandling som helt eller delvis kan omfattas av något av leden i punkt 3.

Artikel 14

Den registrerades rätt till tillgång till personuppgifter

Med förbehåll för artikel 15 ska medlemsstaterna föreskriva att den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse av huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna och följande information:

a) Ändamålen med behandlingen och dess rättsliga grund.

b) De kategorier av personuppgifter som behandlingen gäller.

c) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats ut, särskilt mottagare i tredjeländer eller internationella organisationer.

d) Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om det inte är möjligt, de kriterier som används för att fastställa denna period.

e) Rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifter eller begränsning av behandling av personuppgifter som rör den registrerade.

f) Rätten att lämna in klagomål till tillsynsmyndigheten samt tillsynsmyndighetens kontaktuppgifter.

g) Information om vilka personuppgifter som håller på att behandlas och all tillgänglig information om varifrån dessa uppgifter härstammar.

Artikel 15

Begränsningar av rätten till tillgång

1. Medlemsstaterna får anta lagstiftningsåtgärder som helt eller delvis begränsar den registrerades rätt till tillgång i den utsträckning och så länge en sådan partiell eller fullständig begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att

a) undvika att hindra officiella eller rättsliga utredningar, förundersökningar eller förfaranden,

b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,

c) skydda den allmänna säkerheten,

d) skydda den nationella säkerheten,

e) skydda andra personers rättigheter och friheter.

2. Medlemsstaterna får anta lagstiftningsåtgärder för att fastställa kategorier av behandling som helt eller delvis kan omfattas av undantagen i punkt 1 a–e.

3. I de fall som avses i punkterna 1 och 2 ska medlemsstaterna föreskriva att den personuppgiftsansvarige utan onödigt dröjsmål ska informera den registrerade skriftligen om varje vägran eller begränsning av tillgång och om skälen för vägran eller begränsningen. Denna information kan utelämnas om tillhandahållandet skulle undergräva ett ändamål enligt punkt 1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underrätta den registrerade om möjligheten att lämna in ett klagomål till en tillsynsmyndighet eller begära rättslig prövning.

4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska dokumentera de sakliga och rättsliga grunderna för beslutet. Denna information ska göras tillgänglig för tillsynsmyndigheterna.

Artikel 16

Rätt till rättelse eller radering av personuppgifter och begränsning av behandling

1. Medlemsstaterna ska föreskriva att den registrerade ska ha rätt att utan onödigt dröjsmål av den personuppgiftsansvarige få felaktiga personuppgifter som rör honom eller henne rättade. Med beaktande av ändamålet med behandlingen ska medlemsstaterna föreskriva att den registrerade ska ha rätt att få ofullständiga personuppgifter kompletterade, inbegripet genom att tillhandahålla en kompletterande inlaga.

2. Medlemsstaterna ska kräva att den personuppgiftsansvarige utan onödigt dröjsmål ska radera personuppgifter och ge den registrerade rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få till stånd radering av personuppgifter som rör honom eller henne om behandlingen står i strid med de bestämmelser som antas enligt artiklarna 4, 8 och 10 eller om personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

3. I stället för radering ska den personuppgiftsansvarige begränsa behandling om

a) den registrerade bestrider personuppgifternas korrekthet och korrektheten inte kan fastställas, eller

b) personuppgifterna måste sparas som bevisning.

Om behandlingen begränsas enligt första stycket led a ska den personuppgiftsansvarige underrätta den registrerade innan begränsningen av behandlingen upphävs.

4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige underrättar den registrerade skriftligen om eventuell vägran att rätta, radera eller begränsa behandlingen och om skälen till vägran. Medlemsstaterna får anta lagstiftningsåtgärder som helt eller delvis begränsar skyldigheten att tillhandahålla sådan information i den utsträckning som en sådan begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att

a) undvika att hindra offentliga eller rättsliga utredningar, undersökningar eller förfaranden,

b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,

c) skydda den allmänna säkerheten,

d) skydda den nationella säkerheten,

e) skydda andra personers rättigheter och friheter.

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underrätta den registrerade om möjligheterna att lämna in ett klagomål till en tillsynsmyndighet eller begära rättslig prövning.

5. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska meddela varje rättelse av oriktiga personuppgifter till den behöriga myndighet från vilken de oriktiga personuppgifterna kommer.

6. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, när personuppgifter har rättats, raderats eller begränsats i enlighet med punkterna 1, 2 och 3, ska underrätta mottagarna och att mottagarna ska rätta eller radera personuppgifterna eller begränsa den behandling som utförs under deras ansvar.

Artikel 17

Den registrerades utövande av rättigheter och kontroll genom tillsynsmyndigheten

1. I de fall som avses i artiklarna 13.3, 15.3 och 16.4 ska medlemsstaterna anta bestämmelser om att den registrerades rättigheter även kan utövas genom den behöriga tillsynsmyndigheten.

2. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underrätta den registrerade om hans eller hennes möjlighet att utöva sina rättigheter genom tillsynsmyndigheten enligt punkt 1.

3. När den rättighet som avses i punkt 1 utövas ska tillsynsmyndigheten åtminstone underrätta den registrerade om att alla nödvändiga kontroller eller en översyn genom tillsynsmyndigheten har ägt rum. Tillsynsmyndigheten ska också informera den registrerade om hans eller hennes rätt att begära rättslig prövning.

Artikel 18

Den registrerades rättigheter i brottsutredningar och straffrättsliga förfaranden

Medlemsstaterna får föreskriva att de rättigheter som avses i artiklarna 13, 14 och 16 ska utövas i enlighet med medlemsstaternas nationella rätt om personuppgifterna ingår i ett domstolsbeslut eller ett rättsligt protokoll eller ärende som behandlas i samband med brottsutredningar och straffrättsliga förfaranden.

KAPITEL IV

Personuppgiftsansvarig och personuppgiftsbiträde

Avsnitt 1

Allmänna skyldigheter

Artikel 19

Den personuppgiftsansvariges skyldigheter

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, med beaktande av behandlingens art, omfattning, sammanhang och ändamål, samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa, och kunna visa, att behandlingen utförs i enlighet med detta direktiv. Dessa åtgärder ska ses över och uppdateras vid behov.

2. Om det står i proportion till behandlingen, ska de åtgärder som avses i punkt 1 omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.

Artikel 20

Inbyggt dataskydd och dataskydd som standard

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, med beaktande av den senaste utvecklingen och genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål, samt de risker, av varierande sannolikhetsgrad och allvar för fysiska personers rättigheter och friheter som behandlingen utgör, både vid tidpunkten för beslut om vilka medel behandlingen ska utföras med och vid tidpunkten för själva behandlingen, ska genomföra lämpliga tekniska och organisatoriska åtgärder, såsom pseudonymisering, vilka är utformade för genomförande av dataskyddsprinciper, såsom uppgiftsminimering, på ett effektivt sätt och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, för att uppfylla kraven i detta direktiv och skydda den registrerades rättigheter.

2. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige genomför lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

Artikel 21

Gemensamt personuppgiftsansvariga

1. Medlemsstaterna ska föreskriva att två eller flera personuppgiftsansvariga har gemensamt ansvar för registret, om de gemensamt fastställer behandlingens ändamål och medel. De ska under öppna former fastställa sitt respektive ansvar för efterlevnaden av detta direktiv, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artikel 13, genom ett inbördes arrangemang, såvida inte och i den mån som de personuppgiftsansvarigas respektive skyldigheter fastställs i unionsrätt eller medlemsstaternas nationella rätt som de personuppgiftsansvariga omfattas av. Inom ramen för arrangemanget ska en kontaktpunkt för de registrerade utses. Medlemsstaterna får fastslå vem av de gemensamt personuppgiftsansvariga som kan fungera som enda kontaktpunkt för de registrerade i fråga om utövandet av deras rättigheter.

2. Oavsett formerna för det arrangemang som avses i punkt 1 får medlemsstaterna föreskriva att den registrerade får utöva sina rättigheter enligt de bestämmelser som antas i enlighet med detta direktiv med avseende på var och en av de personuppgiftsansvariga.

Artikel 22

Personuppgiftsbiträde

1. Medlemsstaterna ska, om en behandling ska genomföras på en personuppgiftsansvarigs vägnar, föreskriva att den personuppgiftsansvarige endast ska anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i detta direktiv och säkerställer att den registrerades rättigheter skyddas.

