

En omarbetad domstolsdatalag

Anpassning till EU:s dataskyddsförordning



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 Regeringskansliets förvaltningsavdelning.

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

Omslag: Regeringskansliets standard
Tryck: Elanders Sverige AB, Stockholm 2017

ISBN 978-91-38-24667-2

ISSN 0284-6012

Förord

Chefen för Justitiedepartementet beslutade den 9 september 2016 att ge mig i uppdrag att biträda Justitiedepartementet med att lämna förslag på de författningsändringar som behövs i domstolsdatalagen (2015:728) och domstolsdataförordningen (2015:729) med anledning av EU:s dataskyddsförordning. Jag fick även i uppdrag att ta ställning till om det finns behov av direktåtkomst för t.ex. Kammarkollegiet, länsstyrelserna, Naturvårdsverket och Havs- och vattenmyndigheten till den s.k. miljöbok som förs vid respektive mark- och miljödomstol och att lämna de författningsförslag som i så fall behövs. Uppdraget fick beteckningen Ju 2016:G.

Kammarrättsassessorn Nina Stierna har sedan den 1 oktober 2016 biträtt mig som sekreterare i uppdraget.

Utredningstiden har, genom beslut den 7 april 2017, förlängts till den 30 september 2017. Samtidigt har jag även fått tilläggsuppdrag som redovisas i andra promemorior än denna.

Vi får härmed överlämna promemorian *En omarbetad domstolsdatalag* (Ds 2017:41).

Uppdraget är med detta slutfört.

Jönköping i augusti 2017

Peder Liljeqvist

/Nina Stierna

Innehåll

Vissa förkortningar	15
Sammanfattning	17
1 Författningsförslag.....	23
1.1 Förslag till lag om ändring i domstolsdatalagen (2015:728)	23
1.2 Förslag till förordning om ändring i domstolsdataförordningen (2015:729).....	32
1.3 Förslag till förordning om ändring i förordningen (1998:1388) om vattenverksamhet m.m.....	36
1.4 Förslag till förordning om ändring i förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd	37
2 Uppdraget och dess genomförande.....	39
2.1 Uppdraget.....	39
2.2 Avgränsningar	39
2.3 Uppdragets genomförande.....	40
2.4 Promemorians disposition	41
3 Gällande rätt.....	43
3.1 FN.....	43
3.2 OECD	43
3.3 Europarådet	44

3.3.1	Europakonventionen	44
3.3.2	Dataskyddskonventionen	44
3.4	EU	45
3.4.1	Stadgan	45
3.4.2	Dataskyddsdirektivet och dataskyddsrambeslutet	45
3.5	Svensk rätt	46
3.5.1	Regeringsformen	46
3.5.2	Personuppgiftslagen	47
3.5.3	Domstolarnas personuppgiftsbehandling	47
4	Nya regelverk för personuppgiftsbehandling	51
4.1	EU:s dataskyddsreform	51
4.1.1	Dataskyddsförordningen	51
4.1.2	2016 års dataskyddsdirektiv	52
4.2	Två nya svenska regelverk	53
4.3	Avgränsning av domstolsdatalagens tillämpningsområde	54
4.3.1	Dataskyddsförordningen eller 2016 års dataskyddsdirektiv?	54
4.3.2	Bedömning	55
4.4	Vilket regelverk är tillämpligt?	57
5	Nationella registerförfattningar	59
5.1	Registerförfattningarnas förenlighet med dataskyddsförordningen	59
5.2	Allmänna principer för behandling av personuppgifter	61
5.3	Bedömning	62
6	Rättslig grund för domstolarnas personuppgiftsbehandling	65
6.1	Dataskyddslagen	66

6.2	Myndighetsutövning, uppgift av allmänt intresse eller rättslig förpliktelse?	67
6.2.1	Tidigare förarbeten	67
6.2.2	Uppgift av allmänt intresse	68
6.2.3	Myndighetsutövning	70
6.2.4	Rättslig förpliktelse	71
6.2.5	Bedömning.....	72
7	Lagens syfte och tillämpningsområde	77
7.1	Domstol.....	77
7.1.1	Dataskyddsförordningen	77
7.1.2	Hyres- och arrendenämnderna	77
7.1.3	Hyres- och arrendenämndernas rättsliga ställning	79
7.1.4	Bedömning.....	81
7.2	Rättskipande och rättsvårdande verksamhet.....	82
7.2.1	Domstolsdatalagen	82
7.2.2	Tidigare förarbeten	83
7.2.3	Offentlighets- och sekretesslagen	84
7.2.4	Rättegångsbalken.....	85
7.2.5	Ärendelagen	85
7.2.6	Innebörden av begreppet rättskipning	86
7.2.7	Innebörden av begreppet rättsvårdande verksamhet	87
7.2.8	Bedömning.....	89
7.3	Automatiserad behandling och manuella register.....	90
8	Dömande verksamhet.....	93
8.1	Nuvarande tillsyn över domstolarna.....	94
8.1.1	Datainspektionen	94
8.1.2	Justitieombudsmannen och Justitiekanslern	95
8.2	Dataskyddsförordningen och 2016 års dataskyddsdirektiv	96
8.2.1	Tolkningen av gemenskapsrättsliga bestämmelser	96

8.2.2	Olika språkliga versioner av dataskyddsförordningen	97
8.2.3	Skälen till dataskyddsförordningen och till 2016 års dataskyddsdirektiv.....	99
8.2.4	Europeiska datatillsynsmannens uppfattning.....	101
8.3	Andra rättsakter och EU-domstolens avgöranden	102
8.4	Bedömning.....	104
9	Ändamålsbestämmelser	109
9.1	Befintliga ändamålsbestämmelser	109
9.1.1	Rättslig reglering	109
9.1.2	Tidigare förarbeten	110
9.1.3	Ett uttryckligt angivet och tydligt ändamål.....	112
9.1.4	Finalitetsprincipen	113
9.1.5	Precisering av rättslig grund eller ändamålsbestämmelser?	114
9.1.6	Bedömning	115
9.2	Komplettering av ändamålsbestämmelserna.....	119
10	Förhållandet till annan lagstiftning	123
10.1	Förhållandet till personuppgiftslagen	123
10.2	Förhållandet till dataskyddsförordningen	124
10.3	Förhållandet till dataskyddslagen	126
10.4	Förhållandet till 2013 års lag.....	127
10.5	Förhållandet till kvarstadsförordningen	127
10.6	Befintliga hänvisningar till personuppgiftslagen och hänvisningar till dataskyddslagen	129
10.6.1	Definitioner	129
10.6.2	Förhållandet till offentlighetsprincipen.....	129
10.6.3	Grundläggande krav på behandling av personuppgifter	130
10.6.4	Behandling av personnummer och samordningsnummer	130
10.6.5	Information till den registrerade och rättelse	131

10.6.6	Säkerhet vid behandlingen	131
10.6.7	Överföring till tredje land	132
10.6.8	Personuppgiftsombud och förhandskontroll	132
10.6.9	Tillsynsmyndighetens handläggning och beslut	133
10.6.10	Skadestånd.....	138
10.6.11	Förhållandet till tryck- och yttrandefriheten	138
10.7	Sanktionsavgifter.....	139
11	Tillgången till personuppgifter	143
12	Personuppgiftsansvar	145
13	Dataskyddsombud	147
13.1	Dataskyddsförordningen.....	147
13.1.1	Möjlighet att föreskriva att dataskyddsombud ska utses	147
13.1.2	Dataskyddsombudets ställning, uppgifter m.m.....	148
13.2	1995 års dataskyddsdirektiv och personuppgiftslagen	150
13.3	Domstolsdatalagen	151
13.4	Domstolarnas uppfattning	153
13.5	Bedömning	154
13.5.1	Behovet av en analys.....	155
13.5.2	Dataskyddsombudet – ”internrevisor” med något utökat uppdrag	155
13.5.3	Dataskyddsombud även för den dömande verksamheten	157
13.5.4	Tystnadsplikt för dataskyddsombudet	161
13.5.5	Anmälan till tillsynsmyndigheten	161
13.5.6	Skyldighet att föra förteckning.....	162
14	Upplysningar till allmänheten	165
15	Den registrerades rättigheter.....	167

15.1	Inledande kommentar	167
15.2	En generell möjlighet till undantag	168
15.3	Information när personuppgifter samlas in från den registrerade.....	169
15.3.1	Domstolsdatalagen.....	169
15.3.2	Dataskyddsförordningen och dataskyddslagen ..	170
15.3.3	Bedömning	171
15.4	Information när personuppgifter samlas in från någon annan än den registrerade.....	173
15.4.1	Domstolsdatalagen.....	173
15.4.2	Dataskyddsförordningen.....	174
15.4.3	Bedömning	174
15.5	Information efter begäran.....	176
15.5.1	Domstolsdatalagen.....	176
15.5.2	Dataskyddsförordningen och dataskyddslagen ..	176
15.5.3	Bedömning	177
15.6	Rättelse och radering samt rätt att göra invändningar och begära begränsning av behandling.....	180
15.6.1	Domstolsdatalagen, personuppgiftslagen och 1995 års dataskyddsdirektiv.....	180
15.6.2	Dataskyddsförordningen.....	181
15.6.3	Bedömning	184
15.7	Rätt till skadestånd	190
15.7.1	Domstolsdatalagen och personuppgiftslagen.....	190
15.7.2	Dataskyddsförordningen.....	190
15.7.3	Dataskyddslagen	192
15.7.4	Bedömning	192
15.8	Information om personuppgiftsincident	194
15.8.1	Dataskyddsförordningen.....	194
15.8.2	Bedömning	194
16	Känsliga personuppgifter m.m.....	197
16.1	Dataskyddsförordningen och 1995 års dataskyddsdirektiv.....	197

16.2	Domstolsdatalagen	198
16.2.1	Rätten att behandla känsliga personuppgifter	198
16.2.2	Sökbegränsningar	200
16.3	Dataskyddslagen	201
16.4	2016 års dataskyddsdirektiv	202
16.5	Bedömning	203
16.5.1	Rätten att behandla känsliga personuppgifter	203
16.5.2	Huvudregel för behandling av känsliga personuppgifter	206
16.5.3	Begränsning av behandling av känsliga personuppgifter	208
16.5.4	Sökbegränsningar	209
17	Elektroniskt utlämnande	213
17.1	Proportionalitetsbedömning	213
17.2	Utlämnande på medium för automatiserad behandling	214
17.2.1	Domstolsdatalagen och tidigare förarbeten	214
17.2.2	Bedömning	216
17.3	Direktåtkomst	217
17.3.1	Innebörden av direktåtkomst	217
17.3.2	Domstolsdatalagen	219
17.3.3	Tidigare förarbeten	220
17.3.4	Bedömning	222
18	Överklagandebestämmelser	227
18.1	Domstolsdatalagen	227
18.2	Dataskyddsförordningen och stadgan	229
18.3	Dataskyddslagen	230
18.3.1	Överklagande av en myndighets beslut	231
18.3.2	Dröjsmålstalan	231
18.3.3	Överklagande av tillsynsmyndighetens beslut	232
18.3.4	Beslut om enskilt organs behandling för arkivändamål	233
18.3.5	Överklagandebestämmelserna är uttömmande ...	234

18.4	Bedömning.....	234
18.4.1	Överklagande av tillsynsmyndighetens beslut	235
18.4.2	Dröjsmålstalan.....	236
18.4.3	Överklagande av beslut som domstol fattar som personuppgiftsansvarig myndighet	237
18.4.4	Andra beslut får inte överklagas.....	238
19	Bevarande av personuppgifter	239
19.1	Domstolsdatalagen och personuppgiftslagen.....	239
19.2	Dataskyddsförordningen	241
19.3	Dataskyddslagen.....	243
19.4	Bedömning.....	244
19.4.1	Begreppet arkivändamål av allmänt intresse	245
19.4.2	Arkivering ingår i den rättskipande och rättsvårdande verksamheten	247
19.4.3	Komplettering av domstolsdatalagen.....	247
19.4.4	Personuppgifter som behandlats enligt brottsdatalagen och dess registerförfattning.....	249
19.4.5	Hänvisning till dataskyddslagen och säkerhetsåtgärder.....	250
20	Föreskriftsrätten	253
20.1	Domstolsdataförordningen	253
20.2	Bedömning.....	253
21	Andra myndigheters direktåtkomst till mark- och miljödomstolarnas miljöbok	255
21.1	Miljöboken – en översikt	255
21.1.1	Rättslig reglering och innehåll.....	255
21.1.2	Miljöboken innehåller personuppgifter.....	256
21.2	Direktåtkomst	257
21.3	Rättslig grund för behandling av personuppgifter i miljöboken	259
21.4	Vilka myndigheter är aktuella för direktåtkomst?	264

21.5	De aktuella myndigheternas verksamhet relaterat till miljöboken.....	265
21.5.1	Ansökan respektive anmälan om vattenverksamhet.....	265
21.5.2	Ansökan respektive anmälan om miljöfarlig verksamhet	266
21.5.3	Omprövning av tillstånd	267
21.5.4	Tillsyn och tillsynsvägledning.....	267
21.5.5	Samhällsplanering	269
21.6	De aktuella myndigheternas möjlighet till direktåtkomst	269
21.6.1	Proportionalitetsbedömning.....	269
21.6.2	Behovet av direktåtkomst	270
21.6.3	Avvägning mellan behovet och integritetsskyddet	274
21.7	Reglering av myndigheternas direktåtkomst	280
21.7.1	Direktåtkomsten ryms inte inom de primära ändamålen.....	280
21.7.2	Direktåtkomst är för närvarande inte förenlig med det sekundära ändamålet	281
21.7.3	En ny sekundär ändamålsbestämmelse?	281
21.7.4	Rättsligt stöd för utlämnandet av miljöbokens personuppgifter	282
21.7.5	Bestämmelserna om direktåtkomst bör kompletteras	284
22	Övergångs- och ikraftträdandebestämmelser.....	287
22.1	Två olika ikraftträdandedatum	287
22.2	Befintliga ikraftträdande- och övergångsbestämmelser.....	289
22.3	Pågående ärenden.....	290
22.4	Beslut som har meddelats före ikraftträdandet.....	291
22.5	Skada som har orsakats före ikraftträdandet.....	294
22.6	Sanktioner mot överträdelser som har skett före ikraftträdandet.....	295

23	Konsekvenser av förslagen	297
23.1	Inledning	297
23.2	Tillsynsmyndighetens handläggning och beslut samt sanktionsavgifter.....	298
23.3	Dataskyddsbud.....	299
23.4	Andra myndigheters direktåtkomst till miljöboken	300
24	Författningskommentar	303
24.1	Förslaget till lag om ändring av domstolsdatalagen (2015:728)	303
24.2	Förslaget till förordning om ändring i domstolsdataförordningen (2015:729)	310
24.3	Förslaget till förordning om ändring i förordningen (1998:1388) om vattenverksamhet m.m.	312
24.4	Förslaget till förordning om ändring i förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd	313
Bilaga 1	Uppdraget.....	315
Bilaga 2	Konsoliderade versioner av domstolsdatalagen och domstolsdataförordningen enligt våra förslag.....	319
Bilaga 3	Europaparlamentets och rådets förordning (EU) 2016/679	331

Vissa förkortningar

1995 års dataskyddsdirektiv	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
2016 års dataskyddsdirektiv	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
a.a.	anfört arbete
a.prop.	anförd proposition
dataskyddsförordningen	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)

dir.	direktiv
Ds	Departementsserien
EDPS	Europeiska datatillsynsmannen
EU	Europeiska unionen
EU-domstolen	Europeiska unionens domstol/ Europeiska gemenskapernas domstol
Europadomstolen	Europeiska domstolen för de mänskliga rättigheterna
Europakonventionen	Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna
f./ff.	följande sida/sidor
FN	Förenta nationerna
HFD	Högsta förvaltningsdomstolens årsbok
JK	Justitiekanslern
JO	Justitieombudsmannen/Riksdagens ombudsmän
MB	Miljöbalken
MSB	Myndigheten för samhällsskydd och beredskap
NJA	Nytt juridiskt arkiv
OECD	Organisationen för ekonomiskt samarbete och utveckling
OSL	Offentlighets- och sekretesslagen (2009:400)
prop.	regeringens proposition
PuL	Personuppgiftslagen (1998:204)
RF	Regeringsformen
RÅ	Regeringsrättens årsbok
SOU	Statens offentliga utredningar
TF	Tryckfrihetsförordningen

Sammanfattning

Anpassningar till EU:s dataskyddsförordning

EU:s dataskyddsreform innebär att en ny dataskyddsförordning¹ kommer att utgöra grunden för generell personuppgiftsbehandling inom EU från och med den 25 maj 2018. Reformen omfattar även ett nytt direktiv med särregler för den personuppgiftsbehandling som utförs av behöriga myndigheter för bl.a. brottsbekämpning, lagföring och straffverkställighet.² Denna promemoria innehåller förslag till de författningsändringar som behövs i domstolsdatalagen (2015:728) och domstolsdataförordningen (2015:729) med anledning av dataskyddsförordningen.

Tillämpningsområdet

Domstolsdatalagen omfattar för närvarande både sådan personuppgiftsbehandling som kommer att omfattas av dataskyddsförordningens tillämpningsområde och sådan som kommer att omfattas av det nya direktivets tillämpningsområde. För att anpassa domstolsdatalagen till det nya regelverket för personuppgiftsbehandling föreslår vi att lagen endast ska gälla för sådan behandling av personuppgifter som omfattas av dataskyddsförordningens tillämpningsområde. I övrigt innebär vårt förslag att lagens tillämpningsområde ska kvarstå oförändrat, med undantag

¹ Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för enskilda 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).

² 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.

för den bestämmelse som reglerar förhållandet till lag (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen, som ska upphävas.

Dataskyddsförordningen ska tillämpas i Sverige som om den vore nationell rätt, men hindrar inte förekomsten av nationella registerförfattningar. Dessa kommer framöver dock endast att utgöra en komplettering till dataskyddsförordningen, vilket enligt vårt förslag ska klargöras i domstolsdatalagen.

Grundläggande bestämmelser

Den rättsliga grunden för den personuppgiftsbehandling som utförs inom domstolsdatalagens tillämpningsområde utgörs enligt vår bedömning av att behandlingen är nödvändig för att fullgöra en rättslig förpliktelse, för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning.

Någon förändring av lagens befintliga ändamålsbestämmelser föranleds enligt vår mening inte av dataskyddsförordningen. Vi föreslår dock en komplettering av dessa bestämmelser i två avseenden. För det första ska det klargöras att personuppgifter som behandlas eller har behandlats för handläggning av mål och ärenden ska få behandlas också om det behövs för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål, förutsatt att de säkerhetsåtgärder som framgår av artikel 89.1 i dataskyddsförordningen vidtas. För det andra ska även personuppgifter som behandlas eller har behandlats med stöd av de författningar som genomför 2016 års dataskyddsdirektiv få behandlas för det nyss nämnda ändamålet samt om det behövs för att fullgöra uppgiftslämnande som sker i enlighet med lag eller förordning. De sistnämnda kompletteringarna har sin grund i att sådan behandling av personuppgifter omfattas av dataskyddsförordningen och inte av 2016 års dataskyddsdirektiv.

Begreppet *dömande verksamhet* förekommer i olika sammanhang i dataskyddsförordningen. Som exempel kan nämnas att de nationella tillsynsmyndigheterna inte kommer att vara behöriga att utöva tillsyn över domstolar som behandlar personuppgifter i sin dömande verksamhet och att den personuppgiftsbehandling som

genomförs som en del av domstolarnas dömande verksamhet är undantagen från myndigheters skyldighet att utse dataskyddsombud (i dag kallat personuppgiftsombud).

Dataskyddsförordningens begrepp *dömande verksamhet* är unionsrättsligt och innefattar enligt vår bedömning sannolikt all den personuppgiftsbehandling som utförs i det enskilda målet eller ärendet från att detta anhängiggörs vid domstolen tills ett slutligt avgörande har meddelats. Utifrån den bedömningen omfattas en stor del av, men inte hela, den personuppgiftsbehandling som sker inom domstolsdatalagens tillämpningsområde av begreppet. Detta medför en gränsdragningsproblematik, som kommer att få betydelse för regelverket kring domstolarnas personuppgiftsbehandling. Exempelvis kommer frågor om tillsynsmyndighetens behörighet att utfärda förelägganden mot domstolarna eller att påföra dem administrativa sanktionsavgifter att avgöras utifrån var gränsen för den dömande verksamheten går. För att bl.a. kompensera tillsynsmyndighetens begränsade behörighet och skapa ett ytterligare skydd för de registrerades personliga integritet föreslår vi att domstolarna, trots dataskyddsförordningens undantag för den dömande verksamheten, även fortsättningsvis ska utse ett eller flera ombud som har hela den rättskipande och rättsvårdande verksamheten som sitt ansvarsområde.

Övriga materiella bestämmelser

Till stora delar föranleder dataskyddsförordningen ingen ändring av domstolsdatalagen. Exempelvis kommer bestämmelserna om behörighetsbegränsningar, personuppgiftsansvar, utlämnande av personuppgifter på medium för automatiserad behandling och direktåtkomst att kunna kvarstå oförändrade. Även vad gäller domstolarnas behandling av känsliga personuppgifter kan nuvarande bestämmelser finnas kvar i princip oförändrade. Dock bör dessa bestämmelser anpassas så att definitionen av känsliga personuppgifter överensstämmer med dataskyddsförordningens begrepp, där sexuell läggning, genetiska uppgifter och biometriska uppgifter för att entydigt identifiera en fysisk person har tillkommit.

När dataskyddsförordningen börjar tillämpas ska personuppgiftslagen (1998:204) upphävas.³ I enlighet med vad som tidigare gällt i förhållande till personuppgiftslagen föreslår vi att domstolsdatalagen ska gälla i stället för den föreslagna lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (förkortad dataskyddslagen), som föreslås komplettera EU:s dataskyddsförordning på ett generellt plan i svensk rätt (se Dataskyddsutredningens betänkande [SOU 2017:39]). Det ska i domstolsdatalagen särskilt anges vilka bestämmelser i dataskyddslagen som ska gälla inom tillämpningsområdet.

Genom hänvisningar till dataskyddslagens bestämmelser kommer stora delar av den tidigare regleringen för personuppgiftsbehandling att behållas. Det gäller bl.a. domstolarnas rätt att behandla uppgifter om personnummer och samordningsnummer, begränsningen av den registrerades rätt till registerutdrag för uppgifter i löpande text eller minnesanteckningar och rätten för domstolarna att återanvända personuppgifter i arkiverade mål och ärenden. Även de undantag som för närvarande finns från den registrerades rätt till information vid insamling av personuppgifter samt från rätten till ett s.k. registerutdrag kommer på detta sätt att upprätthållas.

Dataskyddsförordningen innehåller bestämmelser som i vissa fall ger den registrerade rätt till information om en inträffad personuppgiftsincident. För att säkerställa att den registrerade inte genom sådan information får del av uppgifter som det råder sekretess för gentemot honom eller henne, föreslår vi att det införs ett undantag från denna rättighet. Undantaget ska gälla om den personuppgiftsansvarige, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämna ut uppgifter till den registrerade. De undantag från dataskyddsförordningens bestämmelser om den registrerades rättigheter som vi föreslagit får – tillsammans med de undantag som finns i dataskyddsförordningen – till följd att domstolarnas verksamhet kan fortgå även om den registrerade utnyttjar sina rättigheter enligt dataskyddsförordningen. Handläggning av enskilda mål eller ärenden behöver inte avstanna, bevarande och arkivering av processmaterialet kommer att vara möjlig,

³ Se kommittédirektiv till Dataskyddsutredningen (Dir. 2016:15 s. 6).

personuppgifter i avslutade och arkiverade mål och ärenden kan fortsätta behandlas och allmänhetens tillgång till allmänna handlingar inskränks inte.

Tillsyn och överklagande

Dataskyddsförordningen och förslaget till dataskyddslag kommer att förändra systemet för sanktioner vid otillåten personuppgiftsbehandling. Vi föreslår att dataskyddslagens bestämmelser om administrativa sanktionsavgifter mot myndigheter ska gälla även för domstolarna i tillämpliga delar. Detsamma gäller för dataskyddslagens bestämmelser om tillsynsmyndighetens handläggning och beslut. Genom en hänvisning till dataskyddslagen ska det även klargöras att den rätt till skadestånd för registrerade som framgår av dataskyddsförordningen även gäller vid överträdelser av dataskyddslagens (i tillämpliga delar) och domstolsdatalagens bestämmelser.

Domstolsdatalagen ska alltså innehålla uttömmande överklagandebestämmelser för tillämpningsområdet. Det kommer att finnas en rätt att överklaga tillsynsmyndighetens beslut, exempelvis vad gäller administrativa sanktionsavgifter eller besked om handläggningen av ett klagomål. Detsamma gäller de beslut som domstolarna fattat i egenskap av personuppgiftsansvariga myndigheter. För dessa överklaganden ska även fortsättningsvis en speciell instansordning gälla för samtliga domstolar utom hyres- och arrendenämnderna.

Direktåtkomst till miljöboken

I vårt uppdrag ingår att ta ställning till t.ex. Kammarkollegiets, länsstyrelsernas, Naturvårdsverkets och Havs- och vattenmyndighetens behov av direktåtkomst till den s.k. miljöbok som förs vid respektive mark- och miljödomstol. Vi har i denna analys även inkluderat Myndigheten för samhällsskydd och beredskap och kommunernas miljönämnder, som har liknande uppgifter på miljöskyddsområdet. Vår bedömning är att de fördelar som direktåtkomst till miljöboken skulle medföra – bl.a. effektivisering och ett upprätthållt skydd för miljön i tillståndsprocessen –

överväger de begränsade integritetsrisker som åtkomsten innebär. Vi föreslår därför att mark- och miljödomstolarna ska få möjlighet att ge de aktuella myndigheterna sådan direktåtkomst.

För att bl.a. säkerställa att det finns en rättslig grund enligt dataskyddsförordningen för förandet av miljöboken föreslår vi kompletteringar i förordningen (1998:1388) om vattenverksamhet m.m. och förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd. Vi föreslår vidare att den aktuella direktåtkomsten ska möjliggöras genom att dessa båda förordningar kompletteras med en skyldighet för mark- och miljödomstolarna att efter begäran lämna ut uppgifter i miljöboken till de aktuella myndigheterna. På så sätt kan den personuppgiftsbehandling som myndigheternas direktåtkomst till miljöboken innebär utföras med stöd av domstolsdatalagens befintliga sekundära ändamålsbestämmelse, eftersom behandlingen behövs för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

För att skapa ett ytterligare integritetsskydd föreslår vi att det i domstolsdataförordningen förtydligas att myndigheternas direktåtkomst till miljöboken ska omfatta samma typer av personuppgifter som bl.a. Högsta domstolens och Mark- och miljööverdomstolens direktåtkomst till miljöboken.

1 Författningsförslag

1.1 Förslag till lag om ändring i domstolsdatalagen (2015:728)

Härigenom föreskrivs i fråga om domstolsdatalagen (2015:728)
dels att 12 § ska upphävas,
dels att rubrikerna närmast före 4 och 12 §§ ska utgå,
dels att 2–5, 7, 10, 11, 13, 14, 17, 19, 20 och 22 §§ samt rubrikerna närmast före 10 och 11 §§ ska ha följande lydelse,
dels att det ska införas fyra nya paragrafer, 3 a, 5 a, 17 a och 19 a §§, och närmast före 3 a § en ny rubrik av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Denna lag gäller vid behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och hyres- och arrendenämndernas rättsskipande och rättsvårdande verksamhet. Lagen gäller också när personuppgifterna vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran.

2 §
Om inte annat anges i 3 §, gäller denna lag vid behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och hyres- och arrendenämndernas rättsskipande och rättsvårdande verksamhet. Lagen gäller också när personuppgifterna vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran.

Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är

tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

3 §¹

De avvikande bestämmelser som finns i lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polis-samarbete och straffrättsligt samarbete inom Europeiska unionen eller i föreskrifter som regeringen har meddelat i anslutning till den lagen, ska tillämpas i stället för bestämmelserna i denna lag. Detsamma gäller i fråga om Europaparlamentets och rådets förordning (EU) nr 655/2014 av den 15 maj 2014 om inrättande av ett europeiskt förfarande för kvarstad på bankmedel för att underlätta gränsöverskridande skuldindrivning i mål och ärenden av privaträttslig natur.

Denna lag gäller inte vid behandling av personuppgifter i de allmänna domstolarnas och de allmänna förvaltningsdomstolarnas verksamhet som omfattas av brottsdatalogens (2018:xx) tillämpningsområde.

Förhållandet till annan lagstiftning

3 a §

Denna lag innehåller kompletterande bestämmelser till 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

¹ Senaste lydelse 2016:759.

uppgifter och om upphävande av direktiv 95/46/EG.

4 §

Om inte något annat anges i 5 §, gäller denna lag i stället för *personuppgiftslagen (1998:204)*.

Om inte något annat anges i 5 §, gäller denna lag i stället för *lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (2018:xx)*.

5 §²

När personuppgifter behandlas enligt denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller följande bestämmelser i *personuppgiftslagen (1998:204)*:

1. 3 § om definitioner,
2. 8 § om förhållandet till offentlighetsprincipen,
3. 9 § om grundläggande krav på behandling av personuppgifter,
4. 22 § om behandling av personnummer,
5. 23 och 25–27 §§ om information till den registrerade,
6. 28 § om rättelse,
7. 30 och 31 §§ samt 32 § första stycket om säkerheten vid behandling,
8. 33–35 §§ om överföring av personuppgifter till tredjeland,
9. 38, 40 och 41 §§ om personuppgiftsombud m.m.,
10. 43 och 44 §§, 45 § första stycket och 47 § om tillsynsmyndighetens befogenheter, och

När personuppgifter behandlas enligt denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller följande bestämmelser i *lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (2018:xx)*:

1. 1 kap. 4 § första stycket om förhållandet till tryck- och yttrandefriheten,
2. 3 kap. 13 § om behandling av personnummer och samordningsnummer,
3. 4 kap. 1 § om användningsbegränsningar för arkiverade personuppgifter,
4. 5 kap. 1 § första stycket och 5 kap. 2 § om begränsning av vissa rättigheter och skyldigheter,
5. 6 kap. 1–5 §§ om tillsynsmyndighetens handläggning och beslut,
6. 7 kap. 1, 3 och 4 §§ om administrativa sanktionsavgifter, och

² Ändringen innebär bl.a. att andra stycket tas bort.

11. 48 § om skadestånd.

7. 8 kap. 1 § om skadestånd.

Förbud enligt 44 eller 45 § personuppgiftslagen får inte förenas med vite.

5 a §

De avvikande bestämmelser som finns i Europaparlamentets och rådets förordning (EU) nr 655/2014 av den 15 maj 2014 om inrättande av ett europeiskt förfarande för kvarstad på bankmedel för att underlätta gränsöverskridande skuldindrivning i mål och ärenden av privaträttslig natur, ska tillämpas i stället för bestämmelserna i denna lag.

7 §

Personuppgifter som behandlas enligt 6 § får även behandlas om det behövs för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

Personuppgifter som behandlas eller har behandlats enligt 6 § får även behandlas om det behövs

1. för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning, eller

2. för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i Europaparlamentets och rådets förordning (EU) 2016/679.

Personuppgifter får även behandlas för de ändamål som framgår av första stycket när de

behandlas eller har behandlats med stöd av brottsdatalagen (2018:xx) eller [namnet på den registerförfattning som kompletterar brottsdatalagen för domstolarnas verksamhet] (2018:xx).

Personuppgiftsombud

Dataskyddsbud

10 §³

Den personuppgiftsansvarige ska utse ett eller flera personuppgiftsombud.

Den personuppgiftsansvarige ska utse ett eller flera dataskyddsbud.

Den personuppgiftsansvarige ska anmäla till tillsynsmyndigheten enligt personuppgiftslagen (1998:204) när ett personuppgiftsombud utses eller entledigas.

Förteckning över personuppgiftsbehandlingar

Begränsningar av vissa rättigheter och skyldigheter

11 §

Den som är personuppgiftsombud ska föra en förteckning över de behandlingar som utförs med stöd av denna lag.

Bestämmelserna om den registrerades rätt att få information om en personuppgiftsincident enligt artikel 34 i Europaparlamentets och rådets förordning (EU) 2016/679, gäller inte om den personuppgiftsansvarige, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämna ut uppgifter till den registrerade.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om vilka uppgifter en sådan förteckning ska innehålla.

³ Ändringen innebär bl.a. att andra stycket tas bort.

13 §

Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om *personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.*

Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om *personen genom sådana särskilda kategorier av uppgifter som anges i artikel 9.1 i Europaparlamentets och rådets förordning (EU) 2016/679 (känsliga personuppgifter).*

14 §

Vid sökning i personuppgifter är det förbjudet att *som sökbegrepp använda uppgifter som avslöjar*

1. *ras eller etniskt ursprung,*
2. *politiska åsikter,*
3. *religiös eller filosofisk övertygelse,*
4. *medlemskap i fackförening,*
5. *hälsa,*
6. *sexualliv,*
7. *nationell anknytning, eller*
8. *brott eller misstanke om*

brott.

Vid sökning i personuppgifter är det förbjudet att *använda sökbegrepp som avslöjar känsliga personuppgifter enligt 13 §, uppgifter om nationell anknytning eller uppgifter om brott eller misstanke om brott.*

Användning av särskilda beteckningar för identifiering av en viss mål- eller ärendetyp som sökbegrepp omfattas inte av förbudet i första stycket.

17 §

Direktåtkomst får endast medges

1. en allmän domstol,
2. en allmän förvaltningsdomstol,
3. en hyres- och arrendenämnd, *eller*
4. en part eller partens ombud, biträde eller försvarare.

3. en hyres- och arrendenämnd,
4. en part eller partens ombud, biträde eller försvarare, *eller*

5. Havs- och vattenmyndigheten, Kammarkollegiet, länsstyrelserna, Myndigheten för samhällsskydd och beredskap, Naturvårdsverket och de kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet.

Direktåtkomst enligt första stycket 4 får endast avse personuppgifter i partens mål eller ärende.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar av direktåtkomst enligt första stycket och om behörighet och säkerhet vid sådan åtkomst.

17 a §

Direktåtkomst enligt 17 § 4 får endast avse personuppgifter i partens mål eller ärende.

Direktåtkomst enligt 17 § 5 får endast avse personuppgifter i den förteckning som förs över en mark- och miljödomstols avgöranden i frågor som rör miljöbalken eller lagen (1998:812) med särskilda bestämmelser om vattenverksamhet (miljöboken).

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om

begränsningar av direktåtkomst enligt 17 § och om behörighet och säkerhet vid sådan åtkomst.

19 §

Tillsynsmyndighetens beslut enligt denna lag eller enligt de bestämmelser i personuppgiftslagen (1998:204) som anges i 5 § om annat än föreskrifter får överklagas till allmän förvaltningsdomstol. Prövnings- tillstånd krävs vid överklagande till kammarrätten.

Tillsynsmyndighetens beslut enligt Europaparlamentets och rådets förordning (EU) 2016/679 och enligt 7 kap. 1 § lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

19 a §

Tillsynsmyndighetens beslut att avslå en begäran om besked enligt 6 kap. 5 § lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning får 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 får inte överklagas.

20 §

En hovrätts, tingsrätts eller förvaltningsrätts beslut om upplysningar enligt 12 § eller om information till den registrerade

En hovrätts, tingsrätts eller förvaltningsrätts beslut om registrerades rättigheter enligt artiklarna 12.5, 15–19 och 21 i

enligt 26 § personuppgiftslagen (1998:204) och om rättelse och underrättelse till tredje man enligt 28 § samma lag får överklagas till kammarrätten. En kammarrätts beslut i sådana frågor får överklagas till Högsta förvaltningsdomstolen. Europaparlamentets och rådets förordning (EU) 2016/679, får överklagas till kammarrätt. En kammarrätts beslut i sådana frågor får överklagas till Högsta förvaltningsdomstolen.

Högsta domstolens och Högsta förvaltningsdomstolens beslut i frågor som avses i första stycket får inte överklagas.

22 §⁴

Andra beslut än sådana som avses i 19–21 §§ eller i 47 § personuppgiftslagen (1998:204) får inte överklagas. Andra beslut än sådana som avses i 19–21 §§ får inte överklagas.

Vid överklagande av förvaltningsrättens beslut i frågor som avses i 47 § personuppgiftslagen krävs prövningstillstånd vid överklagande till kammarrätten.

1. Denna lag träder i kraft den 1 maj 2018 i fråga om 3 och 5 a §§ och i övrigt den 25 maj 2018.

2. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats med stöd av de föreskrifterna.

⁴ Ändringen innebär bl.a. att andra stycket tas bort.

1.2 Förslag till förordning om ändring i domstolsdataförordningen (2015:729)

Härigenom föreskrivs i fråga om domstolsdataförordningen (2015:729)

dels att 3–5 och 14 §§ ska ha följande lydelse,

dels att det ska införas en ny paragraf, 11 b §, av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Användningen i allmän domstol enligt 15 § första stycket 1 domstolsdatalagen (2015:728) av sökbegrepp som avslöjar brott eller misstanke om brott får inte avse sökning i personuppgifter i tvistemål. *Användningen av sådana sök- begrepp får inte heller avse sökning i personuppgifter i mål eller ärenden som har avgjorts slutligt genom en dom eller ett beslut fem år efter utgången av det kalenderår då avgörandet fick laga kraft.*

3 §

Användningen i allmän domstol enligt 15 § första stycket 1 domstolsdatalagen (2015:728) av sökbegrepp som avslöjar brott eller misstanke om brott, får inte avse sökning i personuppgifter i tvistemål.

I mål eller ärenden som har avgjorts slutligt får användningen av sådana sökbegrepp inte heller avse sökning i personuppgifter fem år efter utgången av det kalenderår då avgörandet fick laga kraft.

4 §

Personnamn, personnummer,

Vid sökning i personuppgifter i

samordningsnummer och andra uppgifter som direkt kan hänföras till en fysisk person som är i livet får inte användas som sökbegrepp vid sökning i personuppgifter i brottmål som har avgjorts slutligt genom en dom eller ett beslut fem år efter utgången av det kalenderår då avgörandet fick laga kraft.

brottmål som har avgjorts slutligt genom en dom eller ett beslut får personnamn, personnummer, samordningsnummer och andra uppgifter som direkt kan hänföras till en fysisk person som är i livet inte användas som sökbegrepp fem år efter utgången av det kalenderår då avgörandet fick laga kraft.

5 §

Användningen i allmän förvaltningsdomstol enligt 15 § första stycket 2 domstolsdatalagen (2015:728) av sökbegrepp som avslöjar hälsa, brott eller misstanke om brott får inte avse sökning i personuppgifter i mål som handläggs av Migrationsöverdomstolen eller av en migrationsdomstol.

Användningen av sådana sökbegrepp får inte heller avse sökning i personuppgifter i mål som har avgjorts slutligt genom en dom eller ett beslut tjugo år efter utgången av det kalenderår då avgörandet fick laga kraft.

Användningen i allmän förvaltningsdomstol enligt 15 § första stycket 2 domstolsdatalagen (2015:728) av sökbegrepp som avslöjar hälsa, brott eller misstanke om brott får inte avse sökning i personuppgifter i mål som handläggs av Migrationsöverdomstolen eller av en migrationsdomstol.

I mål eller ärenden som har avgjorts slutligt får användningen av sådana sökbegrepp inte heller avse sökning i personuppgifter tjugo år efter utgången av det kalenderår då avgörandet fick laga kraft.

11 b §

Direktåtkomst enligt 11 a § får även medges de myndigheter som anges i 17 § 5 domstolsdatalagen.

14 §

Domstolsverket får meddela närmare föreskrifter om tillgången till personuppgifter. För tilldelning av behörighet för tillgång till personuppgifter ska det särskilt beaktas att det utöver behovet av uppgifterna ställs krav på utbildning och erfarenhet.

Domstolsverket får även meddela

1. ytterligare föreskrifter om vilka uppgifter som en förteckning enligt 11 § domstolsdatalagen (2015:728) ska innehålla,

2. föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter på medium för automatiserad behandling,

3. ytterligare föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter genom direktåtkomst och om behörighet och säkerhet vid sådant utlämnande,

4. ytterligare föreskrifter om begränsningar för behandling av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts slutligt genom en dom eller ett beslut som har fått laga kraft, och

5. de ytterligare föreskrifter som behövs för verkställighet av domstolsdatalagen (2015:728) och denna förordning.

1. föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter på medium för automatiserad behandling,

2. ytterligare föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter genom direktåtkomst och om behörighet och säkerhet vid sådant utlämnande,

3. ytterligare föreskrifter om begränsningar för behandling av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts slutligt genom en dom eller ett beslut som har fått laga kraft, och

4. de ytterligare föreskrifter som behövs för verkställighet av domstolsdatalagen (2015:728) och denna förordning.

Denna förordning träder i kraft den 25 maj 2018.

1.3 Förslag till förordning om ändring i förordningen (1998:1388) om vattenverksamhet m.m.

Härigenom föreskrivs att 8 § förordningen (1998:1388) om vattenverksamhet m.m. ska ha följande lydelse.

8 §¹

Mark- och miljödomstolens förteckning över vattenverksamheter inom domsområdet ska föras i en miljöbok som en vattenbok ska ingå i.

Domstolsverket får meddela föreskrifter om *miljöboken*.

En mark- och miljödomstol ska föra en miljöbok. I denna ska domstolens förteckning över vattenverksamheter inom domsområdet (vattenbok) ingå.

Domstolsverket får meddela föreskrifter om *vattenboken*.

Mark- och miljödomstolarna är skyldiga att efter begäran lämna ut uppgifter i vattenboken till Havs- och vattenmyndigheten, Kammarkollegiet, länsstyrelserna, Myndigheten för samhällsskydd och beredskap, Naturvårdsverket och de kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet.

Denna förordning träder i kraft den 25 maj 2018.

¹ Senaste lydelse 2010:961.

1.4 Förslag till förordning om ändring i förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd

Härigenom föreskrivs att det i förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd ska införas en ny paragraf, 48 a §, och närmast före 48 a § en ny rubrik av följande lydelse.

Miljöbok

48 a §

En mark- och miljödomstol ska i den miljöbok som avses i 8 § förordningen (1998:1388) om vattenverksamhet m.m. föra en förteckning över avgöranden som rör miljöfarlig verksamhet enligt miljöbalken och som domstolen meddelar som första instans.

Domstolsverket får meddela föreskrifter om förteckningen.

Mark- och miljödomstolarna är skyldiga att efter begäran lämna ut uppgifter i förteckningen till Havs- och vattenmyndigheten, Kammarkollegiet, länsstyrelserna, Myndigheten för samhällsskydd och beredskap, Naturvårdsverket och de kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet.

Denna förordning träder i kraft den 25 maj 2018.

2 Uppdraget och dess genomförande

2.1 Uppdraget

Mitt uppdrag är att lämna förslag på de författningsändringar som behövs i domstolsdatalagen (2015:728) och domstolsdataförordningen (2015:729) med anledning av EU:s dataskyddsförordning¹. Jag ska även ta ställning till om det finns behov av direktåtkomst för t.ex. Kammarkollegiet, länsstyrelserna, Naturvårdsverket och Havs- och vattenmyndigheten till den s.k. miljöbok som förs vid respektive mark- och miljödomstol. Enligt uppdragsbeskrivningen ska jag lämna fullständiga författningsförslag utifrån de överväganden som görs. Jag ska även belysa vilka konsekvenser de föreslagna ändringarna bedöms få. Om förslagen förväntas leda till kostnadsökningar för det allmänna, ska jag föreslå hur dessa ska finansieras. Den fullständiga uppdragsbeskrivningen framgår av *bilaga 1*.

Med anledning av tilläggsuppdrag, som inte är av relevans för denna promemoria, har uppdraget förlängts och ska redovisas senast den 30 september 2017.

2.2 Avgränsningar

Det ligger inte inom uppdraget att presentera en heltäckande redogörelse för dataskyddsförordningens bestämmelser eller skillnaderna mellan det gamla och det nya regelverket för

¹ Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för enskilda 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).

personuppgiftsbehandling. Eventuella tillämpningsproblem som uppstått till följd av den nuvarande utformningen av domstolsdatalagen ligger inte heller inom ramen för uppdraget och kan på grund av den tidsmässiga aspekten inte behandlas av oss.

Utredningen om 2016 års dataskyddsdirektiv (Ju 2016:06) har vidare i uppdrag att lämna förslag till de författningsförändringar som krävs för att genomföra Europaparlamentets och rådets direktiv (EU) 2016/680 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. Den utredningen ska även föreslå de anpassningar som krävs i domstolsdatalagen och domstolsdataförordningen med anledning av det nya direktivet. Dessa frågor behandlas således inte av oss. Däremot har vi i vår promemoria i vissa avseenden analyserat möjligheten att anpassa den reglering vi föreslår till de författningsförslag som Utredningen om 2016 års dataskyddsdirektiv lämnar. Detta har i sådant fall skett i ett försök att skapa enhetlighet i domstolarnas personuppgiftsbehandling.

2.3 Uppdragets genomförande

Utredningsarbetet har bedrivits på sedvanligt sätt, dock utan särskild expert- eller referensgrupp. I stället har samråd med Domstolsverket skett kontinuerligt under utredningstiden.

Vi har vidare ingått i en informell samordningsgrupp med andra utredningar som haft i uppdrag att anpassa svensk rätt till EU:s dataskyddsreform. Utöver detta samarbete har vi under utredningstiden löpande samrått med Utredningen om 2016 års dataskyddsdirektiv (Ju 2016:06).

Den del av arbetet som gäller direktåtkomst till miljöboken har vi samrått med medarbetare vid mark- och miljödomstolen vid Vänersborgs tingsrätt och vid Mark- och miljööverdomstolen. Vi har även haft möten med representanter från de berörda myndigheterna. Vad gäller länsstyrelserna har vi på grund av den korta utredningstiden fått begränsa oss till Länsstyrelsen i Skåne län, Länsstyrelsen i Västra Götalands län och Länsstyrelsen i

Stockholms län. Vi har också, genom ett utskick med riktade frågor, gett de nyssnämnda länsstyrelserna, Kammarkollegiet, Naturvårdsverket, Sveriges kommuner och landsting, Havs- och vattenmyndigheten samt Myndigheten för samhällsskydd och beredskap möjlighet att komma med synpunkter gällande behovet av direktåtkomst.

2.4 Promemorians disposition

Promemorian är indelad i 24 kapitel.

I kapitel 1 finns författningsförslagen. Kapitel 2 behandlar uppdraget och dess genomförande. I kapitel 3 redogör vi för gällande internationell och nationell rätt på personuppgiftsområdet.

EU:s dataskyddsreform och dess konsekvenser för domstolsdatalagen behandlas i kapitel 4. Därefter följer en bedömning av möjligheten att behålla eller införa nationella registerförfattningar (kapitel 5) och av vilken eller vilka av dataskyddförordningens s.k. rättsliga grunder som ger stöd för den personuppgiftsbehandling som utförs inom domstolsdatalagens tillämpningsområde (kapitel 6). I kapitel 7 behandlar vi domstolsdatalagens syfte och tillämpningsområde. Därefter gör vi, i kapitel 8, en analys och bedömning av det unionsrättsliga begreppet *dömande verksamhet*. Kapitel 9 innehåller en bedömning av domstolsdatalagens ändamålsbestämmelser och behovet av att komplettera dessa. Sedan följer i kapitel 10 våra överväganden av lagens förhållande till annan lagstiftning och hur dess befintliga hänvisningar till personuppgiftslagen (1998:204) ska hanteras. I kapitel 11 behandlar vi bestämmelserna om tillgång till personuppgifter för anställda m.fl. och i kapitel 12 personuppgiftsansvaret. Kapitel 13 innehåller våra överväganden vad gäller domstolarnas skyldighet att utse dataskyddsombud även för den dömande verksamheten. Våra överväganden vad gäller domstolsdatalagens bestämmelse om domstolarnas skyldighet att lämna upplysningar om sin personuppgiftsbehandling till allmänheten finns i kapitel 14. Därefter redogör vi, i kapitel 15, för de viktigaste förändringarna dataskyddsförordningen innebär för domstolarna vad gäller de registrerades rättigheter. Där gör vi också en analys av möjligheterna och behovet av att begränsa de registrerades

rättigheter i vissa fall. Vår bedömning av hur dataskyddsförordningens bestämmelser om behandling av känsliga personuppgifter påverkar domstolsdatalagen finns i kapitel 16. Därefter följer en bedömning av lagens bestämmelser om elektroniskt utlämnande av personuppgifter (kapitel 17). Förändringar av domstolsdatalagens överklagandebestämmelser behandlas i kapitel 18 och i kapitel 19 behandlas vilka förändringar som krävs för att bevarande och arkivering av personuppgifter fortsatt ska vara tillåtet inom domstolsdatalagens tillämpningsområde. Slutligen behandlas Domstolsverkets föreskriftsrätt i kapitel 20.

Kapitel 21 innehåller våra särskilda överväganden vad gäller andra myndigheters direktåtkomst till den s.k. miljöbok som förs vid respektive mark- och miljödomstol.

I kapitel 22 behandlar vi frågor om ikraftträdande- och övergångsbestämmelser och i kapitel 23 vilka konsekvenser som följer av våra förslag. I kapitel 24 finns en kort författningskommentar till de författningsändringar som föreslås.

För att läsaren ska få en bättre överblick över hur våra förslag påverkar domstolsdatalagstiftningens innehåll finns i *bilaga 2* en sammanställning av hur domstolsdatalagen och domstolsdataförordningen kommer att se ut i sin helhet om våra förslag genomförs (konsoliderade versioner). Slutligen finns dataskyddsförordningen bifogad som *bilaga 3*.

3 Gällande rätt

3.1 FN

Förenta Nationerna (FN) antog år 1948 den allmänna förklaringen om de mänskliga rättigheterna, som inte är formellt bindande för medlemsstaterna. Vidare har det inom FN utarbetats en internationell konvention om medborgerliga och politiska rättigheter, som trädde i kraft 1976. Sverige har anslutit sig till konventionen. I både den allmänna förklaringen och konventionen (artikel 12 respektive artikel 17) finns bestämmelser om rätten till skydd för enskildas privata sfär. Av artikel 29 i den allmänna förklaringen framgår vidare att en person vid utövandet av sina rättigheter och friheter endast får underkastas sådana inskränkningar som har fastställts i lag och enbart i syfte att trygga tillbörlig hänsyn till och respekt för andras rättigheter och friheter samt för att tillgodose ett demokratiskt samhälles berättigade krav på moral, allmän ordning och allmän välfärd.

FN:s generalförsamling antog år 1990 riktlinjer om datoriserade register med personuppgifter, som innehåller de grundläggande principer som medlemsstaterna ska ta hänsyn till vid lagstiftning avseende sådana register.

3.2 OECD

OECD:s (Organisationen för ekonomiskt samarbete och utveckling) råd antog år 1980 riktlinjer i fråga om integritetsskyddet och personuppgiftsflödet över gränserna. Samtidigt utfärdades en rekommendation till medlemsländernas regeringar om att beakta riktlinjerna i nationell lagstiftning. Riktlinjerna gäller för både privat och offentlig sektor, de ska uppfattas som minimiregler och de motsvarar i princip de bestämmelser som finns

i Europarådets dataskyddskonvention. Samtliga medlemsländer har åtagit sig att följa riktlinjerna.

3.3 Europarådet

3.3.1 Europakonventionen

Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) gäller som lag i Sverige.¹ Av 2 kap. 19 § regeringsformen framgår också att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av konventionen.

Enligt artikel 8 i Europakonventionen har var och en rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Offentliga myndigheter får inte inskränka denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till den nationella säkerheten, den allmänna säkerheten, landets ekonomiska välbefinnande, förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter.

3.3.2 Dataskyddskonventionen

Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (dataskyddskonventionen) trädde i kraft år 1985. Samtliga EU:s medlemsstater har ratificerat konventionen, som är bindande.

Konventionen innehåller grundläggande principer för dataskydd som de konventionsanslutna staterna ska beakta i sin nationella lagstiftning. Syftet med konventionen är att säkerställa rätten till personlig integritet i samband med automatiserad behandling av personuppgifter. Personuppgifterna ska enligt konventionen inhämtas och behandlas på ett korrekt sätt och de ska vara relevanta med hänsyn till ändamålet. Vissa kategorier av personuppgifter får inte behandlas genom automatiserad databehandling

¹ Lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.

om inte den nationella lagstiftningen ger ett ändamålsenligt skydd. Till sådana kategorier hör personuppgifter som avslöjar ras, politisk tillhörighet, religiös tro eller övertygelse i övrigt, sexualliv samt uppgifter om brott.

Utöver dataskyddskonventionen har det inom Europarådet utarbetats flera icke bindande rekommendationer på dataskyddsområdet.

3.4 EU

3.4.1 Stadgan

Europeiska unionens stadga om de grundläggande rättigheterna (stadgan) är en del av EU:s primärrätt och bindande för både EU:s institutioner och medlemsstaterna vid tillämpning av unionsrätten.²

I artikel 7 i stadgan anges att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Av artikel 8 i stadgan framgår att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Det framgår också att personuppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har också 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. Enligt artikel 47 i stadgan har var och en vars unionsrättsligt garanterade fri- och rättigheter har kränkts rätt till ett effektivt rättsmedel inför en domstol.

3.4.2 Dataskyddsdirektivet och dataskyddsrambeslutet

Den allmänna regleringen om behandling av personuppgifter inom EU finns för närvarande 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. Vi kommer fortsatt i denna promemoria att hänvisa till detta direktiv som *1995 års dataskyddsdirektiv*.

² Se artikel 61.1 i Lissabonfördraget och artikel 51 i stadgan.

Direktivets syfte är, enligt artikel 1.1, att garantera att medlemsstaterna skyddar fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter. Av artikel 1.2 framgår vidare att syftet är att främja ett fritt flöde av personuppgifter mellan medlemsstaterna i EU.

Behandling av personuppgifter på områden som faller eller tidigare föll utanför unionsrätten, till exempel allmän säkerhet och försvar samt statens verksamhet på straffrättens område, omfattas inte av 1995 års dataskyddsdirektiv. Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet) är, enligt artikel 1.2 i beslutet, tillämpligt på personuppgiftsbehandling i form av överföring mellan medlemsstaterna i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. Dataskyddsrambeslutet gäller dock inte för nationell personuppgiftsbehandling. Från tillämpningsområdet undantas också personuppgiftsbehandling inom området nationell säkerhet. Dataskyddsrambeslutet har genomförts i svensk rätt främst genom lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.

3.5 Svensk rätt

3.5.1 Regeringsformen

Enligt 2 kap. 6 § andra stycket regeringsformen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Skyddet får enligt 2 kap. 20 och 21 §§ regeringsformen begränsas genom lag, men endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av

folkstyrelsens grundvalar. Begränsningen får inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

3.5.2 Personuppgiftslagen

Sverige har genomfört 1995 års dataskyddsdirektiv främst genom personuppgiftslagen (1998:204), förkortad PuL. Lagen trädde i kraft den 24 oktober 1998 och har till syfte att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Lagen följer i princip samma struktur som 1995 års dataskyddsdirektiv och innehåller – liksom direktivet – bestämmelser om bland annat personuppgiftsansvar, grundläggande krav för behandling av personuppgifter och information till den registrerade. Personuppgiftslagen gäller för både myndigheter och enskilda som behandlar personuppgifter. Lagen är subsidiär, vilket innebär att dess bestämmelser inte ska tillämpas om det finns avvikande bestämmelser i en annan lag eller förordning. Det finns en stor mängd sådana bestämmelser i de sektorsspecifika s.k. registerförfattningar (eller informationshanteringsförfattningar³) som reglerar myndigheternas personuppgiftsbehandling.

Personuppgiftslagen kompletteras av bestämmelser i personuppgiftsförordningen (1998:1191), som bland annat pekar ut Datainspektionen som tillsynsmyndighet. Datainspektionen bemyndigas i förordningen att meddela närmare föreskrifter om bland annat i vilka fall behandling av personuppgifter är tillåten och vilka krav som ställs på den personuppgiftsansvarige.

3.5.3 Domstolarnas personuppgiftsbehandling

Vera-förordningarna

För myndigheters behandling av personuppgifter finns, som vi nyss nämnt, en stor mängd registerförfattningar. Syftet med dessa författningar är att anpassa personuppgiftsregleringen till de särskilda behov som myndigheterna har i sina respektive verksamheter samt att göra avvägningar mellan verksamhetens

³ Jfr Informationshanteringsutredningens betänkande (SOU 2015:39 s. 967 ff.).

behov av effektivitet och den enskildes rätt till skydd för sin integritet.

Domstolarnas behandling av personuppgifter reglerades tidigare till stor del av de s.k. Vera-förordningarna, som trädde i kraft den 1 oktober 2001. Dessa utgjordes av

- förordningen (2001:639) om registerföring m.m. vid allmänna domstolar med hjälp av automatiserad behandling,
- förordningen (2001:640) om registerföring m.m. vid förvaltningsrätt med hjälp av automatiserad behandling,
- förordningen (2001:641) om registerföring m.m. vid Högsta förvaltningsdomstolen och kammarrätterna med hjälp av automatiserad behandling, och
- förordningen (2001:642) om registerföring m.m. vid hyres- och arrendenämnder med hjälp av automatiserad behandling.

Vera-förordningarna tillkom som en provisorisk lösning för att tillgodose det behov av regler som uppstod då datalagen (1973:289) upphörde att gälla och personuppgiftslagen kom i dess ställe. De reglerade all automatiserad behandling av personuppgifter – i register eller på annat sätt – inom den rättskipande och rättsvårdande verksamheten vid domstolarna och hyres- och arrendenämnderna. Förordningarna innehöll detaljerade och uttömmande uppräknningar av vilka uppgifter som fick behandlas i domstolarnas och nämndernas register.

Domstolsdatalagen och domstolsdataförordningen

Eftersom regleringen i Vera-förordningarnas inte var teknikneutral behövdes det en översyn av regelverket.⁴ Översynen resulterade i domstolsdatalagen (2015:728) och domstolsdataförordningen (2015:729), vilka till övervägande del trädde i kraft den 1 januari 2016. Dessa författningar gäller vid behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och hyres- och arrendenämndernas rättskipande och rättsvårdande

⁴ Departementspromemoria med förslag till domstolsdatalag (Ds 2013:10 s. 40).

verksamhet. För läsbarvnlighetens skull kommer vi framöver i denna promemoria att med det generella begreppet domstolar även avse hyres- och arrendenämnderna, om inget annat anges.

Domstolsdatalagen och domstolsdataförordningen gäller även när personuppgifter i den rättskipande och rättsvårdande verksamheten vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran. Domstolsdatalagen gäller i stället för personuppgiftslagen, men innehåller hänvisningar till de bestämmelser i den lagen som ska gälla inom tillämpningsområdet.

4 Nya regelverk för personuppgiftsbehandling

4.1 EU:s dataskyddsreform

Europeiska kommissionen presenterade den 25 januari 2012 förslag till en genomgripande reform av EU:s regler om skydd för personuppgifter. Reformen omfattar dels en förordning som ersätter 1995 års dataskyddsdirektiv och dels ett nytt direktiv med särregler för personuppgiftsbehandling som utförs för bl.a. brottsbekämpning, lagföring och straffverkställighet.

4.1.1 Dataskyddsförordningen

Den 27 april 2016 antogs Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för enskilda 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). Den vedertagna förkortningen för förordningen är GDPR. I likhet med de flesta andra utredningar som nu ser eller har sett över svensk lagstiftning på detta område har vi dock valt att i vår promemoria som kortform för den nya rättsakten använda oss av *dataskyddsförordningen*.

Av skäl 13 till dataskyddsförordningen framgår att syftet med förordningen bl.a. är att säkerställa en enhetlig skyddsnivå över hela unionen och att undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden.

Dataskyddsförordningen kommer från och med den 25 maj 2018 att ersätta 1995 års dataskyddsdirektiv och utgöra grunden för generell personuppgiftsbehandling inom EU. Enligt artikel 288 andra stycket 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. Förordningens bestämmelser ska således tillämpas av enskilda, myndigheter och domstolar på samma sätt som om de vore nationella författningsbestämmelser. Även om dataskyddsförordningen är direkt tillämplig innehåller den emellertid många bestämmelser som förutsätter eller ger utrymme för kompletterande nationella bestämmelser av olika slag.

4.1.2 2016 års dataskyddsdirektiv

Samtidigt med dataskyddsförordningen 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. I fortsättningen kommer vi i vår promemoria att kalla detta direktiv för *2016 års dataskyddsdirektiv*. Direktivet ska vara genomfört i nationell rätt senast den 6 maj 2018.

Enligt artikel 1.1 i 2016 års dataskyddsdirektiv innehåller direktivet bestämmelser om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. Även sådan personuppgiftsbehandling som utförs hos behöriga myndigheter för att skydda mot, förebygga och förhindra hot mot den allmänna säkerheten ingår i tillämpningsområdet. Av artikel 2.2 d i dataskyddsförordningen framgår att förordningen inte gäller för sådan personuppgiftsbehandling som omfattas av dataskyddsdirektivets tillämpningsområde.

Av artikel 1.2 i 2016 års dataskyddsdirektiv framgår att syftet med direktivet är att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Det framgår också att syftet är att säkerställa att det utbyte av personuppgifter som krävs inom unionen mellan behöriga myndigheter varken begränsas eller förbjuds av skäl som

rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter.

4.2 Två nya svenska regelverk

När dataskyddsförordningen börjar tillämpas ska personuppgiftslagen upphävas.¹ Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) lämnat förslag till en ny lag; lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (förkortad dataskyddslagen). Som framgår av namnet ska denna lag komplettera EU:s dataskyddsförordning på ett generellt plan i svensk rätt. Dataskyddsutredningen har även lämnat förslag till en förordning till dataskyddslagen; förordning med kompletterande bestämmelser till EU:s dataskyddsförordning. I likhet med vad som gäller för personuppgiftslagen föreslås avvikande bestämmelser i annan lag eller förordning ha företräde framför bestämmelserna i dataskyddslagen. Vi kommer i vår promemoria att utgå från det förslag till dataskyddslag som Dataskyddsutredningen har lämnat, trots att detta ännu inte lett till lagstiftning.

Utöver denna generella reglering kommer kompletteringar till bestämmelserna i EU:s dataskyddsförordning att finnas i de sektorsspecifika registerförfattningar som i stor utsträckning reglerar svenska myndigheters personuppgiftsbehandling. Ett omfattande arbete pågår eller har nyligen pågått inom utredningsväsendet för att, i likhet med det uppdrag vi har fått, anpassa dessa sektorsspecifika författningar till det nya regelverket.

Den personuppgiftsbehandling som sker hos behöriga myndigheter i syfte att bl.a. förebygga, förhindra, utreda, avslöja eller lagföra brott samt verkställa straffrättsliga påföljder kommer dock att styras av 2016 års dataskyddsdirektiv. Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande (SOU 2017:29) föreslagit att detta direktiv ska genomföras i svensk rätt genom en ny generell tillämplig lag, kallad brottsdatalagen. Denna lag ska enligt utredningens förslag kompletteras av en förordning, kallad brottsdataförordningen.

¹ Se kommittédirektiv till Dataskyddsutredningen (Dir. 2016:15 s. 6).

Även på brottsdatalagens tillämpningsområde finns det en mängd sektorsspecifika registerförfattningar. Det ligger inom Utredningen om 2016 års dataskyddsdirektivs uppdrag att analysera och bedöma i vilken utsträckning dessa registerförfattningar behöver förändras med hänsyn till direktivets förpliktelser och till den nya ramlagstiftning som brottsdatalagen kommer att utgöra.²

4.3 Avgränsning av domstolsdatalagens tillämpningsområde

4.3.1 Dataskyddsförordningen eller 2016 års dataskyddsdirektiv?

För många myndigheter får EU:s dataskyddsreform effekten att personuppgiftsbehandlingen i vissa delar av verksamheten tillhör dataskyddsförordningens tillämpningsområde medan den i andra delar av verksamheten tillhör 2016 års dataskyddsdirektivs tillämpningsområde. Dataskyddsförordningen gäller, enligt artikel 2.2 d i förordningen jämförd med artikel 1.1 i direktivet, inte för sådan personuppgiftsbehandling som omfattas av direktivets tillämpningsområde. Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande (SOU 2017:29 s. 155 f.) föreslagit att brottsdatalagen – som ska genomföra direktivet i svensk rätt – ska vara tillämplig vid behandling av personuppgifter som behöriga myndigheter utför för vissa syften. Dessa är bl.a. att förebygga, förhindra eller upptäcka brottslig verksamhet, att utreda eller lagföra brott samt att verkställa straffrättsliga påföljder. Det avgörande för vilket av regelverken som är tillämpligt för en myndighets personuppgiftsbehandling kommer således att vara för vilket syfte den aktuella behandlingen utförs.

För domstolarnas del resulterar detta i att när de allmänna domstolarna exempelvis hanterar mål och ärenden om lagföring av brott eller verkställighet av straffrättsliga påföljder ska personuppgiftsbehandlingen utföras i enlighet med bestämmelserna i brottsdatalagen och de bestämmelser i registerförfattning som

² Se kommittédirektiv till Utredningen om 2016 års dataskyddsdirektiv (Dir. 2016:21 s. 9).

kompletterar denna lag. Personuppgiftsbehandlingen i tvistemål – som enligt vår bedömning ligger utanför brottsdatalagens tillämpningsområde – ska dock utföras i enlighet med dataskyddsförordningen och de bestämmelser i registerförfattning som kompletterar förordningen. Det sistnämnda gäller också den stora merparten av de ärenden som handläggs vid allmän domstol. Vissa av dessa ärenden har av Utredningen om 2016 års dataskyddsdirektiv dock bedömts ligga inom brottsdatalagens tillämpningsområde. Som exempel kan nämnas handläggningen av hemliga tvångsmedel under förundersökning och ärenden enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.³

Eftersom personuppgiftsbehandling som utförs i syfte att verkställa straffrättsliga påföljder ligger under brottsdatalagens tillämpningsområde kommer denna lag också att tillämpas i delar av de allmänna förvaltningsdomstolarnas verksamhet. Utredningen om 2016 års dataskyddsdirektiv har exempelvis gjort bedömningen att den personuppgiftsbehandling som utförs när frågor prövas enligt lagen (1991:1129) om rättspsykiatrisk vård faller under brottsdatalagens tillämpningsområde. Detsamma gäller de personuppgifter som behandlas när frågor enligt fängelselagen (2010:610) prövas. För en mer utförlig beskrivning av brottsdatalagens tillämpningsområde hänvisar vi till Utredningen om 2016 års dataskyddsdirektivs delbetänkande (SOU 2017:29 kap. 7 och 8).

4.3.2 Bedömning

Förslag: Domstolsdatalagen ska inte gälla vid behandling av personuppgifter i de allmänna domstolarnas och de allmänna förvaltningsdomstolarnas verksamhet som omfattas av brottsdatalagens tillämpningsområde.

När dataskyddsförordningen börjar tillämpas och brottsdatalagen träder i kraft kommer domstolarna (dock inte hyres- och arrendenämnderna) att behöva förhålla sig till två olika regelverk

³ Se Utredningen om 2016 års dataskyddsdirektivs delbetänkande (SOU 2017:29 s. 207 f.).

för personuppgiftsbehandling. Det ena består av dataskyddsförordningen, domstolarnas registerförfattning samt den nya svenska dataskyddslagen i tillämpliga delar (se avsnitt 4.2). Det andra består av brottsdatalagen med tillhörande brottsdataförordning och domstolarnas registerförfattning.

Domstolsdatalagen och domstolsdataförordningen omfattar för närvarande all den personuppgiftsbehandling som sker i domstolarnas rättskipande och rättsvårdande verksamhet. Detta leder till vissa praktiska problem om dessa författningar nu ska anpassas till både dataskyddsförordningen och brottsdatalagen.

För den del av verksamheten som ligger inom brottsdatalagens tillämpningsområde kommer förekomsten av en generellt tillämplig brottsdatalag förmodligen att leda till att en del av domstolsdatalagens bestämmelser blir överflödiga. För den del av verksamheten som faller inom dataskyddsförordningens tillämpningsområde bör domstolsdatalagen enligt vår bedömning i materiellt hänseende snarare kvarstå oförändrad i så stor utsträckning som möjligt.

Dessa praktiska problem skulle eventuellt kunna lösas genom att domstolsdatalagen och domstolsdataförordningen delas in i olika kapitel utifrån tillämpningsområde. Vi anser dock att en sådan lösning riskerar att ytterligare komplicera ett redan svårtillgängligt rättsområde. Domstolsdatalagens förhållande till både dataskyddsförordningen, dataskyddslagen och brottsdatalagen skulle behöva beskrivas i lagen. Vidare skulle det enligt vår bedömning finnas risk för att korshänvisningar och undantag måste användas i stor utsträckning.

Utöver de rent lagtekniska aspekterna skulle bestämmelser med samma lydelse riskera att få olika innebörd, beroende på inom vilken del av verksamheten de tillämpas. I den del av verksamheten där personuppgiftsbehandlingen styrs av 2016 års dataskyddsdirektiv skulle bestämmelserna behöva tolkas i ljuset av brottsdatalagen och direktivet. På motsvarande sätt skulle bestämmelserna behöva tolkas i ljuset av dataskyddsförordningen i resterande del av verksamheten.

För att göra regelverket mer lättillgängligt för tillämparen föreslår vi därför, i samråd med Utredningen om 2016 års dataskyddsdirektiv, att domstolsdatalagen och domstolsdataförordningen fortsättningsvis endast ska reglera den person-

uppgiftsbehandling i domstolarnas rättskipande och rättsvårdande verksamhet som faller under dataskyddsförordningens tillämpningsområde. Vi kommer i vår promemoria att lämna förslag till förändringar i dessa författningar. Utredningen om 2016 års dataskyddsdirektiv kommer i sitt slutbetänkande att lämna förslag till hur den personuppgiftsbehandling hos domstolarna som faller under direktivets tillämpningsområde ska regleras.

Som vi nämnt ovan avgränsas dataskyddsförordningens materiella tillämpningsområde bl.a. genom att den behandling av personuppgifter som faller under 2016 års dataskyddsdirektiv inte omfattas av förordningen. Domstolsdatalagens tillämpningsområde måste enligt vår mening avgränsas på samma sätt. Mot den bakgrunden och för att tydliggöra förhållandet mellan de två registerförfattningar med tillhörande förordningar som framöver kommer att finnas för domstolarnas verksamhet, föreslår vi att det i domstolsdatalagen upplyses om att den lagen inte gäller vid behandling av personuppgifter i de allmänna domstolarnas och de allmänna förvaltningsdomstolarnas verksamhet som omfattas av brottsdatalagens tillämpningsområde. Detta omfattar den personuppgiftsbehandling som utförs med stöd av brottsdatalagen, dess kompletterande registerförfattning för domstolarna och de förordningar som i sin tur kompletterar dessa lagar.⁴

4.4 Vilket regelverk är tillämpligt?

När det vid en domstol uppkommer fråga om vilket av regelverken som är tillämpligt för en viss personuppgiftsbehandling kommer – som vi tidigare nämnt – det avgörande att vara för vilket syfte den aktuella personuppgiftsbehandlingen utförs. För domstolarnas del kommer det enligt vår bedömning främst att behöva avgöras om den aktuella behandlingen utförs i syfte att lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Ledning i denna fråga kan lämpligen hämtas ur Utredningen om 2016 års dataskyddsdirektivs delbetänkande

⁴ Av Utredningen om 2016 års dataskyddsdirektivs delbetänkande (SOU 2017:29 s. 140) framgår att utgångspunkten för den utredningens arbete är att brottsdatalagen ska kompletteras av registerförfattningar. Det finns därmed anledning att anta att en sådan registerförfattning kommer att föreslås även för domstolarnas verksamhet.

(SOU 2017:29 kap. 7 och 8). Där finns en omfattande analys av brottsdatalagens tillämpningsområde och de gränsdragningsfrågor som kan uppstå vid myndigheters personuppgiftsbehandling.

Om tillämparen i en faktisk situation kommer fram till att syftet med personuppgiftsbehandlingen exempelvis är att lagföra brott, ska domstolsdatalagen inte tillämpas. Skulle tillämparen däremot komma fram till att personuppgiftsbehandlingen inte utförs för något av de syften som ligger inom brottsdatalagens tillämpningsområde, ska dataskyddsförordningen med kompletterande domstolsdatalag (och dataskyddslagen i tillämpliga delar) tillämpas vid behandlingen.

Sammanfattningsvis – och något förenklat – kommer dataskyddsförordningen och domstolsdatalagen som huvudregel att tillämpas vid behandling av personuppgifter i tvistemål och ärenden i allmän domstol samt i mål i allmän förvaltningsdomstol. Hyres- och arrendenämndernas personuppgiftsbehandling faller utslutande under dataskyddsförordningens tillämpningsområde.

5 Nationella registerförfattningar

5.1 Registerförfattningarnas förenlighet med dataskyddsförordningen

När dataskyddsförordningen börjar tillämpas kommer den att vara direkt tillämplig på all personuppgiftsbehandling som i medlemsstaterna utförs inom dess materiella och territoriella tillämpningsområde. Personuppgiftslagen kommer då att upphävas.¹ Den nya dataskyddslagen kommer dock, enligt Dataskyddsutredningens betänkande (SOU 2017:39), att innehålla en ny generell svensk reglering för personuppgiftsbehandling. Denna lag ska enligt Dataskyddsutredningens förslag, i likhet med personuppgiftslagen, vara subsidiär i förhållande till bestämmelser om behandling av personuppgifter i andra författningar.

