EUROPEISKA
KOMMISSIONEN

Bryssel den 19.11.2025
COM(2025) 837 final

2025/0360 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om ändring av förordningarna (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 och direktiven 2002/58/EG, (EU) 2022/2555 och (EU) 2022/2557 vad gäller förenkling av lagstiftningsramen på det digitala området och om upphävande av förordningarna (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 och direktiv (EU) 2019/1024 (det digitala omnibuspaketet)

{SWD(2025) 836 final}

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

I sitt meddelande om genomförande och förenkling (*Ett enklare och snabbare Europa*)[1] lade kommissionen fram sin strategi för att anpassa unionens regelverk till en mer instabil värld: en ny satsning för att förenkla, förtydliga och förbättra EU:s regelverk, som en nyckelåtgärd för att stödja EU:s konkurrenskraft.

Denna vision speglar den bredare plan som kommissionsordförande Ursula von der Leyen lade fram i sina politiska riktlinjer för mandatperioden 2024–2029[2]. Som även betonas i rapporterna från Draghi[3] och Letta[4] har ackumuleringen av regler ibland haft en negativ inverkan på konkurrenskraften. Snabba och synliga förbättringar för både människor och företag kan uppnås genom ett mer kostnadseffektivt och innovationsvänligt genomförande av våra regler, samtidigt som höga standarder och överenskomna mål upprätthålls.

I Europeiska rådets slutsatser av den 20 mars 2025 uppmanades kommissionen att ”fortsätta att se över och stresstesta EU:s regelverk för att identifiera sätt att ytterligare förenkla och konsolidera befintlig lagstiftning"[5]. Rådet betonade även behovet av att följa upp med ytterligare förenklingsinitiativ. I sina slutsatser av den 26 juni betonade Europeiska rådet vikten av lagstiftning om ”inbyggd enkelhet”, ”utan att undergräva förutsägbarheten, de politiska målen och de höga standarderna”[6]. I Europeiska rådets slutsatser av den 23 oktober 2025 bekräftades på nytt det brådskande behovet av att främja en ambitiös och horisontellt driven agenda för förenkling och bättre lagstiftning på alla nivåer – EU-nivå, nationell nivå och regional nivå – och på alla områden för att säkerställa EU:s konkurrenskraft. Rådet uppmanade även kommissionen att snabbt lägga fram ytterligare ambitiösa förenklingspaket, bland annat om digitalisering[7].

I sin resolution om ”genomförande och rationalisering av EU:s regler för den inre marknaden för att stärka den inre marknaden”, som röstades igenom i plenum den 11 september[8], betonade Europaparlamentet behovet av förenkling för att underlätta företagens efterlevnad utan att äventyra EU:s centrala politiska mål.

---

1 Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, *Ett enklare och snabbare Europa: Meddelande om genomförande och förenkling*, COM(2025) 47 final, 11 februari 2025.

2 von der Leyen, U. (2024) *Europas val*: *Politiska riktlinjer för nästa Europeiska kommission 2024–2029*. Tillgänglig på: e6cd4328-673c-4e7a-8683-f63ffb2cf648_sv.

3 Draghi, M. (2024) *The future of European competitiveness*. Tillgänglig på: Draghis rapport om EU:s konkurrenskraft.

4 Letta, E. (2024) *Much more than a market*. Tillgänglig på: Enrico Letta – *Much more than a market* (april 2024).

5 Europeiska rådet, Slutsatser, EUCO 1/25, Bryssel, 20 mars 2025, punkt 13.

6 Europeiska rådet, Slutsatser, EUCO 12/25, Bryssel, 26 juni 2025, punkt 30.

7 Europeiska rådet, Slutsatser, EUCO 18/25, Bryssel, 23 oktober 2025, punkterna 33 och 35.

8 Europaparlamentet, Resolution om genomförande och rationalisering av EU:s regler för den inre marknaden för att stärka den inre marknaden, 11 september 2025 (2025/2009/INI).

Vid kommissionens insatser för samråd och deltagande kring förenklingsagendan har berörda parter som företräder olika intressen efterlyst riktade ändringar av vissa digitala regler, både för att effektivisera efterlevnadskostnaderna och för att klargöra samspelet mellan reglerna inom deras sektorer.

Med ett mervärde på 791 miljarder euro i Europeiska unionen 2022[9] spelar IKT-sektorn en avgörande roll för att främja EU:s konkurrenskraft inom alla sektorer av ekonomin, både genom att låta digitala företag växa och genom att erbjuda viktiga digitala lösningar på alla områden. Digitala regler har bidragit till att skapa ett rättvist företagsklimat i EU, och har gjort det möjligt att inrätta en verklig inre marknad för digitala tjänster. EU har gått i spetsen för den digitala regleringen och satt högsta möjliga standard när det gäller skyddet av grundläggande rättigheter, konsumentsäkerhet och skydd av europeiska värderingar.

Kommissionen har åtagit sig att göra ett omfattande ”stresstest” av det digitala regelverket under hela lagstiftningsmandatet. Målet är mycket tydligt: att se till att reglerna är ändamålsenliga för att stödja innovation och tillväxt, att de bidrar till de uppsatta målen och att de fortsätter att vara en drivkraft för konkurrenskraft. Under hela denna process kommer kommissionen att sträva efter att tillhandahålla tvingande lösningar för att förenkla, förtydliga och befästa reglernas ändamålsenlighet och deras tillämpning genom alla tillgängliga instrument, oavsett om det rör sig om anpassningar av lagstiftningen, utökat samarbete mellan myndigheterna, främjande av digitala lösningar som förenklar den ”inbyggda” regelefterlevnaden eller andra kompletterande åtgärder.

Förslaget om ett digitalt omnibuspaket är ett första steg mot att optimera tillämpningen av det digitala regelverket. I paketet ingår en uppsättning tekniska ändringar av ett stort antal digitala rättsakter som valts ut för att skyndsamt hjälpa företag, offentliga förvaltningar och medborgare att stimulera konkurrenskraften. Det omedelbara målet är att se till att efterlevnaden av reglerna sker till en lägre kostnad, bidrar till samma mål och i sig medför en konkurrensfördel för ansvarsfulla företag. Ändringarna prioriterades med utgångspunkt i samråden med berörda parter och de inledande genomförandedialoger som anordnades av verkställande vice ordförande Henna Virkkunen och kommissionsledamot Michael McGrath.

Av dessa skäl har ändringarna inriktats på att frigöra möjligheter att använda data som en grundläggande resurs i EU:s ekonomi, inte minst för att stödja utvecklingen och användningen av tillförlitliga lösningar för artificiell intelligens på EU:s marknad. Riktade ändringar av reglerna för dataskydd och integritet stöder detta mål och leder till omedelbara förenklingsåtgärder för företag och enskilda, vilket stärker deras förmåga att utöva sina rättigheter.

Dessutom syftar ändringarna av förordning (EU) 2024/1689 (rättsakten om artificiell intelligens[10]), vilken presenteras som ett lagförslag i en separat del av det digitala omnibuspaketet, till att underlätta en smidig och effektiv tillämpning av reglerna för säker och tillförlitlig utveckling och användning av AI.

---

[9] Eurostat (2025) *Statistics explained : ICT sector – value added, employment and R&D*. Tillgänglig på: ICT sector – value added, employment and R&D – Statistics Explained – Eurostat.

[10] Enligt separat lagförslag.

I det digitala omnibuspaketet föreslås även en mycket tydlig lösning för att effektivisera rapporteringen av cybersäkerhetsincidenter, vilket gör att alla tillhörande rapporteringsskyldigheter omfattas av en gemensam rapporteringsmekanism.

Slutligen innebär förslaget att föråldrade regler på området för reglering av plattformar upphävs och ersätts av nyare föreskrifter.

Syftet med ändringarna är att effektivisera reglerna, minska antalet rättsakter och harmonisera bestämmelserna. De minskar även de administrativa kostnaderna genom att förenkla bestämmelser och förfaranden. Ändringarna innebär att små midcapföretag befrias från vissa skyldigheter i datalagstiftningen och förordning (EU) 2024/1689 (rättsakten om artificiell intelligens[11]), eftersom små företag och mikroföretag redan omfattas av ett särskilt system. De stimulerar även ett dynamiskt företagsklimat genom att skapa större rättssäkerhet och bättre möjligheter, i synnerhet när det gäller att dela och vidareutnyttja data, behandla personuppgifter eller träna system och modeller för artificiell intelligens.

Samtidigt förblir de föreslagna ändringarna tekniska till sin natur, eftersom de syftar till att anpassa regelverket men inte till att ändra dess underliggande mål. Åtgärderna kalibreras för att upprätthålla samma standard för skyddet av grundläggande rättigheter.

Samtidigt med det digitala omnibuspaketet lägger kommissionen också fram sitt förslag till en **förordning om europeiska företagsplånböcker** som ett centralt initiativ för att förenkla regelefterlevnaden och minska företagens administrativa börda. Företagsplånböckerna kommer att utformas som säkra digitala verktyg för företagen och fungera som en gemensam plattform för att förenkla deras samverkan i hela EU. Ett unikt och beständigt identifikationsnummer kommer att ge företagen befogenhet att digitalt verifiera identiteter, underteckna handlingar, utfärda tidsstämplar och utbyta verifierad digital information över gränserna med hjälp av en enda lösning. Antagandet av europeiska företagsplånböcker kommer att ge företag, särskilt små och medelstora företag, möjlighet att säkerställa efterlevnaden på ett enkelt sätt och frigöra viktiga resurser till tillväxt och innovation.

Som ett andra steg i åtagandet att ”stresstesta” det digitala regelverket **utför kommissionen även en kontroll av den digitala ändamålsenligheten**. Förslagen om ett digitalt omnibuspaket är omedelbara och målinriktade, men kommissionens analys av den digitala ändamålsenligheten kommer att vara inriktad på de digitala reglernas kumulativa inverkan för att utröna hur de stöder EU:s konkurrenskraft och på vilka områden det behövs ytterligare anpassningar under den andra hälften av lagstiftningsmandatet.

Kontrollen av den digitala ändamålsenligheten inleds med ett brett offentligt samråd samtidigt som förslaget om ett omnibuspaket läggs fram. Kommissionen strävar efter att samarbeta och samråda i omfattande utsträckning med alla berörda parter. Målet är att följa upp med en översikt och en bred kartläggning av hur det digitala regelverket omfattar strategiska sektorer inom EU:s industri och hur reglernas kumulativa effekt påverkar deras konkurrenskraft. På denna grund kommer analysen i ett andra steg att gå djupare in på de synergier och områden

[11] Enligt separat förslag.

som skulle kunna anpassas ytterligare, från definitioner och rättsliga begrepp till ändamålsenligheten hos och samspelet mellan styrningssystemen och andra stödåtgärder.

”Stresstestet” av det digitala regelverket kommer även att fortsätta genom genomförandedialoger och med **utvärderingar av alla de viktigaste rättsliga instrumenten**. Enligt den nuvarande planen för 2026 ska kommissionen bland annat offentliggöra en översyn av rättsakten om digitala marknader, policyprogrammet för det digitala decenniet, förordningen om halvledare och direktivet om audiovisuella medietjänster samt en utvärdering av direktivet om upphovsrätt. Planen för 2027 omfattar bland annat en utvärdering av cybersolidaritetsakten, förordningen om öppet internet, NIS2 och förordningen om digitala tjänster. År 2028 ska kommissionen bland annat utvärdera den europeiska mediefrihetsförordningen och dataförordningen, följt av en utvärdering av förordningen om artificiell intelligens under 2029 och en utvärdering av tidsfristklausulen i förordningen om inrättande av Europeiska kompetenscentrumet och nätverket för cybersäkerhet.

Berörda parter har upprepade gånger betonat att förenklingsarbetet i många fall handlar mindre om att ändra reglerna och mer om att göra deras tillämpning tydligare. **Kommissionen prioriterar ett antal riktlinjer** som syftar till att stödja en enhetlig tillämpning av reglerna utan att påverka domstolens tolkningar.

När det gäller regelverket för datalagstiftning tillkännagav kommissionen sina prioriteringar i strategin för dataunionen, särskilt med fokus på riktlinjer om rimlig ersättning för att klargöra vad som kan tas ut för datadelning och skapa rättssäkerhet för både innehavare och mottagare av data, samt riktlinjer för förtydligande av definitioner.

För att underlätta tillämpningen av förordningen om artificiell intelligens fortsätter kommissionen att prioritera utfärdandet av riktlinjer om flera olika aspekter, vilket beskrivs närmare i motiveringen till förslaget om ett digitalt omnibuspaket om ändring av lagen om artificiell intelligens.

Förslag i det digitala omnibuspaketet

Under de senaste åren har **”regelverket för datalagstiftning”** utvidgats till en rad olika förordningar, vilket har lett till rättslig komplexitet, däribland vissa överlappningar, dåligt anpassade definitioner samt frågor kring samspelet mellan instrumenten. Till exempel utformades och antogs förordning (EU) 2018/1807 (förordningen om det fria flödet av andra data än personuppgifter) för att skapa en inre marknad för molntjänster. Den har delvis ersatts av kapitel VI i förordning (EU) 2023/2854 (dataförordningen), där skyldigheterna vid byte av databehandlingstjänster fastställs.

Ett annat exempel är kapitel II i förordning (EU) 2022/868 (dataförvaltningsakten), som kompletterar reglerna om vidareutnyttjande av information från den offentliga sektorn i direktiv (EU) 2019/1024 (direktivet om öppna data) för data som inte får vidareutnyttjas utan begränsningar. Andra kapitel i förordning (EU) 2022/868 (dataförvaltningsakten) innehöll bestämmelser om dataförmedlingstjänster, dataaltruism, krav för utländska myndigheters begäran om tillgång till andra data än personuppgifter och inrättandet av Europeiska datainnovationsstyrelsen. Genom förordning (EU) 2023/2854 (dataförordningen) infördes å andra sidan en väsentlig skyldighet för tillverkare av uppkopplade enheter och leverantörer av tillhörande tjänster att dela data med sina användare, eller för företag att dela data med statliga organ, samt regler om rättvisa avtal om datadelning.

För att ta itu med detta föreslås i omnibuspaketet att föråldrade regler ska upphävas, särskilt de gällande reglerna i förordning (EU) 2018/1807 (förordningen om det fria flödet av andra data än personuppgifter), med undantag av förbudet mot datalokaliseringskrav i unionen, och att reglerna i förordning (EU) 2022/868 (dataförvaltningsakten) ska konsolideras och effektiviseras, däribland reglerna om dataaltruism och dataförmedlingstjänster för att göra dessa mekanismer mer attraktiva. Samtidigt slås reglerna i dataförvaltningsakten om vidareutnyttjande av skyddade data ihop med reglerna i direktiv (EU) 2019/1024 (direktivet om öppna data) för att skapa en enhetlig ram för vidareutnyttjande av data som innehas av offentliga organ, vilket återspeglas i förordning (EU) 2023/2854 (dataförordningen). Denna lösning ger många fördelar, både för offentliga förvaltningar som innehar data från den offentliga sektorn och för vidareutnyttjare, eftersom de kan effektivisera processerna och minska den administrativa bördan i samband med tolkning och genomförande av olika nationella lagar.

Genom ändringen införs dessutom en möjlighet för offentliga organ att fastställa olika villkor och ta ut högre avgifter för vidareutnyttjande av mycket stora företag, särskilt företag som utsetts till grindvakter, enligt definitionen i artikel 3 i förordning (EU) 2022/1925 (förordningen om digitala marknader), vilka har betydande makt och inflytande över den inre marknaden. För att förhindra att dessa enheter utnyttjar sitt betydande marknadsinflytande på bekostnad av rättvis konkurrens och innovation ska offentliga organ kunna fastställa särskilda villkor för enheternas vidareutnyttjande av data och handlingar.

Förslaget omfattar de konsoliderade och rationaliserade reglerna i förordning (EU) 2024/1689 (förordningen om det fria flödet av uppgifter), förordning (EU) 2022/868 (dataförvaltningsakten) och direktiv (EU) 2019/1024 (direktivet om öppna data) i förordning (EU) 2023/2854 (dataförordningen), vilka tillsammans skapar ett enda konsoliderat instrument för Europas dataekonomi. Förordning (EU) 2024/1689 (förordningen om det fria flödet av uppgifter), direktiv (EU) 2019/1024 (direktivet om öppna data) och förordning (EU) 2022/868 (dataförvaltningsakten) ska upphöra att gälla. Reglerna i alla de fyra instrumenten har anpassats och rationaliserats för att öka tydligheten och enhetligheten, och därigenom öka deras effektivitet och hjälpa företagen att driva på innovation. Detta initiativ är förenligt med strategin för dataunionen, vilken i grunden syftar till att driva på förenklingen av den rättsliga ramen.

För att ge ytterligare stöd till mindre företag utvidgas dessutom de regler som underlättar efterlevnaden av EU:s datalagstiftning för små och medelstora företag till att även omfatta små midcapföretag. Förordning (EU) 2023/2854 (dataförordningen), som trädde i kraft den 12 september 2025, är ett viktigt steg mot en rättvis och konkurrenskraftig dataekonomi i EU. De ändringar som föreslås i detta förslag syftar inte till att införa ändringar av resultaten av förordning (EU) 2023/2854 (dataförordningen).

För att fullt ut uppnå målet att balansera innovation och datatillgänglighet med skyddet av datahållarnas rättigheter och intressen måste dock fyra centrala delar anpassas till varandra. Framför allt är det viktigt att säkerställa att förordning (EU) 2023/2854 (dataförordningen) inte bara minskar bördorna, utan även ökar den rättsliga klarheten och främjar konkurrenskraften. För det första är det brådskande att stärka skyddsåtgärderna mot risken för spridning av företagshemligheter till tredjeländer inom ramen för de obligatoriska bestämmelserna om datadelning inom sakernas internet. För det andra skulle den omfattande räckvidden av ramverket mellan företag och myndigheter kunna leda till rättslig oklarhet. För det tredje skulle rättslig osäkerhet kunna följa av bestämmelserna om grundläggande krav på smarta kontrakt för genomförande av datadelningsavtal. Slutligen har bestämmelserna i

förordning (EU) 2023/2854 (dataförordningen) om byten av databehandlingstjänster kvar sin relevans som ett centralt bidrag till en öppnare och mer konkurrenskraftig molnmarknad. Dessa bestämmelser var emellertid inte tillräckligt anpassade till den specifika situationen för tjänster som måste anpassas till kundens behov för att vara användbara eller som tillhandahålls av små och medelstora företag och små midcapföretag. De ändringar som ingår i detta förslag kommer att upprätthålla ambitionen att motverka inlåsning av leverantörer, särskilt när det gäller avgifter för byte och uttag, och samtidigt minska den administrativa bördan för leverantörer av ovannämnda tjänster. Förslaget innehåller därför ändringar som ökar den rättsliga klarheten och som är tydligt anpassade till de övergripande målen i förordning (EU) 2023/2854 (dataförordningen).

För att ge ytterligare stöd mindre företag utvidgas dessutom de regler som underlättar efterlevnaden av EU:s dataregelverk för små och medelstora företag till att även omfatta små midcapföretag.

När det gäller personuppgifter blev förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och fri rörlighet för sådana uppgifter (den allmänna dataskyddsförordningen) tillämplig den 25 maj 2018, vilket ledde till införandet av unionsomfattande standarder, regler och skyddsåtgärder för behandlingen av enskilda personers personuppgifter och de registrerades rättigheter samt en allmän rättslig ram för alla som behandlar personuppgifter. De flesta berörda parter har funnit att förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) är balanserad och sund och att den fortfarande är ändamålsenlig, men vissa enheter, särskilt mindre företag och sammanslutningar som sällan behandlar uppgifter, ofta med låg risk, har uttryckt oro över tillämpningen av vissa skyldigheter i den allmänna dataskyddsförordningen. Vissa av dessa farhågor kan bemötas genom en mer konsekvent och harmoniserad tolkning och tillämpning i medlemsstaterna, medan andra kräver riktade ändringar av lagstiftningen. I detta sammanhang syftar ändringarna i detta förslag till att bemöta farhågorna, särskilt genom att klargöra vissa centrala definitioner, däribland begreppet personuppgifter. Målet är att underlätta efterlevnaden, till exempel genom att bistå personuppgiftsansvariga när det gäller kriterierna och metoderna för att avgöra om pseudonymiserade uppgifter utgör personuppgifter, i förhållande till informationskrav och anmälningar om uppgiftsincidenter till tillsynsmyndigheterna, samt genom att klargöra vissa aspekter av behandlingen av data för träning och utveckling av AI. De föreslagna ändringarna syftar även till att åtgärda bristen på tydlighet när det gäller villkoren för vetenskaplig forskning, däribland genom att tillhandahålla en definition av vetenskaplig forskning, klargöra att ytterligare bearbetning för vetenskapliga ändamål är förenlig med det ursprungliga syftet med bearbetningen samt klargöra att vetenskaplig forskning utgör ett berättigat intresse. Det föreslås även att undantagen från informationsskyldigheten i samband med behandling ska förlängas. I förekommande fall speglar detta förslag ändringarna av den allmänna dataskyddsförordningen i förordning (EU) 2018/1725 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer.

Det är även brådskande att hitta en lagstiftningslösning när det gäller trötthetten i samband med samtycke till kakor. Direktiv (EU) 2002/58/EG om integritet och elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation), som senast reviderades 2009, tillhandahåller en ram för att skydda konfidentialiteten vid kommunikation och kompletterar förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) i de fall där personuppgifter behandlas i samband med elektronisk kommunikation. Den skyddar även användarnas terminalutrustning, så att den inte används för att inkräkta på deras privatliv och samla in deras information. En viktig del av användningen av terminalutrustning – däribland

telefoner och persondatorer – är att konsumera innehåll och använda onlinetjänster. Många av dessa onlinetjänster är beroende av intäkter från reklam, inklusive personanpassad reklam. Detta gäller även för medietjänster. Leverantörer av onlinetjänster använder så kallade kakor eller liknande teknik som utnyttjar terminalutrustningens bearbetnings- och lagringskapacitet för att få tillgång till information som lagras i eller skickas ut från terminalutrustningen. Denna information används för en rad olika syften, däribland för att optimera tillhandahållandet av tjänsten till terminalutrustningen och säkerställa säkerheten för terminalutrustningen och den övergripande tjänsten, men även för att spåra individens beteende och samverkan med olika onlinetjänster för att tillhandahålla individanpassade annonser.

Om användningen av denna teknik inte är nödvändig för teknisk lagring eller åtkomst som endast sker för att utföra eller underlätta överföringen av en kommunikation via ett elektroniskt kommunikationsnät, eller om den är absolut nödvändig för att leverera en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt, krävs samtycke enligt direktiv (EU) 2002/58/EG (direktivet om integritet och elektronisk kommunikation). Detta samtycke begärs vanligen via popup-meddelanden som visas på webbplatsen eller mobilapplikationen. Meddelandena innehåller information om syftena med behandlingen, ofta kopplat till olika typer av kakor och datamottagare, och är inte alltid lätta att förstå för enskilda personer. Av dessa skäl är det inte säkert att de fullgör sitt syfte, dvs. att informera den enskilde användaren och ge honom eller henne kontroll över sin integritet och behandlingen av personuppgifter, utan snarare uppfattas som ett besvär. Samtidigt medför utformningen av meddelanden som uppfyller kraven stora kostnader för leverantörerna av onlinetjänster.

Den ökande komplexiteten framgår även av att artikel 5.3 i direktiv (EU) 2002/58/EG (direktivet om integritet och elektronisk kommunikation) är tillämplig på utplaceringen av kakor eller liknande teknik för att hämta information från en användares terminalutrustning, medan den efterföljande behandlingen av personuppgifter omfattas av förordning (EU) 2016/679 (den allmänna dataskyddsförordningen). Även om samtycke krävs för att säkerställa den registrerades kontroll är detta inte alltid den lämpligaste rättsliga grunden för den efterföljande behandlingen, till exempel om behandlingen är nödvändig för att utföra andra tjänster än informationssamhällets tjänster. Detta har lett till rättslig osäkerhet och högre efterlevnadskostnader för personuppgiftsansvariga som behandlar personuppgifter som hämtats från terminalutrustning. Dessutom har den dubbla ordningen med direktivet om integritet och elektronisk kommunikation och den allmänna dataskyddsförordningen lett till att olika nationella myndigheter varit behöriga att övervaka reglerna i de två rättsliga ramarna.

Av dessa skäl föreslås en omedelbar förenkling av samspelet mellan de tillämpliga reglerna. Behandlingen av personuppgifter på och från terminalutrustning bör endast regleras av förordning (EU) 2016/679 (den allmänna dataskyddsförordningen), vilket även omfattar det tydliga kravet på samtycke för tillgång till en fysisk persons terminalutrustning när personuppgifter samlas in. Genom de föreslagna ändringarna föreskrivs även vissa ändamål där det inte bör vara nödvändigt att erhålla samtycke och där den efterföljande behandlingen bör anses vara laglig, särskilt om den utgör en låg risk för den registrerades rättigheter och friheter eller om utplaceringen av sådan teknik är nödvändig för tillhandahållandet av en tjänst som den registrerade har begärt.

Slutligen banar förslaget väg för automatiserade och maskinläsbara upplysningar om individuella val och respekten för dessa upplysningar från leverantörer av webbplatser och mobilapplikationer när normerna väl finns tillgängliga. Detta bygger på 2009 års ändring av

direktiv (EU) 2002/58/EG (direktivet om integritet och elektronisk kommunikation) (se skäl 66 i direktiv 2009/136/EG), som redan då uppmuntrade till att göra det möjligt för användaren att uttrycka sitt samtycke genom lämpliga inställningar i en webbläsare eller annan applikation där detta är tekniskt möjligt och effektivt, artikel 21.5 i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) samt kommissionens förslag från 2017 om en förordning om respekt för privatlivet och skydd av personuppgifter (COM(2017) 10), där det föreslogs att användarens val skulle hanteras genom webbläsarens inställningar. Detta ger kommissionen mandat att begära att standardiseringsorganen ska utarbeta en uppsättning standarder för kodning av automatiserade och maskinläsbara upplysningar om den registrerades val och överföringen av dessa val från webbläsare till webbplatser och från mobilapplikationer till webbtjänster. När dessa väl finns tillgängliga, och efter en tidsfrist på sex månader, är personuppgiftsansvariga som använder webbplatser och mobilapplikationer för att tillhandahålla sina tjänster skyldiga att respektera dessa kodade automatiserade och maskinläsbara upplysningar. Om personuppgiftsansvariga säkerställer att deras webbplatser eller mobilapplikationer uppfyller dessa standarder bör de kunna åberopa en presumtion om överensstämmelse. På denna grund förväntas även att relevanta inställningar utvecklas för webbläsare. Bestämmelserna formuleras på ett teknikneutralt sätt, så att även andra verktyg, t.ex. agentisk AI, kan hjälpa användarna att göra samtyckesval, såvida de är anpassade för att säkerställa att kraven i den allmänna dataskyddsförordningen efterlevs. Med tanke på vikten av intäkter från nätet för den oberoende journalistiken, som är en oumbärlig pelare i ett demokratiskt samhälle, bör leverantörer av medietjänster enligt definitionen i förordning (EU) 2024/1083 (den europeiska mediefrihetsförordningen) inte vara skyldiga att respektera dessa signaler, så att de kan samverka direkt med användarna när de informerar dem och gör det möjligt för dem att göra sina samtyckesval.

De ändringar som läggs fram i den här förordningen kommer att leda till införandet av **en gemensam kontaktpunkt genom vilken de olika enheterna samtidigt kan fullgöra sina skyldigheter att rapportera incidenter inom ramen för flera rättsakter**. Genom att främja principen att ”rapportera en gång och dela många gånger” kommer den gemensamma kontaktpunkten att minska den administrativa bördan för enheterna och samtidigt säkerställa ett effektivt och säkert flöde av information om säkerhetsincidenter till de mottagare som fastställs i respektive lagstiftning.

I förslaget fastställs att Enisa ska utveckla den gemensamma kontaktpunkten, med beaktande av den gemensamma rapporteringsplattformen för anmälningar om aktivt utnyttjade sårbarheter och allvarliga incidenter enligt förordning (EU) 2024/2847 (cyberresiliensförordningen). Genom ändringen föreskrivs särskilda krav för verktyget, som en säker kanal för information som rapporteras av enheterna och skickas vidare till de behöriga myndigheterna. De underliggande rättsliga kraven för rapportering av incidenter är oförändrade, men arbetsflödet och de resurser som krävs från enheterna optimeras avsevärt.

I förslaget föreskrivs även att en gemensam kontaktpunkt ska användas för en rad nära sammankopplade skyldigheter för rapportering av incidenter som fastställs i direktiv (EU) 2022/2555 (NIS2-direktivet), förordning (EU) 2016/679 (dataskyddsförordningen), förordning (EU) 2022/2554 (DORA-förordningen), förordning (EU) 910/2014 (eIDA-förordningen) samt direktiv (EU) 2022/2557 (CER-direktivet). Andra sektorsövergripande rapporteringsskyldigheter, vilka fastställs inom ramen för nätföreskrifterna avseende cybersäkerhetsaspekter av gränsöverskridande elflöden (NCCS) och de relevanta instrumenten för luftfartssektorn, kommer också att tas upp i den gemensamma kontaktpunkten genom ändringar av de respektive delegerade akter och genomförandeakter som fastställer rapporteringsskyldigheterna enligt dessa ramar.

Förslaget syftar även till att effektivisera innehållet i den rapporterade informationen genom att införa befogenheter för flera rättsakter, om sådana inte finns. I förslaget klargörs att kommissionen vid utarbetandet av gemensamma rapporteringsmallar för direktiv (EU) 2022/2555, direktiv (EU) 2022/2557 eller förordning (EU) 2016/679 bör ta vederbörlig hänsyn till de erfarenheter som gjorts och de gemensamma mallar som utarbetats enligt förordning (EU) 2022/2554 (DORA-förordningen) för att säkerställa enhetlighet, främja synergier och minska den administrativa bördan för enheterna genom att minimera antalet datafält som ska fyllas i.

Utöver dessa grundläggande ändringar upphävs även Europaparlamentets och rådets förordning (EU) 2019/1150 av den 20 juni 2019 om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster (förordningen om förbindelserna mellan plattformar och företag eller P2B-förordningen). Förordningen har varit tillämplig sedan den 12 juli 2020 och var det första steget mot att tillhandahålla en övergripande rättslig ram för plattformsekonomin. Sedan den trädde i kraft har andra EU-rättsakter införts för att reglera onlinebaserade förmedlingstjänster och onlineplattformar. Dessa omfattar förordning (EU) 2022/1925 (förordningen om digitala marknader) och förordning (EU) 2022/2065 (förordningen om digitala tjänster), vilka i stor utsträckning ersätter bestämmelserna i P2B-förordningen. Vissa bestämmelser i P2B-förordningen kommer att finnas kvar för att säkerställa rättssäkerheten för rättsakter som innehåller korshänvisningar till dessa bestämmelser, däribland direktiv (EU) 2024/2831 om förbättring av arbetsvillkoren för plattformsarbete. Generellt sett kommer förenklingen av regelverket för onlineplattformar att minska efterlevnadskostnaderna på grund av dubbla och överlappande regler, vilket har efterfrågats av berörda parter. Leverantörer av onlinebaserade förmedlingstjänster kommer att gynnas av en ökad tydlighet i de rättsliga bestämmelserna. Verkställigheten kommer att bli mer målinriktad.

- **Förenlighet med befintliga bestämmelser inom området**

Förslaget åtföljs av ett andra förslag om ändring av förordning (EU) 2024/1689 (förordningen om artificiell intelligens). Dessa förslag utgör tillsammans ett ”digitalt omnibuspaket” och är det första steget mot att förenkla det digitala regelverket. Utöver det digitala omnibuspaketet kommer förslaget till översyn av förordning (EU) 2019/881 (cybersäkerhetsförordningen) bland annat att omfatta det uppdaterade mandatet för Europeiska unionens cybersäkerhetsbyrå (Enisa) samt åtgärder för att förenkla efterlevnaden av cybersäkerhetskraven.

Det digitala omnibuspaketet ingår i en bredare strategi för förenkling av lagstiftningen som tillkännagavs genom det digitala paketet, vilket beskrivs mer ingående i inledningen till denna motivering.

- **Förenlighet med unionens politik inom andra områden**

Förslaget är en del av kommissionens agenda för förenkling av EU:s regelverk. Variationen bland de rättsakter som omfattas av ändringarna visar att det finns goda möjligheter till förenkling genom att effektivisera samspelet mellan olika regler, däribland när de hänför sig olika politikområden. Detta är till exempel fallet för den digitala förenklingslösning som tagits fram inom ramen för den gemensamma kontaktpunkten för incidentrapportering, vilken inte berör de underliggande regleringsskyldigheterna, utan sammanför cybersäkerhetsregler som gäller för väsentliga entiteter, regler som är tillämpliga på finanssektorn, dataskyddsregler m.m. i samma gränssnitt.

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

• Rättslig grund

Förslaget grundar sig på artiklarna 114 och 16 i fördraget om Europeiska unionens funktionssätt, vilket utgör den rättsliga grunden för de ändrade rättsakterna. Den tillämpliga rättsliga grunden för bestämmelserna om ändring av förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) och förordning (EU) 2018/1725 är artikel 16 i fördraget. Eftersom alla andra ändrade rättsakter grundar sig på artikel 114 i fördraget, är samma rättsliga grund även tillämplig på motsvarande ändringsbestämmelser i den här förordningen.

• Subsidiaritetsprincipen (för icke-exklusiv befogenhet)

Eftersom de ändrade reglerna är unionsregler, kan de endast ändras på unionsnivå. De tekniska anpassningar som beskrivs i den här förordningen bevarar den subsidiaritetsprincip som ligger till grund för de ändrade rättsakterna.

När det gäller förordning (EU) 2023/2854 (dataförordningen) förstärker ändringarna förordningens mål att undanröja hinder på den inre marknaden för den datadrivna ekonomin. De bidrar till detta genom att lägga till befintliga regler i förordningen. Syftet med de riktade ändringarna av dessa regler är att förenkla, skapa klarhet och minska den administrativa bördan för både den privata sektorn och de nationella myndigheterna. De påverkar inte medlemsstaternas eller EU-institutionernas behörighet.

Detta gäller även upphävandet av direktiv (EU) 2019/1024 (direktivet om öppna data), eftersom dess materiella regler överförs till förordning (EU) 2023/2854 (dataförordningen) utan att medlemsstaternas befogenheter ändras väsentligt. En stor del av uppgifterna från den offentliga sektorn omfattas redan i dag av den direkt tillämpliga genomförandeförordningen (EU) 2023/138 om värdefulla dataset[12]. Omvandlingen till en förordning kommer att underlätta en enhetlig tillämpning av de föreslagna ändringarna i alla medlemsstater. Den kommer särskilt att stödja offentliga förvaltningar som innehar uppgifter från den offentliga sektorn, men även vidareutnyttjare av sådana uppgifter, genom att effektivisera förfarandena och minska den administrativa bördan i samband med tolkning och genomförande av olika nationella lagar. Verkställigheten av de direkt tillämpliga reglerna kommer sannolikt att bli mer konsekvent. Förslaget ändrar inte de nationella systemen för tillgång till data, utan syftar till att ge tillräcklig flexibilitet för nationella lösningar – en förmånsrätt som medlemsstaterna betonar.

När det gäller förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) och förordning (EU) 2018/1725 syftar de föreslagna ändringarna till att skapa klarhet och förutsägbarhet vid tillämpningen av de befintliga reglerna och att om möjligt minska den administrativa bördan utan att undergräva den höga dataskyddsnivån enligt förordning (EU) 2016/679 (dataskyddsförordningen) och förordning (EU) 2018/1725. Likaså förblir medlemsstaternas, EU-organens och EU-institutionernas behörighet oförändrad.

---

[12] Genomförandeförordning (EU) 2013/138.

Med införandet av en gemensam kontaktpunkt för incidentrapportering föreslås en EU-omfattande lösning för att tillhandahålla en gemensam kanal där företag kan fullgöra flera rättsliga skyldigheter genom att väsentligen rapportera samma incident. Lösningen ändrar inte på något sätt de nationella myndigheternas rättigheter och behörigheter att ta emot sådana rapporter. I stället uppmuntras rapporteringen genom tillhandahållandet av en gemensam kontaktpunkt i ett användarvänligt gränssnitt där inlämningen av en enda rapport samtidigt svarar mot flera rättsliga skyldigheter. Eftersom många av de berörda tjänsterna tillhandahålls över gränserna, och eftersom tjänsteleverantörerna är verksamma i flera av medlemsstaterna, är en europeisk lösning nödvändig.