2. Medlemsstaterna ska föreskriva att personuppgiftsbiträdet inte får anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet alltid informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.

3. Medlemsstaterna ska föreskriva att ett personuppgiftsbiträdes behandling ska regleras genom ett avtal eller annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige och i vilken föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade samt den personuppgiftsansvariges skyldigheter och rättigheter anges. Avtalet eller den andra rättsakten ska särskilt föreskriva att personuppgiftsbiträdet

a) endast handlar enligt instruktioner från den personuppgiftsansvarige,

b) säkerställer att personer som har tillstånd att behandla personuppgifterna har förbundit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt,

c) på lämpligt sätt ska bistå den personuppgiftsansvarige att säkerställa efterlevnad av bestämmelserna om den registrerades rättigheter,

d) beroende på vad den personuppgiftsansvarige väljer, ska radera eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av uppgiftsbehandlingstjänster har avslutats och raderar befintliga kopior, såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt,

e) ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att denna artikel efterlevs,

f) respekterar de villkor som avses i punkterna 2 och 3 för anlitande av ett annat personuppgiftsbiträde.

4. Det avtal eller den andra rättsakt som avses i punkt 3 ska vara skriftligt, inbegripet i elektronisk form.

5. Om ett personuppgiftsbiträde i strid med detta direktiv fastställer ändamålen och medlen för behandlingen ska personuppgiftsbiträdet anses vara personuppgiftsansvarig med avseende på den behandlingen.

Artikel 23

Behandling under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende

Medlemsstaterna ska föreskriva att personuppgiftsbiträdet och personer som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, endast får behandla dessa uppgifter enligt instruktion från den personuppgiftsansvarige, såvida han eller hon inte är skyldig att göra det enligt unionsrätten eller medlemsstaternas nationella rätt.

Artikel 24

Register över behandling

1. Medlemsstaterna ska föreskriva att alla personuppgiftsansvariga ska föra ett register över alla kategorier av verksamheter i samband med behandling som de ansvarar för. Detta register ska innehålla samtliga följande uppgifter:

a) Namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga och dataskyddsombudet.

b) Ändamålen med behandlingen.

c) De kategorier av mottagare som personuppgifterna har lämnats ut till eller ska lämnas ut till, inbegripet mottagare i tredjeländer eller internationella organisationer.

d) En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.

e) Användning av profilering, i tillämpliga fall.

f) I tillämpliga fall, kategorier av personuppgiftsöverföringar till ett tredjeland eller en internationell organisation.

g) En uppgift om den rättsliga grunden för den behandling, inbegripet överföringar, för vilken personuppgifterna är avsedda.

h) Om möjligt, de planerade tidsfristerna för radering av de olika personuppgiftskategorierna.

i) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 29.1.

2. Medlemsstaterna ska föreskriva att alla personuppgiftsbiträden ska upprätthålla ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning, vilket ska omfatta följande:

a) Namn och kontaktuppgifter för personuppgiftsbiträdet eller registerförarna, för varje personuppgiftsansvarig för vars räkning personuppgiftsbiträdet agerar samt, i tillämpliga fall, för dataskyddsombudet.

b) De kategorier av behandling som har utförts för varje personuppgiftsansvarigs räkning.

c) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen, om den personuppgiftsansvarige uttryckligen begär detta.

d) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 29.1.

3. De register som avses i punkterna 1 och 2 ska upprättas skriftligen, inbegripet i elektronisk form.

Den personuppgiftsansvarige och personuppgiftsbiträdet ska på begäran göra registren tillgängliga för tillsynsmyndigheten.

Artikel 25

Loggning

1. Medlemsstaterna ska säkerställa att loggar förs över åtminstone följande typer av behandlingar i automatiserade behandlingssystem: insamling, ändring, läsning, utlämning inbegripet överföringar, sammanförande och radering. Loggarna över läsning och utlämning ska göra det möjligt att fastställa motivering, datum och tidpunkt för sådan behandling och i möjligaste mån vem som har läst eller lämnat ut personuppgifter, samt vilka som har fått tillgång till personuppgifterna.

2. Loggarna bör endast användas för att kontrollera om behandlingen är tillåten, för egenkontroll, för att säkerställa personuppgifternas integritet och säkerhet, samt inom ramen för straffrättsliga förfaranden.

3. Den personuppgiftsansvarige och personuppgiftsbiträdet ska på begäran göra loggarna tillgängliga för tillsynsmyndigheten.

Artikel 26

Samarbete med tillsynsmyndigheten

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige och personuppgiftsbiträdet på begäran ska samarbeta med tillsynsmyndigheten vid utförandet av dess uppgifter.

Artikel 27

Konsekvensbedömning avseende dataskydd

1. Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter, ska medlemsstaterna säkerställa att den personuppgiftsansvarige före behandlingen utför en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.

2. Den bedömning som avses i punkt 1 ska åtminstone innehålla en allmän beskrivning av den planerade behandlingen, en bedömning av riskerna för de registrerades rättigheter och friheter, de åtgärder som planeras för att hantera dessa risker, skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifter och för att visa att detta direktiv efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

Artikel 28

Förhandssamråd med tillsynsmyndigheten

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige eller personuppgiftsbiträdet ska samråda med tillsynsmyndigheten före behandling av personuppgifter som kommer att ingå i ett nytt register som ska inrättas, om

a) en konsekvensbedömning avseende dataskydd enligt artikel 27 visar att behandlingen skulle leda till en hög risk om inte den registeransvarige vidtar åtgärder för att minska risken, eller om

b) typen av behandling, särskilt vid användning av ny teknik eller nya rutiner eller förfaranden, medför en hög risk för de registrerades rättigheter och friheter.

2. Medlemsstaterna ska föreskriva att tillsynsmyndigheten ska rådfrågas under utarbetandet av ett förslag till lagstiftningsåtgärd som ska antas av ett nationellt parlament eller av en regleringsåtgärd som grundar sig på en sådan lagstiftningsåtgärd som rör behandling.

3. Medlemsstaterna ska föreskriva att tillsynsmyndigheten får upprätta en förteckning över de olika typer av uppgiftsbehandling som omfattas av förhandssamråd enligt punkt 1.

4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige till tillsynsmyndigheten lämnar in den konsekvensbedömning avseende dataskydd som avses i artikel 27 och, på begäran, eventuell övrig information som gör att tillsynsmyndigheten kan göra en bedömning av behandlingens överensstämmelse och särskilt av riskerna för skyddet av den registrerades personuppgifter och av därmed sammanhängande skyddsåtgärder.

5. Medlemsstaterna ska, om tillsynsmyndigheten anser att den planerade behandling som avses i punkt 1 i denna artikel inte skulle vara förenlig med de bestämmelser som antas i enlighet med detta direktiv, särskilt om den personuppgiftsansvarige inte i tillräcklig mån har fastställt eller reducerat risken, föreskriva att tillsynsmyndigheten inom en period på högst sex veckor från det att begäran om samråd mottagits ska ge den personuppgiftsansvarige och, i tillämpliga fall, personuppgiftsbiträdet skriftliga råd och får utnyttja alla de befogenheter som den har enligt artikel 47. Denna period får förlängas med en månad beroende på hur komplicerad den planerade behandlingen är. Tillsynsmyndigheten ska informera den personuppgiftsansvarige och, i tillämpliga fall, personuppgiftsbiträdet om en sådan förlängning inom en månad från det att begäran om samråd mottagits, tillsammans med orsakerna till förseningen.

Avsnitt 2

Säkerhet för personuppgifter

Artikel 29

Säkerhet i samband med behandling

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige och personuppgiftsbiträdet, med beaktande av den senaste utvecklingen och genomförandekostnader och med hänsyn till behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, i synnerhet när det gäller de särskilda kategorier av personuppgifter som avses i artikel 10.