När det gäller personuppgiftsbehandling som är nödvändig för att fullgöra en rättslig förpliktelse, för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning ger artikel 6.2 i dataskyddsförordningen medlemsstaterna möjlighet att behålla eller införa mer specifika bestämmelser, där bl.a. specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling närmare fastställs. Av skäl 10 till dataskyddsförordningen framgår att möjligheten att specificera bestämmelserna för personuppgiftsbehandling också gäller känsliga personuppgifter.

Även artikel 6.3 andra stycket i dataskyddsförordningen ger medlemsstaterna möjlighet att specificera villkoren för personuppgiftsbehandling. Här anges att den rättsliga grunden kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i dataskyddsförordningen. Som exempel nämns de

¹ Se kommittédirektiv till Dataskyddsutredningen (Dir 2016:15 s. 6).

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. Även förfaranden för behandling nämns. Här ingår åtgärder för att tillförsäkra en laglig och rättvis behandling, t.ex. i de särskilda situationer som framgår av kapitel IX. Det kapitlet reglerar bl.a. förhållandet till yttrande- och informationsfriheten samt offentlighetsprincipen. Även medlemsstaternas rätt att närmare bestämma på vilka villkor nationella identifikationsnummer får behandlas framgår av detta kapitel. Det anges också i artikel 6.3 att unionsrätten eller medlemsstaternas nationella rätt i dessa fall ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas. Av artikel 4.7 i dataskyddsförordningen framgår att vem som är personuppgiftsansvarig kan föreskrivas i den nationella rätten, om ändamålen och medlen för behandling fastställs av medlemstatens nationella rätt.

I artikel 6.3 andra stycket anges förvisso att de särskilda bestämmelserna ska vara en del av "den rättsliga grunden". Dataskyddsutredningen (SOU 2017:39 s.135) har vad gäller artikel 6 tolkat dataskyddsförordningen på så sätt att med den rättsliga grunden för personuppgiftsbehandling avses någon av de grunder för behandling som anges i artikel 6.1 (se kapitel 6). Den rättsliga grunden skulle med detta synsätt vara exempelvis den bestämmelse i nationell rätt där en myndighets uppgift av allmänt intresse eller dess myndighetsutövande uppdrag fastställs. I svensk rätt är det dock vanligare att denna "rättsliga grund" inte innehåller bestämmelser om personuppgiftsbehandling. I stället återfinns dessa bestämmelser ofta i sektorsspecifika registerförfattningar. Vi anser att det måste vara möjligt att tolka dataskyddsförordningen så att den ger handlingsutrymme att följa de nationella lagstiftningstraditionerna på området. Enligt vår mening måste exemplifieringen av frågor som enligt artikel 6.3 andra stycket kan fastställas i den nationella rätten för svensk del därmed kunna ses som en exemplifiering av de bestämmelser som kan förekomma i registerförfattningarna.

5.2 Allmänna principer för behandling av personuppgifter

Dataskyddsutredningen gör i sitt betänkande (SOU 2017:39 s. 105) bedömningen att de svenska registerförfattningarna framför allt kommer att innehålla en precisering av de allmänna principer för personuppgiftsbehandling som framgår av artikel 5 i dataskyddsförordningen. Dessa principer motsvaras i princip av artikel 6 i 1995 års dataskyddsdirektiv, som införts i svensk rätt genom 9 § PuL. Artikel 5.1 i dataskyddsförordningen lyder i sin helhet som följer.

Artikel 5

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).
- 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).

Det är således dessa ovan angivna principer som registerförfattningarna till stor del är menade att precisera.

5.3 Bedömning

Bedömning: Dataskyddsförordningen hindrar inte den typ av nationell registerlagstiftning som domstolsdatalagen utgör.

Dataskyddsförordningen hindrar inte heller att medlemsstaterna i registerförfattning inför mer restriktiva bestämmelser för myndigheternas personuppgiftsbehandling än vad som följer av förordningen eller utökar de nationella myndigheternas skyldigheter gentemot de registrerade.

Sammanfattningsvis anser vi att artikel 6.2 och 6.3 i dataskyddsförordningen ger medlemsstaterna möjlighet att i den nationella lagstiftningen närmare precisera hur personuppgifter får behandlas när behandlingen är nödvändig för att fullgöra en rättslig förpliktelse, för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Detta kan ske genom exempelvis den typ av registerlagstiftning som domstolsdatalagen utgör. Medlemsstaterna har här enligt vår mening frihet att välja vilket område eller vilken verksamhet en registerförfattning ska reglera, så länge lagstiftningen omfattar sådant som ryms inom begreppen rättslig förpliktelse, uppgift av allmänt intresse eller myndighetsutövning.

Dataskyddsutredningen gör i sitt betänkande (SOU 2017:39 s. 105) bedömningen att registerförfattningarna framför allt kommer att innehålla en precisering av de allmänna principer för personuppgiftsbehandling som framgår av artikel 5 i dataskyddsförordningen. Det kan vidare nämnas att det är tillåtet för en medlemsstat, som genomför förtydliganden och begränsningar av dataskyddsförordningens bestämmelser genom den nationella

rätten, att införliva delar av förordningen i nationell rätt. Detta framgår av skäl 8 till dataskyddsförordningen. Ett direkt återgivande av de bestämmelser som finns i dataskyddsförordningen och som förvisso skulle ha gällt även utan ett sådant återgivande är därmed tillåtet i nationell rätt. Enligt skäl 8 kan syftet med detta bl.a. vara att göra de nationella bestämmelserna begripliga.

Dataskyddsförordningen innehåller inte något förbud mot att personuppgiftsansvariga utökar skyddet för de personuppgifter som behandlas, går utöver sina skyldigheter vad gäller information till de registrerade eller liknande. Dataskyddsförordningen ger vidare, som framgår ovan, möjlighet till nationell specificering vad gäller myndigheternas behandling av personuppgifter. Det är enligt vår mening rimligt att medlemsstaterna vid denna specificering har samma möjlighet att för sina myndigheter föreskriva ett skydd för personuppgifter som går utöver dataskyddsförordningens skyldigheter. I artikel 1.2 i dataskyddsförordningen fastställs vidare att syftet med förordningen är att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd för personuppgifter. Mot den bakgrunden bedömer vi att nationell lagstiftning som skapar ett förstärkt skydd för sådana personuppgifter bör vara förenlig med dataskyddsförordningen. Medlemsstaterna bör således ha möjlighet att införa mer restriktiva bestämmelser för sina myndigheters personuppgiftsbehandling än vad som följer av dataskyddsförordningen. Det bör även vara möjligt för medlemsstaterna att utöka de nationella myndigheternas skyldigheter gentemot de registrerade.

6 Rättslig grund för domstolarnas personuppgiftsbehandling

Dataskyddsförordningen utgår, liksom 1995 års dataskyddsdirektiv, från att varje behandling av personuppgifter måste vila på en rättslig grund. Enligt artikel 6.1 i dataskyddsförordningen får personuppgifter endast behandlas om någon av de rättsliga grunder som räknas upp i artikeln föreligger. Den rättsliga grund som närmast kommer i fråga för domstolarnas personuppgiftsbehandling i den rättskipande och rättsvårdande verksamheten är den som framgår av artikel 6.1 e. Enligt denna bestämmelse är personuppgiftsbehandling tillåten om den är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Personuppgiftsbehandling är även tillåten om den är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Detta framgår av artikel 6.1 c.

I artikel 6.3 första stycket finns ett uttryckligt krav på att grunden för personuppgiftsbehandlingen enligt artikel 6.1 c och e – dvs. den rättsliga förpliktelsen, myndighetsutövningen eller uppgiften av allmänt intresse – ska vara fastställd i enlighet med unionsrätten eller den nationella rätten.

Som framgår av ordalydelsen i artikel 6.1 c och e innehåller dessa rättsliga grunder även ett nödvändighetsrekvisit. För att en myndighets personuppgiftsbehandling exempelvis ska vara tillåten enligt artikel 6.1 e måste den vara *nödvändig* för att myndigheten ska kunna utföra den uppgift av allmänt intresse som den genom författning tilldelats, alternativt *nödvändig* för att myndigheten ska kunna utföra den myndighetsutövning som den anförtrotts. På samma sätt är en personuppgiftsbehandling laglig enligt

artikel 6.1 c om den är *nödvändig* för att fullgöra en rättslig förpliktelse.

Dataskyddsutredningen konstaterar i sitt betänkande (SOU 2017:39 s. 105 f.) att det unionsrättsliga begreppet *nödvändig* inte har samma strikta innebörd som i svenska språket. Även om exempelvis en uppgift av allmänt intresse skulle kunna utföras utan behandling av personuppgifter, kan behandlingen ur ett unionsrättsligt perspektiv anses vara nödvändig och därmed tillåten enligt artikel 6 om den leder till effektivitetsvinster.¹

Alla myndigheter utför en rad administrativa uppgifter som krävs för att myndigheten ska fungera, men som varken direkt eller indirekt kan sägas framgå av uppdraget. Dataskyddsutredningen konstaterar i sitt betänkande (a.a. s. 129) att en myndighet inte kan utföra sina fastställda uppgifter om den inte fungerar och att således även administrativa åtgärder som är nödvändiga för myndighetens förvaltning och funktion därmed är rättsligt grundade i dataskyddsförordningens mening.

Utöver att personuppgiftsbehandlingen ska vara nödvändig för den rättsliga förpliktelsen, utförandet av uppgiften av allmänt intresse eller myndighetsutövningen, måste behandlingen naturligtvis även utföras i enlighet med de allmänna principer som framgår av artikel 5 i dataskyddsförordningen. Detta innebär bland annat att behandlingen måste vara skäligen eller rimligen (*korrekthet*) i förhållande till den registrerade. Behovet av den konkreta behandlingen måste därmed alltid vägas emot den registrerades intresse av personlig integritet.

6.1 Dataskyddslagen

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit att det i dataskyddslagen ska tas in en bestämmelse som tydliggör att begreppet *uppgift av allmänt intresse* avser 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. Dataskyddsutredningen har även föreslagit

¹ Se SOU 1997:39 s. 359, Dom Huber mot Tyskland, C-524/06, EU:C:2008:724 och dom Pharmacontiente mot Saúde e Higiene m.fl., C-683/13, EU:C:2014:2028.

att det i dataskyddslagen ska tas in en bestämmelse som tydliggör att myndighetsutövning utgör en rättslig grund för behandling av personuppgifter endast om denna sker enligt lag eller annan författning.

Vidare föreslår Dataskyddsutredningen att dataskyddslagen ska innehålla en bestämmelse som tydliggör att en rättslig förpliktelse utgör en rättslig grund för behandling av personuppgifter endast om förpliktelsen gäller enligt lag eller annan författning, följer av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

De nyss nämnda bestämmelserna ska, enligt Dataskyddsutredningens förslag, finnas i 2 kap. 2 och 3 §§ dataskyddslagen. Dataskyddsutredningen framhåller i sitt betänkande (SOU 2017:39 s. 112) att den rättsliga grunden inte nödvändigtvis måste fastställas i eller i enlighet med en av riksdagen beslutad lag, men att den däremot måste vara fastställd i laga ordning, på ett konstitutionellt korrekt sätt. Detta bör enligt vår mening innebära att även exempelvis förordningar som meddelats av regeringen, med stöd av den restkompetens som följer av regeringsformen, kan utgöra den rättsliga grunden för personuppgiftsbehandling. Detsamma bör gälla befogenheter som anges i annan föreskrift än lag eller förordning, förutsatt att föreskriften har meddelats i den ordning som följer av regeringsformens bestämmelser om normgivningskompetens.

6.2 Myndighetsutövning, uppgift av allmänt intresse eller rättslig förpliktelse?

6.2.1 Tidigare förarbeten

När dataskyddsförordningen börjar tillämpas kommer personuppgifter att få behandlas endast under förutsättning att någon av de rättsliga grunderna i artikel 6.1 i dataskyddsförordningen föreligger. Bestämmelsen i artikel 6.1 motsvarar i stora drag artikel 7 i 1995 års dataskyddsdirektiv, som har genomförts i svensk rätt genom 10 § PUL.

Enligt 2 § domstolsdatalagen gäller den lagen vid behandling av personuppgifter i domstolarnas rättskipande och rättsvårdande verksamhet samt när personuppgifterna vidarebehandlas i den

administrativa verksamheten för att lämnas ut efter begäran. Enligt 6 § domstolsdatalagen får personuppgifterna behandlas i denna verksamhet endast om det behövs för handläggning av mål och ärenden. De personuppgifter som behandlas enligt 6 § får dock även behandlas om det behövs för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Detta framgår av 7 § domstolsdatalagen.

I departementspromemorian med förslag till domstolsdatalag (Ds 2013:10 s. 65) gjordes bedömningen att den personuppgiftsbehandling som sker i domstolarnas rättskipande och rättsvårdande verksamhet och inom ramen för handläggning av mål och ärenden eller för uppgiftslämnande som sker i överensstämmelse med lag eller förordning, får anses vara nödvändig för att domstolarna ska kunna fullgöra sina rättsliga förpliktelser eller kunna utföra sina arbetsuppgifter av allmänt intresse. Sådan behandling bedömdes även vara nödvändig som ett led i myndighetsutövningen.

Regeringen har vid domstolsdatalagens tillkomst således ansett att samtliga de rättsliga grunder som numera framgår av artikel 6.1 c och e i dataskyddsförordningen utgör den rättsliga grunden för domstolarnas personuppgiftsbehandling inom domstolsdatalagens tillämpningsområde. Vi kommer i följande avsnitt att göra en kort redogörelse för innebörden av dessa rättsliga grunder. Vi anser också att en förnyad analys av vilken eller vilka av dessa grunder som utgör stödet för domstolarnas personuppgiftsbehandling inom ramen för domstolsdatalagen bör vara av intresse för de personuppgiftsansvariga domstolarna. I vår redogörelse utgår vi i allt väsentligt från den analys av begreppen uppgift av allmänt intresse, myndighetsutövning och rättslig förpliktelse som har gjorts av Dataskyddsutredningen. För den som har behov av en mer utförlig redogörelse hänvisar vi till Dataskyddsutredningens betänkande i denna del.²

6.2.2 Uppgift av allmänt intresse

Som framgår av artikel 6.1 e och artikel 6.3 första stycket i dataskyddsförordningen samt 2 kap. 3 § förslaget till dataskydds-

² SOU 2017:39 kapitel 8.

lag, är personuppgiftsbehandling laglig om den är nödvändig för att den personuppgiftsansvarige ska kunna utföra en uppgift av allmänt intresse som följer av lag eller annan författning eller av beslut som har meddelats med stöd av lag eller annan författning. Dataskyddsutredningen anser att mycket talar för att begreppet uppgift av allmänt intresse har fått en vidare unionsrättslig betydelse genom dataskyddsförordningen än det hittills har haft i svensk rätt.³

Dataskyddsförordningen skiljer sig från 1995 års dataskyddsdirektiv på så sätt att en myndighet inte längre kommer att kunna grunda sin personuppgiftsbehandling på en intresseavvägning mellan myndighetens berättigade intresse och den registrerades intressen eller grundläggande rättigheter och friheter. Den bestämmelse i dataskyddsförordningen som reglerar personuppgiftsbehandling efter en sådan intresseavvägning, artikel 6.1 f, gäller nämligen inte för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter. Även myndigheternas utrymme för att grunda personuppgiftsbehandlingen på samtycke från den registrerade kan antas minska genom dataskyddsförordningen. I skäl 43 till förordningen anges att samtycke inte bör utgöra giltig grund för behandling i de 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.

Dataskyddsutredningen gör bedömningen att begreppet uppgift av allmänt intresse rent språkligt kan antas avse något som är av intresse för eller berör många människor på ett bredare plan. Av skäl 45 till dataskyddsförordningen följer också att allmänintresset inbegriper hälso- och sjukvårdsändamål, folkhälsa, socialt skydd och förvaltning av hälso- och sjukvårdstjänster. Dataskyddsutredningen gör vidare bedömningen att alla uppgifter som utförs av statliga myndigheter i syfte att uppfylla ett uttryckligt uppdrag av riksdag eller regering är av allmänt intresse.⁴

³ Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 123).

⁴ A.a. s. 124.

6.2.3 Myndighetsutövning

Enligt artikel 6.1 e och artikel 6.3 första stycket i dataskyddsförordningen samt 2 kap. 3 § förslaget till dataskyddslag, är personuppgiftsbehandling laglig om den är nödvändig som ett led i myndighetsutövning som den personuppgiftsansvarige utövar enligt lag eller annan författning.

Domstolar är en särskild form av myndighet.⁵ Detta framgår bl.a. direkt av 11 kap. 5 § RF, som stadgar att rättstvister mellan enskilda inte utan stöd av lag får avgöras av andra myndigheter än domstolar.

Dataskyddsutredningen anser att man bör kunna utgå från att det som i Sverige brukar anses vara myndighetsutövning även faller under motsvarande unionsrättsliga begrepp.⁶ Myndighetsutövning definieras i svensk rätt ofta som ”utövning av befogenhet att bestämma om förmån, rättighet, skyldighet, disciplinär bestraffning eller annat jämförbart förhållande”. Definitionen härstammar från 3 § i 1971 års förvaltningslag.⁷

Begreppet myndighetsutövning förekommer vidare i bl.a. skadeståndsrättsliga regler. I förarbetena till 3 kap. 2 § skadeståndslagen (1972:207) anges att myndighetsutövning avser beslut eller åtgärder som är ett uttryck för det allmännas rätt att utöva makt över medborgarna. Karaktäristiskt är att den enskilde står i ett beroendeförhållande till myndigheten, som bestämmer över den enskildes rättigheter och skyldigheter på ett sätt som inte förekommer i privaträttsliga sammanhang.⁸

Myndighetsutövningen är således ytterst ett uttryck för samhällets maktbefogenheter i förhållande till medborgarna. Befogenheten till myndighetsutövning måste vara grundad på lag eller annan författning eller på annat sätt kunna härledas ur bemyndiganden från de högsta statsorganen. Till myndighetsutövning hör först och främst sådan offentlig verksamhet, varigenom myndigheterna ensidigt bestämmer om enskildas skyldigheter eller om ingrepp i enskildas frihet eller egendom. Hit

⁵ Melin, *Våra domstolar Organisation och verksamhet m.m.*, 2012, s. 40–41.

⁶ Se *Dataskyddsutredningens betänkande SOU 2017:39* s. 119, med hänvisning till *Datalagskommitténs betänkande SOU 1997:39* s. 365.

⁷ Holmberg m.fl. *Grundlagarna, Zetee*, kommentar till 12 kap. 4 § RF samt prop. 1971:30 s. 333.

⁸ Jfr prop. 1972:5 s. 498 f. och t.ex. *NJA* 2013 s. 1210.

hör alltså beslut som innebär ålägganden att göra eller underlåta något eller som avser ingrepp i personlig frihet eller egendom, men även rent faktiska åtgärder som innebär sådana ingrepp, vare sig de grundas på formliga beslut eller inte. Så långt kan begreppet myndighetsutövning sägas sammanfalla med begreppet offentlig maktutövning. Men även åtskilliga gynnande beslut faller in under begreppet myndighetsutövning, exempelvis beslut om sociala förmåner, statsbidrag och liknande. Den enskilde står här i ett beroendeförhållande till det allmänna, som ensamt har möjlighet att tillmötesgå hans eller hennes anspråk och därigenom i viss mening kan sägas utöva makt mot honom eller henne. Till myndighetsutövning bör vidare hänföras vissa beslut, vilka till skillnad från de hittills nämnda inte innehåller direkta handlingsmönster utan har indirekta rättsverkningar gentemot den enskilde, t.ex. registreringsbeslut och beslut om utfärdande av legitimationshandlingar samt beslut i samband med obligatorisk kontrollverksamhet.

Utanför begreppet myndighetsutövning faller råd, upplysningar och andra icke bindande uttalanden samt sådan faktisk verksamhet som inte innebär tvång mot den enskilde (t.ex. undervisning eller sjukvård). Till myndighetsutövning räknas inte heller sådan verksamhet som stat eller kommun utövar i privaträttsliga former. Gränsdragningen mellan offentligrättsliga och privaträttsliga regler är sålunda av stor vikt när det gäller att bestämma begreppet myndighetsutövning.⁹

6.2.4 Rättslig förpliktelse

Enligt artikel 6.1 c och artikel 6.3 första stycket i dataskyddsförordningen samt 2 kap. 2 § förslaget till dataskyddslag är personuppgiftsbehandling laglig om den är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som följer av lag eller annan författning eller av beslut som har meddelats med stöd av lag eller annan författning.

Dataskyddsutredningen gör bedömningen att det faktum att den rättsliga förpliktelsen måste ha en legal grund inte innebär att

⁹ Lundell/Strömberg, Allmän förvaltningsrätt, 26 uppl., s. 20 f.

förpliktelsen nödvändigtvis måste framgå av en författning eller liknande. Rättsliga förpliktelser kan också framgå av exempelvis förelägganden, myndighetsbeslut och domar som har meddelats med stöd av gällande rätt.¹⁰

Dataskyddsutredningen konstaterar att även domstolar och statliga myndigheter vid sidan av sina uppgifter och uppdrag kan sägas ha rättsliga förpliktelser och att det inte finns något i artikel 6.1 c i dataskyddsförordningen som begränsar tillämpningen till den privata sektorn. Domstolar och myndigheter har också andra författningsreglerade förpliktelser som i sig kräver personuppgiftsbehandling, exempelvis när det gäller personaladministration.¹¹ Datainspektionen har vidare ansett att den skyldighet för myndigheter som följer av offentlighetsprincipen är en sådan rättslig skyldighet som avses i personuppgiftslagen och som motsvaras av dataskyddsförordningens begrepp rättslig förpliktelse.¹²

6.2.5 Bedömning

Bedömning: Den personuppgiftsbehandling som utförs inom domstolsdatalagens tillämpningsområde har en sådan rättslig grund som avses i artikel 6.1 c och e i dataskyddsförordningen, eftersom den är nödvändig för att fullgöra en rättslig förpliktelse, för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning.

De allmänna domstolarna, de allmänna förvaltningsdomstolarna och hyres- och arrendenämnderna är myndigheter. Deras rättskipande och rättsvårdande uppgift, som innebär att avgöra mål och ärenden, är fastställd genom lag eller annan författning. Den enskilde står vidare i ett uppenbart beroendeförhållande till domstolarna, som har makt att bestämma över den enskildes rättigheter och skyldigheter. Den rättskipande och rättsvårdande

¹⁰ Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 113 f.).

¹¹ A.a. s. 116 f, jfr även SOU 1997:39 s. 363.

¹² Datainspektionens rapport 2005:3 Övervakning i arbetslivet – Kontroll av de anställdas Internet och e-postanvändning m.m. s. 15.

verksamhet som utförs av domstolarna i mål och ärenden motsvarar enligt vår mening därmed tydligt den beskrivning av myndighetsutövning som framgår av avsnitt 6.2.3.

Vi anser dock att domstolarnas rättskipande och rättsvårdande verksamhet också utgör en uppgift av allmänt intresse. I en rättsstat måste det anses vara av allmänt intresse att rättskipningen utförs på ett rättsäkert sätt av oberoende domstolar. Som framgår ovan har domstolarna uttryckligen anförtrotts detta uppdrag av riksdagen genom de lagar som reglerar deras verksamhet. Eftersom domstolarnas uppgift i denna del således är fastställd i den laga ordning som gäller i Sverige finns det även med detta synsätt en hållbar rättslig grund för personuppgiftsbehandlingen.

Den personuppgiftsbehandling som utförs med stöd av processuella bestämmelser eller för att domstolarna på ett rättsäkert sätt ska kunna genomföra den rättskipande och rättsvårdande uppgift de har anförtrotts, måste enligt vår mening vidare anses vara *nödvändig* som ett led i domstolarnas myndighetsutövning och för att utföra den uppgift av allmänt intresse som domstolarna anförtrotts. Detta gäller även den personuppgiftsbehandling som utförs för att effektivisera domstolarnas framtida målhantering och skapa en enhetlig rättspraxis, exempelvis i den miljöbok som förs vid samtliga mark- och miljödomstolar.

Det rättsliga stödet för den personuppgiftsbehandling som utförs inom ramen för domstolarnas rättskipande och rättsvårdande verksamhet står enligt vår mening således att finna i artikel 6.1 e i dataskyddsförordningen, eftersom verksamheten utgör både myndighetsutövning och en uppgift av allmänt intresse.

Domstolsdatalagen gäller emellertid även för den del av domstolarnas administrativa verksamhet som innebär att personuppgifter som behandlats för handläggning av mål och ärenden lämnas ut i överensstämmelse med lag eller förordning. Detta framgår bl.a. av den sekundära ändamålsbestämmelsen i 7 §, som behandlas närmare i kapitel 9. Möjligheten att behandla personuppgifter för detta ändamål har dock relevans när det gäller att fastställa den rättsliga grunden för den behandling som utförs inom domstolsdatalagens tillämpningsområde.

Ett utlämnande av personuppgifter med stöd av lag eller förordning innefattar t.ex. sådant utlämnande av uppgifter som sker

med stöd av tryckfrihetsförordningen. Dataskyddsförordningens bestämmelser om skydd för personuppgifter hindrar inte att en myndighets allmänna handlingar lämnas ut i enlighet med bestämmelser i den nationella lagstiftningen som tillgodoser allmänhetens rätt att få tillgång till allmänna handlingar, såsom den svenska offentlighetsprincipen. Detta framgår av artikel 86 i dataskyddsförordningen.

Datainspektionen har tidigare gjort bedömningen att en myndighets skyldighet enligt offentlighetsprincipen utgör en rättslig skyldighet. Rättslig skyldighet är 1995 års dataskyddsdirektivs och personuppgiftslagens motsvarighet till dataskyddsförordningens begrepp rättslig förpliktelse. Mot bakgrund av att myndigheters skyldighet enligt offentlighetsprincipen är en lagreglerad förpliktelse anser vi inte att det finns anledning att göra någon annan bedömning. Den personuppgiftsbehandling som utförs när en domstol lämnar ut uppgifter från den rättskipande och rättsvårdande verksamheten i enlighet med tryckfrihetsförordningen utgör således en sådan rättslig förpliktelse som avses i artikel 6.1 c i dataskyddsförordningen.

Ett utlämnande av uppgifter enligt tryckfrihetsförordningen utgör enligt vår mening dock även en sådan uppgift av allmänt intresse som avses i artikel 6.1 e i dataskyddsförordningen. Myndigheternas skyldighet att lämna ut handlingar är reglerad i lag och den insyn i myndigheternas verksamhet som offentlighetsprincipen bidrar till måste anses vara av intresse för allmänheten.

Samma resonemang bör enligt vår mening kunna föras när det gäller annat utlämnade av uppgifter som är reglerat i lag eller förordning. Om lagstiftaren har ansett att en skyldighet att lämna ut uppgifter är av sådan vikt att den ska författningsregleras anser vi att det får förutsättas att det handlar om en sådan uppgift av allmänt intresse som avses i artikel 6.1 e i dataskyddsförordningen. Enligt vår uppfattning bör det faktum att skyldigheten är författningsreglerad också innebära att den utgör en rättslig förpliktelse enligt artikel 6.1 c i förordningen.

Slutligen kan det övervägas om det i domstolsdatalogen ska tas in en hänvisning till 2 kap. 2 och 3 §§ dataskyddslagen, där dataskyddsförordningens bestämmelser om rättslig grund kommer till tydligt uttryck. Det som talar för att en sådan hänvisning bör göras är att det i annat fall skulle kunna uppstå föreställningar om

att innehållet i dessa bestämmelser inte är tillämpligt för domstolarnas rättskipande och rättsvårdande verksamhet. Data-skyddslagens krav på rättslig grund för behandlingen är dock endast ett införlivande av en direkt tillämplig bestämmelse i dataskyddsförordningen. Den får således enligt vår mening ses som en upplysningsbestämmelse utan egen rättsverkan. Vi föreslår också att domstolsdatalagen ska innehålla en upplysning om att lagen innehåller kompletterande bestämmelser till dataskyddsförordningen (se avsnitt 10.2). Vidare har lagstiftaren genom domstolsdatalagen gjort de bedömningar som behövs vad gäller den rättsliga grunden för domstolarnas personuppgiftsbehandling. Mot den bakgrunden anser vi att det i domstolsdatalagen inte behöver eller bör tas in en hänvisning till 2 kap. 2 och 3 §§ dataskyddslagen.

Det faktum att domstolarnas personuppgiftsbehandling – såväl inom ramen för den rättskipande och rättsvårdande verksamheten som vid utlämnande i enlighet med lag eller förordning – vilar på flera av de rättsliga grunder som anges i artikel 6.1 i dataskyddsförordningen, innebär naturligtvis inte att personuppgifter får behandlas på vilket sätt som helst i denna verksamhet. Dataskyddsförordningens allmänna principer för personuppgiftsbehandling måste alltid följas (se avsnitt 5.2) och i enlighet med det nödvändighetsrekvisit som finns i artikel 6.1 c och e måste frågan om den enskilda personuppgiften är nödvändig att behandla för utförandet av den aktuella verksamheten avgöras för varje enskild behandling. En annan sak är att vissa kategorier av personuppgifter alltid kommer att vara nödvändiga att behandla för att vissa delar av verksamheten ska kunna utföras rättsäkert. Som exempel kan nämnas att personuppgifter som på ett tillräckligt säkert sätt identifierar parterna alltid kommer att vara nödvändiga att registrera i det enskilda målet eller ärendet.

7 Lagens syfte och tillämpningsområde

7.1 Domstol

7.1.1 Dataskyddsförordningen

Begreppet domstol, i den del det har betydelse för domstolarnas registerförfattningar, förekommer i följande bestämmelser i dataskyddsförordningen.

- I artikel 9.1 görs ett undantag från förbudet att behandla känsliga personuppgifter bl.a. för det fall personuppgiftsbehandlingen är nödvändig som en del av domstolarnas dömande verksamhet.
- I artikel 37.1 görs ett undantag från skyldigheten att utse dataskyddsombud om personuppgiftsbehandlingen genomförs som en del av domstolarnas dömande verksamhet.
- I artikel 55.3 anges att tillsynsmyndigheterna inte ska vara behöriga att utöva tillsyn över domstolar som behandlar personuppgifter i sin dömande verksamhet.

7.1.2 Hyres- och arrendenämnderna

Domstolsdatalagen gäller, enligt 2 §, för den behandling av personuppgifter som sker hos de allmänna domstolarna, de allmänna förvaltningsdomstolarna och hyres- och arrendenämnderna. Lagen gäller vidare främst för den behandling som sker inom ramen för dessa myndigheters rättskipande och rättsvårdande verksamhet. Innebörden av detta begrepp behandlas i avsnitt 7.2.

Hyres- och arrendenämnderna är myndigheter inom Sveriges domstolar och utför rättsskipande och rättsvårdande verksamhet. Det har emellertid i flera tidigare lagstiftningsärenden bekräftats att nämnderna inte är domstolar utan förvaltningsmyndigheter.¹ I förarbetena till domstolsdatalagen redogjordes inte för någon annan uppfattning.² Fråga uppkommer därmed om hyres- och arrendenämnderna utgör domstolar i dataskyddsförordningens mening.

Hyres- och arrendenämndernas verksamhet

Hyres- och arrendenämndernas verksamhet regleras i lagen (1973:188) om arrendenämnder och hyresnämnder, nedan förkortad nämndlagen. Nämnderna består enligt 2, 3, 5 och 6 §§ nämndlagen i regel av en lagfaren ordförande (hyresråd) och två intresseledamöter, som är väl förtrogna med förhållandena för de två intressen som representeras i tvisten.

Enligt 4 § nämndlagen har hyresnämnderna bl.a. till uppgift att

- medla och vara skiljenämnd i hyres- eller bostadsrättstvister,
- pröva en rad uppräknade tvister enligt 12 kap. jordabalken, bl.a. tvister om överlåtelse av hyresrätt enligt 34–37 §§, upplåtelse av lägenhet i andra hand enligt 40 §, förlängning av hyresavtal enligt 49 § samt återbetalning och fastställande av hyra enligt 55 e §,
- pröva tvister om hyresvillkor enligt 22–24 §§ hyresförhandlingslagen (1978:304),
- pröva tvister om hyresvillkor enligt 3 kap. 14 § lagen (2002:93) om kooperativ hyresrätt,
- pröva tvister om medlemskap enligt 2 kap. 10 § bostadsrättslagen (1991:614), och
- pröva tvister mellan hyresvärd och hyresgästorganisation enligt hyresförhandlingslagen.

¹ Se t.ex. prop. 1971:30 s. 607, prop. 1973:23 s. 199 och prop. 1974:151 s. 145.

² Se bl.a. Ds 2013:10 s. 45 och prop. 2014/15:148 s. 24.

Enligt 1 § nämndlagen har arrendenämnderna bl.a. till uppgift att

- medla och vara skiljenämnd i arrendetvister,
- pröva tvister om förlängning av arrendeavtal vid jordbruksarrende, bostadsarrende eller fiskearrende, och
- pröva frågor enligt lagen (1985:658) om arrendatorers rätt att förvärva arrendeställe.

7.1.3 Hyres- och arrendenämndernas rättsliga ställning

Frågans tidigare behandling

I departementspromemorian ”Effektivare hyres- och arrendenämnder” (Ds 2016:4 s. 13) beskrivs nämnderna som förvaltningsmyndigheter med domstolsliknande uppgifter.

I förarbetena till dåvarande lagen (1988:205) om rättsprövning av vissa förvaltningsbeslut uttalades att hyres- och arrendenämndernas funktion, organisation, utredningsmöjligheter och självständiga ställning i allt väsentligt motsvarar vad som brukar utmärka en domstol. Det anfördes att starka skäl därför talar för att likställa nämnderna med domstolar (prop. 1987/88:69 s. 36).

Målutredningen (SOU 2010:44 s. 291–293) föreslog i sitt betänkande att ett generellt krav på prövningstillstånd skulle införas för överklagande till hovrätt och kammarrätt. Målutredningen gjorde i samband med detta bedömningen att en prövning av hyres- och arrendenämnd uppfyller Europadomstolens krav på domstolsprövning och att kravet på prövningstillstånd därför också skulle gälla för nämndernas avgöranden. Målutredningen konstaterade att det avgörande för denna fråga var om man betraktar nämnderna som domstolsliknande organ, dvs. om deras prövning kan sägas helt ersätta den första domstolsinstansens prövning. Enligt Målutredningen var så fallet om nämndernas prövning uppfyller kraven för domstolsprövning enligt artikel 6 Europakonventionen. Utredningen noterade att det av Europadomstolens praxis framgår att också myndigheter som inte nationellt sett utgör domstolar kan betraktas som domstolar i Europakonventionens mening. Avgörande är om organet vid sin prövning uppfyller de rättssäkerhetsgarantier som Europa-

konventionen kräver. Målutredningen noterade också att hyres- och arrendenämnderna är opartiska organ som är upprättade med stöd av lag och med lagfarna ordförande samt konstaterade att regeringen anställer hyresråden med fullmakt efter Domarnämndens förslag och att övriga ledamöter har särskild sakkunskap inom hyres- respektive arrendenämndernas områden. Enligt Målutredningen har nämnderna därför en minst lika kvalificerad sammansättning som tingsrätterna. Utredningen noterade vidare att nämndernas verksamhet i stor utsträckning är sådan att den hade kunnat utföras av tingsrätt samt att också det faktum att besluten överklagas direkt till hovrätt talar för att nämndernas prövning motsvarar en prövning av tingsrätt. Enligt utredningen påminner även nämndernas procedurregler om de vid domstol.³

EU-domstolen

Som framgår ovan är Europadomstolens domstolsbegrepp vidare än det svenska. Inte heller EU-domstolen använder domstolsbegreppet lika snävt som i svenskt språkbruk.⁴

I artikel 267 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) regleras en skyldighet respektive möjlighet för medlemsstaternas domstolar att begära förhandsavgörande av EU-domstolen. Enligt bestämmelsen finns det en skyldighet för domstol som utgör sista instans enligt nationell lagstiftning att begära ett förhandsavgörande när en fråga som sådant kan begäras för uppkommer i ett ärende vid domstolen. Domstol som inte utgör sista instans har inte sådan skyldighet, däremot en möjlighet att begära förhandsavgörande av EU-domstolen om de anser att det är nödvändigt för att döma i saken.

EU-domstolen har i olika avgöranden slagit fast vilka kriterier som är av betydelse vid bedömningen av vilka organ som omfattas av domstolsbegreppet enligt artikel 267 i EUF-fördraget. Det krävs enligt EU-domstolen att organet är upprättat enligt lag och är av stadigvarande karaktär. Vidare krävs att dess jurisdiktion är av

³ Jfr Utredningen om hyres- och arrendetvistens betänkande (SOU 2012:82 s. 114–145).

⁴ Se bl.a. Melin, Våra domstolar, organisation och verksamhet m.m. [2012, Zeteo], s. 40.

tvingande art, att förfarandet är kontradiktoriskt, att det tillämpar rättsregler och att det har en oberoende ställning.⁵

EU-domstolen har i sin praxis ansett att Överklagandenämnden för högskolan omfattas av domstolsbegreppet och därmed har rätt att begära förhandsavgörande.⁶ Det samma gäller den tidigare Utlänningsnämnden.⁷ Dock har EU-domstolen inte ansett att Skatterättsnämnden omfattas av begreppet.⁸

7.1.4 Bedömning

Bedömning: Hyres- och arrendenämnderna utgör domstolar i dataskyddsförordningens mening.

Hyres- och arrendenämnderna består av kvalificerade ledamöter och har en lagfaren ordförande som utses av regeringen. Av de exempel på hyres- och arrendenämndernas verksamhet som finns i avsnitt 7.1.2 framgår att nämndernas verksamhet i huvudsak består i att lösa tvister mellan enskilda. Processen är således kontradiktorisk. Besluten är vidare bindande för parterna. Eftersom nämnderna är förvaltningsmyndigheter garanteras deras självständighet i beslutsfattandet vid myndighetsutövning mot enskilda och vid lagtillämpning av 12 kap. 2 § RF. Mot den bakgrunden förefaller nämndernas sammansättning och uppgifter vara väldigt lika domstolarnas. Detta talar för att hyres- och arrendenämnderna bör betraktas som domstolar i unionsrättslig mening och därmed även i dataskyddsförordningens mening.

Av skäl 20 i dataskyddsförordningen framgår vidare att syftet med att begränsa tillsynsmyndigheternas behörighet så att den inte omfattar domstolarnas dömande verksamhet är att säkerställa domstolsväsendets oberoende när det utför sin rättskipande verksamhet, inbegripet när det fattar beslut. Vikten av en oberoende bedömning – som således är skälet till att domstolarnas dömande verksamhet ligger utanför tillsynsmyndigheternas

⁵ Se bl.a. målen *Gabalfrisa m.fl.*, C-110-147/98, EU:C:2000:145.

⁶ Målen *Abrahamsson och Andersson*, C-407/98, EU:C:2000:367.

⁷ Mål *Jia*, C-1/05, EU:C:2007:1.

⁸ Mål *Victoria Film*, C-134/97, EU:C:1998:535.

behörighet – gör sig naturligtvis gällande även för hyres- och arrendenämndernas verksamhet.

Mot den bakgrunden bedömer vi att hyres- och arrendenämnderna utgör domstolar i dataskyddsförordningens mening. När det i dataskyddsförordningen föreskrivs vissa regler för domstolar bör utgångspunkten enligt vår mening därför vara att detta även gäller för hyres- och arrendenämnderna.

7.2 Rättskipande och rättsvårdande verksamhet

7.2.1 Domstolsdatalagen

Enligt 1 § domstolsdatalagen är syftet med lagen att ge de allmänna domstolarna, de allmänna förvaltningsdomstolarna och hyres- och arrendenämnderna möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin rättskipande och rättsvårdande verksamhet och att skydda människor mot att deras personliga integritet kränks vid sådan behandling. Lagens syftesbestämmelse har enligt vår mening ingen självständig rättslig betydelse, eftersom tillämpningsområdet beskrivs i 2 § domstolsdatalagen. Vid tillkomsten av domstolsdatalagen gjorde regeringen dock bedömningen att lagens dubbla syfte på detta sätt borde komma till tydligt uttryck (prop. 2014/15:148 s. 29).

Av 2 § första stycket domstolsdatalagen framgår att lagen gäller vid behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och hyres- och arrendenämndernas rättskipande och rättsvårdande verksamhet. Det anges vidare att lagen också gäller när personuppgifterna vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran.

Dataskyddsförordningen innehåller vissa bestämmelser som omfattar domstolarnas dömande verksamhet, t.ex. artikel 55.3 där undantag från tillsynsmyndighetens behörighet görs för denna verksamhet. Det faktum att begreppet rättskipande och rättsvårdande verksamhet inte används i dataskyddsförordningen hindrar emellertid inte att tillämpningsområdet för en nationell registerförfattning avgränsas till dessa verksamheter (se avsnitt 5.3).

En analys av begreppet dömande verksamhet finns i kapitel 8. För att kunna relatera detta begrepp till de svenska domstolarnas

verksamhet krävs enligt vår mening även en analys av innebörden av begreppet rättskipande och rättsvårdande verksamhet. Det är även av intresse vilken del av domstolarnas verksamhet som är rättskipande respektive rättsvårdande och vilka eventuella skillnader som finns mellan dessa verksamheter.

7.2.2 Tidigare förarbeten

Begreppet rättskipande och rättsvårdande verksamhet användes redan år 2001 för att avgränsa Vera-förordningarnas tillämpningsområde. I Domstolsdatautredningens slutbetänkande (SOU 2001:100 s. 66) anförs att det förhållandet att Vera-förordningarna endast omfattar rättskipande och rättsvårdande verksamhet innebär att omfattningen begränsas till i huvudsak handläggningen av mål och ärenden och de andra arbetsuppgifter som har anknytning till handläggningen. I departementspromemorian med förslag till domstolsdatalag (Ds 2013:10 s. 46) har sedan konstaterats att den rättskipande och rättsvårdande verksamheten utgör domstolarnas s.k. kärnverksamhet.

I förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 27–28) gjorde regeringen följande ställningstagande gällande begreppet rättskipande och rättsvårdande verksamhet.

Begreppet rättskipande och rättsvårdande verksamhet inskränker sig i detta sammanhang inte enbart till handläggningsåtgärder som vidtas enligt en processuell bestämmelse, utan är avsett att ha en vidare innebörd. Exempelvis är hanteringen av ansökningsavgifter, liksom omlottning och förtursförklaring av mål, åtgärder som har en omedelbar koppling till mål- och ärendehantering och som därför bör betraktas som en del av den rättskipande och rättsvårdande verksamheten. Detta gäller både insamlandet av personuppgifter och den vidare hanteringen av uppgifterna. Insamling av personuppgifter avseende ombud, tolkar, vittnen och andra aktörer samt den fortsatta hanteringen av dessa uppgifter i samband med registerföring, kallelser och utbetalning av ersättningar är andra exempel på personuppgiftsbehandlingar som också är avsedda att rymmas i begreppet rättskipande och rättsvårdande verksamhet. Personuppgifter avseende anställda vid domstolen behandlas enligt regeringens bedömning såväl i den administrativa som i den rättskipande och rättsvårdande verksamheten. I den administrativa verksamheten hanteras sådana personuppgifter exempelvis i samband med löneutbetalning, vid indelning på avdelningar eller enheter och när beredskapslistor upprättas. Sådan behandling är inte avsedd att omfattas av den nya

lagen. Personuppgifter som avser domstolens anställda behandlas emellertid också i direkt anslutning till hanteringen av mål och ärenden, exempelvis i domar, uppropslistor och förelägganden. Behandlingen av personuppgifter i sådana fall får enligt regeringen anses ske i den rättskipande och rättsvårdande verksamheten. När det gäller nämndemän behandlar domstolarna också personuppgifter i flera olika sammanhang. Insamling av sådana personuppgifter, liksom den fortsatta hanteringen i form av exempelvis behörighetskontroller, kontroll av utdrag ur belastningsregistret, upprättande av adressregister och indelningsbeslut sker i den administrativa verksamheten som styrs av personuppgiftslagen. Samma sak gäller utbetalning av ersättning till nämndemän för deras medverkan i handläggningen. Nämndemäns personuppgifter behandlas emellertid också i direkt anslutning till hanteringen av mål och ärenden, t.ex. vid upprättande av domar. Denna behandling sker i den rättsvårdande och rättskipande verksamheten och i dessa fall blir således domstolsdatalagen tillämplig.

Valet av begreppet rättskipande och rättsvårdande verksamhet i domstolsdatalagen förefaller således ha gjorts främst för att utesluta domstolarnas administrativa verksamhet, såsom personal- och löneadministration eller lokalförsörjningsfrågor, från lagens tillämpningsområde. Någon anledning för lagstiftaren att i anslutning till registerlagstiftningen närmare definiera vilken del av domstolarnas kärnverksamhet som består av rättskipning respektive rättsvård har därför inte funnits.

7.2.3 Offentlighets- och sekretesslagen

I offentlighets- och sekretesslagen (2009:400), förkortad OSL, förekommer begreppet rättskipande och rättsvårdande verksamhet i ett flertal bestämmelser. Som exempel kan nämnas att enligt 6 kap. 8 och 9 §§ OSL gäller en särskild instansordning för överklagande av beslut som meddelats av vissa domstolar i deras rättskipande och rättsvårdande verksamhet. Enligt 36 kap. 2 § OSL gäller vidare sekretess i en domstols rättskipande eller rättsvårdande verksamhet under vissa förutsättningar för uppgift om en myndighets eller en enskilds affärs- eller driftsförhållanden. Ett annat exempel är den överföring av sekretess som enligt 43 kap. 2 § OSL i vissa fall gäller när en domstol i sin rättskipande eller rättsvårdande verksamhet får sekretessreglerad uppgift från en domstol eller en annan myndighet.

Någon redogörelse för skillnaden mellan de två begreppen lämnas inte i förarbetena till OSL. Det framkommer dock att det samlade begreppet ”rättskipande och rättsvårdande verksamhet” valts för att utesluta domstolarnas rent administrativa verksamhet från bestämmelsernas tillämpningsområde.⁹

7.2.4 Rättegångsbalken

Inom juridiken har man traditionellt skilt mellan stridig och frivillig rättsvård. Den stridiga rättsvården har sedan länge betecknats som rättskipning. Ett exempel på begreppet rättskipning är det primära tillämpningsområdet för rättegångsbalken, vilket består av tvistemåls- och brottmålsrättegångar i allmän domstol.¹⁰ Ärendeutredningen (SOU 2007:65 s. 116) menade i sitt betänkande att utgångspunkten i mål som handläggs enligt rättegångsbalken regelmässigt är ett rättsförhållande som uppstått före processen och att det typiskt sett gäller för domstol att ta ställning till vad som förekommit i förfluten tid.

7.2.5 Ärendelagen

För de ärenden i allmän domstol som ska tas upp av en tingsrätt men inte ska handläggas enligt rättegångsbalken gäller lagen (1996:242) om domstolsärenden, nedan förkortad ärendelagen. Detta framgår av 1 § ärendelagen, där det också framgår att de ärenden som handläggs enligt lagen kallas rättsvårdsärenden. Ärendeutredningen (SOU 2007:65 s. 116) menade att ärendelagens primära tillämpningsområde är den s.k. frivilliga rättsvården, där processen i allmänhet inte fokuserar på vad som redan förevarit.

De ärenden som avgörs med stöd av de processuella reglerna i ärendelagen är bl.a.

- associationsärenden; exempelvis näringsförbud enligt lagen (2014:836) om näringsförbud och dödande av handling i

⁹ Jfr prop. 1979/80:2 Del A s. 299.

¹⁰ Se Fitger, Lagen om domstolsärenden, (1 augusti 2004, Zeteo), kommentaren till 1 § samt Ärendeutredningens betänkande (SOU 2007:65 s. 116).

samband med utmätning och konkurs enligt lagen (2011:900) om dödande av förkommen handling,

- ärenden med anknytning till föräldrabalken; exempelvis handläggning av ärenden om adoption enligt 4 kap., förordnande av förvaltare och god man enligt 11 kap. och överklagande av överförmyndarens beslut enligt 20 kap.,
- ärenden med anknytning till äktenskapsbalken; exempelvis förordnande av bodelningsförrättare enligt 17 kap.,
- disciplinärenden; exempelvis överklagande av ett beslut om disciplinpåföljd enligt lagen (1994:1811) om disciplinansvar inom totalförsvaret m.m.,
- exekutionsrättsliga ärenden; exempelvis överklagande av Kronofogdemyndighetens beslut enligt 18 kap. 1 § utsökningsbalken, överklagande av Kronofogdemyndighetens beslut om avräkning enligt lagen (1985:146) om avräkning vid återbetalning av skatter och avgifter samt överklagande av Kronofogdemyndighetens beslut om arbetsgivares kvittningsrätt enligt lagen (1970:215) om arbetsgivares kvittningsrätt,
- felparkeringsärenden; exempelvis överklagande av Polismyndighetens beslut att avslå begäran om ändring i betalningsansvar enligt lagen (1976:206) om felparkeringsavgift,
- kallelser på okända borgenärer; exempelvis överklagande av Kronofogdemyndighetens eller Bolagsverkets beslut i fråga om kungörelse enligt lagen (1981:131) om kallelse på okända borgenärer.

7.2.6 Innebörden av begreppet rättskipning

Rättskipning innefattar allmän domstols handläggning av mål i enlighet med de processuella reglerna i rättegångsbalken. Utifrån den traditionella definitionen av rättskipning såsom stridig rättsvård, måste begreppet rättskipning enligt vår mening också innefatta de allmänna förvaltningsdomstolarnas handläggning av mål i enlighet med förvaltningsprocesslagen (1971:291) med anledning av överklagande av beslut fattade av förvaltnings-

myndigheter. Även i dessa fall rör det sig om stridig rättsvård, dock ”slits tvisten” i den stora merparten av målen mellan en myndighet och en eller flera fysiska eller juridiska personer.

Även i de fall mål i förvaltningsrätt inleds genom en ansökan har målen karaktären av en tvåpartsprocess, där olika intressen står mot varandra. Som exempel kan nämnas en leverantörs ansökan om överprövning av en offentlig upphandling enligt 20 kap. 4 § lagen (2016:1145) om offentlig upphandling. Ett annat exempel är Skatteverkets ansökan om betalningssäkring för att säkerställa betalning av skatter m.m. enligt lagen (1978:880) om betalningssäkring för skatter, tullar och avgifter eller om betalningsskyldighet för företrädare för juridiska personer (s.k. företrädaransvar) enligt 59 kap. 16 § skatteförfarandelagen (2011:1244). Ytterligare ett exempel är ansökan om utdömande av vite enligt viteslagen (1985:206).

Vidare måste en socialnämnds ansökan om att en person ska vårdas med stöd av lagen (1990:52) med särskilda bestämmelser om vård av unga eller lagen (1988:870) om vård av missbrukare i vissa fall, anses ingå i begreppet rättsskipning. Det rör sig här om mycket ingripande beslut för enskilda personer och en förutsättning för att ansökan ska bifallas är att vården inte kan ges på frivillig väg. Motsvarande gäller ansöknings- eller anmälningsförfarandet enligt lagen (1991:1128) om psykiatrisk tvångsvård respektive lagen (1991:1129) om rättspsykiatrisk vård.

Även hyres- och arrendenämndernas verksamhet bör utifrån den traditionella definitionen av begreppet utgöra rättsskipande verksamhet. Som framgår av exemplen i avsnitt 7.1.2 består nämndernas verksamhet i huvudsak i att lösa tvister mellan enskilda.

7.2.7 Innebörden av begreppet rättsvårdande verksamhet

Begreppet rättsvård förefaller traditionellt sett ha ansetts innefatta den ärendehantering som sker i allmän domstol. Efter Ärendeutredningens betänkande flyttades år 2011 vissa otvistiga ärenden, som huvudsakligen avser s.k. frivillig rättsvård, över till

förvaltningsmyndighet.¹¹ Syftet med detta var att renodla domstolarnas verksamhet till att avse endast dömande uppgifter. Ärendeutredningen gjorde i sitt betänkande en i princip heltäckande kartläggning av de ärendetyper som hanteras av allmän domstol. I enlighet med Ärendeutredningens uppdrag att renodla domstolarnas verksamhet får det förutsättas att de ärenden som nu kvarstår hos domstolarna har sådan karaktär att en domstolsprövning anses viktig. Skälen till detta kan bl.a. vara rättssäkerhetsaspekter eller att ärendena har bedömts kräva sådana rättsliga överväganden som lämpar sig bäst för domstol.¹²

Som åskådliggjorts i exemplen i avsnitt 7.2.5 är de ärenden som alltjämt handläggs av allmän domstol av mycket olika karaktär. I vissa fall liknar de den tvåpartsprocess mellan myndighet och enskild som avgörs genom de allmänna förvaltningsdomstolarnas rättskipning. Som exempel kan nämnas ärenden om felparkeringsavgift och disciplinärenden. I andra fall rör det sig om en regelrätt ansökan, men där en bedömning av enskildas intressen måste göras av domstolen. Detta gäller exempelvis adoptionsärenden, där domstolen ska ta hänsyn till barnets bästa. Ett annat exempel är en överförmyndarnämnds ansökan om förvaltare för en enskild, som kan resultera i ett mycket ingripande beslut för den enskilde.

Vi bedömer att de s.k. rättsvårdsärenden som numera handläggs av de allmänna domstolarna har större likheter med den rättskipning som sker i de allmänna domstolarna och de allmänna förvaltningsdomstolarna än med den ärendehandläggning som sker hos förvaltningsmyndigheterna. Vår bedömning i denna del har betydelse för tolkningen av dataskyddsförordningens begrepp ”dömande verksamhet” (se avsnitt 8.4).

¹¹ Exempelvis flyttades ärenden om dödande av förkommen handling över till Kronofogdemyndigheten, ansvarig inskrivningsmyndighet respektive Bolagsverket (se 4 § lagen (2011:900) om dödande av förkommen handling). Ett annat exempel är handläggningen av ärenden om registrering av äktenskapsförord och bodelning, som flyttades över till Skatteverket (se 7 kap. 3 § och 9 kap. 1 ÅktB).

¹² Jfr SOU 2007:65 s. 24 och prop. 2010/11:119 s. 1.

7.2.8 Bedömning

Förslag: Om inte annat anges i den bestämmelse som reglerar avgränsningen mot den personuppgiftsbehandling som faller under 2016 års dataskyddsdirektivs tillämpningsområde, ska domstolsdatalagen även fortsättningsvis gälla vid behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och hyres- och arrendenämndernas rättskipande och rättsvårdande verksamhet samt när personuppgifterna vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran.

Medlemsstaternas har, enligt artikel 6.2 i dataskyddsförordningen, möjlighet att utarbeta eller behålla registerförfattningar. Inom ramen för denna möjlighet bör medlemsstaterna kunna bestämma tillämpningsområdet för registerförfattningarna på ett sätt som är lämpligt, så länge förordningens allmänna principer för behandling av personuppgifter följs (se avsnitt 5.3).

Regeringen har i tidigare förarbeten gjort bedömningen att domstolsdatalagens syfte bör komma till tydligt uttryck (prop. 2014/15:148 s. 29). Dataskyddsförordningen föranleder inte heller någon ändring av den inledande syftesbestämmelsen i 1 § domstolsdatalagen. Denna bör därför kvarstå i sin nuvarande lydelse.

Den verksamhet som omfattas av tillämpningsbestämmelsen i 2 § första stycket domstolsdatalagen är vidare väl definierad i förarbetena. Eftersom dataskyddsförordningen inte föranleder någon ändring av tillämpningsområdet i denna del bör domstolsdatalagen även framöver gälla vid behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och hyres- och arrendenämndernas rättskipande och rättsvårdande verksamhet samt när personuppgifterna vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran.

Vi har dock, i avsnitt 4.3.2, föreslagit att domstolsdatalagen inte ska gälla vid behandling av personuppgifter i de allmänna domstolarnas och de allmänna förvaltningsdomstolarnas verksamhet som omfattas av brottsdatalagens tillämpningsområde. För att underlätta för tillämparen har vi föreslagit att detta klargörs

redan i domstolsdatalagens inledande bestämmelser om tillämpningsområdet.

7.3 Automatiserad behandling och manuella register

Bedömning: Dataskyddsförordningen föranleder ingen ändring av domstolsdatalagens bestämmelse om att lagen endast gäller för sådan personuppgiftsbehandling som är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Domstolsdatalagen är enligt 2 § andra stycket tillämplig på personuppgiftsbehandling som är ”helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier”. Avgränsningen av domstolsdatalagens tillämpningsområde motsvarar i denna del därmed personuppgiftslagens tillämpningsområde så som det beskrivs i 5 §.

Dataskyddsförordningens materiella tillämpningsområde framgår av artikel 2.1 och beskrivs som “behandling av personuppgifter som helt eller delvis företas på automatisk väg samt annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register”. Förordningens tillämpningsområde är därmed något annorlunda beskrivet än domstolsdatalagens tillämpningsområde. Tillämpningsområdet för 2016 års dataskyddsdirektiv beskrivs på liknande sätt i artikel 2.2.

Av skäl 15 till dataskyddsförordningen, där förordningens tillämpningsområde berörs, framgår att ”*skyddet för fysiska personer bör vara tillämpligt på både automatiserad och manuell behandling av deras personuppgifter...*”. I skälen används således begreppet ”automatiserad” i stället för ”på automatisk väg”. De två uttrycken kan därmed inte gärna uppfattas som annat än synonyma. Någon begreppsskillnad mellan förordningens ”på automatisk väg” respektive domstolsdatalagens ”automatiserad” finns enligt vår bedömning därmed inte.

Begreppet *automatiserad* har använts i personuppgiftslagen under lång tid och är väl inarbetat även i de svenska registerförfattningarna.¹³ Vi anser att det inte finns någon risk för att domstolsdatalagens tillämpningsområde misstolkas om begreppet får kvarstå. Mot den bakgrunden anser vi att begreppet *automatiserad* bör kvarstå i domstolsdatalagen.

I artikel 4.6 i dataskyddsförordningen framgår att med register i förordningens mening 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”. Samma definition finns i artikel 3.6 i 2016 års dataskyddsdirektiv. Någon saklig skillnad mellan dataskyddsförordningens ”register” och domstolsdatalagens ”strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier” finns enligt vår uppfattning inte, eftersom den avslutande bisatsen i dataskyddsförordningens definition inte ändrar avgränsningen av definitionen i sak.

Trots de något olika uttrycken i dataskyddsförordningen respektive domstolsdatalagen gör vi bedömningen att förordningens materiella tillämpningsområde i denna del stämmer överens med domstolsdatalagens nuvarande tillämpningsområde.

Vid införandet av personuppgiftslagen gjordes bedömningen att begreppet register är otidsenligt (prop. 1997/98:44 s. 39). Mot den bakgrunden valde lagstiftaren att inte använda det begreppet. I stället användes i personuppgiftslagen den längre beskrivning av begreppet register som nu också används i domstolsdatalagen.

När dataskyddsförordningen börjar tillämpas kommer de svenska registerförfattningarna att utgöra en komplettering till förordningen. Man skulle därför kunna argumentera för att begreppet register bör användas även i domstolsdatalagen. Detta skulle kunna undanröja risken för missförstånd och skilda tolkningar av begreppet. Definitionen av register i artikel 4.6 i dataskyddsförordningen innehåller vidare, som vi pekat på ovan, ytterligare beskrivningar av begreppet än ”tillgänglighet enligt särskilda kriterier”. En användning av samma begrepp i

¹³ Se bl.a. 1 kap. 2 § andra stycket polisdatalagen (2010:361) och 1 kap. 2 § andra stycket kustbevakningsdatalagen (2012:145).

domstolsdatalagen skulle innebära att man inte tappar delar av definitionen.

Utredningen om 2016 års dataskyddsdirektiv har dock i sitt betänkande (SOU 2017:29) föreslagit att uttrycket ”strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier” ska användas i brottsdatalagen i stället för begreppet register. Det är enligt vår mening värdefullt att, så långt det är möjligt, använda samma begrepp i alla de svenska författningar som rör personuppgiftsbehandling. Brottsdatalagen och dess kompletterande registerförfattning kommer vidare att vara tillämplig på den del av domstolarnas verksamhet som styrs av 2016 års dataskyddsdirektiv, (se kapitel 4). Det uttryck som föreslagits för brottsdatalagen är dessutom väl inarbetat i svensk rätt genom bl.a. personuppgiftslagen och registerförfattningar. Mot den bakgrunden bedömer vi att domstolsdatalagens tillämpningsområde kan och bör kvarstå oförändrat i denna del.

8 Dömande verksamhet

Begreppet *dömande verksamhet* förekommer i tre olika sammanhang i dataskyddsförordningen.

- I artikel 9.1 görs undantag från förbudet att behandla känsliga personuppgifter bl.a. för det fall personuppgiftsbehandlingen är nödvändig som en del av domstolarnas dömande verksamhet.
- I artikel 37.1 görs undantag från skyldigheten att utse dataskyddsombud om personuppgiftsbehandlingen genomförs som en del av domstolarnas dömande verksamhet.
- I artikel 55.3 anges att de nationella tillsynsmyndigheterna inte ska vara behöriga att utöva tillsyn över domstolar som behandlar personuppgifter i sin dömande verksamhet.

De svenska domstolarnas rättskipande och rättsvårdande verksamhet anses omfatta domstolarnas kärnverksamhet. I denna kärnverksamhet ingår handläggningen av mål och ärenden, men även de andra arbetsuppgifter som har anknytning till denna handläggning (se vidare avsnitt 7.2.2). I motsats till den vida innebörden av rättskipande och rättsvårdande verksamhet kan begreppet *dömande verksamhet* i svenskt språkbruk te sig relativt snävt. Det ligger nära till hands att – utifrån ordalydelsen – i begreppet endast innefatta den del av domstolarnas verksamhet som innebär att domar eller beslut utformas och meddelas. Frågan uppkommer om dataskyddsförordningens begrepp ska ges denna snäva innebörd, eller om det även omfattar ytterligare delar av den rättskipande och rättsvårdande verksamheten.

Vi anser att det inom ramen för vårt uppdrag finns anledning att göra en bedömning av dataskyddsförordningens begrepp *dömande verksamhet*. Det handlar om ett begrepp som inte har sin motsvarighet i 1995 års dataskyddsdirektiv och som kommer att ha

stor betydelse för bl.a. tillsynen av domstolarnas verksamhet. Detta får i sin tur genomslag när det gäller dataskyddsombudets arbetsuppgifter (se avsnitt 13.5.3) och den information som i vissa fall ska lämnas till de registrerade (se avsnitt 15.3.3).

Vi kommer därför i detta kapitel att ge en bild av de faktorer som vi anser bör vägas in när begreppet ska fastställas. För att kunna ta ställning till hur de frågor som påverkas av begreppet ska bedömas kommer vi också att göra en bedömning av begreppets innebörd utifrån dessa faktorer. Den slutliga definitionen av begreppet och var gränsen går för tillsynsmyndighetens behörighet över domstolarnas verksamhet får dock slutligt avgöras av unionsrättslig praxis.

8.1 Nuvarande tillsyn över domstolarna

8.1.1 Datainspektionen

Enligt artikel 55.3 i dataskyddsförordningen utesluts domstolarnas dömande verksamhet från tillsynsmyndigheternas behörighet att utöva tillsyn. I 1995 års dataskyddsdirektiv finns inte någon motsvarande bestämmelse. Datainspektionens tillsyn av domstolarnas verksamhet begränsas dock för närvarande av bestämmelsen i 11 kap. 3 § RF, som ger uttryck för principen om domstolarnas självständighet i dömandet. Enligt denna bestämmelse får ingen myndighet, inte heller riksdagen, bestämma hur en domstol ska döma i det enskilda fallet eller hur en domstol i övrigt ska tillämpa en rättsregel i ett särskilt fall.

I rättsfallet HFD 2014 ref. 32 uttalade Högsta förvaltningsdomstolen att bestämmelsen i 11 kap. 3 § RF inte omfattar sådana beslut som en domstol fattar i den egna verksamheten avseende domstolens administration. Högsta förvaltningsdomstolen bedömde därefter att det inte fanns hinder för Datainspektionen att utöva tillsyn över den behandling av personuppgifter som skett genom att en domstol publicerat uppropplistor på den egna webbplatsen.

Den slutsats som kan dras av Högsta förvaltningsdomstolens resonemang är att den administrativa verksamhet som sker inom en domstol inte omfattas av skyddet i 11 kap. 3 § RF. Vidare innebär åtminstone den behandling av personuppgifter som består av att en

domstol offentliggör uppspelslistor på internet ett led i den administrativa verksamheten och inte den dömande. Om detta även gäller själva framtagandet av uppspelslistor med hjälp av domstolarnas verksamhetsstöd framgår inte av rättsfallet. Utifrån Högsta förvaltningsdomstolens hänvisning till förordningen (1996:381) med tingsrättsinstruktion gällande tingsrätts skyldighet att upprätta uppspelslistor kan man dock förutsätta att så är fallet.

Datainspektionen har vidare år 2014 utfört tillsyn gentemot fyra domstolar med inriktning på ”allmänhetens terminaler”, som gav allmänheten möjlighet att söka i verksamhetsregistret vid den domstol där terminalen var belägen.¹ Datainspektionens ansåg att innehållet i allmänhetens terminal innebar att domstolarna behandlade personuppgifter i strid med 9 § första stycket f PuL. Domstolarna förelades av Datainspektionen att inrätta behandlingen av personuppgifter i allmänhetens terminal på så sätt att endast de uppgifter behandlades som var nödvändiga med hänsyn till ändamålet med behandlingen, vilket var att tillgodose allmänhetens intresse av att ta del av allmänna handlingar.

Det faktum att Datainspektionen har ansett sig behörig att utöva tillsyn gentemot domstolarna vad gäller allmänhetens terminal tyder på att Datainspektionen anser att ett elektroniskt utlämnade av uppgifter till allmänheten genom egen sökning, inte omfattas av det grundlagsstadgade skyddet för domstolarnas oberoende.

8.1.2 Justitieombudsmannen och Justitiekanslern

Även Justitieombudsmannen (JO) och Justitiekanslern (JK) utövar tillsyn över domstolarna. JO:s tillsynsuppgift preciseras i 13 kap. 6 § RF och utgör tillsyn över tillämpningen i offentlig verksamhet av lagar och andra föreskrifter. JK:s tillsynsuppdrag omfattar, enligt 1 § lagen (1975:1339) om Justitiekanslerns tillsyn, tillsyn över att de som utövar offentlig verksamhet efterlever lagar och andra författningar samt i övrigt fullgör sina åligganden.

¹ Datainspektionens beslut den 30 september 2014 mot Attunda tingsrätt (Dnr 1316-2013), Förvaltningsrätten i Uppsala (Dnr 1317-2013), Uppsala tingsrätt (Dnr 1318-2013) och Västmanlands tingsrätt (Dnr 1319-2013).

Både JO och JK får väcka åtal och inleda disciplinförfaranden mot bl.a. domare. Som framgår av de nyss citerade bestämmelserna innefattas även själva dömandet i JO:s och JK:s tillsyn.² Tillsynen avser alltså inte bara t.ex. ordning, handläggning, process och liknande. När det gäller dömandet iakttar JO och JK ändå vissa begränsningar. Den viktigaste är att domstolarnas bedömningar i rättsfrågor och bevisfrågor så gott som aldrig granskas. Här gäller dock enligt praxis ett undantag för bedömningar som är uppenbart oriktiga. Mot sådana anser sig både JO och JK kunna ingripa. För JK:s del sammanhänger detta delvis med myndighetens verksamhet som reglerare av skadeståndsanspråk som riktas mot staten. Enligt 3 kap. 2 § skadeståndslagen ska staten ersätta skador som vållas genom fel eller försummelse vid statens myndighetsutövning. Bedömningar i rättsfrågor och bevisfrågor anses normalt vara felaktiga i bestämmelsens mening endast om de är uppenbart oriktiga.³ Det betyder att JK för att kunna avgöra skadestånds-ärenden ibland måste ta ställning till om en domstols bedömning har varit uppenbart oriktig.⁴

8.2 Dataskyddsförordningen och 2016 års dataskyddsdirektiv

8.2.1 Tolkingen av gemenskapsrättsliga bestämmelser

För att åstadkomma en enhetlig rättstillämpning har unionsrätten i stor utsträckning behövt utveckla sina egna rättsliga begrepp. I CILFIT-avgörandet år 1982 underströk EU-domstolen att EU-rätten använder en egen, särskild terminologi.⁵ Målet gällde ett förhandsavgörande avseende tolkingen av artikel 177 tredje stycket i EEG-fördraget. Sammanfattningsvis uttalade EU-domstolen följande.

² Ett konkret exempel på att JO utövat tillsyn över utformning av domar och beslut när det gäller personuppgiftsbehandling är JO 1998/99 s. 184. JO uttalade här att uppgift om diagnos inte borde ha lämnats i en dom som meddelats av Länsrätten i Gotlands län i ett mål enligt lagen (1993:387) om stöd och service till vissa funktionshindrade.

³ Se bl.a. NJA 2003 s. 285; jfr dock NJA 2007 s. 584.

⁴ Göran Lambertz, Tillsynen över domstolarna, publicerad i festskriften Regeringsrätten 100 år, 2009, s. 254 f.

⁵ Bernitz, Kjellgren, Europarättens grunder, upplaga 5, 2014 s. 190.

Till en början ska hänsyn tas till att gemenskapsrättens bestämmelser är avfattade på flera språk och att de olika språkversionerna är lika giltiga. En tolkning av en gemenskapsrättslig bestämmelse kräver följaktligen en jämförelse av de olika språkversionerna. Vidare ska det, även om de olika språkversionerna helt överensstämmer med varandra, beaktas att gemenskapsrätten använder en egen, särskild terminologi. Det ska för övrigt understrykas att de rättsliga begreppen inte nödvändigtvis har samma innehåll i gemenskapsrätten och i de olika nationella rättsordningarna. Slutligen måste varje gemenskapsrättslig bestämmelse sättas in i sitt sammanhang och tolkas mot bakgrund av gemenskapsrätten som helhet, med hänsyn tagen till gemenskapsrättens syften och dess utvecklingsstadium vid den tidpunkt då den ifrågavarande bestämmelsen ska tillämpas.⁶

EU-domstolen har senare uttalat att samma princip gäller för sekundärrätten, dvs. bland annat förordningar och direktiv. I exempelvis avgörandet *Pie Optiek* uttalade EU-domstolen att det följer av domstolens fasta praxis, såväl av kravet på en enhetlig tillämpning av unionsrätten som av likhetsprincipen, att lydelsen i en unionsbestämmelse som inte innehåller någon uttrycklig hänvisning till medlemsstaternas rättsordningar för fastställandet av bestämmelsens innebörd och tillämpningsområde normalt ska ges en självständig och enhetlig tolkning inom hela Europeiska unionen, med beaktande av bestämmelsens sammanhang och det mål som eftersträvas med den aktuella lagstiftningen.⁷

8.2.2 Olika språkliga versioner av dataskyddsförordningen

I den engelska versionen av dataskyddsförordningen har i samtliga fall begreppet *courts acting in their judicial capacity* valts för att beskriva det som i den svenska versionen kallas för *domstolarnas dömande verksamhet*. I den tyska versionen har uttrycket *Gerichten die im Rahmen ihrer justiziellen Tätigkeit handeln* valts.

I Maastrichtfördraget används engelskans *judicial* och tyskans *justiziell* för det svenska ordet *rättsligt*. Exempel på detta är det

⁶ Dom CILFIT mot Ministero della Sanità, C-283/81, EU:C:1982:335 punkterna 18–20.

⁷ Dom *Pie Optiek*, C-376/11, EU:C:2012:502, punkt 33, med hänvisning till tidigare avgöranden.

engelska respektive tyska ordvalet för svenskans *civil-* respektive *straffrättsligt samarbete* inom den tidigare tredje pelaren i Maastrichtfördraget.⁸ Engelskans *judicial capacity* skulle dock även kunna översättas till *rättskipande verksamhet*. Exempel på detta finns i artikel 46 c i 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. Här används engelskan *judicial capacity* när den svenska versionen använder begreppet *rättskipande funktion*.

I den franska versionen av dataskyddsförordningen används genomgående uttrycket *les juridictions dans l'exercice de leur fonction juridictionnelle*.

Vi anser att såväl det engelska som det tyska och franska ordvalet närmast kan översättas till *domstolarnas rättsliga verksamhet* alternativt *domstolarnas rättskipande verksamhet*. Språkligt sett förefaller dessa begrepp enligt vår mening vara vidare än den traditionella svenska synen på begreppet *domstolarnas dömande verksamhet* (jfr avsnitt 8.1).