- **Proportionalitetsprincipen**

Förslaget omfattar tekniska ändringar som är nödvändiga för att uppnå målen att minska den administrativa bördan och skapa klarhet i lagstiftningen, samtidigt som de underliggande målen i den ändrade lagstiftningen bevaras och optimeras. Ändringarna är proportionerliga, eftersom de endast medför försumbara, eller obefintliga, övergångs- och anpassningskostnader för företag och myndigheter, samtidigt som de möjliggör höga kostnadsbesparingar under de kommande åren.

Flera av de ändringar som läggs fram i den här förordningen syftar till att uppnå förenklingsmålet genom att i första hand skapa rättssäkerhet och klargöra tillämpningen av reglerna – till exempel när det gäller förtydliganden om skydd för företagshemligheter för uppgiftsinnehavare i förordning (EU) 2023/2854 (dataförordningen), förtydliganden om träning av AI-modeller och AI-system som omfattar personuppgifter som regleras av förordning (EU) 2016/679 (den allmänna dataskyddsförordningen), eller begreppet *personuppgifter* i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) och förordning (EU) 2018/1725. Vissa av bestämmelserna syftar till att kodifiera tolkningar av Europeiska unionens domstol, t.ex. när det gäller den pseudonymisering av personuppgifter som klargörs ytterligare i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen). De innehåller därför mycket riktade ändringar av reglerna, samtidigt som en stor inverkan förväntas på rättssäkerheten för företag och investerare.

De ändringar som föreslås i den här förordningen syftar även till att minska de direkta kostnaderna för företag och myndigheter, eftersom de säkerställer att samma regleringsmål kan uppnås med lägre bördor och att reglerna är proportionerliga. Till exempel omvandlas den obligatoriska ordning för dataförmedlingstjänster som föreskrivs i förordning (EU) 2022/868 (dataförvaltningsakten) till en frivillig, förtroendebaserad ordning i förordning (EU) 2023/2854 (dataförordningen).

Utvidgningen av vissa bestämmelser som är tillämpliga på små och medelstora företag till att även omfatta små midcapföretag är en riktad förenklingsåtgärd som medför minimala ändringar av omfattningen av dessa skyldigheter, samtidigt som den ger rättssäkerhet till ett större antal företag med stor potential att bidra till EU:s konkurrenskraft. Förslagen är begränsade till de ändringar som är nödvändiga för att säkerställa att små midcapföretag drar nytta av samma rättsliga ram som små och medelstora företag.

Den gemensamma kontaktpunkten för incidentrapportering och underrättelser om uppgiftsincidenter medför höga kostnadsbesparingar för företagen, samtidigt som det generella problemet med bristande rapportering undanröjs. Detta är inte bara en proportionerlig lösning, utan även en viktig förenklingslösning som genom ett digitalt verktyg ökar effektiviteten i de rapporteringsskyldigheter som omfattas av kontaktpunkten.

Upphävandet av förordning (EU) 2019/1150 (P2B-förordningen) är nödvändigt för att undvika att reglerna överlappar. Förordningen har endast ett restvärde, och mot bakgrund av den proportionerliga strategin för regleringen av onlineplattformar är det nödvändigt att undanröja dubbla skyldigheter.

- **Val av instrument**

Ändringarna föreslås genom en förordning, med tanke på de ändrade reglernas karaktär. Om direktiv ändras riktas bestämmelserna till europeiska organ, såvida de inte utgör riktade ändringar för att utarbeta bestämmelser som senare ska vidareutvecklas i förordningar.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

- **Efterhandsutvärderingar/kontroller av ändamålsenligheten med befintlig lagstiftning**

Merparten av den lagstiftning som behandlas i detta förslag är relativt ny, under förutsättning att resultaten har utvärderats kontinuerligt. Viktiga iakttagelser sammanfattas i det åtföljande arbetsdokumentet från kommissionens avdelningar.

Ett undantag från detta är den preliminära översynen 2023 av förordning (EU) 2019/1150 (förordningen om förbindelserna mellan plattformar och företag eller P2B-förordningen[13]). I rapporten konstaterades till exempel inledande positiva effekter i fråga om avtalsmässig transparens för företagsanvändare och korrekta förfaranden vid hantering av klagomål. Rapporten visade emellertid även att företagsanvändare och leverantörer av onlinebaserade förmedlingstjänster och sökmotorer inte kände till sina respektive rättigheter och skyldigheter enligt förordning (EU) 2019/1150 (P2B-förordningen). Detta kunde även kopplas till en bristande efterlevnad av förordning (EU) 2019/1150 (P2B-förordningen), vilket ledde till brister i genomförandet. Ett mycket begränsat antal klagomål togs emot inom ramen för förordning (EU) 2019/1150 (P2B-förordningen) fram till 2023. I rapporten drogs slutsatsen att den fulla potentialen hos förordning (EU) 2019/1150 (P2B-förordningen) inte hade uppnåtts vid den aktuella tidpunkten. Sedan dess har förordning (EU) 2022/2065 (förordningen om digitala tjänster) och förordning (EU) 2022/1925 (förordningen om digitala marknader) börjat tillämpas fullt ut och i stor utsträckning ersatt bestämmelserna i förordning (EU) 2019/1150 (P2B-förordningen).

- **Samråd med berörda parter**

Flera samråd genomfördes i samband med utarbetandet av förslaget. Varje samråd sågs som ett komplement till de andra och berörde antingen olika aktuella aspekter eller olika intressentgrupper.

---

[13] Arbetsdokument från kommissionens avdelningar, rapport från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén om den första preliminära översynen av genomförandet av förordning (EU) 2019/1150 om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster {SWD(2023) 300 final}.

Tre offentliga samråd och inbjudningar att lämna synpunkter om huvudpelarna i förslaget offentliggjordes under våren 2025. Ett samråd genomfördes om strategin för AI-tillämpningar från den 9 april till den 4 juni[14], ett annat om översynen av förordning (EU) 2019/881 (cybersäkerhetsförordningen) från den 11 april till den 20 juni[15] och ett tredje om strategin för en europeisk dataunion från den 23 maj till den 20 juli[16]. Varje frågeformulär hade ett särskilt avsnitt (eller ibland flera) om frågor kring genomförande och förenkling, som var direkt kopplat till reflexionerna kring det digitala omnibuspaketet. Allt som allt togs 718 unika svar emot inom ramen för detta första samråd.

En inbjudan att lämna synpunkter på det digitala omnibuspaketet offentliggjordes från den 16 september till den 14 oktober 2025[17]. Syftet var att ge berörda parter möjlighet att kommentera ett konsoliderat förslag om tillämpningsområdet för det digitala omnibuspaketet. Sammantaget inkom 513 svar från olika intressentgrupper, framför allt företag och näringslivsorganisationer, civilsamhället, den akademiska världen, myndigheter samt enskilda bidrag från medborgare.

Verkställande vice ordförande Henna Virkkunen stod värd för två genomförandedialoger om de huvudfrågor som behandlas i det digitala omnibuspaketet: den första om datapolitik[18] (1 juli 2025) och den andra om cybersäkerhetspolitik[19] (15 september).

Kommissionsledamot McGrath stod värd för en genomförandedialog om tillämpningen av den allmänna dataskyddsförordningen (16 juli 2025).

Kommissionens avdelningar genomförde även flera ”lägeskontroller” – djupgående fokusgrupper med företag och företrädare för det civila samhället som anordnades mellan den 15 september och den 6 oktober 2025 för att diskutera de praktiska utmaningarna med genomförandet och uppskatta efterlevnadskostnaderna.

För att genomföra ett särskilt samråd med små och medelstora företag och inhämta deras synpunkter anordnades en särskild panel för små och medelstora företag via Enterprise Europe Network (EEN)[20] mellan den 4 september och den 16 oktober 2025.

Slutligen kan nämnas att kommissionens avdelningar tog emot ett antal ståndpunktsdokument och stod värd för bilaterala möten med en rad olika intressenter. Kommissionens avdelningar

---

[14] Europeiska kommissionen (2025), *Inbjudan att lämna synpunkter på strategin för AI-tillämpningar*. Tillgänglig på: Strategi för AI-tillämpningar – för en starkare AI-kontinent.

[15] Europeiska kommissionen (2025), *Inbjudan att lämna synpunkter på översynen av cybersäkerhetsförordningen*. Tillgänglig på: EU:s cybersäkerhetsförordning.

[16] Europeiska kommissionen (2025), *Inbjudan att lämna synpunkter på strategin för en europeisk dataunion*. Tillgänglig på: Strategi för en europeisk dataunion.

[17] Europeiska kommissionen (2025), *Inbjudan att lämna synpunkter på det digitala omnibuspaketet*. Tillgänglig på: Förenklad datalagstiftning.

[18] Europeiska kommissionen (2025), *Implementation dialogue – data policy*. Tillgänglig på: Implementation dialogue – data policy – Europeiska kommissionen.

[19] Europeiska kommissionen (2025), *Implementation dialogue on cybersecurity policy with Executive Vice-President Henna Virkkunen*. Tillgänglig på: Implementation dialogue on cybersecurity policy with Executive Vice-President Henna Virkkunen – Europeiska kommissionen.

[20] EEN är världens största stödnätverk för små och medelstora företag. Det genomförs av Genomförandeorganet för Europeiska innovationsrådet samt för små och medelstora företag (Eismea), som inrättats av Europeiska kommissionen.

samarbetade även med medlemsstaterna i samband med rundabordssamtal eller inom ramen för rådets arbetsgrupper.

De flesta av synpunkterna från de berörda parterna gällde behovet av en förenklad tillämpning av vissa av de digitala reglerna. De berörda parterna välkomnade en inriktning mot samstämmighet och konsolidering av reglerna och ett fokus på att optimera efterlevnadskostnaderna.

Det fanns ett tydligt önskemål om att effektivisera dataregelverket och konsolidera reglerna. Detta behandlas i förslaget tillsammans med riktade ändringar som stöds av berörda parter, bland annat när det gäller den allmänna dataskyddsförordningen och den trötthet som meddelandena om kakor orsakar. Dessutom har företag lyft fram ytterligare bedömningar av samspelet mellan datareglerna som motiverar en djupare analys genom verktygen för bättre lagstiftning, särskilt den kommande kontrollen av digital ändamålsenlighet.

Företag inom olika sektorer har även pekat på de omotiverade bördor som följer av den dubbla rapporteringen av incidenter inom flera rättsliga ramar. Denna uppmaning till åtgärder hanteras genom förslaget om en gemensam kontaktpunkt för incidentrapportering.

När det gäller rättsakten om artificiell intelligens har berörda parter pekat på behovet av rättssäkerhet vid tillämpningen av reglerna, och särskilt betonat behovet av tillgängliga standarder och riktlinjer innan reglerna tillämpas. Dessa farhågor behandlas i det separata lagstiftningsförslaget inom ramen för det digitala omnibuspaketet.

Slutligen har de berörda parterna inte uttalat sig om effekterna av förordningen om förbindelserna mellan plattformar och företag, vilket bekräftar resultaten av den preliminära utvärderingsrapporten att reglerna varken är välkända eller ändamålsenliga när det gäller att uppnå deras mål. I den här förordningen föreslås att reglerna för förbindelser mellan plattformar och företag ska upphävas, särskilt mot bakgrund av överlappning med nyare regler.

En detaljerad översikt över dessa samråd med berörda parter och hur de återspeglades i förslaget finns i det arbetsdokument från kommissionens avdelningar som åtföljer det digitala omnibuspaketet.

- **Insamling och användning av sakkunnigutlåtanden**

Utöver de samråd som beskrivs ovan förlitade sig kommissionen främst på intern analys av detta förslag. Två studier gjordes också till stöd för analysen av kapitlen om data i förslaget. Den första studien var inriktad på genomförandet av förordning (EU) 2018/1807 (förordningen om det fria flödet av andra data än personuppgifter), direktiv (EU) 2019/1024 (direktivet om öppna data) och förordning (EU) 2022/868 (dataförvaltningsakten). Den andra studien var närmare kopplad till meddelandet om strategin om en dataunion (som antogs som en del av samma förenklingspaket vid sidan av det digitala omnibuspaketet) och fokuserade på utvecklingen av datapolitiken med koppling till generativ AI, regelefterlevnad och internationella dimensioner. Båda undersökningarna håller på att slutföras och kommer att offentliggöras i ett senare skede.

Kommissionens avdelningar har även genomfört en studie om samspelet mellan förordning (EU) 2022/2065 (förordningen om digitala tjänster) och andra lagstiftningsakter, däribland förordning (EU) 2019/1150 (P2B-förordningen). Som en del av det digitala paketet offentliggör kommissionen en rapport som beskriver samspelet mellan förordning (EU) 2022/2065 (förordningen om digitala tjänster) och andra närstående regler, i enlighet med kravet i artikel 91 i förordning (EU) 2022/2065 (förordningen om digitala tjänster).

- **Konsekvensbedömning**

De ändringar som föreslås i den här förordningen är riktade och tekniska till sin karaktär. De är utformade för att säkerställa ett effektivare genomförande av reglerna. De medför inte flera olika politiska alternativ som skulle kunna testas och jämföras på ett meningsfullt sätt, och de underbyggs inte, i linje med riktlinjerna för bättre lagstiftning, av en fullständig konsekvensbedömningsrapport.

Det bifogade arbetsdokumentet från kommissionens avdelningar går djupare in i interventionslogiken för ändringarna, de berörda parternas åsikter om de olika åtgärderna och kostnads-nyttoanalysen av förslagen, inbegripet de kostnadsbesparingar som genereras och andra typer av effekter. I många fall bygger det på de respektive konsekvensbedömningar som ursprungligen gjordes av de olika rättsakterna.

- **Lagstiftningens ändamålsenlighet och förenkling**

Den föreslagna förordningen innebär en mycket kraftig minskning av bördorna för företag, offentliga förvaltningar och medborgare. De inledande beräkningarna pekar på möjliga besparingar på minst 1 miljard euro om året från och med ikraftträdandet, med ytterligare besparingar på 1 miljard euro i engångskostnader, vilket motsvarar minst 5 miljarder euro under de tre åren fram till 2029. Betydande icke-kvantifierbara fördelar förväntas också, framför allt tack vare en effektivare uppsättning av regler som kommer att underlätta införandet och efterlevnaden. I beräkningarna ingår inte heller de affärsmöjligheter som skapas genom den föreslagna regleringsstrategin.

Små och medelstora företag omfattas redan av undantag från flera bestämmelser i de rättsakter som ändras genom det digitala omnibuspaketet, men ytterligare stödåtgärder läggs fram när det gäller byte av moln. I kapitlet om harmoniserade regler för datadelning utvidgas vissa undantag som redan beviljas små och medelstora företag till att även omfatta små midcapföretag.

Förslaget är även helt förenligt med kommissionens ”digitala kontroll”, som syftar till att säkerställa en lämplig anpassning av politiska förslag till digitala miljöer. Mer information om detta finns i kapitel 4 i den bifogade finansierings- och digitaliseringsöversikten.

- **Grundläggande rättigheter**

De föreslagna ändringarna stöder företagens innovationsmöjligheter på den inre marknaden och främjar därmed rätten att bedriva verksamhet i unionen.

Vissa av bestämmelserna gäller även skydd och främjande av andra grundläggande rättigheter, särskilt rätten till integritet och skydd av personuppgifter, och har anpassats för att bevara högsta möjliga skyddsnivå och för att hjälpa enskilda att utöva sina rättigheter på ett effektivt sätt, samtidigt som kostnaderna optimeras och fler innovationsmöjligheter skapas. På så sätt följer förslaget strikt proportionalitetsprincipen i artikel 52 i stadgan.

I det specifika fallet med de riktade ändringarna av förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) och förordning (EU) 2018/1725 skulle de föreslagna ändringarna förenkla kraven för behandling med låg risk, harmonisera vissa standarder och klargöra vissa centrala begrepp i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) och förordning (EU) 2018/1725, och därmed göra det möjligt för personuppgiftsansvariga att genomföra effektivare dataskyddsstrategier. Detta skulle göra det möjligt för dem att rikta

sina resurser till mer dataintensiva och riskfyllda verksamheter där åtgärderna för att skydda personuppgifter är mest kritiska.

När det gäller integriteten i samband med kommunikation har förslaget kvar den högsta skyddsnivån, inklusive samtyckesbaserad tillgång till terminalutrustning. Ändringen av direktiv (EU) 2002/58/EG (direktivet om integritet och elektronisk kommunikation) ändrar inte det materiella skyddet. Genom ändringen anpassas reglerna för behandling av personuppgifter på och från terminalutrustning till reglerna i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen). Reglerna om terminalutrustningens integritet inom ramen för direktivet upprätthålls när andra data än personuppgifter behandlas.

4. BUDGETKONSEKVENSER

Budgetkonsekvenserna av att Europeiska unionens cybersäkerhetsbyrå (Enisa) inrättar och upprätthåller en gemensam kontaktpunkt för incidentrapportering beskrivs närmare i översynen av förordning (EU) 2019/881 (cybersäkerhetsförordningen), som en del av Enisas resurser.

5. ÖVRIGA INSLAG

- **Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering**

Ej tillämpligt

- **Ingående redogörelse för de specifika bestämmelserna i förslaget**

Ändringar av förordning (EU) 2023/2854 – dataförordningen

Ändringarna av den rättsliga ramen för data innebär att bestämmelserna i förordning (EU) 2018/1807 (förordningen om det fria flödet av uppgifter), förordning (EU) 2022/868 (dataförvaltningsakten) och direktiv (EU) 2019/1024 (direktivet om öppna data) konsolideras i förordning (EU) 2023/2854 (dataförordningen) på ett genomgripande och effektivt sätt. Kapitel I innehåller även riktade ändringar för att anpassa de nuvarande reglerna i förordning (EU) 2023/2854 (dataförordningen).

Artikel 1 omfattar ändringar av förordning (EU) 2023/2854 (dataförordningen) om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828.

Följande ändringar föreslås i artikel 1:

I punkt 1 uppdateras tillämpningsområdet för förordning (EU) 2023/2854 (dataförordningen), i vilken nya kapitel kommer att införas enligt förklaringen nedan.

I punkt 2 ändras vissa definitioner samtidigt som nya införs.

I punkt 3 skapas en ny regel enligt artikel 4.8 i förordning (EU) 2023/2854 (dataförordningen) som gör det möjligt för uppgiftsinnehavare att vägra att röja företagshemligheter för en användare om det finns en hög risk för att de olagligen anskaffas, används eller lämnas ut till tredjeländer, eller enheter som står under deras kontroll, som omfattas av jurisdiktioner med svagare skydd än i unionen.

I punkt 5 införs samma regel för artikel 5.11 i förordning (EU) 2023/2854 (dataförordningen), beträffande datahållare som röjer företagshemligheter för tredje part.

I punkterna 5–19 begränsas tillämpningsområdet för kapitel V från ”exceptionella behov” till ”allmänna nödlägen”. Genom ändringarna stryks artiklarna 14 och 15, samtidigt som en ny artikel 15a skapas som den enda artikeln för begäranden i allmänna nödlägen enligt ordningen för datadelning från företag till myndigheter i förordning (EU) 2023/2854 (dataförordningen). Begärandena kan göras när det är nödvändigt för att hantera ett allmänt nödläge (artikel 15a.2) eller för att mildra eller stödja återhämtningen från ett allmänt nödläge (artikel 15a.3). Korshänvisningarna justeras i enlighet med detta, medan språket förenklas och förtydligas. Genom artikel 1.21 skapas en ny artikel 22a som utgör ramen för ordningen för klagomål enligt kapitel V och sammanför tidigare upprepade bestämmelser.

Punkterna 20–22 omfattar vissa undantag från kapitel VI i förordning (EU) 2023/2854 (dataförordningen) (byte av databehandlingstjänster): I artikel 31 införs en enklare specifik ordning för databehandlingstjänster som är skräddarsydda, dvs. databehandlingstjänster som inte är standardtjänster och som inte skulle fungera utan föregående anpassning till användarens behov och ekosystem, om dessa tillhandahålls på grundval av avtal som ingåtts före den 12 september 2025. Likaså införs i artikel 31 en ny och enklare specifik ordning för databehandlingstjänster som tillhandahålls av små och medelstora företag och små midcapföretag på grundval av avtal som ingåtts före den 12 september 2025, med ett förtydligande om att dessa leverantörer kan föra in straffavgifter för förtida uppsägning i tidsbegränsade avtal.

Punkterna 23–25 omfattar ändringar av artikel 32 i förordning (EU) 2023/2854 (dataförordningen) till följd av integreringen av organ som för närvarande omfattas av förordning (EU) 2022/868 (dataförvaltningsakten) i förordning (EU) 2023/2854 (dataförordningen).

I punkt 26 upphävs skyldigheterna för leverantörer av smarta kontrakt att uppfylla väsentliga krav, och kommissionen ges befogenhet att anta harmoniserade standarder.

I punkt 27 integreras två rättsordningar som för närvarande ingår i förordning (EU) 2022/868 (dataförvaltningsakten), en förordning som kommer att upphävas när omnibuspaketet träder i kraft. Denna punkt reformerar de nuvarande reglerna i kapitlen III och IV i dataförvaltningsakten, vilka föreskriver en obligatorisk anmälningsordning för leverantörer av dataförmedlingstjänster och en frivillig registreringsordning för dataaltruismorganisationer. De två ordningarna ska införas som ett nytt kapitel VIIa i förordning (EU) 2023/2854 (dataförordningen). Mot bakgrund av den framväxande karaktären hos marknaden för dataförmedlingstjänster ska skyldigheterna enligt förordning (EU) 2022/868 (dataförvaltningsakten) göras mer flexibla för att denna marknad ska kunna växa. För det första ska ordningen för leverantörer av dataförmedlingstjänster göras om till ett frivilligt system. För det andra kommer den mest kritiska skyldigheten, dvs. skyldigheten att hålla dataförmedlingstjänster juridiskt åtskilda från alla andra tjänster som ett företag kan vilja erbjuda, att ersättas med en skyldighet att hålla tjänsterna funktionellt åtskilda baserat på en ytterligare uppsättning villkor. Slutligen ska förteckningen över skyldigheter kortas ner drastiskt. När det gäller dataaltruism upphävs såväl rapporterings- och transparenskraven för dataaltruismorganisationer som idén att komplettera reglerna i förordning (EU) 2022/868 (dataförvaltningsakten) i ett ”dataaltruismregelverk” med ännu mer detaljerade regler.

Genom ändringen införs ett nytt kapitel som kapitel VIIb, enligt vilket förbudet mot lokaliseringskrav för andra data än personuppgifter inom unionen, vilket tidigare ingick i den upphävda förordningen (EU) 2018/1807 (förordningen om det fria flödet av andra data än personuppgifter), ska införas i förordning (EU) 2023/2854 (dataförordningen). Skyldigheten att underrätta kommissionen bibehålls, men samtidigt avskaffas den nationella informationspunkten online där medlemsstaterna skulle offentliggöra tillämpliga datalokaliseringskrav.

Genom punkterna 4 och 33–58 införs de sammanslagna bestämmelserna om vidareutnyttjande av data och handlingar som innehas av offentliga organ enligt kapitel II i förordning (EU) 2022/868 (dataförvaltningsakten) och direktiv (EU) 2019/1024 (direktivet om öppna data).

- Genom punkt 4 förs definitioner från de införda bestämmelserna över till förordning (EU) 2023/2854 (dataförordningen) för att harmonisera definitionen av data och handlingar genom en strikt avgränsning mellan digitalt (data) och icke-digitalt (handlingar) innehåll.
- Genom ändringen införs ett nytt kapitel som kapitel VIIc om vidareutnyttjande av data och handlingar som innehas av offentliga organ.
- Genom ändringen införs ett nytt avsnitt som avsnitt 1, där de allmänna principer som är tillämpliga på det nyligen införda kapitlet beskrivs.
- Genom ändringen införs ämnet och tillämpningsområdet för det sammanslagna kapitlet, där de gemensamma reglerna i kapitel II i förordning (EU) 2022/868 (dataförvaltningsakten) och direktiv (EU) 2019/1024 (direktivet om öppna data) kombineras.
- Genom ändringen fastställs den gemensamma principen om icke-diskriminering vid delning av öppna offentliga data och vissa kategorier av skyddade data.
- Genom ändringen fastställs ett förbud mot exklusiva avtal som är gemensamt för ordningen med öppna offentliga data och vissa kategorier av skyddade data.
- Genom ändringen fastställs allmänna principer för uttag av avgifter för vidareutnyttjande av öppna offentliga data eller vissa kategorier av skyddade data. En ny regel är att offentliga organ kommer att behöva säkerställa att alla avgifter även kan betalas online genom allmänt tillgängliga gränsöverskridande betaltjänster, utan diskriminering för vidareutnyttjande av öppna offentliga data. Detta är en utvidgning av den regel som tidigare endast tillämpades på vidareutnyttjande av vissa kategorier av skyddade data enligt kapitel II i förordning (EU) 2022/868 (dataförvaltningsakten).
- Genom ändringen föreskrivs att vidareutnyttjare av öppna offentliga data och vissa kategorier av skyddade data ska ha rätt att få information om tillgängliga möjligheter till prövning i samband med beslut eller förfaranden som påverkar dem.
- Genom ändringen införs avsnittet om regler för vidareutnyttjande av öppna offentliga data, vilket tidigare ingick i direktiv (EU) 2019/1024 (direktivet om öppna data).
- Genom ändringen fastställs avsnittets tillämpningsområde, däribland att det inte är tillämpligt på vissa kategorier av skyddade data som omfattas av det allmänna kapitlet om vidareutnyttjande av data och handlingar som innehas av offentliga organ.

- Genom ändringen fastställs den allmänna principen för vidareutnyttjande av öppna offentliga data.
- Genom ändringen fastställs reglerna för behandling av begäranden om vidareutnyttjande av öppna offentliga data genom införandet av den tidigare bestämmelsen i direktiv (EU) 2019/1024 (direktivet om öppna data).
- Genom ändringen införs reglerna om tillgängliga format för vidareutnyttjande av öppna offentliga data, vilka tidigare ingick i direktiv (EU) 2019/1024 (direktivet om öppna data).
- Genom ändringen införs reglerna om uttag av avgifter för öppna offentliga data, vilka tidigare reglerades genom direktiv (EU) 2019/1024 (direktivet om öppna data). En ny regel är att offentliga organ kan ta ut högre avgifter av mycket stora företag som vidareutnyttjar data. Dessa avgifter ska vara proportionerliga, och deras belopp ska baseras på objektiva kriterier.
- Genom ändringen införs reglerna om standardiserade licenser för vidareutnyttjande av öppna offentliga data, vilka tidigare ingick i direktiv (EU) 2019/1024 (direktivet om öppna data). En ny regel är att offentliga organ kan föreskriva särskilda villkor för mycket stora företag. Dessa villkor ska vara proportionerliga och vara grundade på objektiva kriterier.
- Genom ändringen införs reglerna om praktiska arrangemang som tidigare ingick i direktiv (EU) 2019/1024 (direktivet om öppna data) för att underlätta sökningen efter data eller handlingar som är tillgängliga för vidareutnyttjande i förordning (EU) 2023/2854 (dataförordningen).
- Genom ändringen införs reglerna om forskningsdata, vilka tidigare ingick i direktiv (EU) 2019/1024 (direktivet om öppna data), i förordning (EU) 2023/2854 (dataförordningen).
- Genom ändringen införs reglerna om värdefulla dataset, vilka tidigare ingick i direktiv (EU) 2019/1024 (direktivet om öppna data) i förordning (EU) 2023/2854 (dataförordningen).
- Genom ändringen inrättas ett nytt avsnitt om vidareutnyttjande av vissa kategorier av skyddade data för att inkludera de tidigare reglerna i kapitel II i förordning (EU) 2022/868 (dataförvaltningsakten) i kapitlet. I punkten beskrivs tillämpningsområdet för detta tredje avsnitt, vilket inte omfattar de data och handlingar som omfattas av avsnitt två och som styr ordningen för vidareutnyttjande av öppna offentliga data. En ny regel är att handlingar ingår i tillämpningsområdet för detta avsnitt.
- Genom ändringen fastställs den allmänna principen om vidareutnyttjande av vissa kategorier av skyddade data. Detta är den princip som fastställs i kapitel II i förordning (EU) 2022/868 (dataförvaltningsakten), dvs. avsnittet medför inte någon skyldighet för offentliga organ att tillåta vidareutnyttjande av skyddade data, utan fastställer snarare minimivillkor om offentliga organ beslutar att göra sådana data tillgängliga för vidareutnyttjande.
- Genom ändringen införs reglerna om villkoren för vidareutnyttjande av vissa kategorier av skyddade data, vilka tidigare ingick i kapitel II i förordning (EU) 2022/868 (dataförvaltningsakten), i förenklad och anpassad form. Ändringen omfattar ett förtydligande av vilka regler som är tillämpliga i fall där personuppgifter

har anonymiserats. Kraven avseende överföring av data som inte är personuppgifter till tredjeländer bevaras men delas upp i en ny artikel enligt punkt 54.

- Genom ändringen införs reglerna om uttag av avgifter, vilka tidigare ingick i kapitel II i förordning (EU) 2022/868 (dataförvaltningsakten), i förordning (EU) 2023/2854 (dataförordningen). En ny regel är att offentliga organ kan föreskriva högre avgifter för mycket stora företag som vidareutnyttjar data. Dessa avgifter ska vara proportionerliga och vara grundade på objektiva kriterier. Den särskilda prioriteringen att uppmuntra små och medelstora företag att vidareutnyttja data utvidgas till små midcapföretag.
- Genom ändringen införs reglerna om behöriga organ, vilka tidigare ingick kapitel II i förordning (EU) 2022/868 (dataförvaltningsakten), i förordning (EU) 2023/2854 (dataförordningen). Behöriga organ ska hjälpa offentliga organ att handlägga begäranden om vidareutnyttjande av data och handlingar som omfattas av avsnitt 3.
- Genom ändringen införs reglerna om den gemensamma informationspunkten, vilka tidigare ingick i kapitel II i förordning (EU) 2022/868 (dataförvaltningsakten) i förordning (EU) 2023/2854 (dataförordningen). De gemensamma informationspunkterna är utformade för att hjälpa vidareutnyttjare att enkelt hitta information om vidareutnyttjande av vissa kategorier av skyddade data.
- Genom ändringen införs reglerna om förfarandet för begäranden om vidareutnyttjande av vissa kategorier av skyddade data, vilka tidigare reglerades i kapitel II i förordning (EU) 2022/868 (dataförvaltningsakten), i förordning (EU) 2023/2854 (dataförordningen).

I punkt 57 integreras de grundläggande reglerna för Europeiska datainnovationsstyrelsen (EDIB), en grupp som ger kommissionen råd om en konsekvent tillämpning av dataförordningen och som fungerar som ett samordningsforum för beslutsfattande på området dataekonomi. Detta kommer att integrera de grundläggande reglerna i dataförordningen. Ändringarna kommer att göra det möjligt för kommissionen att ändra de relevanta grundläggande dokumenten för EDIB (kommissionens beslut av den 20 februari 2023 – C(2023)1074 final) och utvidga medlemskapet till företrädare för nationella beslutsfattare utöver behöriga myndigheter.

Punkterna 61–65 innehåller ändringar av bestämmelserna i förordning (EU) 2023/2854 (dataförordningen) om kommittéförfarandet och delegeringsbefogenheterna, och punkt 66 innehåller ändringar av förordning (EU) 2022/868 (dataförvaltningsakten) som är nödvändiga för att införa reglerna i förordning (EU) 2022/868 (dataförvaltningsakten) och direktiv (EU) 2019/1024 (direktivet om öppna data) i förordning (EU) 2023/2854 (dataförordningen).

Genom punkt 68 utvidgas den särskilda inriktningen på små och medelstora företag i samband med utvärderingen till att även omfatta små midcapföretag, och genom punkt 69 införs utvärderingen av de nyligen införda reglerna i förordning (EU) 2023/2854 (dataförordningen).

Genom artikel 2 införs de relevanta hänvisningarna till dataförmedlingstjänster och dataaltruism i punkten om att ”starta, driva och avveckla ett företag” i bilagan till förordning (EU) 2018/1724.

Ändringar av förordning (EU) 2016/679, förordning (EU) 2018/1725 och direktiv 2002/58/EG

Artikel 3 i förslaget innehåller förslag till ändringar av förordning (EU)2016/679 (den allmänna dataskyddsförordningen).

Följande ändringar föreslås i artikel 3:

I punkt 1 klargörs definitionen av personuppgifter enligt artikel 4 i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) genom att ange att information inte ska betraktas som personuppgifter för en viss enhet om den inte har de hjälpmedel som rimligen kan förväntas för att identifiera den fysiska person som informationen avser. Till följd av detta skulle ett sådant företag i princip inte omfattas av den förordningens tillämpningsområde.

I punkt 2 föreskrivs ytterligare två undantag från behandlingen av särskilda kategorier av data. Ett undantag införs från det allmänna förbudet mot behandling av biometriska uppgifter, om behandlingen är nödvändig för att bekräfta den registrerades identitet och om den registrerade har ensam kontroll över uppgifterna och medlen för kontrollen. Ett andra undantag införs för behandling av särskilda kategorier av kvarstående personuppgifter för utveckling och drift av ett AI-system eller en AI-modell, på vissa villkor, inbegripet lämpliga organisatoriska och tekniska åtgärder för att säkerställa att särskilda kategorier av personuppgifter inte samlas in och att sådana uppgifter tas bort.

I punkt 3 klargörs den situation enligt artikel 12 i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) där rätten till tillgång missbrukas av registrerade för andra ändamål än skydd av deras personuppgifter. Därmed skulle den personuppgiftsansvarige kunna vägra att tillmötesgå en begäran eller ta ut en rimlig avgift. Villkoren för att visa att en begäran om tillträde var överdriven skulle också klargöras.

Punkt 4 är inriktad på den personuppgiftsansvariges skyldighet att informera de registrerade om behandlingen av deras personuppgifter enligt artikel 13 i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) genom att upphäva denna skyldighet i situationer där det finns rimliga skäl att anta att den registrerade redan har tillgång till denna information, såvida inte den personuppgiftsansvarige överför uppgifterna till andra mottagare eller kategorier av mottagare, överför uppgifterna till ett tredjeland, utför automatiserat beslutsfattande eller om behandlingen sannolikt medför en hög risk för den registrerades rättigheter.

I punkt 5 klargörs kraven för automatiserat individuellt beslutsfattande enligt artikel 22 i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) i samband med ingående eller fullgörande av ett avtal mellan den registrerade och en personuppgiftsansvarig, särskilt att kravet på ”nödvändighet” gäller oavsett om beslutet kan fattas på annat sätt än enbart med automatiserade metoder.

Genom punkt 6 anpassas den personuppgiftsansvariges skyldighet att anmäla personuppgiftsincidenter till den behöriga tillsynsmyndigheten enligt artikel 33 i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) till dess skyldighet att underrätta registrerade om sådana incidenter genom att föreskriva att en underrättelse endast krävs om en personuppgiftsincident sannolikt kommer att leda till en hög risk för den registrerades rättigheter. Tidsfristen för anmälan förlängs också till 96 timmar. Det föreslås även att personuppgiftsansvariga ska använda den gemensamma kontaktpunkten när de anmäler uppgiftsincidenter till tillsynsmyndigheten. Dessutom skulle Europeiska dataskyddsstyrelsen vara skyldig att utarbeta ett förslag till en gemensam mall för anmälningar av personuppgiftsincidenter och överlämna förslaget till kommissionen, varefter kommissionen skulle ha befogenhet att anta mallen genom en genomförandeakt efter att vid behov ha granskat den.

Genom punkt 7 harmoniseras förteckningarna över vilka behandlingar som kräver och som inte kräver konsekvensbedömningar avseende dataskydd genom att föreskriva att en enda

förteckning över behandlingar som kräver och som inte kräver en konsekvensbedömning avseende dataskydd ska tillhandahållas på EU-nivå, vilket därmed skulle bidra till harmoniseringen av begreppet hög risk. Europeiska dataskyddsstyrelsen skulle vara skyldig att utarbeta förslag till sådana förteckningar. Den skulle även vara skyldig att utarbeta ett förslag till en gemensam mall och en gemensam metod för genomförande av konsekvensbedömningar avseende dataskydd, vilka kommissionen skulle ha befogenhet att anta genom en genomförandeakt efter att vid behov ha granskat dem.

I punkt 8 fastställs att kommissionen, tillsammans med Europeiska dataskyddsstyrelsen, kan bistå personuppgiftsansvariga i bedömningen av huruvida data som härrör från pseudonymisering inte utgör personuppgifter genom att ange vilka hjälpmedel och kriterier som är relevanta för en sådan bedömning, inbegripet den senaste tekniska utvecklingen av tillgänglig teknik och kriterier för att bedöma risken för avanonymisering.