2. När det gäller automatiserad behandling ska varje medlemsstat föreskriva att den personuppgiftsansvarige eller personuppgiftsbiträdet, efter en bedömning av riskerna, ska vidta åtgärder i syfte att

a) vägra varje obehörig person åtkomst till utrustning för behandling som används för behandling (*åtkomstskydd för utrustning*),

b) förhindra obehörig läsning, kopiering, ändring eller radering av datamedier (*kontroll av datamedier*),

c) förhindra obehörig registrering av personuppgifter och obehörig kännedom om, ändring eller radering av lagrade personuppgifter (*lagringskontroll*),

d) förhindra att obehöriga kan använda automatiserade behandlingssystem med hjälp av utrustning för dataöverföring (*användarkontroll*),

e) säkerställa att personer som är behöriga att använda ett automatiserat behandlingssystem endast har tillgång till personuppgifter som omfattas av deras behörighet (*åtkomstkontroll*),

f) säkerställa att det kan kontrolleras och fastställas till vilka organ personuppgifter har överförts eller kan överföras och för vilka organ uppgifterna har gjorts tillgängliga eller kan göras tillgängliga med hjälp av utrustning för dataöverföring (*kommunikationskontroll*),

g) säkerställa att det är möjligt att i efterhand kontrollera och fastställa vilka personuppgifter som förts in i ett automatiserat behandlingssystem, samt när och av vem personuppgifterna infördes (*indatakontroll*),

h) förhindra obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med överföring av sådana uppgifter eller under transport av databärare (*transportkontroll*),

i) säkerställa att de system som används kan återställas vid störningar (*återställande*),

j) säkerställa att systemet fungerar, att funktionsfel rapporteras (*driftsäkerhet*) och att de lagrade personuppgifterna inte kan förvanskas genom funktionsfel i systemet (*dataintegritet*).

Artikel 30

Anmälan av en personuppgiftsincident till tillsynsmyndigheten

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige vid en personuppgiftsincident utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om incidenten, anmäler den till tillsynsmyndigheten, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar, ska den åtföljas av en motivering till förseningen.

2. Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident.

3. Den anmälan som avses i punkt 1 ska åtminstone

a) beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antal registrerade som berörs samt de kategorier av och det ungefärliga antal personuppgiftsposter som berörs,

b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller annan kontaktpunkt där mer information kan erhållas,

c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten,

d) beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, i tillämpliga fall, åtgärder för att mildra dess potentiella negativa effekter.

4. Om, och i den utsträckning, det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

5. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter som avses i punkt 1, inbegripet omständigheterna rörande personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av denna artikel.

6. Medlemsstaterna ska föreskriva att den information som avses i punkt 3, om personuppgiftsincidenten rör personuppgifter som har överförts av eller till den personuppgiftsansvarige i en annan medlemsstat, utan onödigt dröjsmål ska meddelas den personuppgiftsansvarige i den medlemsstaten.

Artikel 31

Information till den registrerade om en personuppgiftsincident

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, om personuppgiftsincidenten sannolikt kommer att leda till en hög risk för fysiska personers rättigheter och friheter, utan onödigt dröjsmål ska informera den registrerade om personuppgiftsincidenten.

2. Den information till den registrerade som avses i punkt 1 i den här artikeln ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone de upplysningar och åtgärder som avses i artikel 30.3 b, c och d.

3. Information till den registrerade i enlighet med punkt 1 ska inte krävas om något av följande villkor är uppfyllda:

a) Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder har tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som gör personuppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till dem, såsom kryptering.

b) Om den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter som avses i punkt 1 sannolikt inte längre kommer att uppstå.

c) Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.

4. Om personuppgiftsbiträdet inte redan har informerat den registrerade om personuppgiftsincidenten får tillsynsmyndigheten, efter att ha bedömt sannolikheten för att personuppgiftsincidenten medför en hög risk, kräva att personuppgiftsbiträdet gör det, eller besluta att något av de villkor som avses i punkt 3 är uppfyllt.

5. Den information till den registrerade som avses i punkt 1 i den här artikeln kan senareläggas, begränsas eller utelämnas på de villkor och av de skäl som avses i artikel 13.3.

Avsnitt 3

Dataskyddsombud

Artikel 32

Utnämning av dataskyddsombudet

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska utnämna ett dataskyddsombud. Medlemsstaterna får undanta domstolars och andra oberoende rättsliga myndigheters dömande verksamhet från denna skyldighet.

2. Dataskyddsombudet ska utnämnas på grundval av sina yrkesmässiga kvalifikationer och, i synnerhet, sin sakkunskap om lagstiftning och praxis i fråga om dataskydd samt förmåga att fullgöra de uppgifter som avses i artikel 34.

3. Ett enda dataskyddsombud får utnämnas för flera behöriga myndigheter med hänsyn tagen till organisationsstruktur och storlek.

4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.

Artikel 33

Dataskyddsombudets ställning

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

2. Den personuppgiftsansvarige ska stödja dataskyddsombudet i utförandet av de uppgifter som avses i artikel 34 genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap.

Artikel 34

Dataskyddsombudets uppgifter

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska anförtro dataskyddsombudet åtminstone följande uppgifter:

a) Att informera och ge råd till den personuppgiftsansvarige och de anställda som utför behandling om deras skyldigheter enligt detta direktiv och annan unionsrätt eller medlemsstaters bestämmelser om dataskydd.

b) Att övervaka efterlevnaden av detta direktiv, annan unionsrätt eller medlemsstaternas bestämmelser om dataskydd och av den personuppgiftsansvariges strategier för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandlingen och tillhörande granskning.

c) Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den enligt artikel 27.

d) Att samarbeta med tillsynsmyndigheten.

e) Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, inbegripet det förhandssamråd som avses i artikel 28, och, om så är lämpligt, samråda i andra frågor.

KAPITEL V

Överföringar av personuppgifter till tredjeländer eller internationella organisationer

Artikel 35

Allmänna principer för överföringar av personuppgifter

1. Medlemsstaterna ska föreskriva att de behöriga myndigheterna endast ska överföra personuppgifter som håller på att behandlas eller är avsedda att behandlas efter det att de överförts till ett tredjeland eller en internationell organisation, inklusive för vidare överföring till ett annat tredjeland eller en annan internationell organisation, under förutsättning att de nationella bestämmelser som antas i enlighet med andra bestämmelser i detta direktiv respekteras och endast om de villkor som fastställs i detta kapitel uppfylls, nämligen:

a) Överföringen är nödvändig för de ändamål som anges i artikel 1.1.

b) Personuppgifterna överförs till en personuppgiftsansvarig i ett tredjeland eller en internationell organisation som är en behörig myndighet för de ändamål som avses i artikel 1.1.

c) Den aktuella medlemsstaten, om personuppgifter överförs eller görs tillgängliga från en annan medlemsstat, har gett förhandstillstånd till överföringen i enlighet med medlemsstaternas nationella rätt.

d) Kommissionen har antagit ett beslut om adekvat skyddsnivå i enlighet med artikel 36 eller, om inget sådant beslut föreligger, när lämpliga skyddsåtgärder har vidtagits eller föreligger enligt artikel 37 eller, om inget beslut om adekvat skyddsnivå enligt artikel 36 föreligger och inga lämpliga skyddsåtgärder enligt artikel 37 har vidtagits, när undantag för särskilda situationer gäller i enlighet med artikel 38.

e) Att den behöriga myndighet som gjorde den ursprungliga överföringen eller en annan behörig myndighet i samma medlemsstat vid vidare överföring till ett annat tredjeland eller en internationell organisation godkänner vidareöverföringen efter vederbörligt beaktande av alla relevanta faktorer, inbegripet brottets allvar, det ändamål för vilket personuppgifterna ursprungligen överfördes och nivån på skyddet av personuppgifter i tredjelandet till vilket eller den internationella organisationen till vilken personuppgifterna förts vidare.

2. Medlemsstaterna ska föreskriva att överföringar utan förhandstillstånd av en annan medlemsstat i enlighet med punkt 1 c tillåts endast om överföringen av personuppgifter är nödvändig för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en medlemsstat eller ett tredjeland eller mot en medlemsstats väsentliga intressen och förhandstillstånd inte kan erhållas i tid. Den myndighet som har ansvar för att ge förhandstillstånd ska underrättas utan dröjsmål.

3. Alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den skyddsnivå för fysiska personer som säkerställs genom detta direktiv inte undergrävs.

Artikel 36

Överföring på grundval av ett beslut om adekvat skyddsnivå

1. Medlemsstaterna ska föreskriva att personuppgifter får överföras till ett tredjeland eller en internationell organisation om kommissionen har beslutat att tredjelandet, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå. En sådan överföring ska inte kräva ett särskilt tillstånd.