Av skäl 20 i dataskyddsförordningen framgår vidare att syftet med att begränsa tillsynsmyndigheternas behörighet vad gäller domstolarnas dömande verksamhet är att säkerställa oberoendet i den *rättskipande verksamheten*. I den engelska versionen av dataskyddsförordningen har här begreppet *the judicial tasks* valts. I den tyska versionen används begreppet *gerichtlichen Aufgaben* och i den franska versionen *missions judiciaires*⁹. Samtliga dessa begrepp kan enligt vår mening närmast översättas till svenskans *rättslig uppgift/verksamhet*. Vi kan också konstatera att den engelska versionen använder ordet *judicial* för både svenskans *dömande* och svenskans *rättskipande*. Vid en studie av dataskyddsförordningens olika språkliga versioner anser vi därmed sammanfattningsvis att det finns stöd för en vidare tolkning än den traditionellt svenska av det som i den svenska versionen kallas *dömande verksamhet*.

⁸ Avdelning VI, artikel K1.6 och artikel K1.7 i Maastrichtfördraget om Europeiska unionen.

⁹ I avdelning VI, artikel K1.6 och artikel K1.7. I Maastrichtfördraget används det franska begreppet *coopération judiciaire* för de svenska begreppen (civil- och straff)rättsligt samarbete.

8.2.3 Skälen till dataskyddsförordningen och till 2016 års dataskyddsdirektiv

I 2016 års dataskyddsdirektiv begränsas tillsynsmyndighetens behörighet på samma sätt som i dataskyddsförordningen. Enligt artikel 45.2 i direktivet ska medlemsstaterna ”föreskriva att varje tillsynsmyndighet inte ska vara behörig att utöva tillsyn över domstolar som behandlar personuppgifter inom ramen för sin dömande verksamhet”. Enligt samma artikel får medlemsstaterna ”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”. Av skäl 80 i direktivet framgår följande gällande bestämmelsen i artikel 45.2.

(80) Detta direktiv är visserligen tillämpligt på nationella domstolar 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.

Under lagstiftningsärendet gällande dataskyddsförordningen föreslog Europaparlamentet efter första behandlingen att förordningens skäl skulle motsvara den skrivning som senare fastställdes för skäl 80 i 2016 års dataskyddsdirektiv.¹⁰ Under lagstiftningsärendets gång ändrades dock lydelsen av dataskyddsförordningens skäl. Av skäl 20 i förordningen framgår numera följande.

¹⁰ Position of the European Parliament adopted at first reading on 12 March 2014 with a view to the adoption of Regulation (EU) No .../2014 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

(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.

Av skälen till både 2016 års dataskyddsdirektiv och dataskyddsförordningen framgår således att syftet med att begränsa tillsynsmyndighetens behörighet på det sätt som gjorts är att säkerställa domstolarnas oberoende. I direktivet uttrycks det som ska skyddas som *domarnas oberoende när de utför sina rättsliga uppgifter*. I förordningen används i stället ordvalet *domstolsväsendets oberoende när det utför sin rättsskipande verksamhet*. Vi anser att det ordval som gjorts i båda fallen talar för att dataskyddsförordningens och direktivets begrepp *dömande verksamhet* är avsett att ha en vidare innebörd och innefatta fler delar av domstolarnas kärnverksamhet än endast utformandet av beslut eller domar. För denna slutsats talar även valet att lägga till beslutsfattandet som ett exempel på dömande verksamhet i skäl 20 i dataskyddsförordningen.

Vad gäller dataskyddsförordningens undantag från skyldigheten att utse dataskyddsombud framgår av skäl 97 i förordningen att myndigheter bör utse dataskyddsombud, med ”undantag för domstolar eller oberoende rättsliga myndigheters behandling av personuppgifter som en del av deras dömande verksamhet”. Vi anser att det faktum att även andra myndigheter än domstolar anses kunna bedriva dömande verksamhet tyder på att begreppet är avsett att ha en vid omfattning.

8.2.4 Europeiska datatillsynsmannens uppfattning

Under lagstiftningsarbetets gång inom EU har Europeiska datatillsynsmannen, förkortad EDPS, framfört sin uppfattning om bland annat undantaget för domstolarnas dömande verksamhet från tillsynsmyndighetens behörighet. Dokumentet *Opinion of the European Data Protection Supervisor on the data protection reform package* den 7 mars 2012 innehåller EDPS rekommendationer efter det första utkastet till 2016 års dataskyddsdirektiv och dataskyddsförordningen. EDPS efterlyste här bättre vägledning i skälen angående vad som anses ingå i den dömande verksamhet som är undantagen från tillsynsmyndighetens behörighet. EDPS menade vidare att han tolkar att undantaget för dömande verksamhet innefattar *more particularly the processing of personal data in judicial proceedings on individual cases. On the other hand, the data protection principles – including supervision – should remain applicable, for instance, to processing of personal data by the registry, publication of public reports of proceedings, and publication of judicial decisions.*¹¹

Det förslag som då fanns från kommissionen var vad gäller artikel 55.3 i dataskyddsförordningen i stort sett identiskt med den slutliga versionen. Förslaget till det som nu är skäl 20 i dataskyddsförordningen motsvarade dock inte den ordalydelse som därefter valdes. Förslaget till skäl hade dock stora likheter med de skäl (80) som nu återfinns i 2016 års dataskyddsdirektiv. I den slutliga versionen av dataskyddsförordningen har dock förstärkningsorden tagits bort. *Strikt inskränkt till genuint rättsliga verksamheter i domstolsmål* anges numera endast som *inskränkt till rättsliga verksamheter i domstolsmål*.

EDPS gav vidare den 28 oktober 2015 rekommendationer inför utformandet av 2016 års dataskyddsdirektiv.¹² EDPS konstaterade här att möjligheten att undanta domstolarnas dömande verksamhet från tillsyn väcker stora frågor angående bestämmelsens tolkning och räckvidd.¹³ EDPS anförde också att han anser att kriteriet för

¹¹ Se punkterna 425–426.

¹² Opinion 6/2015 A further step towards comprehensive EU data protection EDPS recommendations on the Directive for data protection in the police and justice sectors.

¹³ ”The possibility to exclude the courts, acting in their judicial capacity, from supervision raises serious issues of interpretation and scope. We, therefore, recommend – with a reference to recital 55 of the proposal of the Commission – to keep the term “genuine” judicial activities

att undanta domstolars personuppgiftsbehandling bör vara om behandlingen äger rum inom ramen för *the judicial activity* snarare än att gränsen ska gå mellan olika kategorier av personuppgiftsansvariga. Som exempel på *judicial activity* nämns rättegångar, rättsliga förfaranden och rättsliga aktiviteter i domstolsmål (trial, judicial proceeding, judicial activities in court cases) eller att behandlingen sker inom ramen för andra aktiviteter där domare är involverade med stöd av nationell lag.¹⁴

Det ovan sagda visar enligt vår mening att EDPS förespråkar en relativt snäv tolkning av begreppet *dömande verksamhet*. Exempelvis verkar EDPS inte anse att den personuppgiftsbehandling som sker när personuppgifter registreras i det automatiserade verksamhetsstödet tillhör den dömande verksamheten. Det bör dock tilläggas att den åsikt EDPS gett uttryck för inte avspeglas i de slutliga versionerna av vare sig dataskyddsförordningen eller 2016 års dataskyddsdirektiv. I stället har de förstärkningsord som skulle kunna tala för en snäv tolkning av undantaget tagits bort i de slutliga versionerna. För dataskyddsförordningens del har exemplifieringen i skäl 20 enligt vår mening snarare öppnat upp för en vidare tolkning av begreppet dömande verksamhet. Vi tänker här på det faktum att beslutsfattandet snarast framstår som ett exempel på vad som ingår i denna verksamhet.

8.3 Andra rättsakter och EU-domstolens avgöranden

EDPS har till uppgift att övervaka gemenskapsinstitutionernas behandling av personuppgifter. EU-domstolen är dock undantagen denna övervakning i dess rättskipande funktion. Detta framgår av artikel 46 c i Europaparlamentets och rådets förordning (EG) nr

which was deleted by the Council. The rationale for the Article 44(2) exemption seems to be, as emphasized by the recital, "to safeguard the independence of judges in the performance of their judicial tasks." (Se s. 8).

¹⁴ *"The EDPS considers that the criterion for exempting from or including in the supervision by DPAs the data processing activity should be, respectively, whether the processing of personal data takes place in the context of the judicial activity ("trial", judicial proceeding, judicial activities in court cases) or in the context of other activities where judges might be involved in accordance with national law, rather than being based on the distinction tout court between categories of data controllers, namely the court, on the one side, and the public prosecutor – as example of "other judicial authority" – on the other side".* (Se fotnot 23).

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.

De utlåtanden (s.k. opinions) som EDPS har framställt angående EU-domstolens personuppgiftshantering gäller i princip endast den administrativa verksamheten. Den större delen av utlåtandena gäller personuppgiftsbehandling i den personaladministrativa verksamheten. Ett fåtal utlåtanden gäller personuppgiftsbehandling inom ramen för offentliga upphandlingar när EU-domstolen är upphandlande myndighet. EU-domstolen själv har gett uttryck för uppfattningen att publicering på internet av namnet på fysiska personer som är part i en process vid domstolen utgör en del av den rättskipande verksamheten.¹⁵

Även vad gäller allmänhetens rätt till tillgång till unionens institutioners handlingar finns undantag för EU-domstolen. Enligt artikel 15.3 första stycket i EUF-fördraget ska varje unionsmedborgare ha rätt till tillgång till unionens institutioners, organs och byråers handlingar, oberoende av medium, enligt de principer och villkor som ska bestämmas i enlighet med den här punkten. Av fjärde stycket framgår dock att EU-domstolen omfattas av bestämmelserna endast när den utövar sina administrativa funktioner.

Närmare bestämmelserna för unionsmedborgarnas tillgång till institutionernas handlingar finns i förordning. Vad gäller Europaparlamentet, rådets och kommissionens handlingar regleras detta i Europaparlamentet och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar. EU-domstolen har i de förenade målen Sverige m.fl. mot API och kommissionen,¹⁶ som gällde tillämpning av förordning (EG) nr 1049/2001, uttalat att undantaget för domstolens verksamhet innebär att dömande verksamhet som sådan är utesluten från tillämpningsområdet. EU-domstolen konstaterade vidare att ”de inlagor som kommissionen lämnar till domstolen inom ramen för ett domstolsförfarande har ytterst speciella karakteristiska

¹⁵ Brev från EU-domstolens ordförande till Europeiska datatillsynsmannen den 8 december 2009, inkommet till Europeiska datatillsynsmannen den 11 december 2009, Dnr 2009-0264.

¹⁶ Dom Sverige m.fl. mot API och kommissionen, C-514-07 P, EU:C:2010:541, C-528/07 P, EU:C:2009:2 och C-532-07 P, EU:C:2009:2, punkterna 77, 79–82 och 131.

egenskaper. De utgör nämligen till sin natur mer en del av domstolens dömande verksamhet än av kommissionens förvaltningsverksamhet”. Domstolen menade vidare att den dömande verksamheten är avslutad när förfarandet har avslutats.

8.4 Bedömning

Bedömning: Det unionsrättsliga begreppet *dömande verksamhet* innefattar sannolikt all den personuppgiftsbehandling som utförs i det enskilda målet eller ärendet från att detta anhängiggörs vid domstolen tills ett slutligt avgörande har meddelats. Denna bedömning innebär att en stor del av, men inte hela, de svenska domstolarnas rättskipande och rättsvårdande verksamhet omfattas av begreppet.

Utifrån hur Datainspektionens tillsyn sker i dag kan man sluta sig till att upprättandet av uppropplistor och tillgängliggörandet av uppgifter om domstolens registrerade mål för allmänheten inte har ansetts vara undantagna från tillsyn med hänsyn till bestämmelsen i 11 kap. 3 § RF om domstolarnas oberoende. Anledningen till detta torde vara att dessa verksamheter inte har ansetts utgöra en del av domstolarnas dömande verksamhet så som begreppet tillämpats i Sverige. Någon ledning gällande förordningens begrepp *dömande verksamhet* är dock enligt vår mening svår att hämta från Datainspektionens nuvarande tillsynsområde, eftersom ställningstagandena endast har sitt ursprung i den svenska grundlagens princip om domstolarnas oberoende. Eftersom JO:s och JK:s tillsyn till viss del omfattar domstolarnas dömande verksamhet är det enligt vår mening även vanskligt att leta efter en avgränsning mellan domstolarnas dömande och övriga verksamhet i dessa myndigheters tillsyn.

Vi anser att det ställningstagande som nu ska göras i stället måste ha sin utgångspunkt i en tolkning av dataskyddsförordningen och ett eventuellt unionsrättsligt begrepp. Detta stämmer enligt vår mening väl överens med den praxis gällande tolkningen av gemenskapsrättsliga bestämmelser som utvecklats av EU-domstolen och som redovisas i avsnitt 8.2.1.

Utifrån en studie av de engelska, franska och tyska versionerna av förordningen uppfattar vi att undantaget från tillsynsmyndigheternas behörighet omfattar domstolarnas *rättsliga* eller *rättskipande verksamhet*. Även i skälen till 2016 års dataskyddsdirektivs bestämmelse om tillsynsmyndighetens behörighet anges att det är domstolarnas *rättsliga uppgifter* som är undantagna från tillsyn. Dataskyddsförordningens skäl 20 anger vidare att det är oberoendet i den *rättskipande verksamheten* som ska säkerställas genom att tillsynsmyndighetens behörighet begränsas. För svensk del förefaller den *rättsliga eller rättskipande verksamheten* omfatta betydligt mer än den *dömande verksamheten*.

Som tidigare konstaterats (avsnitt 7.2.7) anser vi vidare att de ärenden som numera finns kvar på allmän domstol har större likheter med de allmänna förvaltningsdomstolarnas och de allmänna domstolarnas rättskipning än med ärendehantering hos förvaltningsmyndigheterna. Mot den bakgrunden är det vår uppfattning att inte bara det område som traditionellt sett har ansetts utgöra rättskipning – utan även den ärendehantering som har ansetts utgöra rättsvårdande verksamhet – kan omfattas av begreppet *dömande verksamhet*.

Frågan är därefter vilka delar av den rättskipande och rättsvårdande verksamheten som ingår i den dömande verksamheten. Dataskyddsförordningens skäl 97 talar enligt vår mening för en vid tolkning av begreppet, eftersom även andra rättsliga myndigheter än domstolarna anses kunna utföra dömande verksamhet.

Vi anser att begreppet *dömande verksamhet* sannolikt omfattar betydligt mer än endast utformandet av beslut och domar. För detta talar bl.a. den möjlighet som dataskyddsförordningen enligt skäl 20 ger medlemsstaterna att anförtro tillsynen över domstolarnas behandling av personuppgifter i den dömande verksamheten till särskilda organ inom rättsväsendet. Att ett sådant tillsynsorgan skulle ha som enda uppgift att övervaka den personuppgiftsbehandling som utförs vid utformandet av domar och beslut förefaller föga ändamålsenligt.

Ytterligare stöd för att det unionsrättsliga begreppet *dömande verksamhet* omfattar det stora flertalet av de åtgärder som utförs inom domstolarnas kärnverksamhet finns i EU-domstolens

avgörande Sverige m.fl. mot API och kommissionen.¹⁷ EU-domstolen bedömde här att en partsinlaga var del av den dömande verksamheten och att den dömande verksamheten avslutas när förfarandet har avslutats. Målet rörde förvisso frågan om allmänhetens tillgång till institutioners handlingar. Den beskrivning som EU-domstolen gör av vad dömande verksamhet innefattar talar enligt vår mening dock med styrka för att dömande verksamhet omfattar större delen av domstolarnas kärnverksamhet, men inte den rent administrativa verksamheten. Det logiska vore enligt vår mening att tillskriva begreppet samma innebörd när det gäller tolkning av andra delar av EU-rätten.

För den europeiska datatillsynsmannen (EDPS) gäller vidare i princip samma undantag i tillsynsbehörigheten som enligt dataskyddsförordningen kommer att gälla för de nationella tillsynsmyndigheterna. EDPS har inte behörighet att övervaka den behandling av personuppgifter som sker i EU-domstolens rättsskipande verksamhet. De utlåtanden (opinions) EDPS utfärdat gällande EU-domstolens personuppgiftsbehandling har endast behandlat den administrativa verksamheten. Även detta talar enligt vår mening för att det unionsrättsliga begreppet *dömande verksamhet* ska ges en vid tolkning.

Vad gäller begreppet *dömande verksamhet* relaterat till de svenska domstolarnas verksamhet gör vi följande bedömning.

Den dömande uppgift som svenska domstolar har anförtrotts påbörjas enligt vår mening när ett mål eller ett ärende anhängiggörs. De processuella bestämmelserna styr därefter hur målet handläggs fram till dess att ett slutligt avgörande fattas. Handläggningen i sig innefattar en rad beslut. Vissa av dessa dokumenteras i verksamhetsstödet såsom ”ej slutliga beslut”. Det kan handla om avvísning av bevisning, förordnanden av offentliga biträden eller interimistiska beslut. Att denna typ av beslut, liksom domstolens slutliga avgörande av saken, hör till den dömande verksamheten förefaller för oss tämligen självklart.

Handläggningen av ett mål innefattar dock inte endast dessa ej slutliga beslut. Mer frekvent förekommande är de otaliga beredningsbeslut, som endast kommer till uttryck genom själva

¹⁷ Dom Sverige m.fl. mot API och kommissionen, C-514-07 P, EU:C:2010:541, C-528/07 P, EU:C:2009:2 och C-532-07 P, EU:C:2009:2, punkterna 77, 79-82 och 131.

beredningsåtgärden. Exempel på detta är kommunicering, remisser och kallelser. Det kan också handla om förelägganden till en part om viss komplettering, där en underlåtenhet att komma in med uppgifter kan leda till rättsförlust för parten. Tanken att dessa beslut skulle ligga utanför domstolarnas dömande verksamhet ter sig främmande för oss.

Mot denna bakgrund anser vi att en rimlig tolkning av dataskyddsförordningens begrepp *dömande verksamhet* ur ett unionsrättsligt perspektiv är att begreppet innefattar all den personuppgiftsbehandling som sker i det enskilda målet eller ärendet från att målet eller ärendet anhängiggörs vid domstolen tills att ett slutligt avgörande har meddelats. Eftersom begreppet med denna tolkning endast omfattar de enskilda målen bör dock exempelvis upprättandet av uppropplistor och praxissammansställningar – som ju görs i den rättskipande och rättsvårdande verksamheten – falla utanför begreppsramen. Sammanfattningsvis innebär vår bedömning att den dömande verksamheten innefattar en stor del av, men inte hela, domstolarnas rättskipande och rättsvårdande verksamhet. Som vi tidigare påpekat får dock gränsen mellan den dömande verksamheten och övrig rättskipande och rättsvårdande verksamhet slutligen avgöras av rättspraxis.

Enligt vårt synsätt kommer dataskyddsförordningen sannolikt att påverka den svenska tillsynsmyndighetens möjlighet att bedriva tillsyn över domstolarnas kärnverksamhet. Vi vill dock avslutningsvis tydliggöra att oavsett vilken bedömning som görs gällande gränsdragningen mellan domstolarnas dömande och övriga verksamhet är det vår uppfattning att dataskyddsförordningens principer och bestämmelser ska följas i all personuppgiftsbehandling som sker i domstolarna. Det framgår nämligen klart av skäl 20 i dataskyddsförordningen att förordningen gäller även i domstolarnas verksamhet. Att den nationella tillsynsmyndigheten inte är behörig att utöva tillsyn över vissa delar av domstolarnas personuppgiftsbehandling är en annan fråga.

9 Ändamålsbestämmelser

9.1 Befintliga ändamålsbestämmelser

9.1.1 Rättslig reglering

Av artikel 5.1 b i dataskyddsförordningen framgår att personuppgifter endast får samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Detta kallas för ändamålsbegränsning och det senare ledet benämns ofta finalitetsprincipen (se avsnitt 9.1.4). Motsvarande bestämmelse finns i artikel 6.1 b i 1995 års dataskyddsdirektiv och har införts i svensk rätt genom 9 § första stycket c och d PuL. Domstolsdatalagen hänvisar till personuppgiftslagens bestämmelser genom 5 § första stycket 3.

Registerförfattningarnas ändamålsbestämmelser brukar delas upp i primära och sekundära ändamål. Bestämmelserna om primära ändamål tillgodoser behovet av att behandla personuppgifter i myndighetens egen verksamhet och anger för vilka ändamål myndigheten får samla in personuppgifter. Uttrycket insamling ska här ses i en vid bemärkelse och omfattar inte bara de situationer då uppgifter lämnas till en domstol efter domstolens egen begäran. Även andra situationer som innebär att en domstol får tillgång till personuppgifter omfattas, exempelvis genom att en enskild lämnar in ett överklagande. De primära ändamålen ger även rättsligt stöd för vidarebehandling av uppgifterna i form av exempelvis lagring och utlämning. Bestämmelser om sekundära ändamål medger inte insamling utan reglerar hur personuppgifter som redan har samlats in och behandlas i verksamheten får vidarebehandlas.¹

¹ Se förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 38 ff.).

Domstolsdatalagens primära ändamålsbestämmelse finns i 6 § och innebär att domstolarna får behandla personuppgifter för handläggning av mål och ärenden. För att ytterligare begränsa den behandling som är tillåten inom ramen för detta ändamål anges att personuppgifter får behandlas endast *om det behövs* för handläggning av mål och ärenden.

Det enda uttryckliga sekundära ändamålet anges i 7 § domstolsdatalagen och innebär att domstolarna även får behandla sådana personuppgifter som behandlats för handläggning av mål och ärenden för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Även den sekundära ändamålsbestämmelsen innehåller en begränsning genom att personuppgifter för detta ändamål får behandlas endast *om det behövs*.

Av förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 104) framgår att lagens ändamålsbestämmelser utgör en uttömmande reglering av för vilka ändamål personuppgifter får behandlas i domstolarnas och nämndernas rättskipande och rättsvårdande verksamhet.

9.1.2 Tidigare förarbeten

I förarbetena till domstolsdatalagen angav regeringen att domstolsdatalagens primära ändamålsbestämmelse är tänkt att ha en vid innebörd och gjorde följande uttalande gällande tolkningen (prop. 2014/15:148 s. 39 f.).

Domstolarna behöver samla in och vidarebehandla personuppgifter i de fall då handläggningen av mål och ärenden kräver det. /.../ Vilka uppgifter som domstolarna ska samla in i mål och ärenden och hur de fortsatt ska hanteras inom ramen för handläggning av mål och ärenden är frågor som således styrs främst av processrätten och som inte ska regleras genom domstolsdatalagen eller andra personuppgiftsbestämmelser. Detta gör att det varken är möjligt eller lämpligt att i domstolsdatalagen i detalj ange för vilka ändamål personuppgifter ska få samlas in och vidarebehandlas. I domstolsdatalagen bör det därför anges att domstolarna får behandla (dvs. samla in eller vidarebehandla) personuppgifter om det behövs för handläggning av mål och ärenden. En sådan bestämmelse är tillräckligt flexibel för att domstolarnas organisation och arbetssätt ska kunna fortsätta att utvecklas och för att domstolarna ska kunna hantera nya måltyper. Samtidigt innebär bestämmelsen ett skydd mot integritetskränkning genom att bestämmelsen inte medger behandling av personuppgifter som inte är

befogad i domstolarnas verksamhet. Avsikten är inte att en bestämmelse med det beskrivna innehållet ska tolkas alltför snävt. /.../ bedömningen av om en viss behandling är nödvändig ska göras i förhållande till mål- och ärendehandläggningen i stort och inte i förhållande till handläggningen av ett specifikt mål eller ärende. Sökning efter tidigare avgöranden och hantering av sådana avgöranden kommer således att rymmas inom vad som är tillåtet enligt ändamålsbestämmelserna, oavsett om åtgärderna sker i syfte att underlätta praxisdiskussioner, domskrivningsarbete eller annat kompetensutvecklingsarbete.

Samtliga Vera-förordningar innehöll en bestämmelse om att de register över mål och ärenden som handläggs vid domstolen fick användas för planering, uppföljning och utvärdering av verksamheten.² I remissförfarandet inför införandet av domstolsdatalagen anförde Datainspektionen att det för den enskilde är alltför otydligt att det primära ändamålet i 6 § domstolsdatalagen även omfattar vidarebehandling av personuppgifter för planering, uppföljning och utvärdering hos de enskilda myndigheterna. Regeringen har för domstolsdatalagen emellertid gjort samma bedömning som för bl.a. lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet och polisdatalagen (2010:361). Bedömningen innebär att personuppgifter som får användas i myndighetens verksamhet också får användas för planering, uppföljning och utvärdering av verksamheten utan att detta uttryckligen anges i lagen.³ Av förarbetena till lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet (prop. 2004/05:164 s. 66) framgår att Lagrådet då påpekade att administrativ intern tillsyn, kontroll och uppföljning m.m. av verksamheten måste anses vara en integrerad del av själva verksamheten och inte kan ses som någon från denna fristående aktivitet. Att uppgifter som får användas i verksamheten också får användas för planering m.m. framstår därför enligt Lagrådet som så självklart att det inte behöver sägas. Lagrådet förordade mot den bakgrunden att en föreslagen särskild bestämmelse om att

² Se 2 § 3 förordningen (2001:639) om registerföring m.m. vid allmänna domstolar med hjälp av automatiserad behandling, 2 § 2 förordningen (2001:640) om registerföring m.m. vid förvaltningsrätt med hjälp av automatiserad behandling, 2 § 3 förordningen (2001:641) om registerföring m.m. vid Högsta förvaltningsdomstolen och kammarrätterna med hjälp av automatiserad behandling och 2 § 2 förordning (2001:642) om registerföring m.m. vid hyres- och arrendenämnderna med hjälp av automatiserad behandling.

³ Se förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 38 ff.).

personuppgifter fick behandlas för planering, uppföljning och utvärdering av verksamheten skulle utgå.

Vad gäller domstolsdatalagens sekundära ändamålsbestämmelse framgår av förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 41 f.) följande.

En allmän förutsättning för sådan behandling som sker för utlämnande till andra bör vara att uppgiftslämnandet sker i överensstämmelse med lag eller förordning, dvs. med stöd av bestämmelser som påbjuder eller tillåter utlämnande. När bestämmelser som påbjuder eller tillåter utlämnande har införts får det förutsättas att det har gjorts en avvägning mellan intresset av att uppgiften lämnas ut och intresset av att skydda enskilda personers integritet, och att man vid denna avvägning funnit att uppgiften ska eller får lämnas ut, jfr propositionen Patientdatalag m.m. (prop. 2007/08:126 s. 60). Bestämmelser av detta slag som berör domstolarnas verksamhet finns i många olika sammanhang, vilket framgår av det följande. För det första är domstolarna enligt olika författningsbestämmelser skyldiga att på begäran lämna ut uppgifter. Domstolarna är t.ex. enligt 6 kap. 5 § offentlighets- och sekretesslagen (2009:400) skyldiga att på begäran av en annan myndighet lämna uppgifter som domstolen förfogar över under förutsättning att uppgifterna inte är sekretessbelagda och att det inte skulle hindra arbetets behöriga gång. För det andra är domstolarna enligt bestämmelser i olika författningar skyldiga att lämna uppgifter till utpekade myndigheter. Genom de reformer som följer av RIF-samarbetet kommer en del av denna hantering att bli helt automatiserad. /.../ För det tredje bör de situationer beaktas i vilka det inte finns någon skyldighet att lämna uppgifter men där det ändå kan anses påbjudet eller önskvärt att en domstol lämnar uppgifter till andra domstolar, myndigheter eller andra utomstående. Det kan t.ex. vara fråga om en åtgärd som vidtas för att fullgöra serviceskyldigheten gentemot enskilda enligt 4 § förvaltningslagen (1986:223).

9.1.3 Ett uttryckligt angivet och tydligt ändamål

Av artikel 6.3 andra stycket i dataskyddsförordningen framgår att den nationella rätten kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen och att dessa bestämmelser kan innehålla bland annat de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål samt ändamålsbegränsningar. Detta ger enligt vår mening stöd för förekomsten av både primära och sekundära ändamålsbestämmelser i nationella registerförfattningar.

Ändamålet med personuppgiftsbehandlingen måste vara uttryckligt angivet och tillräckligt tydligt. Detta framgår av de allmänna principer som gäller enligt artikel 5.1 b i dataskyddsförordningen och skäl 39 till förordningen. Om ändamålen med personuppgiftsbehandlingen inte har en viss grad av precision är det vidare svårt att bedöma om behandlingen uppfyller den princip om uppgiftsminimering som framgår av artikel 5.1 c i dataskyddsförordningen. Enligt denna princip ska personuppgifterna vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål som de samlades in för. En bedömning av om en uppgift är nödvändig för ett visst ändamål eller hur relevant uppgiften är för ändamålet, är svår att göra om ändamålet inte är tillräckligt tydligt angivet.⁴

9.1.4 Finalitetsprincipen

Av intresse för ändamålsbestämmelserna är finalitetsprincipen, som kommer till uttryck i artikel 5.1 b och artikel 6.4 i dataskyddsförordningen. Principen återfinns också i artikel 6.1 b i 1995 års dataskyddsdirektiv och har införts i svensk rätt genom 9 § d PuL.

Enligt artikel 5.1 b i dataskyddsförordningen ska – som vi tidigare nämnt – personuppgifter samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Av bestämmelsen framgår också att personuppgifterna inte senare får behandlas på ett sätt som är oförenligt med dessa ändamål. Det framgår emellertid även att ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 inte ska anses vara oförenliga med de ursprungliga ändamålen.

Av artikel 6.4 i dataskyddsförordningen framgår vilka faktorer som kan vara av betydelse för att fastställa om en personuppgiftsbehandling för andra ändamål är förenlig med det ändamål som de samlades in för. De faktorer som anges i artikel 6.4 a–e är i sin helhet följande.

- a) Kopplingar mellan de ändamål för vilka personuppgifterna har samlats in och ändamålen med den avsedda ytterligare behandlingen.

⁴ Jfr Socialdatautredningens betänkande (SOU 1999:109 s. 156).

- 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.

Av skäl 50 till dataskyddsförordningen framgår dock också att om en personuppgiftsbehandling 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 medlemsstaternas nationella rätt fastställa och närmare ange för vilka uppgifter och syften ytterligare behandling bör betraktas som ”förenlig och laglig”. Tillåtligheten av en vidarebehandling kan således säkerställas genom nationell lagstiftning som reglerar när sådan vidarebehandling ska vara tillåten (jfr artikel 6.3 andra stycket i dataskyddsförordningen och avsnitt 5.1). En sådan nationell reglering ersätter således, enligt vår mening, den prövning som annars ska göras enligt artikel 6.4 i dataskyddsförordningen av om ändamålet är förenlighet med det ursprungliga.⁵

9.1.5 **Precisering av rättslig grund eller ändamålsbestämmelser?**

Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande (SOU 2017:29 s. 241 ff.) gjort bedömningen att tillåtna rättsliga grunder för behandling och ändamålsbestämmelser ibland har blandats samman.⁶ Detta kan enligt den utredningen leda till att tillämparen förväxlar rättslig grund med ändamål och godtar ett i författning angivet allmänt ändamål som ett särskilt och

⁵ Jfr förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 104).

⁶ Se även informationshanteringsutredningens slutbetänkande (SOU 2015:39).

tillräckligt preciserat ändamål. Som ett exempel nämns bestämmelsen i 2 kap. 7 § polisdatalagen. Här anges att Polismyndigheten får behandla personuppgifter för att utföra vissa av sina arbetsuppgifter, t.ex. om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller beivra brott. Utredningen ifrågasätter om sådana bestämmelser utgör ändamålsbestämmelser eller om de i stället bör betraktas som en precisering av den rättsliga grunden. Vi är i detta avseende inte av någon annan uppfattning.

Man kan ställa sig frågan om de ändamålsbestämmelser som finns i 6 och 7 §§ domstolsdatalagen snarare utgör en precisering av den rättsliga grund som domstolarnas rätt till personuppgiftsbehandling inom domstolsdatalagens tillämpningsområde vilar på. Den myndighetsutövning eller uppgift av allmänt intresse (jfr artikel 6.1 e i dataskyddsförordningen) som har anförtrotts domstolarna utgörs ju av den rättskipande och rättsvårdande verksamheten, som ytterligare kan brytas ner till handläggning av mål och ärenden. På samma sätt bör det utlämnande som sker i enlighet med lag eller förordning utgöra en uppgift av allmänt intresse eller en rättslig förpliktelse (jfr artikel 6.1 c och e i dataskyddsförordningen).

Den verksamhet som domstolarna har ålagts att utföra är emellertid relativt begränsad och tydligt avgränsad. Detta får enligt vår mening till följd att den rättsliga grunden och de ändamål som personuppgifter behandlas för ligger varandra nära. Vi anser därför att det inte finns något principiellt hinder mot att behålla de ändamål för behandling som nu finns i domstolsdatalagen.

9.1.6 Bedömning

Bedömning: Dataskyddsförordningen föranleder ingen ändring vad gäller förekomsten av ändamålsbestämmelser i domstolsdatalagen. Det är inte heller nödvändigt att ytterligare precisera de befintliga ändamålen för behandling.

Vi anser att de tillåtna ändamålen för personuppgiftsbehandling bör framgå av domstolsdatalagen. Skälen för detta är följande.

Enligt domstoldalagens primära ändamålsbestämmelse får personuppgifter behandlas om det behövs för handläggning av mål och ärenden. Som framgår av tidigare förarbeten till domstoldalagen skiljer domstolarnas personuppgiftsbehandling sig från många andra myndigheters, eftersom det finns annan lagstiftning som i stor utsträckning reglerar vilka personuppgifter som ska behandlas vid handläggningen av mål och ärenden (se avsnitt 9.1.2).⁷ Som vi konstaterat i avsnitt 9.1.4 är den verksamhet som domstolarna har ålagts att utföra dessutom relativt begränsad och tydligt avgränsad. På dessa sätt skiljer sig domstolarnas verksamhet från t.ex. de brottsbekämpande myndigheternas, där mer övergripande ändamål riskerar att leda till att personuppgifter behandlas i strid med kraven på ändamålsbegränsning och uppgiftsminimering (artikel 5.1 b och c).

Vi anser också att en lagreglering av personuppgiftsbehandlingen ändamål ger en tydlighet för både de registrerade och de tjänstemän vid domstolarna som ska behandla personuppgifterna. Eftersom domstoldalagens ändamålsbestämmelser dessutom är avsedda att vara uttömmande kommer det inte att vara upp till enskilda tjänstemän att bedöma om en behandling för andra ändamål är förenlig med det ursprungliga. Detta utgör enligt vår mening i sig ett skydd för de registrerades integritet.

Enligt artikel 5.1 b i dataskyddsförordningen måste ändamålen med personuppgiftsbehandlingen vara uttryckligt angivna. För det fall det i domstoldalagen inte anges för vilka ändamål personuppgifter får behandlas måste ändamålet för varje behandling framgå på något annat sätt. Vad gäller handläggningen av de specifika målen och ärendena torde ändamålet med behandlingen förvisso framgå av sammanhanget, t.ex. prövning av saken X på talan av klaganden Y. Det kan dock inte uteslutas att det för vissa av de övriga arbetsuppgifter som ingår i det vidare begreppet *handläggning av mål och ärenden* (se avsnitt 9.1.2) skulle krävas en dokumentation av ändamålet med personuppgiftsbehandlingen, t.ex. ett angivande av vad det specifika syftet är med en viss rättsfallssammanställning eller med en viss specifik statistiksammanställning. En sådan ordning skulle enligt vår mening utgöra

⁷ Jfr även Öman, Särskilda registerförfattningar, Festskrift till Peter Seipel, 2006, s. 703.

en större administrativ belastning för domstolarna än den nuvarande.

Frågan är då om det finns anledning att se över ändamålsbestämmelsernas utformning eller om de redan nu är så specifikt och uttryckligt angivna som kan krävas (jfr artikel 5.1 b i dataskyddsförordningen)

Som framgår ovan innehåller 1995 års dataskyddsdirektiv samma reglering om ändamålet för personuppgiftsbehandling som dataskyddsförordningen. Domstolsdatalagens nuvarande ändamålsbestämmelse har således bedömts utifrån samma krav som nu återfinns i dataskyddsförordningen. Detta innebär att regeringen i och med införandet av domstolsdatalagen måste ha bedömt att de ändamål som anges i lagens 6 och 7 §§ är så uttryckligt angivna och tydliga som krävs enligt unionsrätten.

De mål och ärenden som handläggs av de aktuella domstolarna inom ramen för den rättskipande och rättsvårdande verksamheten är vidare av mycket olika karaktär. Av förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 39 f.) framgår också att begreppet *handläggning av mål och ärenden* syftar till mål- och ärendehandläggningen i stort. Vi anser att det inte finns något i bestämmelsens ordalydelse som talar mot en sådan tolkning, eftersom det inte framgår att det endast är handläggningen av det *enskilda* målet eller ärendet som avses. Ändamålet, dvs. handläggningen av mål och ärenden, måste därmed anses rymma alla de åtgärder som vidtas inom ramen för domstolarnas rättskipande och rättsvårdande verksamhet. Det handlar om vitt skilda åtgärder såsom kommunikering, sökning i verksamhetsstöd för att svara på parterers frågor, framställning av databaser som miljöboken, sammanställning av underlag för praxisdiskussioner och författande av föredragningspromemorior, rättsutredningar, domar m.m. Därutöver pågår naturligtvis kontinuerligt en planering och uppföljning av verksamheten. Domstolsdatalagens primära ändamålsbestämmelse måste även anses rymma den behandling av personuppgifter som sker då domstolarna lämnar ut respektive tar del av personuppgifter genom den direktåtkomst som är tillåten mellan domstolarna enligt 17 § domstolsdatalagen (se vidare avsnitt 17.3.2). Domstolsdatalagens ändamålsbestämmelse rymmer således en mängd olika arbetsuppgifter som innefattar behandling av personuppgifter.

Mot bakgrund av den diversifierade verksamhet som omfattas av domstolsdatalagens primära ändamålsbestämmelse måste en ändamålsbestämmelse som är avsedd att träffa hela denna verksamhet enligt vår mening ha en vid formulering. Vi anser därför att domstolsdatalagens primära ändamålsbestämmelse är så specifik och tydlig som kan krävas i denna verksamhet. Enligt vår uppfattning vore det vidare olämpligt att i ett försök att skapa tydlighet ändra bestämmelsens lydelse. En exemplifiering av de arbetsuppgifter som omfattas av den primära ändamålsbestämmelsen skulle enligt vår mening i stället riskera att göra lagstiftningen ofullständig och skapa förvirring gällande tillåtligheten av de arbetsuppgifter som inte nämns.

Det får dock inte glömmas bort att personuppgiftsbehandlingen måste behövas för att vara tillåten. Frågan om huruvida behandlingen av en viss personuppgift är adekvat, relevant och inte för omfattande i ett enskilt ärende eller för en enskild arbetsuppgift (jfr artikel 5.1 c i dataskyddsförordningen) får enligt vår mening bedömas utifrån det enskilda ärendets eller arbetsuppgiftens karaktär. Samma sak gäller när personuppgifter behandlas i den del av den rättskipande eller rättsvårdande verksamheten som inte direkt rör ett enskilt mål eller ärende.

Enligt domstolsdatalagens sekundära ändamålsbestämmelse får personuppgifter som samlats in för att de behövs för handläggning av mål och ärenden även behandlas om det behövs för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Enligt artikel 6.3 andra stycket i dataskyddsförordningen är det möjligt att i nationell rätt reglera för vilka ändamål uppgifter får lämnas ut. Som framgår av tidigare förarbeten till domstolsdatalagen (prop. 2014/15:148 s. 41–42) får det också förutsättas att det vid de aktuella lagarnas och förordningarnas tillkomst har gjorts en avvägning mellan intresset av att uppgiften lämnas ut och intresset av att skydda enskilda personers integritet.

Vi anser att domstolsdatalagens sekundära ändamålsbestämmelse medverkar till att ge en heltäckande bild av vilken personuppgiftsbehandling som är tillåten inom domstolarnas rättskipande och rättsvårdande verksamhet. Bestämmelsen innebär också att det inte råder några tvivel om att det utlämnande av

personuppgifter som sker med stöd av annan lag eller förordning är tillåtet även enligt dataskyddsförordningen.

Sammantaget gör vi bedömningen att någon förändring av domstolsdatalagens ändamålsbestämmelser inte behöver eller bör göras. Vissa redaktionella ändringar behöver dock göras av dessa bestämmelser till följd av dataskyddsförordningens bestämmelser om behandling av personuppgifter för arkivändamål. Dessa förändringar behandlas i avsnitt 19.4.

9.2 Komplettering av ändamålsbestämmelserna

Förslag: Personuppgifter ska få behandlas om det behövs för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning när de behandlas eller har behandlats med stöd av brottsdatalagen eller dess kompletterande registerförfattning för domstolarna.

I föreslaget till 2 kap. 21 § brottsdatalagen finns en upplysning om att dataskyddsförordningen ska tillämpas när en behörig myndighet behandlar personuppgifter för ändamål utanför brottsdatalagens tillämpningsområde. Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande (SOU 2017:29 s. 292) vidare gjort bedömningen att dataskyddsförordningen – och inte brottsdatalagen – är tillämplig när sådana behöriga myndigheter som avses i brottsdatalagen behandlar personuppgifter för att tillhandahålla dessa till andra myndigheter, om ändamålet med behandlingen ligger utanför brottsdatalagens tillämpningsområde.

Mot den bakgrunden måste enligt vår mening utlämnade enligt lag eller förordning av personuppgifter som domstolarna har behandlat för handläggning av mål och ärenden med stöd av brottsdatalagen eller dess kompletterande registerförfattning för domstolarna alltjämt regleras av domstolsdatalagen. Lagens sekundära ändamålsbestämmelse bör således omfatta även sådan personuppgiftsbehandling, förutsatt att utlämnandet inte sker med stöd av brottsdatalagen. Som exempel på ett utlämnande av personuppgifter som kommer att omfattas av domstolsdatalagen kan nämnas när en allmän domstol lämnar ut handlingar i ett brottmål enligt tryckfrihetsförordningen. Eftersom det ligger inom

Utredningen om 2016 års dataskyddsdirektivs uppdrag att analysera tillämpningsområdet för direktivet, hänvisar vi till den utredningens betänkande för en mer ingående beskrivning av vilka utlämnanden av personuppgifter som inte omfattas av brottsdatalagen och dess registerförfattningar.

Utlämnande av personuppgifter som har behandlats i domstolarnas verksamhet med stöd av brottsdatalagen och dess kompletterande registerförfattning utförs i domstolarnas rättskipande och rättsvårdande verksamhet, vilket förvisso utgör den yttre ramen för domstolsdatalagens tillämpningsområde. Vi har emellertid föreslagit att domstolsdatalagens tillämpningsområde ska avgränsas på så sätt att lagen inte omfattar den personuppgiftsbehandling i de allmänna domstolarnas och de allmänna förvaltningsdomstolarnas verksamhet som omfattas av brottsdatalagens tillämpningsområde (se avsnitt 4.3). Mot den bakgrunden bedömer vi att det krävs en förändring av domstolsdatalagens sekundära ändamålsbestämmelse för att den ska omfatta även utlämnande av personuppgifter som har behandlats för handläggning av mål och ärenden med stöd av brottsdatalagen och dess registerförfattning.

Domstolsdatalagens sekundära ändamålsbestämmelse innebär att de uppgifter som har behandlats enligt den primära ändamålsbestämmelsen – dvs. för handläggning av mål och ärenden inom domstolsdatalagens tillämpningsområde – får lämnas ut i överensstämmelse med lag eller förordning. Personuppgifter i den del av domstolarnas verksamhet som omfattas av brottsdatalagen har förvisso också behandlats för handläggning av mål och ärenden. Detta har dock inte skett enligt domstolsdatalagen, utan enligt brottsdatalagen och dess kompletterande registerförfattning. För att den sekundära ändamålsbestämmelsen ska omfatta även utlämnande av uppgifter som primärt har behandlats med stöd av brottsdatalagen bedömer vi därmed att den måste kompletteras. Vi föreslår att detta sker genom ett tillägg, där det framgår att personuppgifter även får behandlas för de angivna sekundära ändamålen när de behandlas eller har behandlats med stöd av brottsdatalagen eller dess kompletterande registerförfattning för domstolarna. Den avgränsningsbestämmelse mot brottsdatalagens tillämpningsområde som vi har föreslagit kommer att medföra att tillägget till de sekundära ändamålen endast innefattar den

personuppgiftsbehandling som inte ska ske med stöd av brottsdatalagen. Vår bedömning av rätten att för arkivändamål behandlar personuppgifter som primärt har behandlats med stöd av brottsdatalagen finns i avsnitt 19.4.

10 Förhållandet till annan lagstiftning

10.1 Förhållandet till personuppgiftslagen

Förslag: Domstolsdatalagens bestämmelse om hur lagen förhåller sig till personuppgiftslagen ska upphävas och samtliga hänvisningar till personuppgiftslagen utgå.

Enligt 4 § domstolsdatalagen gäller den lagen i stället för personuppgiftslagen, om inte annat anges i 5 §. Den senare bestämmelsen innehåller i sin tur hänvisningar till de bestämmelser i personuppgiftslagen som gäller när personuppgifter behandlas enligt domstolsdatalagen eller enligt föreskrifter som har meddelats i anslutning till lagen.

När dataskyddsförordningen börjar tillämpas kommer personuppgiftslagen att upphävas.¹ Domstolsdatalagens bestämmelse om hur lagen förhåller sig till personuppgiftslagen måste därmed upphävas och samtliga hänvisningar till personuppgiftslagen utgå. I avsnitt 10.6 redogör vi för innehållet i domstolsdatalagens befintliga hänvisningar till personuppgiftslagen och gör en bedömning av om dessa ska ersättas.

¹ Se kommittédirektiv till Dataskyddsutredningen (Dir 2016:15 s. 6).

10.2 Förhållandet till dataskyddsförordningen

Förslag: Det ska framgå av domstolsdatalagen att lagen innehåller kompletterande bestämmelser till dataskyddsförordningen.

Bedömning: Hänvisningarna till personuppgiftslagen bör inte ersättas med hänvisningar till motsvarande bestämmelser i dataskyddsförordningen.

När dataskyddsförordningen börjar tillämpas kommer den att vara direkt tillämplig på all personuppgiftsbehandling som sker inom dess materiella och territoriella tillämpningsområde i medlemsstaterna. Dataskyddsförordningens bestämmelser kommer därmed att gälla på domstolsdatalagens tillämpningsområde oberoende av om förhållandet till förordningen regleras i domstolsdatalagen. För att underlätta för tillämparen anser vi dock att det bör införas en upplysningsbestämmelse i domstolsdatalagen som klargör att lagen innehåller kompletterande bestämmelser till dataskyddsförordningen.

Innehållet i flera av personuppgiftslagens bestämmelser kommer framöver att återfinnas i dataskyddsförordningen (se avsnitt 4.1.1). Det kan därmed ligga nära till hands att ersätta domstolsdatalagens hänvisningar till personuppgiftslagen med hänvisningar till dataskyddsförordningens bestämmelser. Hänvisningar till endast vissa av förordningens bestämmelser – som dessutom är förhållandevis komplexa – riskerar dock enligt vår mening att skapa otydlighet för tillämparen. Det finns även en risk för missuppfattningen att de bestämmelser i dataskyddsförordningen som domstolsdatalagen inte hänvisar till inte är tillämpliga. Vi anser därför att det i domstolsdatalagen inte bör införas några hänvisningar till enskilda bestämmelser i dataskyddsförordningen endast i upplysningssyfte.

Hänvisningsteknik

Vi föreslår i vår promemoria att vissa bestämmelser i domstolsdatalagen ska innehålla hänvisningar till bestämmelser i

dataskyddsförordningen, t.ex. när det finns möjlighet och anledning att göra undantag från dataskyddsförordningens bestämmelser (se bl.a. kapitel 15). Sådana hänvisningar kan vara antingen statiska eller dynamiska. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse. En dynamisk hänvisning innebär att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen.

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 80 f.) gjort bedömningen att den föreslagna dataskyddslagens hänvisningar till dataskyddsförordningen ska vara dynamiska. Undantaget är en bestämmelse som rör behandling av personuppgifter utanför dataskyddsförordningens egentliga tillämpningsområde. Vi anser att även de hänvisningar till dataskyddsförordningen som görs i domstolsdatalagen bör omfatta eventuella framtida ändringar av dataskyddsförordningen och således vara dynamiska. Skälen till detta är följande.

I vårt förslag till ändring av 7 § domstolsdatalagen finns en hänvisning till artikel 89.1 i dataskyddsförordningen. Hänvisningen har föreslagits för att klargöra att sådana säkerhetsåtgärder som framgår av den senare bestämmelsen krävs för att bl.a. behandling för arkivändamål ska vara tillåten. Eftersom sådana säkerhetsåtgärder är ett krav som framgår av dataskyddsförordningen bör hänvisning enligt vår mening gälla även för det fall förordningen ändras i denna del.

Den föreslagna 11 § domstolsdatalagen innehåller undantag från den registrerades rätt att enligt dataskyddsförordningen få information om en personuppgiftsincident. Vi anser att undantaget bör gälla även om det genomförs mindre ändringar i dataskyddsförordningen. Skulle större ändringar genomföras kan valet av en dynamisk hänvisning dock innebära att en översyn av den svenska regleringen behöver göras.

Den föreslagna ändringen av 13 § domstolsdatalagen hänvisar till den definition av begreppet *känsliga personuppgifter* som finns i dataskyddsförordningen. Hänvisningen föreslås bl.a. för att anpassa domstolsdatalagen till dataskyddsförordningens terminologi. Det ter sig enligt vår mening därmed naturligt att en eventuell ändring av dataskyddsförordningen begrepp får genomslag även i domstolsdatalagen.

De föreslagna ändringarna av 19 och 20 §§ domstolsdatalagen innebär att vissa beslut enligt dataskyddsförordningen får överklagas. För att överklaganderätten inte ska gå förlorad om dataskyddsförordningens bestämmelser ändras i denna del bör hänvisningen enligt vår mening omfatta dataskyddsförordningen vid varje givet tillfälle.

10.3 Förhållandet till dataskyddslagen

Förslag: Domstolsdatalagen ska inom sitt tillämpningsområde gälla i stället för den föreslagna dataskyddslagen.

Det ska i domstolsdatalagen särskilt anges vilka bestämmelser i dataskyddslagen som ska gälla på domstolsdatalagens tillämpningsområde.

Dataskyddslagen kommer enligt Dataskyddsutredningens förslag att innehålla de författningsbestämmelser som på ett generellt plan kompletterar dataskyddsförordningen.² Dataskyddsutredningen föreslår att dataskyddslagen, i likhet med personuppgiftslagen, ska vara subsidiär i förhållande till bestämmelser om behandling av personuppgifter i andra författningar. Liksom vad som för närvarande gäller i förhållande till personuppgiftslagen, anser vi att domstolsdatalagen helt ska ersätta dataskyddslagen inom sitt tillämpningsområde. På detta sätt blir regleringen tydlig och bestämmelserna i domstolsdatalagen måste inte först jämföras med bestämmelserna i dataskyddslagen för att det ska kunna fastställas vilka bestämmelser som är tillämpliga i ett enskilt fall.³ Vi föreslår därför att det i domstolsdatalagen ska införas en bestämmelse som reglerar att den lagen gäller i stället för dataskyddslagen, om inte annat anges. Det ska i samband med den bestämmelsen hänvisas till de bestämmelser i dataskyddslagen som ska gälla på domstolsdatalagens tillämpningsområde.

² Se Dataskyddsutredningens betänkande (SOU 2017:39).

³ Jfr förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 29).

10.4 Förhållandet till 2013 års lag

Förslag: Domstolsdatalagens bestämmelse om förhållandet till lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen och föreskrifter som har meddelats i anslutning till den lagen ska upphävas.

Utredningen om 2016 års dataskyddsdirektiv har i sitt betänkande (SOU 2017:29) föreslagit att lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen (2013 års lag) ska upphävas. Detta gäller även de bestämmelser i svensk rätt som hänvisar till den lagen.⁴ I enlighet med denna bedömning föreslår vi att domstolsdatalagens bestämmelse om hur lagen förhåller sig till 2013 års lag och föreskrifter som har meddelats i anslutning till den lagen ska upphävas.

10.5 Förhållandet till kvarstadsförordningen

Bedömning: Dataskyddsförordningen föranleder ingen ändring av domstolsdatalagens bestämmelse om förhållandet till Europaparlamentets och rådets förordning (EU) nr 655/2014.

Den 15 maj 2014 antogs Europaparlamentets och rådets förordning (EU) nr 655/2014 om inrättande av ett europeiskt förfarande för kvarstad på bankmedel i mål och ärenden av privaträttslig natur, den s.k. kvarstadsförordningen. Förordningen trädde i kraft den 17 juli samma år och började tillämpas fullt ut den 18 januari 2017. Genom kvarstadsförordningen skapas ett självständigt unionsrättsligt förfarande för kvarstad på bankmedel. Förordningen reglerar förfarandet för att meddela ett beslut om kvarstad och för verkställighet av beslutet. Syftet är att underlätta för de fordringsägare inom EU som är verksamma i den gränsöverskridande handeln att driva in sina fordringsanspråk över gränserna.

⁴ Se SOU 2017:29 s. 145 f. för de överväganden som gjorts i denna del.

Detta ska ske genom att gäldenärerna förhindras att snabbt flytta sina bankmedel från en medlemsstat till en annan i syfte att undkomma verkställighet.⁵

Av artikel 48 d i kvarstadsförordningen framgår att förordningen inte påverkar tillämpningen av direktiv 95/46/EG (1995 års dataskyddsdirektiv), om inte annat föreskrivs i artiklarna 14.8 eller 47. I artikel 47 i förordningen finns vissa bestämmelser om skydd för personuppgifter. Enligt artikel 14.8 i förordningen inskränks den registrerades rätt att få information om att hans eller hennes personuppgifter har lämnats ut i vissa fall.

Enligt 3 § andra meningen domstolsdatalagen ska de avvikande bestämmelser som finns i kvarstadsförordningen tillämpas i stället för bestämmelserna i domstolsdatalagen. Av förarbetena till bestämmelsen (prop. 2015/16:148 s. 49) framgår att kvarstadsförordningens bestämmelser om uppgiftsskydd har företrädare framför bestämmelserna i domstolsdatalagen. Vidare har bedömningen gjorts att det bör införas en hänvisning till kvarstadsförordningen i domstolsdatalagen för att uppmärksamma detta förhållande.

I artikel 48 d i kvarstadsförordningen regleras således förhållandet mellan den förordningen och 1995 års dataskyddsdirektiv, som upphör att gälla när dataskyddsförordningen börjar tillämpas. Enligt artikel 94 i dataskyddsförordningen ska dock hänvisningar till 1995 års dataskyddsdirektiv ses som hänvisningar till dataskyddsförordningen. Mot den bakgrunden anser vi att 3 § andra meningen domstolsdatalagen – som reglerar förhållandet mellan den lagen och kvarstadsförordningen – i materiellt hänseende kan kvarstå oförändrad. Vi har dock föreslagit att nuvarande 3 § första meningen domstolsdatalagen ska utgå (se föregående avsnitt) och en delvis ny disposition och struktur i rubriksättningen. Detta medför vissa redaktionella ändringar i lagtexten.

⁵ Se förarbetena till domstolsdatalagen (prop. 2015/16:148 s. 11).

10.6 Befintliga hänvisningar till personuppgiftslagen och hänvisningar till dataskyddslagen

10.6.1 Definitioner

I 5 § första stycket 1 domstolsdatalagen finns en hänvisning till 3 § PuL, som behandlar definitioner. När dataskyddsförordningen börjar tillämpas kommer de definitioner som är aktuella för domstolsdatalagen att finnas i artikel 4 i dataskyddsförordningen. Mot bakgrund av vårt ställningstagande om hänvisningar till enskilda bestämmelser i dataskyddsförordningen anser vi att någon hänvisning till dataskyddsförordningens bestämmelse inte bör göras i denna del.

10.6.2 Förhållandet till offentlighetsprincipen

I 5 § första stycket 2 domstolsdatalagen finns en hänvisning till 8 § PuL. Första stycket i sistnämnda bestämmelse behandlar förhållandet till offentlighetsprincipen. Vad gäller andra stycket, som bl.a. behandlar arkivering, finns våra överväganden i kapitel 19.

När dataskyddsförordningen börjar tillämpas kommer förhållandet mellan offentlighetsprincipen och regelverket för personuppgiftsbehandling inom dataskyddsförordningens tillämpningsområde att regleras direkt av artikel 86 i förordningen. I denna artikel anges att personuppgifter i allmänna handlingar som förvaras av en myndighet, 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 organet omfattas av. Det anges vidare att syftet är att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd av personuppgifter i enlighet med dataskyddsförordningen.

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 130) gjort bedömningen att artikel 86 i dataskyddsförordningen innebär att den svenska offentlighetsprincipen har företräde framför dataskyddsförordningen avseende bl.a. handlingar som förvaras hos myndigheter och andra offentliga organ. Frågan om offentlighetsprincipens förhållande till regelverket kring

personuppgiftsbehandling regleras därmed fullt ut genom dataskyddsförordningen. Mot bakgrund av vårt tidigare ställningstagande anser vi att någon hänvisning till dataskyddsförordningens bestämmelse inte bör göras i denna del.

10.6.3 Grundläggande krav på behandling av personuppgifter

I 5 § första stycket 3 domstolsdatalagen finns en hänvisning till 9 § PuL, vars första stycke behandlar grundläggande krav på behandling av personuppgifter. Vad gäller andra, tredje och fjärde stycket, som bl.a. behandlar arkivering, finns våra överväganden i kapitel 19.

Artikel 5 i dataskyddsförordningen innehåller de grundläggande principer för behandling av personuppgifter som kommer att gälla när förordningen börjar tillämpas (se vidare avsnitt 5.2). Mot bakgrund av vårt tidigare ställningstagande anser vi att någon hänvisning till dataskyddsförordningens bestämmelse inte bör göras i denna del.

10.6.4 Behandling av personnummer och samordningsnummer

Förslag: Uppgifter om personnummer eller samordningsnummer ska även fortsättningsvis få behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Regleringen ska genomföras genom en hänvisning i domstolsdatalagen till den föreslagna bestämmelsen i 3 kap. 13 § dataskyddslagen.

I 5 § första stycket 4 domstolsdatalagen finns en hänvisning till 22 § PuL. Enligt den bestämmelsen får uppgifter om personnummer eller samordningsnummer behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. I förarbetena till domstolsdatalagen (prop. 2014:15:148 s. 51) har regeringen gjort bedömningen att 22 § PuL

innebär en flexibel reglering som är väl avpassad för att förhindra omotiverad behandling av personnummer och samordningsnummer även i domstolarnas verksamhet.

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit att 3 kap. 13 § dataskyddslagen ska innehålla en bestämmelse som till sin lydelse helt motsvarar 22 § PuL. Vi föreslår att det i domstolsdatalagen införs en hänvisning till dataskyddslagens bestämmelse i denna del. På så sätt behålls den reglering av användandet av personnummer och samordningsnummer som för närvarande anses vara ändamålsenlig i domstolarnas verksamhet.

10.6.5 Information till den registrerade och rättelse

I 5 § första stycket 5 och 6 domstolsdatalagen finns hänvisningar till 23, 25–28 §§ PuL. Dessa bestämmelser reglerar information till den registrerade och den registrerades rätt till rättelse, blockering och utplåning av personuppgifter. I kapitel 15 finns en redogörelse för vad som kommer att gälla i dessa frågor när dataskyddsförordningen börjar tillämpas. Där finns även våra överväganden av vilka hänvisningar som bör göras till dataskyddslagen i denna del.

10.6.6 Säkerhet vid behandlingen

I 5 § första stycket 7 domstolsdatalagen finns en hänvisning till 30 och 31 §§ och till 32 § första stycket PuL. Dessa bestämmelser reglerar hur ett personuppgiftsbiträde får behandla personuppgifter, den personuppgiftsansvariges ansvar för att lämpliga skyddsåtgärder vidtas och tillsynsmyndighetens rätt att besluta om säkerhetsåtgärder. Innehållet i 30 och 31 §§ PuL återfinns i delar av artikel 28 och delar av artikel 32 i dataskyddsförordningen. Vilka befogenheter tillsynsmyndigheten har regleras i artikel 58 i dataskyddsförordningen. Mot bakgrund av vårt tidigare ställningstagande anser vi att någon hänvisning till dataskyddsförordningens bestämmelser inte bör göras i denna del.

10.6.7 Överföring till tredje land

I 5 § första stycket 8 domstolsdatalagen finns en hänvisning till 33–35 §§ PuL, som gäller överföring av personuppgifter till tredje land. Bestämmelser om under vilka förutsättning personuppgifter får överföras till tredje land finns i artikel 44–49 i dataskyddsförordningen. Mot bakgrund av vårt tidigare ställningstagande anser vi att någon hänvisning till dataskyddsförordningens bestämmelser inte bör göras i denna del.

10.6.8 Personuppgiftsombud och förhandskontroll

I 5 § första stycket 9 domstolsdatalagen finns hänvisningar till 38, 40 och 41 §§ PuL. Dessa bestämmelser reglerar vilka arbetsuppgifter ett personuppgiftsombud har (38 och 40 §§) samt en rätt för regeringen att meddela föreskrifter om att vissa behandlingar av personuppgifter ska anmälas för förhandskontroll till tillsynsmyndigheten (41 §).

I kapitel 13 finns vårt förslag om hur domstolsdatalagens bestämmelser om personuppgiftsombud bör förändras med anledning av dataskyddsförordningen.

I artikel 55–58 i dataskyddsförordningen finns bestämmelser om tillsynsmyndigheternas behörighet, uppgifter och befogenheter. Här finns bl.a. – i artikel 36 och artikel 58.3 a och c – bestämmelser om förhandssamråd och förhandstillstånd, som är dataskyddsförordningens motsvarighet till personuppgiftslagens bestämmelser om förhandskontroll. Mot bakgrund av vårt tidigare ställningstagande anser vi att någon hänvisning till dataskyddsförordningens bestämmelser inte bör göras i denna del. Upplyningsvis kan sägas att möjligheten att med stöd av artikel 36.5 i dataskyddsförordningen införa nationella bestämmelser om krav på förhandstillstånd av tillsynsmyndigheten för vissa behandlingar, inte har utnyttjats i det förslag till dataskyddslag som finns i Dataskyddsutredningens betänkande (SOU 2017:39 s. 243 ff.).

10.6.9 Tillsynsmyndighetens handläggning och beslut

Förslag: Dataskyddslagens bestämmelser om tillsynsmyndighetens handläggning och beslut ska gälla även på domstolsdatalagens tillämpningsområde. Regleringen ska genomföras genom en hänvisning i domstolsdatalagen till de föreslagna bestämmelserna i 6 kap. 1–5 §§ dataskyddslagen.

I 5 § första stycket 10 domstolsdatalagen finns hänvisningar till 43 och 44 §§, 45 § första stycket och 47 § PuL. Här regleras tillsynsmyndighetens befogenheter att vidta åtgärder mot de personuppgiftsansvariga.

Tillsynsmyndighetens behörighet, uppgifter och befogenheter regleras utförligt i artikel 55–59 i dataskyddsförordningen. Enligt dessa bestämmelser har tillsynsmyndigheten bl.a. befogenhet att behandla klagomål från registrerade, utfärda varningar och reprimander mot personuppgiftsansvariga, rikta förelägganden mot personuppgiftsansvariga samt besluta om begränsning av eller förbud mot en viss behandling. Tillsynsmyndigheten har enligt artikel 83 i dataskyddsförordningen även rätt att påföra de personuppgiftsansvariga administrativa sanktionsavgifter. Våra överväganden vad gäller sanktionsavgifter finns i avsnitt 10.7. Mot bakgrund av vårt tidigare ställningstagande anser vi att någon hänvisning till dataskyddsförordningens bestämmelser om tillsynsmyndighetens befogenheter m.m. inte bör göras i denna del.

Enligt det förslag som finns i Dataskyddsutredningens betänkande (SOU 2017:39) kommer dataskyddslagen dock att innehålla vissa kompletterande bestämmelser om tillsynsmyndighetens handläggning och beslut. Dessa finns enligt förslaget i 6 kap. dataskyddslagen. I de följande avsnitten kommer vi att redogöra för dessa bestämmelser och för varje bestämmelse göra en bedömning av om den bör gälla även på domstolsdatalagens tillämpningsområde.

Det finns i detta sammanhang anledning att uppmärksamma att tillsynsmyndigheten, enligt artikel 55.3 i dataskyddsförordningen, inte är behörig att utöva tillsyn över den personuppgiftsbehandling som sker i domstolarnas dömande verksamhet. Enligt vår bedömning omfattar den dömande verksamheten all personuppgiftsbehandling som sker i det enskilda målet eller ärendet från

att detta anhängiggörs till att ett slutligt avgörande har fattats. Utifrån den definitionen är det endast en relativt liten del av domstolarnas rättskipande och rättsvårdande verksamhet som står under tillsynsmyndighetens tillsyn (se vidare kapitel 8).

Tillsynsmyndighetens befogenheter

Av förslaget till 6 kap. 1 § dataskyddslagen framgår att de befogenheter som tillsynsmyndigheten har enligt artikel 58.1–3 i dataskyddsförordningen ska gälla även vid tillsyn över efterlevnaden av bestämmelserna i dataskyddslagen och andra författningar som kompletterar dataskyddsförordningen. De aktuella bestämmelserna i dataskyddsförordningen handlar om tillsynsmyndighetens utredningsbefogenheter, korrigerande befogenheter och befogenheter att utfärda tillstånd och ge råd.

Som framgår av ordalydelsen i den föreslagna 6 kap. 1 § dataskyddslagen ska tillsynsmyndighetens befogenheter gälla oavsett om de kompletterande nationella bestämmelserna finns i dataskyddslagen eller i sektorsspecifika registerförfattningar. Dataskyddsutredningen uttalar i sitt betänkande (SOU 2017:39 s. 311) att det krävs att tillsynsmyndigheten kan vidta samma åtgärder vid sin tillsyn över efterlevnaden av de nationella bestämmelser som kompletterar förordningen, för att dataskyddsförordningens intentioner ska få genomslag.

Att tillsynsmyndigheten har behörighet att övervaka hur dataskyddsförordningens bestämmelser följs i den del av domstolarnas rättskipande och rättsvårdande verksamhet som inte är dömande framgår redan av artikel 57.1 a i dataskyddsförordningen. Enligt den bestämmelsen ansvarar tillsynsmyndigheten på sitt territorium för att övervaka och verkställa tillämpningen av förordningen. Vi anser att det inte finns några bärande skäl mot att tillsynen över den del av domstolarnas verksamhet som inte är dömande sker på samma sätt som för övriga myndigheter. Mot den bakgrunden föreslår vi att det tas in en hänvisning till 6 kap. 1 § dataskyddslagen i domstolsdatalagen. På detta sätt kommer dataskyddsförordningens bestämmelser om utredningsbefogenheter, korrigerande befogenheter samt befogenheter att utfärda tillstånd och ge råd, att gälla även för den

tillsyn som sker av domstolarnas tillämpning av dataskyddslagen (i tillämpliga delar) och domstolsdatalagens bestämmelser.

Ansökan hos förvaltningsrätten

Enligt förslaget till 6 kap. 2 § första stycket dataskyddslagen gäller följande. Om tillsynsmyndigheten vid handläggningen av ett ärende finner att det finns skäl att ifrågasätta giltigheten av en unionsrättsakt som påverkar tillämpningen av dataskyddsförordningen i ärendet, får tillsynsmyndigheten hos allmän förvaltningsdomstol ansöka om att en åtgärd enligt artikel 58.2 i dataskyddsförordningen ska vidtas. Artikel 58.2 i förordningen reglerar tillsynsmyndighetens korrigerande befogenheter, så som att förelägga en personuppgiftsansvarig att radera personuppgifter eller att förbjuda en personuppgiftsansvarig att behandla personuppgifter.

Enligt förslaget framgår det av 6 kap. 2 § andra stycket dataskyddslagen att tillsynsmyndighetens ansökan i dessa fall ska göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av tillsynsmyndighetens beslut. I den föreslagna 8 kap. 6 § dataskyddslagen klargörs att denna typ av beslut kan överklagas och av 6 kap. 2 § tredje stycket dataskyddslagen framgår att det krävs prövningstillstånd vid överklagande till kammarrätten.

Dataskyddsutredningen redogör i sitt betänkande (SOU 2017:39 s. 318 f.) för innebörden av 6 kap. 2 § dataskyddslagen på följande sätt.

Om det finns skäl att ifrågasätta om en unionsrättsakt som påverkar tillämpningen av dataskyddsförordningen är giltig, till exempel om ett kommissionsbeslut är förenligt med förordningen och fördragen, kan det vara olämpligt att tillsynsmyndigheten själv fattar beslut om åtgärder enligt artikel 58.2 i dataskyddsförordningen, såsom att den personuppgiftsansvarige ska föreläggas att radera personuppgifter eller att behandling av personuppgifter ska förbjudas. I en sådan situation bör tillsynsmyndigheten i stället kunna ansöka hos allmän förvaltningsdomstol om att åtgärden ska beslutas. Om domstolen i ett sådant mål delar tillsynsmyndighetens tvivel angående giltigheten av den unionsrättsakt som förhindrar eller kräver att åtgärden vidtas, kan domstolen begära ett förhandsavgörande från EU-domstolen och därigenom få rättsaktens giltighet prövad innan något beslut om åtgärden fattas./.../ Denna typ av ansökningsförfarande hos domstol finns redan på ett flertal tillsynsområden, bland annat i 47 § PUL, och

skulle därmed inte i sig utgöra något främmande element i svensk processrätt. På detta sätt kan således förordningens krav på rättsmedel för tillsynsmyndigheten uppfyllas, utan att något nytt processuellt institut behöver tillskapas.

De situationer som bestämmelsen i 6 kap. 2 § dataskyddslagen avser att träffa bör rimligen vara sällsynt förekommande. Vi anser dock att det inte finns anledning att ha en annan reglering för den tillsyn som sker över domstolarnas rättskipande och rättsvårdande verksamhet. Det bör därför enligt vår mening införas en hänvisning i domstolsdatalagen till 6 kap. 2 § dataskyddslagen.

Kommunicering och delgivning

Av den föreslagna 6 kap. 3 § dataskyddslagen framgår att innan tillsynsmyndigheten fattar ett beslut enligt artikel 58.2 i dataskyddsförordningen, ska den som beslutet gäller ges tillfälle att inom en bestämd tid yttra sig över allt material av betydelse för beslutet. Undantag görs om det är uppenbart obehövligt. Om saken är brådskande får tillsynsmyndigheten dock, i avvaktan på yttrandet, besluta att behandlingen av personuppgifter tillfälligt ska begränsas eller förbjudas i enlighet med artikel 58.2 f i dataskyddsförordningen. Det tillfälliga beslutet ska omprövas, när tiden för yttrande har gått ut.

Enligt den föreslagna 6 kap. 4 § dataskyddslagen ska ett beslut enligt 6 kap. 3 § delges, om det inte är uppenbart obehövligt. Delgivning enligt 34–37 §§ delgivningslagen (2010:1932) får användas bara om det finns särskild anledning att anta att mottagaren har avvikit eller på annat sätt håller sig undan. Paragraferna i delgivningslagen avser vissa typer av stämningsmannadelgivning, som innebär att handlingen överlämnas till en annan person än delgivningsmottagaren.

Bestämmelser om kommunikering och delgivning finns i 46 § PuL, som gäller i samband med att tillsynsmyndigheten beslutar om vite. Dessa bestämmelser motsvarar de föreslagna bestämmelserna i 6 kap. 3 och 4 §§ dataskyddslagen. Personuppgiftslagens bestämmelser om vite gäller inte på domstolsdatalagens tillämpningsområde (se 5 § andra stycket domstols-

datalagen) och det har därmed inte funnits någon anledning att ta in en hänvisning till 46 § PuL i domstolsdatalagen.

Enligt artikel 83.5 e och 85.6 i dataskyddsförordningen ska den personuppgiftsansvarige påföras administrativa sanktionsavgifter om denne inte rättar sig efter ett föreläggande som meddelats av tillsynsmyndigheten. Detta innebär att de administrativa sanktionsavgifterna i vissa delar får samma effekt som ett vite. Eftersom administrativa sanktionsavgifter enligt vårt förslag ska få riktas även mot domstolarna (se avsnitt 10.7) finns det anledning att överväga om dataskyddslagens bestämmelser om kommunikering och delgivning ska gälla även vid tillsyn över domstolarna.

Mot bakgrund av att underlåtenheten att följa ett föreläggande kan leda till att administrativa sanktionsavgifter tas ut har Dataskyddsutredningen gjort bedömningen att de processuella skyddsåtgärder som nu kringgärdar tillsynsmyndighetens vitesförelägganden bör gälla för alla beslut som myndigheten kan meddela med stöd av artikel 58.2 i dataskyddsförordningen. Mottagaren av tillsynsmyndighetens föreläggande bör därmed som huvudregel, precis som enligt 46 § PuL, både få möjlighet att yttra sig över materialet i ärendet och få del av föreläggandet på något av de sätt som föreskrivs i delgivningslagen (se SOU 2017:39 s. 313 f.).