Genom punkt 12 reformeras den rättsliga ordningen för behandling av personuppgifter på eller från terminalutrustning (”anslutna enheter”), vilken för närvarande ingår i direktiv 2002/58/EG (direktivet om integritet och elektronisk kommunikation). En ny artikel införs som artikel 88a i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) i syfte att fastställa kravet på samtycke för lagring eller tillgång till personuppgifter på fysiska personers terminalutrustning och se till behandlingen av personuppgifter på och från terminalutrustning omfattas av bestämmelserna i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen). En ny artikel införs som artikel 88b i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen), med bestämmelser om automatiserade och maskinläsbara upplysningar om individuella val och hur dessa ska uppfyllas av webbplatsleverantörer när standarder väl finns tillgängliga.

Följande ändringar föreslås i artikel 4:

Artikel 4 i förslaget syftar till att införa riktade ändringar av förordning (EU) 2018/1725 för att anpassa texten till de ändringar av förordning (EU) 2016/679 som införs i artikel 3.

Följande ändringar föreslås i artikel 5:

I artikel 5 föreskrivs ändringar av direktiv 2002/58/EG, direktivet om integritet och elektronisk kommunikation. Artikel 4 i det direktivet ska upphöra att gälla. Tillägget till artikel 5.3 i det direktivet gör det möjligt att flytta reglerna om lagring och tillgång till personuppgifter från en fysisk persons terminalutrustning till förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) genom att införa en ny artikel som artikel 88a i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) enligt beskrivningen ovan.

Den gemensamma kontaktpunkten för incidentrapportering

Följande ändringar föreslås i artikel 6:

Genom punkterna 1 och 2 inrättas en gemensam kontaktpunkt för incidentrapportering, tillsammans med särskilda krav för Enisa. Vidare fastställs att rapportering av incidenter enligt NIS2-direktivet bör ske via den nya gemensamma kontaktpunkten.

Följande ändringar föreslås i artikel 7: Den gemensamma kontaktpunkten föreskrivs även för rapportering av incidenter enligt förordning (EU) nr 910/2014 (eIDA-förordningen).

Följande ändringar föreslås i artikel 8: Den gemensamma kontaktpunkten föreskrivs även för förordning (EU) 2022/2554 (DORA-förordningen).

Följande ändringar föreslås i artikel 9: Den gemensamma kontaktpunkten föreskrivs även för direktiv (EU) 2022/2557 (CER-direktivet).

Dessutom anges i artikel 3.6 att rapporteringen av incidenter i samband med dataincidenter enligt förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) ska kunna kanaliseras via den gemensamma kontaktpunkten. I artikel 5.1 upphävs rapporteringskraven enligt direktiv 2002/58/EG (direktivet om integritet och elektronisk kommunikation), eftersom de är föråldrade mot bakgrund av bestämmelserna i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen).

Upphävande av rättsakter och slutbestämmelser

Följande ändringar föreslås i artikel 10:

Genom punkt 1 upphävs förordning (EU) 2019/1150 (P2B-förordningen), vilken anses ha förlorat det mesta av sin relevans med tanke på att de senaste reglerna i stort sett täcker samma frågor. Genom undantag gäller punkt 2 alla korshänvisningar till förordning (EU) 2019/1150 (P2B-förordningen) i andra rättsliga instrument. Dessa ska fortsätta att gälla till dess att de har ändrats i de ursprungliga rättsakterna, senast den 31 december 2032, för att undvika eventuell rättslig osäkerhet.

Genom punkt 3 upphävs de rättsakter som införlivats i förordning (EU) 2023/2854 (dataförordningen).

I **artikel 11** fastställs slutbestämmelserna i ändringsförordningen.

2025/0360 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om ändring av förordningarna (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 och direktiven 2002/58/EG, (EU) 2022/2555 och (EU) 2022/2557 vad gäller förenkling av lagstiftningsramen på det digitala området och om upphävande av förordningarna (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 och direktiv (EU) 2019/1024 (det digitala omnibuspaketet)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 16 och 114,

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[21],

med beaktande av Europeiska centralbankens yttrande[22],

med beaktande av Regionkommitténs yttrande[23],

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) I sitt meddelande om ett enklare och snabbare Europa[24] tillkännagav kommissionen sitt åtagande om ett ambitiöst program för att främja en framåtblickande och innovativ politik som stärker unionens konkurrenskraft och drastiskt minskar regelbördan för människor, företag och förvaltningar, samtidigt som den upprätthåller den högsta standarden när det gäller att främja unionens värden. Följaktligen prioriterade kommissionen förslaget om omedelbara anpassningar av lagstiftningen, inbegripet lagstiftningen på det digitala området, för att ta itu med unionens konkurrensutmaningar.

---

[21] EUT C […], […], s. […].

[22] EUT C […], […], s. […].

[23] EUT C […], […], s. […].

[24] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, *Ett enklare och snabbare Europa:* Meddelande om genomförande och förenkling, COM(2025) 47 final, 11 februari 2025.

(2) Unionens lagstiftning på det digitala området fastställer höga standarder i unionen och kan vara en kraftfull källa till konkurrensfördelar för företag som följer reglerna, och är världsledande när det gäller kvalitet, säkerhet och tillförlitlighet. Bestämmelser på det digitala området har skapat tydliga spelregler i unionen för ansvarsfulla företag genom att säkerställa rättvisa och transparens i relationerna mellan företag, stimulera innovativa affärsmodeller, sätta en hög standard för konsumentskydd och säkerhet samt skydda de grundläggande rättigheterna, inte minst när det gäller integritet och dataskydd.

(3) Unionens digitala lagstiftning har utvecklats stegvis under de senaste åren för att hantera den snabbt växande digitala teknikens avtryck i unionens ekonomi och samhällsdynamik, och för att bemöta de nya utmaningarna och främja affärsmöjligheter i EU. Trots att kommissionen har åtagit sig att göra ett systematiskt stresstest av bestämmelserna på det digitala området och av andra unionsregler, vilket kan leda till ytterligare justeringar av lagstiftningen, särskilt efter den kommande kontrollen av digital ändamålsenlighet och andra riktade utvärderingar av de digitala reglerna, krävs omedelbara lagstiftningsändringar. I den här förordningen föreslås därför en första uppsättning ändringar av lagstiftningsramen på det digitala området, med målet att omedelbart förtydliga lagstiftningen för att stimulera innovation på unionsmarknaden och minska de administrativa efterlevnadskostnaderna, särskilt för företagen, och samtidigt minska tillsynsmyndigheternas och de rådgivande organens kostnader för tillsyn och administration. Ändringarna syftar även till att skapa klarhet för enskilda personer.

(4) Med tanke på den grundläggande roll som data spelar för att skapa mervärde i den digitala ekonomin, och i enlighet med målen i meddelandet om en strategi för en europeisk dataunion, syftar de ändringar som läggs fram i den här förordningen till att skapa ett enhetligt och sammanhängande regelverk för tillgång till och användning av data genom att förenkla och konsolidera regelverket i endast två rättsakter, nämligen Europaparlamentets och rådets förordningar (EU) 2016/679[25] och (EU) 2023/2854[26], i stället för de fem olika rättsakter som för närvarande är tillämpliga. Syftet med ändringarna är att minska onödiga administrativa kostnader och stimulera tillgången till data som en förutsättning för att stödja konkurrenskraftiga digitala företag i unionen, samtidigt som den högsta standarden för skydd av integritet, personuppgifter och god affärssed upprätthålls och de grundläggande regleringsmålen uppnås, däribland efterlevnaden av europeisk och nationell konkurrenslagstiftning.

(5) Med tanke på att utvecklingen av övergripande och sektorsspecifika regler har lett till upprepningar är det även nödvändigt att ta itu med överlappningar i vissa bestämmelser som leder till onödiga fördubblingar av den administrativa bördan. Detta gäller krav i flera av reglerna för rapportering av cybersäkerhetsincidenter och

---

[25] 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).

[26] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen).

liknande incidenter, där digitala lösningar, såsom föreslås i den här förordningen, kan leda till en omedelbar lättnad för företag inom alla berörda sektorer.

(6) På grund av upprepningar i regleringen av onlineplattformar under de senaste åren har nyare regler skapat en tydligare och mer ambitiös ram än vissa av de tidigare reglerna, vilka nu har blivit föråldrade. Det är därför nödvändigt att utveckla den rättsliga ramen för att undanröja onödiga dubbleringar som bidrar till rättslig komplexitet.

(7) I Europaparlamentets och rådets förordning (EU) 2022/868[27] fastställs regler för förmedlingsfunktioner i tre olika situationer: a) funktioner som stöder vidareutnyttjande av skyddade data som innehas av offentliga myndigheter under kontrollerade förhållanden, b) dataförmedlingstjänster som underlättar datadelning mellan registrerade, datainnehavare och dataanvändare, och c) dataaltruismorganisationer som stöder användningen av data som görs tillgängliga av registrerade och datainnehavare på altruistisk eller filantropisk grund. Funktioner som stöder vidareutnyttjandet av skyddade data som innehas av offentliga organ har en nära koppling till bestämmelserna i Europaparlamentets och rådets direktiv (EU) 2019/1024[28]. Samspelet mellan dem har skapat förvirring bland offentliga organ. Det är därför nödvändigt att slå ihop de två uppsättningarna av regler. Utvärderingen av reglerna för dataförmedlingstjänster har visat att det finns svagheter i definitionen av leverantörer av dataförmedlingstjänster och att reglerna är alltför stränga för att tjänsteleverantörer ska kunna hitta en hållbar ekonomisk modell. Därför är det även nödvändigt att effektivisera ordningen. När det gäller dataaltruism verkar vissa av reglerna i förordning (EU) 2022/868, särskilt medlemsstaternas skyldighet att införa nationella strategier för dataaltruism, upprättandet av en ”regelbok” och utarbetandet av ett europeiskt formulär för samtycke till dataaltruism, vara onödiga, även mot bakgrund av Europeiska dataskyddsstyrelsens pågående arbete enligt artikel 68 i Europaparlamentets och rådets förordning (EU) 2016/679[29] om vägledning för behandling av personuppgifter inom ramen för vetenskaplig forskning.

(8) Även om vikten av dataförmedlingstjänster erkänns inom ramen för flera initiativ till stöd för datadelning och datasamarbete bör reglerna i förordning (EU) 2022/868 om leverantörer av dataförmedlingstjänster förtydligas. Framför allt bör definitionen av dessa leverantörer preciseras. Delar som bara tjänade som exempel och inte gällde som undantag bör elimineras. Dessutom bör kryphål till följd av tvetydiga formuleringar åtgärdas, särskilt när det gäller begreppet ”sluten grupp”. Tjänster bör inte kunna registreras som dataförmedlingstjänster om de uteslutande används av en sluten grupp av företag och som endast kan utvidgas efter beslut av den gruppen och inte av

---

[27] Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten) (EUT L 152, 3.6.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

[28] Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn (EUT L 172, 26.6.2019, s. 56, ELI: http://data.europa.eu/eli/dir/2019/1024/oj).

[29] 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) (EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

tjänsteleverantören. Framför allt har införandet av en obligatorisk ordning för denna framväxande marknad lett till onödiga efterlevnadskostnader. I detta skede av marknadsutvecklingen verkar en frivillig ordning som gör det möjligt för neutrala aktörer att skilja ut sig från andra aktörer vara tillräcklig. För att möjliggöra hållbara affärsmodeller bör ordningen även göras mindre strikt genom att avskaffa kravet på rättslig åtskillnad mellan dataförmedlingstjänster och andra mervärdestjänster som en tjänst bör få erbjuda och ersätta den med en funktionell åtskillnad samtidigt som vissa skyddsåtgärder bibehålls. Ordningen för administrativ övervakning bör förenklas. I stället för ett offentligt register på nationell nivå och ett på unionsnivå för leverantörer av dataförmedlingstjänster och dataaltruismorganisationer bör det endast finnas offentliga unionsregister, närmare bestämt ett register för leverantörer av dataförmedlingstjänster och ett annat för dataaltruismorganisationer. De behöriga myndigheterna bör vara oberoende i arbetet med övervakning av tilldelningen av beteckningen och enheternas efterlevnad av kraven för att erhålla den. Detta bör tolkas som att de är rättsligt och funktionellt oberoende i förhållande till en dataförmedlingstjänst eller dataaltruismorganisation, även på högsta ledningsnivå. Det bör vara möjligt för statliga organisationer att stödja dataförmedlingstjänster eller dataaltruismorganisationer ekonomiskt, i synnerhet med tanke på dessa enheters framväxande karaktär, förutsatt att de är rättsligt åtskilda enheter. För att säkerställa att erkända enheter är lätta att identifiera i hela unionen inrättade kommissionen genomförandeförordning (EU) 2023/1622 om utformningen av gemensamma logotyper för att identifiera leverantörer av dataförmedlingstjänster och dataaltruismorganisationer som är erkända i unionen.

(9) Förordning (EU) 2023/2854 undanröjer hinder för tillgång till och användning av data, frigör datadriven innovation och konkurrenskraft samt skyddar incitamenten för dem som investerar i datateknik.

(10) Enligt kapitel II i förordning (EU) 2023/2854 ska datahållare göra data, inbegripet data som skyddas som företagshemligheter, tillgängliga för användare och deras utvalda tredje parter, förutsatt att de åtgärder för konfidentialitet som fastställs av datahållaren bibehålls. Detta krav på att upprätthålla konfidentialiteten kompletterar Europaparlamentets och rådets direktiv (EU) 2016/943[30], vilket fastställer standarden för skydd av företagshemligheter inom unionen. Om företagshemligheter röjs för enheter i tredjeland kan emellertid riskerna för deras integritet och konfidentialitet öka om uppgifterna lämnas ut i jurisdiktioner där skyddet är otillräckligt eller svårt att faktiskt verkställa, vilket kan leda till otillåten användning, ekonomisk skada och rättslig osäkerhet.

(11) Det är nödvändigt att stärka förordning (EU) 2023/2854 genom att införa ytterligare ett skäl för datahållare att vägra att röja företagshemligheter, vilket kompletterar befintliga bestämmelser som tillåter avslag om datahållaren påvisar en hög sannolikhet för allvarlig ekonomisk skada. Enligt den nya bestämmelsen får datahållare vägra att röja företagshemligheter om de visar att det finns en hög risk för att de olagligen

[30] Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs (EUT L 157, 15.6.2016, s. 1).

anskaffats, utnyttjats eller lämnats ut till enheter som omfattas av ordningar med otillräckligt skydd eller ojämförbara eller svagare rättsliga ramar än de tillämpliga unionsreglerna. Den nya bestämmelsen omfattar även fall där tredjelandets rättsliga ram i teorin är stabil eller går längre än unionsreglerna, men saknar lämplig verkställighet i praktiken. Dessa risker visar att företagshemligheter kan anskaffas, utnyttjas eller lämnas ut i strid med unionsrätten, vilket hotar företagshemligheternas integritet och konfidentialitet.

(12) Aktiveringen av avslagsmekanismen bör förbli frivillig, och riskerna bör endast påvisas när den har aktiverats. Datahållare bör inte vara skyldiga att fullständigt analysera eller påvisa nivån på skyddet av företagshemligheter i tredjeländer eller hos en enhet i ett tredjeland som en förutsättning för att kunna styrka sin vägran att dela data eller att röja företagshemligheter. I sitt påvisande får datahållarna ta hänsyn till olika faktorer, däribland otillräckliga eller olämpliga rättsliga standarder, bristfällig eller godtycklig verkställighet, historiska överträdelser, utländsk skyldighet att lämna ut uppgifter som strider mot unionsrätten, begränsad tillgång till rättslig prövning eller rättsmedel för unionsenheter, strategiskt missbruk av processtaktik för att undergräva konkurrenter eller otillbörligt politiskt inflytande. Med tanke på de olika enheter, tredjeländer och scenarier för datadelning som berörs bör datahållarna inrikta sin bedömning och sitt påvisande på relevanta risker och agera därefter, däribland genom att fastställa lämpliga skyddsåtgärder eller aktivera mekanismen för att vägra att röja företagshemligheter. En vägran bör vara tydlig, proportionerlig och skräddarsydd för de särskilda omständigheterna i varje enskilt fall, snarare än att tillämpas systematiskt eller på ett allmänt sätt i ett helt tredjeland.

(13) Ett otillräckligt skydd av företagshemligheter och utmaningarna med att upprätthålla dem i tredjeländer kan orsaka irreparabel skada för europeiska företag. Målet är därför att stärka skyddet för företagshemligheter genom att förhindra att de röjs till fysiska eller juridiska personer som är etablerade i eller omfattas av jurisdiktioner där sådana risker förekommer. Detta inbegriper unionsbaserade enheter som kontrolleras av enheter i tredjeland, vilka kan agera i ond tro eller som täckmantel för enheter i tredjeland. Målet är även att avvärja direkt exponering mot enheter i tredjeland som är verksamma inom unionen och som omfattas av sådana jurisdiktioner. En fysisk eller juridisk person som omfattas av en jurisdiktion i ett tredjeland kommer att regleras, kontrolleras eller på annat sätt vara bunden av tredjelandets lagstiftning eller tillsynsmyndighet. Dotterbolag eller bolag som är anknutna till moderbolag i tredjeland kan utnyttja dessa jurisdiktioner för att undgå eller kringgå unionslagstiftningen. Med direkt eller indirekt kontroll avses förmågan att utöva ett avgörande eller bestämmande inflytande över en annan enhets ledning eller strategiska beslut, antingen genom ägande av kapital eller rösträtt, finansiellt deltagande, avtalsenliga arrangemang eller förmedlande enheter. Kontroll kan utövas direkt eller på annat sätt, även utan majoritetsägande. Datahållare bör göra sitt yttersta för att inhämta relevant information, till exempel genom att söka i offentliga register eller begära information direkt från användaren eller tredje part, och samtidigt säkerställa att informationen inte inhämtas på ett sätt som är inkräktande.

(14) Att skydda företagshemligheter från dessa sårbarheter är avgörande för att den europeiska industrin ska kunna bevara sin marknadsställning och sina konkurrensfördelar. Även om datahållarna får göra egna bedömningar när de skyddar sina företagshemligheter bör vägran att dela data begränsas till motiverade och exceptionella omständigheter för att bevara målen i förordning (EU) 2023/2854 om att främja datadriven innovation och en framgångsrik digital ekonomi i unionen.

Skyddsåtgärderna mot missbruk av avslagsmekanismen bör finnas kvar, däribland datahållarens skyldighet att underrätta de behöriga myndigheterna och att på ett vederbörligen motiverat sätt påvisa att utlämnandet utgör en hög risk. Detta påvisande bör stå i proportion till det aktuella fallet och utan onödigt dröjsmål överlämnas skriftligen till användaren eller den tredje parten. Alla berörda parter bör behandla beslutet och det styrkande påvisandet med konfidentialitet för att bevara de berörda företagshemligheternas konfidentiella karaktär. Användare och tredje parter får, i förekommande fall, överklaga datahållarens beslut till den behöriga myndigheten, inför domstol eller genom tvistlösningsorgan.

(15) För att förenkla ramen för datadelning mellan företag och myndigheter enligt förordning (EU) 2023/2854, och för att klargöra tvetydigheter som tidigare medförde mera omfattande skyldigheter för företag, är det nödvändigt att begränsa tillämpningsområdet för kapitel V i den förordningen från ”exceptionellt behov” till ”allmänna nödlägen”. Begreppet *allmänt nödläge*, vilket definieras i artikel 2.29 i förordning (EU) 2023/2854, säkerställer således att de skyldigheter som fastställs i det kapitlet endast åberopas i tydligt definierade och brådskande situationer, vilket minskar de tekniska, administrativa och rättsliga utmaningar som företagen stod inför inom ramen för den tidigare ordningen. Detta skulle säkerställa att begäranden om data är relevanta och proportionerliga för att bemöta, mildra eller stödja återhämtningen från allmänna nödlägen. Eftersom den uppdaterade unionsramen för europeisk statistik enligt Europaparlamentets och rådets förordning (EG) nr 223/2009[31] inte gäller allmänna nödlägen, är det viktigt att bevara den officiella statistikens roll enligt kapitel V i förordning (EU) 2023/2854 för att säkerställa tydligheten och effektiviteten i sådana situationer. Det är även nödvändigt att förtydliga ersättningssystemet för situationer där mikroföretag och små företag är skyldiga att tillhandahålla data för att hantera ett allmänt nödläge, eftersom dessa företag får begära ersättning i sådana fall.

(16) För att minska risken för rättslig osäkerhet som skulle kunna avskräcka från innovativa affärsmodeller är det nödvändigt att ta itu med de betydande tvetydigheter och bördor som är förknippade med efterlevnaden av bestämmelserna om smarta kontrakt för genomförande av datadelningsavtal enligt artikel 36 i förordning (EU) 2023/2854. Avsaknaden av harmoniserade standarder och tydliga definitioner av centrala begrepp som ”robusthet”, ”åtkomstkontroll” och ”enhetlighet med avtalsvillkoren”, i kombination med kravet på en mekanism för ”säkerhet vid uppsägning och avbrott” som skulle kunna vara oförenlig med decentraliserade eller offentliga blockkedjearkitekturer som bygger på oföränderliga liggare, innebar utmaningar för innovatörer ur ett kostnads- och möjlighetsperspektiv. Dessutom riskerar tvetydigheten kring utförandet av bedömningen av överensstämmelse enligt artikel 36.2 i den förordningen att medföra en oproportionerlig börda. Upphävandet av artikel 36 i förordning (EU) 2023/2854 skulle därför främja utvecklingen och

---

[31] Europaparlamentets och rådets förordning (EG) nr 223/2009 av den 11 mars 2009 om europeisk statistik och om upphävande av Europaparlamentets och rådets förordning (EG, Euratom) nr 1101/2008 om utlämnande av insynsskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor, rådets förordning (EG) nr 322/97 om gemenskapsstatistik och rådets beslut 89/382/EEG, Euratom om inrättande av en kommitté för Europeiska gemenskapernas statistiska program (EUT L 87, 31.3.2009, s. 164, ELI: http://data.europa.eu/eli/reg/2009/223/oj).

marknadsinförandet av nya affärsmodeller, uppmuntra innovation och minska hindren för ny teknik.

(17) Vissa databehandlingstjänster som inte omfattas av infrastruktur som tillhandahålls i form av en tjänst är anpassade till kundens behov eller ekosystem. Tillhandahållandet av sådana databehandlingstjänster bygger på tidskrävande avtalsförhandlingar för att fastställa kundens specifika krav och nödvändiga tekniska åtgärder för att anpassa databehandlingstjänsten och leverera en skräddarsydd lösning. Dessa tjänster är inte standardlösningar, utan anpassas till kundens behov för att tillhandahålla en skräddarsydd lösning där de flesta av databehandlingstjänstens funktioner har anpassats av leverantören efter kundens specifika behov och där de flesta av funktionerna inte skulle gå att använda utan en föregående anpassning av leverantören. Tjänsterna skiljer sig därmed från de skräddarsydda databehandlingstjänster som avses i artikel 31.1 i förordning (EU) 2023/2854. Skräddarsydda databehandlingstjänster är tjänster där de flesta av huvudfunktionerna har utformats för att tillgodose en enskild kunds särskilda behov eller databehandlingstjänster som inte erbjuds i bred kommersiell skala via leverantörens tjänstekatalog. För att undvika ytterligare kostnader och administrativ börda när avtal som ingåtts senast den 12 september 2025 behöver återupptas och omförhandlas är det nödvändigt att klargöra att skräddarsydda tjänster som tillhandahålls enligt avtal som ingåtts senast den 12 september 2025 inte bör omfattas av kapitel VI i förordning (EU) 2023/2854, med undantag av skyldigheten att minska och i slutändan avskaffa bytes- och uttagsavgifter.

(18) För att stärka sin finansiella planering och locka till sig investeringar kan leverantörer av databehandlingstjänster, särskilt små och medelstora företag och små midcapföretag, föredra och föreslå avtal med fast löptid. Det är nödvändigt att klargöra att leverantörer av databehandlingstjänster får införa bestämmelser om proportionerliga sanktioner för förtida uppsägning i dessa avtal så länge de inte utgör ett hinder för byte. Dessutom drabbas leverantörer av databehandlingstjänster som är små och medelstora företag eller små midcapföretag särskilt hårt av behovet att anpassa befintliga avtal om tillhandahållande av databehandlingstjänster till förordning (EU) 2023/2854. Det är därför nödvändigt att inrätta en särskild ordning för dessa leverantörer om de tillhandahåller andra databehandlingstjänster än IaaS på grundval av avtal som ingåtts senast den 12 september 2025. Med beaktande av syftet med förordning (EU) 2023/2854 att möjliggöra byte av databehandlingstjänster, och med tanke på att bytesavgifter, inklusive uttagsavgifter, utgör ett allvarligt hinder för byte, bör de nya enklare ordningarna för databehandlingstjänster som är skräddarsydda eller tillhandahålls av små och medelstora företag eller små midcapföretag inte undergräva det gradvisa avskaffandet av dessa avgifter. Avtalsbestämmelser som strider mot detta syfte bör anses aldrig ha existerat om de ingår i avtal om tillhandahållande av tjänster som omfattas av dessa två nya särskilda ordningar.

(19) Genom Europaparlamentets och rådets förordning (EU) 2018/1807[32] infördes en central princip för att stödja den datadrivna ekonomin i unionen, vilken i konkreta termer stöder etableringsfriheten och friheten att tillhandahålla en tjänst. Det ”fria flödet av data” i unionen, som förtydligas genom förbudet att införa datalokalisering, förblir en grundläggande princip som ger företagen rättssäkerhet och bör behållas i förordning (EU) 2023/2854. Bestämmelsen påverkar inte behandlingen av uppgifter så länge den utförs som en del av en verksamhet som inte omfattas av unionsrätten, särskilt när det gäller den nationella säkerheten, i enlighet med artikel 4 i fördraget om Europeiska unionen. Samtidigt ersätts andra bestämmelser i förordning (EU) 2018/1807 av nyare regler. Framför allt har en modern övergripande rättslig ram för byte mellan databehandlingstjänster införts genom kapitel VI i förordning (EU) 2023/2854, vilket har gjort artikel 6 i förordning (EU) 2018/1807 föråldrad i praktiken. Den samtidiga tillämpningen av dessa bestämmelser har ökat företagens rättsliga komplexitet. Därför bör förordning (EU) 2018/1807 upphävas.

(20) Begreppet ”allmän säkerhet”, i den mening som avses i artikel 52 i EUF-fördraget och i enlighet med domstolens tolkning, omfattar både den inre och den yttre säkerheten i en medlemsstat samt andra frågor med bäring på allmän säkerhet, särskilt för att underlätta utredning, upptäckt och lagföring av brott. Det förutsätter att det föreligger ett verkligt och tillräckligt allvarligt hot som påverkar ett av samhällets grundläggande intressen, såsom ett hot mot institutioners och väsentliga offentliga tjänsters funktion samt befolkningens överlevnad, liksom en risk för en allvarlig störning i yttre förbindelser eller av den fredliga samexistensen mellan folken, eller en risk för militära intressen. I överensstämmelse med proportionalitetsprincipen bör datalokaliseringskrav som är motiverade med hänsyn till allmän säkerhet vara anpassade för att uppnå det mål som eftersträvas och bör inte gå utöver vad som är nödvändigt för att uppnå detta mål.

(21) Både direktiv (EU) 2019/1024 och kapitel II i förordning (EU) 2022/868 reglerar vidareutnyttjande av information från den offentliga sektorn för innovationsändamål. Växelverkan mellan de två uppsättningarna av regler har skapat rättslig osäkerhet, särskilt för offentliga organ. Det är därför nödvändigt att lägga samman reglerna i ett enda rättsligt instrument för att öka den rättsliga enhetligheten och säkerheten.

(22) Eftersom det gemensamma målet för både direktiv (EU) 2019/1024 och förordning (EU) 2022/868 är att förbättra vidareutnyttjandet av information från den offentliga sektorn, och för att förenkla reglerna för både offentliga organ och vidareutnyttjare av information från den offentliga sektorn, är det rationellt att upphäva direktiv (EU) 2019/1024 och förordning (EU) 2022/868 och anpassa de två ordningarna och konsolidera reglerna i ett enda kapitel i den här förordningen. Denna lösning kommer att öka harmoniseringen av dessa regler i hela unionen, minska den administrativa bördan i samband med tolkning och genomförande av nationell lagstiftning och göra det lättare för företag att utveckla gränsöverskridande tjänster och produkter. När medlemsstaterna utser sina behöriga organ bör de se till att alla relevanta sektorer

[32] Europaparlamentets och rådets förordning (EU) 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen (EUT L 303, 28.11.2018, s. 59, ELI: http://data.europa.eu/eli/reg/2018/1807/oj).

omfattas, även om sektorsspecifika behöriga organ utses. Ändringarna i den här förordningen bör tolkas så att de inte ändrar tolkningen av de olika definitionerna och begreppen, om inte annat tydligt anges.

(23) Data och handlingar som kan göras tillgängliga för allmänheten för vidareutnyttjande, liksom data och handlingar som som är skyddade på grund av insynsskydd för kommersiella uppgifter, inklusive affärs-, yrkes- och företagshemligheter, insynsskydd för statistiska uppgifter, skydd av tredje parts immateriella rättigheter eller skydd av personuppgifter, innehas ofta av samma offentliga myndigheter. Det är därför nödvändigt att anpassa definitioner och gemensamma principer för all information från den offentliga sektorn och ta itu med frågor som rör samspelet mellan de två uppsättningarna regler.

(24) De befintliga reglerna bör effektiviseras för att öka tydligheten och enhetligheten. De två ordningarna för vidareutnyttjande bör emellertid förbli åtskilda, och deras respektive tillämpningsområde bör fortsätta att vara beroende av uppgifternas eller handlingarnas egenskaper och sammanhanget för deras vidareutnyttjande. Offentliga organ bör tillämpa ordningen med öppna data när detta är möjligt. Endast i de fall där de slår fast att uppgifterna eller dokumenten innehåller information som motsvarar vissa kategorier av skyddade data bör de begränsa allmänhetens tillgång till dem och överväga att göra dem tillgängliga för vidareutnyttjande som skyddade data.

(25) Uppstartsföretag, små företag och företag som betraktas som medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG[33] samt företag i sektorer med mindre utvecklad digital kapacitet kan ha svårt att vidareutnyttja data och handlingar. Samtidigt har ett fåtal mycket stora enheter med betydande ekonomisk styrka vuxit fram i den digitala ekonomin genom ackumulering och aggregering av enorma datavolymer och den tekniska infrastrukturen för monetarisering av dem. Dessa mycket stora enheter omfattar företag som tillhandahåller centrala plattformstjänster och betecknas som grindvakter enligt Europaparlamentets och rådets förordning (EU) 2022/1925[34], vilket innebär att de omfattas av särskilda skyldigheter att hantera obalanserna. För att utjämna dessa obalanser och stärka konkurrensen och innovationen bör offentliga organ kunna införa särskilda villkor i de stora företagens licenser för vidareutnyttjande av data och handlingar. Dessa villkor bör vara proportionerliga och utgå från objektiva kriterier med beaktande av den ekonomiska styrkan, enhetens förmåga att inhämta data eller dess utnämning till grindvakt enligt förordning (EU) 2022/1925, eller andra sådana kriterier i tillämpliga fall. De särskilda villkoren kan bland annat avse avgifterna för eller syftet med vidareutnyttjandet.

(26) För att främja innovation och upprätthålla en rättvis konkurrens på unionens digitala marknad är det absolut nödvändigt att säkerställa att tillgång till och vidareutnyttjande av data från den offentliga sektorn gynnar en rad olika marknadsaktörer och inte

---

33 Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

34 Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (Förordningen om digitala marknader) (EUT L 265, 12.10.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

oavsiktligt förstärker befintliga dominerande ställningar. Mycket stora företag, särskilt företag som utsetts till grindvakter enligt förordning (EU) 2022/1925, har betydande makt och inflytande över den inre marknaden. För att förhindra att dessa enheter utnyttjar sin ställning på bekostnad av rättvis konkurrens och innovation bör offentliga organ kunna införa högre avgifter för vidareutnyttjande av öppna offentliga och skyddade data. Dessa högre avgifter bör vara proportionella och baserade på objektiva kriterier med beaktande av den ekonomiska styrkan och enhetens förmåga att inhämta data. Syftet med denna åtgärd är att värna om mindre företags och nya marknadsaktörers innovations- och konkurrensmöjligheter i den digitala ekonomin.

(27) I den här förordningen föreslås ett antal riktade ändringar av förordning (EU) 2016/679 i syfte att förtydliga och förenkla, samtidigt som samma dataskyddsnivå upprätthålls. Enligt artikel 4 i förordning (EU) 2016/679 avses med personuppgifter varje upplysning som avser en identifierad eller identifierbar fysisk person. För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel som rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. Med beaktande av rättspraxis från Europeiska unionens domstol angående definitionen av personuppgifter är det nödvändigt att förtydliga när en fysisk person bör anses vara identifierbar. Förekomsten av ytterligare information som gör det möjligt att identifiera den registrerade innebär inte i sig att pseudonymiserade uppgifter i samtliga fall och för varje person eller enhet ska anses utgöra personuppgifter vid tillämpning av förordning (EU) 2016/679. Framför allt bör det klargöras att information inte ska betraktas som personuppgifter för en viss enhet om enheten inte har hjälpmedel som rimligen kan komma att användas för att identifiera den fysiska person som informationen avser. Om denna information överförs till tredje parter som på ett rimligt sätt kan identifiera den fysiska person som informationen avser, till exempel genom dubbelkontroll mot andra data som de förfogar över, kommer informationen att betraktas som personuppgifter endast för de tredje parter som har tillgång till sådana hjälpmedel. En enhet för vilken informationen inte utgör personuppgifter omfattas i princip inte av förordning (EU) 2016/679. I detta avseende har Europeiska unionens domstol slagit fast att ett hjälpmedel inte med rimlig sannolikhet kan komma att användas för att identifiera den registrerade om risken för identifiering i praktiken är försumbar på grund av att identifiering av denna person är förbjuden i lag eller omöjlig att genomföra i praktiken, exempelvis på grund av att den skulle kräva orimliga resurser i form av tid, kostnader och arbetskraft. Ett exempel på ett förbud mot återidentifiering finns i hälsodataanvändarnas skyldigheter i artikel 61.3 i Europaparlamentets och rådets förordning (EU) 2025/327[35]. Kommissionen bör, tillsammans med Europeiska dataskyddsstyrelsen, bistå personuppgiftsansvariga vid tillämpningen av denna uppdaterade definition genom att föreskriva tekniska kriterier i en genomförandeakt.

(28) För att bedöma om forskning uppfyller villkoren för vetenskaplig forskning vid tillämpning av den här förordningen kan hänsyn tas till sådana faktorer som de

---

35 Europaparlamentets och rådets förordning (EU) 2025/327 av den 11 februari 2025 om det europeiska hälsodataområdet och om ändring av direktiv 2011/24/EU och förordning (EU) 2024/2847 (EUT L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj).

metoder och de systematiska arbetssätt som används i samband med forskningen på det specifika området. Forskning och teknisk utveckling bör bedrivas i akademiska miljöer, industrimiljöer och andra miljöer, inbegripet små och medelstora företag (artikel 179.2 i EUF-fördraget), och bör alltid vara av hög kvalitet och följa principerna om tillförlitlighet, ärlighet, respekt och ansvarsskyldighet (verifierbarhet).

(29) Det bör upprepas att ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör betraktas som förenlig och laglig behandling av uppgifter. I sådana fall är det inte nödvändigt att på grundval av artikel 6.4 i den här förordningen fastställa om syftet med den ytterligare behandlingen är förenligt med det ändamål för vilket personuppgifterna ursprungligen samlades in.

(30) Tillförlitlig AI är avgörande för att skapa ekonomisk tillväxt och stödja innovation med samhällsnyttiga resultat. Utvecklingen och användningen av AI-system och de underliggande modellerna, såsom stora språkmodeller och generativa videomodeller, bygger på data, inklusive personuppgifter, i olika faser av AI:s livscykel, däribland tränings-, provnings- och valideringsfaserna, vilka i vissa fall kan sparas i AI-systemet eller AI-modellen. Behandlingen av personuppgifter i detta sammanhang kan därför, i tillämpliga fall, utföras med ett berättigat intresse i den mening som avses i artikel 6 i förordning (EU) 2016/679. Detta påverkar inte den personuppgiftsansvariges skyldighet att säkerställa att utvecklingen eller användningen (spridningen) av AI i ett visst sammanhang eller för vissa ändamål stämmer överens med annan unionsrätt eller nationell rätt, eller att säkerställa efterlevnaden om användningen uttryckligen är förbjuden enligt lag. Det påverkar inte heller den personuppgiftsansvariges skyldighet att säkerställa att villkoren i artikel 6.1 f i förordning (EU) 2016/679 och alla andra krav och principer i den förordningen är uppfyllda.