2. När kommissionen bedömer om en adekvat skyddsnivå föreligger ska den särskilt beakta

a) rättsstatsprincipen, respekten för de mänskliga rättigheterna och grundläggande friheterna, relevant lagstiftning, både allmän lagstiftning och sektorslagstiftning, inklusive avseende allmän säkerhet, försvar, nationell säkerhet och straffrätt samt offentliga myndigheters tillgång till personuppgifter liksom tillämpningen av denna lagstiftning, dataskyddsregler, yrkesregler och säkerhetsbestämmelser och regler för vidare överföring av personuppgifter till ett annat tredjeland eller en annan internationell organisation, som ska följas i det tredjeland eller inom den internationella organisation som berörs, rättspraxis, och effektiva och verkställbara rättigheter för registrerade och effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs,

b) huruvida det finns en eller flera effektivt fungerande oberoende tillsynsmyndigheter i tredjelandet, eller som utövar tillsyn över den internationella organisationen, med ansvar för att säkerställa och kontrollera att dataskyddsbestämmelserna följs, inklusive lämpliga verkställighetsbefogenheter, ge registrerade råd och assistans när det gäller utövandet av deras rättigheter och samarbeta med medlemsstaternas tillsynsmyndigheter, och

c) vilka internationella åtaganden det berörda tredjelandet eller den berörda internationella organisationen har gjort, eller andra skyldigheter som följer av rättsligt bindande konventioner eller instrument samt av dess deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter.

3. Kommissionen får, efter att ha bedömt om skyddsnivån är adekvat, genom en genomförandeakt, besluta att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland, eller en internationell organisation, säkerställer en adekvat skyddsnivå i den mening som avses i punkt 2 i den här artikeln. Genomförandeakten ska inrätta en mekanism för regelbunden översyn, minst vart fjärde år, som ska beakta all relevant utveckling i det tredjelandet eller den internationella organisationen. Den territoriella och sektoriella tillämpningen ska regleras i genomförandeakten, där det också i förekommande fall ska anges vilken eller vilka myndigheter som är tillsynsmyndighet(er) enligt punkt 2 b i den här artikeln. Genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 58.2.

4. Kommissionen ska fortlöpande övervaka utveckling i tredjeländer och internationella organisationer vilken kan påverka hur beslut som antagits enligt punkt 3 fungerar.

5. Kommissionen ska, när tillgänglig information visar, i synnerhet efter den översyn som avses i punkt 3 i den här artikeln, att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom tredjelandet i fråga eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå i den mening som avses i punkt 2 i den här artikeln och, i den mån det behövs, genom genomförandeakter dra tillbaka, ändra eller upphäva det beslut som avses i punkt 3 i den här artikeln utan retroaktiv verkan. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 58.2.

När det föreligger vederbörligen motiverade och tvingande skäl till skyndsamhet, ska kommissionen anta omedelbart tillämpliga genomförandeakter i enlighet med det förfarande som avses i artikel 58.3.

6. Kommissionen ska samråda med tredjelandet eller den internationella organisationen i fråga för att lösa den situation som lett till beslutet enligt punkt 5.

7. Medlemsstaterna ska föreskriva att ett beslut enligt punkt 5 inte ska påverka överföringar av personuppgifter till tredjelandet, territoriet eller en eller flera specificerade sektorer inom tredjelandet, eller den internationella organisationen i fråga, enligt artiklarna 37–38.

8. Kommissionen ska i *Europeiska unionens officiella tidning* och på sin webbplats offentliggöra en förteckning över de tredjeländer och de territorier och specificerade sektorer i ett tredjeland samt de internationella organisationer för vilka den har fastställt att en adekvat skyddsnivå inte eller inte längre säkerställs.

Artikel 37

Överföring som omfattas av lämpliga skyddsåtgärder

1. Om det inte föreligger något beslut enligt artikel 36.3 ska medlemsstaterna föreskriva att en överföring av personuppgifter till ett tredjeland eller en internationell organisation får ske om

a) lämpliga skyddsåtgärder för personuppgifter har fastställts i ett rättsligt bindande instrument, eller

b) den personuppgiftsansvarige har bedömt alla omständigheter kring en överföring av personuppgifter och dragit slutsatsen att lämpliga skyddsåtgärder för personuppgifterna föreligger.

2. Den personuppgiftsansvarige ska informera tillsynsmyndigheten om kategorier av överföringar enligt punkt 1 b.

3. När en överföring grundas på punkt 1 b, ska denna överföring dokumenteras, och dokumentationen ska på begäran göras tillgänglig för tillsynsmyndigheten, inbegripet datum och tidpunkt för överföringen, information om den mottagande behöriga myndigheten, skälet till överföringen och de personuppgifter som har överförts.

Artikel 38

Undantag i särskilda situationer

1. Om det inte föreligger något beslut om adekvat skyddsnivå enligt artikel 36 eller lämpliga skyddsåtgärder enligt artikel 37, ska medlemsstaterna föreskriva att en överföring eller en kategori av överföringar av personuppgifter till ett tredjeland eller en internationell organisation får ske endast om överföringen är nödvändig

a) för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan person,

b) för att skydda den registrerades berättigade intressen, om lagstiftningen i den medlemsstat som överför personuppgifterna föreskriver detta,

c) för att avvärja en omedelbar och allvarlig fara för den allmänna säkerheten i en medlemsstat eller ett tredjeland,

d) i enskilda fall för de ändamål som anges i artikel 1.1. eller

e) i ett enskilt fall för att fastslå, göra gällande eller försvara rättsliga anspråk som hänför sig till de ändamål som anges i artikel 1.1.

2. Personuppgifter får inte överföras om den överförande behöriga myndigheten fastställer att den berörda registrerades grundläggande rättigheter och friheter väger tyngre än det allmänna intresset av en sådan överföring som avses i punkt 1 d och e.

3. När en överföring grundas på punkt 1, ska denna överföring dokumenteras, och dokumentationen ska på begäran göras tillgänglig för tillsynsmyndigheten, inbegripet datum och tidpunkt för överföringen, information om den mottagande behöriga myndigheten, skälet till överföringen och de personuppgifter som har överförts.

Artikel 39

Överföringar av personuppgifter till mottagare som är etablerade i tredjeländer

1. Genom undantag från artikel 35.1 b och utan att det påverkar tillämpningen av internationella avtal som avses i punkt 2 i den här artikeln, får det i unionsrätten eller medlemsstaternas nationella rätt föreskrivas att de behöriga myndigheter som avses i artikel 3.7 a, i enskilda och särskilda fall, får överföra personuppgifter direkt till mottagare som är etablerade i tredjeländer endast om de övriga bestämmelserna i detta direktiv efterlevs och samtliga följande villkor är uppfyllda:

a) Överföringen är absolut nödvändig för att utföra en uppgift som en överförande behörig myndighet ansvarar för i enlighet med unionsrätten eller medlemsstaternas nationella rätt för de ändamål som anges i artikel 1.1.

b) Den överförande behöriga myndigheten har fastställt att ingen av den berörda registrerades grundläggande rättigheter och friheter väger tyngre än det allmänna intresse som nödvändiggör överföringen i det aktuella fallet.

c) Den överförande behöriga myndigheten anser att överföring till en myndighet som är behörig för de ändamål som avses i artikel 1.1 i tredjelandet är ineffektivt eller olämpligt, i synnerhet eftersom överföringen inte kan göras inom rimlig tid.

d) Den myndighet i tredjelandet som är behörig för de ändamål som avses i artikel 1.1 har utan dröjsmål informerats, såvida detta inte är ineffektivt eller olämpligt.

e) Den överförande behöriga myndigheten har informerat mottagaren om det eller de specifika ändamål för vilka och personuppgifterna ska behandlas av den senare förutsatt att den behandlingen är nödvändig.

2. Med ett internationellt avtal som avses i punkt 1 avses varje gällande bilateralt eller multilateralt internationellt avtal mellan medlemsstater och tredjeländer inom området för straffrättsligt samarbete och polissamarbete.

3. Den överförande behöriga myndigheten ska informera tillsynsmyndigheten om överföringar enligt denna artikel.

4. Överföringar som grundar sig på punkt 1 ska dokumenteras.