För det fall tillsynsmyndigheten beslutar om ett föreläggande mot en domstol finns det enligt vår mening inte anledning att ha ett annat förfarande än det som kommer att gälla för andra myndigheter. Vi anser därför att en hänvisning till 6 kap. 3 och 4 §§ dataskyddslagen bör tas in i domstolsdatalagen. Det faktum att de typer av stämmingsmannadelgivning som regleras i 34–37 §§ delgivningslagen inte kommer att bli aktuella för domstolarna föranleder inte i sig någon särreglering.

Besked angående handläggningen av ett klagomål

Av den föreslagna 6 kap. 5 § dataskyddslagen framgår att om tillsynsmyndigheten inte inom tre månader från den dag då ett klagomål kom in till myndigheten har behandlat klagomålet ska tillsynsmyndigheten på skriftlig begäran av den registrerade antingen lämna besked i frågan om myndigheten avser att utöva tillsyn med anledning av klagomålet, eller i ett särskilt beslut avslå

begäran om besked. Sådant besked eller beslut ska meddelas inom två veckor från den dag då begäran om besked kom in till tillsynsmyndigheten. Om tillsynsmyndigheten har avslagit en begäran om besked, får den registrerade ge in en ny begäran om besked i ärendet tidigast tre månader efter det att myndighetens beslut meddelades.

Av Dataskyddsutredningens betänkande (SOU 2017:39 s. 305 ff.) framgår att förslaget till 6 kap. 5 § dataskyddslagen har införts för att uppfylla det krav på effektivt rättsmedel som garanteras genom dataskyddsförordningen. Som vi framfört under föregående rubrik anser vi att det inte finns anledning att ha ett annat förfarande för tillsyn över domstolarna än det som kommer att gälla vid tillsyn över andra myndigheter. Vi anser därför att en hänvisning till 6 kap. 5 § dataskyddslagen bör tas in i domstolsdatalagen.

10.6.10 Skadestånd

I 5 § första stycket 11 domstolsdatalagen finns hänvisningar till 48 § PuL, som gäller den registrerades rätt till skadestånd. I avsnitt 15.7 finns en redogörelse för vad som kommer att gälla i denna fråga när dataskyddsförordningen börjar tillämpas. Där finns även våra överväganden av vilka hänvisningar som ska göras till dataskyddslagen i denna del.

10.6.11 Förhållandet till tryck- och yttrandefriheten

Förslag: Bestämmelserna i dataskyddsförordningen, dataskyddslagen och domstolsdatalagen ska inte tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Regleringen ska genomföras genom en hänvisning i domstolsdatalagen till den föreslagna bestämmelsen i 1 kap. 4 § första stycket dataskyddslagen.

Av artikel 85.1 i dataskyddsförordningen följer att medlemsstaterna i lag ska förena rätten till integritet i enlighet med

förordningen med bl.a. yttrande- och informationsfriheten. Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit att det av 1 kap. 4 § första stycket dataskyddslagen ska framgå 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. Bestämmelsen motsvarar den reglering som för närvarande finns i 7 § första stycket PuL, som innebär att bestämmelserna i personuppgiftslagen inte ska tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Det finns för närvarande inte någon hänvisning i domstolsdatalagen till den sistnämnda bestämmelsen.

Dataskyddsutredningen har föreslagit att dataskyddslagen ska vara subsidiär till bestämmelser som rör behandling av personuppgifter i annan lag eller författning (1 kap. 3 § dataskyddslagen). Denna reglering innebär att tryckfrihetsförordningen gäller före dataskyddslagen, något som dessutom följer redan av allmänna rättsliga principer om att bestämmelser i vanlig lag inte tar över bestämmelser i grundlag (lex superior). Hur tryckfrihetsförordningens och yttrandefrihetsgrundlagarnas bestämmelser förhåller sig till dataskyddsförordningens bestämmelser är emellertid inte lika självklart. Mot den bakgrunden föreslår vi att det i domstolsdatalagen görs en hänvisning till den föreslagna 1 kap. 4 § första stycket dataskyddslagen. Hänvisningen ska förstås så att inte bara dataskyddsförordningens och dataskyddslagens, utan även domstolsdatalagens bestämmelser får ge vika för bestämmelserna om tryck- och yttrandefrihet. Bestämmelsens andra stycke, som gäller personuppgifter som behandlas för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande är enligt vår mening inte relevanta för domstolarnas verksamhet.

10.7 Sanktionsavgifter

<p>Förslag: Dataskyddslagens bestämmelser om administrativa sanktionsavgifter ska, med undantag för den bestämmelse som</p>
--

gäller överträdelser av artikel 10 i dataskyddsförordningen, gälla även på domstolsdatalagens tillämpningsområde. Regleringen ska genomföras genom en hänvisning i domstolsdatalagen till de föreslagna bestämmelserna i 7 kap. 1, 3 och 4 §§ dataskyddslagen.

Enligt artikel 83 i dataskyddsförordningen har tillsynsmyndigheten i vissa fall möjlighet att påföra de personuppgiftsansvariga administrativa sanktionsavgifter vid överträdelser av förordningens bestämmelser. Av artikel 83.7 framgår att varje medlemsstat får fastställa regler för om och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och organ som är inrättade i medlemsstaten.

Dataskyddsutredningen föreslår i sitt betänkande (SOU 2017:39) att 7 kap. 1–4 §§ dataskyddslagen ska innehålla bestämmelser om administrativa sanktionsavgifter. Enligt den föreslagna 7 kap. 1 § första stycket dataskyddslagen får sanktionsavgifter tas ut även av myndigheter vid överträdelser som avses i artikel 83.4–6 i dataskyddsförordningen, varvid artikel 83.1–3 ska tillämpas. De sistnämnda punkterna reglerar principerna för påförande av sanktionsavgifter. Enligt den föreslagna 7 kap. 1 § andra stycket dataskyddslagen ska avgiften bestämmas till högst 10 000 000 kr vid överträdelser som avses i artikel 83.4 i dataskyddsförordningen och annars till högst 20 000 000 kr.

I den föreslagna 7 kap. 2 § dataskyddslagen anges att sanktionsavgift får tas ut vid överträdelser av artikel 10 i dataskyddsförordningen. Bestämmelsen reglerar även avgiftens storlek i sådana fall. Administrativa sanktionsavgifter får vidare, enligt den föreslagna 7 kap. 3 § dataskyddslagen, inte beslutas om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig enligt 6 kap. 3 § dataskyddslagen inom fem år från den dag då överträdelsern ägde rum (se avsnitt 10.6.9 under rubriken Kommunikering och delgivning). Enligt 7 kap. 4 § dataskyddslagen ska sanktionsavgifter som beslutats enligt dataskyddsförordningen eller dataskyddslagen tillfalla staten.

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 288 ff.) gjort bedömningen att övervägande skäl talar för att administrativa sanktionsavgifter ska kunna påföras statliga och kommunala myndigheter. Som grund för bedömningen framhöll

Dataskyddsutredningen bl.a. den omfattning av känsliga personuppgifter som hanteras av myndigheter, att enskildas intresse av skydd för den personliga integriteten väger lika tungt vid behandling av personuppgifter i det allmänna verksamhet som i den privata sektorn och att behovet av avskräckande sanktioner inte är mindre när det gäller myndigheternas personuppgiftsbehandling.

Vi vill även i detta sammanhang påminna om att tillsynsmyndigheten, enligt artikel 55.3 i dataskyddsförordningen, inte är behörig att utöva tillsyn över den personuppgiftsbehandling som sker i domstolarnas dömande verksamhet. Enligt vår bedömning omfattar den dömande verksamheten all personuppgiftsbehandling som sker i det enskilda målet eller ärendet från att detta anhängiggörs till att ett slutligt avgörande har fattats. Utifrån den definitionen är det endast en relativt liten del av domstolarnas rättsskipande och rättsvårdande verksamhet som omfattas av tillsynsområdet och kan ge upphov till sanktionsavgifter (se vidare kapitel 8).

För den del av domstolarnas verksamhet som faller under tillsynsmyndighetens behörighet anser vi även i detta fall att det inte finns anledning att ha ett annat förfarande för tillsyn mot domstolarna än det som kommer att gälla vid tillsyn mot andra myndigheter (jfr avsnitt 10.6.9). Vi anser därför att en hänvisning till 7 kap. 1, 3 och 4 §§ dataskyddslagen bör tas in i domstolsdatalagen.

Bestämmelsen i 7 kap. 2 § dataskyddslagen behandlar överträdelser av artikel 10 i dataskyddsförordningen, enligt vilken behandling av personuppgifter som rör bl.a. fällande domar i brottmål endast får utföras under kontroll av myndighet. Eftersom domstolarna, i sin egenskap av myndigheter, inte kan göra sig skyldiga till överträdelser av artikel 10 i dataskyddsförordningen bör det enligt vår mening inte göras någon hänvisning till 7 kap. 2 § dataskyddslagen.

Dataskyddslagens föreslagna bestämmelser om sanktionsavgifter gäller endast överträdelser av de bestämmelser i dataskyddsförordningen som anges i artikel 83.4–6. Beträffande nationella bestämmelser anges i artikel 83.5 d att endast sådana bestämmelser som antagits enligt kapitel IX i förordningen kan föranleda sanktionsavgifter. Det gäller bland annat rätten att

behandla uppgifter om nationella identifikationsnummer (artikel 87) och rätten att behandla personuppgifter i anställningsförhållanden (artikel 88). Detta innebär enligt vår mening motsatsvis att överträdelse av andra nationella bestämmelser än sådana som införts med stöd av kapitel IX inte träffas av dataskyddsförordningens bestämmelser om sanktionsavgifter. Eventuellt skulle dock överträdelse av nationella bestämmelser som utgör ett förtydligande av dataskyddsförordningens bestämmelser kunna ses som en överträdelse av förordningens bestämmelser och därmed kunna föranleda sanktionsavgift.

Som vi anført ovan anser vi att tillsynsmyndigheten bör tillämpa samma förfarande vid tillsyn mot domstolarna som mot andra myndigheter, på det område där tillsynsmyndigheten är behörig att utöva tillsyn. Det finns enligt vår mening emellertid inte anledning att utöka tillsynsmyndighetens möjligheter att besluta om sanktionsavgifter för domstolarna. En sådan reglering skulle dessutom enligt vår mening vidare ha en begränsad praktisk betydelse. Anledningen till detta är att tillsynsmyndigheten inte är behörig att utöva tillsyn över domstolarnas dömande verksamhet, vilken enligt vår bedömning omfattar övervägande delen av den personuppgiftsbehandling som sker inom domstolsdatalagens tillämpningsområde (se kapitel 8).

11 Tillgången till personuppgifter

Bedömning: Dataskyddsförordningen föranleder ingen ändring av domstolsdatalagens och domstolsdataförordningens bestämmelser om tillgången till personuppgifter för anställda m.fl.

Enligt 8 § första stycket domstolsdatalagen ska tillgången till personuppgifter begränsas till det som varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Av andra stycket i samma bestämmelse framgår att regeringen eller den myndighet som regeringen bestämmer med stöd av 8 kap. 7 § regeringsformen kan meddela närmare föreskrifter om tillgången till personuppgifter.

Av 2 § domstolsdataförordningen framgår att den personuppgiftsansvarige ansvarar för att det inom myndigheten finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter för tillgång till personuppgifter.

Den personuppgiftsansvarige har, enligt artikel 24.1 och artikel 32 i dataskyddsförordningen, skyldighet att se till att en lämplig säkerhetsnivå för behandlingen av personuppgifter upprätthålls. Detta ska, enligt samma bestämmelser, ske bl.a. genom att den personuppgiftsansvarige vidtar lämpliga tekniska och organisatoriska åtgärder. Den personuppgiftsansvariges skyldigheter i denna del återfinns även i de allmänna principer för behandling av personuppgifter som framgår av artikel 5.1 f i dataskyddsförordningen.

Vi har gjort bedömningen att sökbegränsningar utgör en säkerhetsåtgärd i dataskyddsförordningens mening (se avsnitt 16.5.4). Detsamma gäller enligt vår uppfattning bestämmelser om behörighetsbegränsningar, tilldelningsstyrning

och andra rutiner som säkerställer att personuppgiftsbehandlingen sker i enlighet med dataskyddsförordningen.

Åtgärder som säkerställer en lämplig säkerhetsnivå ska förvisso vidtas av de personuppgiftsansvariga även utan bestämmelser i registerförfattningar. Bestämmelser om vilka säkerhetsåtgärder som ska vidtas i en viss verksamhet utgör dock enligt vår mening sådana specifika krav på personuppgiftsbehandling som enligt artikel 6.2 i dataskyddsförordningen får fastställas genom nationella registerförfattningar (se kapitel 5).

Att det finns säkerhetsåtgärder för personuppgiftsbehandlingen är vidare en förutsättning för att känsliga personuppgifter ska få behandlas för ett viktigt allmänt intresse med stöd av undantaget i artikel 9.2 g i dataskyddsförordningen. Av avsnitt 16.5.1 framgår att detta undantag har stor betydelse för domstolarnas rättskipande och rättsvårdande verksamhet. Det faktum att en säkerhetsåtgärd kommer till uttryck i en registerförfattning säkerställer enligt vår mening skyddsåtgärden på ett sådant sätt som avses i artikel 9.2 g i förordningen. I avsnitt 20.2 gör vi vidare bedömningen att dataskyddsförordningen inte hindrar att nationella bestämmelser om personuppgiftsbehandling införs i en förordning eller i en myndighetsföreskrift, så länge föreskrifterna tillkommit i laga ordning.

Mot den bakgrunden bedömer vi att bestämmelserna i 8 § domstolsdatalagen och 2 § domstolsdataförordningen är förenliga med dataskyddsförordningen och bör kvarstå i sin nuvarande lydelse.

Vi vill i detta sammanhang betona att förekomsten av behörighetsbegränsningar m.m. i en registerförfattning inte innebär att man kan bortse från de övriga krav på lämpliga säkerhetsåtgärder som dataskyddsförordningen föreskriver. Som ett exempel kan nämnas att det i förordningen ställs krav på att dataskydd byggs in i databehandlingssystem i den utsträckning det är lämpligt med hänsyn till bl.a. kostnader, behandlingens art och omfattning och de risker som behandlingen innebär (artikel 25). Som ett exempel på ett sådant inbyggt dataskydd kan nämnas loggning.

12 Personuppgiftsansvar

Bedömning: Dataskyddsförordningen föranleder ingen ändring av domstolsdatalagens bestämmelse om personuppgiftsansvaret.

I artikel 4.7 i dataskyddsförordningen definieras personuppgiftsansvarig som 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. Enligt samma artikel finns också en möjlighet att i nationell lagstiftning föreskriva vem som är personuppgiftsansvarig för en viss personuppgiftsbehandling. En förutsättning för detta är att ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt. Även i skäl 45 till dataskyddsförordningen framhålls att vem som är personuppgiftsansvarig kan fastställas i den nationella rätten.

Definitionen av personuppgiftsansvaret i dataskyddsförordningen innebär ingen förändring gentemot tidigare regelverk. Artikel 4.7 i dataskyddsförordningen motsvaras av artikel 2 d i 1995 års dataskyddsdirektiv.

För domstolarnas del har den svenska lagstiftaren dock utnyttjat möjligheten att i nationell registerlagstiftning utpeka vem som är personuppgiftsansvarig. Enligt 9 § domstolsdatalagen är en allmän domstol, en allmän förvaltningsdomstol eller en hyres- och arrendenämnd personuppgiftsansvarig för den behandling av personuppgifter som den domstolen eller nämnden utför.

Vid remitteringen av förslaget till domstolsdatalag framfördes synpunkter på att domstolarnas faktiska möjlighet att påverka om och hur en enskild personuppgiftsbehandling ska företas kan vara begränsade eftersom det är Domstolsverket som utformar datorsystemen. I förarbetena till domstolsdatalagen (prop.

2014/15:148 s. 32–36) gjorde regeringen dock bedömningen att fördelarna med att varje enskild domstol är personuppgiftsansvarig bl.a. är att det blir tydligt för den enskilde vem han eller hon ska vända sig till med klagomål. Regeringen uttalade vidare att ett delat eller gemensamt personuppgiftsansvar (mellan domstolarna och Domstolsverket) medför beaktansvärda nackdelar i form av gränsdragningsproblem och otydligheter.

Frågan om vilken eller vilka myndigheter som ska ha personuppgiftsansvaret för domstolarnas personuppgiftsbehandling inom den rättskipande och rättsvårdande verksamheten har således behandlats genom överväganden i tidigare förarbeten. Data-skyddsförordningen föranleder inte någon ändring av den rådande ordningen, eftersom möjligheten att i bl.a. registerförfattning utpeka vem som är personuppgiftsansvarig kvarstår. Vi föreslår därför inte någon ändring av domstolsdatalagen i denna del.

13 Dataskyddsbud

Termen dataskyddsbud definieras inte i dataskyddsförordningen. I artikel 37–39 beskrivs dock bl.a. dataskyddsbudets uppgifter och förhållande till den personuppgiftsansvarige. Utifrån dessa bestämmelser kan man dra slutsatsen att dataskyddsbudet motsvarar det som i 1995 års dataskyddsdirektiv benämns uppgiftsskyddsbud och som i personuppgiftslagen kallas personuppgiftsbud.

13.1 Dataskyddsförordningen

13.1.1 Möjlighet att föreskriva att dataskyddsbud ska utses

Det personuppgiftsbud som enligt domstolsdatalagen för närvarande ska utses har personuppgiftsbehandlingen inom hela den rättskipande och rättsvårdande verksamheten som sitt ansvarsområde. Enligt artikel 37.1 a i dataskyddsförordningen är huvudregeln att ett dataskyddsbud ska utses när personuppgiftsbehandling genomförs av en myndighet. Endast den personuppgiftsbehandling som sker som en del av domstolarnas dömande verksamhet är undantagen från denna skyldighet.

Av artikel 37.4 i dataskyddsförordningen framgår emellertid att även i andra fall än de som regleras i punkten 1 får den personuppgiftsansvarige utnämna ett dataskyddsbud. Enligt samma bestämmelse *ska* ett dataskyddsbud utses om det krävs enligt unionsrätten eller medlemsstaternas nationella rätt. Vi gör bedömningen att detta innebär en möjlighet att i nationell lagstiftning föreskriva att dataskyddsbud ska utses även om det inte är obligatoriskt enligt dataskyddsförordningen.

13.1.2 Dataskyddsbudets ställning, uppgifter m.m.

Dataskyddsbudet beskrivs i skäl 97 till dataskyddsförordningen som ”en person med sakkunskap i fråga om dataskyddslagstiftning och -förfaranden”. Artikel 37 i förordningen innehåller diverse bestämmelser om dataskyddsbudet. Ombudet ska utses på grundval av yrkesmässiga kvalifikationer och bl.a. ha sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som förordningen ålägger ett dataskyddsbud (37.5). Det anges vidare att dataskyddsbudet antingen kan vara en anställd eller utföra uppgiften på grund av tjänsteavtal (37.6). Dataskyddsbudets kontaktuppgifter ska offentliggöras och meddelas till tillsynsmyndigheten (37.7). Vidare framgår att ett enda dataskyddsbud får utnämnas för flera personuppgiftsansvariga myndigheter, med hänsyn till organisationsstruktur och storlek (37.3). Det finns ingen ledning i dataskyddsförordningens skäl om hur bestämmelsen om gemensamt dataskyddsbud ska tolkas. Det man kan sluta sig till är enligt vår mening endast det som framgår av bestämmelsen; de myndigheter som vill utse ett gemensamt dataskyddsbud måste göra en bedömning av om detta är lämpligt utifrån samtliga inblandade myndigheters organisationsstruktur och storlek.

I artikel 38 redogörs bl.a. för dataskyddsbudets självständiga ställning gentemot den personuppgiftsansvarige. Som exempel kan nämnas följande. Den personuppgiftsansvarige ska se till att dataskyddsbudet har tillgång till de uppgifter och resurser som krävs för att fullgöra uppdraget och upprätthålla sin sakkunskap (38.2). Vidare ska den personuppgiftsansvarige säkerställa att ombudet inte tar emot instruktioner om hur han eller hon ska utföra sina uppgifter. Ombudet får inte heller avsättas eller bli föremål för sanktioner för att ha utfört sina uppgifter (38.3). Dataskyddsbudet får fullgöra andra uppgifter och uppdrag, men den personuppgiftsansvarige ska se till att dessa inte leder till en intressekonflikt (38.6).

Av artikel 38.5 i dataskyddsförordningen framgår att dataskyddsbudet vid genomförande av sina uppgifter ska vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt. Mot den bakgrunden har Dataskyddsutredningen i sitt betänkande (SOU 2017:39)

föreslagit att det i 1 kap. 6 § första stycket dataskyddslagen ska regleras att den som utsetts till dataskyddsbud enligt artikel 37 i dataskyddsförordningen inte obehörigen får röja det som han eller hon vid fullgörandet av sin uppgift har fått veta om enskilda personliga och ekonomiska förhållanden. Enligt andra stycket i samma bestämmelse ska det enligt utredningens förslag framgå att offentlighets- och sekretesslagen tillämpas i det allmännas verksamhet i stället för första stycket.

Enligt 2 kap. 1 § OSL första stycket är det förbjudet för myndigheter att röja eller utnyttja en uppgift som det råder sekretess för. Detsamma gäller enligt andra stycket för personer som fått kännedom om uppgiften genom att han eller hon för det allmännas räkning deltagit i en myndighets verksamhet på grund av anställning eller uppdrag hos myndigheten, på grund av tjänsteplikt eller på annan liknande grund. Dataskyddsutredningen har gjort bedömningen att en myndighets dataskyddsbud i allmänhet får anses delta i verksamheten på ett sådant sätt som avses i 2 kap. 1 § OSL andra stycket och att han eller hon därmed omfattas av den sekretess som gäller för den aktuella myndigheten.¹

Artikel 39.1 i dataskyddsförordningen reglerar dataskyddsbudets uppgifter. Dessa ska enligt bestämmelsen åtminstone vara följande.

- a) Informera och ge råd till den personuppgiftsansvarige, personuppgiftsbiträdet och de anställda om deras skyldigheter enligt dataskyddsförordningen och andra dataskyddsbestämmelser.
- b) Övervaka efterlevnaden av dataskyddsförordningen och andra dataskyddsbestämmelser samt efterlevnaden av den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter. Detta inbegriper ansvarstilldelning, information till och utbildning av personal.
- c) På begäran ge råd vad gäller sådana konsekvensbedömningar avseende dataskydd som enligt artikel 35 ska göras om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Dataskyddsbudet ska också övervaka genomförandet av en sådan konsekvensbedömning.
- d) Samarbete med tillsynsmyndigheten.

¹ Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 262).

- e) Vara kontaktpunkt för tillsynsmyndigheten i frågor som rör personuppgiftsbehandling. I detta ingår det förhandssamråd som enligt artikel 36 ska genomföras med tillsynsmyndigheten om en konsekvensbedömning enligt artikel 35 visar att behandlingen utan vidtagna åtgärder leder till en hög risk. Vid behov ska samråd även ske i alla andra frågor.
- f) Vidare får den registrerade, enligt artikel 38.4 i dataskyddsförordningen, kontakta dataskyddsbudet när det gäller alla frågor som rör behandlingen av dennes personuppgifter och utövandet av dennes rättigheter enligt förordningen.

13.2 1995 års dataskyddsdirektiv och personuppgiftslagen

I artikel 18.2 i 1995 års dataskyddsdirektiv finns bestämmelserna om det nuvarande personuppgiftsombudets (i direktivet benämnt uppgiftsskyddsombudets) arbetsuppgifter. För det fall ett personuppgiftsombud utses får medlemsstaterna föreskriva att automatiserade behandlingar inte behöver anmälas till tillsynsmyndigheten. Enligt bestämmelsen ska ett personuppgiftsombud på ett oberoende sätt säkerställa den interna tillämpningen av de nationella bestämmelser som antagits till följd av direktivet. Ombudet ska också föra ett register över de behandlingar som utförs av den registeransvarige. Syftet är att säkerställa att de registrerades fri- och rättigheter sannolikt inte kommer att kränkas som en följd av personuppgiftsbehandling. Enligt artikel 20.2 i 1995 års dataskyddsdirektiv kan personuppgiftsombudet även göra en anmälan till tillsynsmyndigheten om förhandskontroll av personuppgiftsbehandlingar som kan innebära särskilda risker.

1995 års dataskyddsdirektivs bestämmelser om personuppgiftsombud har genomförts i svensk rätt genom 38–40 §§ PuL. Enligt dessa bestämmelser ska personuppgiftsombudet ha till uppgift att självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed. Ombudet ska också påpeka eventuella brister för den personuppgiftsansvarige. Med personuppgiftsombudets ansvar följer enligt personuppgiftslagen även en skyldighet att göra en anmälan till tillsynsmyndigheten om ombudet har anledning att misstänka att den personuppgiftsansvarige bryter mot de

bestämmelser som gäller för behandlingen av personuppgifter och inte vidtar rättelse efter påpekande. Även i övrigt ska personuppgiftsbudet samråda med tillsynsmyndigheten vid tveksamhet om hur de bestämmelser som gäller för behandlingen av personuppgifter ska tillämpas.

Personuppgiftsbudet ska enligt personuppgiftslagens bestämmelser vidare föra en förteckning över vissa av de behandlingar som den personuppgiftsansvarige genomför och som skulle ha omfattats av anmälningsskyldighet till tillsynsmyndigheten om ombudet inte hade funnits. Slutligen ska personuppgiftsbudet hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga.

13.3 Domstolsdatalagen

Enligt 10 § domstolsdatalagen ska den personuppgiftsansvarige utse ett eller flera personuppgiftsbud. Av bestämmelsens andra stycke framgår att den personuppgiftsansvarige ska anmäla till tillsynsmyndigheten när ett personuppgiftsbud utses eller entledigas. Vidare hänvisas, genom 5 § första stycket 9 domstolsdatalagen, till de bestämmelser i personuppgiftslagen (38 och 40 §§) där bl.a. personuppgiftsbudets arbetsuppgifter regleras.

Det har, enligt 1995 års dataskyddsdirektiv och personuppgiftslagen, inte varit obligatoriskt för den som behandlar personuppgifter att utse ett personuppgiftsbud. En av anledningarna för en personuppgiftsansvarig att utse ett personuppgiftsbud är enligt nuvarande regelverk att den personuppgiftsansvarige då inte behöver anmäla automatiserad behandling av personuppgifter till tillsynsmyndigheten (se 36 och 37 §§ PuL). En förutsättning för att undantaget ska gälla är dock att personuppgiftsbudet för en förteckning över de personuppgiftsbehandlingar som den personuppgiftsansvarige utför. Domstolarna har emellertid, enligt 3 § 3 personuppgiftsförordningen (1998:1191), inte omfattats av skyldigheten att anmäla personuppgiftsbehandlingar till tillsynsmyndigheten. Det har därmed inte av den anledningen funnits anledning att utse personuppgiftsbud för domstolarnas rättskipande och rättsvårdande verksamhet.

I förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 84) konstaterade regeringen att domstolarnas personuppgiftsbehandling i den rättskipande och rättsvårdande verksamheten indirekt begränsas av de processuella regelverken och att domstolarna därmed har ett mindre utrymme än exempelvis Polismyndigheten att styra över vilka personuppgifter som ska samlas in och behandlas på andra sätt inom verksamheten. Mot den bakgrunden gjorde regeringen bedömningen att risken för att det i domstolarnas verksamhet utförs obefogade integritetskänsliga behandlingar avseende personuppgifter är mindre än inom Polismyndigheten.

Regeringen ansåg trots detta att det bör vara obligatoriskt för domstolarna att utse personuppgiftsombud, eftersom det åstadkommer ett förstärkt integritetsskydd (prop. 2014/15:148 s. 91). De fördelar med att utse personuppgiftsombud som nämns i förarbetena är följande. Personuppgiftsombudet torde ofta få särskilda kunskaper om personuppgiftsfrågor och kan då ge god service åt enskilda som behöver hjälp för att kunna ta tillvara sin rätt. Enskilda får vidare genom personuppgiftsombudet en tydlig kontaktpunkt vid varje domstol i frågor som rör bl.a. information om behandlingen och rättelse av felaktiga uppgifter. Personuppgiftsombudet kan också bidra till kunskapsspridningen inom sin domstol och vara ett stöd för andra medarbetare. Eftersom det inte funnits någon anledning att utforma personuppgiftsombudets arbetsuppgifter och skyldigheter annorlunda än vad som gäller enligt personuppgiftslagen har en hänvisning till personuppgiftslagens bestämmelser i denna del gjorts.

Av 11 § första stycket domstolsdatalagen framgår att den som är personuppgiftsombud ska föra en förteckning över de behandlingar som utförs med stöd av lagen. Av andra stycket framgår att regeringen eller den myndighet som regeringen bestämmer med stöd av 8 kap. 7 § regeringsformen kan meddela närmare föreskrifter om vilka uppgifter en sådan förteckning ska innehålla. Domstolsverket har fått sådan föreskriftsrätt genom 14 § andra stycket 1 domstolsdataförordningen.

Som nämnts ovan är domstolarna undantagna från skyldigheten att anmäla automatiserad personuppgiftsbehandling till tillsynsmyndigheten (jfr. 36 § första stycket PuL och 3 § 3 personuppgiftsförordningen). Av förarbetena till domstols-

datalagen (prop. 2014/15:148 s. 85 f.) framgår att anledningen till att regeringen ansett att det bör vara obligatoriskt för personuppgiftsombudet att föra en förteckning över domstolens personuppgiftsbehandling är att domstolarna bör föreläggas samma skyldighet att sammanställa och göra tillgänglig den information som en anmälan till tillsynsmyndigheten skulle ha innehållit. Fördelen med detta anges vara att såväl den registrerade som andra kan få tillgång till en uppdaterad beskrivning med mer preciserad information om vilka personuppgiftsbehandlingar som sker vid en domstol än vad som kan utläsas ur domstolsdatalagen. Detta uppges vara särskilt värdefullt med tanke på att domstolsdatalagen inte innehåller några uppräknings av vilka personuppgiftsbehandlingar som ska vara tillåtna. Anledning till att skyldigheten att föra förteckningen ålagts personuppgiftsombudet och inte den personuppgiftsansvarige är enligt förarbetena för att skapa likhet med vad som gäller enligt 2 kap. 2 § polisdatalagen (2010:361). I 2 kap. 2 § polisdatalagen görs en hänvisning till de bestämmelser i personuppgiftslagen som bl.a. gäller personuppgiftsombudets skyldighet att föra en sådan förteckning.

13.4 Domstolarnas uppfattning

Med anledning av den möjlighet som dataskyddsförordningen ger att trots undantaget för domstolarnas dömande verksamhet utse dataskyddsbud för denna verksamhet (se avsnitt 13.1.1) har vi, via Domstolsverket, efterfrågat domstolarnas uppfattning. Förfrågan skickades ut till samtliga allmänna domstolar, allmänna förvaltningsdomstolar och hyres- och arrendenämnder. Av de 53 domstolar och nämnder som svarade ansåg 19 att dataskyddsbudets ansvarsområde borde omfatta även den dömande verksamheten, medan 25 hade motsatt uppfattning. Resterande 9 hade ingen uppfattning i frågan eller ansåg att det krävdes ytterligare utredning för att besvara den.

De argument som framfördes för att dataskyddsbud ska utses även för den dömande verksamheten var bl.a. att det är svårt att se en tydlig gräns mellan den dömande verksamheten och övriga verksamheter och att man på detta sätt undviker gränsdragningsproblem. Vidare framfördes att det finns behov av intern

övervakning av personuppgiftsbehandlingen även i den dömande verksamheten och att det är bra om någon upprätthåller kunskap om regelverket. Det framfördes också att det utifrån ett medborgar- och rättsäkerhetsperspektiv är svårt att motivera att det inte ska finnas ett dataskyddsbud för den dömande verksamheten även i framtiden och att det inte finns några bärande skäl för att domstolarna som enda myndighet ska sakna ett dataskyddsbud för sin kärnverksamhet.

De argument som framfördes mot att dataskyddsbud ska utses även för den dömande verksamheten var bl.a. följande. Den dömande verksamhetens speciella karaktär gör det svårt att utöva någon form av tillsyn och det är rimligare att en korrekt behandling av personuppgifter i den dömande verksamheten säkerställs av domarna. Detta skulle upprätthålla självständighet och oberoende. Vidare framfördes att risken för överträdelser är begränsad med hänsyn till att hanteringen av personuppgifter styrs av de processuella regelverken och till att JO och JK utövar tillsyn över domstolarna. Det ansågs vidare att personuppgiftsbudets arbetsuppgifter redan tar mycket tid i anspråk och att det finns en risk för att arbetsuppgiften blir för omfattande. Små domstolar uppgavs också redan i dag ha svårigheter att hitta rätt kompetens för uppdraget.

13.5 Bedömning

Förslag: Den personuppgiftsansvariga domstolen ska utse ett eller flera dataskyddsbud för personuppgiftsbehandling inom domstolsdatalogens tillämpningsområde.

Domstolsdatalogens bestämmelse om att den personuppgiftsansvarige ska anmäla till tillsynsmyndigheten när ett ombud utses eller entledigas ska upphävas.

Domstolsdatalogens bestämmelser om att ombudet ska föra en förteckning över de behandlingar som utförs med stöd av lagen samt regeringens eller myndighets föreskriftsrätt angående innehållet i sådan förteckning ska upphävas.

13.5.1 Behovet av en analys

Enligt domstolsdatalagens nuvarande lydelse ska den personuppgiftsansvarige utse ett eller flera personuppgiftsombud. Som nämnts ovan (avsnitt 13.1.1) gör vi bedömningen att artikel 37.4 i dataskyddsförordningen ger möjlighet att i nationell lagstiftning föreskriva att en personuppgiftsansvarig ska utse dataskyddsbud även då det inte är obligatoriskt enligt dataskyddsförordningen. Mot den bakgrunden anser vi att det finns möjlighet att även när dataskyddsförordningen börjar tillämpas behålla den ordning med personuppgiftsombud (dataskyddsbud) som gäller enligt domstolsdatalagen i dag. Vi anser därför att en analys bör göras av för- och nackdelarna med att föreskriva att ett ombud ska utses även för den dömande verksamheten.

13.5.2 Dataskyddsbudet – ”internrevisor” med något utökat uppdrag

Dataskyddsförordningens reglering är mer utförlig än 1995 års dataskyddsdirektivs och personuppgiftslagens reglering vad gäller ombudets kvalifikationer och arbetsuppgifter. Även förhållandet till den personuppgiftsansvarige och dennes skyldigheter gentemot ombudet beskrivs mer detaljerat i förordningen. Frågan är emellertid om detta innebär någon skillnad i sak vad gäller de uppgifter ett dataskyddsbud förväntas utföra.

Enligt personuppgiftslagen ska personuppgiftsombudet se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed. Han eller hon ska också påpeka eventuella brister i behandlingen för den personuppgiftsansvarige. Personuppgiftslagens beskrivning av ombudets arbetsuppgifter är således inte speciellt konkret, vilket naturligtvis öppnar för tolkningar av vad ombudet egentligen ska göra och hur detta ska gå till. Vi kan dock inte se annat än att det i uppgiften att ”se till att personuppgifter behandlas lagligt och korrekt” samt ”påpeka eventuella brister för den personuppgiftsansvarige” bör ingå många av de uppgifter som ett dataskyddsbud uttryckligen åläggs enligt dataskyddsförordningen (se avsnitt 13.1.2). Som exempel kan nämnas att informera och ge råd till både den personuppgiftsansvarige och de anställda gällande

dataskyddsbestämmelser, att övervaka hur dessa bestämmelser följs och att medverka i arbetet kring konsekvensbedömningar avseende dataskydd.

Vidare bör en person som ska övervaka personuppgiftsbehandlingen på det sätt som beskrivs i personuppgiftslagen enligt vår mening ha de kvalifikationer (t.ex. sakkunskap inom rättsområdet) som beskrivs i dataskyddsförordningen för att klara av att genomföra uppdraget på ett tillfredsställande sätt.

I personuppgiftslagen föreskrivs att ombudet ska samråda med tillsynsmyndigheten vid tveksamheter. I dataskyddsförordningen föreskrivs i stället att ombudet ska samråda och samarbeta med tillsynsmyndigheten och vara dess kontaktpunkt. Detta innebär eventuellt att ombudets arbetsuppgifter utökas något genom dataskyddsförordningen. Enligt vår uppfattning lär det utökade ansvaret i sådant fall i huvudsak aktualiseras om Datainspektionen söker kontakt med antingen ombudet eller den personuppgiftsansvarige.

Av personuppgiftslagen framgår att personuppgiftsombudet självständigt ska utföra sina uppgifter. Dataskyddsförordningen är mycket mer detaljerad i denna del, främst vad gäller den personuppgiftsansvariges skyldigheter gentemot ombudet. Den personuppgiftsansvarige ska t.ex. se till att ombudet får tillräckliga resurser och inte tar emot instruktioner samt se till att det inte uppstår intressekonflikter med andra uppdrag. Som vi ser det förtydligar dataskyddsförordningens bestämmelser i denna del att det är den personuppgiftsansvarige som ska se till att ombudets självständighet upprätthålls. Vidare specificeras vad som utmärker ett självständigt ombud. Många av de krav som ställs på den personuppgiftsansvarige i denna del ter sig enligt vår mening dock som relativt självklara åtgärder för att upprätthålla ombudets självständighet.

Vissa av de uppgifter som personuppgiftsombudet haft enligt personuppgiftslagen försvinner när dataskyddsförordningen börjar tillämpas. Dataskyddsbudet kommer inte att ha skyldighet att göra en anmälan till tillsynsmyndigheten vid misstanke om att den personuppgiftsansvarige bryter mot dataskyddsbestämmelserna. Inte heller kommer ombudet längre att vara skyldigt att föra en förteckning över vissa av den personuppgiftsansvariges behandlingar. Denna skyldighet kommer i stället att, enligt

artikel 30 i dataskyddsförordningen, ligga på den personuppgiftsansvarige.

Slutligen beskrivs dataskyddsbudets skyldighet gentemot de registrerade på ett något annorlunda sätt i dataskyddsförordningen. Enligt personuppgiftslagen ska ombudet hjälpa de registrerade att få rättelse. Enligt dataskyddsförordningen (artikel 38.4) ”får den registrerade kontakta dataskyddsbudet” när det gäller frågor kring behandling av dennes personuppgifter eller rörande dennes rättigheter. Ordvalet gör att det kan diskuteras om dataskyddsbudets skyldigheter att vara de registrerade behjälpliga är lika långtgående som tidigare.

Mot denna bakgrund gör vi bedömningen att dataskyddsbudets uppgifter enligt dataskyddsförordningen främst innebär ett uppdrag som ”internrevisor” för den personuppgiftsansvariges behandlingar. Beroende på hur uppdraget har utförts tidigare kan det te sig något utökat jämfört med vad som i dag gäller för personuppgiftsbud. Enligt vår bedömning bör det emellertid inte röra sig om några omfattande förändringar i ombudets uppgifter. Det som främst kommer att orsaka merarbete jämfört med i dag är troligtvis i stället det faktum att det införs helt ny och relativt komplicerad lagstiftning på området. Detta, tillsammans med det nya regelverkets komplexitet, talar enligt vår mening dock snarare för att ombudets ”tillsynsområde” ska omfatta domstolarnas hela kärnverksamhet, eftersom intern sakkunskap inom rättsområdet hjälper till att upprätthålla skyddet för de registrerades integritet.

13.5.3 Dataskyddsbud även för den dömande verksamheten

Det bör i detta sammanhang återigen uppmärksammas att dataskyddsförordningen inte ger något klart besked om vad som innefattas i domstolarnas dömande verksamhet. Vår bedömning av begreppet är att den dömande verksamheten sannolikt innefattar all den personuppgiftsbehandling som utförs i det enskilda målet eller ärendet från att detta anhängiggörs vid domstolen tills ett slutligt avgörande har meddelats (se avsnitt 8.4).

Eftersom begreppet saknar en klar definition är det för närvarande oklart vilka personuppgiftsbehandlingar som omfattas

av domstolarnas dömande verksamhet och därmed träffas av undantaget att utse dataskyddsbud. Detta innebär enligt vår mening att det finns en risk med att i domstolsdatalagen föreskriva att domstolarna inte behöver utnämna dataskyddsbud för denna verksamhet.

Skulle skyldigheten att utse dataskyddsbud även för den dömande verksamheten kvarstå försvinner gränsdragningsproblemet vad gäller inom vilken verksamhet ombudet ska verka. Dock uppstår ett annat gränsdragningsproblem som dataskyddsbudet kan komma att behöva ta ställning till. Ombudet ska, enligt artikel 39.1 d och e i dataskyddsförordningen, samarbeta och samråda med tillsynsmyndigheten och fungera som dess kontaktpunkt. Eftersom tillsynsmyndigheten inte har behörighet att utöva tillsyn över den dömande verksamheten (artikel 55.3) kan ombudet enligt vår mening inte heller förväntas samråda m.m. med tillsynsmyndigheten i frågor som gäller denna verksamhet. Att denna gränsdragningsläggs på dataskyddsbudet är enligt vår mening inte helt tillfredsställande. Detta är dock ett resultat av den oklarhet som finns i det aktuella regelverket. Med denna oklarhet följer att det är svårt att komma ifrån att det någonstans uppstår ett gränsdragningsproblem.

Vår bedömning av begreppet dömande verksamhet innebär att större delen av domstolarnas kärnverksamhet kommer att vara undantagen från Datainspektionens tillsyn. Mot just den bakgrunden anser vi att det ur ett integritetsperspektiv finns ett än större behov av att domstolarna biträds av en person som har kunskap kring dataskyddsbestämmelserna.

Vi kan vidare konstatera att bland de domstolar som svarat på den förfrågan som Domstolsverket gjort för vår räkning, är fördelningen relativt jämn mellan de som önskar att dataskyddsbudet ansvarsområde även i framtiden ska omfatta den dömande verksamheten och de som önskar att undantag införs för denna verksamhet. Det som kommit fram i svaren från domstolarna ger inte heller någon entydig bild av hur betungande den nuvarande uppgiften som personuppgiftsbud är på en domstol. Någon domstol har uppgett att arbetsuppgiften tar mycket tid i anspråk, medan en annan har uppgett att åtminstone kontakten med allmänheten för närvarande är mycket sparsam i detta avseende.

Det tyngsta skälet mot dataskyddsbud i den dömande verksamheten är enligt vår mening frågan om domarnas självständighet. Samtliga domare använder emellertid samma verksamhetssystem, med de möjligheter och begränsningar som det innebär. Vi anser inte att domarnas självständighet begränsas av att domstolarna utarbetar riktlinjer för hur personuppgifter bör hanteras i detta verksamhetssystem, och då även i den dömande verksamheten. Även om Domstolsverket har en väsentlig roll i detta arbete kan enligt vår mening ett dataskyddsbud vara den enskilda domstolen behjälplig för att förverkliga de riktlinjer som utarbetats. Ombudet kan också vara ett stöd lokalt för medarbetarna – även domarna – när det gäller personuppgiftsbehandling. Det är naturligtvis en känslig arbetsuppgift att som dataskyddsbud ”utöva tillsyn” över domarnas – eventuellt domarkollegors – hantering av personuppgifter. Som dataskyddsbudets uppgifter beskrivs i dataskyddsförordningen bedömer vi dock att ombudets roll gentemot den personuppgiftsansvarige och dess medarbetare inte är annat än rådgivande. Det anges förvisso att ombudet ska *övervaka* hur dataskyddsbestämmelserna och den interna strategin för personuppgiftsbehandling följs. Någon sanktionsmöjlighet har dataskyddsbudet emellertid inte. Det kommer inte heller att finnas någon anmälningsskyldighet till tillsynsmyndigheten vid misstänka överträdelser. Tillsynsmyndigheten kommer för övrigt inte heller att vara behörig att utöva tillsyn över den dömande verksamheten, vilket enligt vår uppfattning undantar domarnas alla grundläggande arbetsuppgifter. Det slutliga ansvaret för att personuppgifter behandlas i enlighet med dataskyddsförordningen åligger således, även med ett dataskyddsbud för den dömande verksamheten, den personuppgiftsansvariga domstolen eller den ansvarige domaren.

Även om risken för överträdelser i domstolarnas personuppgiftsbehandling är liten, anser vi vidare att dataskyddsbudet kan sätta fokus på personuppgiftsfrågor inom den egna domstolen. Sakkunskap om regelverket kring personuppgiftsbehandling kan naturligtvis upprätthållas även utan ett dataskyddsbud. Fördelen med att göra det obligatoriskt att utse dataskyddsbud för samtliga verksamheter är dock att det skapas en lagstadgad skyldighet för domstolarna att se till att det finns kunskap om detta relativt svårtillgängliga rättsområde på den enskilda

domstolen. Risken för överträdelser bör med detta bli än mindre, vilket förstärker skyddet för de enskildas integritet.

En stor del av de personuppgifter som domstolarna behandlar är också av känslig karaktär. För det fall dataskyddsbudets ansvar omfattar även den dömande verksamheten sänder detta signaler till allmänheten om att domstolarna har en medvetenhet kring dessa personuppgifters skyddsvärde.

Sammantaget anser vi att skälen för att låta dataskyddsbudets arbetsuppgifter omfatta även den dömande verksamheten överväger de som talar mot. Genom att låta ombudet vara behjälpligt även i denna verksamhet undviks större delen av det problem som uppstår på grund av att det inte är klart vilken del av den rättskipande och rättsvårdande verksamheten som utgör dömande verksamhet. Samtidigt bibehålls en naturlig kunskapskälla gällande detta komplexa regelverk lokalt på domstolarna, vilket leder till att skyddet för de enskildas integritet stärks. Mot den bakgrunden föreslår vi att domstolsdatalagens bestämmelse i nuvarande 10 § första stycket, som reglerar att den personuppgiftsansvariga domstolen ska utse ett eller flera personuppgiftsbud, ska finnas kvar. Dock bör ordet personuppgiftsbud ersättas med ordet dataskyddsbud för att anpassa domstolsdatalagen till dataskyddsförordningens begreppsbildning.

För att tydliggöra att det dataskyddsbud som ska utses enligt domstolsdatalagen har samma uppdrag som enligt dataskyddsförordningen skulle man kunna tänka sig att förena domstolsdatalagens bestämmelse om dataskyddsbud med en hänvisning till förordningen. Enligt vårt förslag ska det emellertid framgå av domstolsdatalagen att lagen innehåller kompletterande bestämmelser till dataskyddsförordningen. Det framgår enligt vår mening därmed tillräckligt klart att domstolarnas dataskyddsbud omfattas av artikel 37–39 i dataskyddsförordningen vad gäller bl.a. kvalifikationer, självständighet och arbetsuppgifter. Ett undantag är dock, som vi ovan nämnt, samråd m.m. med tillsynsmyndigheten vad gäller den dömande verksamheten.

Eftersom dataskyddsbudets uppdrag ska ha samma innehåll som enligt dataskyddsförordningen omfattas även möjligheten i artikel 37.3 att utnämna ett gemensamt dataskyddsbud för flera myndigheter. Detta skulle kunna vara en lösning för de mindre domstolar som anser att uppdraget blir betungande för den som

utes eller som har svårigheter att finna den rätta kompetensen för uppdraget. Ett sådant beslut måste dock enligt vår mening föregås av en lämplighetsbedömning utifrån organisationsstruktur och domstolarnas storlek. Att göra en sådan bedömning ligger inte inom vårt uppdrag. Vi vill dock påminna om att för det fall dataskyddsbudet inte är anställt inom den egna myndigheten måste ett tjänsteavtal tecknas med ombudet (se artikel 37.6 i dataskyddsförordningen).

13.5.4 Tystnadsplikt för dataskyddsbudet

I dataskyddsförordningen förutsätts enligt vår mening att dataskyddsbudet är en fysisk person (jfr artikel 37.6 och skäl 97). Om uppdraget även fortsättningsvis utförs av en anställd vid den personuppgiftsansvariga domstolen kommer ombudet att omfattas av den tystnadsplikt som gäller för domstolens anställda enligt offentlighets- och sekretesslagen.

Det finns emellertid inte något som hindrar att en domstol anlitar en utomstående för uppdraget. Vi delar Dataskyddsutredningens bedömning att ett sådant dataskyddsbud får anses delta i domstolens verksamhet på sådant sätt som avses i 2 kap. 1 § OSL och att ombudet därmed omfattas av den sekretess som gäller för personal vid domstolen.² En förutsättning för detta torde dock vara att dataskyddsbudet är en särskilt förordnad och utpekad person, som med stöd av ett tjänsteavtal utför uppdraget. Vi anser att man bör kunna förutsätta att en domstol som anlitar en utomstående som dataskyddsbud uppfyller dessa krav. Mot den bakgrunden anser vi att det inte finns någon anledning att i domstolsdatalagen införa en hänvisning till regleringen om tystnadsplikt för dataskyddsbud i den föreslagna 1 kap. 6 § dataskyddslagen.

13.5.5 Anmälan till tillsynsmyndigheten

Det faktum att samtliga dataskyddsförordningens bestämmelser om dataskyddsbud är tillämpliga för det ombud som utses enligt

² Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 262).

domstolsdatalagen, innebär att vissa bestämmelser i domstolsdatalagen bör upphävas.

Enligt nuvarande 10 § andra stycket domstolsdatalagen ska den personuppgiftsansvarige anmäla till tillsynsmyndigheten när ett personuppgiftsombud utses eller entledigas. Den personuppgiftsansvariges anmälningsskyldighet framgår dock redan av artikel 37.7 i dataskyddsförordningen. Bestämmelsen i domstolsdatalagen bör därför upphävas.

Som vi konstaterat i avsnitt 10.1 måste vidare hänvisningen i 5 § 9 domstolsdatalagen till 38 och 40 §§ PuL om personuppgiftsombud utgå. Bestämmelser om dataskyddsombudets uppgifter finns i artikel 38.4 och artikel 39 i dataskyddsförordningen. Som vi tidigare konstaterat anser vi att det inte bör införas några hänvisningar till enskilda bestämmelser i dataskyddsförordningen i domstolsdatalagen (avsnitt 10.2).

13.5.6 Skyldighet att föra förteckning

Enligt 11 § första stycket domstolsdatalagen ska den som är personuppgiftsombud föra en förteckning över de behandlingar som utförs med stöd av lagen. Av andra stycket framgår att regeringen eller den myndighet som regeringen bestämmer, med stöd av 8 kap. 7 § regeringsformen kan meddela närmare föreskrifter om vilka uppgifter en sådan förteckning ska innehålla.

Enligt personuppgiftslagen är den personuppgiftsansvarige i första hand skyldig att anmäla till tillsynsmyndigheten vilka behandlingar som kommer att utföras. Undantag görs dock om det finns ett personuppgiftsombud som för en förteckning över behandlingarna. Dataskyddsförordningens bestämmelser ser något annorlunda ut. Det finns inte längre någon anmälningsskyldighet för personuppgiftsbehandlingar. De uppgifter som åläggs dataskyddsombudet enligt förordningen innefattar inte heller förandet av någon förteckning. I stället har den personuppgiftsansvarige (och i tillämpliga fall personuppgiftsbiträdet), genom artikel 30 i förordningen ålagts en skyldighet att föra ett register över den personuppgiftsbehandling som utförts under dess ansvar. Vilka uppgifter som ska ingå i registret är relativt utförligt reglerat genom denna bestämmelse (30.1 a–g). Registret ska på begäran

göras tillgängligt för tillsynsmyndigheten (30.4). Mot bakgrund av att tillsynsmyndigheten inte är behörig att utöva tillsyn över den personuppgiftsbehandling som sker i domstolarnas dömande verksamhet (artikel 55.3) kan man enligt vår mening ifrågasätta om tillsynsmyndigheten har behörighet att begära ut domstolarnas register vad gäller den verksamheten.

Ansvaret för att föra en förteckning över personuppgiftsbehandlingar har i dataskyddsförordningen således flyttats över från personuppgiftsombudet till den personuppgiftsansvarige. Att det är den personuppgiftsansvarige som bär ansvaret för att det förs en förteckning som uppfyller dataskyddsförordningens krav medför, enligt vår mening, att en bestämmelse som ålägger dataskyddsbudet en sådan skyldighet blir missvisande. Mot den bakgrunden anser vi att bestämmelsen i 11 § domstolsdatalagen bör upphävas i sin helhet. En följd av detta blir att även Domstolsverkets föreskriftsrätt på området i nuvarande 14 § andra stycket 1 domstolsdataförordningen måste upphävas.

14 Upplysningar till allmänheten

Förslag: Bestämmelsen om skyldighet för den personuppgifts-ansvariga domstolen att till var och en som begär det lämna upplysningar om de behandlingar som utförs med stöd av domstolsdatalagen ska upphävas. Detsamma gäller bestämmelsen om rätten att överklaga domstols beslut om att lämna sådana upplysningar.

Av 12 § domstolsdatalagen framgår att den personuppgifts-ansvarige skyndsamt och på lämpligt sätt ska lämna upplysningar om de behandlingar som utförs med stöd av denna lag till var och en som begär det. Upplysningarna ska omfatta de uppgifter som en förteckning enligt 11 § samma lag ska innehålla. Den personuppgiftsansvarige är dock inte skyldig att lämna ut sekretessbelagda uppgifter eller uppgifter om vilka säkerhetsåtgärder som har vidtagits.

Bestämmelsen i 12 § domstolsdatalagen infördes för att skapa en skyldighet för domstolarna motsvarande den som gäller enligt 42 § PuL. Syftet var att underlätta för allmänheten att få kunskap om vilka behandlingar som utförs av en domstol.¹

Den personuppgiftsansvarige ska enligt artikel 30 i dataskyddsförordningen föra ett register över den personuppgiftsbehandling som utförts under dennes ansvar. Vi har mot den bakgrunden föreslagit att nuvarande 11 § domstolsdatalagen – som reglerar personuppgiftsombudets skyldighet att föra en förteckning över personuppgiftsbehandlingar – ska upphävas (se avsnitt 13.5.6).

Det finns ingen motsvarighet till 42 § PuL i dataskyddsförordningen. Eftersom information till allmänheten om de

¹ Se förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 86).

behandlingar som utförs bidrar till att skydda de registrerades integritet, anser vi i och för sig att dataskyddsförordningen inte hindrar att regleringen i nuvarande 12 § domstolsdatalagen kvarstår (jfr avsnitt 5.3).

Enligt vår bedömning måste dock ett register som en personuppgiftsansvarig domstol för i enlighet med artikel 30 i dataskyddsförordningen anses vara upprättat i enlighet med 2 kap. 7 § TF; antingen som en färdigställd administrativ handling enligt första stycket eller som ett register enligt andra stycket 1. Allmänheten kommer därmed ha rätt att få ut dess offentliga innehåll med stöd av tryckfrihetsförordningen. Ett beslut om att avslå en sådan begäran kan överklagas i enlighet med 6 kap. 7–9 §§ OSL.

Beroende på registrets omfattning kan en avgift komma att tas ut när det begärs ut med stöd av tryckfrihetsförordningen. Även med beaktande av detta anser vi att regleringen om upplysningar till allmänheten i 12 § domstolsdatalagen är överflödigt och bör utgå. Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) inte föreslagit att någon motsvarande bestämmelse ska finnas i dataskyddslagen. Vi kan inte se någon anledning till att domstolarna i detta avseende skulle ha en längre gående skyldighet än övriga myndigheter. Som en följd av att rätten till upplysningar enligt 12 § utgår måste även rätten att, enligt 20 § domstolsdatalagen, överklaga en domstols beslut om sådana upplysningar utgå.

15 Den registrerades rättigheter

15.1 Inledande kommentar

Domstolsdatalagen innehåller inga egna bestämmelser om de registrerades rättigheter. I stället hänvisas i 5 § första stycket 5, 6 och 11 domstolsdatalagen till 23, 25–28 och 48 §§ PuL. Dessa bestämmelser reglerar den registrerades rätt till information, rättelse, blockering och utplåning av personuppgifter samt den registrerades rätt till skadestånd. När dataskyddsförordningen börjar tillämpas kommer personuppgiftslagen att upphävas.¹ Samtliga hänvisningar till personuppgiftslagen måste därmed utgå.

Dataskyddsförordningens bestämmelser om de registrerades rättigheter finns i artiklarna 12–22 och artikel 34. Artikel 12 innehåller övergripande bestämmelser om bl.a. hur och i vilken form information ska lämnas till de registrerade samt tidsfristerna för detta. I artiklarna 13–22 och artikel 34 regleras därefter de registrerades rättigheter relativt detaljerat.

Inledningsvis kan vi konstatera att artikel 20, som gäller rätten till dataportabilitet, inte är tillämplig på personuppgiftsbehandling i domstolarnas rättskipande och rättsvårdande verksamhet, eftersom domstolarnas behandling i denna del inte grundar sig på samtycke eller avtal (se artikel 20.1 a). I artikel 22 i dataskyddsförordningen finns vidare bestämmelser om vad som gäller för automatiserade beslut. Inte heller denna bestämmelse är enligt vår mening relevant att kommentera i vår promemoria, eftersom några sådana beslut för närvarande inte förekommer i domstolarnas rättskipande och rättsvårdande verksamhet.

Vad gäller de registrerades resterande rättigheter enligt dataskyddsförordningen är vår avsikt inte att i detta kapitel göra en

¹ Se kommittédirektiv till Dataskyddsutredningen (Dir 2016:15 s. 6).

heltäckande genomgång. Vårt syfte är i stället att lyfta fram de viktigaste förändringarna för domstolarna.

Det är enligt vår mening vidare av största vikt att domstolarnas handläggning av mål och ärenden inte avstannar. För att denna handläggning ska kunna fortgå måste personuppgifter kunna behandlas utan avbrott i den rättskipande och rättsvårdande verksamheten. Detta gäller inte enbart parternas personuppgifter, utan även de personuppgifter som rör ombud, vittnen, tolkar och andra aktörer. Det är också av stor vikt att de personuppgifter som ingår i processmaterialet kan arkiveras när målet eller ärendet är avgjort. Mot den bakgrunden har vi även för avsikt att i detta kapitel analysera dataskyddsförordningens möjligheter att begränsa de registrerades rättigheter och bedöma behovet av att införa sådana begränsningar.

15.2 En generell möjlighet till undantag

De rättigheter som regleras i artiklarna 13–22 och artikel 34 i dataskyddsförordningen innehåller i vissa fall undantag som endast gäller för den enskilda rättigheten. Dessa redogör vi för i kommande avsnitt. I artikel 23 i dataskyddsförordningen finns emellertid även en generell bestämmelse som ger medlemsstaterna vissa möjligheter att i den nationella lagstiftningen införa undantag från rättigheterna i artiklarna 12–22 samt artikel 34 i förordningen. En sådan begränsning måste ske med respekt för andemeningen i de grundläggande rättigheterna och friheterna. Den måste också utgöra en nödvändig och proportionell åtgärd i ett demokratiskt samhälle. Begränsningen får vidare endast ske i syfte att säkerställa vissa intressen, som räknas upp i artikel 23.1 a–j. För den del av domstolarnas verksamhet som inte består av lagföring m.m. av brott eller verkställighet av straffrättsliga sanktioner, är det enligt vår mening leden e och f som främst kommer i fråga. Enligt led e får en begränsning av de registrerades rättigheter ske i syfte att säkerställa ”en medlemsstats viktiga mål av generellt allmänt intresse”. Som exempel på sådana mål nämns viktiga ekonomiska eller finansiella intressen, där penning-, budget- eller skattefrågor ingår, men även folkhälsa och social trygghet. Enligt led f får en

begränsning av de registrerades rättigheter också ske i syfte att säkerställa rättsväsendets oberoende eller rättsliga åtgärder.

De undantag som införs i nationell rätt med stöd av artikel 23.1 i dataskyddsförordningen ska vidare, enligt artikel 23.2, när det är relevant innehålla specifika bestämmelser om bl.a. ändamålen med behandlingen, omfattningen av de införda begränsningarna, skyddsåtgärder för att förhindra missbruk, specificering av den personuppgiftsansvarige, lagringstid och tillämpliga skyddsåtgärder. Detta är bestämmelser som enligt vår bedömning ofta återfinns i svenska registerförfattningar. Som exempel nämns också bestämmelser om de registrerades rätt att bli informerade om begränsningen, såvida detta inte inverkar menligt på begränsningen.

15.3 Information när personuppgifter samlas in från den registrerade

15.3.1 Domstolsdatalagen

Domstolsdatalagen hänvisar, genom 5 § 5, till 23, 25 och 27 §§ PuL. Enligt 23 § PuL ska den personuppgiftsansvarige självant lämna den registrerade information om behandlingen av personuppgifter när dessa samlas in från den registrerade själv. Informationen ska lämnas i samband med att uppgifterna samlas in.

I 25 § PuL regleras mer detaljerat vilken information som ska lämnas till den registrerade i en sådan situation. Informationen ska omfatta uppgift om den personuppgiftsansvariges identitet, om ändamålen med behandlingen och all övrig information som behövs för att den registrerade ska kunna ta till vara sina rättigheter i samband med behandlingen. Som exempel på sådan övrig information nämns mottagarna av uppgifterna, skyldigheten att lämna uppgifter och rätten att ansöka om information och få rättelse. Information behöver dock inte lämnas om sådant som den registrerade redan känner till.

Den personuppgiftsansvariges informationsplikt begränsas dock av 27 § PuL. Här stadgas att bestämmelserna i 23 och 25 §§ PuL inte gäller om det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den registrerade.

Beträffande uttrycket *insamling av personuppgifter* konstaterade regeringen i förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 39) att detta inte bara avser situationer där uppgifter lämnas till en domstol på begäran av domstolen, utan även andra tillvägagångssätt genom vilka domstolen får del av personuppgifter. Som exempel nämns när en åklagare skickar in en stämningsansökan eller att en enskild lämnar in ett överklagande.

Regeringen har vidare gjort bedömningen att de registrerade som skickar in uppgifter till domstolarna (exempelvis parterna) i de flesta fall torde känna till vilka uppgifter som kommer att behandlas vid domstolarna eftersom detta framgår direkt av domstolsdatalagen, av den förteckning över personuppgiftsbehandlingar som domstolarna är skyldiga att sammanställa och av de processuella regelverk som styr domstolarnas verksamhet. Regeringen menade att domstolarna därför i praktiken sällan torde behöva lämna särskild information till den registrerade även om 23 och 25 §§ PuL görs tillämpliga för domstolarna.²

15.3.2 Dataskyddsförordningen och dataskyddslagen

Enligt artikel 13 i dataskyddsförordningen har en registrerad rätt att få relativt utförlig information från den personuppgiftsansvarige när personuppgifterna samlats in från den registrerade själv. Informationen ska bl.a. innefatta den personuppgiftsansvariges identitet och kontaktuppgifter, kontaktuppgifter till dataskyddsombudet, uppgift om den period under vilken personuppgifterna kommer att lagras eller de kriterier som används för att fastställa denna period, information om rätten att ge in klagomål till tillsynsmyndigheten och om rätten att begära rättelse, radering eller begränsning av behandling av personuppgifterna. Informationen ska lämnas när den personuppgiftsansvarige får personuppgifterna. Den personuppgiftsansvarige behöver dock inte lämna sådan information som den registrerade redan förfogar över.

Enligt Dataskyddsutredningens bestänkande (SOU 2017:39) ska dataskyddslagen i 5 kap. 1 § innehålla en bestämmelse enligt vilken den registrerades rätt till information och tillgång till

² Se förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 86 f.).

personuppgifter enligt artiklarna 13–15 i dataskyddsförordningen inte gäller sådana uppgifter som den personuppgiftsansvarige, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämna ut till den registrerade. Förslaget innebär att det undantag för vissa sekretessbelagda uppgifter som nu finns i 27 § PuL kommer att finnas kvar även när dataskyddsförordningen börjar tillämpas.

15.3.3 Bedömning

Förslag: Den registrerades rätt till information enligt artikel 13 i dataskyddsförordningen ska inte gälla sådana 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. Regleringen ska genomföras genom en hänvisning till den föreslagna 5 kap. 1 § första stycket dataskyddslagen.

Artikel 13 i dataskyddsförordningen reglerar vilka uppgifter den personuppgiftsansvarige ska lämna till en registrerad när uppgifter samlats in från den registrerade själv. Exempel på situationer där domstolarna samlar in personuppgifter från den enskilde själv är när domstolen tar emot ansökningar, partsinlagor och svar på förelägganden. I de allmänna förvaltningsdomstolarna förekommer också att enskilda lämnar in överklaganden direkt till domstolen, t.ex. i laglighetsprövningsmål. Även om uppgifterna kommer från en ställföreträdare eller ett ombud som har i uppdrag att företräda den registrerade bör uppgifterna i dessa situationer bedömas ha samlats in från den registrerade själv.³

Artikel 13 i dataskyddsförordningen liknar till sin uppbyggnad 23 och 25 §§ PuL. En avgörande skillnad mellan dataskyddsförordningens och personuppgiftslagens reglering är att förordningen är mycket mer utförlig när det gäller vilken information som ska lämnas till den registrerade. Precis som enligt personuppgiftslagen görs dock undantag från den person-

³ Sören Öman och Hans-Olof Lindblom, Personuppgiftslagen (15 september 2016, Zetco), kommentar till 23 §.

uppgiftsansvariges informationsskyldighet om den registrerade redan förfogar över den information som ska lämnas.

Vi anser att den registrerade möjligtvis kan anses ha kännedom om vem som är personuppgiftsansvarig och om de ändamål som uppgifterna ska behandlas för, eftersom detta framgår av domstolsdatalagen. Ändamålet framgår enligt vår mening även till viss del av sammanhanget – om uppgifterna samlas in i ett enskilt mål eller ärende är det underförstått att uppgifterna används för handläggning av detsamma. Däremot anser vi inte att den registrerade kan anses känna till exempelvis vem som är domstolens dataskyddsombud eller kriterierna för att fastställa under vilken period uppgifterna kommer att lagras. Även om den registrerades rätt att begära rättelse och radering m.m. framgår av dataskyddsförordningen kan den enskilde enligt vår mening inte heller anses förfoga över denna information. Om tanken vore att bestämmelserna skulle tolkas på detta vis hade någon skyldighet för den personuppgiftsansvarige att lämna information om dessa rättigheter rimligen inte förts in i dataskyddsförordningen.

När domstolarna samlar in personuppgifter från den registrerade själv kan han eller hon enligt vår uppfattning således inte anses förfoga över all den information som ska lämnas enligt artikel 13 i dataskyddsförordningen. Beroende på vilken information som lämnas till de registrerade i nuläget skulle det därmed kunna finnas anledning för domstolarna att se över sina rutiner i denna del. Detta är emellertid ett arbete som sker på verkställighetsnivå och som inte ligger inom ramen för vårt uppdrag att behandla.

Ytterligare en fråga som domstolarna kan komma att behöva ta ställning till i verkställighetsstadiet är i vilka situationer information ska lämnas till den registrerade om rätten att lämna in klagomål till tillsynsmyndigheten. Tillsynsmyndigheten är enligt artikel 55.3 i dataskyddsförordningen inte behörig att utöva tillsyn över domstolar som behandlar personuppgifter i sin dömande verksamhet. Det är dock för närvarande oklart vilken verksamhet som innefattas i denna dömande verksamhet. Vår bedömning av begreppet är att den dömande verksamheten sannolikt innefattar all den personuppgiftsbehandling som sker i det enskilda målet eller ärendet från att detta anhängiggörs vid domstolen tills ett slutligt avgörande har meddelats. Utifrån den bedömningen skulle

domstolarna relativt sällan behöva lämna information om klagorätten till de registrerade. Frågan om vad som innefattas i begreppet dömande verksamhet får dock slutligen avgöras av EU-rättslig praxis (se avsnitt 8.4).

Dataskyddsförordningens bestämmelser skulle enligt vår bedömning sammanfattningsvis kunna innebära att domstolarna behöver utöka den information som ges till de registrerade när personuppgifter samlas in från dem. Endast en ökad administrativ belastning innebär enligt vår mening emellertid inte att det finns möjlighet att begränsa de registrerades rättigheter med stöd av artikel 23 i dataskyddsförordningen. Anledningen är att begränsningen i sådant fall inte görs i syfte att säkerställa viktiga mål av generellt allmänt intresse, rättsväsendets oberoende eller rättsliga åtgärder eller något annat av de syften som räknas upp i artikel 23.1 a–j. Någon annan möjlighet till en generell begränsning finns inte.

En hänvisning bör enligt vår mening dock göras i domstolsdatalagen till den föreslagna 5 kap. 1 § dataskyddslagen, som innebär att den rätt till information som den registrerade har enligt bl.a. artikel 13 i dataskyddsförordningen inte gäller uppgifter som, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämnas ut till den registrerade. På detta sätt upprätthålls det förhållande som nu gäller, nämligen att bestämmelser om sekretess eller tystnadsplikt går före den registrerades rätt att få information om behandlingen av hans eller hennes personuppgifter.

15.4 Information när personuppgifter samlas in från någon annan än den registrerade

15.4.1 Domstolsdatalagen

Enligt 24 § första stycket PuL ska den personuppgiftsansvarige självant lämna den registrerade information om behandlingen av personuppgifter när uppgifterna samlats in från någon annan källa än den registrerade själv. Enligt 24 § andra stycket behöver information till den registrerade emellertid inte lämnas om det finns bestämmelser om registrerandet eller utlämnandet av personuppgifterna i lag eller annan författning.

I förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 87) gjorde regeringen bedömningen att någon hänvisning till 24 § PuL inte behöver tas in i domstolsdatalagen. Som skäl för detta framfördes att det kommer att finnas bestämmelser om registrerandet eller utlämnandet av personuppgifterna i domstolsdatalagen, rättegångsbalken, förvaltningsprocesslagen och övrig lagstiftning som styr domstolarnas verksamhet.

15.4.2 Dataskyddsförordningen

Enligt artikel 14 i dataskyddsförordningen ska relativt utförlig information lämnas till den registrerade när den personuppgiftsansvarige har fått personuppgifterna från någon annan källa än den registrerade själv. Artikel 14.5 c innehåller dock – liksom 24 § PuL – undantag som innebär att den personuppgiftsansvarige inte behöver lämna sådan information, om den personuppgiftsansvarige har rätt att ta emot eller lämna ut uppgifterna enligt medlemsstatens nationella rätt. En förutsättning för att undantaget ska vara tillämpligt är att den nationella rätten fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen. Någon ledning gällande vilken typ av skyddsåtgärder det kan röra sig om finns inte i skälen till förordningen.

15.4.3 Bedömning

Bedömning: Domstolarnas personuppgiftsbehandling i den rättskipande och rättsvårdande verksamheten omfattas av undantaget i artikel 14.5 c i dataskyddsförordningen från skyldigheten att lämna information när personuppgifter har getts in från någon annan än den registrerade själv.

Artikel 14 i dataskyddsförordningen reglerar vilken information som ska lämnas till den registrerade när personuppgifter samlats in från annan än den registrerade själv. För domstolarnas verksamhet är exempel på sådana situationer när den registrerades överklagande kommer in till domstolen från beslutande myndighet eller när överordnad domstol får in den registrerades överklagande från

underinstansen. Andra exempel är yttranden som kommer in från den registrerades motpart och sakkunnig- eller vittnesförhör.

Vi anser emellertid att domstolarnas rättskipande och rättsvårdande verksamhet omfattas av undantaget i artikel 14.5 c i dataskyddsförordningen, vilket innebär att domstolarna inte är skyldiga att lämna information till de registrerade i dessa situationer. Skälen för detta är följande.

Som det konstaterades i förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 87) styrs domstolarnas rätt att i den rättskipande och rättsvårdande verksamheten ta emot respektive lämna ut personuppgifter av bl.a. de processuella regelverken. Även utlämnandet av allmänna handlingar, där personuppgifter naturligtvis kan ingå, regleras av svensk lag. Det finns därmed nationella författningar som reglerar domstolarnas rätt att ta emot eller lämna ut de personuppgifter som behandlas inom domstolsdatalagens tillämpningsområde.

Det får enligt vår mening vidare förutsättas att de personuppgifter som faktiskt behandlas av domstolarna är sådana som domstolen enligt bestämmelser i exempelvis rättegångsbalken, förvaltningsprocesslagen (1971:291), ärendelagen (1996:242) och lagen (1973:188) om arrendenämnder och hyresnämnder får behandla. Det i sig innebär enligt vår mening ett skydd för de registrerades intressen. Domstolsdatalagen innehåller också en mängd bestämmelser som skyddar den registrerades integritet när domstolen behandlar personuppgifter. Som exempel kan nämnas bestämmelser om sökbegränsningar, elektroniskt utlämnande av personuppgifter och tjänstemäns tillgång till personuppgifter. Även förekomsten av ett dataskyddsombud skyddar den registrerades integritet. Enligt vår bedömning finns det därför i nationell rätt ett tillräckligt skydd för den registrerades intressen för att undantaget i artikel 14.5 c i dataskyddsförordningen ska kunna tillämpas av domstolarna. Det behövs enligt vår mening därmed inte någon ytterligare lagstiftningsåtgärd för att domstolarna ska kunna tillämpa undantaget.