(31) När den personuppgiftsansvarige, mot bakgrund av den riskbaserade metod som ligger till grund för anpassningen av skyldigheterna enligt den här förordningen, balanserar den personuppgiftsansvariges eller en tredje parts berättigade intressen mot den registrerades intressen, rättigheter och friheter, bör hänsyn tas till huruvida det intresse som den personuppgiftsansvarige eftersträvar är fördelaktigt för den registrerade och samhället i stort, vilket till exempel kan vara fallet om behandlingen av personuppgifter är nödvändig för att upptäcka och undanröja snedvridning, och därigenom skydda de registrerade från diskriminering, eller om behandlingen av personuppgifter syftar till att säkerställa korrekt och säker utdata för fördelaktig användning, t.ex. för att förbättra tillgången till vissa tjänster. Hänsyn bör även tas till bland annat de registrerades rimliga förväntningar beroende på förhållandet till den personuppgiftsansvarige, lämpliga skyddsåtgärder för att minimera inverkan på de registrerades rättigheter, däribland att ge de registrerade ökad insyn och en ovillkorlig rätt att invända mot behandlingen av deras personuppgifter, efterlevnaden av tekniska föreskrifter för en tjänst som begränsar tredje parters användning av data för AI-utveckling, användningen av annan toppmodern teknik för integritetsskydd i samband AI-träning samt lämpliga tekniska åtgärder för att effektivt minimera riskerna till följd av upprapning, dataläckage och andra planerade eller förutsebara åtgärder.

(32) Behandlingen av personuppgifter för vetenskapliga forskningsändamål och tillämpningen av den allmänna dataskyddsförordningens bestämmelser om vetenskaplig forskning förutsätter att lämpliga skyddsåtgärder antas för de registrerades rättigheter och friheter i enlighet med artikel 89.1 i dataskyddsförordningen. För detta ändamål skapar den allmänna dataskyddsförordningen en jämvikt mellan rätten till skydd av personuppgifter, enligt

artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna, och den vetenskapliga friheten enligt artikel 13 i Europeiska unionens stadga om de grundläggande rättigheterna. Behandlingen av personuppgifter för vetenskaplig forskning har därför ett berättigat intresse i den mening som avses i artikel 6.1 f i förordning (EU) 2016/679, förutsatt att forskningen inte strider mot unionsrätten eller medlemsstaternas nationella rätt. Detta påverkar inte den personuppgiftsansvariges skyldighet att säkerställa att alla andra villkor i artikel 6.1 f i förordning (EU) 2016/679 och alla andra krav och principer i den förordningen är uppfyllda.

(33) Utvecklingen av vissa AI-system och AI-modeller kan inbegripa insamling av stora mängder data, inklusive personuppgifter och särskilda kategorier av dessa. Särskilda kategorier av personuppgifter kan finnas kvar i de dataset som använts för träning, provning eller validering eller lagras i AI-systemet eller AI-modellen, även om de särskilda kategorierna av personuppgifter inte är nödvändiga för behandlingen. För att inte hindra utvecklingen och driften av AI på ett oproportionerligt sätt, och med beaktande av den personuppgiftsansvariges möjligheter att identifiera och ta bort särskilda kategorier av personuppgifter, bör det vara tillåtet att göra undantag från förbudet mot behandling av särskilda kategorier av personuppgifter enligt artikel 9.2 i förordning (EU) 2016/679. Undantaget bör endast gälla om den personuppgiftsansvarige på ett effektivt sätt har genomfört lämpliga tekniska och organisatoriska åtgärder för att undvika behandling av sådana uppgifter, vidtar de lämpliga åtgärderna under ett AI-systems eller en AI-modells hela livscykel, och tar bort uppgifterna på ett effektivt sätt när de har identifierats. Om borttagandet skulle kräva en oproportionerlig ansträngning, särskilt om borttagandet av särskilda kategorier av data som lagrats i AI-systemet eller AI-modellen skulle kräva en ny utformning av AI-systemet eller AI-modellen, bör den personuppgiftsansvarige skydda dessa data på ett effektivt sätt så att de inte används för att dra slutsatser om utdata, lämnas ut eller på annat sätt görs tillgängliga för tredje parter. Detta undantag bör inte gälla om behandlingen av särskilda kategorier av personuppgifter är nödvändig för behandlingen. I detta fall bör den personuppgiftsansvarige åberopa undantagen enligt artikel 9.2 a–j i förordning (EU) 2016/679.

(34) Med biometriska uppgifter, enligt definitionen i artikel 4.14 i förordning (EU) 2016/679, avses behandling av vissa kännetecken hos en fysisk person med hjälp av ett särskilt tekniskt hjälpmedel som möjliggör eller bekräftar identifieringen av denna fysiska person. Begreppet biometriska uppgifter omfattar två olika funktioner, närmare bestämt identifieringen av en fysisk person och kontrollen (även kallad autentiseringen) av hans eller hennes påstådda identitet, vilka båda bygger på olika typer av teknisk behandling. Behandlingen för identifiering bygger på en sökning för identifiering av den registrerades biometriska uppgifter i en databas, medan behandlingen för kontroll bygger på en ett-till-ett-matchning av biometriska uppgifter som den registrerade tillhandahållit för att därigenom hävda sin identitet. Undantag från förbudet att behandla biometriska uppgifter enligt artikel 9.1 i förordningen bör även tillåtas om kontrollen av den registrerades påstådda identitet är nödvändig för ett ändamål som eftersträvas av den personuppgiftsansvarige, och lämpliga skyddsåtgärder tillämpas för att den registrerade ensam ska kunna styra över behandlingen för kontroll. Om till exempel de biometriska uppgifterna lagras på ett säkert sätt enbart hos den registrerade eller om de lagras på ett säkert sätt hos den personuppgiftsansvarige med den senaste krypteringstekniken och endast den registrerade innehar krypteringsnyckeln eller motsvarande medel, kommer behandlingen sannolikt inte att medföra några betydande risker för hans eller hennes grundläggande rättigheter och friheter. Den personuppgiftsansvarige kommer inte,

eller endast under en mycket begränsad tid, att få kännedom om de biometriska uppgifterna under behandlingen för kontroll.

(35) Enligt artikel 15 i förordning (EU) 2016/679 har den registrerade 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 viss ytterligare information. Rätten till tillgång bör göra det möjligt för den registrerade att få kännedom om behandlingen och kontrollera att den är laglig, och göra det möjligt för honom eller henne att utöva sina andra rättigheter enligt förordning (EU) 2016/679. Däremot bör det klargöras i artikel 12 i förordningen att rätten till tillgång, vilken redan från början är till fördel för de registrerade, inte bör missbrukas i den meningen att de registrerade missbrukar dem för andra ändamål än skydd av deras uppgifter. Till exempel skulle ett sådant missbruk av rätten till tillgång uppstå om den registrerade har för avsikt att få den personuppgiftsansvarige att avvisa en begäran om tillgång, för att därefter begära ersättning, eventuellt under hot om skadeståndsanspråk. Andra exempel på missbruk är situationer där registrerade överdrivet utnyttjar rätten till åtkomst i den enda avsikten att orsaka skada för den personuppgiftsansvarige, eller om en enskild person lämnar in en begäran och samtidigt erbjuder sig att dra tillbaka den i utbyte mot någon form av fördel från den personuppgiftsansvarige. För att hålla deras börda på en rimlig nivå bör personuppgiftsansvariga dessutom ha en lägre bevisbörda när en begäran är orimlig än när en begäran är uppenbart ogrundad. Skälet till detta är att en begärans uppenbart ogrundade karaktär beror på omständigheter som huvudsakligen ligger inom den personuppgiftsansvariges ansvarsområde, medan en begärans överdrivna karaktär gäller den registrerades eventuella missbruk, vilket huvudsakligen ligger utanför den personuppgiftsansvariges inflytandesfär, varför den personuppgiftsansvarige endast kan bevisa sådant missbruk till en rimlig nivå. Den registrerade bör under alla omständigheter vara så specifik som möjligt när han eller hon begär tillgång till data enligt artikel 15 i förordning (EU) 2016/679. Överdrivet breda och likartade ansökningar bör också betraktas som överdrivna.

(36) Enligt artikel 13 i förordning (EU) 2016/679 ska den personuppgiftsansvarige lämna viss information till den registrerade om behandlingen av hans eller hennes personuppgifter samt viss ytterligare information som är nödvändig för att säkerställa en rättvis och transparent behandling, enligt definitionen i punkterna 1, 2 och 3 i den bestämmelsen. Enligt artikel 13.4 i förordning (EU) 2016/679 ska denna skyldighet inte tillämpas om och i den mån den registrerade redan förfogar över informationen. För att ytterligare minska bördan för personuppgiftsansvariga, utan att undergräva den registrerades möjligheter att utöva sina rättigheter enligt kapitel III i förordningen, bör detta undantag utvidgas till situationer där behandlingen sannolikt inte leder till en hög risk, i den mening som avses i artikel 35 i förordningen, och det finns rimliga skäl att anta att den registrerade redan har den information som avses i punkt 1 a och c mot bakgrund av det sammanhang i vilket personuppgifterna samlades in, i synnerhet när det gäller förhållandet mellan registrerade och den personuppgiftsansvarige. Detta bör vara situationer där förhållandet mellan den personuppgiftsansvarige och den registrerade är mycket tydligt och avgränsat och där den personuppgiftsansvariges verksamhet inte är dataintensiv, till exempel förhållandet mellan en hantverkare och dennes kunder, där behandlingens omfattning är begränsad till den minsta mängd uppgifter som krävs för att utföra tjänsten. Den personuppgiftsansvariges verksamhet är inte dataintensiv om endast en liten mängd personuppgifter samlas in och om behandlingen av uppgifterna inte är komplicerad, vilket till exempel inte är fallet på sysselsättningsområdet. Under sådana omständigheter, dvs. när behandlingen inte är

dataintensiv och komplicerad och när den personuppgiftsansvarige samlar in en liten mängd personuppgifter, bör det till exempel vara rimligt att förvänta sig att den registrerade har information om såväl den personuppgiftsansvariges identitet och kontaktuppgifter som syftet med behandlingen om behandlingen utförs för att fullgöra ett avtal i vilket den registrerade är part, eller om den registrerade har gett sitt samtycke till denna behandling, i enlighet med kraven i förordning (EU) 2016/679. Detsamma bör gälla för föreningar och sportklubbar där behandlingen av personuppgifter är begränsad till hantering av medlemskap, kommunikation med medlemmarna och organisation av verksamheten. Detta undantag från skyldigheterna i artikel 13 påverkar emellertid inte den personuppgiftsansvariges oberoende skyldigheter enligt artikel 15 i den förordningen, som gäller om den registrerade begär tillgång på grundval av den senare bestämmelsen. Om undantaget från skyldigheterna i artikel 13 inte är tillämpligt får personuppgiftsansvariga, för att balansera behovet av fullständighet med behovet av klarhet för den registrerade, använda en metod med flera nivåer när de tillhandahåller den information som krävs, särskilt genom att göra det möjligt för användare att söka efter ytterligare information.

(37) Om behandlingen sker för vetenskapliga forskningsändamål, och om det visar sig vara omöjligt eller skulle innebära en oproportionell ansträngning att tillhandahålla den registrerade denna information, bör det inte vara nödvändigt att tillhandahålla den information som föreskrivs i artikel 13 i den här förordningen. Den personuppgiftsansvarige bör göra rimliga ansträngningar för att inhämta kontaktuppgifter om de är lätt åtkomliga och inte skulle kräva en oproportionerlig ansträngning. Tillhandahållandet av informationen skulle framför allt medföra en oproportionerlig ansträngning om den personuppgiftsansvarige vid tidpunkten för insamlingen av personuppgifterna inte visste eller förväntade sig att den skulle behandla personuppgifter för vetenskapliga forskningsändamål i ett senare skede, i vilket fall denne eventuellt inte har de registrerades kontaktuppgifter lätt tillgängliga. I sådana situationer bör den personuppgiftsansvarige informera de registrerade indirekt, t.ex. genom att göra informationen allmänt tillgänglig. Tillhandahållandet av sådan information bör säkerställa att så många registrerade som möjligt nås. De relevanta metoderna för att göra informationen allmänt tillgänglig bör fastställas beroende på forskningsprojektets omständigheter och de registrerade som berörs .

(38) I artikel 22 i förordning (EU) 2016/679 föreskrivs regler för behandlingen av personuppgifter när den personuppgiftsansvarige fattar beslut som har rättsliga följder eller på liknande sätt i betydande grad påverkar den registrerade och som enbart grundas på automatiserad behandling. För att öka rättssäkerheten bör det klargöras att beslut som enbart grundas på automatiserad behandling är tillåtna om särskilda villkor är uppfyllda i enlighet med förordning (EU) 2016/679. Det bör även klargöras att det vid bedömningen av huruvida ett beslut är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och en personuppgiftsansvarig, i enlighet med artikel 22.2 a i förordning (EU) 2016/679, inte bör vara ett krav att beslutet endast kan fattas genom enbart automatiserad behandling. Detta innebär att det faktum att beslutet även kan fattas av en människa inte hindrar den personuppgiftsansvarige från att fatta beslutet genom enbart automatiserad behandling. Om det finns flera lika effektiva lösningar för automatiserad behandling bör den personuppgiftsansvarige använda den minst inkräktande.

(39) För att minska bördan för personuppgiftsansvariga och samtidigt säkerställa att tillsynsmyndigheterna har tillgång till relevant information och kan agera vid överträdelser av förordningen bör tröskeln för anmälan av en personuppgiftsincident

till tillsynsmyndigheten enligt artikel 33 i förordning (EU) 2016/679 anpassas till tröskeln för information till den registrerade om en personuppgiftsincident enligt artikel 34 i den förordningen. I händelse av en uppgiftsincident som sannolikt inte kommer att leda till en hög risk för fysiska personers rättigheter och friheter bör den personuppgiftsansvarige inte vara skyldig att underrätta den behöriga tillsynsmyndigheten. Den högre tröskeln för att anmäla en uppgiftsincident till tillsynsmyndigheten påverkar inte den personuppgiftsansvariges skyldighet att dokumentera incidenten i enlighet med artikel 33.5 i förordning (EU) 2016/679 eller dess skyldighet att visa att förordningen efterlevs, i enlighet med artikel 5.2 i den förordningen. För att underlätta efterlevnaden för personuppgiftsansvariga och ett harmoniserat tillvägagångssätt i unionen bör styrelsen utarbeta en gemensam mall för anmälan av uppgiftsincidenter till den behöriga tillsynsmyndigheten och en gemensam förteckning över omständigheter under vilka en personuppgiftsincident sannolikt kommer att leda till en hög risk för en fysisk persons rättigheter och friheter. Kommissionen bör ta vederbörlig hänsyn till det förslag som utarbetats av styrelsen och vid behov se över det innan det antas. För att ta hänsyn till nya hot mot informationssäkerheten bör den gemensamma mallen och förteckningen ses över minst vart tredje år och uppdateras vid behov. Avsaknaden av en gemensam förteckning över omständigheter under vilka en personuppgiftsincident sannolikt kommer att leda till en hög risk för en fysisk persons rättigheter och friheter bör inte påverka de personuppgiftsansvarigas skyldighet att anmäla dessa incidenter.

(40) Enligt artikel 35 i förordning (EU) 2016/679 ska personuppgiftsansvariga göra en konsekvensbedömning avseende dataskydd om behandlingen av personuppgifter sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. De tillsynsmyndigheter som inrättas i enlighet med den förordningen ska upprätta och offentliggöra en förteckning över de typer av behandlingar som omfattas av kravet på en konsekvensbedömning avseende dataskydd. I förordningen föreskrivs dessutom att tillsynsmyndigheterna får upprätta och offentliggöra en förteckning över de typer av behandlingar som inte kräver någon konsekvensbedömning avseende dataskydd. För att bidra till målet att uppnå konvergens i ekonomierna på ett effektivt sätt, och för att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna, öka rättssäkerheten, underlätta de personuppgiftsansvarigas efterlevnad av reglerna och säkerställa en harmoniserad tolkning av begreppet hög risk för de registrerades rättigheter och friheter, bör en enda förteckning över behandlingar tillhandahållas på EU-nivå för att ersätta de befintliga nationella förteckningarna. Dessutom bör det bli obligatoriskt att offentliggöra en förteckning över de typer av behandlingar som inte kräver någon konsekvensbedömning avseende dataskydd, vilket för närvarande är frivilligt. Förteckningarna över behandlingar bör utarbetas av styrelsen och antas av kommissionen som en genomförandeakt. För att göra det lättare för de personuppgiftsansvariga att uppfylla kraven bör styrelsen även utarbeta en gemensam mall och en gemensam metod för genomförande av konsekvensbedömningar avseende dataskydd, som ska antas av kommissionen i form av en genomförandeakt. Kommissionen bör ta vederbörlig hänsyn till de förslag som utarbetats av styrelsen och vid behov se över dem innan de antas. För att ta hänsyn till den tekniska

utvecklingen bör förteckningarna och den gemensamma mallen och metoden ses över minst vart tredje år och uppdateras vid behov.

(41) Europaparlamentets och rådets förordning (EU) 2018/1725[36] är tillämplig på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer. Europaparlamentets och rådets direktiv (EU) 2016/680[37] är tillämpligt på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. Förordning (EU) 2018/1725 och direktiv (EU) 2016/680 bör anpassas till de ändringar av förordning (EU) 2016/679 som införs genom den här förordningen.

(42) När en bestämmelse i förordning (EU) 2018/1725 följer samma principer som en bestämmelse i förordning (EU) 2016/679 bör dessa båda bestämmelser, enligt rättspraxis från Europeiska unionens domstol, tolkas enhetligt, vilket klargörs i skäl 5 i förordning (EU) 2018/1725. Den systematik som förordning (EU) 2018/1725 bygger på bör uppfattas som en motsvarighet till systematiken bakom förordning (EU) 2016/679. Genom den här förordningen ändras därför även de bestämmelser i förordning (EU) 2018/1725 som berörs av ändringarna av förordning (EU) 2016/679, i den mån de senare ändringarna även är relevanta i samband med behandling av personuppgifter som utförs av unionens institutioner, organ och byråer.

(43) För att säkerställa en stark och enhetlig ram för dataskydd i unionen bör de nödvändiga anpassningarna av direktiv (EU) 2016/680 och alla andra unionsrättsakter som är tillämpliga på denna behandling av personuppgifter utföras när den här förordningen har antagits för att möjliggöra en så nära tillämpning som möjligt av ändringarna av förordning (EU) 2016/679 och förordning (EU) 2018/1725.

(44) Lagring av personuppgifter eller tillgång till redan lagrade personuppgifter i en terminalutrustning och efterföljande behandling av sådana uppgifter bör regleras inom en enda rättslig ram, närmare bestämt förordning (EU) 2016/679, om abonnenten av den elektroniska kommunikationstjänsten eller användaren av terminalutrustningen är en fysisk person. De ändringar som läggs fram i den här förordningen fortsätter att erbjuda högsta möjliga skyddsnivå för personuppgifter, samtidigt som det blir enklare för de registrerade att utöva sina rättigheter och uttrycka sina val online. Ändringarna gäller framför allt lagring av information i den utrustningen och tillgång till eller annan insamling av information från den utrustningen som omfattar behandling av personuppgifter genom kakor eller liknande teknik för att inhämta information från terminalutrustningen. De relevanta reglerna bör även gälla oavsett om

---

[36] Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

[37] 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 (EUT L 119, 4.5.2016, s. 89. ELI: http://data.europa.eu/eli/dir/2016/680/oj).

terminalutrustningen ägs av den fysiska personen eller av en annan juridisk eller fysisk person.

Lagring av personuppgifter eller tillgång till redan lagrade personuppgifter i terminalutrustning bör även fortsättningsvis endast tillåtas på grundval av samtycke. I likhet med tillvägagångssättet i direktiv 2002/58/EG bör detta krav inte utesluta lagring av personuppgifter eller tillgång till redan lagrade personuppgifter i en fysisk persons terminalutrustning om detta grundar sig på unionsrätten eller medlemsstaternas nationella rätt i den mening som avses i artikel 6 i förordning (EU) 2016/679, uppfyller alla villkor för lagenlighet som fastställs i den bestämmelsen och utförs för de syften som fastställs i artikel 23.1 i förordning (EU) 2016/679.

För att minska regelbördan och ge personuppgiftsansvariga rättslig klarhet, och med tanke på att vissa ändamål med behandlingen utgör en låg risk för de registrerades rättigheter och friheter eller att sådan behandling kan vara nödvändig för att tillhandahålla en tjänst som den registrerade begär, är det nödvändigt att upprätta en begränsad förteckning över ändamål för vilka behandlingen bör tillåtas utan samtycke. När det gäller lagring av personuppgifter, eller tillgång till redan lagrade personuppgifter, i terminalutrustning, och senare behandling som är nödvändig för dessa ändamål, bör det därför föreskrivas i den här förordningen att behandlingen är laglig. Den personuppgiftsansvarige, till exempel en leverantör av medietjänster, får ge ett personuppgiftsbiträde, till exempel ett marknadsundersökningsföretag, i uppdrag att utföra behandlingen för dennes räkning.

För efterföljande behandling av personuppgifter för andra ändamål än de som anges i den begränsande förteckningen bör artikel 6 och, i tillämpliga fall, artikel 9 i förordning (EU) 2016/679 tillämpas. Mot bakgrund av principen om ansvarsskyldighet är det den personuppgiftsansvariges ansvar att välja lämplig rättslig grund för den planerade behandlingen. För att kunna åberopa ett berättigat intresse enligt artikel 6.1 f i förordning (EU) 2016/679 som grund för den efterföljande behandlingen av personuppgifter måste den personuppgiftsansvarige visa att denne agerar i sitt eget eller en tredje parts berättigade intresse, att behandlingen är nödvändig för att uppnå syftet med detta berättigade intresse och att den registrerades intressen eller grundläggande rättigheter inte väger tyngre än den personuppgiftsansvariges intressen. I detta sammanhang bör personuppgiftsansvariga ta största möjliga hänsyn till om den registrerade är ett barn, den registrerades rimliga förväntningar, konsekvenserna för den enskilde, antingen på grund av de behandlade uppgifternas omfattning eller de behandlade uppgifternas känslighet, behandlingens omfattning i den meningen att behandlingen inte kan vara särskilt omfattande på grund av mängden uppgifter eller antalet kategorier av uppgifter, att behandlingen bör baseras på uppgifter som är begränsade till vad som är nödvändigt och inte får baseras på övervakning av stora delar av de registrerades aktivitet online, och andra relevanta faktorer vid behov. Behandlingen bör inte leda till kontinuerlig övervakning av den registrerades privatliv.

Om den personuppgiftsansvarige inte kan åberopa ett berättigat intresse som rättslig grund för den efterföljande behandlingen bör behandlingen baseras på en annan grund i artikel 6.1, särskilt på samtycke i enlighet med artiklarna 6 och 7 i förordning (EU) 2016/679, förutsatt att alla principer i förordning (EU) 2016/679 följs.

(45) Registrerade som har avslagit en begäran om samtycke ställs ofta inför en ny begäran om att ge sitt samtycke varje gång de besöker den personuppgiftsansvariges onlinetjänst. Detta kan ha negativa konsekvenser för de registrerade, eftersom de kan

välja att samtycka bara för att undvika att begäran upprepas. Den personuppgiftsansvarige bör därför vara skyldig att respektera den registrerades val att avslå en begäran om samtycke under åtminstone en viss period.

(46) De registrerade bör ha möjlighet att förlita sig på automatiserade och maskinläsbara indikationer om deras val att samtycka till eller avslå en begäran om samtycke eller invända mot behandlingen av uppgifter. Sådana metoder bör följa den senaste utvecklingen. De kan ingå i webbläsarens inställningar eller i den europeiska digitala identitetsplånboken i enlighet med förordning (EU) nr 914/2014, eller tillämpas på annat lämpligt sätt. De regler som fastställs i den här förordningen bör stödja framväxten av marknadsdrivna lösningar med lämpliga gränssnitt. Den personuppgiftsansvarige bör vara skyldig att respektera automatiska och maskinläsbara upplysningar om den registrerades val när det väl finns tillgängliga standarder. Med tanke på vikten av oberoende journalistik i ett demokratiskt samhälle och för att inte undergräva den ekonomiska grunden för denna verksamhet bör leverantörer av medietjänster inte vara skyldiga att respektera de maskinläsbara upplysningarna på den registrerades val. Skyldigheten för leverantörer av webbläsare att se till att de registrerade har tillgång till tekniska hjälpmedel när de gör sina val avseende behandlingen av uppgifter bör inte undergräva medietjänstleverantörernas möjlighet att begära samtycke från de registrerade.

(47) Genom direktiv 2002/58/EG om integritet och elektronisk kommunikation, som senast reviderades 2009, föreskrivs en ram för skydd av rätten till integritet, inbegripet konfidentialitet vid kommunikation. Förordning (EU) 2016/679 anges också när det gäller behandling av personuppgifter i samband med elektroniska kommunikationstjänster. Det skyddar integriteten hos användarens eller abonnentens terminalutrustning som används för sådan kommunikation. Den nuvarande bestämmelsen i artikel 5.3 i direktiv 2002/58/EG bör förbli tillämplig i den mån abonnenten eller användaren inte är en fysisk person och den information som lagras eller hämtas inte utgör eller leder till behandling av personuppgifter.

(48) Artikel 4 i direktiv 2002/58/EG bör upphävas. I artikel 4 i direktiv 2002/58/EG fastställs krav för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster när det gäller att säkerställa tjänsternas säkerhet och anmäla eventuella incidenter. I direktiv (EU) 2022/2555 fastställs nya krav när det gäller riskhanteringsåtgärder för cybersäkerhet och rapportering av incidenter för dessa leverantörer. För att minska överlappningen av skyldigheter för enheter inom sektorn för elektronisk kommunikation bör artikel 4 i direktiv 2002/58/EG upphävas. När det gäller säkerheten vid behandling av personuppgifter enligt artikel 4.1 och 4.1a i det direktivet och anmälan av personuppgiftsbrott enligt artikel 4.3–4.5 i direktiv 2002/58/EG, innehåller förordning (EU) 2016/679 redan omfattande och uppdaterade regler. Dessa regler bör därför gälla för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster och leverantörer av allmänna kommunikationsnät för att därigenom säkerställa att en ordning tillämpas på personuppgiftsansvariga och personuppgiftsbiträden.

(49) Flera övergripande eller sektorsspecifika unionsrättsakter innehåller krav på att samma händelse ska anmälas till olika myndigheter med hjälp av olika tekniska hjälpmedel och kanaler. Den gemensamma kontaktpunkten för incidentrapportering bör göra det möjligt för enheter att fullgöra rapporteringsskyldigheterna enligt direktiv (EU) 2022/2555, förordning (EU) 2016/679, förordning (EU) 2022/2554, förordning (EU) nr 910/2014 och direktiv (EU) 2022/2557 genom att lämna in anmälningar via ett enda gränssnitt. Dessutom bör den gemensamma kontaktpunkten ge enheterna möjlighet att

hämta information som de tidigare har lämnat via kontaktpunkten så att de kan kontrollera att de har uppfyllt sina rapporteringsskyldigheter i samband med specifika incidenter.

(50) För att säkerställa säkerheten hos den gemensamma kontaktpunkten bör Enisa vidta lämpliga och proportionella tekniska, operativa och organisatoriska åtgärder för att hantera riskerna för den gemensamma kontaktpunktens säkerhet och den information som lämnas eller sprids via den gemensamma kontaktpunkten. Vid bedömningen av riskerna och åtgärdernas lämplighet och proportionalitet bör Enisa ta hänsyn till känsligheten hos den information som lämnas in eller sprids i enlighet med relevanta unionsrättsakter. Enisa bör samråda med behöriga myndigheter inom ramen för relevanta unionsrättsakter när byrån utarbetar de tekniska, operativa och organisatoriska åtgärder som krävs för att inrätta, upprätthålla och på ett säkert sätt driva den gemensamma kontaktpunkten genom att använda de befintliga samarbetsgrupper och nätverk i medlemsstaterna som inrättats enligt dessa rättsakter.

(51) Innan det blir möjligt att anmäla incidenter bör Enisa testa hur den gemensamma kontaktpunkten fungerar, vilket bör inbegripa en grundlig genomgång av de specifika egenskaperna och kraven för anmälningarna enligt de relevanta unionsrättsakterna. På grundval av resultaten av testerna bör kommissionen bedöma den gemensamma kontaktpunktens funktion, tillförlitlighet, integritet och konfidentialitet. När kommissionen gör sin bedömning bör den samråda med CSIRT-nätverket och de behöriga myndigheterna i enlighet med relevanta unionsrättsakter genom att använda de befintliga samarbetsgrupper och nätverk i medlemsstaterna som inrättats enligt dessa akter. När kommissionen konstaterar att den gemensamma kontaktpunkten säkerställer korrekt funktion, tillförlitlighet, integritet och konfidentialitet bör den offentliggöra ett tillkännagivande om detta i *Europeiska unionens officiella tidning*. Om kommissionen anser att korrekt funktion, tillförlitlighet, integritet och konfidentialitet inte säkerställs bör Enisa vidta alla nödvändiga korrigerande åtgärder, varefter kommissionen gör en ny bedömning.

(52) För att säkerställa kontinuitet och interoperabilitet med befintliga nationella tekniska lösningar som underlättar rapporteringen av incidenter bör Enisa i möjligaste mån ta hänsyn till dessa nationella tekniska lösningar vid utarbetandet av specifikationerna för de tekniska, operativa och organisatoriska åtgärder som krävs för att inrätta, upprätthålla och på ett säkert sätt driva den gemensamma kontaktpunkten. Enisa bör även överväga att använda tekniska protokoll och verktyg, däribland programmeringsgränssnitt och maskinläsbara standarder, som gör att enheterna kan integrera rapporteringskraven i sina affärsprocesser och att myndigheterna kan ansluta den gemensamma kontaktpunkten till sina nationella rapporteringssystem.

(53) För att säkerställa att den gemensamma kontaktpunkten gör det möjligt för de berörda enheterna att lämna in den typ av information och de format som krävs enligt de relevanta unionsrättsakterna bör Enisa samråda med kommissionen och de behöriga myndigheterna inom ramen för dessa akter. Om en unionsrättsakt inte har harmoniserats fullt ut när det gäller typen av information och anmälningarnas format bör medlemsstaterna informera Enisa om sina nationella bestämmelser.

(54) Med utgångspunkt i förordning (EU) 2022/2554 har finanssektorn gått i spetsen för genomförandet av en harmoniserad, övergripande och effektiv ram, även när det gäller rapportering av incidenter. För att underlätta efterlevnaden är det lämpligt att anpassa den ram för incidentrapportering som inrättats enligt förordning (EU) 2022/2554 till den gemensamma kontaktpunkten och samtidigt säkerställa den befintliga

rapporteringsramens kontinuitet och stabilitet, och ta i beaktande att den gemensamma kontaktpunkten tas i drift först när att det har bedömts att den säkerställer korrekt funktion, tillförlitlighet, integritet och konfidentialitet. Genom förordning (EU) 2022/2554 infördes dessutom standardiserade rapporteringsmallar som förenklar innehållet i rapporter om allvarliga IKT-relaterade incidenter för finanssektorn. Erfarenheterna från antagandet av dessa mallar ger värdefulla insikter och exempel på bästa praxis som bör beaktas när typen av information, formatet och förfarandet specificeras för anmälan för rapportering till den gemensamma kontaktpunkten enligt direktiv (EU) 2022/2555, direktiv (EU) 2022/2557 eller förordning (EU) 2016/679, i förekommande fall. För detta ändamål bör kommissionen ta vederbörlig hänsyn till de tekniska standarder för tillsyn som antagits i enlighet med förordning (EU) 2022/2554, vilka specificerar innehållet i såväl den ursprungliga anmälan som i delrapporterna och slutrapporterna om större IKT-relaterade incidenter. Syftet med detta tillvägagångssätt är att säkerställa konsekvens, främja synergieffekter och minska enheternas administrativa börda genom att minimera antalet datafält som enheterna måste fylla i och därigenom göra rapporteringsprocesserna enklare och mer effektiva.

(55) Enligt relevanta unionsrättsakter ska viss incidentspecifik information i ett senare skede utbytas mellan behöriga myndigheter för att underlätta en effektiv tillsyn och samordning. Därför bör den gemensamma kontaktpunkten utformas för att ta hänsyn till och stödja informationsutbytet på den nivån för varje relevant unionsrättsakt och säkerställa att lämpliga dataflöden mellan myndigheterna möjliggörs på ett säkert, snabbt och effektivt sätt om medlemsstaterna beslutar att använda denna kompletterande funktion.

(56) För att säkerställa att rapporteringen av incidenter görs via den gemensamma kontaktpunkten bör därför direktiv (EU) 2022/2555, förordning (EU) 2016/679, förordning (EU) 2022/2554, förordning (EU) 910/2014 och direktiv (EU) 2022/2557 ändras i enlighet med detta. Den gemensamma kontaktpunkten bör börja användas för rapportering enligt dessa rättsakter inom 18 månader efter det att den här förordningen har trätt i kraft. Om kommissionen initierar mekanismerna i tillkännagivandet och tillämpningsdatumet skjuts upp till 24 månader efter förordningens ikraftträdande bör motsvarande bestämmelser i direktiv (EU) 2022/2555, förordning (EU) 910/2014, förordning (EU) 2022/2554 och direktiv (EU) 2022/2557 fortsätta att gälla så att de rapporteringsskyldigheter som fastställs i bestämmelserna kan uppfyllas.

(57) Om det i undantagsfall är tekniskt omöjligt att lämna in anmälningar om incidenter via den gemensamma kontaktpunkten bör enheterna uppfylla sina rapporteringsskyldigheter med alternativa metoder. I detta syfte bör mottagare av anmälningar om incidenter enligt de relevanta unionsrättsakterna säkerställa att de kan ta emot sådana anmälningar med alternativa metoder och se till att information om dessa alternativa metoder finns allmänt tillgänglig.

(58) Europeiska datatillsynsmannen rådfrågades i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725[38] och avgav sitt yttrande

[38] Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och

den [DATUM]. Europeiska dataskyddsstyrelsen rådfrågades i enlighet med artikel 42.2 i förordning (EU) 2018/1725 och avgav ett yttrande den [DATUM].

(59) I förordning (EU) 2019/1150 fastställs en uppsättning målinriktade obligatoriska bestämmelser på unionsnivå för att säkerställa rättvisa, förutsebara, hållbara och förtroendeskapande affärsvillkor online på den inre marknaden. Förordning (EU) 2022/2065 och förordning (EU) 2022/1925 utgör ett övergripande regelverk för en säker, förutsebar och tillförlitlig onlinemiljö för alla slutanvändare av onlinetjänster och möjliggör lika villkor för företag på digitala marknader. För att förenkla unionslagstiftningen på området för onlinebaserade förmedlingstjänster och onlineplattformar, och med tanke på att målen och de centrala bestämmelserna i förordningen om förbindelserna mellan plattformar och företag till stor del omfattas av förordningen om digitala tjänster och förordningen om digitala marknader, bör förordning (EU) 2019/1050 upphävas. Förordning (EU) 2022/2065 och förordning (EU) 2022/1925 bidrar till ett fullständigt harmoniserat regelverk för digitala tjänster och digitala marknader genom tillnärmning av de nationella åtgärderna avseende kraven för leverantörer av förmedlingstjänster och öppenheten och rättvisan hos de centrala plattformstjänster som tillhandahålls av grindvakter. Av rättssäkerhetsskäl kommer vissa av definitionerna i artikel 2, bestämmelserna om begränsning och tillfälligt avbrytande i artikel 4 samt bestämmelserna om det interna systemet för hantering av klagomål i artikel 11 i förordning (EU) 2019/1150, till vilka det finns korshänvisningar i andra rättsakter, särskilt direktiv (EU) 2024/2831 om förbättrade arbetsvillkor för plattformsarbete, samt artikel 15 om efterlevnad att vara tillämpliga fram till dess att de ursprungliga rättsakterna har ändrats.