Artikel 40

Internationellt samarbete för skydd av personuppgifter

När det gäller tredjeländer och internationella organisationer ska kommissionen och medlemsstaterna vidta lämpliga åtgärder för att

a) utveckla rutiner för det internationella samarbetet för att underlätta en effektiv tillämpning av lagstiftningen om skydd av personuppgifter,

b) på internationell nivå erbjuda ömsesidigt bistånd för en effektiv tillämpning av lagstiftningen om skydd av personuppgifter, bland annat genom underrättelse, hänskjutande av klagomål, bistånd vid utredningar samt informationsutbyte, med iakttagande av lämpliga skyddsåtgärder för personuppgifter samt skyddet av andra grundläggande rättigheter och friheter,

c) involvera berörda aktörer i diskussioner och åtgärder som syftar till att öka det internationella samarbetet när det gäller tillämpningen av lagstiftningen om skydd av personuppgifter,

d) främja utbyte och dokumentation om lagstiftning och praxis för skydd av personuppgifter, inklusive avseende behörighetskonflikter med tredjeländer.

KAPITEL VI

Oberoende tillsynsmyndigheter

Avsnitt 1

Oberoende ställning

Artikel 41

Tillsynsmyndighet

1. Varje medlemsstat ska föreskriva att en eller flera offentliga myndigheter ska vara ansvariga för att övervaka tillämpningen av detta direktiv, i syfte att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandlingen samt att underlätta det fria flödet av sådana uppgifter inom unionen (*tillsynsmyndighet*).

2. Varje tillsynsmyndighet ska bidra till en enhetlig tillämpning av detta direktiv i hela unionen. För det ändamålet ska tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen i enlighet med kapitel VII.

3. Medlemsstaterna får föreskriva att en tillsynsmyndighet som har inrättats enligt förordning (EU) 2016/679 ska vara den tillsynsmyndighet som avses i detta direktiv och ta på sig ansvaret för de uppgifter som ska utföras av den tillsynsmyndighet som inrättas enligt punkt 1 i denna artikel.

4. Om det finns fler än en tillsynsmyndighet i en medlemsstat ska medlemsstaten utse den tillsynsmyndighet som ska företräda myndigheterna i fråga i den styrelse som avses i artikel 51.

Artikel 42

Oberoende

1. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet ska vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med detta direktiv.

2. Medlemsstaterna ska föreskriva att dess tillsynsmyndigheters ledamot eller ledamöter i utförandet av sina uppgifter och i utövandet av sina befogenheter enligt detta direktiv ska stå fria från utomstående påverkan, direkt såväl som indirekt, och varken begära eller ta emot instruktioner av någon.

3. Medlemsstaternas tillsynsmyndigheters ledamot eller ledamöter ska avhålla sig från alla handlingar som står i strid med deras tjänsteutövning och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet som står i strid med deras tjänsteutövning.

4. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet förfogar över de personella, tekniska och finansiella resurser samt de lokaler och den infrastruktur som behövs för att myndigheten ska kunna utföra sina uppgifter och utöva sina befogenheter, inklusive inom ramen för det ömsesidiga biståndet, samarbetet och deltagandet i styrelsens verksamhet.

5. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet väljer och förfogar över egen personal, som ska ta instruktioner uteslutande från den berörda tillsynsmyndighetens ledamot eller ledamöter.

6. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet är föremål för finansiell kontroll, utan att detta påverkar tillsynsmyndighetens oberoende och att de förfogar över en separat, offentlig årsbudget som kan ingå i den övergripande statsbudgeten eller nationella budgeten.

Artikel 43

Allmänna villkor för tillsynsmyndighetens ledamöter

1. Medlemsstaterna ska föreskriva att varje ledamot av deras tillsynsmyndigheter ska utses genom ett öppet förfarande av

— deras parlament

— deras regering

— deras statschef, eller

— ett oberoende organ som enligt medlemsstaternas nationella rätt anförtrotts utnämningen.

2. Varje ledamot ska ha de kvalifikationer, den erfarenhet och den kompetens, särskilt på området skydd av personuppgifter, som krävs för att de ska kunna utföra sitt uppdrag och utöva sina befogenheter.

3. En ledamots uppdrag ska upphöra då mandattiden löper ut eller om ledamoten avgår eller avsätts från sin tjänst i enlighet med den nationella rätten i den berörda medlemsstaten.

4. En ledamot ska avsättas endast på grund av allvarlig försummelse eller när ledamoten inte längre uppfyller de krav som ställs för att kunna utföra sina uppgifter.

Artikel 44

Regler för inrättandet av en tillsynsmyndighet

1. Varje medlemsstat ska i lag fastställa samtliga följande:

a) Varje tillsynsmyndighets inrättande.

b) De kvalifikationer och de villkor för lämplighet som krävs för att någon ska kunna utnämnas till ledamot av en tillsynsmyndighet.

c) Regler och förfaranden för att utse varje tillsynsmyndighets ledamot eller ledamöter.

d) Mandattiden för varje tillsynsmyndighets ledamot eller ledamöter, vilken inte får understiga fyra år, utom vid tillsättandet av de första ledamöterna efter den 6 maj 2016, då ett stegvis tillsättningsförfarande med kortare perioder för några av ledamöterna får tillämpas om detta är nödvändigt för att säkerställa myndighetens oberoende.

e) Huruvida varje tillsynsmyndighets ledamot eller ledamöter får ges förnyat mandat, och om så är fallet, för hur många perioder,

f) Vilka villkor som gäller för de skyldigheter som varje tillsynsmyndighets ledamot eller ledamöter och personal har, förbud mot handlingar, yrkesverksamhet och förmåner som står i strid därmed under och efter mandattiden och vilka bestämmelser som gäller för anställningens upphörande.

2. Varje tillsynsmyndighets ledamot eller ledamöter och personal ska i enlighet med unionsrätten eller medlemsstaternas nationella rätt omfattas av tystnadsplikt både under och efter sin mandattid vad avser konfidentiell information som de fått kunskap om under utförandet av deras uppgifter eller utövandet av deras befogenheter. Under mandatperioden ska denna tystnadsplikt i synnerhet gälla rapporter från fysiska personer om överträdelser av detta direktiv.

Avsnitt 2

Behörighet, uppgifter och befogenheter

Artikel 45

Behörighet

1. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet ska vara behörig att utföra de uppgifter och utöva de befogenheter som tilldelas den i enlighet med detta direktiv inom sin egen medlemsstats territorium.

2. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet inte ska vara behörig att utöva tillsyn över domstolar som behandlar personuppgifter inom ramen för sin dömande verksamhet. Medlemsstaterna får föreskriva att deras tillsynsmyndighet inte ska vara behörig att utöva tillsyn över andra oberoende rättsliga myndigheter som behandlar personuppgifter inom ramen för sin rättsliga verksamhet.

Artikel 46

Uppgifter

1. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet inom sitt territorium ska

a) övervaka och verkställa tillämpningen av de bestämmelser som antas i enlighet med detta direktiv och dess genomförandeåtgärder,

b) öka allmänhetens medvetenhet och kunskaper om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen,

c) i enlighet med medlemsstaternas nationella rätt ge rådgivning åt det nationella parlamentet, regeringen och andra institutioner och organ om lagstiftningsmässiga och administrativa åtgärder rörande skyddet av fysiska personers rättigheter och friheter när det gäller behandling,

d) öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter enligt detta direktiv,

e) på begäran tillhandahålla information till registrerade om hur de ska utöva sina rättigheter enligt detta direktiv, och om så krävs samarbeta med tillsynsmyndigheter i andra medlemsstater för detta ändamål,

f) behandla klagomål från en registrerad eller från ett organ, en organisation eller en sammanslutning enligt artikel 55, och där så är lämpligt undersöka den sakfråga som klagomålet gäller och inom rimlig tid underrätta den enskilde om hur undersökningen fortskrider och om resultatet, i synnerhet om det krävs ytterligare undersökningar eller samordning med en annan tillsynsmyndighet,

g) kontrollera att behandling enligt artikel 17 är laglig och inom en rimlig period informera den registrerade om resultatet av kontrollen enligt artikel 17.3 eller om skälen till att kontrollen inte har genomförts,

h) samarbeta, inbegripet genom att utbyta information, med och ge ömsesidigt bistånd till andra tillsynsmyndigheter för att se till att detta direktiv tillämpas och verkställs på ett enhetligt sätt,

i) utföra undersökningar om tillämpningen av detta direktiv, inbegripet på grundval av information som erhålls från en annan tillsynsmyndighet eller annan offentlig myndighet,

j) följa sådan utveckling som påverkar skyddet av personuppgifter, bland annat inom informations- och kommunikationsteknik,

k) ge råd om sådan behandling av personuppgifter som avses i artikel 28, och

l) bidra till styrelsens verksamhet.