15.5 Information efter begäran

15.5.1 Domstolsdatalagen

Domstolsdatalagen hänvisar, genom 5 § första stycket 5, till 26 och 27 §§ PuL. Enligt 26 § första stycket PuL är den personuppgiftsansvarige skyldig att, efter begäran, en gång per kalenderår lämna besked om huruvida personuppgifter som rör den sökande behandlas eller inte (ett s.k. registerutdrag). Om sådana uppgifter behandlas ska den registrerade också få information om vilka uppgifter som behandlas, varifrån de har hämtats, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut.

Enligt 26 § tredje stycket PuL behöver sådan information inte lämnas vad gäller personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. Undantaget gäller dock inte om uppgifterna har lämnats ut till tredje man eller om uppgifterna behandlas enbart för historiska, statistiska eller vetenskapliga ändamål. Inte heller gäller undantaget för löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats under längre tid än ett år.

Den personuppgiftsansvariges informationsplikt begränsas också av 27 § PuL. Enligt denna bestämmelse gäller inte skyldigheten i 26 § PuL om det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den registrerade.

15.5.2 Dataskyddsförordningen och dataskyddslagen

Enligt artikel 15 i dataskyddsförordningen har den registrerade rätt att av den personuppgiftsansvarige få bekräftelse på om personuppgifter som rör honom eller henne håller på att behandlas. Om så är fallet har den registrerade rätt till relativt utförlig information om behandlingen av dessa personuppgifter. Information ska bl.a. lämnas om ändamålen med behandlingen, vilka kategorier av uppgifter som behandlas, mottagarna av uppgifterna, den period under vilken uppgifterna kommer att lagras eller kriterierna för att

fastställa denna period, rätten att begära rättelse eller radering av uppgifterna samt rätten att ge in klagomål till en tillsynsmyndighet. Några undantag från rätten att få information om personuppgiftsbehandlingen efter begäran finns inte i artikel 15.

Av artikel 12.5 framgår att utgångspunkten är att information enligt bl.a. artikel 15 ska tillhandahållas kostnadsfritt. Det framgår dock även att om begäran är uppenbart ogrundad eller orimlig, särskilt på grund av deras repetitiva art, får den personuppgiftsansvarige antingen ta ut en rimlig avgift eller vägra att tillmötesgå begäran. Det är den personuppgiftsansvarige som ska visa att en begäran är uppenbart ogrundad eller orimlig. Av skäl 63 till förordningen framgår att de registrerade bör ha rätt att få tillgång till personuppgifter på detta sätt med rimliga intervall.

Enligt Dataskyddsutredningens förslag (SOU 2017:39) ska den nya dataskyddslagen i 5 kap. 2 § innehålla en bestämmelse som motsvarar undantaget i 26 § tredje stycket PuL för personuppgifter i löpande text som inte fått sin slutliga utformning eller som utgör minnesanteckningar. Vidare ska den nya dataskyddslagen, enligt Dataskyddsutredningens förslag, i 5 kap. 1 § innehålla en bestämmelse enligt vilken bl.a. artikel 15 i dataskyddsförordningen inte gäller uppgifter som, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämnas ut till den registrerade.

15.5.3 Bedömning

Förslag: Den registrerades rätt till information enligt artikel 15 i dataskyddsförordningen ska inte gälla sådana 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. Regleringen ska genomföras genom en hänvisning till den föreslagna 5 kap. 1 § första stycket dataskyddslagen.

Den registrerade rätt till tillgång till personuppgifter enligt artikel 15 i dataskyddsförordningen ska inte gälla personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller

liknande. Undantaget ska inte gälla om personuppgifterna har lämnats ut till tredje part, behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål eller har behandlats under längre tid än ett år i löpande text som inte fått sin slutliga utformning. Regleringen ska genomföras genom en hänvisning till den föreslagna 5 kap. 2 § dataskyddslagen.

Den information som ska lämnas till den registrerade enligt artikel 15 i dataskyddsförordningen är något mer utförlig än den som i nuläget ska lämnas i enlighet med domstolsdatalagen och personuppgiftslagen. För de informationspunkter som är nya (t.ex. perioden för lagring samt information om möjligheten att begära rättelse och radering) bör det enligt vår mening vara möjligt att ta fram standardiserad information som kan användas vid de flesta förfrågningar. Detta borde innebära att de nya bestämmelserna inte skulle medföra en alltför stor administrativ belastning för domstolarna.

Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande (SOU 2017:29) föreslagit att 4 kap. 7 § brottsdatalagen ska innehålla en bestämmelse som innebär att den personuppgiftsansvarige får avslå en begäran om viss personrelaterad information, exempelvis vilka personuppgifter om sökanden som behandlas, om den är orimlig eller uppenbart ogrundad. Vidare föreslår utredningen att 4 kap. 12 § brottsdatalagen ska innehålla en bestämmelse som innebär att den personuppgiftsansvarige får ta ut en rimlig avgift eller avslå begäran om någon begär sådan information oftare än en gång per år.⁴

För att uppnå samstämmighet i de regelverk som ska tillämpas vid personuppgiftsbehandling hos domstolarna vore det önskvärt med en liknande konkretisering av vad som ska anses vara ett rimligt tidsintervall för registerutdrag vad gäller den del av domstolarnas personuppgiftsbehandling som styrs av dataskyddsförordningen. Det faktum att det, enligt artikel 12.5 andra stycket i förordningen, är den personuppgiftsansvarige som ska visa att en begäran är uppenbart ogrundad eller orimlig talar enligt vår mening dock för att vad som är ett rimligt intervall för en begäran måste

⁴ Se Utredningen om 2016 års dataskyddsdirektivs delbetänkande (SOU 2017:29 s. 400 ff.).

avgöras i det enskilda fallet. I dataskyddsförordningen anges inte heller uttryckligen att det skulle finnas en möjlighet att i nationell rätt införa bestämmelser som förtydligar vilket tidsintervall för avgiftsfri information som ska anses vara rimligt. Det torde således inte vara fråga om en sådan situation som beskrivs i artikel 6.2 i dataskyddsförordningen eller i dess skäl 8 och som skulle kunna ge möjlighet att precisera eller införliva delar av förordningen i nationell rätt (jfr avsnitt 5.3). Mot den bakgrunden bedömer vi att det inte finns något utrymme för att i domstolsdatalagen införa bestämmelser liknande de som föreslagits för brottsdatalagen.

Som vi nämnt i avsnitt 15.5.2 finns det i artikel 15 i dataskyddsförordningen inte några undantag från rätten att få information om personuppgiftsbehandlingen efter begäran. Vi anser dock att en hänvisning bör göras i domstolsdatalagen till den föreslagna 5 kap. 1 § första stycket dataskyddslagen. Den bestämmelsen innebär att artiklarna 13–15 i dataskyddsförordningen inte gäller uppgifter som, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämnas ut till den registrerade.⁵ På detta sätt kommer bestämmelser om sekretess eller tystnadsplikt att gå före den registrerades rätt att få information om behandlingen av hans eller hennes personuppgifter även när dataskyddsförordningen börjar tillämpas.

Vi anser vidare att det bör göras en hänvisning i domstolsdatalagen till den föreslagna 5 kap. 2 § dataskyddslagen, som motsvarar 26 § tredje stycket PuL. Genom en sådan hänvisning kommer domstolarnas tjänstemän även framöver att under en rimlig tid få ha sina ofärdiga alster i fred. På samma sätt som i nuläget måste detta enligt vår mening anses vara en rimlig avvägning mellan den registrerades rätt till information och domstolarnas oberoende.

Vid information enligt artikel 15 i dataskyddsförordningen kommer domstolarna, på samma sätt som när information ska lämnas enligt artikel 13 i förordningen, att behöva ta ställning till i vilka situationer information om rätten att lämna in klagomål till tillsynsmyndigheten ska lämnas till den registrerade. För detta resonemang hänvisar vi till avsnitt 15.3.3.

⁵ Se Dataskyddsutredningens betänkande (SOU 2017:39).

Slutligen anser vi att det inte finns anledning att i domstolsdatalagen införa bestämmelser som begränsar den registrerades rättigheter enligt artikel 15 i dataskyddsförordningen ytterligare. Genom de hänvisningar till 5 kap. 1 och 2 §§ dataskyddslagen som vi föreslagit kommer samma undantag som i dag att gälla. Vi kan inte se att det finns några ytterligare behov av att begränsa rättigheterna för att säkerställa viktiga mål av generellt allmänt intresse, rättsväsendets oberoende eller rättsliga åtgärder.

15.6 Rättelse och radering samt rätt att göra invändningar och begära begränsning av behandling

15.6.1 Domstolsdatalagen, personuppgiftslagen och 1995 års dataskyddsdirektiv

Domstolsdatalagen hänvisar, genom 5 § 6, till 28 § PuL. Enligt denna bestämmelse är den personuppgiftsansvarige skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med personuppgiftslagen eller föreskrifter som har utfärdats med stöd av den lagen. Om den registrerade begär det ska den personuppgiftsansvarige också underrätta mottagarna av uppgifterna om åtgärden. Detsamma gäller om mera betydande skada eller olägenhet för den registrerade skulle kunna undvikas genom en sådan underrättelse. Underrättelse behöver dock inte lämnas om det visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

I domstolsdatalagen nämns endast att hänvisningen till 28 § PuL gäller bestämmelsen om rättelse. Av förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 92) framgår dock att hänvisningen även avser rätten till blockering och utplåning av personuppgifter.

Domstolsdatalagen hänvisar även, i 5 § 3, till 9 § PuL om grundläggande krav på behandling av personuppgifter. Enligt denna bestämmelse ska den personuppgiftsansvarige se till att alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen.

Kort kan sägas att *rättelse* av en personuppgift innebär att en felaktig eller ofullständig uppgift ersätts av en uppgift om de rätta förhållandena eller att uppgifterna annars kompletteras. Med *blockering* avses en åtgärd som vidtas för att personuppgifterna ska förse med information om att de är spärrade och om anledningen till spärren, för att personuppgifterna inte ska lämnas ut till tredje man annat än med stöd av 2 kap. TF. *Utplånande* innebär helt enkelt att de aktuella personuppgifterna förstörs så att de inte kan återskapas.⁶

När personuppgifter behandlas för att utföra en arbetsuppgift av allmänt intresse eller som ett led i myndighetsutövning, ska medlemsstaterna enligt artikel 14 a i 1995 års dataskyddsdirektiv tillförsäkra den registrerade rätten att motsätta sig behandling av uppgifter som rör honom eller henne. Rätten ska enligt bestämmelsen gälla om den nationella lagstiftningen inte föreskriver annat. Genom 12 § andra stycket PuL har lagstiftaren gjort den registrerades rätt att motsätta sig behandling mycket begränsad. Enligt denna bestämmelse har den registrerade endast rätt att motsätta sig sådan behandling av personuppgifter som är tillåten enligt personuppgiftslagen när behandlingen sker för ändamål som gäller direkt marknadsföring eller om behandlingen sker med stöd av samtycke.⁷

15.6.2 Dataskyddsförordningen

Rättelse

Enligt artikel 16 i dataskyddsförordningen har den registrerade rätt att utan onödigt dröjsmål få felaktiga personuppgifter rättade. Den registrerade ska även, med beaktande av ändamålet med behandlingen, ha rätt att komplettera ofullständiga personuppgifter.

⁶ Sören Öman och Hans-Olof Lindblom, Personuppgiftslagen (15 september 2016, Zeteeo), kommentaren till 28 §.

⁷ Se förarbetena till personuppgiftslagen (prop. 1997/98:44 s. 64 ff.).

Radering

Enligt artikel 17 i dataskyddsförordningen har den registrerade i vissa fall rätt att få sina personuppgifter raderade utan onödigt dröjsmål. Detta motsvarar personuppgiftslagens begrepp *utplåning*. De situationer som främst är av intresse för domstolarnas rättskipande och rättsvårdande verksamhet är de som framgår av artikel 17.1 a, c och d i förordningen. Led a avser situationen att personuppgifterna inte längre är nödvändiga för de ändamål som de samlats in för eller på annat sätt behandlats för. Led c avser situationen att den registrerade har gjort invändningar mot behandlingen i enlighet med artikel 21.1 och det saknas berättigade skäl för behandlingen som väger tyngre än den registrerades skäl för radering. Led d avser situationen att personuppgifterna har behandlats på ett olagligt sätt.

Det finns dock en rad undantag från rätten till radering. De som enligt vår mening främst är av intresse är de som framgår av artikel 17.3 b, d och e i förordningen. Enligt led b har den registrerade inte rätt att få sina personuppgifter raderade om behandlingen av uppgifterna är nödvändig för att uppfylla en rättslig förpliktelse enligt unionsrätten eller en medlemsstats nationella rätt. Rätten till radering gäller inte heller om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Den registrerade har vidare inte, enligt led d, rätt att få sina personuppgifter raderade om behandlingen är nödvändig för bl.a. arkivändamål av allmänt intresse eller statistiska ändamål, i den utsträckning som raderingen sannolikt omöjliggör eller avsevärt försvårar uppnåendet av syftet med den behandlingen. Avslutningsvis gäller inte rätten till radering enligt led e om behandlingen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

Rätt att göra invändningar och begära begränsning av behandling

Om behandlingen av personuppgifter grundar sig på en uppgift av allmänt intresse eller myndighetsutövning har den registrerade, enligt artikel 21.1 i dataskyddsförordningen, rätt att av skäl som

hänför sig till hans eller hennes specifika situation göra invändningar mot behandlingen. Om en sådan invändning görs får den personuppgiftsansvarige inte längre behandla personuppgifterna om denne inte kan visa att det finns avgörande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter. Personuppgifterna får dock fortsätta behandlas bl.a. om det sker för fastställande, utövande eller försvar av rättsliga anspråk. Följden av att intresseavvägningen utfaller till den registrerades fördel blir, åtminstone om den registrerade begär det, att de aktuella personuppgifterna ska raderas. Detta framgår av artikel 17.1 c i dataskyddsförordningen.

Under den tid det tar för den personuppgiftsansvarige att efter en invändning kontrollera om den registrerades skäl mot behandlingen väger tyngre än den personuppgiftsansvariges skäl för att utföra behandlingen ska behandlingen av uppgifterna begränsas i enlighet med artikel 18.1 d.

Den registrerade har, enligt artikel 18.1 a–c i dataskyddsförordningen, även i vissa andra fall rätt att kräva att behandlingen av hans eller hennes personuppgifter begränsas. När den registrerade har gjort invändningar mot personuppgifternas riktighet ska behandlingen enligt led a begränsas under den tid då den personuppgiftsansvarige kontrollerar om personuppgifterna är riktiga. Enligt led b ska behandlingen begränsas om den är olaglig och den registrerade i stället för radering begär en begränsning av uppgifternas användning. Enligt led c ska behandlingen begränsas om den personuppgiftsansvarige inte längre behöver personuppgifterna för ändamålen med behandlingen men de fortsatt behöver lagras eftersom den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

Under den tid begränsningen gäller får personuppgifterna, enligt huvudregeln i artikel 18.2, inte behandlas på annat sätt än att de lagras. Förfarandet motsvarar det som i personuppgiftslagen kallas blockering. Undantag finns dock, exempelvis får uppgifterna under begränsningsperioden behandlas för att fastställa rättsliga anspråk eller för skäl som rör ett viktigt allmänintresse för en medlemsstat.

Mottagare ska underrättas

Enligt artikel 19 i dataskyddsförordningen ska den personuppgiftsansvarige underrätta varje mottagare av personuppgifterna om de rättelser, raderingar eller begränsningar av behandling som gjorts. Undantag från denna skyldighet får göras om det visar sig vara omöjligt eller medför en oproportionell ansträngning. Om den registrerade begär det ska den personuppgiftsansvarige även informera den registrerade om vilka mottagarna av personuppgifter är.

15.6.3 Bedömning

Bedömning: Det bör inte införas några undantag i domstolsdatalagen från dataskyddsförordningens bestämmelser om de registrerades rättigheter i artiklarna 16–19 eller i artiklarna 21 och 22.

Rättelse

Dataskyddsförordningens bestämmelser om de registrerades rätt att komplettera ofullständiga personuppgifter och få felaktiga personuppgifter rättade (artikel 16) motsvarar vad som, genom domstolsdatalagens hänvisning till 9 och 28 §§ PuL, för närvarande gäller för domstolarnas rättskipande och rättsvårdande verksamhet. Det bör enligt vår mening ligga i domstolarnas intresse att de personuppgifter som behandlas i denna verksamhet är korrekta och fullständiga. Något behov av att på domstolsdatalagens tillämpningsområde införa undantag från dataskyddsförordningens bestämmelse om rättelse finns enligt vår uppfattning därmed inte.

Radering

Dataskyddsförordningens bestämmelser om rätten till radering är mer omfattande än vad som enligt domstolsdatalagen och personuppgiftslagen gäller för domstolarna i dag. Enligt artikel 17.3 b i dataskyddsförordningen gäller dock inte rätten till

radering om behandlingen är nödvändig som ett led i den personuppgiftsansvariges myndighetsutövning eller för att den personuppgiftsansvarige ska kunna utföra en uppgift av allmänt intresse. Som vi tidigare konstaterat (avsnitt 6.2.5) anser vi att den personuppgiftsbehandling som sker inom ramen för domstolarnas rättsskipande och rättsvårdande verksamhet är nödvändig, som ett led i domstolarnas myndighetsutövning eller för att utföra en uppgift av allmänt intresse. Rätten till radering gäller enligt vår mening därför inte uppgifter i pågående mål eller ärenden. Undantaget i artikel 17.3 b garanterar därmed att handläggningen av öppna mål eller ärenden inte avstannar på grund av dataskyddsbestämmelser.

För arkivering finns dessutom, i artikel 17.3 d i dataskyddsförordningen, ett specifikt undantag från rätten till radering. Enligt denna bestämmelse ska den rätten inte gälla för det fall raderingen sannolikt omöjliggör eller avsevärt försvårar att syftet med den behandling som utförs för arkivändamål av allmänt intresse uppnås. Detta medför enligt vår mening att rätten till radering inte heller gäller personuppgifter som ingår i de handlingar som arkiverats i enlighet med gällande arkivlagstiftning. Vi anser att rätten till radering inte heller gäller för de personuppgifter som finns i avslutade mål och ärenden som ännu inte har arkiverats. Bevarandet av allmänna handlingar är en förutsättning för allmänhetens möjlighet att ta del av dessa handlingar med stöd av tryckfrihetsförordningen, vilket enligt vår mening innebär att ett sådant bevarande är nödvändigt för en uppgift av allmänt intresse.

Eftersom redan befintliga undantag i dataskyddsförordningen enligt vår bedömning således garanterar att personuppgifter i både öppna, avslutade och arkiverade mål och ärenden undantas från rätten till radering anser vi att det inte finns något behov av att i domstolsdatalagen föreskriva ytterligare undantag från denna rättighet.

Avslutningsvis vill vi dock påpeka att vi anser att dataskyddsförordningen inte hindrar domstolarna att radera personuppgifter som behandlats i strid med gällande personuppgiftsbestämmelser. En förutsättning är dock naturligtvis att detta är tillåtet enligt det övriga regelverk som styr rätten till radering i verksamhetsystemen, t.ex. svenska processuella regler och arkivregler.

Rätt att göra invändningar och begära begränsning av behandling

Den registrerades rätt att enligt artikel 21.1 i dataskyddsförordningen göra invändningar mot att personuppgifter behandlas för myndighetsutövning eller för en uppgift av allmänt intresse, är en utökning jämfört med vad som för närvarande gäller. Som vi tidigare konstaterat anser vi att den personuppgiftsbehandling som sker på domstolsdatalagens tillämpningsområde utgör myndighetsutövning eller en uppgift av allmänt intresse (se avsnitt 6.2.5). Detta innebär att dataskyddsförordningens bestämmelse om rätten att göra invändningar gäller för den behandling av personuppgifter som sker i enlighet med domstolsdatalagen.

Under den tid det tar för domstolen att efter en registrerads invändning bedöma om skälen för behandlingen väger tyngre än den registrerades skäl mot denna, ska behandlingen begränsas enligt artikel 18.1 d och 18.2 i dataskyddsförordningen. Det samma gäller enligt artikel 18.1 a–c i dataskyddsförordningen under en kontroll av personuppgifternas riktighet, i vissa fall då behandlingen är olaglig eller i vissa fall om uppgifterna inte längre behövs för ändamålen med behandlingen. Den registrerades rätt till begränsning av personuppgiftsbehandling är därmed utförligare än personuppgiftslagens bestämmelser om blockering.

En begränsning innebär enligt huvudregeln i artikel 18.2 att personuppgifter inte får behandlas på något annat sätt än att lagras. Undantag görs dock för det fall behandlingen sker för att fastställa rättsliga anspråk eller av skäl som rör ett viktigt allmänintresse för medlemsstaten.

Att handläggningen av mål och ärenden hos domstolarna inte avstannar utgör enligt vår mening ett viktigt allmänintresse. I förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 48) har regeringen vidare gett uttryck för uppfattningen att domstolarnas kärnverksamhet består i att fastslå rättsliga anspråk. Mot den bakgrunden anser vi att undantaget i artikel 18.2 i dataskyddsförordningen är tillämpligt på de personuppgifter som ingår i pågående mål och ärenden. Följden av detta blir att domstolens handläggning av det enskilda målet eller ärendet inte behöver avstanna i väntan på att en intresseavvägning ska göras efter en invändning (artikel 18.1 d). Samma resonemang bör enligt vår

mening kunna tillämpas vid en invändning om personuppgifternas riktighet (artikel 18.1 a).

Ändamålet med behandlingen av personuppgifter i domstolarnas mål och ärenden är vidare att handlägga just dessa mål och ärenden. Detta borde enligt vår mening medföra att så länge handläggningen av ett mål eller ärende inte är avslutad, behövs personuppgifterna för ändamålet med behandlingen. Rätten till begränsning av uppgifter som inte längre behövs för ändamålet (artikel 18.1 c) bör därmed ha mycket liten betydelse för domstolarna vad gäller pågående mål och ärenden. Skulle en sådan situation uppkomma gör vi emellertid även här bedömningen att personuppgifterna fortsatt kan behandlas i öppna mål och ärenden med stöd av undantaget för fastställande av rättsliga anspråk eller ett viktigt allmänintresse.

För domstolarna är det vidare i stor utsträckning de processuella regelverken som styr vilka personuppgifter som behöver behandlas i de enskilda målen och ärendena. Vi anser därför att en sådan olaglig behandling av personuppgifter där en begränsning av behandling kan krävas (artikel 18.1 b) bör vara mycket sällsynt förekommande.

Vad gäller avslutade mål och ärenden bör bevarande, och senare även arkivering, vara tillåten även om behandlingen av de aktuella personuppgifterna har begränsats, eftersom ett sådant bevarande respektive arkivering vanligtvis endast innebär att personuppgifterna lagras. I domstolarnas verksamhetssystem går det emellertid även att söka bland avslutade mål och ärenden, vilket innebär en behandling av personuppgifterna utöver lagringen. Sådana sökningar är oftast ett led i handläggningen av öppna mål eller ärenden, i syfte att exempelvis hitta tidigare liknande avgöranden eller vägledande praxis. Det utgör enligt vår mening ett viktigt allmänintresse att sådana sökningar får göras, eftersom det är ett led i att säkerställa en enhetlig och effektiv rättstillämpning. Det finns därmed undantag som tillåter att sådan behandling får fortsätta även om behandlingen av personuppgifter har begränsats i enlighet med artikel 18.1 i dataskyddsförordningen. Samma resonemang bör enligt vår mening vara tillämpligt vid domstolarnas återanvändande av personuppgifter i arkiverade mål och ärenden (se avsnitt 19.4.5).

Även allmänhetens tillgång till allmänna handlingar utgör enligt vår mening ett viktigt allmänintresse. Detta medför att utlämnande av allmänna handlingar – både i pågående och avslutade mål och ärenden – är tillåtet även om behandlingen av personuppgifter har begränsats. Myndigheternas rätt att lämna ut personuppgifter i allmänna handlingar i enlighet med nationell rätt säkerställs för övrigt även genom artikel 86 i dataskyddsförordningen.

Skulle en intresseavvägning efter den registrerades invändning enligt artikel 21.1 i dataskyddsförordningen mot förmodan utfalla till den registrerades fördel, skulle domstolen – enligt huvudregeln i artikel 17.1 c – vara tvungen att radera personuppgifterna. Som ovan nämnts har behandlingen av personuppgifter i domstolarnas rättskipande och rättsvårdande verksamhet i tidigare förarbeten dock bedömts utgöra ett fastställande av rättsliga anspråk. Med stöd av den bedömningen bör undantaget i artikel 21.1 i förordningen garantera att handläggningen vid behov får fortsätta även om intresseavvägningen utfaller till den enskildes fördel. Vi har vidare, under föregående rubrik, gjort bedömningen att undantaget i artikel 17.3 b och d i dataskyddsförordningen medför att personuppgifter som behandlas i domstolarnas rättskipande och rättsvårdande verksamhet – inkluderat de som finns i både avslutade och arkiverade mål och ärenden – inte behöver raderas. Även detta undantag säkerställer därmed att behandlingen av personuppgifter kan fortsätta om en intresseavvägning utfaller till den enskildes fördel.

Vi anser sammanfattningsvis att de undantag som finns i artikel 17.3 b och d, artikel 18.2 samt artikel 21.1 i dataskyddsförordningen garanterar att domstolarnas handläggning av enskilda mål eller ärenden inte avstannar, att bevarande och arkivering av processmaterialet är möjlig och att allmänhetens tillgång till allmänna handlingar inte inskränks. Mot den bakgrunden finns det enligt vår mening inte något egentligt behov av att i domstolsdatalagen införa ytterligare inskränkningar av rätten att göra invändningar eller rätten att få personuppgiftsbehandlingen begränsad.

Enligt vårt resonemang blir rätten att göra invändningar och rätten att begära att behandlingen begränsas till stora delar illusorisk vad gäller domstolarnas behandling av personuppgifter. Man skulle kunna argumentera för att det faktum att den

registrerades möjligheter att nå reell framgång med en invändning eller en begäran är ytterst små i en viss verksamhet, innebär att det inte skulle finnas möjlighet att införa ett generellt undantag från dessa rättigheter. Skälet till detta skulle i så fall vara att ett sådant undantag inte är nödvändigt för att säkerställa rättsväsendets oberoende, nationella viktiga mål av generellt allmänt intresse eller något annat av de syften som anges i artikel 23.1 i dataskyddsförordningen. Finns det ingen risk för framgång med en invändning eller en begäran, utgör det inget reellt hot mot exempelvis rättsväsendets oberoende. Vi kan emellertid inte med säkerhet slå fast att det inte finns situationer då det kan finnas grund för en invändning eller en begäran. För att garantera att arbetet i domstolarna kan fortsätta ostört, skulle man därför möjligtvis – med stöd av artikel 23.1 i dataskyddsförordningen – kunna föreskriva ett uttryckligt undantag från rätten enligt artiklarna 18.1 och 21.1 att göra invändningar mot att personuppgifter behandlas och rätten att begära att behandlingen begränsas. Vi stannar emellertid vid bedömningen att en reglering som inskränker de registrerades rättigheter inte bör införas utan sakliga skäl bara för att – sannolikt i ringa omfattning – minska den administrativa bördan med att hantera invändningar eller krav på begränsningar.

Mot denna bakgrund är det vår uppfattning att en bedömning av om behandlingen ska begränsas får göras i varje fall där frågan aktualiseras enligt bestämmelserna i dataskyddsförordningen. Även intresseavvägningen mellan domstolens skäl för behandlingen och den registrerades skäl mot denna, får enligt vår mening göras varje gång en registrerad gör en invändning mot behandlingen i enlighet med artikel 21 i dataskyddsförordningen. En annan sak är att bedömningen och intresseavvägningen i det stora flertalet fall borde kunna göras relativt standardiserat.

Underrättelse till mottagarna

Dataskyddsförordningens bestämmelser om underrättelse till mottagarna av personuppgifter vid rättelse, radering eller begränsning av behandling motsvarar vad som, genom en hänvisning till 28 §§ PuL, för närvarande gäller inom domstols-

datalagens tillämpningsområde. Någon anledning att införa undantag från denna rättighet i domstolsdatalagen har inte kommit fram.

15.7 Rätt till skadestånd

15.7.1 Domstolsdatalagen och personuppgiftslagen

Enligt artikel 22 i 1995 års dataskyddsdirektiv ska medlemsstaterna föreskriva att var och en har rätt att föra talan inför domstol om sådana kränkningar av rättigheter som skyddas av den nationella lagstiftning som är tillämplig på ifrågavarande behandling. Direktivet har i denna del genomförts i svensk rätt genom 48 § PuL. Domstolsdatalagen hänvisar, genom 5 § 11, till denna bestämmelse.

Enligt 48 § PuL ska den personuppgiftsansvarige ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med personuppgiftslagen har orsakat. Domstolsdatalagens hänvisning till bestämmelsen innebär enligt förarbetena till den lagen (prop. 2014/15:148 s. 92 f.) att skadeståndsansvaret även gäller vid personuppgiftsbehandling som skett i strid med domstolsdatalagens bestämmelser. I samma förarbeten framhäver regeringen att det är principiellt viktigt att den som drabbas av skada eller kränkning på grund av att personuppgifter behandlas i strid med domstolsdatalagen, på ett rimligt sätt kan kompenseras genom skadestånd.

15.7.2 Dataskyddsförordningen

Enligt artikel 79.1 i dataskyddsförordningen har alla registrerade rätt till ett effektivt rättsmedel om de anser att deras rättigheter enligt förordningen har åsidosatts som en följd av att deras personuppgifter har behandlats på ett sätt som inte är förenligt med förordningen. Enligt bestämmelsen gäller detta utöver rätten att lämna in ett klagomål till tillsynsmyndigheten. Om den personuppgiftsansvarige – eller personuppgiftsbiträdet – är en myndighet som agerar inom ramen för sin myndighetsutövning ska sådan

tal, enligt artikel 79.2 i dataskyddsförordningen, väckas vid domstolarna i den medlemsstat där den personuppgiftsansvarige, eller personuppgiftsbiträdet, är etablerad.

Rätten till ett effektivt rättsmedel garanteras även av EU:s stadga om de grundläggande rättigheterna. Enligt artikel 47 i stadgan har var och en vars unionsrättsligt garanterade fri- och rättigheter kränkts rätt till ett effektivt rättsmedel inför en domstol. Stadgan ger, enligt artikel 8.1, rätt till skydd av personuppgifter. Som en konkretisering av denna rättighet anges i artikel 8.2 att personuppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av en legitim och lagenlig grund. Var och en ska dessutom ha rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dessa uppgifter. Enligt artikel 8.3 ska en oberoende myndighet kontrollera att dessa regler efterlevs.

Enligt artikel 82 i dataskyddsförordningen har varje person som lidit materiell eller immateriell skada till följd av en överträdelse av förordningen rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan. Enligt bestämmelsen är ansvaret solidariskt om flera personuppgiftsansvariga eller personuppgiftsbiträden har medverkat vid samma behandling. Det finns även en uttrycklig regressrätt mellan de ansvariga i en sådan situation. Den personuppgiftsansvarige – eller personuppgiftsbiträdet – ska dock undgå ansvar om denne visar att den inte på något sätt är ansvarig för den händelse som orsakat skadan.

I skäl 146 till dataskyddsförordningen förtydligas att behandling som strider mot dataskyddsförordningen även omfattar bl.a. behandling som strider mot medlemsstaternas nationella rätt med närmare specifikation av förordningens bestämmelser. Detta innebär enligt vår mening att även överträdelser av bestämmelser i de registerförfattningar som behålls eller införs i svensk rätt med stöd av artikel 6.2 och 6.3 i dataskyddsförordningen (se kapitel 5) omfattas av förordningens bestämmelse om skadeståndsansvar.⁸

⁸ Se även Dataskyddsutredningens betänkande (SOU 2017:39 s. 304 f.).

15.7.3 Dataskyddslagen

Dataskyddsutredningen har i sitt betänkande föreslagit att dataskyddslagen ska innehålla en bestämmelse som innebär att rätten till ersättning enligt artikel 82 i dataskyddsförordningen även gäller vid överträdelser av bestämmelser i dataskyddslagen och andra författningar som kompletterar dataskyddsförordningen. Bestämmelsen beskrivs i Dataskyddsutredningens betänkande (SOU 2017:39 s. 304) som en upplysningsbestämmelse och finns i förslaget till 8 kap. 1 § dataskyddslagen.

15.7.4 Bedömning

Förslag: Rätten till ersättning enligt artikel 82 i dataskyddsförordningen ska gälla även vid överträdelser av bestämmelser i dataskyddslagen och domstolsdatalagen med tillhörande föreskrifter. Regleringen ska genomföras genom en hänvisning till den föreslagna 8 kap. 1 § dataskyddslagen.

Tillsynsmyndigheten har, enligt artikel 55.3 i dataskyddsförordningen, inte behörighet att utöva tillsyn över den personuppgiftsbehandling som sker i domstolarnas dömande verksamhet. Detta innebär att den dömande verksamheten är undantagen från en del av det skydd för den personliga integriteten som garanteras genom dataskyddsförordningen (se vidare avsnitt 8.4). Mot den bakgrunden är frågan om rätten till ett effektivt rättsmedel i högsta grad aktuell för domstolarnas personuppgiftsbehandling.

Vid genomförandet av 1995 års dataskyddsdirektiv bedömdes att personuppgiftslagens skadeståndsbestämmelse – tillsammans med tillsynsmyndighetens möjlighet till vitesföreläggande – utgjorde en effektiv och tillräcklig sanktion.⁹ Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 304) vidare gjort bedömningen att den registrerades rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde tillgodoses i svensk rätt genom möjligheten att vid allmän

⁹ Prop. 1997/98:44 s. 107.

domstol föra talan om ersättning för den skada som en behandling av personuppgifter i strid med förordningen har gett upphov till.

Enligt vårt förslag kommer den registrerade att ha möjlighet att överklaga vissa beslut som fattats av en domstol i dess egenskap av personuppgiftsansvarig (se avsnitt 18.4.4). Dataskyddsförordningens skadeståndsbestämmelse omfattar dessutom även överträdelse av domstolsdatalagens bestämmelser. Man skulle dock kunna ifrågasätta hur den rätt till kontroll av en oberoende myndighet som framgår av artikel 8.3 i stadgan förhåller sig till det faktum att tillsynsmyndigheten inte kommer att vara behörig att utöva tillsyn över domstolarnas dömande verksamhet.

Avsikten med att begränsa tillsynsmyndighetens behörighet är emellertid att säkerställa domstolarnas oberoende (jfr skäl 20 till dataskyddsförordningen). Enligt artikel 47 i stadgan har den vars unionsrättsligt garanterade fri- och rättigheter kränkts rätt att få sin sak prövad inför en oavhängig och opartisk domstol. Dataskyddsförordningens begränsning av tillsynsmyndighetens behörighet bidrar således till att medlemsstaterna kan uppfylla de skyldigheter de har enligt artikel 47 i stadgan. Samtidigt finns det uppenbarligen en konflikt mellan begränsningen och rätten till kontroll av en oberoende myndighet vad gäller skyddet av personuppgifter. Som framgår av avsnitt 8.1.2 har emellertid både Justitieombudsmannen och Justitiekanslern möjlighet att utöva en ganska vittgående tillsyn över domstolarna. Mot den bakgrunden anser vi att den svenska lagstiftningen uppfyller de krav som ställs i artikel 8 i stadgan. Vi anser även att den registrerades rätt till ett effektivt rättsmedel när personuppgiftsbehandling skett på domstolsdatalagens tillämpningsområde tillgodoses genom dataskyddsförordningens skadeståndsbestämmelse i kombination med rätten att överklaga vissa beslut som fattats av den personuppgiftsansvariga domstolen.

Som nämnts ovan kommer dataskyddsförordningens bestämmelser om skadestånd även utan hänvisning till förordningen att gälla även för överträdelse av domstolsdatalagens bestämmelser. Det framgår enligt vår mening dock inte tydligt av artikel 82 i dataskyddsförordningen att skadeståndsansvaret även omfattar överträdelse av de nationella registerförfattningarnas bestämmelser. Vi anser därför att det finns anledning att göra en hänvisning i domstolsdatalagen till den föreslagna 8 kap. 1 §

dataskyddslagen om skadestånd. På detta sätt kommer det att stå fullständigt klart att dataskyddsförordningens bestämmelser om skadestånd gäller även vid överträdelse av domstolsdatalagens bestämmelser.

15.8 Information om personuppgiftsincident

15.8.1 Dataskyddsförordningen

Om en personuppgiftsincident sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om incidenten. Detta framgår av artikel 34.1 i dataskyddsförordningen. I artikel 34.3 a–c finns undantag från den personuppgiftsansvariges skyldighet att lämna sådan information till den registrerade. Information behöver inte lämnas om den personuppgiftsansvarige har vidtagit lämpliga tekniska och organisatoriska skyddsåtgärder (led a), om den personuppgiftsansvarige har vidtagit ytterligare åtgärder som innebär att det inte längre uppstår hög risk för de registrerades rättigheter och friheter (led b) eller om det skulle innebära en opropotionerlig ansträngning att lämna sådan information (led c). För det fall undantag enligt led c blir aktuellt ska dock allmänheten i stället informeras eller så ska en liknande åtgärd vidtas.

15.8.2 Bedömning

Förslag: Den registrerades rätt att få information om en personuppgiftsincident enligt artikel 34 i dataskyddsförordningen ska inte gälla om den personuppgiftsansvarige, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämna ut uppgifter till den registrerade.

Den personuppgiftsansvariges skyldighet att, enligt artikel 34 i dataskyddsförordningen, informera den registrerade om en inträffad personuppgiftsincident innebär en utökning jämfört med vad som för närvarande gäller. Vi anser att det finns anledning att införa en bestämmelse i domstolsdatalagen som innebär att

sekretess eller tystnadsplikt går före den registrerades rätt att få information om en sådan incident. Bakgrunden till detta är följande.

I vissa typer av mål som handläggs hos domstolarna råder det sekretess gentemot en av parterna om att ett sådant mål överhuvudtaget finns registrerat vid den aktuella domstolen. Som exempel kan nämnas de allmänna förvaltningsdomstolarnas mål om betalningssäkring enligt 46 kap. skatteförfarandelagen (2011:1244). I dessa mål gäller sekretess enligt 17 kap. 2 § OSL normalt för uppgifter om identiteten på den part som tvångsåtgärden riktar sig mot, i vart fall till dess domstolen meddelar dom eller beslut i målet. En annan ordning skulle kunna innebära att syftet med betalningssäkringen går förlorat.

Undantagen i artikel 34.3 i dataskyddsförordningen innefattar inte situationer där det råder sekretess eller tystnadsplikt för vissa personuppgifter. Dataskyddsförordningens bestämmelse om information till den registrerade vid en personuppgiftsincident skulle därmed kunna innebära att den registrerade indirekt får information om att han eller hon är motpart i ett mål om exempelvis betalningssäkring.

Mot den bakgrunden föreslår vi att det i domstolsdatalagen införs en bestämmelse med innebörden att bestämmelserna om den registrerades rätt att få information om en personuppgiftsincident enligt artikel 34 i dataskyddsförordningen inte gäller om den personuppgiftsansvarige, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämna ut uppgifter till den registrerade.

Vi anser att ett sådant undantag kan göras med stöd av artikel 23.1 f i dataskyddsförordningen, eftersom det görs i syfte att säkerställa skyddet för rättsliga åtgärder. Vi anser vidare att begränsningen är nödvändig för att skydda de intressen som kommer till uttryck i de aktuella sekretessbestämmelserna och att den utgör en rimlig avvägning mellan dessa intressen och de registrerades intresse av skydd för den personliga integriteten. Begränsningen sker därmed, enligt vår mening, med respekt för andemeningen i de grundläggande rättigheter och friheter som kommer till uttryck i stadgan (se avsnitt 3.4.1).

Den föreslagna lydelsen motsvarar den reglering som Dataskyddsutredningen har föreslagit för 5 kap. 1 § dataskydds-

lagen, där undantag från rätten att få information om och tillgång till personuppgifter enligt artiklarna 13–15 i dataskyddsförordningen regleras (se avsnitt 15.3.2). En sådan ordning skulle vidare motsvara det som enligt Utredningen om 2016 års dataskyddsdirektivs förslag till 3 kap. 11 § brottsdatalagen ska gälla i motsvarande situation i den del av domstolarnas verksamhet som styrs av 2016 års dataskyddsdirektiv.¹⁰

¹⁰ Se Utredningen om 2016 års dataskyddsdirektivs delbetänkande (SOU 2017:29).

16 Känsliga personuppgifter m.m.

16.1 Dataskyddsförordningen och 1995 års dataskyddsdirektiv

Behandling av känsliga personuppgifter regleras i artikel 9 i dataskyddsförordningen. Med känsliga personuppgifter menas enligt dataskyddsförordningen personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter om hälsa och en persons sexualliv eller sexuella läggning. Även behandling av biometriska uppgifter för att entydigt identifiera en fysisk person och genetiska uppgifter utgör känsliga personuppgifter. Begreppet *känsliga personuppgifter* används inte uttryckligen i artikel 9, men förekommer i skäl 10 till dataskyddsförordningen. Det är också väl inarbetat i svensk rätt genom bl.a. 13 § PuL.

Begreppet *känsliga personuppgifter* har i dataskyddsförordningen utökats i förhållande till hur det såg ut i 1995 års dataskyddsdirektiv, genom att uppgifter om en persons sexuella läggning nu uttryckligen ingår i begreppet. Nytt är också att biometriska uppgifter för att entydigt identifiera en fysisk person och genetiska uppgifter utgör känsliga personuppgifter.

Enligt dataskyddsförordningens huvudregel, som framgår av artikel 9.1, är behandling av känsliga personuppgifter förbjuden. Det finns dock en rad undantag från detta förbud. De undantag som främst är intressanta för domstolarnas del framgår av artikel 9.2 f och g.

Enligt artikel 9.2 f är behandling av känsliga personuppgifter tillåten om den är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet. Enligt artikel 9.2 g är behandling av känsliga personuppgifter tillåten om en behandling är nödvändig med

hänsyn till ett viktigt allmänt intresse. Av bestämmelsen framgår vidare att det ”viktiga allmänna intresset” ska framgå av unionsrätten eller medlemsstaternas nationella rätt, som ska stå i proportion till det eftersträvade syftet, vara förenlig 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.

Även enligt 1995 års dataskyddsdirektiv är huvudregeln att behandling av känsliga personuppgifter är förbjuden. Undantaget i artikel 9.2 f i dataskyddsförordningen har till viss del sin motsvarighet i artikel 8.2 e i 1995 års dataskyddsdirektiv. Här fastställs att behandling av känsliga personuppgifter är tillåten om den rör uppgifter som är nödvändiga för att kunna fastslå, göra gällande eller försvara rättsliga anspråk. Bestämmelsen har införts i svensk rätt genom 16 § första stycket c PuL. Det som är nytt för dataskyddsförordningen i denna del är att undantag uttryckligen görs för domstolarnas dömande verksamhet.

Något direkt undantag med hänsyn till viktiga allmänna intressen finns inte i 1995 års dataskyddsdirektiv. Enligt artikel 8.4 har medlemsstaterna dock möjlighet att med hänsyn till ett viktigt allmänt intresse besluta om ytterligare undantag från förbudet att behandla känsliga personuppgifter. Något undantag som skulle kunna träffa domstolarnas rättskipande och rättsvårdande verksamhet har dock inte införts i personuppgiftslagen med stöd av artikel 8.4 i 1995 års dataskyddsdirektiv.

16.2 Domstolsdatalagen

16.2.1 Rätten att behandla känsliga personuppgifter

Enligt 16 § första stycket c PuL får känsliga personuppgifter behandlas om det är nödvändigt för att kunna fastställa rättsliga anspråk. I förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 48 f.) har regeringen gjort bedömningen att detta undantag innefattar den kärnverksamhet som bedrivs i domstolarna och som kommer till uttryck i domstolsdatalagens ändamålsbestämmelser. Av den anledningen innehåller domstolsdatalagen inte någon bestämmelse som klargör rätten för domstolarna att behandla känsliga personuppgifter.

I nämnda förarbeten görs följande bedömning av domstolarnas behov av att behandla känsliga personuppgifter.

Det stora flertalet känsliga personuppgifter som behandlas i domstol härrör från vad parterna anfört i inlagor och vid domstolsförhandlingar, vilket innebär att det ligger utanför domstolarnas kontroll om en viss uppgift förekommer i verksamheten eller inte. För domstolarnas egen del är det i huvudsak fråga om att använda redan inkomna känsliga personuppgifter vid framställning av olika dokument som är nödvändiga för handläggning och avgörande av mål och ärenden. I fråga om formulerande av domskäl har domstolarna i och för sig en möjlighet att påverka i vilken utsträckning känsliga personuppgifter återges eller tillförs texten. Det är dock av principiella skäl uteslutet att genom bestämmelser i domstolsdatalagen inskränka domarnas frihet att formulera domskäl i syfte att undvika att känsliga personuppgifter behandlas. /.../ Det finns strängt taget inga skillnader mellan i vilken utsträckning domstolarna behöver behandla känsliga personuppgifter och andra personuppgifter. För att domstolarna ska kunna sköta sin informationshantering elektroniskt måste de också kunna behandla känsliga personuppgifter för att på ett ändamålsenligt sätt vidta de åtgärder som behövs för att handlägga mål och ärenden. Att domstolarna tillåts behandla känsliga personuppgifter som ett led i handläggningen av mål och ärenden, t.ex. genom elektronisk lagring av partsinlagor, domskrivning, expediering av domar osv., bedöms typiskt sett inte medföra särskilt stora risker i integritetshänseende. Domstolarnas hantering av känsliga personuppgifter är i hög grad styrd av de processuella regelverken, vilket innebär att det finns en yttre ram för vad domstolen överhuvudtaget får göra. Mot denna bakgrund anser regeringen att behovet av att kunna behandla känsliga personuppgifter och de effektivitetsvinster som elektronisk hantering medför väger tyngre än den risk för integritetsintrång som en sådan behandling kan innebära. Behandlingen av känsliga personuppgifter bör därför som utgångspunkt vara tillåten och endast begränsas genom den rättsliga ram som föreslås i avsnitt 8, vilken bl.a. består av verksamhetspecifika ändamålsbestämmelser.

Av 13 § domstolsdatalagen framgår dock att uppgifter om en person inte får behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Av förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 50) framgår att bestämmelsen har införts för att tydliggöra att känsliga personuppgifter inte får användas som enda grund för en behandling av personuppgifter och att det inte är tillåtet att exempelvis föra register över eller på annat sätt göra anteckningar

om enskilda enbart på den grunden att de utifrån t.ex. etniskt ursprung eller hälsa kan hänföras till en viss kategori av människor.

16.2.2 Sökbegränsningar

Enligt 14 § första stycket domstolsdatalagen är det vid sökning i personuppgifter förbjudet att som sökbegrepp använda uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa, sexualliv, nationell anknytning samt brott eller misstanke om brott. Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 179) anfört att en vanligt förekommande skyddsåtgärd i registerförfattningar är sökbegränsningar. Bestämmelsen i 14 § domstolsdatalagen har enligt förarbetena (prop. 2014/15:148 s. 49) också införts för att minimera riskerna för att känsliga personuppgifter missbrukas.

I 14 § andra stycket domstolsdatalagen förtydligas att användning av särskilda beteckningar för identifiering av en viss mål- eller ärendetyp som sökbegrepp inte omfattas av förbudet i första stycket. Detta är ett förtydligande av att målgrupps- och måltypskoder får användas som sökbegrepp. Enligt förarbetena till domstolsdatalagen (a.a s. 63) är skälet till detta att sådana koder används i mycket stor utsträckning i domstolarnas dagliga verksamhet och inte anses medföra några särskilda risker i integritetshänseende.

Som bakgrundsinformation kan här nämnas att myndigheter enligt artikel 10 i dataskyddsförordningen får behandla personuppgifter som rör fällande domar i brottmål. Uppgifter om friande domar och misstanke om brott finns inte särskilt reglerat i dataskyddsförordningen.

I förarbetena till domstolsdatalagen (a.a s. 62) gör regeringen följande bedömning. Det finns integritetsrisker med att tillåta domstolspersonal att använda känsliga sökbegrepp. Domstolens tjänstemäns sökningar begränsas dock redan genom lagens ändamålsbestämmelse och av den bestämmelse i 8 § som innebär att varje tjänsteman endast får ha tillgång till de personuppgifter som behövs för att han eller hon ska kunna fullgöra sina arbetsuppgifter. Därför handlar riskerna främst om att allmänheten med

stöd av offentlighetsprincipen har möjlighet att begära att domstolspersonalen ska använda sökbegrepp för att sammanställa och lämna ut personuppgifter. Ett förbud för tjänstemän att använda vissa sökbegrepp medför att allmänheten inte heller har rätt att begära ut en sammanställning som gjorts utifrån dessa sökbegrepp. Detta framgår av den så kallade begränsningsregeln i 2 kap. 3 § tredje stycket TF.

I nämnda förarbeten framhölls dock också att det finns ett behov av att kunna använda vissa av de integritetskänsliga sökbegreppen i domstolarnas verksamhet. I 15 § domstolsdatalagen finns därför undantag från sökbegränsningarna i 14 §. Undantagen innebär att det är tillåtet att i allmän domstol använda sökbegrepp som avslöjar brott eller misstanke om brott samt att i allmän förvaltningsdomstol använda sökbegrepp som avslöjar hälsa, brott eller misstanke om brott. Sökbegränsningarna gäller inte heller vid sökning i en viss handling eller i ett visst mål eller ärende.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om begränsningar av möjligheten att använda de integritetskänsliga sökbegrepp som tillåts för allmän domstol och allmän förvaltningsdomstol. Regeringen har utnyttjat denna möjlighet och genom 3–6 §§ domstolsdataförordningen infört ytterligare begränsningar i de tillåtna sökningar som framgår av 15 § domstolsdatalagen. Det handlar om tidsbegränsningar för sökningarna och att vissa sökningar inte får göras i tvistemål eller i mål som handläggs av Migrationsöverdomstolen eller av en migrationsdomstol. Det finns även en tidsmässig begränsning för användande av personnamn, personnummer och samordningsnummer vid sökningar i brottmål.

16.3 Dataskyddslagen

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit att dataskyddslagen ska innehålla bestämmelser om rätten att behandla känsliga personuppgifter. Enligt förslaget ska myndigheter få behandla känsliga personuppgifter i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det (3 kap. 3 § 1). Dataskyddsutredningen föreslår också att myndigheter ska få behandla känsliga person-

uppgifter om de lämnats till myndigheten och behandlingen krävs enligt annan lag (3 kap. 3 § 2). Anledningen till detta anges vara att det utgör ett viktigt allmänintresse att myndigheterna ska kunna sköta sitt uppdrag på ett korrekt, rättssäkert och effektivt sätt. Detta förutsätter att den grundlagsstadgade handlings- offentligheten och andra lagstadgade skyldigheter upprätthålls. Det anges också att viss behandling av känsliga personuppgifter är oundvikligt i myndigheternas verksamhet som en direkt följd av exempelvis tryckfrihetsförordningens, offentlighets- och sekretesslagens och förvaltningslagens bestämmelser. Sådan behandling bör uttryckligen tillåtas i dataskyddslagen så att det inte råder någon tveksamhet kring lagligheten av behandlingen.¹

Utöver detta föreslår Dataskyddsutredningen att myndigheter i enstaka fall ska få behandla känsliga personuppgifter om det är absolut nödvändig för ändamålet med behandlingen och inte innebär ett otillbörligt intrång i den registrerades personliga integritet (3 kap. 3 § 3). En myndighet som behandlar känsliga personuppgifter enbart med stöd av 3 kap. 3 § dataskyddslagen ska enligt Dataskyddsutredningens förslag inte få använda sökbegrepp som avslöjar känsliga personuppgifter (3 kap. 4 §).

16.4 2016 års dataskyddsdirektiv

Av artikel 10 i 2016 års dataskyddsdirektiv framgår att behandling av känsliga personuppgifter ska vara tillåten endast om det är absolut nödvändigt och under förutsättning att det finns lämpliga skyddsåtgärder för den registrerades rättigheter och friheter. Dessutom måste ytterligare krav vara uppfyllda för att behandling av känsliga personuppgifter ska få ske; antingen ska behandlingen vara tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, eller ska behandlingen ske för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan fysisk person, eller ska behandlingen röra uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade. 2016 års dataskyddsdirektiv ger således, genom kravet på absolut nödvändighet, mer begränsade möjligheter att behandla känsliga personuppgifter än dataskydds-

¹ Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 176 f.).

förordningen. Direktivet gäller för den behandling av personuppgifter som sker hos en medlemsstats behöriga myndigheter i syfte att bl.a. förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. Detta innebär att det för vissa delar av de allmänna domstolarnas och de allmänna förvaltningsdomstolarnas verksamhet kommer att finnas restriktivare krav för behandling av känsliga personuppgifter än vad som enligt huvudregeln i den föreslagna dataskyddslagen gäller för myndigheters behandling i ärendehandläggningen.

16.5 Bedömning

Förslag: Uppgifter om en person ska inte få behandlas enbart på grund av vad som är känt om personen genom sådana särskilda kategorier av uppgifter som anges i artikel 9.1 i dataskyddsförordningen (känsliga personuppgifter).

Vid sökning i personuppgifter ska det vara förbjudet att använda sökbegrepp som avslöjar känsliga personuppgifter enligt artikel 9.1 i dataskyddsförordningen samt uppgifter om nationell anknytning eller uppgifter om brott eller misstanke om brott.

Bedömning: Dataskyddsförordningen innebär inte att det behövs någon nationell bestämmelse som ger domstolarnas rätt att behandla känsliga personuppgifter.

Domstolarna bör som huvudregel även fortsättningsvis få behandla känsliga personuppgifter i samma utsträckning som andra personuppgifter.

Utöver vad som framgår av våra förslag föranleder dataskyddsförordningen ingen ändring av domstolsdatalagens och domstolsdataförordningens bestämmelser om sökbegränsningar.

16.5.1 Rätten att behandla känsliga personuppgifter

Av artikel 9.2 f i dataskyddsförordningen framgår tydligt att domstolarna får behandla känsliga personuppgifter i sin dömande verksamhet. Vi anser att dataskyddsförordningens begrepp

dömande verksamhet innefattar all den personuppgiftsbehandling som sker i det enskilda målet eller ärendet från att detta anhängiggörs vid domstolen tills ett slutligt avgörande har meddelats. Vår bedömning innebär dock – trots den vida tolkningen av begreppet dömande verksamhet – att undantaget för dömande verksamhet inte omfattar vissa delar av den personuppgiftsbehandling som sker inom domstolsdatalagens tillämpningsområde (se vidare avsnitt 8.4).

Enligt artikel 9.2 f i dataskyddsförordningen gäller undantaget från förbudet att behandla känsliga personuppgifter emellertid även om behandlingen är nödvändig för att fastställa rättsliga anspråk. I tidigare förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 48) har detta undantag ansetts omfatta domstolarnas rättsskipande och rättsvårdande verksamhet i sin helhet.

Vi anser för vår del att det undantag som med störst säkerhet kan sägas omfatta domstolarnas hela rättsskipande och rättsvårdande verksamhet är undantaget för viktiga allmänna intressen i artikel 9.2 g i dataskyddsförordningen. Vi har i avsnitt 6.2.5 gjort bedömningen att hela domstolarnas rättsskipande och rättsvårdande verksamhet utgör en uppgift av allmänt intresse. I personuppgiftslagen har undantaget som rör viktiga allmänna intressen (artikel 8.4 i 1995 års dataskyddsdirektiv) utnyttjats bl.a. för att införa regleringen om behandling av känsliga personuppgifter för forsknings- och statistikändamål i 19 § PuL. Med stöd av samma bestämmelse har medlemsstaterna infört undantag för behandling av känsliga personuppgifter i myndigheters verksamhet, på bankområdet och för att främja jämställdhet och social trygghet.² Att även den uppgift av allmänt intresse som anförtrots domstolarna kan beskrivas som ”viktig” anser vi mot den bakgrunden vara tämligen självklart.

Artikel 9.2 g i dataskyddsförordningen innehåller vissa krav som måste vara uppfyllda för att undantaget ska bli tillämpligt. För det första ska det viktiga allmänna intresset framgå av unionsrätten eller medlemsstaternas nationella rätt. För det andra ska denna lagstiftning stå i proportion till det eftersträfvade syftet, vara förenlig med det väsentliga innehållet i rätten till dataskydd och

² Artikel 29-gruppens Advice paper on special categories of data (”sensitive data”), beslutat den 20 april 2011.

innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

Domstolarnas rättskipande och rättsvårdande uppgift är fastställd genom författning. Vad gäller de grundläggande principerna för personuppgiftsbehandling motsvarar dataskyddsförordningen till allra största delen 1995 års dataskyddsdirektiv. Mot den bakgrunden anser vi att det får förutsättas att den behandling av personuppgifter som sker inom ramen för domstolarnas rättskipande och rättsvårdande verksamhet är proportionerlig mot syftet med behandlingen och inte oförenlig med det grundläggande skyddet för personuppgifter. Genom domstolsdatalagen finns också bestämmelser som säkerställer skyddet för de registrerades integritet, t.ex. i form av behörighets- och sökbegränsningar.

Enligt domstolsdatalagens sekundära ändamålsbestämmelse får domstolarna vidarebehandla personuppgifter som redan finns i den rättskipande och rättsvårdande verksamheten genom att lämna ut dem. En förutsättning för detta är att uppgiftslämnandet sker i överensstämmelse med lag eller förordning. Även känsliga personuppgifter kan naturligtvis ingå bland de personuppgifter som enligt författning ska lämnas ut.

Den personuppgiftsbehandling som sker med stöd av domstolsdatalagens sekundära ändamålsbestämmelse kan enligt vår mening inte anses ske för att den är nödvändig i den dömande verksamheten eller för att fastställa rättsliga anspråk. Dock anser vi att undantaget i artikel 9.2 g i dataskyddsförordningen – viktigt allmänt intresse – är tillämpligt även för denna behandling av känsliga personuppgifter (se avsnitt 6.2.5). Vi har också gjort bedömningen att ett utlämnande av personuppgifter som sker i enlighet med lag eller förordning måste anses vara nödvändigt med hänsyn till ett viktigt allmänt intresse. Det får enligt vår mening vidare förutsättas att ett utlämnande av personuppgifter som föreskrivs i författning är proportionerligt mot syftet med utlämnandet och inte oförenligt med det grundläggande skyddet för personuppgifter. För det fall utlämnandet av känsliga uppgifter sker till annan myndighet finns också ett skydd för uppgifterna eftersom myndigheter enligt Dataskyddsutredningens förslag till dataskyddslag inte får använda sökbegrepp som avslöjar känsliga

personuppgifter. Även de enskilda myndigheternas registerförfattningar kan, precis som domstolsdatalagen, innehålla skyddsåtgärder i form av bl.a. sökbegränsningar eller behörighetsbegränsningar.

Sammanfattningsvis anser vi att samtliga de krav som ställts upp i artikel 9.2 g i dataskyddsförordningen för att känsliga personuppgifter ska få behandlas med hänsyn till ett viktigt allmänt intresse är uppfyllda för den personuppgiftsbehandling som sker i domstolarnas rättskipande och rättsvårdande verksamhet. Det samma gäller för den vidarebehandling av dessa personuppgifter som sker genom att de lämnas ut i överensstämmelse med lag eller förordning. Dataskyddsförordningen tillåter enligt vår mening därmed att känsliga personuppgifter behandlas på hela domstolsdatalagens tillämpningsområde. Någon nationell bestämmelse som ger domstolarnas rätt att behandla känsliga personuppgifter behövs enligt vår mening alltså inte.

16.5.2 Huvudregel för behandling av känsliga personuppgifter

Frågan är då om det i domstolsdatalagen ska införas en bestämmelse som reglerar under vilka övriga förutsättningar domstolarna får behandla känsliga personuppgifter. För det fall ingen bestämmelse införs görs ingen skillnad mellan känsliga personuppgifter och andra personuppgifter. Känsliga personuppgifter får då, liksom övriga personuppgifter, behandlas om det behövs för handläggningen av mål och ärenden eller om det behövs för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Detta framgår av domstolsdatalagens ändamålsbestämmelser.

Som framgår av avsnitt 5.3 anser vi inte att det finns något hinder mot att medlemsstaterna inför mer restriktiva bestämmelser för sina myndigheters personuppgiftsbehandling än vad som följer av dataskyddsförordningen. Vi bedömer därmed att det skulle finnas utrymme för att i domstolsdatalagen föreskriva att domstolarna endast får behandla känsliga personuppgifter i den rättskipande och rättsvårdande verksamheten om det är *absolut nödvändigt* med hänsyn till ändamålet med behandlingen. En sådan reglering skulle motsvara de krav på behandling av känsliga

personuppgifter som föreskrivs i artikel 10 i 2016 års dataskyddsdirektiv.

En reglering som innebär att känsliga personuppgifter får behandlas endast om det är absolut nödvändigt medför en särskild restriktivitet i användandet av dessa personuppgifter. Det tydliggör också att de känsliga personuppgifterna har ett särskilt skyddsvärde. Ett krav på ”absolut nödvändighet” kommer vidare, enligt förslaget till brottsdatalog, att gälla för stora delar av domstolarnas verksamhet.³ Ytterligare en fördel med ett krav på ”absolut nödvändighet” vore därmed att samma förutsättningar för behandling av känsliga personuppgifter skulle gälla för domstolarna hela kärnverksamhet. Risken för felbedömningar gällande en behandlings tillåtlighet skulle då troligtvis minska.

Huvudregeln för de myndigheter vars personuppgiftsbehandling inte kommer att styras av brottsdatalogen och dess kompletterande registerförfattningar kommer dock att vara att de får behandla känsliga personuppgifter i löpande text om uppgifterna har lämnats i ett ärende eller om de är *nödvändiga* för handläggning av ett ärende. Detta följer av Dataskyddsutredningens förslag till dataskyddslag.⁴ Hos domstolarna behandlas känsliga personuppgifter för närvarande till allra största delen i domar eller beslut. Detta sker i löpande text och de känsliga personuppgifter som återges i domen eller beslutet härrör i de allra flesta fall från vad parterna själva har anfört i processen. Hanteringen av känsliga personuppgifter hos domstolarna har därmed stora likheter med den ärendehantering som sker hos förvaltningsmyndigheterna och där huvudregeln ska vara att myndigheterna får behandla känsliga personuppgifter om det är nödvändigt.

Det är obligatoriskt för medlemsstaterna att genomföra 2016 års dataskyddsdirektiv. För den del av domstolarnas verksamhet som är direktivstyrd finns det således inte någon valmöjlighet gällande förutsättningarna att behandla känsliga personuppgifter. Det är vidare rimligt att exempelvis de allmänna domstolarna i sin brottmålshantering har samma begränsningar för behandlingen av känsliga personuppgifter som Åklagarmyndigheten.

³ Jfr Utredningen om 2016 års dataskyddsdirektivs delbetänkande (SOU 2017:29) och vårt avsnitt 4.3.

⁴ Se Dataskyddsutredningens betänkande (SOU 2017:39).

För de delar av domstolarnas verksamhet där personuppgiftsbehandlingen kommer att styras av dataskyddsförordningen är det enligt vår mening dock naturligare att känsliga personuppgifter behandlas enligt den huvudregel som ska gälla för de myndigheter som inte är ”direktivstyrda”.

De allmänna förvaltningsdomstolarna behandlar dessutom en mycket stor mängd känsliga personuppgifter inom ramen för sin målhantering. Samma sak gäller för vissa av de allmänna domstolarnas ärenden, t.ex. ärenden om adoption och förordnande av förvaltare eller god man. Dessa känsliga personuppgifter härrör främst från vad parterna själva anfört i målet eller ärenden. För de allmänna förvaltningsdomstolarna skulle det kunna innebära svårigheter om de inte får behandla känsliga personuppgifter i samma utsträckning som den förvaltningsmyndighet som fattat det överklagade beslutet eller lämnat in en ansökan som ska bedömas av domstolen. Man skulle dock kunna argumentera för att de känsliga personuppgifter som lämnats in av en part i det enskilda målet eller ärendet eller som härrör från den beslutande myndighetens akt är absolut nödvändiga för domstolen att behandla.

Som framgår av förarbetena till domstolsdatalagen (se avsnitt 16.2.1) finns det betänkligheter mot att införa bestämmelser som begränsar domarnas frihet att formulera domar på det sätt de anser lämpligt. Om känsliga personuppgifter får behandlas under samma förutsättningar som andra personuppgifter bidrar detta därmed till att upprätthålla domstolarnas självständighet.

Vi anser mot denna bakgrund att det i domstolsdatalagen inte bör införas bestämmelser som begränsar behandlingen av känsliga personuppgifter till situationer där det är absolut nödvändigt med hänsyn till ändamålet med behandlingen. Känsliga personuppgifter bör även fortsättningsvis som huvudregel få behandlas i samma utsträckning som andra personuppgifter.

16.5.3 Begränsning av behandling av känsliga personuppgifter

Av 13 § domstolsdatalagen framgår att känsliga personuppgifter inte får användas som enda grund för behandlingen av personuppgifter. Om en tjänsteman vid en domstol skulle behandla

personuppgifter på detta sätt utan att det behövs för handläggningen av mål och ärenden skulle behandlingen, även utan förtydligandet i 13 §, i och för sig vara oförenlig med domstolsdatalagen. Lagstiftaren har dock bedömt att det ändå finns anledning att tydliggöra denna begränsning. Mot den bakgrunden och då vi anser att dataskyddsförordningen inte hindrar en sådan bestämmelse är det vår bedömning att bestämmelsen ska finnas kvar.

Vilka personuppgifter som hänförs till kategorin känsliga personuppgifter har utökats genom dataskyddsförordningen. Numera ingår även sexuell läggning och genetiska uppgifter i begreppet. Även biometriska uppgifter för att entydigt identifiera en fysisk person har tillkommit.

Vi anser att det är en självklarhet att sexuell läggning bör omfattas av domstolsdatalagens bestämmelse. Det är vidare svårt att förutse hur den tekniska utvecklingen kommer att förändra möjligheten att behandla personuppgifter i domstolarnas verksamhetssystem. Vi gör därför bedömningen att även genetiska uppgifter samt biometriska uppgifter för att entydigt identifiera en fysisk person bör ingå i uppräkningslistan av de känsliga personuppgifter som inte får utgöra enda grund för behandlingen. Detta görs enligt vår mening lättast genom en hänvisning till artikel 9.1 i dataskyddsförordningen, där de känsliga personuppgifterna räknas upp. En sådan lagstiftningsteknik används även i Dataskyddsutredningens förslag till dataskyddslag. På detta sätt undviks också användningen av ordet *ras* i domstolsdatalagen, vilket är i överensstämmelse med det förslag som nyligen lämnats i betänkandet av Utredningen om transpersoners straffrättsliga skydd m.m. (SOU 2015:103 s. 165 ff.).

16.5.4 Sökbegränsningar

Vid domstolsdatalagens tillkomst identifierades ett antal sökbegrepp som bedömdes medföra särskilda integritetsrisker i domstolarnas verksamhet. Utöver känsliga personuppgifter handlar det om uppgifter om nationell anknytning och om brott eller misstanke om brott. Enligt huvudregeln i 14 § domstolsdatalagen är det förbjudet att använda sökbegrepp som avslöjar denna typ av

uppgifter. Genom de undantag som gjorts från förbudet och de tidsmässiga begränsningar som gäller för sökningar på vissa begrepp, måste lagstiftaren ha ansett att de samlade bestämmelserna om sökbegränsningar i domstolsdatalagen och domstolsdataförordningen utgör en rimlig avvägning mellan skyddet för den personliga integriteten och domstolarnas verksamhetsbehov.

Sökbegränsningar utgör en skyddsåtgärd i dataskyddsförordningens mening. Det finns inte någon bestämmelse i dataskyddsförordningen som föranleder ändring vad gäller förekomsten av sökbegränsningar för domstolarna.

Domstolarna behandlar stora mängder känsliga personuppgifter och det finns en möjlighet för allmänheten att med stöd av tryckfrihetsförordningen begära ut sammanställningar av känsliga personuppgifter, om en sådan sammanställning är tillåten att göra för domstolarnas tjänstemän. Utifrån dessa aspekter är det enligt vår mening önskvärt att behålla det skydd för känsliga personuppgifter som sökbegränsningarna utgör. Samma resonemang gäller naturligtvis för de övriga integritetskänsliga uppgifter som träffas av den nuvarande sökbegränsningen.

Även Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit sökbegränsningar för känsliga personuppgifter som en huvudregel för svenska myndigheter. En sökbegränsning för domstolarna skulle därmed följa denna huvudregel.

Nuvarande 14 § första stycket domstolsdatalagen, som anger vilka sökbegrepp som enligt huvudregeln är förbjudna, bör dock ändras med hänsyn till att det i dataskyddsförordningen har tillkommit kategorier av personuppgifter som ska anses vara känsliga. I detta fall görs ändringen enligt vår mening enklast genom en hänvisning till den paragraf i domstolsdatalagen, där det kommer att finnas en hänvisning till dataskyddsförordningens definition av begreppet känsliga personuppgifter (se avsnitt 16.5.3).

Vissa av domstolsdatalagens och domstolsdataförordningens bestämmelser om sökbegränsningar avser hur sökning av personuppgifter får utföras i de delar av verksamheten där personuppgiftsbehandlingen vid handläggning av mål och ärenden faller under brottsdatalagens tillämpningsområde. Ett exempel är 4 § domstolsdataförordningen, som endast gäller möjligheten att söka i personuppgifter i brottmål. Delar av domstolarnas personuppgifts-

behandling regleras emellertid av dataskyddsförordningen även om personuppgiftsbehandlingen primärt har behandlats för syften som ligger inom brottsdatalagens tillämpningsområde. Det gäller för utlämnande av personuppgifter enligt lag eller förordning som sker utanför brottsdatalagens tillämpningsområde, t.ex. i enlighet med tryckfrihetsförordningen, och för arkivering av personuppgifter (se avsnitt 9.2 och 19.4.4).

De sökbegränsningar som finns i domstolsdatalagen och domstolsdataförordningen i dag har ansetts vara ändamålsenliga för verksamheten. Genom att behålla samtliga dessa sökbegränsningar upprätthålls enligt vår mening integritetsskyddet vid den personuppgiftsbehandling som utförs vid de nyss nämnda utlämnandena och vid domstolarnas arkivering i all rättskipande och rättsvårdande verksamhet. I den mån sökbegränsningarna träffar personuppgiftsbehandlingen i exempelvis brottmål, kommer de att vara tillämpliga endast i de fall behandlingen inte sker med stöd av brottsdatalagen och dess kompletterande registerförfattning, såsom efter arkivläggning av handlingarna i ett mål.

Vi föreslår mindre språkliga anpassningar för de delar av 3–5 §§ domstolsdataförordningen som innehåller en tidsmässig begränsning för vissa sökbegrepp. Ändringarna föreslås endast för att göra bestämmelserna lättare att förstå och för att anpassa dem språkligt till våra övriga förslag. Någon materiell förändring är således inte avsedd.

Avslutningsvis vill vi tillägga att vi inom ramen för vårt uppdrag endast ska föreslå de förändringar i domstolsdatalagen och domstolsdataförordningen som behövs med anledning av dataskyddsförordningen. Eventuella tillämpningsproblem som föranleds av den nuvarande utformningen av dessa författningar ligger därmed utanför vårt uppdrag.

17 Elektroniskt utlämnande

17.1 Proportionalitetsbedömning

Utlämning på medium för automatiserad behandling och direktåtkomst utgör olika sätt att elektroniskt lämna ut uppgifter. I den mån utlämnandet innefattar personuppgifter utgör det en behandling av personuppgifter i dataskyddsförordningens mening.

Dataskyddsförordningen saknar, liksom 1995 års dataskyddsdirektiv, särskilda bestämmelser om elektroniskt utlämnande. Upplivsningvis kan sägas att skäl 31 till dataskyddsförordningen innehåller en skrivning om att ”offentliga myndigheters begäranden om att uppgifter ska lämnas ut alltid ska vara skriftliga och motiverade, läggas fram i enskilda fall och inte gälla hela register eller leda till att register kopplas samman”. Tagen ur sitt sammanhang skulle skrivningen kunna tolkas som ett hinder mot att etablera direktåtkomst mellan myndigheter. Den förekommer dock i samband med ett resonemang om vem som definitionsmässigt ska betraktas som mottagare av personuppgifter i dataskyddsförordningens mening och – indirekt – om möjligheten att göra undantag från viss informationsskyldighet gentemot registrerade.¹ Vi anser inte att skrivningen ska ges någon betydelse utanför detta mycket begränsade sammanhang.²

Enligt artikel 24.1 och artikel 32 i dataskyddsförordningen ska den personuppgiftsansvarige dock genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa att behandlingen utförs i enlighet med förordningen och att en lämplig säkerhetsnivå säkerställs. Enligt artikel 5.1 a i förordningen måste en personuppgiftsbehandling vidare alltid vara korrekt (skälig och rimlig) i

¹ Jfr artikel 4.9 samt 13.1 e, 14.1 e, 15.1 c och 30.1 d i dataskyddsförordningen.