(60) Med tanke på den tekniska karaktären hos de ändringar som föreslås i den här förordningen och det brådskande behovet av en förenklad rättslig ram bör den här förordningen träda i kraft omedelbart efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*. Medlemsstaterna och de reglerade enheterna bör vid behov beviljas en övergångsperiod för att få möjlighet att anpassa sig till reglerna.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Ändringar av förordning (EU) 2023/2854

Förordning (EU) 2023/2854 ska ändras på följande sätt:

1. Artikel 1 ska ändras på följande sätt:

(a) I punkt 1 i ska följande led införas:

”ea) frivillig registrering av dataförmedlingstjänster,

eb) frivillig registrering av enheter som samlar in och behandlar data som tillhandahålls för altruistiska ändamål,

---

byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ec) inrättandet av en europeisk datainnovationsstyrelse,

ed) datalokaliseringskrav och tillgång till data för behöriga myndigheter,

ee) vidareutnyttjandet av vissa data och handlingar som innehas av offentliga organ eller av vissa offentliga företag samt av forskningsdata.”

(b) I punkt 2 ska följande led läggas till:

”g) Kapitel VIIa är tillämpligt på personuppgifter och icke-personuppgifter.

h) Kapitel VIIb är tillämpligt på alla icke-personuppgifter.

i) Kapitel VIIc är tillämpligt på personuppgifter och icke-personuppgifter, närmare bestämt

i) handlingar som innehas av offentliga organ i medlemsstaterna enligt vad som avses

(1) i artikel 32i.1 a, eller av offentliga företag som avses

(2) i artikel 32i.1 b,

ii) forskningsdata som avses i artikel 32i.1 c,

iii) vissa kategorier av skyddade data som avses i artikel 32i.1 a.”

(c) I punkt 3 ska led g ersättas med följande:

”g) Deltagare i dataområden.”

(d) Punkt 7 ska utgå.

(e) Följande punkter ska läggas till som punkterna 11, 12 och 13:

”11. Kapitel VIIb i denna förordning påverkar inte lagar och andra författningar som rör medlemsstaternas interna organisation och som fördelar, bland myndigheter och offentligrättsliga organ, befogenheter och ansvarsområden för databehandling utan avtalsenlig ersättning till privata parter, och inte heller medlemsstaters lagar och andra författningar som föreskriver genomförandet av dessa befogenheter och ansvar.

12. I de fall då sektorsspecifik unionsrätt eller nationell rätt föreskriver att offentliga organ, leverantörer av dataförmedlingstjänster eller erkända dataaltruismorganisationer ska uppfylla särskilda ytterligare tekniska, administrativa eller organisatoriska krav som hänför sig till kapitlen VIIa och VIIb, däribland genom ett auktorisations- eller certifieringssystem, ska de bestämmelserna i den sektorsspecifika unionsrätten eller den nationella rätten också tillämpas. Eventuella sådana särskilda ytterligare krav ska vara icke-diskriminerande, proportionella och objektivt motiverade.

13. När det gäller data och handlingar som omfattas av avsnitt II i kapitel VIIc påverkar kapitel VIIc i denna förordning inte medlemsstaternas möjlighet att anta mer detaljerade eller striktare regler, förutsatt att dessa regler möjliggör ett mer omfattande vidareutnyttjande av data och handlingar.”

2. Artikel 2 ska ändras på följande sätt:

(a) Följande punkter ska införas som punkterna 4a, 4b och 4c:

”4a. *samtycke*: samtycke enligt definitionen i artikel 4.11 i förordning (EU) 2016/679.

4b. *tillstånd*: tillstånd att ge dataanvändare rätt att behandla andra data än personuppgifter.

4c. *tillgång*: dataanvändning i enlighet med särskilda tekniska, rättsliga eller organisatoriska krav, utan att det nödvändigtvis innefattar överföring eller nedladdning av data.”

(b) Punkt 13 ska ersättas med följande:

”13. *datahållare*: en fysisk eller juridisk person som har en rätt eller skyldighet, i enlighet med denna förordning, tillämplig unionsrätt eller nationell lagstiftning som antagits i enlighet med unionsrätten, att använda eller tillgängliggöra data, inbegripet produktdata eller data från tillhörande tjänster som denne har hämtat eller genererat under tillhandahållandet av en tillhörande tjänst, om detta avtalats.”

(c) Följande punkter ska införas som punkterna 28a och 28b:

”28a. *offentligrättsliga organ*: organ som har samtliga följande egenskaper:

a) De har inrättats för att tillgodose behov i det allmännas intresse, utan industriell eller kommersiell karaktär.

b) De är juridiska personer.

c) De finansieras till största delen av statliga, regionala eller lokala myndigheter eller av andra offentligrättsliga organ, eller står under administrativ tillsyn av sådana myndigheter eller organ, eller har ett förvaltnings-, lednings- eller kontrollorgan där mer än hälften av ledamöterna utses av staten, av regionala eller lokala myndigheter eller av andra offentligrättsliga organ.

28b. *offentligt företag*: varje företag över vilket ett offentligt organ har ett direkt eller indirekt bestämmande inflytande till följd av ägarförhållande, finansiellt deltagande eller gällande regler. Offentliga organ ska anses utöva bestämmande inflytande när dessa myndigheter, direkt eller indirekt

a) äger majoriteten av det tecknade kapitalet i företaget,

b) kontrollerar röstmajoriteten för andelarna i företaget,

c) har rätt att utse över hälften av företagets förvaltnings-, lednings- eller kontrollorgan.”

(d) Följande punkter ska införas som punkterna 38a och 38b:

”38a. *dataförmedlingstjänst*: en tjänst som syftar till att upprätta förhållanden av ekonomisk karaktär för datadelning mellan ett obestämt antal registrerade eller datahållare och dataanvändare genom tekniska, rättsliga eller andra medel, inbegripet för att utöva de registrerades rättigheter när det gäller personuppgifter, och som

(1) inte har som huvudsyfte att förmedla upphovsrättsskyddat innehåll,

(2) inte upphandlas gemensamt av flera juridiska personer för exklusiv användning bland dem.

38b. *dataaltruism*: den frivilliga delningen av data på grundval av de registrerades samtycke till behandling av personuppgifter som rör dem, eller tillstånd från datahållare att tillåta användning av deras icke-personuppgifter utan något krav på eller mottagande av ersättning utöver ersättning för de kostnader som de ådragit sig när de gör uppgifterna tillgängliga för mål av allmänintresse, som det föreskrivs i nationell rätt i förekommande fall, såsom hälso- och sjukvård, bekämpande av klimatförändringar, förbättring av mobiliteten, främjande av utveckling, framställning och spridning av officiell statistik, förbättrat tillhandahållande av offentliga tjänster, politiskt beslutsfattande eller vetenskaplig forskning av allmänt intresse.”

(e) Följande punkter ska läggas till som punkterna 44–63:

”44. *medelstort företag*: ett medelstort företag enligt definitionen i artikel 2 i bilaga I till rekommendation 2003/361/EG.

45. *litet midcapföretag*: ett litet midcapföretag enligt definitionen i artikel 2 i bilagan till kommissionens rekommendation (EU) 2025/1099.

46. *universitet*: ett offentligt organ som tillhandahåller högre utbildning som leder till akademiska examina.

47. *standardiserad licens*: en uppsättning på förhand fastställda villkor för vidareutnyttjande i digitalt format, som helst ska vara förenliga med standardiserade offentliga licenser som finns tillgängliga online.

48. *handling*:

a) allt innehåll som inte är digitalt, oavsett medium (papper, ljud, bildinspelningar eller audiovisuella inspelningar), eller

b) varje del av sådant innehåll.

50. *dynamiska data*: data och handlingar i digital form som uppdateras ofta eller i realtid, särskilt på grund av deras volatilitet eller snabba föråldrande. Data som genereras av sensorer anses normalt vara dynamiska data.

51. *forskningsdata*: andra data än vetenskapliga publikationer, som samlas in eller framställs inom ramen för vetenskaplig forskningsverksamhet och som används som bevis i forskningsprocessen eller som i forskarvärlden är allmänt accepterade som nödvändiga för att validera forskningsrön och forskningsresultat.

52. *vidareutnyttjande*: fysiska eller juridiska personers användning av handlingar som innehas av

a) offentliga organ för andra kommersiella eller icke-kommersiella ändamål än det ursprungliga ändamål för vilket handlingarna framställdes inom den offentliga verksamheten, med undantag för utbyte av handlingar mellan offentliga organ som enbart sker i samband med deras offentliga verksamhet, eller

b) offentliga företag enligt kapitel VIIc avsnitt 2 för andra kommersiella eller icke-kommersiella ändamål än det ursprungliga ändamålet att tillhandahålla tjänster av allmänt intresse för vilket handlingarna framställdes, med undantag för utbyte av handlingar

mellan offentliga företag och offentliga organ som enbart sker i samband med offentliga organs offentliga verksamhet.

53. *värdefulla dataset*: data och handlingar vars vidareutnyttjande är förknippat med stora fördelar för samhället, miljön och ekonomin, framför allt på grund av deras lämplighet för att skapa mervärdestjänster, applikationer och nya högkvalitativa och anständiga arbetstillfällen, och på grund av antalet potentiella mottagare av de mervärdestjänster och mervärdesapplikationer som bygger på dessa data och handlingar.

54. *vissa kategorier av skyddade data*: data och handlingar som innehas av offentliga organ och som är skyddade på grund av

a) insynsskydd för kommersiella uppgifter, inklusive affärs-, yrkes- och företagshemligheter,

b) insynsskydd för statistiska uppgifter,

c) skydd av tredje parts immateriella rättigheter, eller

d) skydd av personuppgifter, i den mån uppgifterna inte omfattas av avsnitt 2 i kapitel VIIc.

56. *säker behandlingsmiljö*: fysisk eller virtuell miljö och organisatoriska metoder för att säkerställa överensstämmelse med unionsrätten, särskilt vad gäller de registrerades rättigheter, immateriella rättigheter samt insynsskydd, integritet och tillgänglighet för kommersiella och statistiska uppgifter, samt med tillämplig nationell rätt, och för att göra det möjligt för den enhet som tillhandahåller den säkra behandlingsmiljön att fastställa och övervaka alla databehandlingsåtgärder, inbegripet förevisandet, lagringen, nedladdningen och exporten av data och beräkningen av härledda data med hjälp av dataalgoritmer.

57. *vidareutnyttjare*: en fysisk eller juridisk person som har beviljats rätten att vidareutnyttja data eller handlingar som innehas av ett offentligt organ eller ett offentligt företag enligt kapitel VIIc, forskningsdata eller vissa kategorier av skyddade data.

58. *maskinläsbart format*: ett filformat som är strukturerat på ett sådant sätt att tillämpningsprogramvara enkelt kan identifiera, känna igen och extrahera specifika uppgifter, inklusive enskilda faktauppgifter, och deras interna struktur.

59. *öppet format*: ett filformat som är oberoende av plattform och tillgängligt för allmänheten utan några restriktioner som hindrar vidareutnyttjande av handlingar.

60. *öppen formell standard*: en standard som finns dokumenterad skriftligt och specificerar kraven för hur interoperabilitet mellan mjukvaror ska säkerställas.

61. *rimlig avkastning på investeringar*: en procentandel av den totala avgiften, utöver det belopp som krävs för att täcka de stödberättigande kostnaderna, som uppgår till högst 5 procentenheter över ECB:s fasta ränta.

62. *datalokaliseringskrav*: varje skyldighet, förbud, villkor, begränsning eller annat krav som föreskrivs i en medlemsstats lagar eller andra författningar eller som är ett resultat av en medlemsstats och dess offentligrättsliga organs allmänna och konsekventa administrativa praxis, inbegripet på området för

offentlig upphandling, utan att tillämpningen av direktiv 2014/24/EU påverkas, enligt vilket databehandling ska äga rum på en viss medlemsstats territorium eller hindrar behandling av data i någon annan medlemsstat.

63. *pseudonymisering*: pseudonymisering enligt artikel 4.5 i förordning (EU) 2016/679.”

3. I artikel 4 ska punkt 8 ersättas med följande:

”8. I undantagsfall, om den datahållare som är innehavare av företagshemligheter kan visa att det, trots de tekniska och organisatoriska åtgärder som användaren vidtagit i enlighet med punkt 6 i denna artikel, är mycket sannolikt att han eller hon kommer att lida allvarlig ekonomisk skada till följd av utlämnandet av företagshemligheter eller att utlämnandet av företagshemligheter till användaren utgör en hög risk för olagligt förvärv, olaglig användning eller olagligt utlämnande till enheter i tredjeland, eller enheter som är etablerade i unionen under direkt eller indirekt kontroll av sådana enheter, som omfattas av jurisdiktioner som erbjuder ett svagare eller icke likvärdigt skydd jämfört med det som föreskrivs i unionsrätten, får datahållaren avslå en begäran om tillgång till de specifika uppgifterna i fråga från fall till fall. Detta ska motiveras på vederbörligt sätt på grundval av objektiva faktorer, däribland verkställbarheten av skyddet av företagshemligheter i tredjeländer, de begärda uppgifternas art och sekretessnivå samt den uppkopplade produktens unika och nya karaktär. Motiveringen ska lämnas till användaren skriftligen utan onödigt dröjsmål. Om datahållaren vägrar att dela data enligt den här punkten ska denne underrätta den behöriga myndighet som utsetts enligt artikel 37.”

4. I artikel 5 ska punkt 11 ersättas med följande:

”11. I undantagsfall, om den datahållare som är innehavare av företagshemligheter kan visa att det, trots de tekniska och organisatoriska åtgärder som den tredje parten vidtagit i enlighet med punkt 9 i denna artikel, är mycket sannolikt att han eller hon kommer att lida allvarlig ekonomisk skada till följd av utlämnandet av företagshemligheter eller att utlämnandet av företagshemligheter till den tredje parten utgör en hög risk för olagligt förvärv, olaglig användning eller olagligt utlämnande till enheter i tredjeland, eller enheter som är etablerade i unionen under direkt eller indirekt kontroll av sådana enheter, som omfattas av jurisdiktioner som erbjuder ett svagare eller icke likvärdigt skydd jämfört med det som föreskrivs i unionsrätten, får datahållaren avslå en begäran om tillgång till de specifika uppgifterna i fråga från fall till fall. Detta ska motiveras på vederbörligt sätt på grundval av objektiva faktorer, däribland verkställbarheten av skyddet av företagshemligheter i tredjeländer, de begärda uppgifternas art och sekretessnivå samt den uppkopplade produktens unika och nya karaktär. Motiveringen ska lämnas till den tredje parten skriftligen utan onödigt dröjsmål. Om datahållaren vägrar att dela data enligt den här punkten ska denne underrätta den behöriga myndighet som utsetts enligt artikel 37.”

5. Rubriken på kapitel V ska ersättas med följande:

”GÖRA DATA TILLGÄNGLIGA FÖR OFFENTLIGA ORGAN, KOMMISSIONEN, EUROPEISKA CENTRALBANKEN OCH UNIONSORGAN PÅ GRUNDVAL AV ETT ALLMÄNT NÖDLÄGE"

6. Artiklarna 14 och 15 ska utgå.

7. Följande artikel ska införas som artikel 15a:

”Artikel 15a

Skyldigheten för datahållare att göra data tillgängliga i ett allmänt nödläge

1. Om ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan visar att det föreligger ett exceptionellt behov av att använda vissa data för att fullgöra sina lagstadgade skyldigheter i allmänhetens intresse när de hanterar, mildrar eller stöder återhämtningen från ett allmänt nödläge, får myndigheten eller organet begära att datahållare som är juridiska personer, bortsett från offentliga organ, tillhandahåller dessa data, inbegripet de metadata som krävs för att tolka och använda dessa data. På en sådan vederbörligen motiverad begäran ska datahållarna göra de data och metadata som avses tillgängliga för det begärande offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet. En begäran får även göras om officiell statistik måste tas fram i samband med ett allmänt nödläge.
2. Om de data som begärs är nödvändiga för att hantera ett allmänt nödläge, och om det begärande organet enligt punkt 1 inte kan inhämta de nödvändiga uppgifterna på annat sätt i tid, på ett effektivt sätt och på likvärdiga villkor, ska begäran avse icke-personuppgifter. Om det inte räcker att tillhandahålla icke-personuppgifter för att hantera det allmänna nödläget får personuppgifter också begäras och, om möjligt, göras tillgängliga i pseudonymiserad form, med förbehåll för lämpliga tekniska och organisatoriska åtgärder för att säkerställa deras skydd.
3. Om de data som begärs är nödvändiga för att mildra eller stödja återhämtningen från ett allmänt nödläge får ett begärande organ enligt punkt 1 som agerar på grundval av unionsrätten eller nationell rätt begära specifika icke-personuppgifter vars avsaknad hindrar organet från att mildra eller stödja indrivningen från ett allmänt nödläge. Sådana data ska inte begäras från mikroföretag och små företag.”

8. I artikel 16 ska punkt 2 ersättas med följande:

”2. Detta kapitel ska inte tillämpas på verksamhet som bedrivs av offentliga organ, kommissionen, Europeiska centralbanken eller unionsorgan och som syftar till att förebygga, förhindra, utreda, upptäcka eller lagföra brott eller administrativa överträdelser eller verkställa straffrättsliga påföljder, eller på tull- eller skatteförvaltning. Detta kapitel påverkar inte unionsrätt eller nationell rätt som reglerar sådan verksamhet.”

9. Artikel 17 ska ändras på följande sätt:

a) Punkt 1 ska ändras på följande sätt:

i) Inledningen ska ersättas med följande:

”Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan som begär data enligt artikel 15a ska"

ii) Leden b och c ska ersättas med följande:

”b) visa att villkoren för att framställa en begäran enligt artikel 15a är uppfyllda,

c) förklara syftet med begäran, den avsedda användningen av begärda data, i tillämpliga fall även av en tredje part i enlighet med punkt 4 i

denna artikel, användningens varaktighet, och när så är lämpligt hur behandlingen av personuppgifter ska tillgodose det allmänna nödläget,"

b) Punkt 2 ska ändras på följande sätt:

i) Led c ska ersättas med följande:

”c) stå i proportion till det allmänna nödläget och vara motiverad, i fråga om detaljnivå och omfattning av begärda data och hur ofta dessa begärda data kommer att tillgås,"

ii) Led e ska utgå.

c) Punkterna 5 och 6 ska utgå.

10. Artikel 18 ska ändras på följande sätt:

a) I punkt 2 ska inledningen ersättas med följande:

”2. Utan att det påverkar de särskilda behov vad gäller tillgänglighet av data som fastställs i unionsrätten eller nationell rätt får en datahållare avslå eller ansöka om ändring av en begäran om att göra data tillgängliga enligt detta kapitel utan oskäligt dröjsmål och under alla omständigheter senast fem arbetsdagar efter mottagandet av en begäran enligt artikel 15a.2 och utan oskäligt dröjsmål och, under alla omständigheter, senast 30 arbetsdagar efter mottagandet av en begäran enligt artikel 15a.3, av något av följande skäl:”

b) Punkt 5 ska utgå.

11. Artikel 19 ska ändras på följande sätt:

a) I punkt 1 ska inledningen ersättas med följande:

”Ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan som tar emot data till följd av en begäran enligt artikel 15a"

b) Punkt 3 ska ersättas med följande:

”3. Röjande av företagshemligheter till ett offentligt organ, kommissionen, Europeiska centralbanken eller ett unionsorgan ska endast krävas i den mån det är absolut nödvändigt för att uppnå syftet med en begäran enligt artikel 15a. I sådana fall ska datahållaren eller, om det inte rör sig om samma person, innehavaren av en företagshemlighet identifiera de data som skyddas som företagshemligheter, inbegripet relevanta metadata. Det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet ska före röjandet av företagshemligheter vidta alla nödvändiga och lämpliga tekniska och organisatoriska åtgärder för att bevara konfidentialiteten för företagshemligheterna, när så är lämpligt även användning av standardavtalsvillkor och tekniska standarder samt tillämpning av uppförandekoder.”

12. Artikel 20 ska ersättas med följande:

”Artikel 20

Ersättning för att göra data tillgängliga enligt kapitel V

1. Datahållare ska utan kostnad tillhandahålla de data som krävs för att hantera ett allmänt nödläge enligt artikel 15a.2. Det offentliga organ, kommissionen, Europeiska centralbanken eller det unionsorgan som har tagit emot dessa data ska ge datahållaren offentligt erkännande på begäran av datahållaren.

2. Datahållaren ska ha rätt till skälig ersättning för att göra data tillgängliga i enlighet med en begäran som gjorts enligt artikel 15a.3. Denna ersättning ska täcka de tekniska och organisatoriska kostnader som uppstått till följd av tillmötesgåendet av begäran, inbegripet, vid behov, kostnaderna för anonymisering, pseudonymisering, aggregering och teknisk anpassning, och en rimlig marginal. På begäran av det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet ska datahållaren tillhandahålla information om underlaget till kostnadsberäkningen och den rimliga marginalen.

3. Genom undantag från punkt 1 i den här artikeln får en datahållare som är ett mikroföretag eller ett litet företag begära ersättning för att göra data tillgängliga som svar på en begäran enligt artikel 15a.2, i enlighet med villkoren i punkt 2 i den här artikeln.

4. Datahållare ska inte ha rätt till ersättning för att göra data tillgängliga i enlighet med en begäran som gjorts enligt artikel 15a.3 om den specifika uppgiften av allmänt intresse avser framställning av officiell statistik och om inköp av data inte är tillåtet enligt nationell rätt. Medlemsstaterna ska underrätta kommissionen om inköp av data för framställning av officiell statistik inte är tillåtet enligt nationell rätt.”

13. Artikel 21 ska ändras på följande sätt:

a) Rubriken ska ersättas med följande:

”**Delning av data som erhållits i samband med ett allmänt nödläge med forskningsorganisationer eller statistikorgan"**

b) Punkt 5 ska ersättas med följande:

”5. Om ett offentligt organ eller kommissionen, Europeiska centralbanken eller ett unionsorgan har för avsikt att överföra eller tillgängliggöra data enligt punkt 1, ska det eller den utan oskäligt dröjsmål underrätta den datahållare från vilken dessa data mottogs och uppge följande:

a) Identitet och kontaktuppgifter för den organisation eller enskilda person som tar emot data.

b) Ändamålet med överföringen eller tillgängliggörandet av data.

c) Den period under vilken data ska användas och de tekniska skyddsåtgärder som har vidtagits.

d) De organisatoriska åtgärder som har vidtagits, inbegripet om personuppgifter eller företagshemligheter berörs.”

14. Följande artikel ska införas som artikel 22a före kapitel VI:

”Artikel 22a

Rätt att lämna in klagomål

Om det uppstår en tvist om en begäran om data enligt artikel 15a, inbegripet avslag, ändring, ersättningsnivå eller överföring eller tillgängliggörande av dessa data, får datahållaren, det offentliga organet, kommissionen, Europeiska centralbanken eller unionsorganet inge ett klagomål till den behöriga

myndighet som utsetts enligt artikel 37 i den medlemsstat där datahållaren är etablerad.”

15. I artikel 31 ska följande punkter läggas till som punkterna 1a och 1b:

”1a. De skyldigheter som fastställs i kapitel VI, med undantag av artikel 29, och i artikel 34 ska inte gälla för andra databehandlingstjänster än de som avses i artikel 30.1 om leverantören har anpassat huvuddelen av databehandlingstjänstens funktioner till kundens särskilda behov och om tillhandahållandet av sådana tjänster grundar sig på ett avtal som ingåtts senast den 12 september 2025.

Leverantören av sådana databehandlingstjänster ska inte vara skyldig att omförhandla eller ändra ett avtal om tillhandahållande av dessa tjänster innan det löper ut om avtalet ingicks senast den 12 september 2025. Varje avtalsbestämmelse i avtalet som strider mot artikel 29.1, 29.2 eller 29.3 ska anses vara ogiltig.

1b. En leverantör av en databehandlingstjänst får införa bestämmelser om proportionerliga sanktioner för förtida uppsägning i ett avtal med fast löptid för tillhandahållande av andra databehandlingstjänster än de som avses i artikel 30.1.

Om leverantören av en databehandlingstjänst är ett litet eller medelstort företag eller ett litet midcapföretag ska skyldigheterna i kapitel VI, med undantag av artikel 29, och i artikel 34 inte gälla för andra databehandlingstjänster än de som avses i artikel 30.1 om tillhandahållandet av sådana tjänster grundar sig på ett avtal som ingåtts senast den 12 september 2025.

Om leverantören av en databehandlingstjänst är ett litet eller medelstort företag eller ett litet midcapföretag ska leverantören inte vara skyldig att omförhandla eller ändra ett avtal om tillhandahållande av en annan databehandlingstjänst än de som avses i artikel 30.1 före dess utgång om avtalet ingicks senast den 12 september 2025. Varje avtalsbestämmelse i avtalet som strider mot artikel 29.1, 29.2 eller 29.3 ska anses vara ogiltig.”

16. Artikel 32 ska ändras på följande sätt:

a) Punkterna 1 och 2 ska ersättas med följande:

”1. Leverantörer av databehandlingstjänster, det offentliga organ som tillhandahåller data eller handlingar i enlighet med kapitel VIIc avsnitt 3, den fysiska eller juridiska person som har rätt att vidareutnyttja data eller handlingar i enlighet med kapitel VIIc avsnitt 3, en leverantör av dataförmedlingstjänster eller en erkänd dataaltruismorganisation ska vidta alla lämpliga tekniska, organisatoriska och rättsliga åtgärder, inbegripet avtal, för att förhindra internationell statlig åtkomst och tredjeländers statliga åtkomst till och överföring av icke-personuppgifter som innehas i unionen om denna överföring eller denna åtkomst skulle strida mot unionsrätten eller den berörda medlemsstatens nationella rätt, utan att det påverkar tillämpningen av punkterna 2 eller 3.

2. Beslut eller domar från en domstol i ett tredje land och beslut från förvaltningsmyndigheter i ett tredjeland där det krävs att en leverantör av databehandlingstjänster, det offentliga organ som tillhandahåller data eller handlingar i enlighet med kapitel VIIc avsnitt 3, den fysiska eller juridiska

person som beviljats rätten att vidareutnyttja data eller handlingar i enlighet med kapitel VIIc avsnitt 3, en leverantör av dataförmedlingstjänster eller en erkänd dataaltruismorganisation överför icke-personuppgifter som omfattas av tillämpningsområdet för denna förordning från unionen eller ger tillgång till sådana icke-personuppgifter som innehas i unionen får endast erkännas eller genomföras på något som helst sätt om det grundar sig på en internationell överenskommelse, såsom ett fördrag om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen, eller ett sådant avtal mellan det begärande tredjelandet och en medlemsstat.”

b) I punkt 3 första stycket ska inledningen ersättas med följande:

”3. I de fall då, i avsaknad av en internationell överenskommelse som avses i punkt 2, en leverantör av databehandlingstjänster, det offentliga organ som tillhandahåller data eller handlingar i enlighet med kapitel VIIc avsnitt 3, den fysiska eller juridiska person som beviljats rätten att vidareutnyttja data eller handlingar i enlighet med kapitel VIIc avsnitt 3, en leverantör av dataförmedlingstjänster eller en erkänd dataaltruismorganisation är adressat för ett beslut eller en dom från en domstol i ett tredje land eller ett beslut från en förvaltningsmyndighet i ett tredjeland om att överföra icke-personuppgifter som omfattas av tillämpningsområdet för denna förordning från unionen eller ge tillgång till sådana icke-personuppgifter som innehas i unionen, och efterlevnaden av ett sådant beslut eller en sådan dom skulle riskera att medföra att adressaten bryter mot unionsrätten eller den nationella rätten i den berörda medlemsstaten, ska tredjelandsmyndighetens överföring av eller tillgång till sådana data endast äga rum om"

c) Punkterna 4 och 5 ska ersättas med följande:

”4. Om villkoren i punkt 2 eller 3 är uppfyllda ska leverantören av databehandlingstjänster, det offentliga organ som tillhandahåller data eller handlingar i enlighet med kapitel VIIc avsnitt 3, den fysiska eller juridiska person som har beviljats rätten att vidareutnyttja data eller handlingar i enlighet med kapitel VIIc avsnitt 3, leverantören av dataförmedlingstjänster eller den erkända dataaltruismorganisationen tillhandahålla den minsta mängd data som är tillåten som svar på en begäran, på grundval av en rimlig tolkning av denna begäran från leverantören eller det relevanta nationella organ eller den relevanta myndighet som avses i punkt 3 andra stycket.

5. Leverantören av databehandlingstjänster, det offentliga organ som tillhandahåller data eller handlingar i enlighet med kapitel VIIc avsnitt 3, den fysiska eller juridiska person som har beviljats rätten att vidareutnyttja data eller handlingar i enlighet med kapitel VIIc avsnitt 3, leverantören av dataförmedlingstjänster eller den erkända dataaltruismorganisationen ska informera den fysiska eller juridiska person vars rättigheter och intressen kan påverkas om förekomsten av en begäran från en myndighet i tredjeland om att få tillgång till dess data innan den tillmötesgår denna begäran, utom om begäran tjänar brottsbekämpande ändamål och så länge detta är nödvändigt för att upprätthålla effektiviteten i den brottsbekämpande verksamheten.”

17. Artikel 36 ska utgå.

18. Följande kapitel ska införas som kapitel VIIa, VIIb och VIIc:

”**KAPITEL VIIa**
DATAFÖRMEDLINGSTJÄNSTER
OCH DATAALTRUISMORGANISATIONER

Artikel 32a

Offentliga unionsregister

(1) Kommissionen ska upprätta och regelbundet uppdatera offentliga unionsregister över

a) erkända leverantörer av dataförmedlingstjänster, och

b) erkända dataaltruismorganisationer.

(2) Leverantörer av dataförmedlingstjänster som är registrerade i det offentliga unionsregister som avses i punkt 1 a får använda beteckningen ”leverantör av dataförmedlingstjänster som är erkänd i unionen” i sin skriftliga och talade kommunikation samt den gemensamma logotyp som avses i punkt 4.

(3) Dataaltruismorganisationer som är registrerade i det offentliga unionsregister som avses i punkt 1 b får använda beteckningen ”dataaltruismorganisation som är erkänd i unionen” i sin skriftliga och talade kommunikation samt den gemensamma logotyp som avses i punkt 4.

(4) För att säkerställa att leverantörer av dataförmedlingstjänster som är erkända i unionen är lätta att identifiera i hela unionen har kommissionen befogenhet att anta genomförandeakter för att fastställa utformningen av den gemensamma logotypen. Dessa genomförandeakter ska antas i enlighet med det rådgivande förfarande som avses i artikel 46.1a.

Artikel 32b

Behöriga myndigheter för registrering av leverantörer av dataförmedlingstjänster och dataaltruismorganisationer

(1) Varje medlemsstat ska utse en eller flera behöriga myndigheter som ska vara ansvariga för tillämpningen och verkställigheten av detta kapitel i enlighet med artikel 37.1.

(2) De behöriga myndigheterna ska inrättas på ett sådant sätt att deras oberoende av erkända leverantörer av dataförmedlingstjänster eller erkända dataaltruismorganisationer säkerställs.

Artikel 32c

Allmänna krav för registrering av erkända leverantörer av dataförmedlingstjänster

För att kvalificera sig för registrering i det offentliga unionsregister som avses i artikel 32a.1 a ska leverantörer av dataförmedlingstjänster uppfylla samtliga av följande krav:

a) De använder inte de data för vilka de tillhandahåller dataförmedlingstjänster för andra ändamål än att ställa dem till dataanvändarnas förfogande.

b) De data som de samlar in om en fysisk eller juridisk persons verksamhet för att tillhandahålla dataförmedlingstjänsten, däribland datum, tidpunkt och geolokaliseringsdata, verksamhetens varaktighet och eventuella kopplingar till andra fysiska eller juridiska personer som har inrättats av den person som använder dataförmedlingstjänsten, används endast för att utveckla denna dataförmedlingstjänst.

c) Om de erbjuder ytterligare verktyg och tjänster till datahållare eller registrerade i det särskilda syftet att underlätta utbytet av data, däribland tillfällig lagring, kuratering, konvertering, kryptering, anonymisering och pseudonymisering, används sådana verktyg och tjänster endast på uttrycklig begäran eller efter uttryckligt godkännande av datahållaren eller den registrerade.

d) Om leverantörer av dataförmedlingstjänster som inte är mikroföretag och små företag erbjuder sina kunder andra mervärdestjänster än de tjänster som avses i led c, uppfyller de följande villkor:

   i) Mervärdestjänsterna begärs uttryckligen av användaren.

   ii) Uppgifterna används inte för andra ändamål än att utföra mervärdestjänsten.

   iii) Mervärdestjänsterna erbjuds genom ett funktionellt fristående företag.

   iv) Det företag som har för avsikt att erbjuda mervärdestjänsterna har inte utsetts till grindvakt i enlighet med artikel 3 i förordning (EU) 2022/1925.

   v) De kommersiella villkoren, inbegripet prissättningen, för tillhandahållandet av dataförmedlingstjänster till en datahållare eller dataanvändare är inte beroende av om datahållaren eller dataanvändaren använder mervärdestjänster som tillhandahålls av leverantören av dataförmedlingstjänster eller av en närstående enhet.

e) Leverantören av dataförmedlingstjänster som erbjuder tjänster åt de registrerade agerar i deras bästa intresse när den främjar deras utövande av sina rättigheter, i synnerhet genom att informera och, i lämpliga fall, ge de registrerade råd på ett koncist, transparent, begripligt och lättåtkomligt sätt om dataanvändarnas avsedda dataanvändningar och de standardvillkor som är förbundna med sådan användning, innan de registrerade ger sitt samtycke.

Artikel 32d

Allmänna krav för registrering av erkända dataaltruismorganisationer

För att kvalificera sig för registrering i det offentliga unionsregister som avses i artikel 32a.1 b ska dataaltruismorganisationer uppfylla samtliga av följande krav:

a) De bedriver dataaltruismverksamhet.

b) De är juridiska personer som inrättats i enlighet med nationell rätt för att uppfylla mål av allmänt intresse, i enlighet med i nationell rätt i förekommande fall.

c) De bedriver sin verksamhet på icke-vinstdrivande grund och är rättsligt fristående från alla enheter som bedriver verksamhet på vinstdrivande grund.

d) De bedriver sin dataaltruismverksamhet genom en struktur som är funktionellt åtskild från deras övriga verksamhet.

Artikel 32e

Registrering

(1) Leverantörer av dataförmedlingstjänster som uppfyller kraven i artikel 32c får lämna in en ansökan om registrering i det offentliga unionsregistret över erkända leverantörer av dataförmedlingstjänster till den behöriga myndighet som avses i artikel 32b i den medlemsstat där de har sitt huvudsakliga verksamhetsställe.

Dataaltruismorganisationer som uppfyller kraven i artikel 32d får lämna in en ansökan om registrering i det offentliga unionsregistret över erkända dataaltruismorganisationer till den behöriga myndighet som avses i artikel 32b i den medlemsstat där de har sitt huvudsakliga verksamhetsställe.

(2) Leverantörer av dataförmedlingstjänster och dataaltruismorganisationer som inte har något huvudsakligt verksamhetsställe i unionen ska utse en rättslig företrädare i någon av medlemsstaterna. Den rättsliga företrädaren ska kunna kontaktas utöver eller i stället för leverantören av dataförmedlingstjänster eller dataaltruismorganisationen av behöriga myndigheter eller av registrerade och datahållare. Den rättsliga företrädaren ska på begäran samarbeta med och på ett uttömmande sätt visa den behöriga myndigheten vilka åtgärder som vidtagits och vilka bestämmelser som införts av leverantören av dataförmedlingstjänster eller dataaltruismorganisationen för att säkerställa efterlevnaden av den här förordningen.

Leverantören av dataförmedlingstjänster eller dataaltruismorganisationen ska anses omfattas av jurisdiktionen i den medlemsstat där den rättsliga företrädaren har sin verksamhet. Utnämningen av en rättslig företrädare ska inte påverka eventuella rättsliga åtgärder som kan inledas mot leverantören av dataförmedlingstjänster eller dataaltruismorganisationen.

(3) De behöriga myndigheterna ska ta fram nödvändiga ansökningsblanketter.

(4) Om en leverantör av dataförmedlingstjänster har lämnat in all nödvändig information enligt punkt 3 i den här artikeln, och uppfyller kraven i artikel 32c, ska den behöriga myndigheten inom tolv veckor efter mottagandet av ansökan om registrering fatta beslut om huruvida leverantören uppfyller de kriterier som fastställs i artikel 32c. Om leverantören uppfyller kriterierna ska den behöriga myndigheten lämna relevant information till kommissionen, som ska registrera leverantören i det offentliga unionsregistret som en erkänd leverantör av dataförmedlingstjänster.

Det första stycket är även tillämpligt om en dataaltruismorganisation har lämnat in all nödvändig information enligt punkt 2 och uppfyller registreringskraven i artikel 32d.