2. Varje tillsynsmyndighet ska underlätta inlämningen av klagomål enligt punkt 1 f genom åtgärder, såsom att tillhandahålla ett särskilt formulär för ändamålet, vilket också kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.

3. Utförandet av alla tillsynsmyndigheters uppgifter ska vara avgiftsfritt för den registrerade och för dataskyddsombudet.

4. Om en begäran är uppenbart ogrundad eller orimlig, särskilt på grund av att den är repetitiv, får tillsynsmyndigheten ta ut en rimlig avgift grundad på de administrativa kostnaderna eller vägra att tillmötesgå begäran. Det åligger tillsynsmyndigheten att visa att begäran är uppenbart ogrundad eller orimlig.

Artikel 47

Befogenheter

1. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har effektiva undersökningsbefogenheter. Dessa befogenheter ska minst inbegripa rätten att från den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter som behandlas och all information som tillsynsmyndigheten behöver för att kunna fullgöra sina uppgifter.

2. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har effektiva korrigerande befogenheter, till exempel för att:

a) Utfärda varningar till den personuppgiftsansvarige eller personuppgiftsbiträdet om att planerade behandlingar sannolikt kommer att stå i strid med de bestämmelser som antas i enlighet med detta direktiv.

b) Beordra den personuppgiftsansvarige eller personuppgiftsbiträdet att se till att uppgiftsbehandlingen är förenlig med de bestämmelser som antas enligt detta direktiv, om lämpligt på ett visst sätt och inom en viss tid, bland annat genom att beordra rättelse, eller radering av personuppgifter eller begränsning av behandling enligt artikel 16.

c) Införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, uppgiftsbehandlingen.

3. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har effektiva befogenheter att ge den personuppgiftsansvarige råd i enlighet med det förfarande för förhandssamråd som avses i artikel 28 och att på eget initiativ eller på begäran avge yttranden till det nationella parlamentet, medlemsstatens regering eller, i enlighet med dess nationella rätt, till andra institutioner och organ samt till allmänheten, i frågor som rör skydd av personuppgifter.

4. Utövandet av de befogenheter som tillsynsmyndigheten tilldelas enligt denna artikel ska omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel och rättssäkerhet, som fastställts i unionsrätten och medlemsstaternas nationella rätt i enlighet med stadgan.

5. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har befogenhet att göra rättsliga myndigheter uppmärksamma på överträdelser av de bestämmelser som antas i enlighet med detta direktiv och att, när så är lämpligt, inleda eller på annat sätt delta i rättsliga förfaranden, i syfte att säkerställa efterlevnaden av bestämmelser som antas i enlighet med detta direktiv.

Artikel 48

Rapportering av överträdelser

Medlemsstaterna ska föreskriva att de behöriga myndigheterna ska inrätta effektiva mekanismer för att uppmuntra till konfidentiell rapportering av överträdelser av detta direktiv.

Artikel 49

Verksamhetsrapport

Varje tillsynsmyndighet ska upprätta en årlig rapport om sin verksamhet, vilken kan omfatta en förteckning över typer av anmälda överträdelser och typer av ålagda sanktioner. Rapporterna ska översändas till det nationella parlamentet, regeringen och andra myndigheter som utsetts genom medlemsstaternas nationella rätt. Den ska göras tillgänglig för allmänheten, kommissionen och styrelsen.

KAPITEL VII

Samarbete

Artikel 50

Ömsesidigt bistånd

1. Medlemsstaterna ska föreskriva att tillsynsmyndigheterna ska utbyta relevant information och ge ömsesidigt bistånd i arbetet för att genomföra och tillämpa detta direktiv på ett enhetligt sätt, och ska införa åtgärder som bidrar till ett verkningsfullt samarbete. Det ömsesidiga biståndet ska särskilt omfatta begäranden om information och tillsynsåtgärder, till exempel begäranden om att genomföra samråd, inspektioner och utredningar.

2. Medlemsstaterna ska föreskriva att varje tillsynsmyndighet ska vidta alla lämpliga åtgärder för att kunna besvara en begäran från en annan tillsynsmyndighet utan onödigt dröjsmål och inte senare än en månad efter det att den tagit emot begäran. Till sådana åtgärder hör bland annat att översända relevant information om genomförandet av en pågående utredning.

3. En begäran om bistånd ska innehålla all nödvändig information, inklusive syftet med och skälen till denna. Information som utbytts får endast användas för det syfte för vilket den har begärts.

4. En tillsynsmyndighet som tar emot begäran får bara vägra att tillmötesgå begäran om

a) den inte är behörig att behandla den sakfråga som begäran avser eller de åtgärder som det begärs att den ska utföra, eller

b) det skulle stå i strid med detta direktiv eller med den unionsrätt eller medlemsstatens nationella rätt som den tillsynsmyndighet som mottar begäran omfattas av att tillmötesgå begäran.

5. Den tillsynsmyndighet som tagit emot begäran ska meddela den myndighet som begäran kommer ifrån om resultatet eller, allt efter omständigheterna, om hur de åtgärder som vidtagits för att tillmötesgå begäran fortskrider. Den tillsynsmyndighet som tagit emot begäran ska redogöra för sina skäl för att vägra tillmötesgå begäran i enlighet med punkt 4.

6. Varje tillsynsmyndighet som tar emot begäran ska som regel tillhandahålla den information som begärts av andra tillsynsmyndigheter på elektronisk väg med användning av ett standardiserat format.

7. Tillsynsmyndigheter som tar emot begäran får inte ta ut någon avgift för åtgärder som de vidtagit efter en begäran om ömsesidigt bistånd. Tillsynsmyndigheter får i undantagsfall komma överens med andra tillsynsmyndigheter om regler för ersättning från varandra för vissa utgifter i samband med tillhandahållande av ömsesidigt bistånd.

8. Kommissionen får genom genomförandeakter närmare ange format och förfaranden för sådant ömsesidigt bistånd som avses i denna artikel samt formerna för elektronisk överföring av information tillsynsmyndigheter emellan, samt mellan tillsynsmyndigheter och styrelsen. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 58.2.

Artikel 51

Styrelsens uppgifter

1. Styrelsen som inrättats genom förordning (EU) 2016/679 ska i samband med uppgiftsbehandling som omfattas av detta direktivs tillämpningsområde ha följande uppgifter:

a) Ge kommissionen råd i alla frågor som gäller skydd av personuppgifter inom unionen, till exempel om eventuella förslag till ändring av detta direktiv.

b) På eget initiativ, på begäran av en av sina ledamöter eller av kommissionen behandla frågor om tillämpningen av detta direktiv och utfärda riktlinjer, rekommendationer och bästa praxis i syfte att främja en enhetlig tillämpning av detta direktiv.

c) Utforma riktlinjer för tillsynsmyndigheterna i fråga om tillämpningen av de åtgärder som avses i artikel 47.1 och 47.3.

d) Utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led b i detta stycke för att konstatera personuppgiftsincidenter och fastställa det otillbörliga dröjsmål som avses i artikel 30.1 och 30.2 och för de särskilda omständigheter under vilka ett personuppgiftsbiträde eller en personuppgiftsansvarig är skyldig att anmäla personuppgiftsincidenten.

e) Utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led b i detta stycke angående de omständigheter under vilka en personuppgiftsincident sannolikt kommer att orsaka en hög risk för rättigheterna och friheterna för de fysiska personer som avses i artikel 31.1.

f) Se över den praktiska tillämpningen av de riktlinjer och rekommendationer samt den bästa praxis som avses i leden b och c.

g) Avge ett yttrande till kommissionen för bedömningen av huruvida skyddsnivån i ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland, eller en internationell organisation är adekvat, inbegripet för en bedömning av huruvida det tredjelandet, det territoriet, den specificerade sektorn eller den internationella organisationen inte längre säkerställer en adekvat skyddsnivå.

h) Främja samarbete och effektivt bilateralt och multilateralt utbyte av bästa praxis och information mellan tillsynsmyndigheterna.

i) Främja gemensamma utbildningsprogram och underlätta personalutbyte mellan tillsynsmyndigheterna, och där så är lämpligt även med tillsynsmyndigheter i tredjeland och internationella organisationer.

j) Främja utbyte av kunskap och dokumentation om lagstiftning och bästa praxis på området för dataskydd med tillsynsmyndigheter med ansvar för dataskydd i hela världen.