² Motsatt uppfattning har dock redovisats i eSamverkansprogrammets vägledning ”Elektroniskt informationsutbyte – en vägledning för utlämnande i elektronisk form” s. 22.

förhållande till den registrerade. För att säkerställa att behandlingen av en personuppgift är skäligen i förhållande till den registrerade ska det för varje behandling göras en proportionalitetsbedömning. I den bedömningen vägs behovet av den konkreta behandlingen mot den registrerades intresse av personlig integritet. En behandling av personuppgifter som innebär risker för den personliga integriteten får då genomföras endast om fördelarna med behandlingen står i rimlig proportion till riskerna. Säkerhetsåtgärder som minskar riskerna för den personliga integriteten har här stor betydelse.³

Rent allmänt kan nämnas att ett elektroniskt utlämnande av uppgifter anses medföra en större risk för otillbörliga integritetsintrång, eftersom det ger en större möjlighet att bearbeta och sprida informationen jämfört med ett utlämnande som sker i pappersform.⁴ Detta måste beaktas i den proportionalitetsbedömning som ska göras.

17.2 Utlämnande på medium för automatiserad behandling

17.2.1 Domstolsdatalagen och tidigare förarbeten

Ett utlämnande på medium för automatiserad behandling kan göras exempelvis genom att information förs över via e-post, lämnas ut på ett flyttbart lagringsmedium som ett usb-minne eller förs över från ett datorsystem till ett annat.⁵ Enligt 16 § första stycket domstolsdatalagen får personuppgifter lämnas ut på medium för automatiserad behandling om det inte är olämpligt. Av bestämmelsens andra stycke framgår att regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter på medium för automatiserad behandling.

³ Samma krav gäller enligt artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, Europarådets konvention om skydd för enskilda vid automatiska databehandling av personuppgifter, nr 108, samt artikel 7 och 8 i EU:s stadga om de grundläggande rättigheterna (2010/C 83/02), jfr Datainspektionen Vägledning för integritetsanalys, september 2016 och Integritetsskyddskommitténs betänkande (SOU 2007:22 s. 449 f.).

⁴ Jfr departementspromemorian med förslag till domstolsdatalag (Ds 2013:10 s. 119 f.).

⁵ Jfr förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 75).

Domstolsdataförordningen innehåller inga materiella bestämmelser om möjligheten att lämna ut uppgifter på detta sätt. Domstolsverket har emellertid, enligt 14 § andra stycket 2 domstolsdataförordningen, möjlighet att meddela föreskrifter om begränsning av möjligheterna att lämna ut personuppgifter på medium för automatiserad behandling. Domstolsverket har ännu inte utnyttjat denna möjlighet.

I förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 75 ff.) har regeringen sammanfattningsvis gjort följande bedömning av domstolarnas behov av att lämna ut personuppgifter på medium för automatiserad behandling.

Skälen till att domstolarna behöver ha möjlighet att lämna ut uppgifter på medium för automatiserad behandling är flera. Det är dels en förutsättning för att domstolarna ska kunna använda elektroniska akter, för att RIF-samarbetet ska fungera, för att rätten till partsinsyn ska få ett reellt innehåll och för att kommunikering med parter och deras ombud, biträden eller försvarare ska vara effektiv. Möjligheten likställer även enskilda parter med myndigheter som är part, eftersom myndigheterna har tillgång till stora delar av processmaterialet elektroniskt. Det bidrar även till att effektivisera utlämnandet av uppgifter till andra än parterna, t.ex. i enlighet med offentlighetsprincipen. Det skulle ta stora resurser i anspråk för domstolarna om deras möjlighet att lämna ut domar m.m. genom e-post skulle begränsas. Domstolarnas verksamhet präglas vidare av offentlighet i stora delar. Det finns ett stort intresse och behov av insyn och transparens i domstolarnas dömande makt. Möjligheten att få tillgång till domstolhandlingar i elektroniskt format är väsentlig för hur transparent verksamheten blir i praktiken och hur effektiv granskningen kan vara.

Regeringen konstaterar vidare att de risker som finns med ett utlämnande på medium för automatiserad behandling är att det är lättare för mottagaren att sammanställa eller sprida uppgifterna om de lämnas ut elektroniskt. En bestämmelse som innebär att sådant utlämnande får ske endast om det inte är olämpligt innebär att personuppgifternas art, struktur och antal ska beaktas i varje enskilt fall. Personuppgifternas känslighet och säkerheten vid överföringen ska vägas in i denna bedömning. Bestämmelsen innebär att domstolen vid utlämnande ska agera med försiktighet

och med respekt för berördas integritet. Lämplighetsprövningen ser naturligtvis olika ut beroende på om det exempelvis är en myndighet eller en enskild person som är mottagare.

17.2.2 Bedömning

Bedömning: Dataskyddsförordningen föranleder ingen ändring av bestämmelsen om utlämnande av personuppgifter på medium för automatiserad behandling eller regeringens och Domstolsverkets föreskriftsrätt på det området.

Enligt 16 § domstolsdatalagen får personuppgifter lämnas ut på medium för automatiserad behandling om det inte är olämpligt. Utgångspunkten är således att ett sådant utlämnande är tillåtet. Mot bakgrund av det stora behov av att lämna ut uppgifter på detta sätt som redovisas av tidigare förarbeten, anser vi att detta är en rimlig utgångspunkt. Bestämmelsen innebär dock att domstolarna vid varje utlämnande måste göra en proportionalitetsbedömning där den enskildes integritetsskydd vägs mot de fördelar som finns med att lämna ut uppgifter på detta sätt.

Inom domstolsdatalagens tillämpningsområde handläggs mål och ärenden av mycket olika karaktär. Därmed varierar också den typ av personuppgifter som behandlas och behovet av integritetsskydd. Det är därför enligt vår mening mest ändamålsenligt att den proportionalitetsbedömning som ska göras vid ett utlämnande av personuppgifter via exempelvis e-post sker utifrån omständigheterna i det enskilda fallet. Detta bör också vara i överensstämmelse med dataskyddsförordningens princip om korrekthet i artikel 5.1 a. Det har inte heller framkommit att det skulle finnas något problem med nuvarande reglering i den delen.

Nuvarande bestämmelser ger också regeringen och Domstolsverket möjlighet att vid behov ytterligare specificera innebörden av bestämmelsen i 16 § domstolsdatalagen. På detta sätt kan skyddet för den personliga integriteten ytterligare stärkas om det skulle visa sig behövas. I avsnitt 20.2 gör vi bedömningen att dataskyddsförordningen inte hindrar att bestämmelser om personuppgiftsbehandling införs i en förordning eller i en myndighetsföreskrift, så länge föreskrifterna tillkommit i laga ordning.

Mot denna bakgrund anser vi att domstolsdatalagens bestämmelse om utlämnande av personuppgifter på medium för automatiserad behandling är förenlig med dataskyddsförordningen och bör finnas kvar oförändrad. Detsamma gäller regeringens och Domstolsverkets föreskriftsrätt på området.

17.3 Direktåtkomst

17.3.1 Innebörden av direktåtkomst

Direktåtkomst innebär att uppgifter, däribland personuppgifter, elektroniskt görs tillgängliga för en mottagare utanför myndigheten. Högsta förvaltningsdomstolen ansåg i rättsfallet HFD 2015 ref. 61 att det avgörande för om en direktåtkomst kan anses föreligga är om upptagningen redan i och med möjligheten att ta del av den kan anses förvarad hos den mottagande myndigheten i den mening som avses i 2 kap. 3 § tryckfrihetsförordningen. Enligt denna bestämmelse är så fallet om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas (se vidare avsnitt 21.2).

Informationshanteringsutredningen har i sitt betänkande med förslag till ny myndighetsdatalag gjort följande sammanfattning av begreppet direktåtkomst (SOU 2015:39 s. 121 ff.).

Med direktåtkomst avses vanligtvis att någon har direkt tillgång till någon annans register eller databas och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen (se bl.a. prop. 2009/10:85 s. 168). I begreppet ligger också att den som är personuppgiftsansvarig för registret eller databasen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst söktillfälle tar del av (prop. 2011/12:45 s. 133). Den myndighet som lämnar ut uppgifter genom direktåtkomst fattar således inte något beslut om utlämnande av de uppgifter som den som har direktåtkomst tar del av i varje enskilt fall. I förarbetena till 11 kap. 4 § OSL, som alltså reglerar överföring av sekretess vid direktåtkomst, uttalade sig regeringen om hur direktåtkomst bör definieras (prop. 2007/08:160 s. 164). Med en sådan åtkomst avsågs enligt regeringen att en upptagning är tillgänglig hos den mottagande myndigheten på ett sådant sätt som avses i 2 kap. 3 § andra stycket första meningen TF, dvs. upptagningen ska vara tillgänglig med tekniska hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. /.../ Den omständigheten

att direktåtkomst till en viss mängd uppgifter innebär att de handlingar i vilka uppgifterna ingår anses expedierade till den mottagande myndigheten medför alltså i sin tur att handlingarna är att anse som förvarade, och därmed också som huvudregel som inkomna, hos den myndigheten i den mening som avses i 2 kap. 3 och 6 §§ TF. Handlingarna utgör genom direktåtkomsten således allmänna handlingar även hos den mottagande myndigheten. En direktåtkomst till sekretessreglerade uppgifter innebär vidare att det krävs en sekretessbrytande regel för att utlämnandet av uppgifterna inte ska innebära ett brott mot den sekretess som annars gäller.

Direktåtkomst innebär således ett elektroniskt utlämnande, som kan omfatta bland annat personuppgifter. Jämfört med ett elektroniskt utlämnande av uppgifter som sker efter en ”manuell” förfrågan är direktåtkomsten emellertid mycket mer omfattande. Den mottagande myndigheten tillåts ju söka fritt i den informationssamling som direktåtkomsten avser och samtliga handlingar som omfattas av direktåtkomsten anses ha expedierats i samma ögonblick som direktåtkomsten upprättas.⁶

Integritetsriskerna med direktåtkomst består således i att den mottagande myndigheten på egen hand får söka bland all information som finns i den aktuella informationssamlingen utan att den utlämnande myndigheten har kontroll över vilka uppgifter som lämnas ut. Direktåtkomsten kan också ge möjlighet för personal på den mottagande myndigheten att hämta hem informationen till sitt eget system och bearbeta den där.⁷ Vidare innebär direktåtkomst att den mottagande myndigheten kan vara skyldig att i enlighet med offentlighetsprincipen lämna ut de personuppgifter som omfattas av direktåtkomsten. Givetvis gäller detta med den begränsning som föreskrivs i offentlighets- och sekretesslagen.

Det bör vidare nämnas att offentlighetsprincipen också omfattar uppgifter som ännu inte sammanställts hos en myndighet, men som kan sammanställas med hjälp av tillgänglig teknik och rutinbetonade åtgärder. En sökning är ett exempel på en sådan rutinbetonad åtgärd. Om direktåtkomst tillåter den mottagande myndigheten att göra en viss sökning i värmyndighetens databas, måste den mottagande myndigheten således göra en sökning och

⁶ Jfr Informationshanteringsutredningens betänkande (SOU 2015:39 s. 136).

⁷ Jfr prop. 2007/08:160 s. 56.

lämna ut de uppgifter sökningens resulterar i om den har fått en begäran om att lämna ut en sammanställning av åtkomliga uppgifter i enlighet med tryckfrihetsförordningen.

17.3.2 Domstolsdatalagen

Den yttre ramen för den direktåtkomst som är tillåten i domstolarnas rättskipande och rättsvårdande verksamhet framgår av 17 § domstolsdatalagen. Enligt denna bestämmelse får direktåtkomst endast medges en allmän domstol, en allmän förvaltningsdomstol, en hyres- och arrendenämnd samt en part eller partens ombud, biträde eller försvarare. Direktåtkomst som medges part, parts ombud, biträde eller försvarare får endast avse personuppgifter i partens mål eller ärende.

För att skapa en reglering som är ändamålsenlig över tid framgår av 17 § tredje stycket domstolsdatalagen att regeringen har möjlighet att meddela ytterligare föreskrifter om begränsning av direktåtkomst och om behörighet och säkerhet vid sådan åtkomst.⁸ Regeringen har även möjlighet att vidaredelegera föreskriftsrätt till myndighet i denna del.

Regeringen har utnyttjat sin föreskriftsrätt genom att i 7–13 §§ domstolsdataförordningen reglera i vilka fall direktåtkomst får förekomma. Sammanfattningsvis innebär dessa bestämmelser följande.

Direktåtkomst får endast ges vid överklagande, till rättspraxis och i samband med beredskapsverksamhet. För närvarande är det således inte tillåtet för domstolarna att bevilja parter, deras ombud, biträden och försvarare direktåtkomst. För de allmänna förvaltningsdomstolarna kommer samtliga domstolsdataförordningens bestämmelser om direktåtkomst att börja tillämpas först den 1 januari 2018.

Vid överklagande får direktåtkomst ges både från underrätt till överrätt och från överrätt till underrätt. Direktåtkomst vid överklagande avser inte bara domar och beslut utan även de personuppgifter som kan vara registrerade i domstolarnas verksamhetsstöd i de enskilda målen eller ärendena. I mål där särskilda

⁸ Se förarbetena till domstolsdatalagen(prop. 2014/15:148 s. 68 f.).

rättsmedel åberopas ges samma möjlighet till direktåtkomst som vid överklagande. Direktåtkomst vid överklagande (och särskilda rättsmedel) har en tidsmässig begränsning genom att den endast är tillåten under sex månader efter det att domen eller beslutet fick laga kraft.

Direktåtkomst till domar och beslut för rättspraxis får ges från överrätterna i de allmänna förvaltningsdomstolarna till underrätterna i samma domstolskedja. På samma sätt får överrätterna i de allmänna domstolarna ge direktåtkomst till underrätterna i den domstolskedjan. Denna möjlighet utnyttjas dock inte av de allmänna domstolarna i dag. I 11 § domstolsdataförordningen finns vidare en uppräknig av vilka uppgifter utöver domar och beslut som direktåtkomst för rättspraxis får avse. Direktåtkomst till rättspraxis har en tidsmässig begränsning som innebär att tillgång endast är tillåten under 20 år efter det att domen eller beslutet fick laga kraft.

Vid beredskapsverksamhet behöver domstolar som samarbetar kunna behandla personuppgifter i de aktuella målen hos de andra domstolarna på samma sätt som i mål som handläggs vid den egna domstolen. Direktåtkomsten vid sådan verksamhet ger tillgång till de personuppgifter som *behövs* för handläggningen av de aktuella målen. Inom ramen för beredskapsverksamheten prövas vissa frågor som ligger inom ramen för dataskyddsförordningens tillämpningsområde, t.ex. vissa frågor om kontaktförbud avseende gemensam bostad.⁹

Domstolsverket får, enligt 14 § andra stycket 3 domstolsdataförordningen, meddela ytterligare föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter genom direktåtkomst och om behörighet och säkerhet vid sådant utlämnande. Några sådana föreskrifter finns för närvarande inte.

17.3.3 Tidigare förarbeten

I förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 67 ff.) gjorde regeringen en avvägning av behovet av direktåtkomst mellan

⁹ Se 1 § förordning (1988:31) om tingsrätternas beredskap för prövning av häktningsfrågor m.m. samt Utredningen om 2016 års dataskyddsdirektivs delbetänkande (SOU 2017:29 s. 212).

domstolarna och skyddet för den enskildes integritet. Sammanfattningsvis framgår här följande.

Direktåtkomst mellan domstolarna är av stor betydelse för att domstolarna ska kunna bedriva sitt arbete rättssäkert och effektivt. Som exempel nämns bland annat en effektiv återanvändning av personuppgifter hos överrätten när mål har överklagats, möjligheten för överrätten att i ett överklagat mål ta del av ljud- och bildupptagningar som lagras elektroniskt i underrättens datorsystem och möjligheten att söka bland avgöranden från en annan domstol i syfte att främja en enhetlig rättstillämpning och effektiv handläggning. Det finns således flera verksamhetsmässiga fördelar med direktåtkomst mellan domstolar. Domstolsdatalagen bör därför inte förhindra ett utlämnande av uppgifter genom direktåtkomst.

Regeringen anförde dock även att de integritetsrisker som kan vara förknippade med direktåtkomst måste bemästras och gjorde följande bedömning. Integritetsriskerna består i att personuppgifter blir tillgängliga vid flera domstolar samtidigt. En viktig utgångspunkt för regleringen är därför att den direktåtkomst som tillåts inte blir mer omfattande än vad som är motiverat. Direktåtkomsten bör alltså anpassas efter de olika behov som finns i domstolarnas verksamhet och som kan försvaras ur ett integritetsperspektiv. Den bör noggrant anpassas efter behoven och begränsas både beträffande vilka kategorier av uppgifter som omfattas och vilka domstolar som ska kunna ha direktåtkomst till dessa kategorier av uppgifter.

Vad gäller direktåtkomst mellan domstolar anförde regeringen följande. Samma skydd kommer att gälla i alla led hos både avsändar- och mottagardomstolen eftersom båda domstolarna omfattas av domstolsdatalagen och tillhörande domstolsdataförordning. Av 11 kap. 4 § OSL följer att den sekretess som gäller hos den utlämnande domstolen automatiskt förs över till den mottagande domstolen. Den överförda sekretessen blir dock, enligt 11 kap. 8 § OSL, i vissa fall inte lika stark hos den mottagande domstolen. Av integritetsskyddsskäl bör den tillåtna omfattningen av direktåtkomsten vara så preciserad som möjligt med avseende på vilka domstolar som kan tillåtas ha direktåtkomst till vilka personuppgifter. Behoven ser olika ut beroende på vilket behov som föranleder direktåtkomst. Behoven varierar även över tid och

är bl.a. beroende av hur domstolarnas inre och yttre organisation utformas, arbetsrutiner, målsammansättningen i domstolarna och forumregler. Mot den bakgrunden bör den närmare regleringen om direktåtkomst meddelas av regeringen i förordning. För att åstadkomma en restriktiv ram för direktåtkomst bör huvudregeln enligt förordningsbestämmelserna vara att direktåtkomst är förbjuden utom i de fall som specificeras i förordning.

17.3.4 Bedömning

Förslag: Dataskyddsförordningen föranleder ingen ändring av domstolsdatalagens och domstolsdataförordningens bestämmelser om direktåtkomst.

Enligt domstolsdatalagens och domstolsdataförordningens bestämmelser är direktåtkomst tillåten vid överklagande, för rättspraxis och vid beredskapsverksamhet. Domstolsdatalagen ger också en möjlighet för domstolarna att ge parter och deras ombud, biträden och försvarare direktåtkomst, vilket för närvarande dock inte är tillåtet enligt domstolsdataförordningen.

Om en direktåtkomst innefattar personuppgifter innebär den också en behandling av personuppgifter. För den avsändande domstolen består personuppgiftsbehandlingen av att den lämnar ut personuppgifter och för den mottagande domstolen av att den samlar in dem.

Vi vill inledningsvis påpeka att vi anser att den direktåtkomst som är tillåten enligt domstolsdatalagen och de kompletterande reglerna i domstolsdataförordningen är förenlig med domstolsdatalagens ändamål. Enligt ändamålsbestämmelsen i 6 § domstolsdatalagen får personuppgifter behandlas för handläggning av mål och ärenden. Som framgår av avsnitt 9.1.2 ska ändamålsbestämmelsen ges en vid innebörd, vilket innebär att det är mål- och ärendehandläggningen i stort som avses. Om en part får tillgång till uppgifter i ett pågående mål eller ärende genom direktåtkomst sker detta inom ramen för handläggningen av det enskilda målet eller ärendet. En överrätt som bereder sig tillgång till de personuppgifter som underrätten har registrerat i ett mål som överklagats gör detta för att kunna handlägga det överklagade målet

på ett rättsäkert sätt. Den underrätt som har avgjort ett mål som överklagats har behov av att bevaka målets handläggning i överrätten och målets utgång för att utvärdera den handläggning och de bedömningar i rättsfrågor som gjorts i det enskilda målet. Underrätterna behöver vidare tillgång till överrätternas avgöranden för att hålla sig uppdaterade gällande rättspraxis, vilket är en förutsättning för en rättsäker hantering av framtida mål och ärenden. Avslutningsvis har naturligtvis de domstolar som deltar i beredskapsverksamhet behov av tillgång till personuppgifter i de mål som beredskapen avser, för att kunna fatta beslut och meddela dom i det enskilda målet. Det bör i detta sammanhang påpekas att det vid direktåtkomst mellan domstolar åligger den mottagande domstolen att se till att dess tjänstemän endast bereder sig tillgång till de personuppgifter de *behöver* för handläggningen av mål och ärenden. Detta är dock en bedömning som måste göras i varje enskilt fall.

Direktåtkomst regleras inte uttryckligen vare sig i 1995 års dataskyddsdirektiv eller i dataskyddsförordningen. Precis som enligt 1995 års dataskyddsdirektiv är dock en av grundprinciperna för personuppgiftsbehandlingen enligt dataskyddsförordningen att behandlingen ska vara korrekt i förhållande till den registrerade. Korrektheten innefattar att behandlingen ska vara rimlig eller skälig. Vid bedömningen av om en viss direktåtkomst mellan domstolar är förenlig med dataskyddsförordningen måste man således göra en avvägning mellan å ena sidan de effektivitetsvinster och andra fördelar som direktåtkomsten medför för de inblandade domstolarna och parterna och å andra sidan de risker den innebär för den enskildes integritet. För att direktåtkomst ska vara tillåten måste det efter en sådan proportionalitetsbedömning konstateras att fördelarna med behandlingen står i rimlig proportion till riskerna. Av betydelse är också vilka säkerhetsåtgärder som kan vidtas för att minska riskerna för den personliga integriteten.

Dataskyddsförordningens krav på proportionalitet är inte något nytt. Samma principer gäller enligt 1995 års dataskyddsdirektiv. Vid tillkomsten av domstolsdatalagen måste regeringen därför ha gjort bedömningen att fördelarna med den direktåtkomst som tillåts enligt lagen och tillhörande förordning står i rimlig proportion till riskerna. I förarbetena till domstolsdatalagen

redogörs också för den stora nytta – både för verksamheten och för rättssäkerheten – som följer av direktåtkomst.

Vad gäller integritetsriskerna kan sägas att det är oundvikligt att direktåtkomsten avser ett stort antal fysiska personers personuppgifter eftersom domstolsdatalagen reglerar personuppgiftsbehandlingen hos alla allmänna domstolar, alla allmänna förvaltningsdomstolar och alla hyres- och arrendenämnder. Det ligger vidare i det rättskipande och rättsvårdande uppdragets natur att de personuppgifter som behandlas till stor del är av ett känsligt slag. Samtidigt präglas domstolsförfarandet av en stor öppenhet, där exempelvis domar och beslut som absolut huvudregel är offentliga.

Som framgår ovan gäller vid direktåtkomst samma regler för behandlingen av personuppgifter för den mottagande domstolen som för ”värddomstolen” eftersom de båda omfattas av domstolsdatalagen och domstolsdataförordningen. Detta innebär att det skydd i form av ändamålsbegränsningar, behörighetsbegränsningar och sökbegränsningar som finns för personuppgifterna hos värddomstolen även finns hos den mottagande domstolen. Ändamålsbegränsningen och behörighetsbegränsningen säkerställer att tjänstemän på den mottagande domstolen endast behandlar de personuppgifter som behövs för arbetsuppgifterna. Sökbegränsningarna innebär ett skydd mot att de anställda på domstolen för egen del gör sökningar som inte är tillåtna. De bidrar dessutom till att de anställda inte får ta fram och sammanställa personuppgifter utifrån de förbjudna sökbegreppen efter begäran från allmänheten, vilket är av minst lika stor betydelse ur integritetssynpunkt. Enligt 11 kap. 4 § OSL förs vidare den sekretess som gäller hos värddomstolen över till den mottagande domstolen vid direktåtkomst. Samtliga dessa omständigheter bidrar till att minska integritetsriskerna för den enskilde.

Mot bakgrund av det skydd för den enskildes integritet som domstolsdatalagen och offentlighets- och sekretesslagen innebär och med hänsyn till att en avsaknad av direktåtkomst skulle innebära stora effektivitets- och rättsäkerhetsförluster, anser också vi att fördelarna med den tillåtna direktåtkomsten överväger de nackdelar i integritetshänseende som den medför. Någon anledning att på grund av dataskyddsförordningen ändra domstolsdatalagens

och domstolsdataförordningens bestämmelser i denna del finns därmed inte.

För det fall direktåtkomsten blir för omfattande kan detta dock utgöra ett problem ur ett integritetsperspektiv. Exempelvis kan en handling i ett mål hos en överrätt – som en underrätt har tillgång till med stöd av 9 § domstolsdataförordningen (direktåtkomst vid överklagande) – begäras ut hos underätten med stöd av tryckfrihetsförordningen. Detta får till följd att underätten måste göra en sekretessprövning av handlingar som finns i överrättens mål. Av lätt förståeliga skäl är detta inte en lämplig ordning. Av bland annat denna anledning måste ett noggrant övervägande kring vilka handlingar som rent tekniskt ska kunna nå genom direktåtkomst göras.¹⁰ Detta är emellertid inte en fråga som det ankommer på oss att utreda.

¹⁰ Det bör framhållas att det krävs en sekretessbrytande bestämmelse för att en domstol – genom direktåtkomst eller på annat sätt – ska få föra över annars sekretessbelagda uppgifter till en annan domstol.

18 Överklagandebestämmelser

18.1 Domstolsdatalagen

Enligt 19 § domstolsdatalagen får tillsynsmyndighetens beslut enligt den lagen eller enligt de bestämmelser i personuppgiftslagen som anges i 5 § domstolsdatalagen om annat än föreskrifter, överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

Innebörden av 19 § domstolsdatalagen är att de beslut som tillsynsmyndigheten fattat i enlighet med 32, 44 och 45 §§ PuL kan överklagas.¹ De sistnämnda bestämmelserna reglerar tillsynsmyndighetens rätt att fatta beslut om säkerhetsåtgärder och om förbud av behandling av personuppgifter. Bestämmelsen i 19 § domstolsdatalagen har utformats på samma sätt som motsvarande överklagandebestämmelse i 51 § PuL, med den skillnaden att tillsynsmyndigheten vid beslut som riktas mot domstolarna inte får bestämma att dess beslut ska gälla även om de överklagas.

Av 14 § andra stycket lagen (1971:289) om allmänna förvaltningsdomstolar följer att Förvaltningsrätten i Stockholm är behörig att pröva ett överklagande från en domstol som görs med stöd av 19 § domstolsdatalagen. Detta gäller även överklaganden som görs av exempelvis Högsta förvaltningsdomstolen eller Förvaltningsrätten i Stockholm. Regeringen har i förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 95) gjort bedömningen att det inte behövs någon särskild forumregel för överklaganden som görs av domstolarna i dess egenskap av personuppgiftsansvariga.

Enligt 20 § första stycket domstolsdatalagen får en hovrätts, tingsrätts eller förvaltningsrätts beslut om upplysningar till

¹ Jfr förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 94).

allmänheten enligt 12 § samma lag överklagas till kammarrätten. Detsamma gäller en hovrätts, tingsrätts eller förvaltningsrätts beslut om information till den registrerade enligt 26 § PuL eller om rättelse och underrättelse till tredje man enligt 28 § PuL. Av bestämmelsen framgår vidare att en kammarrätts beslut i dessa frågor får överklagas till Högsta förvaltningsdomstolen samt att Högsta domstolens och Högsta förvaltningsdomstolens beslut i dessa frågor inte får överklagas.

Beträffande vilka beslut som får överklagas motsvarar 20 § domstolsdatalagen i princip vad som gäller enligt 52 § PuL. Av förarbetena till den sistnämnda bestämmelsen (prop. 2005/06:173 s. 51 f.) framgår att möjligheten att överklaga de beslut som myndigheter fattar i sin egenskap av personuppgiftsansvariga inte har sin grund i 1995 års dataskyddsdirektiv, utan motiveras av allmänna förvaltningsrättsliga principer om att förvaltningsbeslut som direkt berör en enskild person ska kunna överprövas av domstol.

Av 21 § domstolsdatalagen framgår att en hyres- och arrendenämnds beslut i de frågor som avses i 20 § första stycket får överklagas till allmän förvaltningsdomstol och att prövnings-tillstånd krävs vid överklagande till kammarrätten.

Vad gäller forumreglerna vid ett överklagande framgår följande av förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 93 f.).

För att förvaltningsrätterna inte ska behöva överpröva sina egna eller högre instansers beslut har det i Vera-förordningarna införts en avvikande instansordning i fråga om överklagande av domstolarnas beslut. Enligt dessa förordningar gäller att förvaltningsrätts beslut överklagas till kammarrätt, kammarrätts beslut till Högsta förvaltningsdomstolen och att tingsrätts och hovrätts beslut överklagas till kammarrätt. Det är också vad som gäller för beslut om utlämnande av handling i domstolarnas administrativa verksamhet enligt offentlighets- och sekretesslagen (6 kap. 8 § offentlighets- och sekretesslagen [2009:400]). Den nu redovisade instansordningen framstår som ändamålsenlig och bör gälla även vid överklagande av beslut enligt domstolsdatalagen. De beslut som är överklagbara utgör administrativa beslut i respektive domstol. Kammarrätten kommer därmed i realiteten att vara första domstolsinstans. Mot den angivna bakgrunden och i enlighet med vad som gäller enligt Vera-förordningarna bör det därför inte gälla något krav på prövnings-tillstånd vid överklagande till kammarrätt. Högsta domstolen är högsta allmänna domstol och Högsta förvaltningsdomstolen är högsta förvaltningsdomstol (11 kap. 1 § regeringsformen). Av detta följer att

dessa domstolars avgöranden inte kan överklagas. Högsta domstolens och Högsta förvaltningsdomstolens egna beslut enligt domstolsdatalagen bör därför inte kunna överklagas. Detta överensstämmer med vad som gäller enligt offentlighets- och sekretesslagen och Veralförordningarna. När det gäller beslut som meddelas av en hyres- eller arrendenämnd finns det inte skäl att avvika från den vanliga ordningen för överklagande av förvaltningsbeslut.

Av 22 § första stycket domstolsdatalagen framgår att andra beslut än sådana som avses i 19–21 §§ samma lag eller i 47 § PuL inte får överklagas. Av andra stycket framgår att det krävs prövningstillstånd vid överklagande till kammarrätten av förvaltningsrättens beslut i frågor som avses i 47 § PuL.

I 47 § PuL behandlas tillsynsmyndighetens rätt att hos förvaltningsrätt ansöka om att personuppgifter som har behandlats på ett olagligt sätt ska utplånas. Bestämmelsen gäller även inom domstolsdatalagens tillämpningsområde genom en hänvisning i 5 § första stycket 10. Genom 22 § domstolsdatalagen förtydligas att en förvaltningsrätts dom i frågor som gäller 47 § PuL kan överklagas enligt förvaltningsprocesslagen (1971:291) på samma sätt som förvaltningsrätternas domar i allmänhet. I personuppgiftslagen finns motsvarande bestämmelse i 53 §.²

18.2 Dataskyddsförordningen och stadgan

Artikel 78 i dataskyddsförordningen reglerar rätten till ett effektivt rättsmedel mot tillsynsmyndighetens beslut. Här framgår att varje fysisk eller juridisk person har rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut som meddelats av en tillsynsmyndighet rörande dem (punkt 1). Det framgår också att varje registrerad person har rätt till ett effektivt rättsmedel om den behöriga tillsynsmyndigheten inte behandlar ett klagomål. Detsamma gäller om tillsynsmyndigheten inte informerar den registrerade inom tre månader om hur arbetet med det klagomål som getts in fortskrider eller vilket beslut som har fattats med anledning av klagomålet (punkt 2). Att det är ett domstolsförfarande som avses i punkterna 1 och 2 förstås av punkten 3. Här framgår att talan mot

² Jfr förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 95).

en tillsynsmyndighet ska väckas vid domstolarna i den medlemsstat där myndigheten har sitt säte.

Enligt artikel 79.1 i dataskyddsförordningen har alla registrerade rätt till ett effektivt rättsmedel om de anser att deras rättigheter enligt förordningen har åsidosatts som en följd av att deras personuppgifter har behandlats på ett sätt som inte är förenligt med förordningen. Enligt bestämmelsen gäller detta utöver rätten att lämna in ett klagomål till tillsynsmyndigheten. Om den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet som agerar inom ramen för sin myndighetsutövning ska sådan talan, enligt artikel 79.2, väckas vid domstolarna i den medlemsstat där den personuppgiftsansvarige – eller personuppgiftsbiträdet – är etablerad.

Den registrerade har vidare, enligt artikel 82 i dataskyddsförordningen, rätt till skadestånd vid överträdelser av förordningens bestämmelser. Denna rättighet behandlar vi i avsnitt 15.7.

Rätten till ett effektivt rättsmedel garanteras även av Europeiska unionens stadga om de grundläggande rättigheterna. Denna rätt, som kommer till uttryck i artikel 47 i stadgan, omfattar de rättigheter som garanteras av unionsrätten. Vad gäller personuppgiftsbehandling ger artikel 8.1 i stadgan var och en rätt till skydd av sådana uppgifter som rör honom eller henne. Som en konkretisering av denna rättighet anges i artikel 8.2 att personuppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av en legitim och lagenlig grund. Var och en har dessutom rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dessa uppgifter. Enligt artikel 8.3 ska en oberoende myndighet kontrollera att dessa regler efterlevs.

18.3 Dataskyddslagen

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit att 8 kap. dataskyddslagen ska innehålla bestämmelser om skadestånd och andra rättsmedel. Rätten till skadestånd behandlas i avsnitt 15.7 i vår promemoria. Vad gäller övriga rättsmedel innehåller förslaget till dataskyddslag följande bestämmelser.

18.3.1 Överklagande av en myndighets beslut

Enligt den föreslagna 8 kap. 2 § dataskyddslagen får beslut enligt artiklarna 12.5, 15–19 eller 21 i dataskyddsförordningen som har meddelats av en myndighet i egenskap av personuppgiftsansvarig överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten och rätten att överklaga gäller inte beslut som fattats av riksdagen, regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller riksdagens ombudsmän.

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 303) sammanfattningsvis gjort följande bedömning.

De förvaltningsrättsliga principer som motiverar att denna typ av beslut ska kunna överprövas av domstol gör sig gällande även avseende vissa av de beslut som personuppgiftsansvariga myndigheter kommer att fatta enligt dataskyddsförordningen till följd av en registrerads begäran. Även dataskyddslagen bör därför förses med en uttrycklig bestämmelse om att vissa myndighetsbeslut får överklagas till allmän förvaltningsdomstol. Rätten att överklaga bör omfatta beslut som en personuppgiftsansvarig myndighet fattar med anledning av att en registrerad utövar sina rättigheter enligt kapitel III i dataskyddsförordningen. De rättigheter som kan föranleda överklagbara beslut rör information (artikel 12.5), registerutdrag m.m. (artikel 15), rättelse (artikel 16), radering (artikel 17), begränsning (artikel 18), underrättelse till tredje man om rättelse, radering eller begränsning (artikel 19) och invändningar (artikel 21).

18.3.2 Dröjsmålstalan

Dataskyddsförordningen garanterar – genom artikel 78.2 – att en registrerad som med stöd av förordningen har lämnat in ett klagomål till tillsynsmyndigheten har rätt till ett effektivt rättsmedel, om myndigheten inte handlägger klagomålet eller tar lång tid på sig. För att uppfylla detta krav finns i den föreslagna 6 kap. 5 § dataskyddslagen bestämmelser om den registrerades rätt att under vissa förutsättningar få besked av tillsynsmyndigheten angående handläggningen av ett klagomål. Enligt vårt förslag ska 6 kap. 5 § dataskyddslagen gälla även på domstolsdatalagens tillämpningsområde (se avsnitt 10.6.9).

Enligt förslaget till 8 kap. 3 § dataskyddslagen får tillsynsmyndighetens beslut att avslå en begäran om besked enligt 6 kap. 5 § samma lag 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 får inte överklagas.

Dataskyddsutredningen anför i sitt betänkande (SOU 2017:39 s. 328 f.) sammanfattningsvis följande.

Skyndsamhetskrav och informationsskyldighet gäller redan enligt förvaltningslagens allmänna bestämmelser och eventuella brister i handläggningen kan anmälas till och bli föremål för prövning av JO. Det praktiska värdet av de bestämmelser rörande besked om handläggningen av ett klagomål och dröjsmålstalan som vi föreslår kan mot denna bakgrund ifrågasättas. I avsaknad av en generell reglering i förvaltningslagen om åtgärder vid dröjsmål bedömer vi dock att de föreslagna bestämmelserna behövs för att dataskyddsförordningens krav på effektiva rättsmedel ska anses uppfyllda. För det fall riksdagen i enlighet med regeringens förslag beslutar om en ny förvaltningslag som innehåller generellt tillämpliga bestämmelser om åtgärder vid dröjsmål kan det dock finnas anledning att särskilt överväga om detta behov kvarstår.

18.3.3 Överklagande av tillsynsmyndighetens beslut

Enligt den föreslagna 8 kap. 4 § dataskyddslagen får tillsynsmyndighetens beslut enligt dataskyddsförordningen och enligt 7 kap. 1 och 2 §§ dataskyddslagen överklagas till allmän förvaltningsdomstol. Vid överklagande till kammarrätten krävs prövningstillstånd.

De föreslagna 7 kap. 1 och 2 §§ dataskyddslagen avser beslut om administrativa sanktionsavgifter. Enligt vårt förslag ska dataskyddslagens bestämmelse i 7 kap. 1 §, men inte i 7 kap. 2 §, gälla på domstolsdatalogens tillämpningsområde (se avsnitt 10.7).

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 325 ff.) sammanfattningsvis gjort följande ställningstagande.

Den rätt till ett effektivt rättsmedel mot tillsynsmyndighetens beslut som framgår av artikel 78.1 i dataskyddsförordningen

tillgodoses i svensk rätt normalt genom möjligheten att överklaga beslutet till allmän förvaltningsdomstol. Rätten att överklaga bör uttryckligen anges i dataskyddslagen och omfatta dels sådana beslut som tillsynsmyndigheten får meddela enligt dataskyddsförordningen, dels sådana beslut om administrativa sanktionsavgifter som får meddelas med stöd av dataskyddslagen. Övriga beslut som fattas av tillsynsmyndigheten enligt dataskyddslagen bör inte omfattas av den generella överklagandebestämmelsen. Liksom enligt personuppgiftslagen bör prövningstillstånd krävas vid överklagande av förvaltningsrättens beslut till kammarrätten. Formerna för överklagande av tillsynsmyndighetens beslut, vilken överklagandefrist som ska gälla, talerätt m.m., bör inte avvika från förvaltningslagens bestämmelser.

18.3.4 Beslut om enskilt organs behandling för arkivändamål

Av den föreslagna 8 kap. 5 § dataskyddslagen framgår att beslut enligt 2 kap. 5 § andra stycket, 3 kap. 6 § tredje stycket och 3 kap. 10 § i den lagen får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

I 2 kap. 5 § andra stycket dataskyddslagen behandlas rätten för myndighet (Riksarkivet) att i enskilda fall besluta att enskilda organ får behandla personuppgifter för arkivändamål av allmänt intresse. Enligt 3 kap. 6 § tredje stycket dataskyddslagen får myndighet (Riksarkivet) på motsvarande sätt fatta beslut som tillåter enskilda organ att behandla känsliga personuppgifter för sådana ändamål. Bestämmelserna är inte relevanta för domstolarnas rättsskipande och rättsvårdande verksamhet.

Bestämmelsen i 3 kap. 10 § dataskyddslagen gäller myndighets beslut att i enskilda fall tillåta behandling av personuppgifter som rör fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel. Myndigheter får dock, enligt artikel 10 i dataskyddsförordningen, behandla sådana uppgifter även utan beslut av tillsynsmyndigheten. Därmed är inte heller 3 kap. 10 § dataskyddslagen relevant inom domstolsdatalagens tillämpningsområde.

18.3.5 Överklagandebestämmelserna är uttömmande

Av den föreslagna 8 kap. 6 § dataskyddslagen framgår att andra beslut enligt lagen än de som avses i 8 kap. 2–5 §§ och 6 kap. 2 § inte får överklagas.

18.4 Bedömning

Förslag: Tillsynsmyndighetens beslut enligt dataskyddsförordningen och enligt den föreslagna 7 kap. 1 § dataskyddslagen ska få överklagas till allmän förvaltningsdomstol. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Tillsynsmyndighetens beslut att avslå en begäran om besked angående handläggningen av ett klagomål enligt den föreslagna 6 kap. 5 § dataskyddslagen ska få 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 få överklagas.

Domstolarnas beslut enligt artiklarna 12.5, 15–19 och 21 i dataskyddsförordningen ska få överklagas. En hovrätts, tingsrätts eller förvaltningsrätts beslut ska få överklagas till kammarrätt. En kammarrätts beslut i sådana frågor ska få överklagas till Högsta förvaltningsdomstolen. Högsta domstolens och Högsta förvaltningsdomstolens beslut i sådana frågor ska inte få överklagas.

Andra beslut ska inte få överklagas.

Bedömning: Dataskyddsförordningen föranleder ingen ändring av domstolsdatalagens reglering av instansordningen vad gäller de beslut som en hyres- och arrendenämnd fattar som personuppgiftsansvarig myndighet.

Inledningsvis vill vi understryka att tillsynsmyndigheten, enligt artikel 55.3 i dataskyddsförordningen, inte är behörig att utöva tillsyn över den personuppgiftsbehandling som sker i domstolarnas dömmande verksamhet. Enligt vår bedömning omfattar den

dömande verksamheten all personuppgiftsbehandling som görs i det enskilda målet eller ärendet från att detta anhängiggörs tills ett slutligt avgörande har fattats (se vidare avsnitt 8.4). Utifrån den definitionen är tillsynsmyndigheten endast behörig att fatta beslut gällande domstolarnas personuppgiftsbehandling inom en relativt liten del av den rättskipande och rättsvårdande verksamheten. Det samma gäller tillsynsmyndighetens rätt att göra en ansökan enligt 6 kap. 2 § dataskyddslagen. Resonemanget återkommer även när det gäller rätten för en registerad begära besked angående handläggningen av ett klagomål enligt 6 kap. 5 § samma lag.

För de beslut som tillsynsmyndigheten enligt sin behörighet kan fatta gällande domstolarnas personuppgiftsbehandling finns det dock enligt vår uppfattning anledning att i domstolsdatalagen reglera rätten att överklaga besluten. Vi anser att också de processuella bestämmelserna kring dröjsmålstalan och ansökan till förvaltningsrätten enligt 6 kap. 2 § dataskyddslagen av denna anledning bör regleras inom domstolsdatalagens tillämpningsområde.

18.4.1 Överklagande av tillsynsmyndighetens beslut

En reglering av rätten att på domstolsdatalagens tillämpningsområde överklaga tillsynsmyndighetens beslut hade kunnat göras genom en hänvisning till 8 kap. 4 § dataskyddslagen. Den lagtekniska lösning som valts för domstolsdatalagen innebär emellertid att samtliga överklagandebestämmelser uttryckligen framgår av lagen och har samlats under en särskild rubrik.³ Därtill kommer att vissa delar av 8 kap. 4 § dataskyddslagen inte är relevanta för domstolarnas rättskipande och rättsvårdande verksamhet. En hänvisning till dataskyddslagens bestämmelse skulle kunna orsaka missuppfattningar kring detta.

Mot den bakgrunden föreslår vi att det i domstolsdatalagen regleras att tillsynsmyndighetens beslut enligt dataskyddsförordningen och 7 kap. 1 § dataskyddslagen får överklagas till allmän förvaltningsdomstol. I likhet med vad som gäller enligt 8 kap. 4 § dataskyddslagen och med vad som för närvarande gäller

³ Jfr förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 95 f.).

enligt 19 § domstolsdatalagen, bör prövningstillstånd krävas vid överklagande till kammarrätten.

Regeringen har i tidigare förarbeten till domstolsdatalagen (prop. 2014/15:148 s. 95) gjort bedömningen att det inte behövs någon särskild forumregel för överklaganden som görs av domstolar i deras egenskap av personuppgiftsansvariga. Detta innebär att Förvaltningsrätten i Stockholm alltid är första instans i sådana mål, i enlighet med 14 § andra stycket lagen (1971:289) om allmänna förvaltningsdomstolar. En sådan ordning kan enligt vår mening orsaka vissa problem – exempelvis skulle det kunna inträffa att Förvaltningsrätten i Stockholm blir part i ett mål som handläggs hos Förvaltningsrätten i Stockholm. Vi anser dock att det inte framkommit skäl att frånga den bedömning som gjorts tidigare.

18.4.2 Dröjsmålstalan

Vi har föreslagit att den registrerades rätt att enligt 6 kap. 5 § dataskyddslagen få besked om handläggningen av ett klagomål ska vara tillämplig även på domstolsdatalagens tillämpningsområde (se avsnitt 10.6.9). Denna typ av beslut får enligt den föreslagna 8 kap. 3 § dataskyddslagen överklagas till allmän förvaltningsdomstol, vars beslut inte får överklagas.

I enlighet med det ställningstagande vi gjort för överklagande av tillsynsmyndighetens beslut, anser vi att rätten att överklaga denna typ av beslut bör framgå av domstolsdatalagen. Vi anser vidare att det – i likhet med vad som gäller för andra beslut som fattats av tillsynsmyndigheten – inte heller i detta fall bör finnas en speciell instansordning för de beslut som gäller personuppgiftsbehandling inom domstolsdatalagens tillämpningsområde (se avsnitt 18.4.1).

Vi föreslår därför att det i domstolsdatalagen införs en bestämmelse med samma innehåll som den föreslagna 8 kap. 3 § dataskyddslagen. Det bör således av domstolsdatalagen framgå att tillsynsmyndighetens beslut att avslå en begäran om besked enligt 6 kap. 5 § dataskyddslagen får överklagas till allmän förvaltningsdomstol. Domstolen bör, om överklagandet bifalls, förelägga tillsynsmyndigheten att inom en bestämd tid lämna besked till den registrerade i frågan om tillsyn kommer att utövas. Domstolens beslut bör inte kunna överklagas.

Regeringen har i och för sig, i prop. 2016/17:180, föreslagit att den nya förvaltningslagen ska innehålla en liknande generell bestämmelse om dröjsmålstalan, som föreslås träda i kraft den 1 juli 2018. Mot bakgrund av att förslaget ännu inte lett till lagstiftning och med hänsyn till att det är angeläget att systematiken i domstolsdatalagen – i den mån det är möjligt – följer dataskyddslagen anser vi trots detta att möjligheten att väcka dröjsmålstalan bör regleras i domstolsdatalagen.

18.4.3 Överklagande av beslut som domstol fattar som personuppgiftsansvarig myndighet

Dataskyddsutredningen har gjort bedömningen att de beslut som en personuppgiftsansvarig myndighet fattar med anledning av att en registrerad utövar sina rättigheter enligt kapitel III i dataskyddsförordningen bör gå att överklaga. Vi finner inte anledning att göra någon annan bedömning för de beslut som fattas av domstolarna i deras egenskap av personuppgiftsansvariga myndigheter. Ställningstagandet stämmer vidare överens med vad som för närvarande gäller; enligt 19 § domstolsdatalagen får bl.a. sådana beslut om information till den registrerade, rättelse och under rättelse till tredje man överklagas.

För överklagande av de beslut som fattats av domstolarna (inte hyres- och arrendenämnderna) i dessa situationer finns emellertid en avvikande instansordning. Denna bör enligt vår mening gälla även fortsättningsvis. Vi föreslår därför att det i domstolsdatalagen regleras att en hovrätts, tingsrätts eller förvaltningsrätts beslut enligt artiklarna 12.5, 15–19 eller 21 i dataskyddsförordningen, får överklagas till kammarrätt. I enlighet med vad som för närvarande gäller bör en kammarrätts beslut i de nu aktuella frågorna få överklagas till Högsta förvaltningsdomstolen. Högsta domstolens och Högsta förvaltningsdomstolens beslut i sådana frågor bör inte få överklagas.

I 21 § domstolsdatalagen klargörs att en hyres- och arrendenämnds beslut får överklagas till allmän förvaltningsdomstol och att prövningstillstånd krävs vid överklagande till kammarrätten. Dataskyddsförordningen föranleder enligt vår mening inte någon ändring av denna instansordning, som motsvarar den ordning för överklagande som enligt Dataskyddsutredningens förslag till 8 kap.

2 § dataskyddslagen kommer att gälla för andra förvaltningsmyndigheters beslut.

18.4.4 Andra beslut får inte överklagas

De bestämmelser om överklagande som vi har föreslagit innebär att samma möjligheter till överklagande kommer att finnas inom domstolsdatalagens tillämpningsområde som i dataskyddslagens generella bestämmelser. Vidare ges både fysiska och juridiska personer rätt till domstolsprövning av de beslut som tillsynsmyndigheten har fattat rörande dem. Detta innebär enligt vår mening att rätten till ett effektivt rättsmedel i artikel 78.1 i dataskyddsförordningen garanteras. Den registrerade ges också rätt till domstolsprövning vid ett sådant dröjsmål i tillsynsmyndighetens handläggning som omfattas av artikel 78.2 i dataskyddsförordningen.

Slutligen medför de bestämmelser vi föreslagit att den registrerade har rätt att överklaga de beslut som domstolarna fattar rörande honom eller henne i egenskap av personuppgiftsansvariga myndigheter, förutsatt att besluten rör den registrerades rättigheter enligt dataskyddsförordningen och stadgan. Dessutom har den registrerade rätt att begära skadestånd av den personuppgiftsansvariga myndigheten (se avsnitt 15.7). Vi anser att detta innebär att samtliga rättigheter till ett effektivt rättsmedel som föreskrivs i dataskyddsförordningen garanteras genom våra förslag.

Vi anser också att de rättigheter som uttryckligen anges i artikel 8 i stadgan (lagenlig behandling av personuppgifter för bestämda ändamål på grundval av en legitim och lagenlig grund samt tillgång till och rättelse av de egna personuppgifterna) garanteras av de överklagandebestämmelser vi föreslagit.

Mot denna bakgrund är det vår uppfattning att domstolsdatalagens överklagandebestämmelser bör vara uttömmande. Detta motsvarar vad som för närvarande gäller enligt 22 § domstolsdatalagen.

19 Bevarande av personuppgifter

19.1 Domstolsdatalagen och personuppgiftslagen

I 5 § första stycket 2 och 3 domstolsdatalagen finns hänvisningar till 8 och 9 §§ PuL. Delar av de sistnämnda bestämmelserna reglerar förhållandet mellan personuppgiftslagens bestämmelser och rätten att bevara handlingar. I 9 § används begreppen *historiska*, *statistiska* och *vetenskapliga ändamål*. *Historiska ändamål* innefattar här bevarande av handlingar för arkivändamål.¹

Arkivering av handlingar innebär att de personuppgifter som ingår i handlingarna vidarebehandlas, dvs. behandlas för ett annat ändamål än det ursprungliga. Av 9 § första stycket d PuL framgår att personuppgifter inte får behandlas för ändamål som är oförenliga med det ändamål som uppgifterna samlades in för (finalitetsprincipen). Behandling av personuppgifter för bl.a. historiska ändamål ska, enligt 9 § andra stycket, emellertid inte ses som oförenlig med de ursprungliga ändamålen. Av förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 104) framgår dock att finalitetsprincipen inte har någon självständig funktion inom domstolsdatalagens tillämpningsområde. Anledningen till detta är att lagens ändamålsbestämmelser utgör en uttömmande reglering av för vilka ändamål personuppgifter får behandlas i domstolarnas rättsskipande och rättsvårdande verksamhet.

Enligt 9 § första stycket i PuL är huvudregeln att personuppgifter inte får bevaras längre än vad som är nödvändigt med hänsyn till det ursprungliga ändamålet. Bestämmelserna i personuppgiftslagen hindrar emellertid inte att myndigheter arkiverar och bevarar handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. I detta fall ska personuppgiftslagens

¹ Jfr förarbetena till personuppgiftslagen (prop. 1997/98:44 s 47 f.).

begränsningar om lagringstid m.m. inte gälla (jfr 8 § andra stycket PuL).

För personuppgifter som behandlas för arkivändamål finns, enligt 9 § fjärde stycket PuL, vissa begränsningar för hur uppgifterna får användas. Sådana uppgifter får inte användas för att vidta åtgärder i fråga om den registrerade, om det inte görs med samtycke eller det annars finns synnerliga skäl med hänsyn till den registrerades intressen att göra detta. I 8 § andra stycket PuL finns dock ett undantag, som innebär att myndigheter får använda information i allmänna handlingar, t.ex. för att vidta åtgärder beträffande enskilda. Bakgrunden till det aktuella undantaget har i doktrinen i första hand bedömts vara att myndigheternas arkiv, enligt 3 § tredje stycket arkivlagen (1990:782), ska tillgodose bl.a. behovet av information för rättskipningen och förvaltningen.²

Det kan i domstolarnas verksamhet även finnas anledning att elektroniskt bevara personuppgifter utan att formellt arkivera dem, t.ex. för att för framtida mål- eller ärendehantering bevara en föredragningspromemoria från ett specifikt mål eller ärende. Regeringen har i förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 81) uttalat att för att möjliggöra detta och åstadkomma en heltäckande bevarandereglering bör domstolsdatalagen hänvisa till bestämmelserna i 9 § första stycket i och tredje stycket PuL. Av 9 § första stycket i framgår att personuppgifter inte får bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Enligt 9 § tredje stycket får personuppgifter dock bevaras för bl.a. historiska ändamål så länge det behövs för detta ändamål. Vi vill i detta sammanhang peka på att regeringen också uttalat att domstolsdatalagens primära ändamålsbestämmelse (handläggning av mål och ärenden) ska ges en vid tolkning, vilket enligt vår mening innebär att även behandling av personuppgifter i exempelvis föredragningspromemorior och rättsutredning ingår i begreppet.

Hänvisningarna i domstolsdatalagen till 8 och 9 §§ PuL innebär sammanfattningsvis följande. Domstolarna får i enlighet med arkivreglerna elektroniskt arkivera personuppgifter som samlats in i den rättskipande och rättsvårdande verksamheten, oavsett om de

² Öman och Lindblom, Personuppgiftslagen (15 sept 2016, Zeteeo), kommentaren till 8 §.

före arkiveringstidpunkten förekommer i allmänna eller icke allmänna handlingar. De personuppgifter som har arkiverats får användas för att vidta åtgärder i fråga om den registrerade. För personuppgifter som bevaras utan att arkiveras (t.ex. rättsutredningar eller föredragningspromemorior) gäller att de får behandlas så länge det är nödvändigt för handläggningen av mål och ärenden i en vidare bemärkelse.

Avslutningsvis kan regeringen eller den myndighet som regeringen bestämmer med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar för behandling av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts genom en dom eller ett beslut som har fått laga kraft. Detta framgår av 18 § domstolsdatalagen. Enligt förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 82 f.) är bestämmelsen avsedd att skapa ett särskilt integritetskydd för uppgifter i avgjorda mål och ärenden, genom att domstolarnas och allmänhetens åtkomst till dessa uppgifter begränsas. Detta kan åstadkommas genom exempelvis begränsningar av direktåtkomst eller sökmöjligheter. Som befintliga exempel kan nämnas domstolsdataförordningens bestämmelser om sökbegränsningar för mål eller ärenden som avgjorts slutligt (3–5 §§).

19.2 Dataskyddsförordningen

Vidarebehandling av personuppgifter får, enligt artikel 5.1 b i dataskyddsförordningen, ske endast om den är förenlig med de ändamål som personuppgifterna samlades in för (finalitetsprincipen). Av bestämmelsen framgår dock att vidarebehandlingen ska anses vara förenlig med de ursprungliga ändamålen när den sker för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1.

Vi bedömer att hänvisningen till artikel 89.1 innebär att arkivering av personuppgifter endast anses förenlig med de ursprungliga ändamålen – och därmed tillåten – om sådana säkerhetsåtgärder som beskrivs i den senare artikeln vidtas. Av artikel 89.1 framgår att behandling av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska

forskningsändamål samt statistiska ändamål ska omfattas av lämpliga skyddsåtgärder för den registrerades rättigheter och friheter. Det framgår också att dessa skyddsåtgärder ska säkerställa att det införs sådana tekniska och organisatoriska åtgärder som garanterar att principen om uppgiftsminimering följs. Som exempel nämns att pseudonymisering eller andra åtgärder som innebär att de registrerade inte kan identifieras ska användas när detta är möjligt med hänsyn till arkivändamålet.

Även vad gäller tiden för lagring av personuppgifter har arkiverade uppgifter en särställning i dataskyddsförordningen. Enligt artikel 5.1 e i förordningen får personuppgifter som enbart behandlas för arkivändamål av allmänt intresse lagras i en form som möjliggör identifiering av den registrerade under längre tid än vad som är nödvändigt för de ändamål som de samlades in för. En förutsättning för att så ska få ske är enligt samma bestämmelse att det genomförs lämpliga tekniska och organisatoriska åtgärder för att säkerställa den registrerades rättigheter och friheter.

Även känsliga personuppgifter kan ingå i de handlingar som arkiveras. Dataskyddsförordningens huvudregel är i och för sig att behandling av känsliga personuppgifter är förbjuden (artikel 9.1). Som ett av undantagen anges dock i artikel 9.2 j att behandling av känsliga personuppgifter är tillåten om den är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1. Behandlingen måste dock ske på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenlig 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. Detta innebär i klartext att det krävs stöd EU-rätten eller i nationell lagstiftning för att känsliga personuppgifter ska få behandlas för bl.a. arkivändamål. Den nationella regleringen måste vidare innehålla säkerhetsåtgärder till skydd för personuppgifterna.

Avslutningsvis vill vi i detta sammanhang nämna att dataskyddsförordningen innehåller vissa undantag från de registrerades rättigheter (kapitel III i förordningen) för de personuppgifter som behandlas för arkivändamål av allmänt intresse. De undantag som

är relevanta inom domstolsdatalagens tillämpningsområde behandlar vi i kapitel 15.

19.3 Dataskyddslagen

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 216) gjort bedömningen att den behandling av personuppgifter som myndigheter och andra organ utför när de som en följd av arkivlagens bestämmelser arkiverar sina allmänna handlingar, utgör en vidarebehandling för arkivändamål av allmänt intresse. Dataskyddsutredningen menar att det därmed inte krävs någon annan rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs för att arkivering av personuppgifter i myndigheters verksamhet ska vara tillåten (jfr artikel 5.1 b i dataskyddsförordningen och skäl 50 till förordningen).

Dataskyddsutredningen har dock föreslagit att dataskyddslagen ska innehålla en bestämmelse som innebär att även känsliga personuppgifter får behandlas för arkivändamål av allmänt intresse, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv. Bestämmelsen finns enligt förslaget i 3 kap. 6 § första stycket dataskyddslagen. Enligt förslaget till andra stycket i samma bestämmelse får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om att känsliga personuppgifter får behandlas för arkivändamål av allmänt intresse även i andra fall än de som avses i första stycket. Av Dataskyddsutredningens betänkande (SOU 2017:39 s. 223) framgår att bestämmelsen i andra stycket tar sikte på enskilda arkiv som inte omfattas av arkivlagstiftningen. Den är därmed inte av intresse för domstolarnas personuppgiftsbehandling.

Dataskyddsutredningen har gjort bedömningen att den svenska lagstiftningen på arkivområdet är proportionell till det eftersträvade syftet och förenlig med det väsentliga innehållet i rätten till dataskydd. I denna bedömning har de skyddsåtgärder som finns i registerförfattningar samt i form av sekretessbestämmelser och gallringsföreskrifter vägts in. De nationella sekretessbestämmelserna bedöms vidare utgöra en särskild skyddsåtgärd,

eftersom de har utformats efter en avvägning mellan behovet av skydd och intresset av insyn.³

Som en ytterligare skyddsåtgärd för arkiverade personuppgifter har Dataskyddsutredningen föreslagit en bestämmelse i dataskyddslagen (4 kap. 1 §) som motsvarar 8 § andra stycket andra meningen och 9 § fjärde stycket PuL.⁴ Enligt den föreslagna bestämmelsen får personuppgifter som behandlas enbart för arkivändamål av allmänt intresse inte användas för att vidta åtgärder i fråga om den registrerade, annat än om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Av bestämmelsens andra stycke framgår att begränsningen inte hindrar myndigheter från att använda personuppgifter som finns i allmänna handlingar.

Dataskyddsutredningen har därutöver föreslagit att dataskyddslagen ska innehålla en bestämmelse som innebär att behandling av personuppgifter om fällande domar i brottmål, lagöverträdelse som innefattar brott eller straffprocessuella tvångsmedel får behandlas om det är nödvändigt för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv (3 kap. 11 §). Vi anser dock att denna bestämmelse inte är relevant inom domstolsdatalagens tillämpningsområde. Anledningen till detta är att sådana uppgifter enligt artikel 10 i dataskyddsförordningen får behandlas av myndigheter. Artikel 10 innehåller inga begränsningar, vilket enligt vår mening måste innebära att detta gäller även när uppgifterna behandlas för arkivändamål.

19.4 Bedömning

Förslag: Personuppgifter som behandlas eller har behandlats för handläggning av mål och ärenden ska också få behandlas om det behövs för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i dataskyddsförordningen. Personuppgifter ska även få behandlas för dessa ändamål när de behandlas eller har

³ Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 221 och 227).

⁴ A.a. s. 222.

behandlats med stöd av brottsdatalagen eller den registerförfattning som kompletterar brottsdatalagen för domstolarnas verksamhet.

Det ska även fortsättningsvis vara möjligt för domstolarna att återanvända personuppgifter i arkiverade mål och ärenden. Regleringen ska genomföras genom en hänvisning i domstolsdatalagen till den föreslagna 4 kap. 1 § dataskyddslagen.

Bedömning: Dataskyddsförordningen föranleder ingen ändring av föreskriftsrätten vad gäller begränsning av behandling av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts genom en dom eller ett beslut som har fått laga kraft.

Det behövs ingen hänvisning till dataskyddslagens föreslagna bestämmelse om rätten att behandla känsliga personuppgifter för arkivändamål av allmänt intresse.

19.4.1 Begreppet arkivändamål av allmänt intresse

I samtliga dataskyddsförordningens bestämmelser som rör bevarande av personuppgifter används begreppen *arkivändamål av allmänt intresse*, *vetenskapliga eller historiska forskningsändamål* och *statistiska ändamål* för att beskriva de ändamål för behandling som träffas av bestämmelserna. Vi har tidigare gjort bedömningen att ett utlämnande av uppgifter enligt tryckfrihetsförordningen utgör en uppgift av allmänt intresse (avsnitt 6.2.5). Bevarandet av allmänna handlingar är en förutsättning för att allmänheten, genom offentlighetsprincipen, ska få fullgod insyn i myndigheternas verksamhet. Redan i förarbetena till personuppgiftslagen (prop. 1997/98:44 s. 47) gjorde regeringen vidare bedömningen att ett bevarande av allmänna handlingar utgör en arbetsuppgift av allmänt intresse. Mot den bakgrunden delar vi Dataskyddsutredningens bedömning att den behandling av personuppgifter som myndigheter och andra organ utför när de arkiverar handlingar enligt gällande arkivlagstiftning, sker för arkivändamål av allmänt intresse. Detta innebär att dataskyddsförordningens begrepp *arkivändamål av allmänt intresse* innefattar den arkivering av handlingar som utförs i domstolarnas verksamhet.

Vi anser dock att det endast är de personuppgifter som finns i handlingar som officiellt tas om hand för arkivering som kan anses behandlas för *arkivändamål av allmänt intresse*. Begreppet omfattar således inte sådant elektroniskt bevarande av personuppgifter som inte sker i arkiveringssyfte.⁵

Detta innebär enligt vår mening att ett elektroniskt bevarande av exempelvis en föredragningspromemoria eller en rättsutredning som innehåller personuppgifter – och som inte formellt arkiveras – måste ske enligt de vanliga reglerna i dataskyddsförordningen och domstolsdatalagen. Vi illustrerar en sådan situation med följande exempel.

När ett mål har avslutats bevarar den handläggande tjänstemannen sin föredragningspromemoria på H: eller G: (beroende på om den ska vara tillgänglig endast för tjänstemannen eller även för andra som arbetar i verksamheten). De personuppgifter som förekommer i promemorian har samlats in för handläggningen av det aktuella målet (jfr 6 § domstolsdatalagen). Domstolsdatalagens ändamålsbestämmelser är uttömmande, vilket innebär att personuppgifter inte får behandlas av domstolarna för andra ändamål än för handläggningen av mål och ärenden. Enligt förarbetena till domstolsdatalagen (prop. 2014/15:148 s 39 f.) ska ändamålsbestämmelserna dock ges en vid tolkning. Bedömningen av om en viss behandling behövs ska göras i förhållande till mål- och ärendehandläggningen i stort och inte i förhållande till handläggningen av ett specifikt mål eller ärende. Så länge det finns ett verksamhetsbehov av att bevara föredragningspromemorian, anser vi därmed att ett bevarande är tillåtet enligt domstolsdatalagen. Ett sådant verksamhetsbehov måste enligt vår mening finnas exempelvis om promemorian bevaras för att underlätta handläggningen av liknande framtida mål eller skapa en enhetlig praxis. I enlighet med dataskyddsförordningens princip om lagringsminimering (artikel 5.1 e) bör det dock övervägas om promemorian ska avidentifieras. Detta ska göras så fort det inte längre finns behov av att kunna identifiera de personer som förekommit i det aktuella målet eller ärendet.

⁵ Jfr förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 81).

19.4.2 Arkivering ingår i den rättskipande och rättsvårdande verksamheten

Genom arkivering tas handlingar från en myndighets kärnverksamhet om hand och bevaras, antingen av myndigheten själv eller av en arkivmyndighet. Informationen i dessa handlingar får dock fortfarande användas för att vidta åtgärder beträffande enskilda, trots att arkivering har skett (8 § andra stycket PuL). Detta gäller även på domstolsdatalagens tillämpningsområde (5 § första stycket 2 domstolsdatalagen). Enligt förslaget i Dataskyddsutredningens betänkande (SOU 2017:39) ska dataskyddslagen innehålla motsvarande bestämmelser.

För oss är det en självklarhet att personuppgifter som härrör från domstolarnas rättskipande och rättsvårdande verksamhet fortsätter vara en del av denna verksamhet även efter det att handlingarna de ingår i har arkiverats, åtminstone så länge arkiveringen sker hos domstolen själv. När handlingarna lämnas över till en arkivmyndighet och inte längre finns kvar hos domstolarna torde domstolsdatalagen inte heller längre vara tillämplig, eftersom domstolarna då inte själva behandlar personuppgifterna i handlingarna.

Att arkivering av personuppgifter i den rättskipande och rättsvårdande verksamheter faller under domstolsdatalagens tillämpningsområde förefaller också vara utgångspunkten i de tidigare förarbetena till lagen. Domstolsdatalagen gäller för domstolarnas personuppgiftsbehandling i den rättskipande och rättsvårdande verksamheten. För det fall lagstiftaren inte hade ansett att arkiverade handlingar alltså utgör en del av denna verksamhet skulle någon hänvisning till personuppgiftslagens bestämmelser om rätten för myndigheter att arkivera allmänna handlingar inte fyllt någon funktion.⁶

19.4.3 Komplettering av domstolsdatalagen

Enligt domstolsdatalagens ändamålsbestämmelser får personuppgifter behandlas om det behövs för handläggning av mål och ärenden (6 §). Personuppgifter som behandlats för detta ändamål

⁶ Jfr förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 79 ff.).

får även behandlas om det behövs för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning (7 §).

Arkivering av personuppgifter omfattas enligt vår mening av domstolsdatalagens tillämpningsområde (se föregående avsnitt), men däremot inte av lagens ändamålsbestämmelser. Genom hänvisningen till 8 § PuL klargörs emellertid att arkivering av personuppgifter i den rättskipande och rättsvårdande verksamheten ändå får ske. Dataskyddslagen kommer enligt Dataskyddsutredningens förslag inte att innehålla någon bestämmelse som motsvarar 8 § andra stycket PuL.⁷ Anledningen till detta är, som vi förstått det, att det framgår av artikel 5.1 b i dataskyddsförordningen att vidarebehandling av personuppgifter för bl.a. arkivändamål av allmänt intresse ska anses vara förenlig med de ursprungliga ändamålen.⁸

Domstolsdatalagens ändamålsbestämmelser är emellertid avsedda att vara uttömmande. Det blir därmed aldrig aktuellt för domstolarna att inom domstolsdatalagens tillämpningsområde bedöma om behandling för andra ändamål än de som angivits i lagen är förenligt med finalitetsprincipen (se avsnitt 9.1.6). Det faktum att rätten att behandla personuppgifter för arkivändamål i dataskyddsförordningen framgår i anslutning till finalitetsprincipen (se avsnitt 9.1.4) väcker enligt vår mening frågor kring om man då kan tillämpa den del av bestämmelsen som tillåter arkivering.

I skäl 50 till dataskyddsförordningen anges att om behandling av personuppgifter 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. Därefter anges att ytterligare behandling för bl.a. arkivändamål av allmänt intresse bör betraktas som förenlig och laglig behandling av uppgifter. Detta skulle enligt vår mening kunna tolkas som att arkivering av personuppgifter alltid är tillåten, även om en registerförfattning har uttömmande ändamålsbestämmelser.

⁷ Se Dataskyddsutredningens betänkande (SOU 2017:39).

⁸ A.a. s. 216.

För att undanröja de tvivel som kan uppstå gällande detta och göra det helt klart för tillämparen att bestämmelserna i domstolsdatalagen inte hindrar att personuppgifter behandlas för arkivändamål av allmänt intresse, anser vi att det uttryckligen bör framgå av domstolsdatalagen att sådan behandling är tillåten för personuppgifter som behandlas eller har behandlats för handläggning av mål och ärenden. Detta utgör enligt vår mening ett sådant införlivande av dataskyddsförordningen som är tillåtet enligt skäl 8 till förordningen (se avsnitt 6.3). Bestämmelsen bör enligt vår mening placeras i samma paragraf som den befintliga sekundära ändamålsbestämmelsen.

För att domstolsdatalagens bestämmelse ska motsvara artikel 5.1 b i dataskyddsförordningen bör den utöver arkivändamål av allmänt intresse även omfatta vetenskapliga eller historiska forskningsändamål samt statistiska ändamål. Den bör även innehålla en hänvisning till artikel 89.1 i förordningen. På detta sätt tydliggörs att det även krävs sådana säkerhetsåtgärder som framgår av den senare bestämmelsen för att behandling för bl.a. arkivändamål ska vara tillåten. I avsnitt 19.4.5 behandlar vi dessa säkerhetsåtgärder.

19.4.4 Personuppgifter som behandlats enligt brottsdatalagen och dess registerförfattning

Utredningen om 2016 års dataskyddsdirektiv har i sitt delbetänkande (SOU 2017:29 s. 287) gjort bedömningen att behandling för arkivändamål omfattas av dataskyddsförordningens tillämpningsområde, oavsett om det är den behöriga myndigheten som arkiverar personuppgifterna eller om de överlämnas till en arkivmyndighet.

Detta får till följd att domstolsdatalagen bör reglera den personuppgiftsbehandling som utförs när handlingar innehållande personuppgifter som har behandlats av domstolarna med stöd av brottsdatalagen och dess kompletterande registerförfattning arkivläggs. För att ge ett konkret exempel; när en allmän domstol behandlar personuppgifter i ett brottmål sker detta enligt brottsdatalagen och dess kompletterande registerförfattning för domstolarna. När handlingarna i målet därefter arkiveras utförs personuppgiftsbehandlingen däremot med stöd av dataskydds-

förordningen och domstolsdatalagen. För att klargöra detta för tillämparen anser vi att det av domstolsdatalagen bör framgå att personuppgifter även får behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i dataskyddsförordningen när de behandlas eller har behandlats med stöd av brottsdatalagen eller dess kompletterande registerförfattning för domstolarnas verksamhet (jfr avsnitt 19.4.3).

Det faktum att domstolsdatalagen ska tillämpas vid arkivering av personuppgifter som behandlats i den del av domstolarnas verksamhet som omfattas av brottsdatalagens tillämpningsområde får betydelse för domstolsdatalagens sökbegränsningar. För vår bedömning i denna del hänvisar vi till avsnitt 16.5.4.

19.4.5 Hänvisning till dataskyddslagen och säkerhetsåtgärder

Enligt artikel 9.2 j i dataskyddsförordningen krävs det stöd EU-rätten eller i nationell rätt för att känsliga personuppgifter ska få behandlas för arkivändamål av allmänt intresse (se avsnitt 19.2).

På domstolsdatalagens tillämpningsområde får känsliga personuppgifter – med de undantag som framgår av lagen – behandlas på samma sätt som andra personuppgifter (se avsnitt 16.5.2). Genom den nya ändamålsbestämmelse gällande bl.a. arkivering som vi föreslagit (se avsnitt 19.4.3) kommer det vidare att klargöras att domstolarna får behandla personuppgifter för arkivändamål av allmänt intresse inom domstolsdatalagens tillämpningsområde. Mot den bakgrunden bedömer vi att bestämmelserna i domstolsdatalagen ger stöd för att känsliga personuppgifter behandlas för arkivändamål. Någon hänvisning till den föreslagna 3 kap. 6 § första stycket dataskyddslagen behövs enligt vår mening därmed inte.

Vad gäller de skyddsåtgärder som enligt artikel 5.1 b, artikel 9.2 j och artikel 89.1 i dataskyddsförordningen krävs för de känsliga personuppgifter som behandlas för bl.a. arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål kan följande sägas.