Registreringen i det offentliga unionsregistret ska vara giltig i alla medlemsstater.

(5) Den behöriga myndigheten får ta ut avgifter för registreringen i enlighet med nationell rätt. Avgifterna ska vara proportionella och objektiva och baseras på de administrativa kostnaderna i samband med övervakningen av efterlevnaden. För små midcapföretag, små och medelstora företag och nystartade företag får den behöriga myndigheten ta ut en nedsatt avgift eller avstå från att ta ut avgiften.

(6) Registrerade enheter ska underrätta den behöriga myndigheten om eventuella senare ändringar av den information som lämnats under ansökningsprocessen eller om de upphör med sin dataförmedling eller dataaltruismverksamhet i unionen.

(7) Den behöriga myndigheten ska utan dröjsmål och på elektronisk väg underrätta kommissionen om alla underrättelser enligt punkt 6. Kommissionen ska utan onödigt dröjsmål uppdatera det offentliga unionsregistret.

Artikel 32f

Skyldigheter för erkända dataaltruismorganisationer

(1) Erkända dataaltruismorganisationer ska på ett tydligt och lättbegripligt sätt underrätta registrerade eller datahållare innan deras data behandlas

a) om de mål av allmänt intresse och, om tillämpligt, de särskilda, uttryckligt angivna och berättigade ändamål för vilka personuppgifter ska behandlas, och för vilka den tillåter att deras data behandlas av dataanvändare, och

b) om platsen för behandlingen och de mål av allmänt intresse för vilka den tillåter behandling som utförs i ett tredjeland, om behandlingen utförs av den erkända dataaltruismorganisationen.

(2) Erkända dataaltruismorganisationer får inte använda data för några andra mål än de mål av allmänt intresse för vilka den registrerade eller datahållaren tillåter behandling. Den erkända dataaltruismorganisationen får inte använda vilseledande marknadsföringsmetoder i samband med förfrågan om tillhandahållande av data.

(3) Erkända dataaltruismorganisationer ska tillhandahålla elektroniska medel för att erhålla samtycke från registrerade eller tillstånd att behandla data som gjorts tillgängliga av datahållare samt för att dra tillbaka samtycket eller tillståndet.

(4) Erkända dataaltruismorganisationer ska utan dröjsmål informera datahållarna i händelse av otillåten överföring av, tillgång till eller användning av icke-personuppgifter som de har delat.

(5) Om erkända dataaltruismorganisationer underlättar tredje parts behandling av data, bland annat genom att tillhandahålla verktyg för att erhålla samtycke från registrerade eller tillstånd att behandla data som gjorts tillgängliga av datahållare, ska de i förekommande fall ange i vilket tredjeland dataanvändningen är avsedd att äga rum.

Artikel 32g

Kontroll av efterlevnaden

(1) De behöriga myndigheter som avses i artikel 32b ska, antingen på eget initiativ eller på begäran av en fysisk eller juridisk person, kontrollera och övervaka huruvida erkända leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer uppfyller kraven i detta kapitel, inbegripet huruvida de fortsätter att uppfylla de registreringskrav som fastställs.

(2) De behöriga myndigheterna ska ha befogenhet att begära all information som krävs för att kontrollera efterlevnaden av kraven i detta kapitel från erkända leverantörer av dataförmedlingstjänster eller erkända dataaltruismorganisationer eller deras rättsliga företrädare. Varje begäran om information ska stå i proportion till uppgiftens utförande och innehålla en motivering.

(3) Om en behörig myndighet finner att en erkänd leverantör av dataförmedlingstjänster eller en erkänd dataaltruismorganisation inte uppfyller ett eller flera av kraven i detta kapitel ska den underrätta enheten, eller dess rättsliga företrädare, om dessa iakttagelser och ge enheten möjlighet att yttra sig inom 30 dagar efter mottagandet av underrättelsen.

(4) Den behöriga myndigheten ska ha befogenhet att kräva att den underlåtenhet som avses i punkt 3 upphör, antingen omedelbart eller inom en rimlig tidsperiod, och att lämpliga och proportionella åtgärder vidtas för att säkerställa efterlevnaden.

(5) Om en erkänd leverantör av dataförmedlingstjänster eller en erkänd dataaltruismorganisation inte uppfyller ett eller flera av kraven i detta kapitel, även efter att ha underrättats i enlighet med punkt 3, ska den enheten

a) förlora sin rätt att använda den beteckning som avses i artikel 32a i skriftlig och muntlig kommunikation,

b) avföras från det offentliga unionsregister som avses i artikel 32a.

Varje beslut om att återkalla rätten att använda beteckningen enligt första stycket led a ska offentliggöras av den behöriga myndigheten.

KAPITEL VIIb

Fritt flöde av andra data än personuppgifter i unionen

Artikel 32h

Förbud mot lokaliseringskrav för andra data än personuppgifter inom unionen

(1) Datalokaliseringskrav för andra data än personuppgifter ska vara förbjudna, såvida de inte är motiverade av hänsyn till allmän säkerhet i enlighet med proportionalitetsprincipen eller fastställs på grundval av unionsrätten.

(2) Medlemsstaterna ska omedelbart underrätta kommissionen om varje utkast till akt som inför ett nytt datalokaliseringskrav eller ändrar ett befintligt datalokaliseringskrav i enlighet med förfarandena i artiklarna 5, 6 och 7 i Europaparlamentets och rådets direktiv (EU) 2015/1535.

KAPITEL VIIc

Vidareutnyttjande av data och handlingar som innehas av offentliga organ

AVSNITT 1

ALLMÄNNA BESTÄMMELSER

Artikel 32i

Innehåll och tillämpningsområde

(1) I detta kapitel fastställs en uppsättning regler för vidareutnyttjande och praktiska arrangemang för att underlätta vidareutnyttjande av

a) befintliga data och handlingar som innehas av offentliga organ i medlemsstaterna, inbegripet vissa kategorier av skyddade data,

b) befintliga data och handlingar som innehas av offentliga företag som

i) är verksamma på de områden som avses i kapitel II i Europaparlamentets och rådets direktiv 2014/25/EU,

ii) är verksamma som kollektivtrafikföretag enligt artikel 2 i Europaparlamentets och rådets förordning (EG) nr 1370/2007,

iii) är verksamma som lufttrafikföretag som fullgör allmän trafikplikt enligt artikel 16 i Europaparlamentets och rådets förordning (EG) nr 1008/2008, eller

iv) är verksamma som rederier inom gemenskapen som fullgör allmän trafikplikt enligt artikel 4 i rådets förordning (EEG) nr 3577/92,

c) forskningsdata enligt villkoren i artikel 32t.

(2) Detta kapitel är inte tillämpligt på

a) data och handlingar vars tillhandahållande inte omfattas av den offentliga verksamhet som bedrivs av de berörda offentliga organen, såsom den definieras i lagstiftning eller andra bindande regler i medlemsstaten eller, om sådana regler saknas, såsom den definieras i enlighet med gängse administrativ praxis i medlemsstaten i fråga, förutsatt att den offentliga verksamheten är tydligt avgränsad och föremål för översyn,

b) data och handlingar som innehas av offentliga företag och som

i) framställs utanför ramen för tillhandahållandet av tjänster av allmänt intresse enligt definitionen i lagstiftning eller andra bindande regler i medlemsstaten,

ii) har anknytning till verksamheter som är direkt konkurrensutsatta och som därför, i enlighet med artikel 34 i direktiv 2014/25/EU, inte omfattas av upphandlingsreglerna,

c) data och handlingar, däribland känsliga uppgifter, som är undantagna från tillgång enligt medlemsstaternas bestämmelser om tillgång till data på grund av skyddet av den nationella säkerheten (det vill säga statens säkerhet), försvaret eller den allmänna säkerheten,

d) data och handlingar som innehas av public service-bolag och deras dotterbolag och av andra organ eller deras dotterbolag för fullgörandet av ett uppdrag att verka i allmänhetens tjänst på radio- eller tv-området.

(3) Avsnitt 2 i detta kapitel är inte tillämpligt på

a) data eller handlingar, däribland känsliga uppgifter eller handlingar, som är undantagna från tillgång enligt medlemsstaternas bestämmelser om tillgång, bland annat med hänsyn till

i) insynsskydd för statistiska uppgifter,

ii) insynsskydd för kommersiella uppgifter (inklusive affärs-, yrkes- eller företagshemligheter),

b) tillgång till data eller handlingar som begränsas genom medlemsstaternas bestämmelser om tillgång

i) i fall där medborgare eller juridiska personer måste bevisa ett särskilt intresse för att få tillgång till handlingar,

ii) av skäl som rör skydd av personuppgifter och delar av data eller handlingar som är tillgängliga enligt de bestämmelserna och som innehåller personuppgifter vilkas vidareutnyttjande enligt lag har fastställts vara oförenligt med lagstiftningen om skydd för enskilda personer när det gäller behandling av personuppgifter eller konstaterats undergräva skyddet av den enskildes privatliv och integritet, särskilt i

enlighet med unionsrätten eller nationell rätt om skydd av personuppgifter, logotyper, heraldiska vapen och insignier,

c) data eller handlingar för vilka tredje part innehar immateriella rättigheter,

d) data eller handlingar som innehas av andra kulturinstitutioner än bibliotek, även universitetsbibliotek, museer och arkiv,

e) data eller handlingar som innehas av utbildningsinstitutioner som bedriver högst grundskoleutbildning och, i fråga om alla andra utbildningsinstitutioner, andra data än de som avses i punkt 1 c,

f) andra data eller handlingar än de som avses i punkt 1 c som innehas av organisationer som utför forskning och organisationer som finansierar forskning, inklusive organisationer som inrättats för överföring av forskningsresultat,

g) data eller handlingar för vilka tillgången är undantagen eller begränsad med hänvisning till skyddet av en kritisk enhet eller kritisk infrastruktur enligt definitionen i artikel 2.1 och 2.4 i direktiv (EU) 2022/2557.

(4) Avsnitt 3 i detta kapitel är inte tillämpligt på

a) data och handlingar som inte ingår i vissa kategorier av skyddade data,

b) data eller handlingar som innehas av offentliga företag,

c) data eller handlingar som innehas av kulturinstitutioner och utbildningsinstitutioner,

d) data och handlingar som omfattas av avsnitt 2 i detta kapitel.

(5) Detta kapitel bygger på, och påverkar inte, unionens och medlemsstaternas bestämmelser om tillgång, särskilt när det gäller beviljande av tillgång till och utlämnande av officiella handlingar.

(6) De skyldigheter som införs i enlighet med detta kapitel bör endast tillämpas i den mån de är förenliga med bestämmelserna i internationella avtal om skydd av immateriella rättigheter, i synnerhet Bernkonventionen för skydd av litterära och konstnärliga verk (*Bernkonventionen*), avtalet om handelsrelaterade aspekter av immaterialrätter (*Trips-avtalet*) och det fördrag om upphovsrätt som har upprättats av Världsorganisationen för den intellektuella äganderätten (*WCT-fördraget*).

(7) En databasproducents rätt enligt artikel 7.1 i direktiv 96/9/EG får inte utövas av offentliga organ för att förhindra vidareutnyttjande av data och handlingar eller begränsa vidareutnyttjandet i högre grad än vad som anges i det här kapitlet.

(8) I det här kapitlet regleras vidareutnyttjandet av befintliga data och handlingar som innehas av offentliga organ och offentliga företag i medlemsstaterna, inbegripet data och handlingar som omfattas av Europaparlamentets och rådets direktiv 2007/2/EG.

(9) Det här kapitlet påverkar inte tillämpningen av unionsrätt och nationell rätt eller internationella avtal i vilka unionen eller medlemsstaterna är parter när det gäller skyddet av de kategorier av data eller handlingar som avses i artikel 2.54.

Artikel 32j

Icke-diskriminering

(1) Alla tillämpliga villkor för vidareutnyttjande av data eller handlingar ska vara icke-diskriminerande, transparenta, proportionella och objektivt motiverade med hänsyn till kategorierna av data eller handlingar, syftet med vidareutnyttjandet och typerna av data eller handlingar för vilka vidareutnyttjande tillåts. Dessa villkor får inte användas för att begränsa konkurrensen. Denna princip ska även gälla för jämförbara kategorier av vidareutnyttjande, även för gränsöverskridande vidareutnyttjande.

(2) Om data eller handlingar vidareutnyttjas av ett offentligt organ som underlag för dess kommersiella verksamhet som inte ryms inom myndighetens offentliga verksamhet ska samma avgifter och övriga villkor för tillhandahållande av data eller handlingar tillämpas för den verksamheten som för andra användare.

Artikel 32k

Exklusiva avtal

(1) Alla potentiella marknadsaktörer ska kunna vidareutnyttja data eller handlingar, även om en eller flera marknadsaktörer redan utnyttjar förädlade produkter som bygger på dessa data eller handlingar. Avtal eller andra överenskommelser eller förfaranden som rör vidareutnyttjande av data eller handlingar och syftar eller leder till att de ger ensamrätt eller begränsar tillgången till data eller handlingar för vidareutnyttjande av andra enheter än parterna i sådana avtal, överenskommelser eller förfaranden, ska vara förbjudna.

(2) Genom undantag från punkt 1 får en ensamrätt som är nödvändig för tillhandahållandet av en tjänst av allmänt intresse beviljas i den utsträckning som är nödvändig för tillhandahållandet av tjänsten eller produkten på följande villkor:

a) Ensamrätten beviljas genom en administrativ åtgärd eller ett avtal i enlighet med tillämplig unionsrätt och nationell rätt och i enlighet med principerna om transparens, likabehandling och icke-diskriminering.

b) De avtal enligt vilka ensamrätten beviljas, inklusive skälen till varför detta beviljande är nödvändigt, är transparenta och görs tillgängliga för allmänheten online i en form som är förenlig med relevant unionsrätt om offentlig upphandling och nationell rätt.

c) Med undantag av ensamrätt i samband med digitalisering av kulturella resurser ska giltigheten av skälet för beviljande av ensamrätt avseende data och handlingar som omfattas av avsnitt 2 ses över regelbundet och under alla omständigheter vart tredje år.

d) Exklusiva avtal som ingås den 16 juli 2019 eller därefter ska göras tillgängliga för allmänheten online minst två månader innan de träder i kraft. De slutliga villkoren i sådana avtal ska vara öppna för insyn och göras tillgängliga för allmänheten online.

(3) Genom undantag från punkt 1 ska varaktigheten för en ensamrätt som gäller digitalisering av kulturella resurser i allmänhet inte överstiga tio år. Om varaktigheten överstiger tio år ska den vara förenlig med tillämplig unionsrätt och nationell rätt och omprövas under det elfte året samt, i tillämpliga fall, vart sjunde år därefter.

(4) När det gäller en sådan ensamrätt som avses i punkt 3 ska den berörda offentliga myndigheten utan kostnad få en kopia av de digitaliserade kulturella resurserna som

en del av det avtalet. Kopian ska finnas tillgänglig för vidareutnyttjande när ensamrätten har löpt ut.

(5) För vissa kategorier av skyddade data får ensamrätten att vidareutnyttja data inte gälla längre än tolv månader. När ett avtal har ingåtts ska avtalets löptid vara samma som perioden för den exklusiva rättigheten.

(6) Avtal eller andra överenskommelser eller förfaranden som, utan att uttryckligen bevilja ensamrätt, syftar till eller rimligen kan förväntas leda till en begränsad tillgång för vidareutnyttjande av data och handlingar inom ramen för avsnitt 2 för andra enheter än parter i sådana överenskommelser ska göras tillgängliga för allmänheten online minst två månader innan de träder i kraft. Sådana rättsliga eller praktiska arrangemangs påverkan på tillgången till data för vidareutnyttjande ska vara föremål för regelbunden översyn och ska, under alla omständigheter, ses över vart tredje år. De slutliga villkoren i sådana avtal ska vara öppna för insyn och göras tillgängliga online för allmänheten.

(7) För befintliga exklusiva avtal ska följande gälla:

a) Exklusiva avtal avseende data och handlingar inom ramen för avsnitt 2 som existerade den 17 juli 2013, som inte omfattas av undantagen i punkterna 2 och 3 och som har ingåtts av offentliga organ ska upphöra att gälla när kontraktet löper ut och under alla omständigheter senast den 18 juli 2043.

b) Exklusiva avtal avseende data och handlingar inom ramen för avsnitt 2 som existerade den 16 juli 2019, som inte omfattas av undantagen i punkterna 2 och 3 och som har ingåtts av offentliga företag ska upphöra att gälla när kontraktet löper ut och under alla omständigheter senast den 17 juli 2049.

Artikel 32l

Allmänna principer för avgifter

(1) Alla avgifter som anges i avsnitt 2 eller 3 ska vara transparenta, icke-diskriminerande, proportionella och objektivt motiverade, och får inte begränsa konkurrensen.

(2) När det gäller standardavgifter för vidareutnyttjande av data eller handlingar ska alla tillämpliga villkor och det faktiska avgiftsbeloppet, inklusive beräkningsgrunden för avgifterna, fastställas i förväg och offentliggöras, om möjligt och lämpligt på elektronisk väg.

(3) När det gäller andra avgifter för vidareutnyttjande än de avgifter som avses i punkt 1 ska de faktorer som beaktas vid beräkningen av avgifterna anges på förhand. På begäran ska innehavaren av berörda data eller handlingar även ange hur avgifterna har beräknats för en specifik ansökan om vidareutnyttjande.

(4) Offentliga organ ska säkerställa att alla avgifter även kan betalas online med hjälp av allmänt tillgängliga gränsöverskridande betalningstjänster, utan diskriminering på grund av betaltjänstleverantörens etableringsort, betalningsinstrumentets utfärdandeort eller den plats där betalkontot finns inom unionen.

Artikel 32m

Information om möjligheter till rättslig prövning

Offentliga organ ska se till att sökande som begärt att få vidareutnyttja data eller handlingar informeras om hur de kan få beslut eller förfaranden som påverkar dem överprövade.

AVSNITT 2

VIDAREUTNYTTJANDE AV ÖPPNA OFFENTLIGA DATA

Underavsnitt 1 Tillämpningsområde och allmänna principer

Artikel 32n

Allmän princip för vidareutnyttjande av öppna offentliga data

(1) Data eller handlingar som omfattas av detta avsnitt ska kunna vidareutnyttjas för kommersiella eller icke-kommersiella ändamål i enlighet med avsnitt 1 och avsnitt 2 underavsnitt 3.

(2) När det gäller data eller handlingar till vilka bibliotek, inklusive universitetsbibliotek, museer och arkiv, innehar immateriella rättigheter, och när det gäller data eller handlingar som innehas av offentliga företag, ska dessa data eller handlingar, om vidareutnyttjande av sådana data eller handlingar tillåts, kunna vidareutnyttjas för kommersiella eller icke-kommersiella ändamål i enlighet med avsnitt 1 och avsnitt 2 underavsnitt 3.

Underavsnitt 2

Begäran om vidareutnyttjande

Artikel 32o

Behandling av begäranden om vidareutnyttjande

(1) De offentliga organen ska, på elektronisk väg om detta är möjligt och lämpligt, behandla en begäran om vidareutnyttjande och ge sökanden tillgång till handlingen för vidareutnyttjande eller, om det krävs en licens, färdigställa licenserbjudandet till sökanden inom en rimlig tid som överensstämmer med den tidsfrist som gäller för behandling av en begäran om tillgång till data eller handlingar.

(2) Om det inte har fastställts några tidsfrister eller andra regler för tillhandahållande av data eller handlingar inom rimlig tid ska de offentliga organen behandla begäran och överlämna berörda data eller handlingar för vidareutnyttjande till sökanden eller, om det krävs en licens, färdigställa licenserbjudandet till sökanden så snart som möjligt eller under alla omständigheter inom 20 arbetsdagar från det att begäran inkommit. Den tidsfristen får förlängas med ytterligare 20 arbetsdagar för begäranden som är omfattande eller komplicerade. I sådana fall ska sökanden så snart som möjligt och åtminstone inom tre veckor från den ursprungliga begäran underrättas om att det behövs mer tid för att handlägga begäran och om skälen för detta.

(3) Om ett negativt beslut har fattats ska de offentliga organen meddela sökanden skälen till avslaget på grundval av relevanta bestämmelser om tillgång i den aktuella medlemsstaten eller bestämmelserna i denna förordning, särskilt artikel 32i.2 a–c och artikel 32i.3 a–d eller artikel 32n (avsnittet om den allmänna principen för vidareutnyttjande). Om ett negativt beslut är grundat på artikel 32i.3 d ska det offentliga organet även lämna en hänvisning till den fysiska eller juridiska person som är rättsinnehavare, om denne är känd, eller till den licensgivare från vilken det

offentliga organet har erhållit det aktuella materialet. Bibliotek, även universitetsbibliotek, museer och arkiv ska dock inte behöva lämna någon sådan hänvisning.

(4) Överprövningsmekanismerna ska inbegripa möjlighet till omprövning av en opartisk omprövningsmyndighet som besitter lämplig sakkunskap, såsom den nationella konkurrensmyndigheten, den berörda myndigheten för tillgång till data eller handlingar, den tillsynsmyndighet som inrättats i enlighet med förordning (EU) 2016/679 eller en nationell rättslig myndighet, vars beslut är bindande för den berörda offentliga myndigheten.

(5) Vid tillämpning av denna artikel ska medlemsstaterna fastställa praktiska arrangemang för att underlätta ett effektivt vidareutnyttjande av data eller handlingar. Dessa arrangemang kan särskilt omfatta metoderna för tillhandahållande av lämplig information om rättigheterna i denna förordning och att erbjuda lämpligt stöd och vägledning.

(6) Denna artikel ska inte tillämpas på följande enheter:

a) Offentliga företag.

b) Utbildningsinstitutioner, organisationer som bedriver forskning och organisationer som finansierar forskning.

Underavsnitt 3

Villkor för vidareutnyttjande

Artikel 32p

Tillgängliga format

(1) Utan att det påverkar tillämpningen av underavsnitt 5 ska offentliga organ och offentliga företag göra sina data eller handlingar tillgängliga i befintliga format och språkversioner samt, om möjligt och lämpligt, på elektronisk väg, i format som är öppna, maskinläsbara, tillgängliga, sökbara och möjliga att vidareutnyttja, tillsammans med tillhörande metadata. Både format och metadata ska, när så är möjligt, vara förenliga med formella öppna standarder.

(2) Medlemsstaterna ska uppmuntra offentliga organ och offentliga företag att framställa data eller handlingar som omfattas av detta avsnitt och göra dem tillgängliga i enlighet med principen om inbyggd öppenhet och öppenhet som standard.

(3) Punkt 1 ska inte medföra någon skyldighet för offentliga organ att skapa eller anpassa data eller handlingar eller tillhandahålla utdrag för att efterleva den punkten, om detta skulle kräva oproportionella ansträngningar och inte endast ett enkelt handgrepp.

(4) Offentliga organ ska inte vara skyldiga att fortsätta med framställning och lagring av en viss typ av handlingar för att dessa data eller handlingar ska kunna vidareutnyttjas av en organisation inom den privata eller offentliga sektorn.

(5) Offentliga organ ska göra dynamiska data tillgängliga för vidareutnyttjande omedelbart efter insamlingen genom lämpliga API:er och, i förekommande fall, som en bulknedladdning.

(6) Om det skulle överskrida det offentliga organets finansiella och tekniska kapacitet att göra de dynamiska data tillgängliga omedelbart efter insamlingen, som avses i punkt 5, och därmed medföra oproportionella ansträngningar, ska dessa dynamiska data

göras tillgängliga för vidareutnyttjande inom en tidsram eller med tillfälliga tekniska begränsningar som inte otillbörligen påverkar utnyttjandet av deras ekonomiska och sociala potential.

(7) Punkterna 1–6 ska tillämpas på befintliga data eller handlingar som innehas av offentliga företag och som är tillgängliga för vidareutnyttjande.

(8) De värdefulla dataset som förtecknas i enlighet med artikel 32v.1 ska göras tillgängliga för vidareutnyttjande i maskinläsbart format via lämpliga API:er och, i förekommande fall, som en bulknedladdning.

Artikel 32q

Principer för uttag av avgifter för öppna offentliga data

(1) Vidareutnyttjande av data eller handlingar som omfattas av detta avsnitt ska vara kostnadsfritt. Det kan emellertid vara tillåtet för det offentliga organ som innehar sådana data eller handlingar att täcka marginalkostnaderna för reproduktion, tillhandahållande och spridning av dessa data eller handlingar samt för anonymisering av personuppgifter och åtgärder som vidtagits för att skydda affärshemligheter.

(2) Punkt 1 ska inte tillämpas på följande enheter:

a) Offentliga organ som är skyldiga att generera intäkter för att täcka en väsentlig del av sina kostnader kopplade till den offentliga verksamheten.

b) Bibliotek, även universitetsbibliotek, museer och arkiv.

c) Offentliga företag.

(3) Medlemsstaterna ska offentliggöra en förteckning över de offentliga organ som avses i punkt 2 a online.

(4) I de fall som avses i punkt 2 a och c ska de sammanlagda avgifterna beräknas utifrån objektiva, transparenta och kontrollerbara kriterier. Dessa kriterier ska fastställas av medlemsstaterna. De samlade intäkterna från tillhandahållande för och tillåtelse till vidareutnyttjande av data och handlingar över en lämplig redovisningsperiod får inte överstiga kostnaderna för insamling, framställning, reproduktion, spridning och datalagring, jämte en rimlig avkastning på investeringar, och, i tillämpliga fall, anonymisering av personuppgifter och åtgärder för att skydda konfidentiell affärsinformation. Avgifterna ska beräknas i enlighet med tillämpliga redovisningsprinciper.

(5) Om de offentliga organ som avses i punkt 2 b tar ut avgifter får de samlade intäkterna från tillhandahållande för och tillåtelse till vidareutnyttjande av data och handlingar under en lämplig redovisningsperiod inte överstiga kostnaderna för insamling, framställning, reproduktion, spridning, datalagring, bevarande och rättighetsklarering och, i tillämpliga fall, anonymisering av personuppgifter och åtgärder för att skydda konfidentiell affärsinformation, tillsammans med en rimlig avkastning på investeringar. Avgifterna ska beräknas i enlighet med de redovisningsprinciper som gäller för de berörda offentliga organen.

(6) Offentliga organ får ta ut högre avgifter av mycket stora företag som vidareutnyttjar data och handlingar än de avgifter som anges i punkterna 1, 4 och 5. Alla sådana avgifter ska vara proportionella och grundade på objektiva kriterier, med beaktande av enhetens ekonomiska makt eller förmåga att inhämta data, särskilt om enheten har utsetts till grindvakt enligt förordning (EU) 2022/1925. Utöver de uppgifter som

anges i punkt 1 i denna artikel får dessa avgifter täcka kostnaderna för insamling, framställning, reproduktion, spridning och datalagring och, i tillämpliga fall, kostnaderna för anonymisering eller åtgärder för att skydda uppgifternas eller handlingarnas konfidentialitet, tillsammans med en rimlig avkastning på investeringar.

(7) Vidareutnyttjandet av följande ska vara kostnadsfritt för användaren:

a) Om inte annat följer av artikel 32v.3, 32v.4 och 32v.5, de värdefulla dataset som förtecknas i enlighet med punkt 1 i den artikeln.

b) Forskningsdata som avses i artikel 32i.1 c.

Artikel 32r

Standardiserade licenser

(1) Vidareutnyttjande av data eller handlingar får inte underkastas villkor såvida inte dessa villkor är objektiva, proportionella, icke-diskriminerande och motiverade av ett allmänintresse.

(2) Om vidareutnyttjande är underkastat villkor, får dessa villkor inte i onödan begränsa möjligheterna till vidareutnyttjande och inte användas för att begränsa konkurrensen.

(3) I de medlemsstater där licenser används ska de offentliga organen se till att standardiserade licenser för vidareutnyttjande av data eller handlingar från den offentliga sektorn, vilka kan anpassas till varje enskild licensansökan, finns tillgängliga i digitalt format och kan behandlas på elektronisk väg.

(4) Offentliga organ får fastställa särskilda villkor för mycket stora företag som vidareutnyttjar data och handlingar. Dessa villkor ska vara proportionella och bör vara grundade på objektiva kriterier. De ska fastställas med beaktande av enhetens ekonomiska makt eller förmåga att inhämta data, särskilt om enheten har utsetts till grindvakt enligt förordning (EU) 2022/1925.

Artikel 32s

Praktiska arrangemang

(1) Medlemsstaterna ska inrätta praktiska arrangemang för att underlätta sökning efter data eller handlingar som finns tillgängliga för vidareutnyttjande, till exempel i form av tillgångsförteckningar över viktiga data eller handlingar med relevanta metadata, om möjligt och lämpligt tillgängliga online och i maskinläsbart format, och i form av portaler som är kopplade till tillgångsförteckningarna. När så är möjligt ska medlemsstaterna underlätta sökning på flera språk efter data eller handlingar, särskilt genom att möjliggöra sammanställning av metadata på unionsnivå.

Medlemsstaterna ska även uppmana offentliga organ att inrätta praktiska arrangemang som underlättar bevarandet av data eller handlingar som finns tillgängliga för vidareutnyttjande.

(2) Medlemsstaterna ska, i samarbete med kommissionen, fortsätta sina ansträngningar för att förenkla tillgången till dataset, särskilt genom att tillhandahålla en gemensam åtkomstpunkt och stegvis göra lämpliga dataset som innehas av offentliga organ tillgängliga med avseende på de data eller handlingar som omfattas av detta avsnitt, samt till data som innehas av unionens institutioner i format som är tillgängliga, enkelt sökbara och kan vidareutnyttjas på elektronisk väg.

Underavsnitt 4

Forskningsdata

Artikel 32t

Forskningsdata

(1) Medlemsstaterna ska stödja tillgången till forskningsdata genom att anta nationella strategier och relevanta åtgärder som syftar till att göra offentligt finansierade forskningsdata tillgängliga (strategier för öppen tillgång) enligt principen öppenhet som standard och i enlighet med Fair-principerna. I detta sammanhang ska frågor avseende immateriella rättigheter, skydd av personuppgifter och insynsskydd, säkerhet och berättigade kommersiella intressen beaktas i enlighet med principen så fri som möjligt och så begränsad som nödvändigt. Dessa strategier för öppen tillgång ska inriktas på organisationer som bedriver forskning och organisationer som finansierar forskning.

(2) Utan att det påverkar tillämpningen av artikel 32n.3 d ska forskningsdata kunna vidareutnyttjas för kommersiella eller icke-kommersiella ändamål i enlighet med avsnitt 1 och avsnitt 2 underavsnitt 3, i den mån de är offentligt finansierade och om forskare, forskningsorganisationer eller organisationer som finansierar forskning redan har gjort dem tillgängliga för allmänheten via ett institutionellt eller ämnesbaserat register. I det sammanhanget ska berättigade kommersiella intressen, kunskapsöverföring och befintliga immateriella rättigheter beaktas.

Underavsnitt 5

Värdefulla dataset

Artikel 32u

Tematiska kategorier av värdefulla dataset

(1) De tematiska kategorierna av värdefulla dataset ska vara de som anges i bilaga I.

(2) Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 45.2a för att ändra bilaga I genom att lägga till nya tematiska kategorier av värdefulla dataset så att den tekniska utvecklingen och marknadsutvecklingen återspeglas.

Artikel 32v

Särskilda värdefulla dataset och arrangemang för offentliggörande och vidareutnyttjande

(1) Kommissionen ska anta genomförandeakter för att fastställa en förteckning över särskilda värdefulla dataset som tillhör de kategorier som anges i bilaga I och som innehas av offentliga organ och offentliga företag bland de data eller handlingar som omfattas av detta avsnitt.

Dessa särskilda värdefulla dataset ska

a) vara tillgängliga avgiftsfritt med förbehåll för punkterna 3, 4 och 5,

b) vara maskinläsbara,

c) tillhandahållas via API:er, och

d) tillhandahållas som en bulknedladdning i förekommande fall.

I dessa genomförandeakter får också ange arrangemangen för offentliggörande och vidareutnyttjande av värdefulla dataset. Dessa arrangemang ska vara förenliga med öppna standardiserade licenser.

Arrangemangen får inbegripa villkor avseende vidareutnyttjande, format för data och metadata och tekniska arrangemang för spridning. Medlemsstaternas investeringar i öppna data-strategier, till exempel investeringar i utvecklingen och ibruktagandet av vissa standarder, ska beaktas och vägas mot de möjliga fördelarna med uppförandet på förteckningen.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 46.2.

(2) Fastställandet av särskilda värdefulla dataset i enlighet med punkt 1 ska grundas på en bedömning av deras potential att

a) skapa viktiga socioekonomiska eller miljömässiga fördelar och innovativa tjänster,

b) gynna ett stort antal användare, i synnerhet små och medelstora företag och små midcapföretag,

c) bidra till att generera intäkter, och

d) kombineras med andra dataset.

I syfte att fastställa dessa särskilda värdefulla dataset ska kommissionen genomföra lämpliga samråd, inklusive på expertnivå, utföra en konsekvensbedömning samt säkerställa komplementaritet med befintliga rättsakter, till exempel Europaparlamentets och rådets direktiv 2010/40/EU, när det gäller vidareutnyttjande av data eller handlingar. Den konsekvensbedömningen ska omfatta en kostnads-nyttoanalys och en analys av huruvida kostnadsfritt tillhandahållande av värdefulla dataset från offentliga organ som är skyldiga att generera intäkter för att täcka en väsentlig del av sina kostnader kopplade till den offentliga verksamheten skulle leda till betydande budgetkonsekvenser för dessa myndigheter. När det gäller värdefulla dataset som innehas av offentliga företag ska konsekvensbedömningen särskilt uppmärksamma de offentliga företagens roll i en konkurrensutsatt ekonomisk miljö.

(3) Genom undantag från punkt 1 andra stycket led a ska de genomförandeakter som avses i den punkten föreskriva att den avgiftsfria tillgången till värdefulla dataset inte ska vara tillämplig på särskilda värdefulla dataset som innehas av offentliga företag om detta skulle leda till en snedvridning av konkurrensen på de berörda marknaderna.

(4) Kravet på att göra värdefulla dataset avgiftsfritt tillgängliga enligt punkt 1 andra stycket led a ska inte vara tillämpligt på bibliotek, även universitetsbibliotek, museer och arkiv.

(5) Medlemsstaterna får undanta offentliga organ som är skyldiga att generera intäkter för att täcka en väsentlig del av sina kostnader kopplade till den offentliga verksamheten från kravet att tillhandahålla värdefulla dataset avgiftsfritt under en period på högst två år från och med det datum då den relevanta genomförandeakten, antagen i enlighet med punkt 1, träder i kraft, om det avgiftsfria tillhandahållandet av dessa värdefulla dataset skulle medföra betydande budgetkonsekvenser för dem.

Avsnitt 3

Vidareutnyttjande av vissa kategorier av skyddade data som innehas av offentliga organ

Artikel 32w

Villkor för vidareutnyttjande

(1) Offentliga organ som enligt nationell rätt är behöriga att bevilja eller vägra tillgång för vidareutnyttjande av data eller handlingar som tillhör vissa kategorier av skyddade data ska offentliggöra villkoren för att tillåta sådant vidareutnyttjande samt förfarandet för att ansöka om vidareutnyttjande via den gemensamma informationspunkt som avses i artikel 32aa. När myndigheterna beviljar eller vägrar tillgång för vidareutnyttjande får de bistås av de behöriga organ som avses i artikel 32z.1.

Medlemsstaterna ska se till att de offentliga organen har de resurser som krävs för att uppfylla kraven i denna artikel och artikel 32x.

(2) Vidareutnyttjande av data eller handlingar ska inte påverka deras skyddade karaktär och ska endast tillåtas

a) i överensstämmelse med immateriella rättigheter,

b) om data som anses vara konfidentiella i enlighet med unionsrätten eller nationell rätt om affärshemligheter eller insynsskydd för statistiska uppgifter inte lämnas ut, efter att vidareutnyttjande har tillåtits, såvida inte detta vidareutnyttjande har tillåtits på grundval av den registrerades samtycke eller datahållarens tillstånd i enlighet med punkt 5,

c) i enlighet med förordning (EU) 2016/679.