Vad gäller första stycket led g ska kommissionen lämna all nödvändig dokumentation till styrelsen, inklusive korrespondens med regeringen i tredjelandet, med territoriet eller den specificerade sektorn i det tredjelandet eller med den internationella organisationen.

2. När kommissionen begär rådgivning från styrelsen får den ange en tidsfrist med hänsyn till hur brådskande ärendet är.

3. Styrelsen ska vidarebefordra sina yttranden, riktlinjer, rekommendationer och exempel på bästa praxis till kommissionen och till den kommitté som avses i artikel 58.1, samt offentliggöra dem.

4. Kommissionen ska hålla styrelsen underrättad om de åtgärder den vidtagit som en följd av styrelsens yttranden, riktlinjer, rekommendationer och bästa praxis.

KAPITEL VIII

Rättsmedel, ansvar och sanktioner

Artikel 52

Rätt att lämna in ett klagomål till en tillsynsmyndighet

1. Utan att det påverkar andra administrativa prövningsförfaranden eller rättsmedel ska medlemsstaterna föreskriva att alla registrerade personer som anser att behandling som avser dem står i strid med de bestämmelser som antas i enlighet med detta direktiv har rätt att lämna in ett klagomål till en enda tillsynsmyndighet.

2. Medlemsstaterna ska föreskriva att den tillsynsmyndighet som mottagit klagomålet ska överlämna det till den behöriga tillsynsmyndigheten utan onödigt dröjsmål, om klagomålet inte inlämnats till den myndighet som är behörig enligt artikel 45.1. Den registrerade ska informeras om överlämnandet.

3. Medlemsstaterna ska föreskriva att den tillsynsmyndighet som mottagit klagomålet ska tillhandahålla ytterligare hjälp på den registrerades begäran.

4. Den registrerade ska underrättas av den behöriga tillsynsmyndigheten om klagomålets handläggning och dess resultat, inbegripet rätten till rättsmedel enligt artikel 53.

Artikel 53

Rätt till ett effektivt rättsmedel mot en tillsynsmyndighets beslut

1. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol ska medlemsstater föreskriva att en fysisk eller juridisk person har rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut som avser dem och som meddelats av en tillsynsmyndighet.

2. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol ska varje registrerad person ha rätt till ett effektivt rättsmedel om den enligt artikel 45.1 behöriga tillsynsmyndigheten inte inom tre månader behandlar ett klagomål eller om tillsynsmyndigheten inte informerar den registrerade om handläggningen eller resultatet av det klagomål som inlämnats enligt artikel 52.

3. Medlemsstaterna ska föreskriva att talan mot en tillsynsmyndighet ska väckas vid domstol i den medlemsstat där tillsynsmyndigheten har sitt säte.

Artikel 54

Rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde

Utan att det påverkar tillgängliga administrativa prövningsförfaranden eller prövningsförfaranden utanför domstol, inbegripet rätten att lämna in ett klagomål till en tillsynsmyndighet enligt artikel 52, ska medlemsstaterna föreskriva en rätt till effektiva rättsmedel för registrerade om han eller hon anser att deras rättigheter enligt de bestämmelser som antas enligt detta direktiv har kränkts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med dessa bestämmelser.

Artikel 55

Företrädande av registrerade personer

Medlemsstaterna ska i enlighet med medlemsstaternas nationella processrätt se till att den registrerade har rätt att ge ett organ, en organisation eller en sammanslutning utan vinstsyfte som har inrättats på lämpligt sätt i enlighet med lagen i en medlemsstat, och vars stadgeenliga mål är av allmänt intresse och som är verksam inom området skydd av registrerades rättigheter och friheter vad gäller skyddet av deras personuppgifter, i uppdrag att lämna in klagomålet för hans eller hennes räkning och att utöva de rättigheter som avses i artiklarna 52, 53 och 54 för hans eller hennes räkning.

Artikel 56

Rätt till ersättning

Medlemsstaterna ska föreskriva att var och en som lidit materiell eller immateriell skada till följd av en olaglig behandling av personuppgifter eller av någon annan åtgärd som står i strid med de nationella bestämmelser som antas i enlighet med detta direktiv ska ha rätt till ersättning för denna skada från den personuppgiftsansvarige eller varje annan myndighet som är behörig enligt medlemsstaternas nationella rätt.

Artikel 57

Sanktioner

Medlemsstaterna ska föreskriva sanktioner för överträdelser av bestämmelser som antas enligt detta direktiv och ska vidta de åtgärder som krävs för att säkerställa att dessa sanktioner genomförs. Sanktionerna ska vara effektiva, proportionella och avskräckande.

KAPITEL IX

Genomförandeakter

Artikel 58

Kommittéförfarande

1. Kommissionen ska biträdas av den kommitté som inrättats enligt artikel 93 i förordning (EU) 2016/679. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

3. När det hänvisas till denna punkt, ska artikel 8 i förordning (EU) nr 182/2011 jämförd med artikel 5 i den förordningen tillämpas.

KAPITEL X

Slutbestämmelser

Artikel 59

Upphävande av rambeslut 2008/977/RIF

1. Rambeslut 2008/977/RIF ska upphöra att gälla från och med den 6 maj 2018.

2. Hänvisningar till det upphävda beslut som avses i punkt 1 ska anses som hänvisningar till detta direktiv.

Artikel 60

Gällande unionsrättsakter

Detta direktiv ska inte påverka särskilda bestämmelser om skydd av personuppgifter i unionsrättsakter på området för straffrättsligt samarbete och polissamarbete som trädde i kraft den 6 maj 2016 eller tidigare, vilka reglerar behandling medlemsstaterna emellan och medlemsstaternas utsedda myndigheters tillgång till informationssystem som inrättats på grundval av fördragen och som är relevanta för detta direktivs tillämpningsområde.

Artikel 61

Förhållande till tidigare ingångna internationella avtal på området för straffrättsligt samarbete och polissamarbete

Internationella avtal som rör överföring av personuppgifter till tredjeländer eller internationella organisationer som ingicks av medlemsstaterna före den 6 maj 2016 och som är förenliga med unionsrätten så som den tillämpades före den dagen ska fortsätta att gälla tills de ändras, ersätts eller återkallas.

Artikel 62

Kommissionens rapporter

1. Kommissionen ska senast den 6 maj 2022 och därefter vart fjärde år överlämna en rapport om utvärderingen och översynen av detta direktiv till Europaparlamentet och rådet. Rapporten ska offentliggöras.

2. Inom ramen för de utvärderingar och översyner som avses i punkt 1 ska kommissionen i synnerhet granska tillämpningen av kapitel V om överföring av personuppgifter till tredjeländer och internationella organisationer samt hur bestämmelserna fungerar, och därvid särskilt beakta beslut som antagits i enlighet med artiklarna 36.3 och 39.

3. För de ändamål som avses i punkterna 1 och 2 får kommissionen begära information från medlemsstaterna och tillsynsmyndigheterna.

4. Kommissionen ska när den utför de utvärderingar och översyner som avses i punkterna 1 och 2 ta hänsyn till ståndpunkter och slutsatser från Europaparlamentet, rådet och andra relevanta organ och källor.

5. Dessa rapporter får vid behov överlämnas tillsammans med lagstiftningsförslag om ändring, i syfte att ändra detta direktiv med särskild hänsyn till informationsteknikens utveckling och informationssamhällets framsteg.