Skydd för arkiverade personuppgifter finns i svensk rätt i form av sekretessbestämmelser och gallringsföreskrifter. Vidare utgör de

behörighetsbegränsningar som finns i domstolsdatalagen sådana skyddsåtgärder som avses i dataskyddsförordningen.

Ytterligare en skyddsåtgärd för personuppgifter som behandlas av domstolarna för arkivändamål m.m. utgörs av regeringens eller myndighets föreskriftsrätt gällande begränsning av behandling av personuppgifter som hänför sig till en lagakraftvunnen dom eller ett lagakraftvunnet beslut (18 § domstolsdatalagen). Föreskriftsrätten har för närvarande utnyttjats för att skapa sök-begränsningarna i 3–5 §§ domstoldataförordningen. Möjlighet finns att vid behov skapa ytterligare integritetsskydd för denna typ av personuppgifter. Dataskyddsförordningen hindrar enligt vår bedömning inte att bestämmelser om personuppgiftsbehandling införs i en förordning eller i en myndighetsföreskrift, så länge dessa tillkommit i laga ordning (se avsnitt 20.2). I avsnitt 16.5.4 har vi vidare gjort bedömningen att 3–5 §§ domstolsdatalagen ska finnas kvar oförändrade i sak. Detsamma bör därmed även gälla föreskriftsrätten i nuvarande 18 § domstolsdatalagen.

Sammantaget anser vi att den befintliga och föreslagna regleringen i domstolsdatalagen, tillsammans med övriga nationella föreskrifter, är tillräckligt för att säkerställa den registrerades rättigheter och intressen vid domstolarnas behandling av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

För närvarande gäller 8 § andra stycket andra meningen och 9 § PuL för personuppgiftsbehandling som utförs inom domstolsdatalagens tillämpningsområde. Motsvarande bestämmelse kommer enligt Dataskyddsutredningens förslag att finnas i 4 kap. 1 § dataskyddslagen. Bestämmelsen innebär att personuppgifter som behandlas endast för arkivändamål av allmänt intresse inte får användas för att vidta åtgärder i fråga om den registrerade, om det inte finns synnerliga skäl för detta med hänsyn till den registrerades vitala intressen. Undantag görs dock för myndigheter som använder personuppgifter som finns i allmänna handlingar.

Vi föreslår att det i domstoldatalagen görs en hänvisning till 4 kap. 1 § dataskyddslagen. Genom en sådan hänvisning kommer det att stå klart för tillämparen att domstolarna får återanvända de personuppgifter som finns i arkiverade mål och ärenden. En förutsättning för detta är enligt vår mening dock att domstolen använder personuppgifterna för ett ändamål som omfattas av

domstolsdatalagen, eftersom dess ändamålsbestämmelser är avsedda att vara uttömmande.⁹

⁹ Se förarbetena till domstolsdatalagen, prop. 2014/15:148 s. 104.

20 Föreskriftsrätten

20.1 Domstolsdataförordningen

I 14 § domstolsdataförordningen finns ett bemyndigande för Domstolsverket att meddela ytterligare föreskrifter om domstolarnas behandling av personuppgifter i vissa fall. Det handlar om föreskrifter om tjänstemäns tillgång till personuppgifter, om vilka uppgifter som en förteckning enligt 11 § domstolsdatalagen ska innehålla och om begränsningar av möjligheterna att lämna ut personuppgifter på medium för automatiserad behandling. Domstolsverket får även meddela föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter genom direktåtkomst och om behörighet och säkerhet vid sådant utlämnande samt om begränsningar för behandling av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts slutligt genom en dom eller ett beslut som har fått laga kraft. Domstolsverket har också rätt att meddela de ytterligare föreskrifter som behövs för verkställighet av domstolsdatalagen och domstolsdataförordningen.

20.2 Bedömning

Bedömning: Utöver vad som tidigare föreslagits gällande föreskrifter om vilka uppgifter en förteckning enligt 11 § domstolsdatalagen ska innehålla föranleder dataskyddsförordningen ingen ändring av bestämmelserna om Domstolsverkets föreskriftsrätt.

Medlemsstaterna har, enligt artikel 6.2 och artikel 6.3 i dataskyddsförordningen, rätt att i nationell lagstiftning behålla eller införa mer

specifika bestämmelser för personuppgiftsbehandling. Detta kan ske exempelvis genom nationella registerförfattningar (se vidare kapitel 5). Varken artikel 6.2 eller artikel 6.3 innehåller något krav på att de bestämmelser som avses måste regleras i lag. Det är därmed vår uppfattning att det bör vara upp till den enskilda medlemsstaten på vilken nivå i normhierarkin sådana bestämmelser införs. I enlighet med detta ställningstagande hindrar dataskyddsförordningen inte att bestämmelser om personuppgiftsbehandling införs i en förordning eller i en myndighetsföreskrift. Detta förutsätter naturligtvis att föreskrifterna tillkommit i laga ordning.

Mot den bakgrunden anser vi att dataskyddsförordningen inte föranleder någon ändring av den föreskriftsrätt som genom 14 § domstolsdataförordningen tilldelats Domstolsverket. Vi har dock, i avsnitt 13.5.6, gjort bedömningen att den föreskriftsrätt som framgår av 14 § andra stycket 1 domstolsdataförordningen ska utgå. Anledningen till detta är att vi föreslår att skyldigheten att föra en förteckning enligt 11 § domstolsdatalagen ska upphöra.

21 Andra myndigheters direktåtkomst till mark- och miljödomstolarnas miljöbok

I vårt uppdrag ingår att ta ställning till om det finns behov av direktåtkomst för t.ex. Kammarkollegiet, länsstyrelserna, Naturvårdsverket och Havs- och vattenmyndigheten till den s.k. miljöbok som förs vid respektive mark- och miljödomstol.

21.1 Miljöboken – en översikt

21.1.1 Rättslig reglering och innehåll

Varje mark- och miljödomstol ska enligt 9 kap. 7 § lagen (1998:812) med särskilda bestämmelser om vattenverksamhet föra en förteckning över vattenverksamhet inom domsområdet (vattenbok) i den utsträckning som regeringen föreskriver. Av 8 § förordningen (1998:1388) om vattenverksamhet m.m. framgår att mark- och miljödomstolens förteckning över vattenverksamheter inom domsområdet ska föras i en miljöbok som en vattenbok ska ingå i. Av samma bestämmelse framgår att Domstolsverket får meddela föreskrifter om miljöboken. Enligt 2 § Domstolsverkets föreskrifter om miljöboken (DVFS 2011:2) ska varje mark- och miljödomstol föra en förteckning över domstolens avgöranden inom domsområdet i frågor som domstolen avgör i egenskap av första instans och som rör miljöbalken eller lagen med särskilda bestämmelser om vattenverksamhet.

Varje mark- och miljödomstol för en egen miljöbok, vilket innebär att det finns fem olika miljöböcker. Varje miljöbok finns i två versioner; en läs- och sökversion och en redigeringsversion.

Alla anställda på mark- och miljödomstolarna har åtkomst till både den egna domstolens miljöbok och – genom direktåtkomst – läs- och sökbehörighet till övriga miljöböcker. Även anställda på Mark- och miljööverdomstolen har direktåtkomst till miljöböckerna. Sedan den 1 juni 2017 får även Högsta domstolen medges sådan direktåtkomst. Behörighet till redigeringsversionen har enbart ett fåtal användare vid respektive mark- och miljödomstol. Dessa användare för in uppgifter om avgöranden från sin domstol.

Av Domstolsverkets föreskrifter om miljöboken framgår att denna är indelad i fem avdelningar. Fyra avser vattenverksamheter och vattentäkter och den femte avser miljöfarlig verksamhet. I Domstolsverkets föreskrifter regleras vidare vad som ska registreras i miljöboken, såvida sekretessföreskrifter inte föranleder något annat. Föreskrifterna anger också vid vilken tidpunkt registrering ska ske. Utöver den förteckning över domstolarnas avgöranden inom domsområdet som rör miljöbalken eller lagen om vattenverksamhet, ska mark- och miljödomstolarna föra in uppgifter om avgöranden från Mark- och miljööverdomstolen eller Högsta domstolen när målen avgjorts där. Om mark- och miljödomstolen får uppgifter om besiktning enligt 18 § förordningen om vattenverksamhet m.m. ska också dessa uppgifter registreras i miljöboken. Registrering ska även ske när domstolen får andra uppgifter än sådana som nämnts ovan och det enligt lag eller förordning finns en skyldighet att registrera uppgifterna.

De uppgifter som ska registreras i miljöboken är verksamhetstyp, anläggningens namn och den prövade anläggningens eller verksamhetens geografiska läge i det för Sverige officiella referenssystemet med en noggrannhet om minst tio meter. Vidare ska – i de fall mark- och miljödomstolen registerar uppgifter om ett avgörande – datum för avgörandet, målnummer och en kort beskrivning av avgörandet föras in i miljöboken. I de fall mark- och miljödomstolen finner att det är lämpligt får ytterligare uppgifter registreras.

21.1.2 Miljöboken innehåller personuppgifter

Miljöboken innehåller vissa direkta personuppgifter i form av personnamn. Detta förekommer dock främst i äldre poster, vilket

betyder att det absoluta flertalet av de personer vars namn anges numera troligtvis har avlidit. Dessa personnamn utgör inte personuppgifter i dataskyddsförordningens mening, eftersom förordningen inte gäller behandling av avlidnas personuppgifter (jfr skäl 27 till förordningen). Det går dock inte att utesluta att miljöboken även innehåller nu levande personers namn. Det förekommer också att anläggningar och parter som är juridiska personer har en benämning som innefattar ett personnamn.

Indirekta personuppgifter förekommer i miljöboken i form av målnummer, domsnummer (ett individuellt nummer som används för äldre avgöranden), geografiska koordinater och fastighetsbeteckningar. Gatunamn och vägnamn förekommer också, men såvitt vi erfarit finns det inte några nummer angivna.

Enligt 1 § Domstolsverkets föreskrifter om miljöboken ska uppgifter som kan sekretessbeläggas inte registreras i miljöboken. Miljöboken innehåller inte heller några känsliga personuppgifter.

21.2 Direktåtkomst

Vi har i avsnitt 17.3.1 redogjort för innebörden av direktåtkomst och vilka integritetsrisker som är förknippade med sådan åtkomst. För en allmän beskrivning i denna del hänvisar vi till det avsnittet. Högsta förvaltningsdomstolen har emellertid relativt nyligen – i rättsfallet HFD 2015 ref. 61 – uttalat sig om innebörden av direktåtkomst. Mot den bakgrunden finns det enligt vår mening anledning att på nytt göra en bedömning av om den typ av åtkomst till miljöboken som skulle vara aktuell i detta fall verkligen utgör direktåtkomst eller om det endast rör sig om annat elektroniskt utlämnande.

Högsta förvaltningsdomstolen uttalade i det ovan nämnda rättsfallet följande. Det avgörande för om en myndighets tillgång till en annan myndighets uppgifter ska anses utgöra direktåtkomst är om upptagningen kan anses förvarad hos den mottagande myndigheten i tryckfrihetsförordningens mening. Så är fallet om upptagningen är tillgänglig för den mottagande myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas (jfr 2 kap. 3 § andra stycket TF).

Det datasystem som var aktuellt i målet, LEFI Online, används när Försäkringskassan lämnar ut uppgifter ur socialförsäkringsdatabasen till socialnämnderna. Genom en elektronisk förfrågan begär nämnderna att få information om en person i socialförsäkringsdatabasen. Efter en behörighetskontroll gör Försäkringskassans IT-system också en kontroll av att begäran endast omfattar sådan information som den aktuella nämnden med hänsyn till sekretessregler är behörig att få ut. Innan uppgifterna lämnas ut görs därefter ytterligare en elektronisk kontroll av att de inte omfattas av sekretess.

Högsta förvaltningsdomstolen konstaterade att socialnämnderna inte på egen hand kan söka information i socialförsäkringsdatabasen, utan att ett utlämnande genom LEFI Online i stället förutsätter att Försäkringskassan reagerar på en begäran om att lämna ut de efterfrågade uppgifterna. Med anledning av att Försäkringskassan därigenom – vid utlämningsstillfället – förfogar över frågan om och i så fall vilka uppgifter som ska lämnas ut, ansåg domstolen att socialnämnderna inte har någon sådan teknisk tillgång till upptagningar som avses i 2 kap. 3 § andra stycket TF. Förfarandet ska därmed inte anses utgöra direktåtkomst.

Frågan är om det finns några likheter mellan miljöboken och det datasystem som beskrivs i Högsta förvaltningsdomstolens avgörande. Vid läsbehörighet till miljöboken – som det skulle vara fråga om här – sker en behörighetskontroll vid inloggning. Därefter har den mottagande myndigheten med tekniska hjälpmedel tillgång till miljöboken och kan utan ytterligare kontroller av mark- och miljödomstolarna ta del av den information som finns där. Någon ytterligare prövning av rätten att ta del av uppgifter görs således inte, varken maskinellt eller manuellt. Mark- och miljödomstolarna har därmed inte någon kontroll över vilka uppgifter den som har läsbehörighet tar del av. I dagsläget sker inte heller någon loggning.

Den som har läsbehörighet kan göra sökningar på exempelvis respektive mark- och miljödomstol, verksamhetstyp (t.ex. vattentäkter eller miljöfarlig verksamhet), län, kommun, avrinningsområde och datum för avgörande. Även fritextsökningar är möjliga. Enligt vad vi erfarit är den fria sökningen bland samtliga uppgifter en del av syftet; utan möjlighet att ta del av all information kan den mottagande myndigheten inte få den helhetsbild av meddelade tillstånd som är avsikten med åtkomsten.

Mot bakgrund av ovanstående gör vi bedömningen att den åtkomst till miljöboken som det är fråga om här utgör direktåtkomst även utifrån den nyare praxis som finns på området.

21.3 Rättslig grund för behandling av personuppgifter i miljöboken

Förslag: Det ska av 8 § förordningen (1998:1388) om vattenverksamhet m.m. framgå att en mark- och miljödomstol ska föra en miljöbok och att domstolens förteckning över vattenverksamheter inom domsområdet (vattenbok) ska ingå i denna. Av samma bestämmelse ska det framgå att Domstolsverket får meddela föreskrifter om vattenboken.

Det ska av förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd framgå att en mark- och miljödomstol i den miljöbok som avses i 8 § förordningen om vattenverksamhet m.m. ska föra en förteckning över avgöranden som rör miljöfarlig verksamhet enligt miljöbalken och som domstolen meddelar som första instans. Av samma bestämmelse ska det framgå att Domstolsverket får meddela föreskrifter om denna förteckning.

För att personuppgiftsbehandling alls ska vara tillåten enligt data-skyddsförordningen måste ett antal krav vara uppfyllda. För det första måste det finnas en rättslig grund för personuppgiftsbehandlingen. De rättsliga grunder som kan komma i fråga framgår av artikel 6.1. Vad gäller domstolarnas verksamhet är det enligt vår mening främst de rättsliga grunderna i artikel 6.1 c och e som är av intresse. Enligt dessa bestämmelser är personuppgiftsbehandling tillåten om den är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige (led c), om den är nödvändig för att utföra en uppgift av allmänt intresse eller om den är nödvändig som ett led i den personuppgiftsansvariges myndighetsutövning (led e).

För det andra finns det – vilket framgår av utformningen av artikel 6.1 c och e – ett krav på att personuppgiftsbehandlingen ska vara *nödvändig* för att fullgöra den rättsliga förpliktelsen, utföra uppgiften av allmänt intresse eller som ett led i myndighets-

utövningen. Det räcker dock att en personuppgiftsbehandling bidrar till att effektivisera en myndighets verksamhet för att den ska anses vara nödvändig i dataskyddsförordningens mening (se kapitel 6).

För det tredje krävs att grunden för behandlingen (den rättsliga förpliktelsen, uppgiften av allmänt intresse eller myndighetsutövningen) är fastställd i unionsrätten eller medlemsstatens nationella rätt. Detta framgår av artikel 6.3 i dataskyddsförordningen.

Som vi tidigare har konstaterat (avsnitt 6.2.5) anser vi att mark- och miljödomstolarna för miljöboken inom ramen för den myndighetsutövande uppgift de har anförtrotts. Eftersom databasen bidrar till att domstolarna kan genomföra sitt uppdrag på ett rättssäkert sätt och till att effektivisera domstolarnas framtida målhantering, är den personuppgiftsbehandling som utförs genom miljöboken enligt vår mening också *nödvändig* som ett led i myndighetsutövningen. Den myndighetsutövning som anförtrotts domstolarna framgår vidare av lag. Utifrån vårt synsätt finns det därmed en rättslig grund enligt dataskyddsförordningen för att föra miljöboken.

Förändet av miljöboken är enligt vår mening också en del av domstolarnas rättskipande och rättsvårdande verksamhet, vilket innebär att personuppgiftsbehandlingen ryms inom domstolsdatalagens tillämpningsområde. Eftersom domstolsdatalagens primära ändamålsbestämmelse är avsedd att innefatta mål- och ärendehandläggningen i stort, är vi också av uppfattningen att den behandling av personuppgifter som sker inom ramen för miljöboken behövs för handläggningen av mål och ärenden (se avsnitt 9.1.6). Domstolarnas förande och användande av miljöboken ryms således även inom domstolsdatalagens ändamålsbestämmelser.

Skulle frågan om vilken rättslig grund som finns för förändet av miljöboken ställas på sin spets är det dock slutligen rättstillämparen som får bedöma om man kan betrakta förändet av miljöboken som en del av mark- och miljödomstolarnas myndighetsutövning. De allmänna domstolarnas myndighetsutövning kommer till uttryck genom den rättskipande verksamheten, för vilken de för närvarande har verksamhetssystemet Vera. En något snävare syn på vad som innefattas i mark- och miljödomstolarnas myndighetsutövning

skulle med den motiveringen kunna leda till att rättstillämparen inte anser att förändret av miljöboken är ett led i domstolarnas myndighetsutövning.

Vi anser dock att man i vart fall kan se förändret av miljöboken som en uppgift av allmänt intresse eller som en rättslig förpliktelse. Om någon av dessa rättsliga grunder utgör grunden för miljöbokens personuppgiftsbehandling bedömer vi emellertid att det finns en brist som måste åtgärdas. Detta har att göra med att förändret av miljöboken, enligt vår mening, inte genom nuvarande bestämmelser är tydligt reglerat vad gäller den del av miljöboken som innehåller uppgifter om tillstånd till miljöfarlig verksamhet.

I enlighet med artikel 6.3 i dataskyddförordningen krävs att den rättsliga förpliktelsen eller uppgiften av allmänt intresse fastställs i unionsrätten eller den nationella rätten. Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) också föreslagit att det i den nya dataskyddslagen ska tas in bestämmelser som tydliggör att begreppet uppgift av allmänt intresse avser 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. Dataskyddsutredningen har även föreslagit en bestämmelse med innebörden att en förpliktelse utgör en rättslig grund för behandling av personuppgifter endast om den gäller enligt lag eller annan författning, följer av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

Dataskyddsutredningen framhåller att formuleringen ”enligt lag eller annan författning” är menad att innefatta t.ex. förordningar som har meddelats av regeringen, med stöd av den restkompetens som följer av regeringsformen. Formuleringen innefattar även befogenheter som anges i myndighetsföreskrifter, förutsatt att föreskrifterna har meddelats med stöd av ett bemyndigande.¹

Om den rättsliga grunden för den personuppgiftsbehandling som sker i samband med registrering m.m. i miljöboken bedöms vara en rättslig förpliktelse eller en uppgift av allmänt intresse krävs således att förändret av miljöboken är rättsligt förankrat och fastställt i den laga ordning som gäller i Sverige. I annat fall uppfylls inte samtliga dataskyddsförordningens krav för att personuppgiftsbehandlingen ska kunna ske med stöd av dessa rättsliga grunder.

¹ Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 362).

Förändret av den del av miljöboken som utgörs av vattenboken regleras i 9 kap. 7 § lagen (1998:812) med särskilda bestämmelser om vattenverksamhet. Enligt denna bestämmelse ska en mark- och miljödomstol föra en förteckning över vattenverksamhet inom domsområdet (vattenbok) i den utsträckning som regeringen föreskriver. Regeringen har, genom 8 § förordningen (1998:1388) om vattenverksamhet m.m., föreskrivit att mark- och miljödomstolens förteckning över vattenverksamheter inom domsområdet ska föras i en miljöbok, som en vattenbok ska ingå i. Av samma bestämmelse framgår att Domstolsverket får meddela föreskrifter om miljöboken.

Enligt 8 kap. 1 § RF ska ett bemyndigande för myndighet att meddela föreskrifter alltid ges i lag eller förordning. Så som bestämmelserna i lagen med särskilda bestämmelser om vattenverksamhet och förordningen om vattenverksamhet m.m. är utformade regleras enligt vår mening endast tydligt att meddelade tillstånd till vattenverksamhet ska föras in i miljöboken. De tillstånd till miljöfarlig verksamhet som domstolarna meddelar nämns inte i lagen eller förordningen. Först i 2 § Domstolsverkets föreskrifter (DVFS 2011:2) om miljöboken framgår att avgöranden i frågor som rör miljöbalken ska föras in i miljöboken.

Vi anser att det kan diskuteras om Domstolsverkets bemyndigande att meddela föreskrifter gällande miljöboken även innefattar de avgöranden som rör miljöfarlig verksamhet enligt 9 kap. MB. I vilket fall anser vi inte att regleringen är klar och tydlig i detta avseende.

För att det framöver ska stå fullständigt klart att den personuppgiftsbehandling som sker inom ramen för miljöboken vilar på en rättslig grund i enlighet med dataskyddsförordningen, anser vi att det bör införas bestämmelser i lag eller förordning som reglerar förändret av den del av miljöboken som avser tillstånd till miljöfarliga verksamheter. Detta skulle även få till följd att det inte skulle finnas någon anledning att tvivla på att Domstolsverkets föreskrifter om miljöbokens innehåll är fattade i laga ordning.

Bestämmelser om förändret av miljöboken bör enligt vår mening falla inom regeringens restkompetens enligt 8 kap. 7 § RF. Detta innebär att bestämmelser om miljöbokens innehåll bör kunna meddelas i förordning.

Ett enkelt sätt att åtgärda problemet med Domstolsverkets bemyndigande vore att komplettera den befintliga bestämmelsen i 8 § första stycket förordningen om vattenverksamhet m.m. så att det framgår att även avgöranden i frågor som rör miljöbalken ska ingå i miljöboken. Denna förordning gäller dock vattenverksamhet och vattenanläggningar (jfr 1 kap. 1 § lagen med särskilda bestämmelser om vattenverksamhet). Att ta in bestämmelser om miljöfarlig verksamhet i den förordningen skulle enligt vår mening innebära att man frångår den befintliga lagstiftningssystematiken.

I stället föreslår vi en lösning där den del av miljöboken som gäller vattenverksamheter (vattenboken) fortsatt regleras i förordningen om vattenverksamhet m.m.. Den del som gäller miljöfarlig verksamhet bör i stället regleras i förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd, som på miljöområdet motsvarar förordningen om vattenverksamhet m.m. För att åstadkomma detta föreslår vi följande.

Bestämmelsen i 8 § förordningen om vattenverksamhet m.m. bör ändras så att det framgår att en mark- och miljödomstol ska föra en miljöbok, där domstolens förteckning över vattenverksamheter inom domsområdet (vattenbok) ska ingå. Domstolsverkets föreskriftsrätt enligt samma bestämmelse bör enbart omfatta föreskrifter om vattenboken.

För att undvika dubbelreglering av den del av miljöboken som rör vattenverksamheter bör förordningen om miljöfarlig verksamhet och hälsoskydd kompletteras med en ny bestämmelse som innebär att en mark- och miljödomstol i den miljöbok som avses i 8 § förordningen om vattenverksamhet m.m. ska föra en förteckning över avgöranden som rör miljöfarlig verksamhet enligt miljöbalken och som domstolen meddelar som första instans. Av samma bestämmelse bör det framgå att Domstolsverket får meddela föreskrifter om denna förteckning.

På detta sätt skulle man enligt vår mening förhållandevis enkelt kunna åtgärda de befintliga oklarheterna kring Domstolsverkets föreskriftsrätt.

Upplysningsvis har vi i vårt arbete med miljöboken blivit uppmärksammade på att den beskrivning av miljöbokens innehåll som för närvarande finns i 8 § förordningen om vattenverksamhet m.m. samt 2 § Domstolsverkets föreskrifter om miljöboken omfattar fler måltyper än de som rent faktiskt registreras i

miljöboken. Det rör sig exempelvis om vissa ersättningsmål, som avgörs i första instans av mark- och miljödomstolarna. Vårt uppdrag innebär emellertid endast att ta ställning till behovet av direktåtkomst till miljöboken för de aktuella myndigheterna samt att se över lagstiftningen med anledning av dataskyddsförordningen. Mot den bakgrunden och med hänsyn till den tidsmässiga aspekten för uppdraget, kan vi inte nu behandla denna fråga.

21.4 Vilka myndigheter är aktuella för direktåtkomst?

I vårt uppdrag har de myndigheter som skulle kunna komma i fråga för direktåtkomst till miljöboken exemplifierats med angivande av Kammarkollegiet, länsstyrelserna, Naturvårdsverket och Havs- och vattenmyndigheten. Dessa myndigheter ska, enligt 22 kap. 6 § första stycket MB, när det behövs föra talan i ansökningsmål vid mark- och miljödomstolarna för att ta tillvara miljöintressen och andra allmänna intressen. De har även behörighet att enligt 24 kap. 7 § MB ansöka om omprövning av befintliga tillstånd. Detta gäller också för Myndigheten för samhällsskydd och beredskap, MSB, som tillsammans med länsstyrelsen är tillsynsmyndighet enligt 15 § lagen (1999:381) om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor (den s.k. Sevesolagen). Enligt 22 kap. 6 § andra stycket MB får också en kommun föra talan i ansökningsmål vid mark- och miljödomstolarna för att tillvarata miljöintressen och andra allmänna intressen inom kommunen. Kommunernas miljönämnder är också tillsynsmyndigheter för vissa miljöfarliga verksamheter (se avsnitt 21.5.4). Utifrån de uppgifter inom miljö- och vattenskydd som MSB och kommunernas miljönämnder har anser vi att även deras behov av en direktåtkomst bör analyseras inom ramen för vårt uppdrag.

För läsbarhetens skull kommer vi framöver i detta kapitel att använda begreppet *de aktuella myndigheterna* när vi avser samtliga de myndigheter vars behov av direktåtkomst vi analyserar.

21.5 De aktuella myndigheternas verksamhet relaterat till miljöboken

21.5.1 Ansökan respektive anmälan om vattenverksamhet

Vattenverksamhet innebär, enligt 11 kap. 3 § MB, bl.a. åtgärder som företas i ett vattenområde. Som exempel kan nämnas uppförande eller ändring av anläggning, fyllning, pålning, grävning, sprängning och rensning. För att få bedriva vattenverksamhet krävs som huvudregel tillstånd, som meddelas av mark- och miljödomstol (se 11 kap. 9 och 9 b §§ MB). När en ansökan om tillstånd till vattenverksamhet kommer in till mark- och miljödomstolen ska domstolen, enligt 22 kap. 4 § MB, skicka kopior av kungörelsen och normalt även ansökningshandlingarna till Naturvårdsverket, Kammarkollegiet, Havs- och vattenmyndigheten, MSB, länsstyrelsen och den eller de berörda kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet. Av 22 kap. 6 § första stycket MB framgår att de nyss nämnda statliga myndigheterna ska föra talan i målet för att tillvarata miljöintressen och andra allmänna intressen, när det behövs. Även en kommun får, enligt andra stycket i samma bestämmelse, föra talan i målet för att tillvarata miljöintressen och andra allmänna intressen inom kommunen.

Vissa vattenverksamheter av mindre omfattning är endast anmälningspliktiga. Vilka dessa är framgår av 19 § förordningen (1998:1388) om vattenverksamhet m.m.. Länsstyrelsen är tillsynsmyndighet för dessa verksamheter, enligt 2 kap. 29 § första stycket 2 miljötillsynsförordningen (2011:13). Länsstyrelsen ska i sin egenskap av tillsynsmyndighet, enligt 21 § förordningen om vattenverksamhet m.m., sända en kopia av anmälan till den kommunala hälso- och miljönämnden. Om det allmänna fiskeintresset berörs, ska en kopia också sändas till Havs- och vattenmyndigheten. Vidare ska de statliga och kommunala myndigheter som kan ha ett särskilt intresse i saken ges tillfälle att yttra sig i anmälningsärendet enligt 22 § förordningen om vattenverksamhet m.m.

21.5.2 Ansökan respektive anmälan om miljöfarlig verksamhet

All användning av mark, byggnader eller anläggningar som kan ge upphov till utsläpp till mark eller vatten eller medföra andra störningar för människors hälsa eller för miljön, anses vara miljöfarlig verksamhet. Vilka typer av verksamhet som omfattas av begreppet definieras i 9 kap. 1 § MB.

Miljöfarlig verksamhet delas in i A-, B- och C-verksamheter beroende på verksamhetens omfattning och miljöpåverkan. Vilken verksamhet som hör till vilken kategori klargörs i miljöprövningsförordningen (2013:251). För att få anlägga, ändra och driva A- och B- anläggningar krävs tillstånd. A-anläggningar – bl.a. gruvdrift, större pappersbruk och större avfallsförbränningsanläggningar – tillståndsprövas av någon av de fem mark- och miljödomstolarna. B-anläggningar, till vilka bl.a. avloppsreningsverk, större anläggningar för djurhållning och större täkter av berg och grus hör, tillståndsprövas av en länsstyrelses miljöprövningsdelegation.²

För A- och B-anläggningar måste en samrådsprocess ske innan prövningen. Detta framgår av 6 kap. 4 § och 22 kap. 1 § 3 MB (vad gäller förfarandet vid mark- och miljödomstol) respektive 19 kap. 4 § 2 MB (vad gäller länsstyrelsens miljöprövningsdelegation). I samrådet deltar länsstyrelsen, tillsynsmyndigheten – som kan vara en miljö- och hälsoskyddsnämnd – och de enskilda som kan antas bli särskilt berörda. Beroende på anläggningens karaktär deltar även andra myndigheter. Exempelvis kan Naturvårdsverket, Havs- och vattenmyndigheten och MSB delta i samrådet om verksamhet antas medföra en betydande miljöpåverkan (6 kap. 4 § 1 och 2 MB).

När en ansökan om tillstånd till miljöfarlig verksamhet kommer in till mark- och miljödomstolen ska domstolen, enligt 22 kap. 4 § MB, skicka kopior av ansökningshandlingar och kungörelse till Naturvårdsverket, Havs- och vattenmyndigheten, Kammarkollegiet, MSB, länsstyrelsen och den eller de berörda kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet. De nyss nämnda statliga myndigheterna ska, enligt 22 kap. 6 § MB, föra talan i målet när det behövs för att tillvarata

² Se 16 § länsstyrelseinstruktionen (2007:825) och förordningen (2011:1237) om miljöprövningsdelegationer.

miljöintressen och andra allmänna intressen. Även en kommun får föra talan för att tillvarata miljöintressen och andra allmänna intressen inom kommunen.

Enligt 9 § förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd ska en länsstyrelse meddela kommunens miljö- och hälsoskyddsnämnd, Naturvårdsverket, Havs- och vattenmyndigheten och MSB när en ansökan om tillstånd att bedriva B-verksamhet har kommit in till länsstyrelsen.

För att få anlägga och driva en C-anläggning krävs endast att en anmälan görs. I de flesta fall är det kommunens miljö- och hälsoskyddsnämnd som ska ta emot en sådan anmälan. Exempel på C-anläggningar är större värmepumpar, täkter av berg eller grus för husbehov och enstaka större vindkraftverk. Miljöfarlig verksamhet som inte klassas som A-, B- eller C-verksamhet behöver inte förprövas eller anmälas. I stället kan kommunens miljö- och hälsoskyddsnämnd, som är tillsynsmyndighet, när som helst kräva åtgärder eller utredningar om det behövs av miljö- eller hälsoskyddsskäl.

21.5.3 Omprövning av tillstånd

Enligt 24 kap. 5 § MB får tillstånd till miljöfarlig verksamhet eller vattenverksamhet under vissa förutsättningar omprövas av tillståndsmyndigheten. Enligt 24 kap. 7 § MB får en ansökan om omprövning göras hos mark- och miljödomstol av Naturvårdsverket, Havs- och vattenmyndigheten, Kammarkollegiet, MSB och länsstyrelsen. Om frågan ska prövas av någon annan myndighet än en domstol eller av en kommun, får den dock tas upp utan någon särskild framställning. En ansökan om omprövning får även göras av en kommun i den utsträckning kommunen har övertagit tillsynen med stöd av 26 kap. 3 § fjärde stycket MB.

21.5.4 Tillsyn och tillsynsvägledning

Av 26 kap. 3 § MB framgår att tillsynen över att balken och dess föreskrifter följs utövas av bl.a. Naturvårdsverket, Havs- och vattenmyndigheten, länsstyrelsen och kommunerna i enlighet med vad regeringen bestämmer. I miljötillsynsförordningen (2011:13)

finns bestämmelser om vilken myndighet som är behörig att utöva miljötillsyn på olika områden.

Den operativa tillsynen regleras i 2 kap. miljötillsynsförordningen och enligt 2 kap. 29 § har länsstyrelsen, med vissa undantag, tillsynsansvar över verksamheter som är tillståndspliktiga enligt miljöprövningsförordningen (2013:251) och bilagan till förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd. Enligt samma bestämmelse har länsstyrelsen det huvudsakliga tillsynsansvaret över vattenverksamheter. Den tillsyn länsstyrelserna bedriver kan initieras antingen på myndighetens eget initiativ (t.ex. genom riktade tillsynskampanjer gällande särskilda objekt) eller genom att exempelvis ett företag eller en privatperson uppmärksammar myndigheten på att en verksamhet bedrivs.

Enligt 2 kap. 31 § miljötillsynsförordningen har en kommuns miljönämnd visst tillsynsansvar över tillståndspliktiga miljöfarliga verksamheter och vattentäkter som omfattas av tillståndsplikt.

Enligt 2 kap. 9 a § miljötillsynsförordningen är Naturvårdverket operativ tillsynsmyndighet för bl.a. vissa frågor gällande skydd för djur- och växtarter (jfr 8 kap. 5 § andra stycket MB).

Enligt 15 § lagen (1999:381) om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor har MSB och länsstyrelsen tillsyn över att den lagen med tillhörande föreskrifter följs.

Enligt 11 kap. 8 § MB och 6 kap. 5–10 §§ lagen (1998:812) med särskilda bestämmelser om vattenverksamhet, kan mark- och miljödomstolarna besluta om särskilda fiskeavgifter. Havs- och vattenmyndigheten har ansvar för användandet av dessa avgifter, som ska betalas till myndigheten när mark- och miljödomstolens dom vunnit laga kraft. Havs- och vattenmyndigheten har också ansvar för att bevaka ett antal allmänna intressen, såsom riksintresset för yrkesfiske, riksintresset för naturvård och friluftsliv inom verksamhetsområdet och riksintresset för anläggningar för dricksvattenförsörjning (se 3 kap 5, 6 och 8 §§ MB).

Utöver den tillsyn över vattenverksamheter eller miljöfarliga verksamheter som många av de aktuella myndigheterna bedriver ska Naturvårdsverket, Havs- och vattenmyndigheten och MSB ge tillsynsvägledning i fråga om tillämpningen av miljöbalken och andra bestämmelser på miljöområdet inom sina respektive

ansvarsområden. Detta framgår av 3 kap. 1, 2, 5 och 8 §§ miljö-tillsynsförordningen.

21.5.5 Samhällsplanering

Sveriges kommuner har, enligt 1 kap. 2 § plan- och bygglagen (2010:900), ansvar för planering av mark och vatten inom sina respektive områden. Av 5 § havsplaneringsförordningen (2015:400) framgår vidare att Havs- och vattenmyndigheten är ansvarig för att ta fram förslag till havsplaner. Syftet med havsplanerna är att ge vägledning om den mest lämpade användningen av havsområdena.

21.6 De aktuella myndigheternas möjlighet till direktåtkomst

21.6.1 Proportionalitetsbedömning

Enligt artikel 5.1 a i dataskyddsförordningen måste behandling av personuppgifter alltid vara korrekt i förhållande till den registrerade. I denna princip om *korrekthet* ingår att behandlingen ska vara skäligen och rimlig i förhållande till den registrerade.³ För att säkerställa att behandlingen av en personuppgift är skäligen ska det för varje behandling göras en proportionalitetsbedömning. I den bedömningen vägs behovet av den konkreta behandlingen mot den registrerades intresse av personlig integritet. En behandling av personuppgifter som innebär risker för den personliga integriteten får då genomföras endast om fördelarna med behandlingen står i rimlig proportion till riskerna. Säkerhetsåtgärder som minskar riskerna för den personliga integriteten har här stor betydelse.⁴

³ Jfr Dataskyddsutredningens betänkande (SOU 2017:39 s. 106 f.).

⁴ Samma krav gäller enligt artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter, nr 108 samt artikel 7 och 8 i EU:s stadga om de grundläggande rättigheterna (2010/C 83/02), jfr Datainspektionen Vägledning för integritetsanalys, september 2016 och Integritetsskyddskommitténs betänkande (SOU 2007:22 s. 449 f.).

21.6.2 Behovet av direktåtkomst

I enlighet med vårt uppdrag har vi inhämtat synpunkter från de aktuella myndigheterna gällande eventuell direktåtkomst till miljöboken. I detta avsnitt gör vi en sammanställning av det behov av sådan åtkomst som myndigheterna själva har gett uttryck för.

Länsstyrelsen

Miljöboken innehåller samtliga vattendomar från år 1919 och framåt. Länsstyrelserna har direktåtkomst till miljöboken och har uppgett att den är den enda tillförlitliga källan gällande tillståndsgivna vattenverksamheter. Länsstyrelserna menar också att miljöboken används i princip dagligen i myndighetens tillsyn över vattenverksamheter. Detta ger en stor tidsvinst, eftersom man genom miljöboken på ett enkelt sätt kan få en överblick över meddelade tillstånd och ta del av information gällande de tillståndsgivna anläggningarna. Som ett konkret exempel har nämnts att det under bevattningssäsongen är mycket tidsbesparande att genom en kontroll i miljöboken få information om en verksamhetsutövers eventuella tillstånd för det vattenuttag som länsstyrelsen uppmärksammas på av en utomstående anmälare.

Miljöboken används också vid tillsyn som initieras av länsstyrelserna själva, exempelvis för att planera tillsynen genom att prioritera bland objekten och besluta inriktningen för tillsynen av enskilda objekt. För anmälningspliktiga vattenverksamheter ger miljöboken vidare information om eventuella äldre meddelade tillstånd för en viss verksamhet eller om det finns tillståndsgivna verksamheter i närheten som behöver beaktas i ett visst ärende. Länsstyrelsen kan t.ex. utifrån informationen i miljöboken bedöma om det i en inlämnad s.k. vattenbalansberäkning i ett anmälningsärende har tagits hänsyn till alla andra uttag av vatten i området.

För länsstyrelsernas del används miljöboken också i samrådsprocessen vid tillståndsprövningar och vid rådgivning till sökande om vilka parter som behöver ingå i samrådskretsen. Eftersom miljöboken ger en samlad överblick av antalet vattenuttag och miljöfarliga verksamheter inom ett specifikt område används den även vid bedömning av vattenstatus och miljökvalitetsnormer i

enlighet med EU:s ramdirektiv för vatten⁵ och förordningen (2004:660) om förvaltning av kvaliteten på vattenmiljön.

Länsstyrelserna menar avslutningsvis att deras trovärdighet som tillsynsmyndighet skulle minska om de inte hade kunskap om befintliga större vattenverksamheter. Utan direktåtkomst till miljöboken skulle länsstyrelserna behöva vända sig till respektive domstol för att få information om befintliga vattendomar. Tillsynsarbetet skulle då försvåras eftersom samma verksamhet kan styras av flera tillstånd som finns i olika domar. Det vore mycket svårare och mer tidsödande att begära ut domar från mark- och miljödomstolarna när målnumren är okända. Både allmänna och enskilda intressen riskerar att skadas om relevanta domar missas i en tillståndsprocess eller i ett tillsyns- eller åtgärdsärende.

Kommunerna

Sveriges kommuner och landsting, SKL, har för kommunernas räkning anfört följande. Kommunernas tillsynsverksamhet kräver tillgång till de senaste domarna och besluten som rör den aktuella verksamheten. För tillsynsuppdraget skulle direktåtkomst till miljöboken underlätta i vissa fall. Även vid hantering av andra ärenden inom hälso- och miljöskydd kan verksamheter som registerats i miljöboken vara av intresse. För planering av mark och vatten inom kommunen enligt plan- och bygglagen (2010:900) finns också behov av att känna till vilka vattenverksamheter och miljöfarliga verksamheter som finns i närområdet. Direktåtkomst skulle därmed vara en intressant möjlighet för att underlätta arbetet och minska tidsåtgången. Detta gäller särskilt i frågor om diknings- och markavvattningsföretag.

Kammarkollegiet

Kammarkollegiet har hänvisat till att direktåtkomst till miljöboken skulle fylla ett behov när kollegiet för talan enligt 22 kap. 6 § MB eller initierar en ansökan om omprövning eller återkallelse av ett

⁵ Europaparlamentets och rådets direktiv 2000/60/EG av den 23 oktober 2000 om upprättande av en ram för gemenskapens åtgärder på vattenpolitikens område.

befintligt tillstånd för att åstadkomma miljöförbättrande åtgärder. Kammarkollegiet menar emellertid även att myndigheten ibland får remisser från mark- och miljödomstolarna och Mark- och miljööverdomstolen i mål där myndigheten inte är part. För ett korrekt yttrande behöver kollegiet då vanligen information om de olika tillstånd som gäller för den aktuella verksamheten.

I mål där Kammarkollegiet för talan i någon form krävs kännedom om tidigare domar och beslut som rör den aktuella och närliggande verksamheter för att processen ska bli effektiv och rättssäker. Som ett praktiskt exempel har tillstånd till vattenverksamheter – exempelvis uppförande och drift av vattenkraftverk – nämnts. För dessa verksamheter kan det finnas flera relevanta domar från olika tidsperioder, där tillstånd, lagligförklaring och villkorsändringar prövats. I äldre avgöranden finns således ofta viktig information om tillståndet i miljön eller villkor för hur verksamheten ska bedrivas. Det är av stor vikt att dessa uppgifter kommer fram vid en ny tillståndsprövning, eftersom det avgör vilken miljöpåverkan som kan komma att följa av domstolens avgörande. Om Kammarkollegiet får direktåtkomst till miljöboken kan kollegiet få kännedom om tidigare avgöranden och risken för att viktig information inte kommer fram vid prövningen minskar.

Havs- och vattenmyndigheten

Havs- och vattenmyndigheten har, i likhet med Kammarkollegiet, anfört att myndigheten ibland föreläggs av mark- och miljödomstolarna att yttra sig i tillståndsmål. Myndigheten menar också att flera miljöbalksmål ofta har en lång historik av avgöranden som behöver beaktas för att talan enligt 22 kap. 6 § MB ska kunna föras på ett rättssäkert sätt. Som exempel nämns att det i mål om tillstånd till utökad produktion vid en gruva oftast finns ett flertal äldre tillstånd, flera deldomar med löpande prövotider och prövningar av en viss avgränsad del av verksamheten som måste beaktas. Även domar som rör andra verksamheter som belastar samma vattenrecipient eller fastighet kan ha betydelse i ett tillståndsmål.

Havs- och vattenmyndigheten menar vidare att det faktum att myndigheten vid direktåtkomst skulle ha tillgång till korrekta

målnummer etc. skulle underlätta mark- och miljödomstolarnas arbete med att eftersöka domar och beslut efter myndighetens begäran. Både domstolarnas och Havs- och vattenmyndighetens arbetssätt skulle på detta sätt effektiviseras och ärendehanteringens hos myndigheten skulle bli mer rättssäker. Även för verksamhetsutövaren skulle detta kunna innebära fördelar i form av snabbare och bättre tillståndsprocesser.

Havs- och vattenmyndigheten har också anfört att en mer rättssäker hantering skulle få positiva effekter för miljön. Det finns risk för att äldre domar med betydelsefull information inte uppmärksammas i tillståndsprocessen vid mark- och miljödomstolarna, vilket i sin tur innebär att inte heller Havs- och vattenmyndigheten får vetskap om dessa domar. Eftersom det i äldre domar kan finnas uppgifter som skulle kunna påverka utgången i målet om de vore kända, har detta indirekt betydelse för vilken påverkan som tillåts ske i miljön. Om Havs- och vattenmyndigheten skulle få direktåtkomst till miljöboken skulle alla tidigare avgöranden bli kända för myndigheten och risken för att viktig information missas skulle minimeras.

Direktåtkomst till miljöboken skulle även innebära att Havs- och vattenmyndighetens hanteringen av särskilda fiskeavgifter kan rationaliseras. Domstolarna skulle inte behöva skicka ett särskilt meddelande till myndigheten när en dom om sådana avgifter vunnit laga kraft. Även arbetet med att vägleda tillsynsmyndigheterna i tillsynsarbetet skulle underlättas om det fanns möjlighet att få en överblick över tillstånd inom olika områden. Vid revidering av befintliga riksintressen inom myndighetens ansvarsområde och havsplanering skulle det också vara till fördel för Havs- och vattenmyndigheten att ha direkt tillgång till meddelade domar och beslut.

MSB

De verksamheter som hanterar farliga ämnen i så stora kvantiteter att de omfattas av den s.k. Sevesolagstiftningen på den högre

kravnivån är skyldiga att upprätta en säkerhetsrapport.⁶ Under tillståndsprövningen remitteras säkerhetsrapporten till MSB, som har anfört att det vid granskning av säkerhetsrapporten kan vara till nytta att se vilka tidigare tillstånd till miljöfarlig verksamhet och vattenverksamhet som finns. MSB har vidare anfört att andra miljöfarliga verksamheter kan påverka de Sevesoanläggningar som MSB och länsstyrelserna utövar tillsyn över. MSB menar också att vissa ansökningar är svåra att förstå utan tillgång till tidigare domar och har – liksom Havs- och vattenmyndigheten och Kammarkollegiet – uppgett att det finns ett behov av att få en fullständig bild av befintliga tillstånd inför exempelvis ett yttrande till mark- och miljödomstol.

Naturvårdsverket

Naturvårdsverket har uppgett att verket har behov av information om domar och slutliga beslut från mark- och miljödomstolarna och från Mark- och miljööverdomstolen bl.a. när verket utför operativ tillsyn, i verkets tillsynsvägledning och när verket agerar part i tillståndsprocessen vid mark- och miljödomstolarna enligt 22 kap. 6 § MB.

21.6.3 Avvägning mellan behovet och integritetsskyddet

Av de synpunkter som de aktuella myndigheterna lämnat framkommer enligt vår mening klart att direktåtkomst till miljöboken fyller ett behov. Det förefaller främst handla om en effektivisering av myndigheternas arbete i deras egenskap av parter i mål om tillstånd och omprövningar samt i rollen som tillståndsgivare och tillsynsmyndigheter. Eftersom myndigheterna vid direktåtkomst skulle ha möjlighet att göra behövliga eftersökningar i miljöboken på egen hand, skulle de behöva kontakta mark- och miljödomstolarna först när de relevanta domarna har identifierats. Detta skulle i sin tur leda till att mark- och miljödomstolarnas

⁶ Se 10 § lagen (1999:381) om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor och 9 § förordning (2015:236) om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor.

administrativa verksamhet avlastas. Direktåtkomst till miljöboken för de aktuella myndigheterna skulle vidare bidra till att det föreskrivna skyddet för miljön och vatten kan upprätthållas i tillståndsprocessen gällande miljöfarliga verksamheter och vattenverksamheter, eftersom det bidrar till att samtliga omständigheter som kan påverka t.ex. en tillståndsprövning uppmärksammas. Detta ligger enligt vår mening i allmänhetens intresse, oavsett om tillståndet meddelas av en förvaltningsmyndighet, en kommun eller av mark- och miljödomstolarna.

Behovet av direktåtkomst hos de aktuella myndigheterna och den samhällsnytta en sådan direktåtkomst skulle kunna innebära ska dock vägas mot de registrerades intresse av skydd för den personliga integriteten.

De personuppgifter som finns i miljöboken är begränsade. Känsliga personuppgifter eller uppgifter för vilka sekretess råder ska inte förekomma. Det rör sig vidare främst om indirekta personuppgifter; personnamn är sparsamt förekommande. Personuppgifternas begränsade förekomst och deras icke integritetskränkande karaktär medför enligt vår uppfattning att integritetsriskerna med direktåtkomst är mycket små. De domar och beslut som registreras i miljöboken rör vidare, i de allra flesta fall, tillstånd som sökts av verksamhetsutövare i en yrkesverksamhet. Av detta drar vi slutsatsen att risken för att uppgifter ur miljöboken skulle kunna användas för att kartlägga fysiska personers liv är i det närmaste obefintlig.

I detta sammanhang vill vi också lyfta fram att den personuppgiftsansvariga mark- och miljödomstolen kommer att ha en skyldighet att, enligt artikel 13.1 e i dataskyddsförordningen, informera den registrerade om vilka mottagare som kommer att ta del av hans eller hennes personuppgifter. Denna rätt till information gäller när personuppgifter samlas in från den registrerade själv, vilket bör vara fallet i de ansökningsmål som anhängiggörs vid mark- och miljödomstolarna av enskilda fysiska personer (se avsnitt 15.3.3). Direktåtkomst utgör ett ständigt utlämnande av alla de uppgifter åtkomsten avser. Detta innebär enligt vår mening att om direktåtkomst till miljöboken inrättas måste mark- och miljödomstolarna vid ansökningar från fysiska personer informera dessa om vilka mottagare som har sådan åtkomst. Den registrerade kommer således att få kännedom om

vilka myndigheter som har tillgång till hans eller hennes personuppgifter och kan därmed ta tillvara sina rättigheter i samband med dessa myndigheters behandling av personuppgifterna. Som vi har uppfattat det kommer ansökningar från fysiska personer dock att vara sparsamt förekommande. När så är fallet kommer domstolarna vidare – även om de aktuella myndigheterna inte har direktåtkomst till miljöboken – att vara tvungna att ge den sökande viss information i enlighet med artikel 13 i dataskyddsförordningen (se avsnitt 15.3.2). Eftersom information om mottagarna av personuppgifterna kan ges standardiserat och vid samma tillfälle som övrig information, anser vi att de aktuella myndigheternas direktåtkomst inte skulle innebära någon stor administrativ börda för mark- och miljödomstolarna i detta avseende.

En integritetsrisk som uppstår vid all direktåtkomst är att den mottagande myndigheten kan vara skyldig att enligt tryckfrihetsförordningen lämna ut de personuppgifter som omfattas av direktåtkomsten. Detta kan också innebära en skyldighet att lämna ut en sammanställning av uppgifter som kan göras genom en sökning bland tillgängliga uppgifter (se avsnitt 17.3.1). Ett sätt att begränsa den integritetsrisk detta skulle kunna medföra vore att begränsa vilka uppgifter direktåtkomsten omfattar. Vad gäller miljöboken anser vi emellertid att detta inte är ett alternativ. Befintliga vattenverksamheter påverkar miljöfarliga verksamheter och tvärtom, vilket medför att det inte vore ändamålsenligt att ge vissa myndigheter tillgång till endast registrerade miljöfarliga verksamheter och andra myndigheter tillgång till endast registrerade vattenverksamheter. Samma ansökan kan dessutom omfatta både vattenverksamhet och miljöfarlig verksamhet. Inte heller tidsmässigt finns det enligt vår mening möjlighet att begränsa tillgången, eftersom de befintliga tillstånd som kan påverkas av eller påverka en ny ansökan om tillstånd eller omprövning kan vara mycket gamla. Dessutom bygger en ansökan om tillstånd ofta på ett redan befintligt tillstånd. Om en myndighet får tillgång till endast delar av miljöbokens innehåll skulle detta också innebära att själva syftet med åtkomsten – en samlad bild av samtliga meddelade tillstånd – går förlorat. Eftersom de personuppgifter som finns i miljöboken inte är av känslig karaktär, inte är sekretessbelagda och mestadels är indirekta, anser vi dock att en

fullständig åtkomst till miljöboken för de aktuella myndigheterna inte utgör en risk för de registerades personliga integritet.

Direktåtkomst innebär vidare att tjänstemännen på den mottagande myndigheten har möjlighet att hämta hem information till sitt eget system och bearbeta den där. Samtliga de aktuella myndigheterna har dock anförtrotts en uppgift av allmänt intresse som innebär att allmänhetens intresse av miljö- och vattenskydd ska tillvaratas. Det får enligt vår mening förutsättas att de personuppgifter som hämtas från miljöboken endast används i denna del av myndigheternas verksamhet. En del av själva syftet med direktåtkomst till miljöboken är vidare att myndigheterna använder den information de får tillgång till, bl.a i sitt tillsynsuppdrag. Med hänsyn till personuppgifternas begränsade förekomst och icke integritetskränkande karaktär anser vi att det inte är nödvändigt att i lag eller förordning föreskriva för vilket ändamål de mottagande myndigheterna får inhämta uppgifter från miljöboken. Det bör dock påpekas att den mottagande myndigheten blir personuppgiftsansvarig för den behandling som utförs av den myndighetens tjänstemän. Med detta följer bl.a. ett ansvar att se till att personuppgifterna hanteras i enlighet med gällande principer och att tillgången till miljöboken begränsas till de tjänstemän som behöver den i sitt arbete.⁷

Vid all direktåtkomst till en annan myndighets databas finns det en risk för att felaktiga uppgifter sprids utanför värdmyndigheten. Enligt artikel 5.1 d i dataskyddsförordningen ska felaktiga personuppgifter rättas utan dröjsmål. Mot den bakgrunden och med hänsyn till att miljöboken innehåller ett mycket begränsat antal direkta personuppgifter, anser vi att denna risk inte utgör något hot mot den personliga integriteten.

Ovanstående analys talar enligt vår mening för att den nytta direktåtkomst till miljöboken skulle innebära för de aktuella myndigheterna och för allmänhetens intresse av miljöskydd, överväger de integritetsrisker som en sådan direktåtkomst kan ge upphov till. Det finns emellertid ytterligare aspekter som bör analyseras före vårt slutliga ställningstagande i frågan.

⁷ Jfr principen om korrekthet i artikel 5.1 a i dataskyddsförordningen. Enligt artikel 32 i förordningen ska den personuppgiftsansvarige vidare vidta tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

Miljöbokens syfte måste enligt vår mening vara att se till att hanteringen av framtida ansökningsmål hos mark- och miljödomstolarna effektiviseras och att rättstillämpningen blir enhetlig. Om innehållet i miljöboken sprids till andra myndigheter som ska ta tillvara allmänhetens intresse av skydd för miljön kan det möjligen diskuteras om det är lämpligt att förandet av miljöboken ligger på domstolarna. Det finns en risk att domstolarnas opartiskhet kan ifrågasättas om de åläggs andra uppgifter av allmänt intresse utöver den rättskipande och rättsvårdande verksamheten. Samtidigt är det mest naturligt att mark- och miljödomstolarna för in information i miljöboken, eftersom databasen endast innehåller dessa domstolars avgöranden.

Ytterligare en aspekt av detta är att samtliga de myndigheter som är aktuella för direktåtkomst till miljöboken har möjlighet att föra talan i ansökningsmål och ansöka om omprövning hos mark- och miljödomstol enligt 22 kap. 6 § respektive 24 kap. 7 § MB. Många av myndigheterna har dessutom anfört att sådan direktåtkomst skulle underlätta för myndigheterna i just denna situation. Det är således fråga om att ge myndigheter som kan agera som offentlig part i mål hos mark- och miljödomstolarna direkt tillgång till en av domstolarnas databaser, som enskild part inte på samma sätt har tillgång till. Det kan diskuteras om detta skulle innebära att enskilda parter missgynnas och att likställighetsprincipen, det vill säga balansen mellan parterna, inte upprätthålls.

Miljöboken är dock inte ett ärendehanteringssystem, utan endast en databas där mark- och miljödomstolarnas avgöranden registreras. Enskilda parter har full tillgång till de uppgifter som finns i miljöboken genom att begära ut dem hos mark- och miljödomstolarna. Den skillnad som skulle uppstå mellan parterna är därmed endast att enskild part inte får samma överskådliga bild av befintliga anläggningar som myndigheterna. Eftersom miljöboken inte innehåller några känsliga personuppgifter eller sekretessbelagda uppgifter skulle man eventuellt kunna åtgärda detta problem genom att göra innehållet i miljöboken publikt tillgängligt på internet. Det ligger dock inte inom ramen för vårt uppdrag att lämna sådana förslag. Det kan i detta sammanhang även påpekas att verksamhetsutövaren under bl.a. det samrådsförfarande som ska föregå en ansökan, skulle ha möjlighet att med hjälp av

länsstyrelsen få tillgång till information om befintliga anläggningar och deras tillstånd.

Även med hänsyn tagen till de nyss nämnda frågeställningarna anser vi att den effektivisering som direktåtkomst till miljöboken kan medföra för de aktuella myndigheternas ärendehandläggning, överväger de mycket begränsade risker för den personliga integriteten som en sådan åtkomst medför. Ytterligare skydd för den personliga integriteten kan emellertid skapas genom att regleringen av direktåtkomsten utformas som en möjlighet för den enskilda mark- och miljödomstolen att bereda de aktuella myndigheterna sådan åtkomst. Detta skulle också stämma överens med hur domstolsdatalagens och domstolsdataförordningens befintliga bestämmelser om direktåtkomst är utformade.⁸ Innan direktåtkomst inrättas bör domstolen överväga om detta i något avseende är olämpligt och göra en risk- och sårbarhetsanalys. Som vi tidigare nämnt är det dock den mottagande myndighetens ansvar att se till att de personuppgifter som myndigheten tar emot behandlas i enlighet med dataskyddsförordningen, bl.a. vad gäller säkerhetsåtgärder och behörighetsbegränsningar. Vår uppfattning är att domstolarna, om inte något tydligt talar för motsatsen, bör kunna förutsätta att de mottagande myndigheterna behandlar personuppgifterna i enlighet med gällande bestämmelser.

Frågan är då om samtliga de aktuella myndigheterna bör ges möjlighet till direktåtkomst. Flertalet av dem har ställt sig mycket positiva till en sådan åtkomst och menar att det vore till stor nytta för verksamheten. Dock har Naturvårdsverket, som vi uppfattar det, inte sett det omedelbara behovet av sådan åtkomst.

Naturvårdsverket har emellertid enligt egen uppgift behov av information om domar och slutliga beslut från mark- och miljödomstolarna och Mark- och miljööverdomstolen. Eftersom denna information finns fullt ut registerad i miljöboken anser vi att även Naturvårdsverket bör ingå i den krets av myndigheter som kan få direktåtkomst till miljöboken. Det vore enligt vår mening olyckligt att helt utesluta en tillsynsmyndighet – som har behov av den information som miljöboken kan ge – från en möjlighet till sådan åtkomst som i framtiden kan vara intressant. Med hänsyn till de

⁸ Se 17 § domstolsdatalagen och 7–12 §§ domstolsdataförordningen.

mycket begränsade integritetsriskerna ser vi inte något hinder mot att även Naturvårdsverket får möjlighet till direktåtkomst.

För det fall de aktuella myndigheternas direktåtkomst till miljöboken regleras som en möjlighet för mark- och miljödomstolarna att ge sådan åtkomst, behöver den myndighet som för närvarande anser sig inte ha behov av den inte heller begära sådan åtkomst. Detta stämmer överens med den allmänna princip om korrekthet vid personuppgiftsbehandling som framgår av artikel 5.1 a i dataskyddsförordningen; det vore inte skäligen gentemot de registerade om en myndighet beredde sig åtkomst till personuppgifter som inte krävs för verksamheten.

Sammanfattningsvis anser vi således att mark- och miljödomstolarna ska få medge Havs- och vattenmyndigheten, Kammarkollegiet, länsstyrelserna, MSB, Naturvårdsverket och kommunernas miljönämnder direktåtkomst till mark- och miljöboken.

21.7 Reglering av myndigheternas direktåtkomst

Nästa fråga att ta ställning till är vilka lagstiftningsåtgärder som krävs för att möjliggöra direktåtkomst till miljöboken för de aktuella myndigheterna.

21.7.1 Direktåtkomsten ryms inte inom de primära ändamålen

Mark- och miljödomstolarna för enligt vår mening miljöboken som ett led i handläggningen av mål och ärenden och således inom ramen för den primära ändamålsbestämmelsen i 6 § domstolsdatalagen. Bestämmelsen ska förvisso ges en vid innebörd (se avsnitt 9.1.6). Vi anser dock att begreppet *handläggning av mål och ärenden* inte ens i sin vidaste bemärkelse kan anses omfatta de aktuella myndigheternas direktåtkomst till miljöboken. Behovet som ligger bakom utlämnandet av miljöbokens personuppgifter genom direktåtkomst finns ju i myndigheternas verksamhet och inte hos mark- och miljödomstolarna. Att det är en fördel även för domstolarnas handläggning att de aktuella myndigheterna är välinformerade vad gäller de omständigheter som kan påverka prövningen ändrar inte den bedömningen. Vi anser således att

direktåtkomst till miljöboken för de aktuella myndigheterna inte ryms inom domstolsdatalagens primära ändamålsbestämmelse.

21.7.2 Direktåtkomst är för närvarande inte förenlig med det sekundära ändamålet

Frågan är då om ett utlämnande genom direktåtkomst till miljöbokens personuppgifter kan ske med stöd av domstolsdatalagens sekundära ändamålsbestämmelse. Denna bestämmelse finns i 7 § och innebär att personuppgifter som behandlats för att de behövs för handläggning av mål och ärenden också får behandlas om det behövs för att fullgöra ett uppgiftslämnande som sker i enlighet med lag eller förordning.

Som vi nämnt i föregående avsnitt anser vi att mark- och miljödomstolarnas förande av miljöboken utgör en del av handläggningen av mål och ärenden. En domstol har vidare en allmän uppgiftsskyldighet gentemot andra myndigheter. Detta framgår av 6 kap. 5 § TF. Enligt bestämmelsen ska en myndighet på begäran av en annan myndighet lämna ut uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång. Som vi uppfattar det innebär bestämmelsen dock endast en skyldighet att lämna ut information efter en direkt begäran från en annan myndighet. Direktåtkomst kan visserligen ses som att mottagarmyndigheten lämnar en ständig begäran om utlämnande till värmyndigheten. Vi anser dock att det sannolikt inte är förenligt med dataskyddsförordningen att lägga en så allmänt hållen bestämmelse till grund för direktåtkomst som innefattar personuppgifter.

21.7.3 En ny sekundär ändamålsbestämmelse?

Möjligheten finns att genom en ny sekundär ändamålsbestämmelse i domstolsdatalagen skapa en lagreglerad möjlighet för mark- och miljödomstolarna att lämna ut personuppgifter ur miljöboken till de aktuella myndigheterna. Av artikel 6.3 andra stycket i dataskyddsförordningen framgår att den nationella rätten kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen och att dessa bestämmelser kan

innehålla bland annat de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål. Av skäl 50 till dataskyddsförordningen framgår också att om behandlingen är nödvändig bl.a. för att fullgöra en uppgift av allmänt intresse som den personuppgiftsansvarige har fått i uppgift att utföra, kan medlemsstaternas nationella rätt fastställa och närmare ange för vilka uppgifter och syften ytterligare behandling bör betraktas som förenlig och laglig.

Domstolsdatalagens nuvarande sekundära ändamålsbestämmelser är dock vidare i sin utformning än vad en ny ändamålsbestämmelse som endast tar sikte på utlämnande av personuppgifter i miljöboken skulle vara. En sådan ändamålsbestämmelse skulle därmed inte följa lagens nuvarande systematik. Utlämnandet av uppgifter från miljöboken via direktåtkomst kommer vidare att utgöra en förhållandevis liten del av domstolarnas verksamhet. En ny sekundär ändamålsbestämmelse som endast reglerar utlämnande av miljöbokens uppgifter skulle därmed lyfta fram just den personuppgiftsbehandlingen på ett sätt som inte avspeglar dess betydelse för domstolarnas verksamhet. Vi rekommenderar därför inte denna lösning.

21.7.4 Rättsligt stöd för utlämnandet av miljöbokens personuppgifter

Förslag: Det ska framgå av förordningen (1998:1388) om vattenverksamhet m.m. samt förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd att en mark- och miljödomstol är skyldig att efter begäran lämna ut uppgifter i vattenboken respektive förteckningen över avgöranden som rör miljöbalken till Havs- och vattenmyndigheten, Kammarkollegiet, länsstyrelserna, Myndigheten för samhällsskydd och beredskap, Naturvårdsverket och de kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet.

Som vi tidigare har konstaterat skulle de aktuella myndigheternas åtkomst till miljöboken vara till stor nytta i myndigheternas arbete, vilket i sin tur skulle ha en positiv inverkan på skyddet för miljön.

Mot den bakgrunden anser vi att man kan betrakta mark- och miljödomstolarnas utlämnande av miljöbokens uppgifter till de aktuella myndigheterna som en uppgift av allmänt intresse. Det finns enligt detta resonemang en självständig rättslig grund i enlighet med artikel 6.1 e i dataskyddsförordningen för den personuppgiftsbehandling som ett utlämnande av miljöbokens personuppgifter skulle innebära.

Den rättsliga grunden för personuppgiftsbehandlingen måste dock, enligt artikel 6.3 första stycket i dataskyddsförordningen, vara fastställd i enlighet med unionsrätten eller den nationella rätten. Detta innebär att uppgiften av allmänt intresse, i detta fall utlämnandet av uppgifter i miljöboken, måste framgå av lag, förordning eller annan författning för att kunna utgöra den rättsliga grunden för personuppgiftsbehandling. Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) också föreslagit att det i den nya dataskyddslagen ska tas in en bestämmelse som tydliggör att begreppet uppgift av allmänt intresse avser en uppgift av allmänt intresse som utförs med stöd av lag eller annan författning.

Mark- och miljödomstolarnas allmänna uppgiftsskyldighet gentemot andra myndigheter enligt 6 kap. 5 § TF omfattar självklart även de uppgifter som finns i miljöboken. Vi anser dock att denna allmänna uppgiftsskyldighet är alltför vag för att utgöra den uppgift av allmänt intresse som kan utgöra den rättsliga grunden för utlämnandet av miljöbokens personuppgifter. I stället bör enligt vår mening mark- och miljödomstolarnas skyldighet att lämna ut de uppgifter, inkluderat personuppgifter, som miljöboken omfattar uttryckligen regleras i annan författning.

I förordningen (1998:1388) om vattenverksamhet m.m. regleras mark- och miljödomstolarnas förande av miljöboken vad gäller vattenverksamheter. Enligt vårt förslag – se avsnitt 21.3 – ska förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd kompletteras med en bestämmelse som innebär att mark- och miljödomstolarna i miljöboken ska föra en förteckning över avgöranden som rör miljöfarlig verksamhet enligt miljöbalken och som domstolen meddelar som första instans. Det vore enligt vår mening ändamålsenligt att i anslutning till dessa bestämmelser i de båda förordningarna reglera mark- och miljödomstolarnas

skyldighet att lämna ut de uppgifter som ingår i miljöboken till de aktuella myndigheterna.

Vi föreslår därför att förordningen om vattenverksamhet m.m. kompletteras med en bestämmelse som innebär att mark- och miljödomstolarna är skyldiga att efter begäran lämna ut uppgifter i vattenboken till Havs- och vattenmyndigheten, Kammarkollegiet, länsstyrelserna, MSB, Naturvårdsverket och de kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet. Förordningen om miljöfarlig verksamhet och hälsoskydd bör kompletteras med motsvarande bestämmelse för uppgifter i den del av miljöboken som rör miljöfarlig verksamhet.

På detta sätt skapas en egen rättslig grund i enlighet med dataskyddsförordningen för den personuppgiftsbehandling som utförs när domstolarna lämnar ut uppgifter ur miljöboken till de aktuella myndigheterna. Regleringen skapar också en författningsreglerad skyldighet för mark- och miljödomstolarna att lämna ut miljöbokens uppgifter till de aktuella myndigheterna, vilket innebär att ett utlämnande till myndigheterna kan ske i enlighet med domstolsdatalagens befintliga sekundära ändamålsbestämmelse.

21.7.5 Bestämmelserna om direktåtkomst bör kompletteras

Förslag: Havs- och vattenmyndigheten, Kammarkollegiet, länsstyrelserna, Myndigheten för samhällsskydd och beredskap, Naturvårdsverket och de kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet ska kunna medges direktåtkomst till mark- och miljödomstolarnas miljöbok. Sådan direktåtkomst får endast avse personuppgifter i miljöboken om

1. målnummer och domsnummer,
2. geografiska koordinater,
3. fastighetsbeteckningar,
4. namn på parter och anläggningar,
5. en sammanfattning av avgörandet, och
6. andra uppgifter med direkt anknytning till ett avgörande.

Om ett avgörande har överklagats ska direktåtkomst även få medges till motsvarande uppgifter som har registrerats om överinstansens avgörande.

Domstolsdatalagens och domstolsdataförordningens bestämmelser om direktåtkomst är heltäckande. Detta innebär att varje form av direktåtkomst måste regleras i dessa författningar för att vara tillåten. För att möjliggöra de aktuella myndigheternas direktåtkomst till miljöbokens personuppgifter måste domstolsdatalagens bestämmelse om direktåtkomst därför kompletteras så att det framgår att även dessa myndigheter kan medges direktåtkomst. Det bör vidare av domstolsdatalagen framgå att de aktuella myndigheternas direktåtkomst endast får avse personuppgifter som finns i miljöboken. Detta skapar ett ytterligare integritetsskydd eftersom det då krävs en ändring i domstolsdatalagen för att utöka myndigheternas direktåtkomst. För att främja läsbarheten föreslår vi också att nuvarande 17 § domstolsdatalagen med de föreslagna ändringarna delas upp i två paragrafer.

Domstolsverket har rätt att meddela närmare föreskrifter om miljöboken, vilket innefattar vilka personuppgifter som ska registreras. För att se till att direktåtkomst till miljöboken endast omfattar de personuppgifter som för närvarande finns registrerade där anser vi att det av domstolsdataförordningen bör framgå att de aktuella myndigheternas direktåtkomst endast får avse uppgifter om

1. målnummer och domsnummer,
2. geografiska koordinater,
3. fastighetsbeteckningar,
4. namn på parter och anläggningar,
5. en sammanfattning av avgörandet, och
6. andra uppgifter med direkt anknytning till ett avgörande.

Om ett avgörande har överklagats bör direktåtkomst även få medges till motsvarande uppgifter som har registrerats om överinstansens avgörande. De föreslagna ändringarna i domstolsdataförordningen görs enligt vår mening lättast genom en hänvisning till den bestämmelse i domstolsdataförordningen som på samma sätt reglerar Högsta domstolens, Mark- och miljööver-

domstolens och mark- och miljödomstolarnas direktåtkomst till miljöboken.

22 Övergångs- och ikraftträdandebestämmelser

22.1 Två olika ikraftträdandedatum

Förslag: Bestämmelsen om domstolsdatalagens förhållande till brottsdatalagen ska träda i kraft den 1 maj 2018. Detsamma gäller den nya paragraf som reglerar förhållandet till Europaparlamentets och rådets förordning (EU) nr 655/2014 (kvarstadsförordningen).

Den bestämmelse som reglerar förhållandet till lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen ska upphävas den 1 maj 2018.

Övriga ändringar i domstolsdatalagen, ändringarna i domstolsdataförordningen samt ändringarna i förordningen (1998:1388) om vattenverksamhet m.m. och förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd ska träda i kraft den 25 maj 2018.

Dataskyddsförordningen ska, enligt artikel 99.2 i förordningen, börja tillämpas den 25 maj 2018. Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit att dataskyddslagen ska träda i kraft vid den tidpunkten. Eftersom domstolsdatalagen kommer att utgöra en komplettering till dataskyddsförordningen och innehålla hänvisningar till dataskyddslagen bör även våra författningsförslag träda i kraft den 25 maj 2018.

Ikraftträdandebestämmelserna kompliceras dock något av att den tidpunkt då dataskyddsförordningen ska börja tillämpas och den tidpunkt då brottsdatalagen ska träda i kraft inte sammanfaller med varandra. Som en följd av bestämmelserna i 2016 års data-

skyddsdirektiv har Utredningen om 2016 års dataskyddsdirektiv i sitt betänkande (SOU 2017:29) föreslagit att brottsdatalagen ska träda i kraft den 1 maj 2018. Enligt vårt förslag ska domstolsdatalagen och domstolsdataförordningen inte längre gälla vid behandling av personuppgifter i sådan verksamhet i de allmänna domstolarna och de allmänna förvaltningsdomstolarna som omfattas av brottsdatalagens tillämpningsområde (se avsnitt 4.3). Detta får till följd att om hela vårt författningsförslag skulle träda i kraft först den 25 maj 2018 skulle den del av domstolarnas verksamhet som faller under brottsdatalagens tillämpningsområde dubbelregleras under perioden den 1–24 maj 2018. Med särskilda ikraftträdandebestämmelser för den del av vårt förslag som reglerar förhållandet till brottsdatalagen kan detta emellertid undvikas.