(3) För att säkerställa att den skyddade karaktär som avses i punkt 2 bevaras får de offentliga organen ange följande krav:

a) Att tillgång för vidareutnyttjande av data eller handlingar endast beviljas om det offentliga organet eller det behöriga organet efter begäran om vidareutnyttjande har säkerställt att dessa data eller handlingar har

i) anonymiserats, när det gäller personuppgifter,

ii) varit föremål för andra former av framställning av personuppgifter,

iii) ändrats, aggregerats eller behandlats med någon annan metod för kontroll av utlämnande, när det gäller affärshemligheter, inbegripet företagshemligheter eller innehåll som skyddas av immateriella rättigheter.

b) Att tillgång till och vidareutnyttjande av data eller handlingar på distans ska ske i en säker behandlingsmiljö som tillhandahålls eller kontrolleras av det offentliga organet.

c) Att tillgång till och vidareutnyttjande av data eller handlingar ska ske i de fysiska lokaler där den säkra behandlingsmiljön är belägen i enlighet med höga säkerhetsnormer, förutsatt att fjärråtkomst inte kan tillåtas utan att tredje parters rättigheter och intressen hotas.

När det gäller vidareutnyttjande som tillåts i enlighet med första stycket led a i ska vidareutnyttjande av data eller handlingar omfattas av reglerna om öppna offentliga data i avsnitt 2. Detta påverkar inte tillämpningen av artikel 32y, vilken har företräde i händelse av konflikter.

När det gäller vidareutnyttjande som tillåts i enlighet med första stycket leden b och c ska de offentliga organen införa villkor som bevarar integriteten hos de tekniska systemens funktionssätt i den säkra behandlingsmiljön.

(4) Det offentliga organet ska förbehålla sig rätten att verifiera processen, metoderna och alla resultat från den behandling av data eller handlingar som görs av vidareutnyttjaren för att bevara integriteten i skyddet av dessa data eller handlingar. Det ska även förbehålla sig rätten att förbjuda användningen av resultat som innehåller information som hotar tredje parts rättigheter och intressen. Beslutet att förbjuda användningen av resultat ska vara lättbegripligt och tydligt för vidareutnyttjaren.

Såvida det i den nationella rätten inte föreskrivs särskilda skyddsåtgärder för tillämpliga skyldigheter i fråga om konfidentiell behandling i samband med vidareutnyttjande av vissa kategorier av skyddade data ska det offentliga organet ställa som villkor för vidareutnyttjandet av data eller handlingar som tillhandahålls i enlighet med punkt 3 att vidareutnyttjaren uppfyller en skyldighet i fråga om konfidentiell behandling som förbjuder utlämnande av information som äventyrar tredje parts rättigheter och intressen och som vidareutnyttjaren kan ha erhållit trots de skyddsåtgärder som införts. Vid otillåtet vidareutnyttjande av icke-personuppgifter ska vidareutnyttjaren utan dröjsmål, och när så är lämpligt med bistånd från det offentliga organet, vara skyldig att underrätta de fysiska eller juridiska personer vars rättigheter och intressen kan påverkas.

(5) Om vidareutnyttjande av data eller handlingar inte kan tillåtas i enlighet med punkterna 3 och 4 ska vidareutnyttjande endast vara möjligt

a) om det inte finns någon annan rättslig grund än samtycke för överföring av uppgifterna enligt förordning (EU) 2016/679, med de registrerades samtycke,

b) med tillstånd från de datahållare vars rättigheter och intressen kan påverkas av detta vidareutnyttjande.

Det offentliga organet ska, i enlighet med unionsrätten och nationell rätt, göra sitt bästa för att bistå potentiella vidareutnyttjare när de begär samtycke från de registrerade eller tillstånd från de datahållare vars rättigheter och intressen kan påverkas av vidareutnyttjandet, om detta är möjligt utan en oproportionerlig börda för det offentliga organet.

När det offentliga organet tillhandahåller sådant bistånd får den bistås av de behöriga organ som avses i artikel 32z.

Artikel 32x

Krav för vidareutnyttjares överföring av icke-personuppgifter till tredjeländer

(1) Om en vidareutnyttjare har för avsikt att överföra vissa kategorier av skyddade data som inte är personuppgifter till ett tredjeland, ska vidareutnyttjaren underrätta det offentliga organet om sin avsikt att överföra sådana data och om syftet med en sådan överföring vid tidpunkten för begäran om vidareutnyttjande av uppgifterna. Vid vidareutnyttjande på grundval av datahållarens tillstånd ska vidareutnyttjaren, när så är lämpligt med bistånd från det offentliga organet, underrätta den fysiska eller juridiska person vars rättigheter och intressen kan påverkas av denna avsikt, om detta syfte och de lämpliga skyddsåtgärderna. Det offentliga organet får inte tillåta vidareutnyttjandet om inte den fysiska eller juridiska personen ger sitt tillstånd till överföringen.

(2) Offentliga organ får endast överföra konfidentiella data som inte är personuppgifter eller data som skyddas av immateriella rättigheter till en vidareutnyttjare som har för

avsikt att överföra dessa data till ett annat tredjeland än ett land som utsetts i enlighet med punkt 7 om vidareutnyttjaren avtalsmässigt åtar sig att

a) fullgöra de skyldigheter som ålagts i enlighet med immateriella rättigheter och unionsrätt eller nationell rätt om affärshemligheter eller insynsskydd för statistiska uppgifter även efter det att data har överförts till tredjelandet,

b) godta behörigheten för domstolarna i den medlemsstat där den överförande offentliga myndigheten är belägen när det gäller tvister som rör efterlevnaden av immateriella rättigheter och unionsrätt eller nationell rätt om affärshemligheter eller insynsskydd för statistiska uppgifter.

(3) Kommissionen får anta genomförandeakter för att fastställa standardavtalsklausuler för fullgörande av de skyldigheter som avses i punkt 2 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 46.2.

(4) Offentliga organ ska, när så är lämpligt och i den utsträckning de kan, ge vidareutnyttjare vägledning och bistånd i fullgörandet av de skyldigheter som avses i punkt 2.

(5) Om det är motiverat på grund av ett betydande antal begäranden i hela unionen om vidareutnyttjandet av icke-personuppgifter i specifika tredjeländer får kommissionen anta genomförandeakter i vilka det intygas att ett tredjelands rättsliga, tillsynsmässiga och verkställighetsmässiga arrangemang

a) säkerställer ett skydd för immateriella rättigheter och företagshemligheter som i allt väsentligt är likvärdigt med det skydd som säkerställs genom unionsrätten,

b) tillämpas och verkställs på ett effektivt sätt, och

c) omfattar effektiva rättsmedel.

(6) Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 46.2.

(7) Enligt särskilda unionslagstiftningsakter kan vissa kategorier av icke-personuppgifter som innehas av offentliga organ anses vara mycket känsliga vid tillämpningen av denna artikel, om överföringen av dem till tredjeländer kan äventyra unionens offentligpolitiska mål, exempelvis säkerhet och folkhälsa, eller leda till risk för återidentifiering av anonymiserade data som inte är personuppgifter. Om en sådan akt antas ska kommissionen anta delegerade akter i enlighet med artikel 45 som kompletterar denna förordning genom att fastställa särskilda villkor som ska tillämpas på överföring av sådana data till tredjeländer.

Om så krävs enligt en särskild unionslagstiftningsakt som avses i första stycket kan dessa särskilda villkor innefatta villkor som är tillämpliga på överföring eller tekniska avtal i detta hänseende, begränsningar vad gäller vidareutnyttjande av data i tredjeländer eller kategorier av personer som har rätt att överföra sådana data till tredjeländer eller, i exceptionella fall, begränsningar vad gäller överföring till tredjeländer.

Den vidareutnyttjare som beviljades rätten att vidareutnyttja icke-personuppgifter får endast överföra dessa data till de tredjeländer för vilka kraven i punkterna 2, 4 och 5 är uppfyllda.

Artikel 32y

Avgifter

(1) Offentliga organ som tillåter vidareutnyttjande av vissa kategorier av skyddade data får ta ut avgifter för att tillåta vidareutnyttjande av sådana data.

(2) Om offentliga organ tar ut avgifter ska de vidta åtgärder för att ge incitament till vidareutnyttjande av vissa kategorier av skyddade data för icke-kommersiella ändamål, såsom vetenskaplig forskning, och av uppstartsföretag, små och medelstora företag och små midcapföretag i enlighet med unionens regler om statligt stöd. I detta avseende får de offentliga organen även göra dessa data tillgängliga till en nedsatt avgift eller kostnadsfritt, särskilt för uppstartsföretag, små och medelstora företag och små midcapföretag, det civila samhället samt forsknings- och utbildningsinstitutioner. Offentliga organ får i detta syfte upprätta en förteckning över kategorier av vidareutnyttjare för vilka data eller handlingar för vidareutnyttjande ska göras tillgängliga till en nedsatt avgift eller kostnadsfritt. Förteckningen och kriterierna för upprättande av den ska offentliggöras.

(3) Avgifterna ska härledas från kostnaderna för att genomföra förfarandet för begäran om vidareutnyttjande av vissa kategorier av skyddade data och vara begränsade till nödvändiga kostnader i samband med

a) reproduktion, tillhandahållande och spridning av data,

b) klarering av upphovsrätt,

c) anonymisering eller andra former av framställning av personuppgifter och affärshemligheter som föreskrivs i artikel 32w.3 [villkor för vidareutnyttjande],

d) underhåll av den säkra behandlingsmiljön,

e) förvärvande av rätten att tillåta vidareutnyttjande i enlighet med detta avsnitt av tredje parter utanför den offentliga sektorn, och bistånd till vidareutnyttjare som begär de registrerades samtycke och tillstånd från datainnehavare vars rättigheter och intressen kan påverkas av vidareutnyttjandet.

(4) Kriterierna och metoden för beräkning av avgifter ska fastställas av medlemsstaterna och offentliggöras. Offentliga organ ska offentliggöra en beskrivning av huvudkategorierna av kostnader och reglerna för fördelning av kostnader.

(5) Offentliga organ får ta ut högre avgifter än de som tillåts i enlighet med punkterna 2 och 3 i denna artikel när det gäller mycket stora företag, på grundval av objektiva kriterier och med beaktande av enhetens ekonomiska styrka eller förmåga att inhämta data, särskilt om företaget har beteckning som grindvakt enligt förordning (EU) 2022/1925. Alla sådana beräknade avgifter ska vara proportionella. Utöver de faktorer som anges i punkt 3 i denna artikel får de täcka kostnaderna för insamling och framställning av data, tillsammans med en rimlig avkastning på investeringar.

Artikel 32z

Behöriga organ

(1) För att utföra de uppgifter som avses i denna artikel ska varje medlemsstat utse ett eller flera behöriga organ i enlighet med artikel 37.1, vilka kan vara behöriga för vissa sektorer, men som kollektivt måste omfatta alla sektorer, för att bistå de offentliga organ som beviljar eller vägrar tillgång till vissa kategorier av skyddade data för vidareutnyttjande. Medlemsstaterna får antingen inrätta ett eller flera nya behöriga organ eller förlita sig på befintliga offentliga organ eller interna avdelningar inom offentliga organ som uppfyller de villkor som fastställs i detta avsnitt.

(2) De behöriga organen får ges befogenhet att bevilja tillgång för vidareutnyttjande av vissa kategorier av skyddade data i enlighet med unionsrätten eller nationell rätt som medger att sådan tillgång beviljas. Om dessa behöriga organ beviljar eller vägrar tillgång för vidareutnyttjande ska de omfattas av artiklarna 32k, 32w, 32x, 32y och 32ab.

(3) De behöriga organen ska ha tillräckliga juridiska, ekonomiska och tekniska resurser och personalresurser för att utföra de uppgifter som de anförtrotts, inbegripet de nödvändiga tekniska kunskaperna för att kunna följa relevant unionsrätt eller nationell rätt om systemen för tillgång till de kategorier av skyddade data som avses i artikel 2.54.

(4) Det bistånd som avses i punkt 1 ska, när så är nödvändigt, innefatta följande:

a) Tekniskt stöd för att tillhandahålla en säker behandlingsmiljö för att ge tillgång för vidareutnyttjande av data eller handlingar.

b) Vägledning och tekniskt stöd om hur data kan struktureras och lagras på bästa sätt för att göra dessa data eller handlingar lättillgängliga.

c) Tekniskt stöd för anonymisering, pseudonymisering och moderna integritetsbevarande metoder, vilket inte ska vara begränsat till personuppgifter, utan även gälla konfidentiell affärsinformation, inbegripet företagshemligheter eller innehåll som skyddas av immateriella rättigheter.

d) Bistånd till offentliga organ, i förekommande fall, för att stödja vidareutnyttjare när de begär registrerades samtycke till vidareutnyttjande eller datainnehavares tillstånd i linje med deras särskilda beslut, däribland om den jurisdiktion där databehandlingen är avsedd att utföras, och bistånd till offentliga organ när de behöver inrätta tekniska mekanismer som gör det möjligt att vidarebefordra begäranden om samtycke eller tillstånd från vidareutnyttjare, när detta är praktiskt genomförbart.

e) Bistånd till offentliga organ vid bedömningen av tillräckligheten i de avtalsmässiga åtaganden som görs av en vidareutnyttjare i enlighet med artikel 32x.2.

Artikel 32aa

Gemensam informationspunkt

(1) Varje medlemsstat ska utse en gemensam informationspunkt. Denna punkt ska säkerställa att lättillgänglig information om tillämpningen av artiklarna 32w, 32x och 32y finns tillgänglig.

(2) Den gemensamma informationspunkten ska vara behörig att ta emot förfrågningar eller ansökningar om vidareutnyttjande av vissa kategorier av skyddade data och, när så är möjligt och lämpligt, automatiskt överföra dessa till de behöriga offentliga organ som avses i artikel 32z.1, i förekommande fall.

(3) Den gemensamma informationspunkten får innefatta en separat, förenklad och väldokumenterad informationskanal för små och medelstora företag, små midcapföretag, nystartade företag och forskningsinstitut som tillgodoser deras behov och förmågor i samband med begäran av vidareutnyttjande av de kategorier av data som avses i artikel 2.54.

(4) Den gemensamma informationspunkten ska på elektronisk väg tillhandahålla en sökbar tillgångsförteckning med en översikt över alla tillgängliga källor till data eller handlingar, däribland, i relevanta fall, de källor till data eller handlingar som finns tillgängliga vid sektorsspecifika, regionala och lokala informationspunkter, tillsammans med relevant information som beskriver tillgängliga data eller handlingar, inbegripet åtminstone dataformatet och datastorleken samt villkoren för vidareutnyttjandet av dessa data.

(5) Kommissionen ska inrätta en europeisk gemensam åtkomstpunkt med ett sökbart elektroniskt register över tillgängliga data eller handlingar i nationella gemensamma informationspunkter och ytterligare information om hur man begär data eller handlingar via dessa nationella gemensamma informationspunkter.

Artikel 32ab

Behandling av begäranden om vidareutnyttjande

(1) Såvida inte kortare tidsfrister har fastställts i enlighet med nationell rätt ska de behöriga offentliga organen eller de behöriga organ som avses i artikel 32z.1 anta ett beslut om begäran om vidareutnyttjande av vissa kategorier av skyddade data inom två månader från dagen för mottagandet av begäran.

(2) Vid exceptionellt omfattande och komplicerade begäranden om vidareutnyttjande får denna tvåmånadersperiod förlängas med högst 30 dagar. I sådana fall ska de behöriga offentliga organen eller de behöriga organ som avses i artikel 32z.1 underrätta den sökande så snart som möjligt om att mer tid krävs för att genomföra förfarandet, tillsammans med skälen till dröjsmålet.

(3) Fysiska eller juridiska personer som direkt påverkas av ett beslut såsom avses i punkt 1 ska ha effektiv rätt till överprövning i den medlemsstat där det relevanta organet är lokaliserat. Denna rätt till överprövning ska föreskrivas i nationell rätt och inbegripa möjlighet till omprövning av en opartisk myndighet som besitter lämplig sakkunskap, såsom den nationella konkurrensmyndigheten, den berörda myndigheten för tillgång till handlingar, den tillsynsmyndighet som inrättats i enlighet med förordning (EU) 2016/679 eller en nationell rättslig myndighet, vars beslut är bindande för den berörda offentliga myndigheten eller det berörda behöriga organet.”

19. Artikel 38 ska ersättas med följande:

(1) ”Utan att det påverkar något annat administrativt prövningsförfarande eller rättsmedel ska fysiska och juridiska personer ha rätt att enskilt eller, i förekommande fall, kollektivt lämna in ett klagomål

a) till den relevanta behöriga myndigheten i den medlemsstat där de har sin hemvist, sin arbetsplats eller sin etableringsort, om de anser att deras rättigheter enligt denna förordning har kränkts,

b) i varje fråga som omfattas av denna förordning, särskilt mot en erkänd leverantör av dataförmedlingstjänster eller en erkänd dataaltruismorganisation, till den relevanta behöriga myndigheten för registrering av dataförmedlingstjänster eller den relevanta behöriga myndigheten för registrering av dataaltruismorganisationer.

(2) Datasamordnaren ska på begäran lämna all nödvändig information till fysiska och juridiska personer så att de kan lämna in klagomål till den relevanta behöriga myndigheten.

(3) Den behöriga myndighet till vilken klagomålet har lämnats in ska i enlighet med nationell rätt informera den klagande om

a) hur förfarandet fortskrider och vilket beslut som fattats, och

b) de rättsmedel som föreskrivs i artikel 39.”

20. I artikel 40 ska följande punkt införas som punkt 6:

”6. Denna artikel ska inte tillämpas på kapitel VIIc.”

21. Efter artikel 41 ska följande rubrik införas:

”KAPITEL IXa

Europeiska datainnovationsstyrelsen”

22. Följande artikel ska införas som artikel 41a:

”Artikel 41a

Europeiska datainnovationsstyrelsen

(1) Europeiska datainnovationsstyrelsen inrättas för att ge råd till och bistå kommissionen i samordningen av tillämpningen av den här förordningen och för att fungera som ett diskussionsforum för utvecklingen av en europeisk dataekonomi och datapolitik.

(2) Den ska åtminstone bestå av företrädare för medlemsstaterna med behörighet i frågor som rör data, de behöriga myndigheterna med avseende på efterlevnaden av kapitlen II, III, V, VIIa och VIIc i denna förordning, Europeiska dataskyddsstyrelsen, Europeiska datatillsynsmannen, Enisa samt EU-företrädaren för små och medelstora företag eller en företrädare som utsetts av nätverket av företrädare för små och medelstora företag. Kommissionen får besluta att lägga till ytterligare kategorier av medlemmar. I sin utnämning av enskilda experter ska kommissionen sträva efter att uppnå jämn könsfördelning och geografisk balans bland medlemmarna av gruppen.

(3) Kommissionen ska besluta om sammansättningen av de olika konstellationer i vilka styrelsen ska fullgöra sina uppgifter.

(4) Kommissionen ska vara ordförande vid Europeiska datainnovationsstyrelsens sammanträden.”

23. Artikel 42 ska ersättas med följande:

”Artikel 42

Europeiska datainnovationsstyrelsens roll

(1) Europeiska datainnovationsstyrelsen ska stödja en konsekvent tillämpning av den här förordningen genom att

a) fungera som ett forum för strategiska diskussioner om datapolitik, dataförvaltning, internationella dataflöden och sektorsövergripande utveckling som främjar den europeiska dataekonomin,

b) ge råd till och bistå kommissionen när det gäller att utveckla en konsekvent praxis hos behöriga myndigheter vid tillämpningen av kapitlen II, III, V, VII, VIIa och VIIc,

c) underlätta samarbetet mellan behöriga myndigheter genom kapacitetsuppbyggnad och informationsutbyte,

d) främja ett utbyte av erfarenheter och god praxis mellan medlemsstaterna när det gäller vidareutnyttjande av information från den offentliga sektorn i samarbete med andra relevanta styrande organ."

24. Artikel 45 ska ändras på följande sätt:

a) Punkt 2 ska ersättas med följande:

"2. Den befogenhet att anta delegerade akter som avses i artiklarna 29.7, 32u.2 och 33.2 ska ges till kommissionen tills vidare."

b) Punkt 3 ska ersättas med följande:

"3. Den delegering av befogenhet som avses i artiklarna 29.7, 32u.2 och 33.2 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 har offentliggjorts i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det ska inte påverka giltigheten av delegerade akter som redan har trätt i kraft."

c) Punkt 6 ska ersättas med följande:

"6. En delegerad akt som antagits enligt artikel 29.7, artikel 32u.2 eller artikel 33.2 ska endast träda i kraft om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på 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 göra några invändningar. Denna period ska förlängas med tre månader på Europaparlamentets eller rådets initiativ."

25. Artikel 46 ska ändras på följande sätt:

a) I punkt 1 ska första meningen ersättas med följande:

"Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011."

b) Följande punkt ska införas som punkt 1a:

"1a. När det hänvisas till denna punkt ska artikel 4 i förordning (EU) nr 182/2011 tillämpas."

26. Artikel 49 ska ändras på följande sätt:

a) Punkt 1 ska ändras på följande sätt:

i) Inledningen ska ersättas med följande:

"1. Kommissionen ska senast den 12 september 2028 genomföra en utvärdering av kapitlen II, III, IV, V, VI, VII och VIII och överlämna en rapport om de viktigaste resultaten till Europaparlamentet, rådet och

Europeiska ekonomiska och sociala kommittén. I utvärderingen ska särskilt följande bedömas:”

ii) Led m ska ersättas med följande:

”m) Inverkan av denna förordning på små och medelstora företag och små midcapföretag när det gäller deras innovationskapacitet och tillgången till databehandlingstjänster för användare i unionen samt bördan som de nya skyldigheterna innebär.”

b) Följande punkt ska införas som punkt 2a:

”2a. Kommissionen ska senast den [datum = datumet för ikraftträdande plus 5 år] göra en utvärdering av kapitlen VIIa, VIIb och VIIc i denna förordning och överlämna en rapport om de viktigaste resultaten till Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén.

I rapporten ska särskilt följande bedömas:

a) Statusen för registreringarna av dataförmedlingstjänster och vilken typ av tjänster de erbjuder.

b) Vilken typ av dataaltruismorganisationer som registrerats och en översikt över de mål av allmänt intresse för vilka data delas, i syfte att fastställa tydliga kriterier i detta avseende.

c) Tillämpningsområdet för och de sociala och ekonomiska konsekvenserna av kapitel VIIc avsnitt 2.

d) Hur mycket vidareutnyttjandet av handlingar från den offentliga sektorn som omfattas av kapitel VIIc avsnitt 2 har ökat, särskilt när det gäller små och medelstora företag och små midcapföretag.

e) Konsekvenserna av värdefulla dataset.

f) Samspelet mellan dataskyddsregler och möjligheter till vidareutnyttjande.

g) Medlemsstaterna ska förse kommissionen med de uppgifter som är nödvändiga för att utarbeta den rapporten.”

c) Punkt 5 ska ersättas med följande:

”5. På grundval av de rapporter som avses i punkterna 1, 2 och 2a får kommissionen vid behov lägga fram ett lagstiftningsförslag för Europaparlamentet och rådet om att ändra denna förordning.”

27. Bilaga I ska läggas till i enlighet med bilaga II till den här förordningen.

Artikel 2

Ändringar av förordning (EU) 2018/1724

I tabellen i bilaga II till förordning (EU) 2018/1724 ska posten ”Starta företag och bedriva affärsverksamhet” ersättas med följande:

Livshändelser	Förfaranden	Förväntat resultat med förbehåll för den behöriga myndighetens bedömning av ansökan i enlighet med

		nationell rätt, där så är relevant
Starta företag och bedriva affärsverksamhet	Anmälan av affärsverksamhet, tillstånd att utöva affärsverksamhet, ändring av affärsverksamhet och avslutande av affärsverksamhet utan insolvens- eller likvidationsförfaranden, undantaget inledande registrering av affärsverksamhet i företagsregistret och undantaget förfaranden för bildande eller senare anmälan av bolag i den mening som avses i artikel 54 andra stycket i EUF-fördraget	Bekräftelse på mottagande av anmälan eller ändring av eller av ansökan om tillstånd för – affärsverksamhet
	Registrera en arbetsgivare (en fysisk person) i ett obligatoriskt pensions- och försäkringssystem	Bekräftelse på registrering eller socialförsäkringsnummer
	Registrera anställda i ett obligatoriskt pensions- och försäkringssystem	Bekräftelse på registrering eller socialförsäkringsnummer
	Lämna in en bolagsskattedeklaration	Bekräftelse på mottagande av deklarationen
	Meddela socialförsäkringssystemet när en anställds kontrakt avslutas, dock ej förfaranden för kollektivt avslutande av anställningskontrakt	Bekräftelse på mottagande av meddelandet
	Betala sociala avgifter för anställda	Kvitto eller annan form av bekräftelse på betalningen av sociala avgifter för anställda
	Registrering som leverantör av dataförmedlingstjänster	Bekräftelse av registreringen
	Registrering som dataaltruismorganisation som är erkänd i unionen	Bekräftelse av registreringen

Artikel 3

Ändringar av förordning (EU) 2016/679 (den allmänna dataskyddsförordningen)

Förordning (EU) 2016/679 ska ändras på följande sätt:

1. Artikel 4 ska ändras på följande sätt:

(a) I punkt 1 ska följande meningar läggas till:

”Upplysningar som avser en fysisk person utgör inte nödvändigtvis personuppgifter för varje annan person eller enhet, enbart på grund av att en annan enhet kan identifiera den fysiska personen. Upplysningar ska inte vara

personliga för en viss enhet om enheten inte kan identifiera den fysiska person som upplysningarna avser, med beaktande av de medel som rimligen sannolikt kommer att användas av den enheten. Sådana upplysningar blir inte personliga för den enheten enbart på grund av att en potentiell efterföljande mottagare har medel som rimligen kan förväntas användas för att identifiera den fysiska person som upplysningarna avser.”

(b) Följande led ska läggas till:

”32. *terminalutrustning*: terminalutrustning enligt definitionen i artikel 1.1 i direktiv 2008/63/EG,

33. *elektroniska kommunikationsnät*: elektroniska kommunikationsnät enligt definitionen i artikel 2.1 i direktiv (EU) 2018/1972,

34. *webbläsare*: en webbläsare enligt definitionen i artikel 2.11 i förordning (EU) 2022/1925,

35. *medietjänst*: en medietjänst enligt definitionen i artikel 2.1 i förordning (EU) 2024/1083,

36. *leverantör av medietjänster*: en leverantör av medietjänster enligt definitionen i artikel 2.2 i förordning (EU) 2024/1083,

37. *onlinegränssnitt*: ett onlinegränssnitt enligt definitionen i artikel 3 m i förordning (EU) 2022/2065,

38. *vetenskaplig forskning*: all forskning som även kan stödja innovation, däribland teknisk utveckling och demonstration. Dessa insatser ska bidra till befintlig vetenskaplig kunskap eller tillämpa befintlig kunskap på nya sätt, utföras i syfte att bidra till att öka samhällets allmänna kunskap och välbefinnande samt följa etiska normer på det relevanta forskningsområdet. Detta utesluter inte att forskningen även kan syfta till att främja ett kommersiellt intresse.”

2. Artikel 5.1 b ska ersättas med följande:

”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 anses vara förenlig med de ursprungliga ändamålen, oberoende av villkoren i artikel 6.4 i denna förordning (*ändamålsbegränsning*).”

3. Artikel 9 ska ändras på följande sätt:

(a) I punkt 2 ska följande led läggas till:

”k) Behandlingen sker i samband med utveckling och drift av ett AI-system enligt definitionen i artikel 3.1 i förordning (EU) 2024/1689 eller en AI-modell, på de villkor som avses i punkt 5.

l) Behandlingen av biometriska uppgifter är nödvändig för att bekräfta en registrerad persons identitet (kontroll), om den registrerade har ensam kontroll över de biometriska uppgifter eller de medel som krävs för kontrollen.”

(b) Följande punkt ska läggas till:

”5. Vid behandling som avses punkt 2 k ska lämpliga organisatoriska och tekniska åtgärder genomföras för att undvika insamling och annan behandling av särskilda kategorier av personuppgifter. Om den personuppgiftsansvarige, trots genomförandet av sådana åtgärder, identifierar särskilda kategorier av personuppgifter i de dataset som används för träning, provning eller validering, eller i AI-systemet eller AI-modellen, ska den personuppgiftsansvarige ta bort dessa data. Om borttagningen av dessa data kräver en oproportionerlig ansträngning ska den personuppgiftsansvarige under alla omständigheter, utan onödigt dröjsmål och på ett effektivt sätt, skydda dessa data så att de inte används för att generera resultat, lämnas ut eller på annat sätt görs tillgängliga för tredje part.”

4. I artikel 12 ska punkt 5 ersättas med följande:

”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 eller även, när det gäller begäranden enligt artikel 15, på grund av att den registrerade missbrukar de rättigheter som följer av denna förordning för andra ändamål än att skydda sina uppgifter, får den personuppgiftsansvarige antingen

a) ta ut en rimlig avgift som täcker de administrativa kostnaderna för att tillhandahålla den information eller vidta den åtgärd som begärts, eller

b) vägra att tillmötesgå begäran.

Det åligger den personuppgiftsansvarige att visa att begäran är uppenbart ogrundad eller att det finns rimliga skäl att anta att den är orimlig.”

5. I artikel 13 ska punkt 4 ersättas med följande:

”4. Punkterna 1, 2 och 3 ska inte tillämpas om personuppgifterna har samlats in inom ramen för ett tydligt och avgränsat förhållande mellan registrerade och en personuppgiftsansvarig som bedriver en verksamhet som inte är dataintensiv och om det finns rimliga skäl att anta att den registrerade redan har den information som avses i punkt 1 a och c, såvida inte den personuppgiftsansvarige överför uppgifterna till andra mottagare eller kategorier av mottagare, överför uppgifterna till ett tredjeland, genomför ett automatiserat beslutsfattande, inbegripet profilering, som avses i artikel 22.1, eller om behandlingen sannolikt kommer att leda till en hög risk för de registrerades rättigheter och friheter i den mening som avses i artikel 35.”

6. I artikel 13 ska följande punkt läggas till som punkt 5:

”5. Om behandlingen äger rum för vetenskapliga forskningsändamål och tillhandahållandet av den information som avses i punkterna 1, 2 och 3 visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning, med förbehåll för de villkor och skyddsåtgärder som avses i 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 försvåra uppfyllandet av målen med den behandlingen, behöver den personuppgiftsansvarige inte tillhandahålla den information som avses i punkterna 1, 2 och 3. 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.”

7. I artikel 22 ska punkterna 1 och 2 ersättas med följande:

”1. Ett beslut som har rättsliga följder för en registrerad eller som på liknande sätt i betydande grad påverkar honom eller henne får endast grundas på automatiserad behandling, inbegripet profilering, om beslutet

a) är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och en personuppgiftsansvarig, oavsett om beslutet kan fattas på annat sätt än enbart genom automatiserade metoder,

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.”

8. Artikel 33 ska ändras på följande sätt:

(a) Punkt 1 ska ersättas med följande:

”1. Vid en personuppgiftsincident som sannolikt kommer att leda till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål och, om möjligt, senast 96 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten via den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555 till den tillsynsmyndighet som är behörig i enlighet med artiklarna 55 och 56. Om anmälan till tillsynsmyndigheten inte görs inom 96 timmar ska den åtföljas av en motivering till förseningen.”

(b) Följande punkt ska läggas till:

”1a. Fram till dess att en gemensam kontaktpunkt har inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555 ska personuppgiftsansvariga fortsätta att anmäla personuppgiftsincidenter direkt till den behöriga tillsynsmyndigheten i enlighet med artiklarna 55 och 56.”

(c) Följande punkter ska läggas till:

”6. Styrelsen ska utarbeta och till kommissionen överlämna ett förslag till en gemensam mall för anmälan av en personuppgiftsincident till den behöriga tillsynsmyndighet som avses i punkt 1 samt ett förslag till en förteckning över de omständigheter under vilka en personuppgiftsincident sannolikt kommer att leda till en hög risk för en fysisk persons rättigheter och friheter. Förslagen ska lämnas in till kommissionen senast den [Publikationsbyråns datum = nio månader efter att den här förordningen har trätt i kraft]. Kommissionen ska efter vederbörligt övervägande se över förslagen vid behov och ges befogenhet att anta dem genom en genomförandeakt i enlighet med det granskningsförfarande som anges i artikel 93.2.

7. Den mall och den förteckning som avses i punkt 6 ska ses över minst vart tredje år och uppdateras vid behov. Styrelsen ska överlämna sin bedömning och eventuella förslag om uppdateringar till kommissionen i god tid. Kommissionen ska efter vederbörligt övervägande se över förslagen och ges befogenhet att anta eventuella uppdateringar enligt förfarandet i punkt 6.”

9. Artikel 35 ska ändras på följande sätt:

(a) Punkterna 4, 5 och 6 ska ersättas med följande:

”4. Styrelsen ska utarbeta och till kommissionen överlämna ett förslag till en förteckning över de typer av behandlingar som omfattas av kravet på en konsekvensbedömning avseende dataskydd enligt punkt 1.

5. Styrelsen ska utarbeta och till kommissionen överlämna ett förslag till en förteckning över de typer av behandlingar för vilka ingen konsekvensbedömning avseende dataskydd krävs.

6. Styrelsen ska utarbeta och till kommissionen överlämna ett förslag till en gemensam mall och en gemensam metod för genomförande av konsekvensbedömningar avseende dataskydd.”

(b) Följande punkter ska införas:

”6a. Förslagen till de förteckningar som avses i punkterna 4 och 5 och till den mall och den metod som avses i punkt 6 ska lämnas in till kommissionen senast den [Publikationsbyråns datum = nio månader efter att den här förordningen har trätt i kraft]. Kommissionen ska efter vederbörligt övervägande se över dem vid behov och ges befogenhet att anta dem genom en genomförandeakt i enlighet med det granskningsförfarande som anges i artikel 93.2.

6b. De förteckningar och den mall och den metod som avses i punkt 6a ska ses över minst vart tredje år och uppdateras vid behov. Styrelsen ska överlämna sin bedömning och eventuella förslag om uppdateringar till kommissionen i god tid. Kommissionen ska efter vederbörligt övervägande se över förslagen och ges befogenhet att anta eventuella uppdateringar enligt förfarandet i punkt 6a.

6c. Förteckningar över de typer av behandlingar som omfattas av kravet på en konsekvensbedömning avseende dataskydd och de typer av behandlingar för vilka det inte krävs någon konsekvensbedömning avseende dataskydd som utarbetats och offentliggjorts av tillsynsmyndigheterna förblir giltiga fram till dess att kommissionen antar den genomförandeakt som avses i punkt 6a.”

10. Följande artikel ska läggas till:

”Artikel 41a

(1) Kommissionen får anta genomförandeakter för att ange metoder och kriterier för att fastställa om data som härrör från pseudonymisering inte längre utgör personuppgifter för vissa enheter.

(2) Vid tillämpning av punkt 1 ska kommissionen

a) bedöma användningen av den senaste tillgängliga tekniken,

b) utarbeta kriterier och/eller kategorier för personuppgiftsansvariga och mottagare för att bedöma risken för avanonymisering i förhållande till typiska mottagare av data.

(3) Genomförandet av de metoder och kriterier som anges i en genomförandeakt får användas för att visa att uppgifterna inte kan leda till avanonymisering av de registrerade.

(4) Kommissionen ska ha ett nära samarbete med Europeiska dataskyddsstyrelsen vid utarbetandet av genomförandeakterna. Europeiska dataskyddsstyrelsen ska avge ett

yttrande om utkasten till genomförandeakter inom åtta veckor efter mottagandet av utkastet från kommissionen.

(5) Genomförandeakterna ska antas i enlighet med det granskningsförfarande som avses i artikel 93.3.”

11. Artikel 57.1 ska ändras på följande sätt:

(a) Led k ska utgå.

12. I artikel 64.1 ska led a utgå.

13. I artikel 70.1 ska led h utgå.

14. I artikel 70.1 ska följande led införas:

”ha) utarbeta och till kommissionen överlämna ett förslag till en förteckning över de typer av behandlingar som omfattas av kravet på en konsekvensbedömning avseende dataskydd och de typer av behandlingar för vilka det inte krävs någon konsekvensbedömning avseende dataskydd enligt artikel 35,

hb) utarbeta och till kommissionen överlämna ett förslag till en gemensam mall och en gemensam metod för genomförande av konsekvensbedömningar avseende dataskydd enligt artikel 35,

hc) utarbeta och till kommissionen överlämna ett förslag till en gemensam mall för anmälan av en personuppgiftsincident till den behöriga tillsynsmyndigheten samt ett förslag till en förteckning över de omständigheter under vilka en personuppgiftsincident sannolikt kommer att leda till en hög risk för en fysisk persons rättigheter och friheter enligt artikel 33,"

15. Efter artikel 88 ska följande artiklar läggas till:

”Artikel 88a

Behandling av personuppgifter i fysiska personers terminalutrustning

(1) Lagring av personuppgifter eller tillgång till redan lagrade personuppgifter i en fysisk persons terminalutrustning är endast tillåten om den personen har gett sitt samtycke i enlighet med denna förordning.