6. Kommissionen ska senast den 6 maj 2019 se över andra rättsakter som antagits av unionen och som reglerar de behöriga myndigheternas behandling för att uppnå de mål som anges i artikel 1.1, inklusive de som avses i artikel 60, i syfte att bedöma om de behöver anpassas till detta direktiv och att, i förekommande fall, lägga fram förslag till ändring av dessa rättsakter för att säkerställa ett enhetligt tillvägagångssätt för skydd av personuppgifter inom detta direktivs tillämpningsområde.

Artikel 63

Införlivande

1. Medlemsstaterna ska senast den 6 maj 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att följa detta direktiv. De ska genast överlämna texten till dessa bestämmelser till kommissionen. De ska tillämpa dessa bestämmelser från och med den 6 maj 2018.

När en medlemsstat antar dessa bestämmelser ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

2. Genom undantag från punkt 1 får medlemsstaterna föreskriva att de automatiserade behandlingssystem som inrättades före den 6 maj 2016 undantagsvis, när det innebär oproportionella ansträngningar, ska bringas i överensstämmelse med artikel 25.1 senast den 6 maj 2023.

3. Genom undantag från punkterna 1 och 2 i denna artikel får en medlemsstat under exceptionella omständigheter bringa ett automatiserat behandlingssystem som avses i punkt 2 i denna artikel i överensstämmelse med artikel 25.1 inom en specifik tidsperiod efter den period som avses i punkt 2 i den här artikeln om det annars skulle uppstå allvarliga problem för driften av detta specifika automatiserade behandlingssystem. Den berörda medlemsstaten ska underrätta kommissionen om skälen till dessa allvarliga problem och skälen till den angivna tidsperioden inom vilken den ska bringa detta specifika automatiserade databehandlingssystem i överensstämmelse med artikel 25.1. Den angivna perioden ska under inga omständigheter inte vara senare än 6 maj 2026.

4. Medlemsstaterna ska till kommissionen överlämna texten till de centrala bestämmelser i medlemsstaternas nationella rätt som de antar inom det område som omfattas av detta direktiv.

Artikel 64

Ikraftträdande

Detta direktiv träder i kraft dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 65

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Bryssel den 27 april 2016.

På Europaparlamentets vägnar	*På rådets vägnar*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT
Ordförande	*Ordförande*

Statens offentliga utredningar 2017

Kronologisk förteckning

1. För Sveriges landsbygder – en sammanhållen politik för arbete, hållbar tillväxt och välfärd. N.
2. Kraftsamling för framtidens energi. M.
3. Karens för statsråd och statssekreterare. Fi.
4. För en god och jämlik hälsa. En utveckling av det folkhälsopolitiska ramverket. S.
5. Svensk social trygghet i en globaliserad värld. Del 1 och 2. S.
6. Se barnet! Ju.
7. Straffprocessens ramar och domstolens beslutsunderlag i brottmål – en bättre hantering av stora mål. Ju.
8. Kunskapsläget på kärnavfallsområdet 2017. Kärnavfallet – en fråga i ständig förändring. M.
9. Det handlar om oss. – unga som varken arbetar eller studerar. U.
10. Ny ordning för att främja god sed och hantera oredlighet i forskning. U.
11. Vägskatt. Volym 1 och 2. Fi.
12. Att ta emot människor på flykt. Sverige hösten 2015. Ju.
13. Finansiering av infrastruktur med privat kapital? Fi.
14. Migrationsärenden vid utlandsmyndigheterna. Ju.
15. Kvalitet och säkerhet på apoteksmarknaden. S.
16. Sverige i Afghanistan 2002–2014. UD.
17. Om oskuldspresumtionen och rätten att närvara vid rättegången. Genomförande av EU:s oskuldspresumtionsdirektiv. Ju.
18. En nationell strategi för validering. U.
19. Uppdrag: Samverkan. Steg på vägen mot fördjupad lokal samverkan för unga arbetslösa. A.
20. Tillträde för nybörjare – ett öppnare och enklare system för tillträde till högskoleutbildning. U.
21. Läs mig! Nationell kvalitetsplan för vård och omsorg om äldre personer. Del 1 och 2. S.
22. Från värdekedja till värdecykel – så får Sverige en mer cirkulär ekonomi. M.
23. digitalforvaltning.nu. Fi.
24. Ett arbetsliv i förändring – hur påverkas ansvaret för arbetsmiljön? A.
25. Samlad kunskap – stärkt handläggning. S.
26. Delningsekonomi. På användarnas villkor. Fi.
27. Vissa frågor inom fastighets- och stämpelskatteområdet. Fi.
28. Ett nationellt centrum för kunskap om och utvärdering av arbetsmiljö. A.
29. Brottsdatalag. Ju
30. En omreglerad spelmarknad. Del 1 och 2. Fi.
31. Stärkt konsumentskydd på bostadsrättsmarknaden. Ju.
32. Substitution i Centrum – stärkt konkurrenskraft med kemikaliesmarta lösningar. M.
33. Stärkt ställning för hyresgäster. Ju.
34. Ekologisk kompensation – Åtgärder för att motverka nettoförluster av biologisk mångfald och ekosystemtjänster, samtidigt som behovet av markexploatering tillgodoses. M.
35. Samling för skolan. Nationell strategi för kunskap och likvärdighet. U.
36. Informationssäkerhet för samhällsviktiga och digitala tjänster. Ju.
37. Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra. Ju.

38. Kvalitet i välfärden – bättre upphandling och uppföljning. Fi.
39. Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning. Ju.
40. För dig och för alla. S.
41. Meddelarskyddslagen – fler verksamheter med stärkt meddelarskydd. Ju.
42. Vem har ansvaret? M.
43. På lika villkor! Delaktighet, jämlikhet och effektivitet i hjälpmedelsförsörjningen. S.
44. Entreprenad, fjärrundervisning och distansundervisning. U.
45. Ny lag om företagshemligheter. Ju.
46. Stärkt ordning och säkerhet i domstol. Ju.
47. Nästa steg på vägen mot en mer jämlik hälsa. Förslag för ett långsiktigt arbete för en god och jämlik hälsa. S.
48. Kunskapsbaserad och jämlik vård. Förutsättningar för en lärande hälso- och sjukvård. S.
49. EU:s dataskyddsförordning och utbildningsområdet. U.
50. Personuppgiftsbehandling för forskningsändamål. U.
51. Utbildning, undervisning och ledning – reformvård till stöd för en bättre skola. U.
52. Så stärker vi den personliga integriteten. Ju.
53. God och nära vård. En gemensam färdplan och målbild. S.
54. Fler nyanlända elever ska uppnå behörighet till gymnasiet. U.
55. En ny kamerabevakningslag. Ju.

Statens offentliga utredningar 2017

Systematisk förteckning

Socialdepartementet

För en god och jämlik hälsa. En utveckling av det folkhälsopolitiska ramverket. [4]

Svensk social trygghet i en globaliserad värld. Del 1 och 2.[5]

Kvalitet och säkerhet på apoteksmarknaden. [15]

Läs mig! Nationell kvalitetsplan för vård och omsorg om äldre personer. Del 1 och 2. [21]

Samlad kunskap – stärkt handläggning. [25]

För dig och för alla. [40]

På lika villkor! Delaktighet, jämlikhet och effektivitet i hjälpmedelsförsörjningen. [43]

Nästa steg på vägen mot en mer jämlik hälsa. Förslag för ett långsiktigt arbete för en god och jämlik hälsa. [47]

Kunskapsbaserad och jämlik vård. Förutsättningar för en lärande hälso- och sjukvård. [48]

God och nära vård. En gemensam färdplan och målbild. [53]

Utbildningsdepartementet

Det handlar om oss. – unga som varken arbetar eller studerar. [9]

Ny ordning för att främja god sed och hantera oredlighet i forskning. [10]

En nationell strategi för validering [18]

Tillträde för nybörjare – ett öppnare och enklare system för tillträde till högskoleutbildning. [20]

Samling för skolan. Nationell strategi för kunskap och likvärdighet. [35]

Entreprenad, fjärrundervisning och distansundervisning. [44]

EU:s dataskyddsförordning och utbildningsområdet. [49]

Personuppgiftsbehandling för forskningsändamål.[50]

Utbildning, undervisning och ledning – reformvård till stöd för en bättre skola. [51]

Fler nyanlända elever ska uppnå behörighet till gymnasiet. [54]

Utrikesdepartementet

Sverige i Afghanistan 2002–2014. [16]