Vi föreslår därför att den nya lydelsen av 3 § domstolsdatalagen, som innebär att domstolsdatalagen inte ska omfatta den verksamhet som faller under brottsdatalagens tillämpningsområde, ska träda i kraft redan den 1 maj 2018.

I sin nuvarande lydelse reglerar 3 § domstolsdatalagen förhållandet till lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen (2013 års lag) samt Europaparlamentets och rådets förordning (EU) nr 655/2014 (kvarstadsförordningen). Vi har, i avsnitt 10.4, föreslagit att bestämmelsen som reglerar förhållandet till 2013 års lag ska upphävas. Enligt Utredningen om 2016 års dataskyddsdirektivs förslag ska 2013 års lag upphävas den 1 maj 2018.¹ Det är därmed ändamålsenligt att även domstolsdatalagens bestämmelse i denna del upphävs vid denna tidpunkt.

I avsnitt 10.5 har vi föreslagit att bestämmelsen om förhållandet till kvarstadsförordningen ska finnas kvar oförändrad i sak. Den ska enligt vårt förslag dock framöver finnas i den nya 5 a §. För att förhållandet mellan domstolsdatalagen och kvarstadsförordningen inte ska vara oreglerat under perioden den 1–24 maj 2018 bör även den av oss föreslagna 5 a § träda i kraft den 1 maj 2018.

I övriga delar bör våra förslag träda i kraft den 25 maj 2018. Det samma gäller ändringarna i förordningen (1998:1388) om vattenverksamhet m.m. och förordningen (1998:899) om

¹ Se Utredningen om 2016 års dataskyddsdirektivs delbetänkande (SOU 2017:29).

miljöfarlig verksamhet och hälsoskydd, eftersom dessa föreslag är en följd av den möjlighet till direktåtkomst till miljöboken som föreslås införas i domstolsdatalagen och domstolsdataförordningen. Med anledning av att domstolsdataförordningen innehåller kompletterande föreskrifter om sådan behandling av personuppgifter som omfattas av domstolsdatalagen skulle den särskilda ikraftträdandebestämmelsen för 3 § domstolsdatalagen få genomslag även för förordningen. Någon motsvarande delad ikraftträdandebestämmelse behövs enligt vår mening därmed inte för domstolsdataförordningen.

22.2 Befintliga ikraftträdande- och övergångsbestämmelser

Bedömning: Det krävs inte någon ny övergångsbestämmelse med anledning av att de bestämmelser som omfattas av punkten 2 i domstolsdataförordningens befintliga övergångsbestämmelser inte kommer att ha trätt i kraft den 25 maj 2018.

Domstolsdatalagen saknar för närvarande övergångsbestämmelser. Domstolsdataförordningen har däremot övergångsbestämmelser i fyra punkter. När dataskyddsförordningen börjar tillämpas den 25 maj 2018 kommer tidpunkten för dessa övergångsbestämmelser att ha passerats, med undantag för punkten 2. Övergångsbestämmelsen i denna punkt gäller bestämmelserna i 3 § andra meningen, 4 §, 5 § andra meningen och 13 § domstolsdataförordningen. Dessa bestämmelser reglerar begränsningar för sökning och direktåtkomst i fråga om slutligt avgjorda mål och ärenden. Enligt övergångsbestämmelsen ska bestämmelserna börja tillämpas första gången den 1 januari 2019.

Vårt förslag innebär vissa redaktionella ändringar i de aktuella bestämmelserna. De ändringar vi föreslagit innebär emellertid inte att det behövs en ny övergångsbestämmelse för de nyss nämnda bestämmelserna. Anledningen är att den nuvarande ikraftträdandebestämmelsen i punkt 2 domstolsdataförordningens ikraftträdande- och övergångsbestämmelser även kommer att omfatta de

föreslagna ändringarna i de aktuella paragraferna.² De aktuella bestämmelserna kommer således – även om lydelsen eller paragrafnumret har ändrats – alltså att börja tillämpas först den 1 januari 2019.

22.3 Pågående ärenden

Bedömning: Den föreslagna övergångsbestämmelsen till dataskyddslagen som reglerar att äldre föreskrifter fortfarande gäller för ärenden hos Datainspektionen som har inletts men inte avgjorts före ikraftträdandet, gäller även på domstolsdatalogens tillämpningsområde.

Datainspektionen har befogenhet att vidta åtgärder mot domstolarna i deras egenskap av personuppgiftsansvariga. Datainspektionen kan exempelvis förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än att lagra dem samt ansöka om utplåning av personuppgifter hos allmän förvaltningsdomstol. Datainspektionen får vidare besluta om säkerhetsåtgärder som den personuppgiftsansvarige ska vidta. De materiella bestämmelserna finns i 32 §, 43 och 44 §§, 45 § första stycket och 47 § PuL, till vilka domstolsdatalogen hänvisar genom 5 § första stycket 7 och 10.

Som framgår av avsnitt 22.1 har Dataskyddsutredningen föreslagit att dataskyddslagen ska träda i kraft den 25 maj 2018. Vid samma tidpunkt föreslår den utredningen att personuppgiftslagen ska upphävas. I Dataskyddsutredningens betänkande (SOU 2017:39) finns emellertid förslag på en övergångsbestämmelse som innebär att äldre föreskrifter fortfarande gäller för ärenden hos Datainspektionen som har inletts men inte avgjorts före ikraftträdandet. Som skäl för detta har utredningen anfört att exempelvis förelägganden om säkerhetsåtgärder eller radering inte kan baseras på dataskyddsförordningens bestämmelser innan dessa är tillämpliga. Med äldre föreskrifter menas enligt Dataskydds-

² Se Ds 2014:1 s. 100.

utredningen personuppgiftslagen, personuppgiftsförordningen och föreskrifter som meddelats med stöd av dessa.³

Datainspektionens ärenden gentemot en personuppgiftsansvarig domstol drivs enligt vår mening med stöd av personuppgiftslagens bestämmelser och handläggs enligt den lagens regelverk. En annan sak är att Datainspektionen i sin tillsyn inte bara bedömer om en personuppgiftsansvarig myndighet har behandlat personuppgifter i enlighet med personuppgiftslagen, utan även beaktar tillämplig registerförfattning som t.ex. domstolsdatalagen. Mot den bakgrunden bedömer vi att dataskyddslagens föreslagna övergångsbestämmelse är tillämplig även på de eventuella ärenden som Datainspektionen har inlett mot domstolar men som inte har avgjorts när våra författningsförslag träder i kraft. Någon särskild övergångsbestämmelse i domstolsdatalagen som täcker sådana ärenden behövs enligt vår mening därmed inte.

22.4 Beslut som har meddelats före ikraftträdandet

Förslag: Äldre föreskrifter ska fortfarande gälla för överklagande av beslut som har meddelats med stöd av de föreskrifterna.

Bestämmelser om överklagande av vissa beslut som fattats med stöd av personuppgiftslagen finns i 51–53 §§ PuL. Av 51 och 52 §§ framgår att Datainspektionens beslut respektive beslut av en personuppgiftsansvarig myndighet i vissa fall får överklagas till allmän förvaltningsdomstol. Enligt 53 § får även en förvaltningsrätts beslut efter Datainspektionens ansökan om utplåning av personuppgifter överklagas.

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit en övergångsbestämmelse till dataskyddslagen som innebär att äldre föreskrifter fortfarande gäller för överklagande av beslut som har meddelats med stöd av dessa föreskrifter. Det framgår inte uttryckligen av Dataskyddsutredningens betänkande om övergångsbestämmelsen är tänkt att gälla samtliga typer av beslut

³ Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 340 ff.).

som kan överklagas enligt personuppgiftslagen. Eftersom inget annat framgår anser vi dock att man får förutsätta att så är fallet.

Domstolsdatalagen innehåller inga hänvisningar till personuppgiftslagens överklagandebestämmelser. I stället finns samtliga överklagandebestämmelser samlade i 19–22 §§ domstolsdatalagen. Rätten att överklaga Datainspektionens beslut regleras i 19 § och rätten att överklaga beslut som en domstol fattat i sin egenskap av personuppgiftsansvarig finns i 20 och 21 §§. Rätten att överklaga beslut som fattats av en förvaltningsdomstol efter Datainspektionens ansökan om utplåning av personuppgifter regleras i 22 §.

Det faktum att domstolsdatalagen innehåller särskilda bestämmelser om överklagande av beslut innebär att dataskyddslagens övergångsbestämmelse inte blir tillämplig för de beslut som kan överklagas enligt domstolsdatalagen. Frågan är då om det till domstolsdatalagen ska finnas en övergångsbestämmelse liknande dataskyddslagens i denna del.

Av skäl 171 till dataskyddsförordningen framgår att behandling som redan pågår den dag då förordningen börjar tillämpas bör bringas i överensstämmelse med förordningen inom en period av två år från det att förordningen träder i kraft, dvs. senast den 24 maj 2018.⁴ Innebörden av detta är inte helt lättolkad; vid samordning med andra utredningar har frågan lyfts om skäl 171 utgör ett absolut hinder mot övergångsbestämmelser som innebär att äldre föreskrifter fortsatt ska gälla i vissa fall. Enligt vår mening innebär skäl 171 endast att de personuppgiftsansvariga måste ha anpassat sin personuppgiftsbehandling till dataskyddsförordningens regelverk vid den tid då förordningen börjar tillämpas. Vi anser att skälet inte kan ges någon betydelse utöver detta, vilket innebär att det enligt vår bedömning inte utgör något hinder för övergångsbestämmelser som träffar den behandling av personuppgifter som har skett före det att dataskyddsförordningen börjar tillämpas.

Huvudprincipen när det gäller förvaltningsrättsliga föreskrifter är att de föreskrifter som är i kraft vid tidpunkten för prövningen

⁴ Dataskyddsförordningen träder i kraft den tjugonde dagen efter det att den har offentliggjorts i Europeiska unionens officiella tidning, vilket skedde den 4 maj 2016. Förordningen börjar tillämpas den 25 maj 2018 (se artikel 99 i dataskyddsförordningen).

av ett mål eller ärende ska ligga till grund för prövningen. Principen är emellertid inte undantagslös; bl.a. måste EU-rättslig praxis och förbudet mot retroaktiv tillämpning i 2 kap. 10 § RF beaktas. Undantag kan vidare följa av övergångsbestämmelser eller av uttalanden i motiven till lagstiftningen. För civilrättslig lagstiftning är utgångspunkten en annan; som regel träffar sådan lagstiftning inte rättshandlingar som har utförts innan lagstiftningen träder i kraft.⁵

Vi anser att man inte rimligen kan begära att de personuppgiftsansvariga ska utföra sin personuppgiftsbehandling i enlighet med dataskyddsförordningens regelverk även innan den ska börja tillämpas. Enligt vår mening är det därmed även rimligt att handläggningen i domstol efter överklagande av beslut som fattats enligt personuppgiftslagens regelverk sker enligt detta regelverk. Det faktum att det för dataskyddslagen ska finnas en övergångsbestämmelse med denna innebörd talar enligt vår mening vidare för att det även i domstolsdatalagen bör införas en sådan bestämmelse. På detta sätt kan enhetlighet upprätthållas för samtliga överprövningar på området.

Det kan enligt vår mening inte heller uteslutas att det kan uppstå situationer där den registrerade skulle ha vunnit framgång med ett överklagande om det hade handlagts enligt äldre föreskrifter, men inte om det hade handlagts enligt bestämmelserna i dataskyddsförordningen och dess kompletterande regelverk. Utan en övergångsbestämmelse liknande den som föreslagits för dataskyddslagen skulle den registrerade i dessa fall göra en rättsförlust. Skulle situationen bli den motsatta – den registrerade skulle haft framgång med sitt överklagande om det handlagts enligt de nyare föreskrifterna men inte enligt de äldre – finns alltid möjligheten för den registrerade att på nytt framställa en begäran till den personuppgiftsansvarige och därmed få sin begäran bedömd utifrån det nya regelverket. Mot den bakgrunden föreslår vi att det till våra författningsförslag ska finnas en övergångsbestämmelse med innebörden att äldre föreskrifter fortfarande gäller för överklagande av beslut som har meddelats med stöd av de föreskrifterna. Övergångsbestämmelsen är avsedd att träffa beslut som meddelats av Datainspektionen och som kan överklagas enligt 19 § domstolsdatalagen samt de beslut domstolarna fattar i sin

⁵ Jfr RÅ 1996 ref. 57, med hänvisning till RÅ 1988 ref. 132.

egenskap av personuppgiftsansvariga myndigheter och som kan överklagas enligt 20 och 21 §§ domstolsdatalagen.

22.5 Skada som har orsakats före ikraftträdandet

Bedömning: Det behövs inte några övergångsbestämmelser gällande skadestånd för skada som har orsakats före ikraftträdandet.

Domstolsdatalagen hänvisar, genom 5 § första stycket 11, till 48 § PuL. Den sistnämnda bestämmelsen reglerar personuppgiftsansvarigas skadeståndsansvar om en behandling har utförts i strid med personuppgiftslagen. Hänvisningen innebär, enligt förarbetena till domstolsdatalagen (prop. 2014/15:148 s. 92 f), att skadeståndsansvaret även gäller vid personuppgiftsbehandling som skett i strid med domstolsdatalagens bestämmelser.

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39) föreslagit att det till dataskyddslagen ska finnas en övergångsbestämmelse som innebär att äldre föreskrifter om skadestånd fortfarande gäller för skada som har orsakats före ikraftträdandet.

Det faktum att domstolsdatalagen hänvisar till bestämmelsen om skadeståndsansvar i 48 § PuL innebär enligt vår mening att en övergångsbestämmelse till dataskyddslagen som träffar den bestämmelsen även omfattar den rätt till skadestånd som en registrerad kan ha enligt domstolsdatalagen. Redan av den anledningen anser vi att någon särskild övergångsbestämmelse för skadeståndsärenden inte behövs till våra författningsförslag.

Skulle en annan bedömning göras följer det också av allmänna principer att äldre bestämmelser gäller för ett anspråk om skadestånd som har uppkommit före det att nya bestämmelser träder i kraft.⁶ Oavsett vilken bedömning som görs anser vi därmed att det inte behövs någon övergångsbestämmelse gällande skadeståndsanspråk till våra författningsförslag.

⁶ Jfr förarbetena till lagen (1987:667) om ekonomiska föreningar (prop. 2015/16:4 s. 205).

22.6 Sanktioner mot överträdelse som har skett före ikraftträdandet

Bedömning: Det behövs inte några övergångsbestämmelser gällande sanktioner mot överträdelse som har skett före ikraftträdandet.

Dataskyddsförordningen och Dataskyddsutredningens förslag till dataskyddslag innebär att systemet för sanktioner gentemot de personuppgiftsansvariga förändras. Den straffrättsliga reglering som finns i 49 § PuL kommer inte att ha någon motsvarighet i det nya regelverket. Inte heller kommer den möjlighet som nu finns för Datainspektionen att förena sina förelägganden med vite (44 och 45 §§ PuL) att finnas kvar.⁷ I stället ska tillsynsmyndigheten, enligt artikel 83 i dataskyddsförordningen, under vissa förutsättningar besluta om administrativa sanktionsavgifter mot en personuppgiftsansvarig som har behandlat personuppgifter i strid med förordningens bestämmelser.

Vårt förslag innebär att dataskyddslagens bestämmelser om administrativa sanktionsavgifter mot myndigheter ska gälla även för domstolarna. Regleringen ska genomföras genom en hänvisning i domstolsdatalagen till de aktuella bestämmelserna i dataskyddslagen (se avsnitt 10.7). Personuppgiftslagens bestämmelser om vite och straff gäller för närvarande emellertid inte på domstolsdatalagens tillämpningsområde. Detta innebär att det inte behövs någon övergångsbestämmelse som klargör vilket av sanktionssystemen – det gamla eller det nya – som ska tillämpas för överträdelse som skett före ikraftträdandet.

I 2 kap. 10 § RF finns vidare ett förbud mot retroaktiv straff- och skattelagstiftning. Förbudet mot retroaktiv skattelag anses analogvis vara tillämpligt på straffliknande administrativa påföljder.⁸ Mot den bakgrunden finns det enligt vår mening inte heller anledning att införa någon övergångsbestämmelse som reglerar att administrativa sanktionsavgifter inte får beslutas för överträdelse som skett innan våra författningsförslag träder i kraft.

⁷ Se Dataskyddsutredningens betänkande (SOU 2017:39 s. 294 ff.).

⁸ Se prop. 1975/76:209 s. 125.

23 Konsekvenser av förslagen

23.1 Inledning

I vårt uppdrag ingår att belysa vilka konsekvenser de föreslagna ändringarna bedöms få. Om förslagen förväntas leda till kostnadsökningar för det allmänna, ska vi även föreslå hur dessa ska finansieras.

Dataskyddsförordningen kommer, när den börjar tillämpas, att innehålla de grundläggande bestämmelserna för domstolarnas personuppgiftsbehandling. Vår konsekvensbedömning omfattar inte de förändringar i regelverket som följer direkt av dataskyddsförordningen eller som är en följd av förordningens tvingande bestämmelser. En sådan analys möter enligt vår mening oöverstigliga hinder; exempelvis har vi inte möjlighet att bedöma vilka anpassningar som måste göras av befintliga datasystem för att domstolarnas personuppgiftsbehandling ska vara förenlig med dataskyddsförordningens bestämmelser om dataskydd.

Det ligger enligt vår mening inte heller inom vårt uppdrag att bedöma konsekvenserna av att EU:s dataskyddsreform innebär att domstolarna kommer att behöva förhålla sig till två regelverk för personuppgiftsbehandling; brottsdatalagen med tillhörande registerförfattning respektive dataskyddsförordningen med tillhörande registerförfattning samt – i tillämpliga delar – dataskyddslagen.

Vår analys kommer således endast att behandla konsekvenserna av de förslag som materiellt innebär en förändring gentemot nuvarande reglering och där det finns ett utrymme att nationellt bedöma vilken reglering som ska införas.

Med undantag för det som framgår i följande avsnitt bedömer vi vidare att våra förslag inte innebär några konsekvenser för andra än de personuppgiftsansvariga domstolarna. Förslagen får således inte

någon betydelse för kommuner eller företag. Inte heller innebär de att några samhällsekonomiska konsekvenser uppstår. Det rör sig vidare främst om ett administrativt regelverk för personuppgiftsbehandling, som inte har några konsekvenser för brottsligheten eller det brottsförebyggande arbetet, sysselsättningen, offentlig service, jämställdhet eller möjligheterna att nå de integrationspolitiska målen.

23.2 Tillsynsmyndighetens handläggning och beslut samt sanktionsavgifter

Bedömning: De eventuella kostnader som uppstår för domstolarna med anledning av våra förslag rymms inom befintliga anslag.

Vi har föreslagit att dataskyddslagens föreslagna bestämmelser om tillsynsmyndighetens handläggning och beslut ska gälla även på domstolsdatalagens tillämpningsområde. Vissa av dessa bestämmelser är nya jämfört med den nuvarande regleringen. Det gäller möjligheten för tillsynsmyndigheten att under vissa speciella omständigheter väcka talan i domstol (6 kap. 2 § första och andra stycket dataskyddslagen). Det gäller även rätten för den registrerade att i vissa fall begära besked från tillsynsmyndigheten angående ett tillsynsärende (6 kap. 5 § dataskyddslagen) och rätten till dröjsmålstalan mot tillsynsmyndighetens beslut i ett sådant ärende (8 kap. 3 § dataskyddslagen som motsvaras av vårt förslag till 19 a § domstolsdatalagen). Vårt förslag innebär också att dataskyddslagens bestämmelser om sanktionsavgifter mot myndigheter ska gälla även för domstolarnas rättskipande och rättsvårdande verksamhet (7 kap. 1, 3 och 4 §§ dataskyddslagen).

Dataskyddsutredningen har i sitt betänkande (SOU 2017:39 s. 348 f.) gjort en bedömning av vilka konsekvenser de ovan nämnda bestämmelserna i dataskyddslagen kommer att få för tillsynsmyndigheten och för de allmänna förvaltningsdomstolar som har att pröva de aktuella målen. Dataskyddsutredningen menar att de ärenden och mål som blir följden av denna reglering kommer att vara sparsamt förekommande. Det faktum att den generella regleringen kommer att gälla även inom domstolsdatalagens

tillämpningsområde bör enligt vår mening därmed medföra endast försumbara kostnader för tillsynsmyndigheten och de allmänna förvaltningsdomstolar som ska pröva målen. Dessa bör enligt vår mening rymmas inom den befintliga budgeten.

23.3 Dataskyddsombud

Bedömning: Genom förslaget skapas ett förstärkt integritetskydd för de registrerade, som delvis kan kompensera det faktum att tillsynsmyndigheten inte är behörig att utöva tillsyn över den personuppgiftsbehandling som sker i domstolarnas dömande verksamhet.

Förslaget medför inte några kostnader för domstolarna som inte ryms inom befintliga anslag.

Enligt vårt förslag ska domstolarna utse ett eller flera dataskyddsombud även för den dömande verksamheten, vilket inte är obligatoriskt enligt dataskyddsförordningen. Skyldigheten att utse dataskyddsombud även för denna verksamhet innebär enligt vår mening ett förstärkt skydd för de registrerades personliga integritet, bl.a. genom att det internt på domstolarna kommer att finnas en person som har kunskap om regelverket för personuppgiftsbehandling. Detta kan bidra till att uppväga det integritetskydd som går förlorat genom att tillsynsmyndigheten inte är behörig att utöva tillsyn över den personuppgiftsbehandling som utförs i domstolarnas dömande verksamhet.¹

Vårt förslag innebär ingen förändring jämfört med nuvarande reglering, eftersom domstolarnas även för närvarande är skyldiga att utse ett eller flera personuppgiftsombud för hela den rättskipande och rättsvårdande verksamheten. Beroende på hur respektive ombud utför sitt uppdrag i dag kan uppdraget som dataskyddsombud enligt dataskyddsförordningen dock komma att innebära vissa smärre förändringar av arbetsuppgifterna. De eventuella ekonomiska konsekvenser som uppstår till följd av detta måste enligt vår mening emellertid anses vara marginella.

¹ Se artikel 55.3 i dataskyddsförordningen.

Domstolarna kommer vidare, när dataskyddsförordningen börjar tillämpas, fortfarande att vara skyldiga att utse dataskyddsombud för den administrativa verksamheten och för den del av den rättskipande och rättsvårdande verksamheten som inte utgör dömande verksamhet. Behövliga utbildningsinsatser med anledning av det nya regelverket kommer enligt vår mening därmed väsentligen att vara desamma, oavsett om ombudens uppdrag även omfattar den dömande verksamheten. Mot den bakgrunden uppskattar vi att vårt förslag i denna del inte får några kostnadsmässiga konsekvenser som inte rymms inom domstolarnas ordinarie budgetramar.

23.4 Andra myndigheters direktåtkomst till miljöboken

Bedömning: De kostnader som kan bli följden av att andra myndigheter ska kunna medges direktåtkomst till miljöboken kompenseras till viss del genom de effektivitetsvinster förslaget medför. Kostnaderna för förslaget bör kunna rymmas inom de befintliga anslagen.

Myndigheternas förbättrade tillgång till miljöinformation kommer rimligen att leda till miljövinster och förbättrad miljöinformation för allmänheten.

Vi har föreslagit att Havs- och vattenmyndigheten, Kammarkollegiet, länsstyrelserna, Myndigheten för samhällsskydd och beredskap, Naturvårdsverket och de kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet ska kunna medges direktåtkomst till personuppgifterna i den miljöbok som förs av mark- och miljödomstolarna. I avsnitt 21.6.3 har vi gjort en avvägning mellan de aktuella myndigheternas behov av sådan åtkomst och skyddet för de registrerades integritet. För en analys av de konsekvenser vårt förslag har för den personliga integriteten hänvisar vi till det avsnittet.

Det kan inte uteslutas att kostnader uppstår för Domstolsverket eller mark- och miljödomstolarna i samband med att de aktuella myndigheternas direktåtkomst till miljöboken inrättas. Länsstyrelserna har emellertid redan direktåtkomst till miljöboken,

vilket torde innebära att de tekniska lösningar som krävs för myndigheternas åtkomst redan finns. Vi har vidare fått information om att den tekniska utvecklingen dessutom medför att en ny version av miljöboken måste tas fram inom en snar framtid. Den investering detta kommer att innebära för Domstolsverket uppstår oberoende av om de aktuella myndigheterna medges direktåtkomst eller inte. Det är enligt vår mening rimligt att anta att de eventuella kostnader som uppkommer till följd av att den nya applikationen även ska möjliggöra direktåtkomst för andra myndigheter är förhållandevis små.

Vi vill i detta sammanhang påtala de effektivitetsvinster som den aktuella direktåtkomsten skulle medföra för både de aktuella myndigheterna och domstolarna. Om myndigheterna får möjlighet att på egen hand göra de efterforskningar bland meddelade domar och beslut som behövs vid exempelvis handläggningen av ett ärende, kommer myndigheternas arbete att effektiviseras. Den administrativa bördan för mark- och miljödomstolarna kommer i sin tur att minska. En eventuell kostnad för att tekniskt möjliggöra direktåtkomsten skulle därmed vägas upp av dessa effektivitetsvinster. Sammantaget bedömer vi att de kostnader förslaget medför bör kunna finansieras inom ramen för ordinarie budget.

Samtliga myndigheter som föreslås få direktåtkomst till miljöboken har fått i uppgift att värna miljön. Om dessa myndigheter får en bättre överblick över meddelade tillstånd till vattenverksamhet och miljöfarlig verksamhet borde de enligt vår bedömning få bättre förutsättningar att sköta det uppdrag som tilldelats dem i denna del. Detta borde i förlängningen medföra positiva effekter för miljön. Det faktum att de aktuella myndigheterna får ökad tillgång till miljöinformation torde också innebära att allmänhetens tillgång till sådan information ökar, eftersom det bör vara naturligare att rikta förfrågningar till de myndigheter som har till uppgift att tillgängliggöra miljöinformation än till en domstol, som inte har samma typ av uppdrag.

24 Författningskommentar

Vi har i föregående kapitel utförligt redogjort för de överväganden som ligger bakom de förändringar av domstolsdatalagens bestämmelser som vi föreslår i denna promemoria. Av den anledningen är författningskommentarerna begränsade till att i huvudsak avse hänvisningar till de avsnitt i betänkandet där respektive bestämmelse behandlas.

24.1 Förslaget till lag om ändring av domstolsdatalagen (2015:728)

2 §

Om inte annat anges i 3 §, gäller denna lag vid behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och hyres- och arrendenämndernas rättskipande och rättsvårdande verksamhet. Lagen gäller också när personuppgifterna vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran.

Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Paragrafen är ändrad. Förslaget behandlas i avsnitt 7.2.8.

3 §

Denna lag gäller inte vid behandling av personuppgifter i de allmänna domstolarnas och de allmänna förvaltningsdomstolarnas verksamhet som omfattas av brottsdatalogens (2018:xx) tillämpningsområde.

Paragrafen är ändrad. Förslaget behandlas i avsnitt 4.3 och 10.4.

Förhållandet till annan lagstiftning

3 a §

Denna lag innehåller kompletterande bestämmelser till 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.

Paragrafen är ny. Förslaget behandlas i avsnitt 10.2.

4 §

Om inte något annat anges i 5 §, gäller denna lag i stället för lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (2018:xx).

Paragrafen är ändrad. Förslaget behandlas i avsnitt 10.3.

5 §

När personuppgifter behandlas enligt denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller följande bestämmelser i lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (2018:xx):

1.1 kap. 4 § första stycket om förhållandet till tryck- och yttrandefriheten,

2. 3 kap. 13 § om behandling av personnummer och samordningsnummer,

3. 4 kap. 1 § om användningsbegränsningar för arkiverade personuppgifter,

4. 5 kap. 1 § första stycket och 5 kap. 2 § om begränsning av vissa rättigheter och skyldigheter,

5. 6 kap. 1–5 §§ om tillsynsmyndighetens handläggning och beslut,

6. 7 kap. 1, 3 och 4 §§ om administrativa sanktionsavgifter, och

7. 8 kap. 1 § om skadestånd.

Paragrafen är ändrad. Förslaget behandlas i avsnitt 10.3 vad gäller paragrafens ingress. I övrigt behandlas förslaget i avsnitt 10.6.11 (punkten 1), avsnitt 10.6.4 (punkten 2), avsnitt 19.4.5 (punkten 3), avsnitt 15.5.4 (punkten 4), avsnitt 10.6.9 (punkten 5), avsnitt 10.7 (punkten 6) och avsnitt 15.7.4 (punkten 7).

5 a §

De avvikande bestämmelser som finns i Europaparlamentets och rådets förordning (EU) nr 655/2014 av den 15 maj 2014 om inrättande av ett europeiskt förfarande för kvarstad på bankmedel för att underlätta gränsöverskridande skuldindrivning i mål och ärenden av privaträttslig natur, ska tillämpas i stället för bestämmelserna i denna lag.

Paragrafen är ny, men utgör endast en redaktionell ändring och motsvaras i sak av 3 § andra meningen i den nuvarande lydelsen. Förslaget behandlas i avsnitt 10.5.

7 §

Personuppgifter som behandlas eller har behandlats enligt 6 § får även behandlas om det behövs

1. för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning, eller

2. för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med

artikel 89.1 i Europaparlamentets och rådets förordning (EU) 2016/679.

Personuppgifter får även behandlas för de ändamål som framgår av första stycket när de behandlas eller har behandlats med stöd av brottsdatalagen (2018:xx) eller [namnet på den registerförfattning som kompletterar brottsdatalagen för domstolarnas verksamhet] (2018:xx).

Paragrafen är ändrad. Förslaget behandlas i avsnitt 19.4.3 (vad gäller första stycket andra punkten) samt i avsnitt 9.2 och 19.4.4 (vad gäller andra stycket).

Dataskyddsbud

10 §

Den personuppgiftsansvarige ska utse ett eller flera dataskyddsbud.

Paragrafen är ändrad. Förslaget behandlas i avsnitt 13.5.3.

Begränsningar av vissa rättigheter och skyldigheter

11 §

Bestämmelserna om den registrerades rätt att få information om en personuppgiftsincident enligt artikel 34 i Europaparlamentets och rådets förordning (EU) 2016/679, gäller inte om den personuppgiftsansvarige, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämna ut uppgifter till den registrerade.

Paragrafen är ändrad. Förslaget behandlas i avsnitt 13.5.6 och 15.8.2.

13 §

Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personen genom sådana särskilda kategorier av uppgifter som anges i artikel 9.1 i Europaparlamentets och rådets förordning (EU) 2016/679 (känsliga personuppgifter).

Paragrafen är ändrad. Förslaget behandlas i avsnitt 16.5.3.

14 §

Vid sökning i personuppgifter är det förbjudet att använda sökbegrepp som avslöjar känsliga personuppgifter enligt 13 §, uppgifter om nationell anknytning eller uppgifter om brott eller misstanke om brott.

Användning av särskilda beteckningar för identifiering av en viss mål- eller ärendetyp som sökbegrepp omfattas inte av förbudet i första stycket.

Paragrafen är ändrad. Förslaget behandlas i avsnitt 16.5.4.

17 §

Direktåtkomst får endast medges

- 1. en allmän domstol,*
- 2. en allmän förvaltningsdomstol,*
- 3. en hyres- och arrendenämnd,*
- 4. en part eller partens ombud, biträde eller försvarare, eller*
- 5. Havs- och vattenmyndigheten, Kammarkollegiet, länsstyrelserna,*

Myndigheten för samhällsskydd och beredskap, Naturvårdsverket och de kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet.

Paragrafen är ändrad. Övervägandena finns i avsnitt 21.6.3 och 21.7.

17 a §

Direktåtkomst enligt 17 § 4 får endast avse personuppgifter i partens mål eller ärende.

Direktåtkomst enligt 17 § 5 får endast avse personuppgifter i den förteckning som förs över en mark- och miljödomstols avgöranden i frågor som rör miljöbalken eller lagen (1998:812) med särskilda bestämmelser om vattenverksamhet (miljöboken).

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar av direktåtkomst enligt 17 § och om behörighet och säkerhet vid sådan åtkomst.

Paragrafen är ny men första och tredje stycket utgörs av bestämmelser som för närvarande finns i 17 §. Vad gäller andra stycket finns våra överväganden i avsnitt 21.7.5.

19 §

Tillsynsmyndighetens beslut enligt Europaparlamentets och rådets förordning (EU) 2016/679 och enligt 7 kap. 1 § lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen är ändrad. Förslaget behandlas i avsnitt 18.4.1.

19 a §

Tillsynsmyndighetens beslut att avslå en begäran om besked enligt 6 kap. 5 § lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning får 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 får inte överklagas.

Paragrafen är ny. Förslaget behandlas i avsnitt 18.4.2.

20 §

En hovrätts, tingsrätts eller förvaltningsrätts beslut om registrerades rättigheter enligt artiklarna 12.5, 15–19 och 21 i Europaparlamentets och rådets förordning (EU) 2016/679, får överklagas till kammarrätt. En kammarrätts beslut i sådana frågor får överklagas till Högsta förvaltningsdomstolen.

Högsta domstolens och Högsta förvaltningsdomstolens beslut i frågor som avses i första stycket får inte överklagas.

Paragrafen är ändrad. Förslaget behandlas i avsnitt 18.4.4.

22 §

Andra beslut än sådana som avses i 19–21 §§ får inte överklagas.

Paragrafen är ändrad. Förslaget behandlas i avsnitt 10.1 och 18.4.4.

24.2 Förslaget till förordning om ändring i domstolsdataförordningen (2015:729)

3 §

Användningen i allmän domstol enligt 15 § första stycket 1 domstolsdatalagen (2015:728) av sökbegrepp som avslöjar brott eller misstanke om brott, får inte avse sökning i personuppgifter i tvistemål.

I mål eller ärenden som har avgjorts slutligt får användningen av sådana sökbegrepp inte heller avse sökning i personuppgifter fem år efter utgången av det kalenderår då avgörandet fick laga kraft.

Paragrafens andra stycke innehåller redaktionella ändringar som inte är avsedda att utgöra någon förändring i sak. Förslaget behandlas i avsnitt 16.5.4.

4 §

Vid sökning i personuppgifter i brottmål som har avgjorts slutligt genom en dom eller ett beslut får personnamn, personnummer, samordningsnummer och andra uppgifter som direkt kan hänföras till en fysisk person som är i livet inte användas som sökbegrepp fem år efter utgången av det kalenderår då avgörandet fick laga kraft.

Paragrafen innehåller endast redaktionella ändringar som inte är avsedda att utgöra någon förändring i sak. Förslaget behandlas i avsnitt 16.5.4.

5 §

Användningen i allmän förvaltningsdomstol enligt 15 § första stycket 2 domstolsdatalagen (2015:728) av sökbegrepp som avslöjar hälsa, brott eller misstanke om brott får inte avse sökning i personuppgifter i mål som handläggs av Migrationsöverdomstolen eller av en migrationsdomstol.

I mål eller ärenden som har avgjorts slutligt får användningen av sådana sökbegrepp inte heller avse sökning i personuppgifter tjugo år efter utgången av det kalenderår då avgörandet fick laga kraft.

Paragrafens andra stycke innehåller redaktionella ändringar som inte är avsedda att utgöra någon förändring i sak. Förslaget behandlas i avsnitt 16.5.4.

11 b §

Direktåtkomst enligt 11 a § får även medges de myndigheter som anges i 17 § 5 domstolsdatalagen.

Paragrafen är ny. Förslaget behandlas i avsnitt 21.6.3 och 21.7.

14 §

Domstolsverket får meddela närmare föreskrifter om tillgången till personuppgifter. För tilldelning av behörighet för tillgång till personuppgifter ska det särskilt beaktas att det utöver behovet av uppgifterna ställs krav på utbildning och erfarenhet.

Domstolsverket får även meddela

1. föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter på medium för automatiserad behandling,

2. ytterligare föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter genom direktåtkomst och om behörighet och säkerhet vid sådant utlämnande,

3. ytterligare föreskrifter om begränsningar för behandling av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts slutligt genom en dom eller ett beslut som har fått laga kraft, och

4. de ytterligare föreskrifter som behövs för verkställighet av domstolsdatalagen (2015:728) och denna förordning.

Paragrafen är ändrad på så sätt att den tidigare punkten 1 i andra stycket har utgått. Förslaget behandlas i avsnitt 13.5.6.

24.3 Förslaget till förordning om ändring i förordningen (1998:1388) om vattenverksamhet m.m.

8 §

En mark- och miljödomstol ska föra en miljöbok. I denna ska domstolens förteckning över vattenverksamheter inom domsområdet (vattenbok) ingå.

Domstolsverket får meddela föreskrifter om vattenboken.

Mark- och miljödomstolarna är skyldiga att efter begäran lämna ut uppgifter i vattenboken till Havs- och vattenmyndigheten, Kammarkollegiet, länsstyrelserna, Myndigheten för samhällsskydd och beredskap, Naturvårdsverket och de kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet.

Paragrafen är ändrad. Förslaget behandlas i avsnitt 21.3 vad gäller första och andra stycket och i avsnitt 21.7 vad gäller tredje stycket.

24.4 Förslaget till förordning om ändring i förordningen (1998:899) om miljöfarlig verksamhet och hälsoskydd

Miljöbok

48 a §

En mark- och miljödomstol ska i den miljöbok som avses i 8 § förordningen (1998:1388) om vattenverksamhet m.m. föra en förteckning över avgöranden som rör miljöfarlig verksamhet enligt miljöbalken och som domstolen meddelar som första instans.

Domstolsverket får meddela föreskrifter om förteckningen.

Mark- och miljödomstolarna är skyldiga att efter begäran lämna ut uppgifter i förteckningen till Havs- och vattenmyndigheten, Kammarkollegiet, länsstyrelserna, Myndigheten för samhällsskydd och beredskap, Naturvårdsverket och de kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet.

Paragrafen är ny. Förslaget behandlas i avsnitt 21.3 vad gäller första och andra stycket och i avsnitt 21.7 vad gäller tredje stycket.

Uppdraget

Anpassning av domstolsdatalagen till EU:s nya dataskyddsförordning

Uppdraget

En utredare ges i uppdrag att lämna förslag på de författningsändringar som behövs i domstolsdatalagen (2015:728) och domstolsdataförordningen (2015:729) med anledning av EU:s dataskyddsförordning. Utredaren ska även ta ställning till om det finns behov av direktåtkomst för t.ex. Kammarkollegiet, länsstyrelserna, Naturvårdsverket och Havs- och vattenmyndigheten till den s.k. miljöbok som förs vid respektive mark- och miljödomstol och lämna de författningsförslag som i så fall behövs. Uppdraget ska redovisas senast den 8 maj 2017.

Bakgrund

Den 27 april 2016 antogs Europaparlamentets och rådets förordning (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). Samtidigt antogs Europaparlamentets och rådets direktiv (EU) 2016/680 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. Förordningen ska börja tillämpas

den 25 maj 2018 och direktivet ska ha genomförts i nationell rätt senast den 6 maj 2018.

Sedan den 1 januari 2016 regleras all automatiserad behandling av personuppgifter i den rättskipande och rättsvårdande verksamheten vid de allmänna domstolarna, de allmänna förvaltningsdomstolarna och hyres- och arrendenämnderna i domstolsdatalagen. Lagen innehåller hänvisningar till personuppgiftslagens (1998:204) bestämmelser om bl.a. grundläggande krav på behandling av personuppgifter, överföring av personuppgifter till tredjeland och skadestånd. Kompletterande bestämmelser till lagen finns i domstolsdataförordningen.

Regeringen har den 25 februari 2016 tillsatt en utredning (Dataskyddsutredningen) med uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som dataskyddsförordningen ger anledning till (dir. 2016:15). Uppdraget ska redovisas senast den 12 maj 2017. Regeringen har den 17 mars 2016 även tillsatt en utredning med uppdrag att föreslå hur direktivet ska genomföras i svensk rätt (dir. 2016:21). Uppdraget ska slutredovisas senast den 30 september 2017.

Varje mark- och miljödomstol ska föra en s.k. miljöbok som bl.a. innehåller en förteckning av domstolsavgöranden på miljöområdet. Uppgifterna i respektive miljöbok har stor betydelse för bl.a. Kammarkollegiet, länsstyrelserna, Naturvårdsverket och Havs- och vattenmyndigheten.

Närmare om uppdraget

I uppdraget till Dataskyddsutredningen ingår inte att se över eller lämna förslag till förändringar av sektorsspecifik reglering om behandling av personuppgifter i olika myndigheters verksamhet. Det finns därför behov av en närmare analys av vilka bestämmelser som behövs för att komplettera dataskyddsförordningen i regleringen av domstolarnas och nämndernas rättskipande och rättsvårdande verksamhet.

När det gäller genomförandet av dataskyddsdirektivet ingår det i den utredningens uppdrag att lämna förslag till författningsändringar som krävs för att anpassa exempelvis domstolsdatalagen och domstolsdataförordningen till direktivet. Det ingår därför inte

i utredarens uppdrag att se över domstolsdatalagen och domstolsdataförordningen med anledning av direktivet.

Utredaren ska även analysera och överväga om det finns behov av direktåtkomst för exempelvis Kammarkollegiet, länsstyrelserna, Naturvårdsverket och Havs- och vattenmyndigheten till mark- och miljödomstolarnas respektive miljöbok.

Utredaren ska lämna fullständiga författningsförslag utifrån de överväganden som görs.

Utredaren ska belysa vilka konsekvenser de föreslagna ändringarna bedöms få. Om förslagen förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras.

Utredaren ska följa och i lämplig omfattning samråda med andra utredningar som fått i uppdrag att anpassa svensk rätt till EU:s nya dataskyddsregelverk. Utredaren ska också samråda med Domstolsverket, Kammarkollegiet, Naturvårdsverket och Havs- och vattenmyndigheten och vid behov inhämta synpunkter från övriga myndigheter som berörs.

Uppdraget ska redovisas senast den 8 maj 2017.

(Justitiedepartementet)

Konsoliderade versioner av domstolsdatalagen och domstolsdataförordningen enligt våra förslag

I syfte att underlätta för läsaren åskådliggör vi i denna bilaga hur domstolsdatalagen och domstolsdataförordningen kommer att se ut i sin helhet om samtliga förslag i denna promemoria leder till lagstiftning. Vi har emellertid exkluderat både befintliga och föreslagna ikraftträdande- och övergångsbestämmelser.

Domstolsdatalag (2015:728)

Lagens syfte

1 §

Syftet med denna lag är att ge de allmänna domstolarna, de allmänna förvaltningsdomstolarna och hyres- och arrendenämnderna möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin rättskipande och rättsvårdande verksamhet och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

Lagens tillämpningsområde

2 §

Om inte annat anges i 3 §, gäller denna lag vid behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och hyres- och arrendenämndernas

rättskipande och rättsvårdande verksamhet. Lagen gäller också när personuppgifterna vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran.

Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

3 §

Denna lag gäller inte vid behandling av personuppgifter i de allmänna domstolarnas och de allmänna förvaltningsdomstolarnas verksamhet som omfattas av brottsdatalagens (2018:xx) tillämpningsområde.

Förhållandet till annan lagstiftning

3 a §

Denna lag innehåller kompletterande bestämmelser till 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.

4 §

Om inte något annat anges i 5 §, gäller denna lag i stället för lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (2018:xx).

5 §

När personuppgifter behandlas enligt denna lag, eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller följande bestämmelser i lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (2018:xx):

1. 1 kap. 4 § första stycket om förhållandet till tryck- och yttrandefriheten,

2. 3 kap. 13 § om behandling av personnummer och samordningsnummer,

3. 4 kap. 1 § om användningsbegränsningar för arkiverade personuppgifter,

4. 5 kap. 1 § första stycket och 5 kap. 2 § om begränsning av vissa rättigheter och skyldigheter,

5. 6 kap. 1–5 §§ om tillsynsmyndighetens handläggning och beslut,

6. 7 kap. 1, 3 och 4 §§ om administrativa sanktionsavgifter, och

7. 8 kap. 1 § om skadestånd.

5 a §

De avvikande bestämmelser som finns i Europaparlamentets och rådets förordning (EU) nr 655/2014 av den 15 maj 2014 om inrättande av ett europeiskt förfarande för kvarstad på bankmedel för att underlätta gränsöverskridande skuldindrivning i mål och ärenden av privaträttslig natur, ska tillämpas i stället för bestämmelserna i denna lag.

Ändamål

6 §

Personuppgifter får behandlas om det behövs för handläggning av mål och ärenden.

7 §

Personuppgifter som behandlas eller har behandlats enligt 6 § får även behandlas om det behövs

1. för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning, eller

2. för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i Europaparlamentets och rådets förordning (EU) 2016/679.

Personuppgifter får även behandlas för de ändamål som framgår av första stycket när de behandlas eller har behandlats med stöd av brottsdatalagen (2018:xx) eller [namnet på den registerförfattning som kompletterar brottsdatalagen för domstolarnas verksamhet] (2018:xx).

Tillgången till personuppgifter

8 §

Tillgången till personuppgifter ska begränsas till det som varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om tillgången till personuppgifter.

Personuppgiftsansvar

9 §

En allmän domstol, en allmän förvaltningsdomstol eller en hyres- och arrendenämnd är personuppgiftsansvarig för den behandling av personuppgifter som den domstolen eller nämnden utför.

Dataskyddsombud

10 §

Den personuppgiftsansvarige ska utse ett eller flera dataskyddsombud.

Begränsningar av vissa rättigheter och skyldigheter

11 §

Bestämmelserna om den registrerades rätt att få information om en personuppgiftsincident enligt artikel 34 i Europaparlamentets och rådets förordning (EU) 2016/679, gäller inte om den personuppgiftsansvarige, enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning, inte får lämna ut uppgifter till den registrerade.

12 §

Upphävd genom SFS 2018:xx

Behandling av känsliga personuppgifter

13 §

Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personen genom sådana särskilda kategorier av uppgifter som anges i artikel 9.1 i Europaparlamentets och rådets förordning (EU) 2016/679 (känsliga personuppgifter).

Sökbegränsningar

14 §

Vid sökning i personuppgifter är det förbjudet att använda sökbegrepp som avslöjar känsliga personuppgifter enligt 13 §, uppgifter om nationell anknytning eller uppgifter om brott eller misstanke om brott.

Användning av särskilda beteckningar för identifiering av en viss mål- eller ärendetyp som sökbegrepp omfattas inte av förbudet i första stycket.

15 §

Förbudet i 14 § första stycket gäller inte användning

1. i allmän domstol av sökbegrepp som avslöjar brott eller misstanke om brott, och

2. i allmän förvaltningsdomstol av sökbegrepp som avslöjar hälsa, brott eller misstanke om brott.

Förbudet i 14 § första stycket gäller inte heller vid sökning i en viss handling eller i ett visst mål eller ärende.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om begränsningar av möjligheten att använda de sökbegrepp som anges i första stycket.

Elektroniskt utlämnande av personuppgifter

16 §

Personuppgifter får lämnas ut på medium för automatiserad behandling om det inte är olämpligt.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare

föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter på medium för automatiserad behandling.

17 §

Direktåtkomst får endast medges

1. en allmän domstol,
2. en allmän förvaltningsdomstol,
3. en hyres- och arrendenämnd,
4. en part eller partens ombud, biträde eller försvarare, eller
5. Havs- och vattenmyndigheten, Kammarkollegiet, länsstyrelserna, Myndigheten för samhällsskydd och beredskap, Naturvårdsverket och de kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet.

17 a §

Direktåtkomst enligt 17 § 4 får endast avse personuppgifter i partens mål eller ärende.

Direktåtkomst enligt 17 § 5 får endast avse personuppgifter i den förteckning som förs över en mark- och miljödomstols avgöranden i frågor som rör miljöbalken eller lagen (1998:812) med särskilda bestämmelser om vattenverksamhet (miljöboken).

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar av direktåtkomst enligt 17 § och om behörighet och säkerhet vid sådan åtkomst.

Personuppgifter i avgjorda mål och ärenden

18 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar för behandling av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts genom en dom eller ett beslut som har fått laga kraft.

Överklagande

19 §

Tillsynsmyndighetens beslut enligt Europaparlamentets och rådets förordning (EU) 2016/679 och enligt 7 kap. 1 § lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

19 a §

Tillsynsmyndighetens beslut att avslå en begäran om besked enligt 6 kap. 5 § lagen (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning får 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 får inte överklagas.

20 §

En hovrätts, tingsrätts eller förvaltningsrätts beslut om registrerades rättigheter enligt artiklarna 12.5, 15–19 och 21 i Europaparlamentets och rådets förordning (EU) 2016/679, får överklagas till kammarrätt. En kammarrätts beslut i sådana frågor får överklagas till Högsta förvaltningsdomstolen.

Högsta domstolens och Högsta förvaltningsdomstolens beslut i frågor som avses i första stycket får inte överklagas.

21 §

En hyres- och arrendenämnds beslut i frågor som avses i 20 § första stycket får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

22 §

Andra beslut än sådana som avses i 19–21 §§ får inte överklagas.

Domstolsdataförordningen (2015:729)

Allmän bestämmelse

1 §

I denna förordning finns kompletterande föreskrifter om sådan behandling av personuppgifter som omfattas av domstolsdatalagen (2015:728).

De uttryck som används i denna förordning har samma innebörd och tillämpningsområde som i lagen. Med domstol eller domstolsinstans avses i denna förordning en allmän domstol, en allmän förvaltningsdomstol eller en hyres- och arrendenämnd.

2 §

Den personuppgiftsansvarige ansvarar för att det inom myndigheten finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter för tillgång till personuppgifter.

Sökbegränsningar

Sökning i de allmänna domstolarna

3 §

Användningen i allmän domstol enligt 15 § första stycket 1 domstolsdatalagen (2015:728) av sökbegrepp som avslöjar brott eller misstanke om brott, får inte avse sökning i personuppgifter i tvistemål.

I mål eller ärenden som har avgjorts slutligt får användningen av sådana sökbegrepp inte heller avse sökning i personuppgifter fem år efter utgången av det kalenderår då avgörandet fick laga kraft.

4 §

Vid sökning i personuppgifter i brottmål som har avgjorts slutligt genom en dom eller ett beslut får personnamn, personnummer, samordningsnummer och andra uppgifter som direkt kan hänföras till en fysisk person som är i livet inte användas som sökbegrepp fem år efter utgången av det kalenderår då avgörandet fick laga kraft.

Sökning i de allmänna förvaltningsdomstolarna

5 §

Användningen i allmän förvaltningsdomstol enligt 15 § första stycket 2 domstolsdatalagen (2015:728) av sökbegrepp som avslöjar hälsa, brott eller misstanke om brott får inte avse sökning i personuppgifter i mål som handläggs av Migrationsöverdomstolen eller av en migrationsdomstol.

I mål eller ärenden som har avgjorts slutligt får användningen av sådana sökbegrepp inte heller avse sökning i personuppgifter tjugo år efter utgången av det kalenderår då avgörandet fick laga kraft.

Undantag från sökförbuden

6 §

Förbuden i 3–5 §§ gäller inte vid sökning i en viss handling eller i ett visst mål eller ärende.

Direktåtkomst

När är direktåtkomst tillåten

7 §

Direktåtkomst enligt 17 § domstolsdatalagen (2015:728) får medges endast i de fall som anges i 8–12 §§ och med de ytterligare begränsningar som enligt 13 § gäller för direktåtkomst till personuppgifter i mål och ärenden som har avgjorts slutligt.

Direktåtkomst vid överklagande

8 §

När ett mål eller ärende överklagas får den lägre domstolsinstans som har prövat målet eller ärendet medge högre domstolsinstanser direktåtkomst till personuppgifterna i målet eller ärendet och till personuppgifterna i andra mål och ärenden som har samband med det överklagade målet eller ärendet.

9 §

När ett mål eller ärende överklagas får en högre domstolsinstans medge de lägre domstolsinstanser som har prövat målet eller ärendet direktåtkomst till personuppgifterna i målet eller ärendet och till personuppgifterna i andra mål och ärenden som har samband med det överklagade målet eller ärendet.

10 §

Vid tillämpningen av 8 och 9 §§ ska en ansökan om resning eller om återställande av försutten tid eller en klagan över domvilla jämnställas med ett överklagande.

Direktåtkomst till rättspraxis

11 §

Högsta domstolen och hovrätterna får medge en allmän domstol eller en hyres- och arrendenämnd direktåtkomst till domar och beslut. Högsta förvaltningsdomstolen och kammarrätterna får medge en allmän förvaltningsdomstol direktåtkomst till domar och beslut. Direktåtkomsten får även avse

1. uppgifter om parterna och deras ombud, biträden eller försvarare,
2. uppgifter om expediering, delgivning, överklagande och laga kraft,
3. uppgift om saken,
4. ärendemening,
5. uppgift om samband med andra mål,
6. en sammanfattning av domen eller beslutet,
7. uppgifter om domare, handläggare och andra tjänstemän vid domstolen, och
8. andra uppgifter med direkt anknytning till en dom eller ett beslut.

Direktåtkomst till miljöboken

11 a §

En mark- och miljödomstol får medge Högsta domstolen, Mark- och miljööverdomstolen eller en annan mark- och miljödomstol direktåtkomst till den förteckning som förs över

domstolens avgöranden inom domsområdet i frågor som rör miljöbalken eller lagen (1998:812) med särskilda bestämmelser om vattenverksamhet (miljöboken). Direktåtkomsten får avse

1. målnummer och domsnummer,
2. geografiska koordinater,
3. fastighetsbeteckningar,
4. namn på parter och anläggningar,
5. en sammanfattning av avgörandet, och
6. andra uppgifter med direkt anknytning till ett avgörande.

Om ett avgörande har överklagats får direktåtkomst medges även till uppgifter som har registrerats om överinstansens avgörande och som motsvarar de uppgifter som anges i första stycket.

11 b §

Direktåtkomst enligt 11 a § får även medges de myndigheter som anges i 17 § 5 domstolsdatalagen.

Direktåtkomst i samband med beredskapsverksamhet

12 §

Domstolar som tillsammans deltar i beredskap får medge varandra direktåtkomst till personuppgifter som behövs för handläggningen av de mål och ärenden som omfattas av beredskapsverksamheten.

Ytterligare begränsning av direktåtkomst till slutligt avgjorda mål och ärenden

13 §

När ett mål eller ärende har avgjorts slutligt genom en dom eller ett beslut som har fått laga kraft får direktåtkomst till personuppgifterna i målet eller ärendet medges endast

1. under sex månader efter det att domen eller beslutet fick laga kraft vid direktåtkomst enligt 8–10 §§, och
2. under tjugo år efter det att domen eller beslutet fick laga kraft vid direktåtkomst enligt 11 §.

Bemyndigande

14 §

Domstolsverket får meddela närmare föreskrifter om tillgången till personuppgifter. För tilldelning av behörighet för tillgång till personuppgifter ska det särskilt beaktas att det utöver behovet av uppgifterna ställs krav på utbildning och erfarenhet.

Domstolsverket får även meddela

1. föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter på medium för automatiserad behandling,
2. ytterligare föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter genom direktåtkomst och om behörighet och säkerhet vid sådant utlämnande,
3. ytterligare föreskrifter om begränsningar för behandling av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts slutligt genom en dom eller ett beslut som har fått laga kraft, och
4. de ytterligare föreskrifter som behövs för verkställighet av domstolsdatalagen (2015:728) och denna förordning.

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 ⁽¹⁾,

med beaktande av Regionkommitténs yttrande ⁽²⁾,

i enlighet med det ordinarie lagstiftningsförfarandet ⁽³⁾, 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 ⁽⁴⁾ 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.

⁽¹⁾ EUT C 229, 31.7.2012, s. 90.

⁽²⁾ EUT C 391, 18.12.2012, s. 127.

⁽³⁾ 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.

⁽⁴⁾ 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 (EGTL 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 fastställs 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 snedvrída 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 byggas på artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG⁽¹⁾.
- (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⁽²⁾ 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

⁽¹⁾ 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).

⁽²⁾ 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⁽¹⁾. 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 strukturer. 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 rättskipande 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⁽²⁾, särskilt bestämmelserna om tjänstelevererande mellanhanders 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 informations-samhällets tjänster mellan medlemsstaterna.
- (22) All behandling av personuppgifter som sker inom ramen för arbetet på personuppgiftsansvariga 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.

⁽¹⁾ 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).

⁽²⁾ Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informations-samhällets 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 fräntas 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 utbudande 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 nätidentifikatorer 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 serverna, 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⁽¹⁾, 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 kroppsdelen 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

⁽¹⁾ 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 företags 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 inte 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⁽¹⁾ 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 oskäligen 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 ojämlighet 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 – inbegriper 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 offentlig-rättslig 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

(1) Rådets direktiv 93/13/EEG av den 5 april 1993 om oskäligen 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 biometrisk uppgift 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 gränsoverskridande 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⁽¹⁾, 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.

⁽¹⁾ 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 personuppgiftsbehandlings 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 fullständig 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 anförtrots 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 innebära 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 innebära 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 sörja 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 sörja 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 överträdelse 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 överträdelse 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 personuppgiftsbitrådets 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 dataskyddsbud. 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 iaktas, 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 personuppgiftsbitråden 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 personuppgiftsbitrådenas 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 personuppgiftsbitråden 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 personuppgiftsbitrådena 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 överträdelse 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 personuppgiftsbitrådets vägnar och kan kontaktas av samtliga tillsynsmyndigheter. Företrädaren bör uttryckligen utses genom en skriftlig fullmakt från den personuppgiftsansvarige eller från personuppgiftsbitrådet att agera på dennes vägnar med avseende på dennes skyldigheter enligt denna förordning. Utnämningen av företrädaren inverkar inte på den personuppgiftsansvariges eller på personuppgiftsbitrådets ansvar enligt denna förordning. Företrädaren bör utföra sina uppgifter i enlighet med erhållen fullmakt från den personuppgiftsansvarige eller från personuppgiftsbitrådet, vilket inbegriper samarbete med de behöriga tillsynsmyndigheterna i fråga om alla åtgärder som vidtas för att sörga för efterlevnad av denna förordning. Den utsedda företrädaren bör underkastas verkställighetsförfaranden i händelse den personuppgiftsansvarige eller personuppgiftsbitrådet 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 sakskapskap, 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. Personuppgiftsbitrådets 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 personuppgiftsbitrådet och den personuppgiftsansvarige, där föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade anges, med beaktande av personuppgiftsbitrådets 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 personuppgiftsbitrådet 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 personuppgiftsbitrådet återlämna eller radera personuppgifterna, beroende på vad den personuppgiftsansvarige väljer, såvida inte lagring av personuppgifterna krävs enligt den unionsrätt eller medlemsstaternas nationella rätt som personuppgiftsbitrådet 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 obehörigt 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 sörga 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 dataskydd 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 anmälningskyldigheter 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 personuppgiftsskyddet 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, biometrisk 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 personuppgiftsbitrådets 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 dataskyddsbud 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 uppmanas 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 uppmanas, 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 dataskyddövervakning 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 personuppgifter behandlas inom en eller flera specifika sektorer. Tredjelandet bör framför allt säkerställa en effektiv oberoende dataskyddövervakning och sörja för samarbetsmekanismer med medlemsstaternas dataskyddsmyndigheter, och de registrerade bör tillförsäkras effektiva och lagstadgade rättigheter samt effektiv administrativ och rättslig prövning.
- (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 personuppgiftsbitrådets möjlighet att använda standardiserade dataskyddsbestämmelser som antagits av kommissionen eller av en tillsynsmyndighet bör inte hindra att de infogars

(*) 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 uppmanas 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 kontaktpårning 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 anförtratts 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 mandatid 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 personuppgiftsbiträdes 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 personuppgiftsbiträdes 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 personuppgiftsbiträdes 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 personuppgiftsbiträdes 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 om 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 lägga 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 överträdelse 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 förhållande tillstånd 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 personuppgiftsbitrådets behandling men den sakfråga som klagomålet gäller eller den möjliga överträdelsen endast rör den personuppgiftsansvariges eller personuppgiftsbitrådets 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 överträdelse 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 eventuellt 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 fördrar 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 stadgeeignade 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 tillsynsmyndigheterna 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 uttalanden 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 överträdelse 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⁽¹⁾, påverka tillämpningen av sådana särskilda bestämmelser.
- (148) För att stärka verkställigheten av denna förordning bör det utdömas sanktioner, inbegripet administrativa sanktionsavgifter, för överträdelse 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 uppsåtligt, vilka åtgärder som vidtagits för att lindra skadan, graden av ansvar eller eventuella tidigare överträdelse 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 försärande 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 överträdelse av denna förordning, inbegripet för överträdelse 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 överträdelse av denna förordning. Utdömandet av straffrättsliga påföljder för överträdelse 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 överträdelse av denna förordning bör samtliga tillsynsmyndigheter ha befogenhet att utfärda administrativa sanktionsavgifter. Det bör i denna

⁽¹⁾ 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 överträdelse 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 överträdelse 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 sammanjämknigen 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 iaktas. 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 betydande under tidigare totalitära regimer, folkmord, brott mot mänskligheten, särskilt Förintelsen, eller krigsförbrytelse.

- (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 insynskydd 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 preciseringsregler 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 insynskyddade 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 genomförandekter 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, ömsidigt 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 genomförandekter, 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 ⁽¹⁾.
- (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 ⁽²⁾, 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.

⁽¹⁾ EUT C 192, 30.6.2012, s. 7.

⁽²⁾ 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 tjänstelevererande mellanhanders 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) utbudande 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 identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringuppgift 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 personuppgiftsbitrådets 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 överförs, 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 personuppgiftsbitrådets verksamhetsställen i unionen där den huvudsakliga behandlingen inom ramen för verksamheten vid ett av personuppgiftsbitrådets 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
- den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad på tillsynsmyndighetens medlemsstats territorium,
 - registrerade som är bosatta i den tillsynsmyndighetens medlemsstat i väsentlig grad påverkas eller sannolikt i väsentlig grad kommer att påverkas av behandlingen, eller
 - ett klagomål har lämnats in till denna tillsynsmyndighet,
23. *gränsöverskridande behandling*:
- 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
 - 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 ⁽¹⁾,
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:
- Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (*laglighet, korrekthet och öppenhet*).
 - 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*).
 - De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (*uppgiftsminimering*).
 - 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*).

⁽¹⁾ 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 överträdelse 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 föräldransvar 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 föräldrans ansvar 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 budet 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 eftersträfvade 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 begärs, 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 förutsetta 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 förutsetta 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 uttalande.

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 vänt 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 uttrycka 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 överträdelse 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 överträdelse, 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 personuppgiftsbitrådets uppdrag, utöver eller i stället för den personuppgiftsansvarige eller personuppgiftsbitrådet, 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 personuppgiftsbitrådet utser en företrädare ska inte påverka de rättsliga åtgärder som skulle kunna inledas mot den personuppgiftsansvarige eller personuppgiftsbitrådet.

Artikel 28

Personuppgiftsbitråden

1. Om en behandling ska genomföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige endast anlita personuppgiftsbitråden 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. Personuppgiftsbitrådet får inte anlita ett annat personuppgiftsbitråde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbitrådet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbitråden eller ersätta personuppgiftsbitråden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.
3. När uppgifter behandlas av ett personuppgiftsbitråde ska hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbitrådet 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 personuppgiftsbitrådet
 - 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 personuppgiftsbitrådet omfattas av, och i så fall ska personuppgiftsbitrådet 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 iakta 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 anlitaandet av ett annat personuppgiftsbitråde,
 - 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 personuppgiftsbitrådet har tillgång till,
 - 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:

- Namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet.
- Ändamålen med behandlingen.
- 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 personuppgiftsbitrådets 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 personuppgiftsbitrådets 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 fallande 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 personuppgiftsbitrådets 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 överträdelse 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 personuppgiftsbitrådets 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 personuppgiftsbitrådets 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 överträdelse, 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 personuppgiftsbitrådets 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 personuppgiftsbitrådets 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 personuppgiftsbitrådets strategi för skydd av personuppgifter, inbegripet ansvarstildelning, 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 föräldrans svar 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 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 förenligt 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 överträdelse 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 uppmanra, 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 personuppgiftsbitrådets 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 samlar 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⁽¹⁾ i enlighet med EN-ISO/IEC 17065/2012 och med de ytterligare krav som fastställs 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,

⁽¹⁾ Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknads kontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

- b) förbundet 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 överträdelse 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 personuppgiftsbitrådets 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 effektivt 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 enligt 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 enligt 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 rättsligt 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 gruppen 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 gruppen 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 korrigering 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 gruppen 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 om överföringen 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 utövat av deras befogenheter. Under mandatperioden ska denna tystnadsplikt i synnerhet gälla rapportering från fysiska personer om överträdelse 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 personuppgiftsbitrådets huvudsakliga verksamhetsställe eller enda verksamhetsställe vara behörig att agera som ansvarig tillsynsmyndighet för den personuppgiftsansvariges eller personuppgiftsbitrådets 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 personuppgiftsbitrådet 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 personuppgiftsbitrådets enda motpart när det gäller den registreringsansvariges eller den personuppgiftsbitrådets 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 personuppgiftsbitrådets 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 dataskyddsbudet.
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 personuppgiftsbitrådets 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 överträdelse 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 överträdelse 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 personuppgiftsbitrådets 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 avisas 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 personuppgiftsbitrådets 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 avisande 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 utbyts 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

Twistlösning 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 inletts 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 inletts 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 skyndsamt 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 överträdelse 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 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 ⁽¹⁾.

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.

⁽¹⁾ 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 medlemsstat 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 uppgiftsbehandlings 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 personuppgiftsbitrådets 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 underlåtenhet 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 till 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.

L 119/88

SV

Europeiska unionens officiella tidning

4.5.2016

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 27 april 2016.

På Europaparlamentets vägnar

M. SCHULZ
Ordförande

På rådets vägnar

J.A. HENNIS-PLASSCHAERT
Ordförande

Departementsserien 2017

Kronologisk förteckning

1. Elektronisk övervakning av kontaktförbud. Ju.
2. Åldersdifferentierat underhållsstöd och höjt grundavdrag för bidragsskyldiga föräldrar. S.
3. Genomförande av ICT-direktivet. Ju.
4. Sjukpenning i avvaktan på slutligt beslut. S.
5. Effektivare sanktioner i livsmedelskedjan m.m. N.
6. Förslag till lag om ersättning till personer som har fått ändrad könstillhörighet fastställd i vissa fall. S.
7. Kommunikation för vår gemensamma säkerhet. Uppdrag om en utvecklad och säker kommunikationslösning för aktörer inom allmän ordning, säkerhet, hälsa och försvar. Ju.
8. Kultursamverkan för ett Sverige som håller ihop. Framtida inriktning och utvecklingsmöjligheter för kultursamverkansmodellen. Ku.
9. Förstärkt rehabilitering för återgång i arbete. S.
10. ILO:s konvention om anständiga arbetsvillkor för hushållsarbetare. A.
11. Ändrade regler om retroaktivitet avseende efterlevandestöd. S.
12. Om förenklat beslutsfattande och särskilda boendeformer för äldre. S.
13. Skadeståndets bestämmande vid finansiell rådgivning. Fi.
14. Vissa ändringar i läkemedelslagen. S.
15. Ökat konsulärt skydd för unionsmedborgare och deras familjemedlemmar. Genomförande av direktiv (EU) 2015/637. UD.
16. Arbetsplatsinspektioner och höjd särskild avgift. Ju.
17. En ny lag om försäkringsdistribution. Fi.
18. Karensavdrag – en mer rättvis självrisk. S.
19. Anpassningar av de fastighetsrättsliga, associationsrättsliga, transporträttsliga och immaterialrättsliga författningarna till dataskyddsförordningen. Ju.
20. Regionalt utvecklingsansvar i Stockholms, Kalmar och Blekinge län. Fi.
21. Skyldighet för vissa offentliga funktionärer att anmäla innehav av finansiella instrument. Fi.
22. Utstationering och vägtransporter. A.
23. Kompletterande bestämmelser till EU:s förordning om personlig skyddsutrustning. Fi.
24. Skjutvapen och explosiva varor – Skärpta straff för de grova brotten. Ju.
25. Nya ungdomspåföljder. Ju.
26. En anpassning till dataskyddsförordningen – kreditupplysningslagen och några andra författningar. Ju.
27. Genomförande av säsongsanställningsdirektivet. Ju.
28. En anpassning till dataskyddsförordningen av dataskyddsbestämmelser inom Näringsdepartementets verksamhetsområde. N.
29. Utökade möjligheter till utbyte av läkemedel. S.
30. Ett entreprenörsansvar i bygg- och anläggningsbranschen. A.
31. Elektroniska fakturor vid offentlig upphandling. Fi.
32. Biologiskt mångfald och ekosystemtjänster. Kontrollstation 2016. M.
33. Anpassningar till dataskyddsförordningen av registerförfattningar inom Arbetsmarknadsdepartementets ansvarsområde. A.
34. Ändringar i bestämmelser om val till Sametinget. K.
35. Körkortslån. A.
36. En snabbare lagföring. Försöksprojekt med ett snabbförfarande i brottmål. Ju.

37. Frekventa och omfattande ärenden om utlämnande av allmän handling. Ju.
38. Livstidsstraff för mord. Ju.
39. Legitimation för hälso- och sjukvårdskuratorer. S.
40. Ändringar i vissa författningar inom Finansdepartementets ansvarsområde med anledning av EU:S dataskyddsreform. Fi.
41. En omarbetad domstolsdatalag. Anpassning till EU:s dataskyddsförordning. Ju.

Departementsserien 2017

Systematisk förteckning

Arbetsmarknadsdepartementet

- ILO:s konvention om anständiga arbetsvillkor för hushållsarbetare. [10]
- Utstationering och vägtransporter. [22]
- Ett entreprenörsansvar i bygg- och anläggningsbranschen. [30]
- Anpassningar till dataskyddsförordningen av registerförfattningar inom Arbetsmarknadsdepartementets ansvarsområde. [33]
- Körkortslån. [35]

Finansdepartementet

- Skadeståndets bestämmande vid finansiell rådgivning. [13]
- En ny lag om försäkringsdistribution. [17]
- Regionalt utvecklingsansvar i Stockholms, Kalmar och Blekinge län. [20]
- Skyldighet för vissa offentliga funktionärer att anmäla innehav av finansiella instrument. [21]
- Kompletterande bestämmelser till EU:s förordning om personlig skyddsutrustning. [23]
- Elektroniska fakturor vid offentlig upphandling. [31]
- Ändringar i vissa författningar inom Finansdepartementets ansvarsområde med anledning av EU:s dataskyddsreform. [40]

Justitiedepartementet

- Elektronisk övervakning av kontaktförbud. [1]
- Genomförande av ICT-direktivet. [3]
- Kommunikation för vår gemensamma säkerhet. Uppdrag om en utvecklad och säker kommunikationslösning för aktörer inom allmän ordning, säkerhet, hälsa och försvar. [7]
- Arbetsplatsinspektioner och höjd särskild avgift. [16]

Anpassningar av de fastighetsrättsliga, associationsrättsliga, transporträttsliga och immaterialrättsliga författningarna till dataskyddsförordningen. [19]

Skjutvapen och explosiva varor – Skärpta straff för de grova brotten. [24]

Nya ungdomspåföljder. [25]

En anpassning till dataskyddsförordningen – kreditupplysningslagen och några andra författningar. [26]

Genomförande av säsongsanställningsdirektivet. [27]

En snabbare lagföring. Försöksprojekt med ett snabbförfarande i brottmål. [36]

Frekventa och omfattande ärenden om utlämnande av allmän handling. [37]

Livstidsstraff för mord. [38]

En omarbetad domstolsdatalag. Anpassning till EU:s dataskyddsförordning. [41]

Kulturdepartementet

Kultursamverkan för ett Sverige som håller ihop. Framtida inriktning och utvecklingsmöjligheter för kultursamverkansmodellen. [8]

Ändringar i bestämmelser om val till Sametinget. [34]

Miljö- och energidepartementet

Biologisk mångfald och ekosystemtjänster. Kontrollstation 2016. [32]

Näringsdepartementet

Effektivare sanktioner i livsmedelskedjan m.m. [5]

En anpassning till dataskyddsförordningen av dataskyddsbestämmelser inom Näringsdepartementets verksamhetsområde. [28]

Socialdepartementet

- Åldersdifferentierat underhållsstöd och höjt grundavdrag för bidragsskyldiga föräldrar. [2]
- Sjukpenning i avvaktan på slutligt beslut. [4]
- Förslag till lag om ersättning till personer som har fått ändrad könstillhörighet fastställd i vissa fall. [6]
- Förstärkt rehabilitering för återgång i arbete. [9]
- Ändrade regler om retroaktivitet avseende efterlevandestöd. [11]
- Om förenklat beslutsfattande och särskilda boendeformer för äldre. [12]
- Vissa ändringar i läkemedelslagen. [14]
- Karensavdrag – en mer rättvis självrisk. [18]
- Utökade möjligheter till utbyte av läkemedel. [29]
- Legitimation för hälso- och sjukvårdskuratorer. [39]

Utrikesdepartementet

- Ökat konsulärt skydd för unionsmedborgare och deras familjemedlemmar. Genomförande av direktiv (EU) 2015/637. [15]