(2) Punkt 1 utesluter inte lagring av personuppgifter eller tillgång till redan lagrade personuppgifter i en fysisk persons terminalutrustning, på grundval av unionsrätten eller medlemsstaternas nationella rätt i den mening som avses i, och med förbehåll för villkoren i, artikel 6, för att skydda de mål som avses i artikel 23.1.

(3) Lagring av personuppgifter eller tillgång till redan lagrade personuppgifter i en fysisk persons terminalutrustning utan samtycke, och efterföljande behandling, ska anses vara laglig i den mån den är nödvändig för att

a) överföra elektronisk kommunikation via ett elektroniskt kommunikationsnät,

b) tillhandahålla en tjänst som uttryckligen begärts av den registrerade,

c) skapa aggregerad information om användningen av en onlinetjänst för att definiera målgruppen för en sådan tjänst, om detta endast görs för eget bruk av den personuppgiftsansvarige för onlinetjänsten,

d) upprätthålla eller återställa säkerheten hos en tjänst som tillhandahålls av den personuppgiftsansvarige och som begärs av den registrerade eller den terminalutrustning som används för att tillhandahålla tjänsten.

(4) Om lagring av personuppgifter eller tillgång till redan lagrade personuppgifter i en fysisk persons terminalutrustning grundar sig på samtycke ska följande gälla:

a) Den registrerade ska kunna avslå en begäran om samtycke på ett enkelt och begripligt sätt med en enda knapp eller motsvarande medel.

b) Om den registrerade ger sitt samtycke ska den personuppgiftsansvarige inte göra en ny begäran om samtycke för samma ändamål för den period under vilken den personuppgiftsansvarige lagligen kan åberopa den registrerades samtycke.

c) Om den registrerade avslår en begäran om samtycke får den personuppgiftsansvarige inte göra en ny begäran om samtycke för samma ändamål under en period på minst sex månader.

Denna punkt ska även tillämpas på senare behandling av personuppgifter som grundar sig på samtycke.

(5) Denna artikel ska tillämpas från och med den [Publikationsbyrån: för in datum = sex månader efter dagen för den här förordningens ikraftträdande]

Artikel 88b

Automatiserade och maskinläsbara upplysningar om den registrerades val när det gäller behandling av personuppgifter i fysiska personers terminalutrustning

(1) Personuppgiftsansvariga ska säkerställa att deras onlinegränssnitt gör det möjligt för registrerade att

a) ge sitt samtycke genom automatiserade och maskinläsbara metoder, förutsatt att villkoren för samtycke i denna förordning är uppfyllda,

b) avslå en begäran om samtycke och utöva rätten att invända enligt artikel 21.2 genom automatiserade och maskinläsbara metoder.

(2) Personuppgiftsansvariga ska respektera de val som gjorts av de registrerade i enlighet med punkt 1.

(3) Punkterna 1 och 2 ska inte tillämpas på personuppgiftsansvariga som är leverantörer av medietjänster när de tillhandahåller en medietjänst.

(4) Kommissionen ska, i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012, begära att en eller flera europeiska standardiseringsorganisationer utarbetar standarder för tolkning av maskinläsbara upplysningar om de registrerades val.

Onlinegränssnitt som används av personuppgiftsansvariga och som överensstämmer med de harmoniserade standarder eller delar därav till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning* ska förutsättas överensstämma med de krav som omfattas av dessa standarder eller delar av dem, vilka anges i punkt 1.

(5) Punkterna 1 och 2 ska tillämpas från och med den [Publikationsbyrån: för in datum = 24 månader efter dagen för den här förordningens ikraftträdande].

(6) Leverantörer av webbläsare som inte är små eller medelstora företag ska tillhandahålla tekniska hjälpmedel för att göra det möjligt för registrerade att ge sitt samtycke, att avslå en begäran om samtycke och att utöva rätten att invända enligt artikel 21.2 genom de automatiserade och maskinläsbara metoder som avses i punkt 1 i den här artikeln, som de tillämpas enligt punkterna 2–5 i den här artikeln.

(7) Punkt 6 ska tillämpas från och med den [Publikationsbyrån: för in datum = 48 månader efter dagen för den här förordningens ikraftträdande].

Artikel 88c

Behandling i samband med utveckling och drift av AI

Om behandlingen av personuppgifter är nödvändig för ändamål som rör den personuppgiftsansvariges intressen i samband med utveckling och drift av ett AI-system enligt definitionen i artikel 3.1 i förordning (EU) 2024/1689 eller en AI-modell, får behandlingen utföras för berättigade intressen i den mening som avses i artikel 6.1 f i förordning (EU) 2016/679, när så är lämpligt, utom om annan unionsrätt eller nationell rätt uttryckligen kräver samtycke och om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

All sådan behandling ska omfattas av lämpliga organisatoriska och tekniska åtgärder och skyddsåtgärder för den registrerades rättigheter och friheter, däribland för att säkerställa att principen om uppgiftsminimering efterlevs i samband med valet av källor och under träningen och provningen av ett AI-system eller en AI-modell, att kvarvarande data i AI-systemet eller AI-modellen inte lämnas ut samt att de registrerade har god insyn i behandlingen av deras personuppgifter och en ovillkorlig rätt att invända mot behandlingen.”

Artikel 4

Ändringar av förordning (EU) 2018/1725 (EUDPR)

Förordning (EU) 2018/1725 ska ändras på följande sätt:

1. Artikel 3 ska ändras på följande sätt:

(a) I punkt 1 ska följande meningar läggas till:

”Upplysningar som avser en fysisk person utgör inte nödvändigtvis personuppgifter för varje annan person eller enhet, enbart på grund av att en annan enhet kan identifiera den fysiska personen. Upplysningar ska inte vara personliga för en viss enhet om enheten inte kan identifiera den fysiska person som upplysningarna avser, med beaktande av de medel som rimligen sannolikt kommer att användas av den enheten. Sådana upplysningar blir inte personliga för den enheten enbart på grund av att en potentiell efterföljande mottagare har medel som rimligen kan förväntas användas för att identifiera den fysiska person som upplysningarna avser.”

(b) Punkt 25 ska ersättas med följande:

”25. *elektroniska kommunikationsnät*: elektroniska kommunikationsnät enligt definitionen i artikel 2.1 i direktiv (EU) 2018/1972.”

(c) Följande led ska läggas till:

”27. *mobil applikation*: en mobil applikation enligt definitionen i artikel 3.2 i direktiv (EU) 2016/2102.

28. *onlinegränssnitt*: ett onlinegränssnitt enligt definitionen i artikel 3 m i förordning (EU) 2022/2065.

29. *vetenskaplig forskning*: all forskning som även kan stödja innovation, däribland teknisk utveckling och demonstration. Dessa insatser ska bidra till befintlig vetenskaplig kunskap eller tillämpa befintlig kunskap på nya sätt, utföras i syfte att bidra till att öka samhällets allmänna kunskap och välbefinnande samt följa etiska normer på det relevanta forskningsområdet. Detta utesluter inte att forskningen även kan syfta till att främja ett kommersiellt intresse.”

2. Artikel 4.1 b ska ersättas med följande:

”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 13 ska anses vara förenlig med de ursprungliga ändamålen, oberoende av villkoren i artikel 6 i denna förordning (*ändamålsbegränsning*).”

3. Artikel 10 ska ändras på följande sätt:

(a) I punkt 2 ska följande led läggas till:

”k) Behandlingen sker i samband med utveckling och drift av ett AI-system enligt definitionen i artikel 3.1 i förordning (EU) 2024/1689 eller en AI-modell, på de villkor som avses i punkt 4. .

l) Behandlingen av biometriska uppgifter är nödvändig för att bekräfta en registrerad persons identitet (kontroll), om den registrerade har ensam kontroll över de biometriska uppgifter eller de medel som krävs för kontrollen.”

(b) Följande punkt ska läggas till som punkt 4:

”4. Vid behandling som avses punkt 2 k ska lämpliga organisatoriska och tekniska åtgärder genomföras för att undvika insamling och annan behandling av särskilda kategorier av personuppgifter. Om den personuppgiftsansvarige, trots genomförandet av sådana åtgärder, identifierar särskilda kategorier av personuppgifter i de dataset som används för träning, provning eller validering, eller i AI-systemet eller AI-modellen, ska den personuppgiftsansvarige ta bort dessa data. Om borttagningen av dessa data kräver en oproportionerlig ansträngning ska den personuppgiftsansvarige under alla omständigheter, utan onödigt dröjsmål och på ett effektivt sätt, skydda dessa data så att de inte används för att generera resultat, lämnas ut eller på annat sätt görs tillgängliga för tredje part.”

4. I artikel 14 ska punkt 5 ersättas med följande:

”5. Information som tillhandahållits enligt artiklarna 15 och 16, all kommunikation och samtliga åtgärder som vidtas enligt artiklarna 17–24 och 35 ska tillhandahållas kostnadsfritt. Om begäranden från en registrerad är

uppenbart ogrundade eller orimliga, särskilt på grund av deras repetitiva art eller även, när det gäller begäranden enligt artikel 17, på grund av att den registrerade missbrukar de rättigheter som följer av denna förordning för andra ändamål än att skydda sina uppgifter, får den personuppgiftsansvarige vägra att tillmötesgå begäran. Det åligger den personuppgiftsansvarige att visa att begäran är uppenbart ogrundad eller att det finns rimliga skäl att anta att den är orimlig.”

5. I artikel 15 ska följande punkt läggas till som punkt 5:

”5. Om behandlingen äger rum för vetenskapliga forskningsändamål och tillhandahållandet av den information som avses i punkterna 1, 2 och 3 visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning, med förbehåll för de villkor och skyddsåtgärder som avses i artikel 13, eller i den mån den skyldighet som avses i punkt 1 i den här artikeln sannolikt kommer att göra det omöjligt eller avsevärt försvåra uppfyllandet av målen med den behandlingen, behöver den personuppgiftsansvarige inte tillhandahålla den information som avses i punkterna 1, 2 och 3. 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.”

6. I artikel 24 ska punkterna 1 och 2 ersättas med följande:

”1. Ett beslut som har rättsliga följder för en registrerad eller som på liknande sätt i betydande grad påverkar honom eller henne får endast grundas på automatiserad behandling, inbegripet profilering, om beslutet

a) är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och en personuppgiftsansvarig, oavsett om beslutet kan fattas på annat sätt än enbart genom automatiserade metoder,

b) tillåts enligt den unionsrätt 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.”

7. I artikel 34 ska punkt 1 ersättas med följande:

”1. Vid en personuppgiftsincident som sannolikt kommer att leda till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål och, om möjligt, senast 96 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till Europeiska datatillsynsmannen. Om anmälan till Europeiska datatillsynsmannen inte görs inom 96 timmar ska den åtföljas av en motivering till förseningen.”

8. I artikel 37 ska följande införas:

”2. Lagring av personuppgifter eller tillgång till redan lagrade personuppgifter i en fysisk persons terminalutrustning är endast tillåten om den personen har gett sitt samtycke i enlighet med denna förordning.

3. Punkt 1 utesluter inte lagring av personuppgifter eller tillgång till redan lagrade personuppgifter i en fysisk persons terminalutrustning, på grundval av

unionsrätten i den mening som avses i, och med förbehåll för villkoren i, artikel 5, för att skydda de mål som avses i artikel 25.1.

4. Lagring av personuppgifter eller tillgång till redan lagrade personuppgifter i en fysisk persons terminalutrustning utan samtycke, och efterföljande behandling, ska anses vara laglig i den mån den är nödvändig för att

a) överföra elektronisk kommunikation via ett elektroniskt kommunikationsnät,

b) tillhandahålla en tjänst som uttryckligen begärts av den registrerade,

c) skapa aggregerad information om användningen av en onlinetjänst för att definiera målgruppen för en sådan tjänst, om detta endast görs för eget bruk av den personuppgiftsansvarige för onlinetjänsten,

d) upprätthålla eller återställa säkerheten hos en tjänst som tillhandahålls av den personuppgiftsansvarige och som begärs av den registrerade eller den terminalutrustning som används för att tillhandahålla tjänsten.

5. Om lagring av personuppgifter eller tillgång till redan lagrade personuppgifter i en fysisk persons terminalutrustning grundar sig på samtycke ska följande gälla:

a) Den registrerade ska kunna avslå en begäran om samtycke på ett enkelt och begripligt sätt med en enda knapp eller motsvarande medel.

b) Om den registrerade ger sitt samtycke ska den personuppgiftsansvarige inte göra en ny begäran om samtycke för samma ändamål för den period under vilken den personuppgiftsansvarige lagligen kan åberopa den registrerades samtycke.

c) Om den registrerade avslår en begäran om samtycke får den personuppgiftsansvarige inte göra en ny begäran om samtycke för samma ändamål under en period på minst sex månader.

Denna punkt ska även tillämpas på senare behandling av personuppgifter som grundar sig på samtycke.

6. Denna artikel ska tillämpas från och med den [Publikationsbyrån: för in datum = sex månader efter dagen för den här förordningens ikraftträdande]

7. Personuppgiftsansvariga ska säkerställa att deras onlinegränssnitt gör det möjligt för registrerade att

a) ge sitt samtycke genom automatiserade och maskinläsbara metoder, förutsatt att villkoren för samtycke i denna förordning är uppfyllda,

b) avslå en begäran om samtycke genom automatiserade och maskinläsbara metoder.

8. Personuppgiftsansvariga ska respektera de val som gjorts av de registrerade i enlighet med punkt 7.

9. Onlinegränssnitt som används av personuppgiftsansvariga och som överensstämmer med de harmoniserade standarder eller delar därav som avses i artikel 88b.4 i förordning (EU) 2016/679 ska förutsättas överensstämma med

de krav som omfattas av dessa standarder eller delar av dem, vilka anges i punkt 7.

10. Punkterna 7–9 ska tillämpas från och med den [Publikationsbyrån: infoga datum = 24 månader efter dagen för denna förordnings ikraftträdande].”

(8) Artikel 39 ska ändras på följande sätt:

a) Punkt 4 ska ersättas med följande:

”4. De förteckningar, den mall och den metod som antagits av kommissionen och som avses i artikel 35.6a i förordning (EU) 2016/679 bör tillämpas vid behandlingen av personuppgifter enligt denna förordning.”

b) Punkterna 5 och 6 ska utgå.

(9) Följande artikel ska läggas till:

”Artikel 45a

De gemensamma kriterier som antagits av kommissionen och som avses i artikel 41a i förordning (EU) 2016/679 bör tillämpas vid behandling av personuppgifter enligt denna förordning.”

Artikel 5

Ändringar av direktiv 2002/58/EG (direktivet om integritet och elektronisk kommunikation)

Direktiv 2002/58/EG ska ändras på följande sätt:

1. Artikel 4 ska utgå.

2. Efter artikel 5.3 ska följande stycke läggas till:

”Denna punkt ska inte tillämpas om abonnenten eller användaren är en fysisk person och om den information som lagras eller används utgör eller leder till behandling av personuppgifter.”

Artikel 6

Ändringar av direktiv (EU) 2022/2555

Direktiv (EU) 2022/2555 ska ändras på följande sätt:

1. Följande artikel ska läggas till som artikel 23a:

”Artikel 23a

En gemensam kontaktpunkt för incidentrapportering

(1) Enisa ska utarbeta och upprätthålla en gemensam kontaktpunkt för att underlätta fullgörandet av skyldigheten att rapportera incidenter och relaterade händelser enligt de unionsrättsakter där detta föreskrivs (*den gemensamma kontaktpunkten*). Utan att det påverkar tillämpningen av artikel 16 i Europaparlamentets och rådets förordning (EU) 2024/2847 får Enisa säkerställa att den gemensamma kontaktpunkten bygger på den gemensamma rapporteringsplattform som inrättats enligt den förordningen.

(2) Enisa ska vidta lämpliga och proportionella tekniska, operativa och organisatoriska åtgärder för att hantera de risker som är förknippade med den gemensamma

kontaktpunktens säkerhet och den information som lämnas eller sprids via den gemensamma kontaktpunkten. Enisa ska ta hänsyn till känsligheten hos den information som lämnas eller sprids i enlighet med de unionsrättsakter som avses i punkt 1 och se till att behöriga myndigheter enligt dessa unionsrättsakter har tillgång till och behandlar den information som krävs enligt dessa unionsrättsakter.

(3) Enisa ska tillhandahålla och genomföra specifikationer för tekniska, operativa och organisatoriska åtgärder avseende inrättande, underhåll och säker drift av den gemensamma kontaktpunkten. Enisa ska utarbeta specifikationerna i samarbete med kommissionen, CSIRT-nätverket och de behöriga myndigheterna inom ramen för de unionsrättsakter som avses i punkt 1. Specifikationerna ska säkerställa att

a) den nödvändiga kapaciteten för interoperabilitet med avseende på andra relevanta rapporteringsskyldigheter som avses i punkt 1 säkerställs,

b) tekniska arrangemang för de relevanta entiteterna och myndigheterna enligt de unionsrättsakter som avses i punkt 1 för att få tillgång till, lämna in, inhämta, överföra eller på annat sätt behandla information från den gemensamma kontaktpunkten har införts tillsammans med tekniska protokoll och verktyg som gör det möjligt för entiteterna och myndigheterna att vidarebehandla den mottagna informationen inom sina system,

c) särdragen hos de krav på rapportering av incidenter som fastställs i de unionsrättsakter som avses i punkt 1 beaktas i vederbörlig ordning,

d) den gemensamma kontaktpunkten, i förekommande fall, är förenlig och kompatibel med de europeiska företagsplånböcker som avses i [*förslag till förordning: ange förslagets titel*] och att de europeiska företagsplånböckerna åtminstone kan användas för att identifiera och autentisera entiteter som använder den gemensamma kontaktpunkten,

e) entiteter som använder den gemensamma kontaktpunkten kan hämta och komplettera information som de tidigare har lämnat via den gemensamma kontaktpunkten,

f) en enda anmälan av information som lämnats av en entitet via den gemensamma kontaktpunkten kan användas för att uppfylla rapporteringsskyldigheterna enligt någon av de andra unionsrättsakter som föreskriver rapportering av incidenter till den gemensamma kontaktpunkten.

(4) Om inte annat föreskrivs i de unionsrättsakter som avses i punkt 1 i denna artikel ska Enisa inte ha tillgång till de anmälningar som lämnas in via den gemensamma kontaktpunkten.

(5) Inom [18] månader efter det att den här förordningen har trätt i kraft ska Enisa göra en provundersökning av hur den gemensamma kontaktpunkten fungerar för varje tillagd unionsrättsakt, däribland genom provning som utgår från de särskilda villkor och krav för anmälningar som fastställs i varje enskild unionsrättsakt och efter samråd med kommissionen och de relevanta behöriga myndigheterna i enlighet med respektive unionsrättsakt. Enisa ska inte göra det möjligt att anmäla incidenter enligt varje unionsrättsakt som avses i punkt 1 förrän efter att provundersökningen av funktionen har genomförts och efter att kommissionen har offentliggjort ett tillkännagivande i enlighet med punkt 6.

(6) Kommissionen ska, i samarbete med Enisa, bedöma den gemensamma kontaktpunktens funktion, tillförlitlighet, integritet och konfidentialitet. När

kommissionen, efter samråd med CSIRT-nätverket och de behöriga myndigheterna enligt de unionsrättsakter som avses i punkt 1, har konstaterat att den gemensamma kontaktpunkten säkerställer korrekt funktion, tillförlitlighet, integritet och konfidentialitet ska den offentliggöra ett tillkännagivande om detta i *Europeiska unionens officiella tidning*.

(7) Om kommissionen i sin bedömning konstaterar att den gemensamma kontaktpunkten inte säkerställer korrekt funktion, tillförlitlighet, integritet eller konfidentialitet ska Enisa, i samarbete med kommissionen och utan onödigt dröjsmål, vidta alla nödvändiga korrigerande åtgärder för att säkerställa korrekt funktion, tillförlitlighet, integritet eller konfidentialitet och utan dröjsmål informera kommissionen om resultaten. Därefter ska kommissionen ompröva den gemensamma kontaktpunktens funktion, tillförlitlighet, integritet eller konfidentialitet och offentliggöra ett tillkännagivande i enlighet med punkt 6.”

2. Artikel 23 ska ändras på följande sätt:

a) I punkt 1 ska första meningen ersättas med följande:

”Varje medlemsstat ska säkerställa att väsentliga och viktiga entiteter utan onödigt dröjsmål underrättar sin CSIRT-enhet eller, i tillämpliga fall, sin behöriga myndighet i enlighet med punkt 4 i denna artikel om alla incidenter som har en betydande inverkan på tillhandahållandet av deras tjänster enligt punkt 3 i denna artikel (*betydande incident*) via den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a.”

a) Följande punkt ska läggas till som punkt 12:

”Om en tillverkare anmäler en allvarlig incident enligt artikel 14.3 i förordning (EU) 2024/2847 och incidentrapporteringen enligt den artikeln innehåller relevant information i enlighet med punkt 4 i den här artikeln, ska tillverkarens rapportering enligt artikel 14.3 i förordning (EU) 2024/2847 utgöra rapportering av information enligt punkt 4 i den här artikeln.”

3. I artikel 30 ska punkt 1 ersättas med följande:

”1. Medlemsstaterna ska säkerställa att underrättelser, utöver den underrättelseskyldighet som föreskrivs i artikel 23, kan lämnas in till CSIRT-enheterna eller, i tillämpliga fall, till de behöriga myndigheterna, på frivillig basis via den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a, av

a) väsentliga och viktiga entiteter med avseende på incidenter, cyberhot och tillbud,

b) andra entiteter än de som avses i led a, oberoende av om de omfattas av detta direktiv, vad gäller om betydande incidenter, cyberhot och tillbud.”

Artikel 7

Ändring av förordning (EU) nr 910/2014

Förordning (EU) 910/2014 ska ändras på följande sätt:

1. I artikel 19a ska följande punkt införas som punkt 1a:

”1a. Anmälningar enligt punkt 1 b i den här artikeln till tillsynsorganet och, i tillämpliga fall, till andra relevanta behöriga myndigheter, ska lämnas in genom den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555.”

2. I artikel 24 ska följande punkt införas som punkt 2a:

”2a. Anmälningar enligt punkt 2 fb i den här artikeln till tillsynsorganet och, i tillämpliga fall, till andra relevanta behöriga organ, ska lämnas in genom den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555.”

3. I artikel 45a ska följande punkt införas som punkt 3a:

”3a. Anmälningar enligt punkt 3 till kommissionen och till det behöriga tillsynsorganet ska lämnas in genom den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555.”

Artikel 8

Ändringar av förordning (EU) 2022/2554

Artikel 19 i förordning (EU) 2022/2554 ska ändras på följande sätt:

1. I punkt 1 ska första stycket ersättas med följande:

”Finansiella entiteter ska rapportera allvarliga IKT-relaterade incidenter till den relevanta behöriga myndighet som avses i artikel 46 via den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555 i enlighet med punkt 4 i den här artikeln.”

2. I punkt 2 ska första stycket ersättas med följande:

”Finansiella entiteter får på frivillig basis, via den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555, rapportera betydande cyberhot till den relevanta behöriga myndigheten, när de anser att hotet är relevant för det finansiella systemet, tjänsteanvändarna eller kunderna. Den relevanta behöriga myndigheten får lämna sådan information till de andra relevanta myndigheter som avses i punkt 6.”

Artikel 9

Ändringar av direktiv (EU) 2022/2557

Artikel 15 i direktiv (EU) 2022/2557 ska ändras på följande sätt:

1. I punkt 1 ska första meningen ersättas med följande:

”Medlemsstaterna ska säkerställa att kritiska entiteter utan onödigt dröjsmål, via den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555, lämnar in en anmälan till den behöriga myndigheten om incidenter som medför en betydande störning eller kan medföra en betydande störning av tillhandahållandet av samhällsviktiga tjänster.”

2. I punkt 2 ska följande stycke läggas till:

”Kommissionen får anta genomförandeakter för att ytterligare specificera typ och format för den information som ska anmälas enligt artikel 15.1. Dessa

genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 24.2.”

Artikel 10

Upphävanden och övergångsklausuler

1. Förordning 2019/1150/EU ska upphöra att gälla med verkan från och med [datum = den här förordningens ikraftträdande].

2. Genom undantag från punkt 1 ska följande bestämmelser fortsätta att tillämpas till och med den 31 december 2032:

   (a) Artikel 2.1.

   (b) Artikel 2.2.

   (c) Artikel 2.5.

   (d) Artikel 4.

   (e) Artikel 11.

   (f) Artikel 15.

3. Följande rättsakter ska upphöra att gälla med verkan från och med den [datum, i linje med ändringarnas ikraftträdande]:

   a) Förordning (EU) 2022/868.

   b) Förordning (EU) 2018/1807.

   c) Direktiv (EU) 2019/1024.

4. Hänvisningar till förordning (EU) 2022/868, förordning (EU) 2018/1807 och direktiv 2019/1024 ska läsas i enlighet med jämförelsetabellen i bilaga I till den här förordningen.

Artikel 11

Slutbestämmelser

Denna förordning träder i kraft den tredje dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Genom undantag från punkt 3 träder artikel 5.2 i kraft sex månader efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 3.8 a–c, artikel 6.2 och 6.3 samt artiklarna 7–9 träder i kraft 18 månader efter det att den här förordningen har trätt i kraft. Genom undantag från den första meningen, om kommissionen i sin bedömning i enlighet med artikel 23a.7 i direktiv (EU) 2022/2555 finner att den gemensamma kontaktpunkten inte säkerställer korrekt funktion, tillförlitlighet, integritet eller konfidentialitet, träder den skyldighet att rapportera via den gemensamma kontaktpunkten som fastställs i artikel 23.4 i direktiv (EU) 2022/2555, artikel 19a.1a, artikel

24.2a och artikel 45a.3a i förordning (EU) 910/2014, artikel 33.1 i förordning (EU) 2016/679, artikel 19.1 och 19.2 i förordning (EU) 2022/2554 och artikel 15.1 i direktiv (EU) 2022/2557 i kraft 24 månader efter det att den här förordningen har trätt i kraft.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

FINANSIERINGSÖVERSIKT OCH DIGITAL ÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1 Förslagets eller initiativets titel

Förslag till Europaparlamentets och rådets förordning om förenkling av det digitala regelverket, om ändring av förordning (EU) 2023/2854, förordning (EU) 2016/679, förordning (EU) 2024/1689, direktiv 2002/58/EG och direktiv (EU) 2022/2555 samt om upphävande av förordning (EU) 2022/868, förordning (EU) 2018/1807, förordning (EU) 2019/1150 och direktiv (EU) 2019/1024 (digitalt omnibuspaket för det digitala regelverket)

1.2 Berörda politikområden

Kommunikationsnät, innehåll och teknik

Inre marknaden, industri, entreprenörskap samt små och medelstora företag

1.3 Mål

1.3.1Allmänt/allmänna mål

Förenkling av tillämpningen av det digitala regelverket och kostnadsbesparingar för företag

1.3.2Specifikt/specifika mål

Specifikt mål nr 1

Att förbättra styrningen och den effektiva tillämpningen av det digitala regelverket genom att minska reglernas komplexitet, sänka de administrativa kostnaderna för företag och administrationer och upphäva vissa rättsakter

Specifikt mål nr 2

Att tillhandahålla en gemensam kontaktpunkt för incidentrapportering inom flera rättsliga ramar

1.3.3Verkan eller resultat som förväntas

Beskriv den verkan som förslaget eller initiativet förväntas få på de mottagare eller den del av befolkningen som berörs.

Minskade kostnader för företag till följd av minskad komplexitet i lagstiftningen och effektivare rapportering

1.3.4Prestationsindikatorer

Ange indikatorer för övervakning av framsteg och resultat.

Indikator 1

Beräknade kostnadsminskningar för företag

Indikator 2

Kostnadsbesparingar för företagens incidentrapportering

Indikator 3

1.4 Förslaget eller initiativet avser

☐ en ny åtgärd

☐ en ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd[39]

☒ en förlängning av en befintlig åtgärd

☐ en sammanslagning eller omdirigering av en eller flera åtgärder mot en annan/en ny åtgärd

1.5 Grunder för förslaget eller initiativet

1.5.1Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet

Ikraftträdandet förväntas inom tre dagar efter offentliggörandet i Europeiska unionens officiella tidning. Tillämpningen bör inledas omedelbart, med viktiga undantag för de regler som kräver en övergångsperiod. För kapitel III om rapportering av incidenter och regler för plattformar krävs en tillräcklig genomförandeperiod som är anpassad till företagens, medlemsstaternas och EU-organens behov.

1.5.2Mervärdet av en åtgärd på EU-nivå (som kan följa av flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökad effektivitet eller komplementaritet). Med ”mervärdet av en åtgärd på EU-nivå” i detta avsnitt avses det värde en åtgärd från unionens sida tillför utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.

Skälen till att åtgärder vidtas på EU-nivå är att ändringarna rör befintlig EU-lagstiftning och minskar komplexiteten i EU-lagstiftningen (på förhand).

Det förväntade EU-mervärdet (i efterhand) består i att effektivisera EU-lagstiftningen, minska den administrativa bördan och sänka kostnaderna för företagen.

När det gäller inrättandet av den gemensamma kontaktpunkten för incidentrapportering genereras det särskilda mervärdet genom att en lösning på unionsnivå tillhandahålls för att tillgodose nationella krav. Företagens kostnader optimeras genom tillhandahållandet av en gemensam kontaktpunkt, oavsett var den rapporterande enheten har sitt säte i unionen och vilka myndigheter som har i uppdrag att ta emot rapporterna.

1.5.3Erfarenheter från tidigare liknande åtgärder

Ändringarna av de respektive förordningarna har underbyggts av den praktiska erfarenheten av genomförandet av reglerna, vilket beskrivs närmare i det åtföljande arbetsdokumentet från kommissionens avdelningar. De bygger på omfattande samråd med berörda parter, främst med inriktning på den dagliga tillämpningen av reglerna.

1.5.4Förenlighet med den fleråriga budgetramen och eventuella synergieffekter med andra relevanta instrument

Ändringarna är förenliga med den fleråriga budgetramen, eftersom inga ytterligare utgifter förväntas.

[39] I den mening som avses i artikel 58.2 a eller b i budgetförordningen.

1.5.5Bedömning av de olika finansieringsalternativ som finns att tillgå, inbegripet möjligheter till omfördelning

Ej tillämpligt

1.6 Förslagets eller initiativets varaktighet och budgetkonsekvenser

5. ☐ begränsad varaktighet

☐ verkan från och med [den DD/MM]ÅÅÅÅ till och med [den DD/MM]ÅÅÅÅ

☐ budgetkonsekvenser från och med ÅÅÅÅ till och med ÅÅÅÅ för åtagandebemyndiganden och från och med ÅÅÅÅ till och med ÅÅÅÅ för betalningsbemyndiganden.

6. ☒ obegränsad varaktighet

Efter en inledande period ÅÅÅÅ–ÅÅÅÅ,

beräknas genomförandetakten nå en stabil nivå.

1.7 Planerad(e) genomförandemetod(er)[40]

7. ☒ **Direkt förvaltning** som sköts av kommissionen

☒ via dess avdelningar, vilket också inbegriper personalen vid unionens delegationer;

☐ via genomförandeorgan

8. ☐ **Delad förvaltning** med medlemsstaterna

9. ☐ **Indirekt förvaltning** genom att uppgifter som ingår i budgetgenomförandet anförtros

☐ tredjeländer eller organ som de har utsett

☐ internationella organisationer och organ kopplade till dem (ange vilka)

☐ Europeiska investeringsbanken och Europeiska investeringsfonden

☐ organ som avses i artiklarna 70 och 71 i budgetförordningen

☐ offentligrättsliga organ

☐ privaträttsliga organ som har anförtrotts offentliga förvaltningsuppgifter i den utsträckning som de har försetts med tillräckliga ekonomiska garantier

☐ organ som omfattas av privaträtten i en medlemsstat, som anförtrotts genomförandeuppgifter inom ramen för ett offentlig-privat partnerskap och som har försetts med tillräckliga ekonomiska garantier

☐ organ eller personer som anförtrotts genomförandet av särskilda åtgärder inom den gemensamma utrikes- och säkerhetspolitiken enligt avdelning V i fördraget om Europeiska unionen och som fastställs i den grundläggande akten

☐ organ som är etablerade i en medlemsstat och som omfattas av en medlemsstats privaträtt eller unionsrätten och som i enlighet med sektorsspecifika regler kan

[40] Närmare förklaringar av de olika genomförandemetoderna med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på webbplatsen Budgpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

anförtros genomförandet av unionsmedel eller budgetgarantier, i den mån sådana organ kontrolleras av offentligrättsliga organ eller privaträttsliga organ som anförtrotts offentliga förvaltningsuppgifter och har tillräckliga finansiella garantier i form av gemensamt och solidariskt ansvar från kontrollorganens sida eller likvärdiga finansiella garantier, som för varje åtgärd kan vara begränsad till det högsta beloppet för unionens stöd.

I

2. FÖRVALTNING

2.1 Regler om uppföljning och rapportering

10. Ändringarna kommer att övervakas som en del av den ändrade lagstiftningen.

2.2 Förvaltnings- och kontrollsystem

2.2.1 Motivering av den budgetgenomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås

11. De förvaltnings- och kontrollsystem som tillämpas på den befintliga lagstiftningen säkerställer även en effektiv kontroll av ändringarna.

2.2.2 Uppgifter om identifierade risker och om det eller de interna kontrollsystem som inrättats för att begränsa riskerna

12. Inga ytterligare risker har identifierats

2.2.3 Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)

13. Kostnaden för kontroll kommer inte att skilja sig från den tidigare kostnaden

2.3 Åtgärder för att förebygga bedrägeri och oriktigheter

14. Samma förebyggande åtgärder fortsätter att vara tillämpliga för ändringarna

3. FÖRSLAGETS ELLER INITIATIVETS BERÄKNADE BUDGETKONSEKVENSER

3.1 Berörda rubriker i den fleråriga budgetramen och utgiftsposter i den årliga budgeten

Befintliga budgetposter

15. Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd

Rubrik i den fleråriga budgetramen	Budgetpost	Typ av utgifter	Bidrag			
	Nummer	Diff./Icke-diff.[41]	från Efta-länder[42]	från kandidatländer och potentiella kandidater[43]	från andra tredjeländer	övriga inkomster avsatta för särskilda ändamål
	20 02 06 Administrativa utgifter	Icke-diff.	NEJ	NEJ	NEJ	NEJ

Nya budgetposter som föreslås

16. Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd

Rubrik i den fleråriga budgetramen	Budgetpost	Typ av utgifter	Bidrag			
	Nummer	Diff./Icke-diff.	från Efta-länder	från kandidatländer och potentiella kandidater	från andra tredjeländer	övriga inkomster avsatta för särskilda ändamål

[41] Differentierade respektive icke-differentierade anslag.
[42] Efta: Europeiska frihandelssammanslutningen.
[43] Kandidatländer och i förekommande fall potentiella kandidater i västra Balkan.

3.2 Förslagets beräknade budgetkonsekvenser för anslagen

3.2.1 Sammanfattning av beräknad inverkan på driftsanslagen

☒ Förslaget/initiativet kräver inte att driftsanslag tas i anspråk

☐ Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

3.2.1.1 Anslag i den antagna budgeten

Miljoner EUR (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	Nummer	

GD: <…….>			År **2024**	År **2025**	År **2026**	År **2027**	**TOTALT Budgetram 2021–2027**
Driftsanslag							
Budgetpost	Åtaganden	(1a)					**0,000**
	Betalningar	(2a)					**0,000**
Budgetpost	Åtaganden	(1b)					**0,000**
	Betalningar	(2b)					**0,000**
Anslag av administrativ natur som finansieras genom ramanslagen för särskilda program[44]							
Budgetpost		(3)					**0,000**
TOTALA anslag för GD <…….>	Åtaganden	=1a+1b+3	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
	Betalningar	=2a+2b+3	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

[44] Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

==========

Detta avsnitt ska fyllas i med hjälp av det datablad för budgetuppgifter av administrativ natur som först ska föras in i bilagan till finansierings- och digitaliseringsöversikt för rättsakt (bilaga 5[45] till kommissionens beslut om interna bestämmelser för genomförandet av kommissionens avsnitt av Europeiska unionens allmänna budget), vilken ska laddas upp i DECIDE som underlag för samråden mellan kommissionens avdelningar.

GD: <…….>		År **2024**	År **2025**	År **2026**	År **2027**	**TOTALT Budgetram 2021–2027**
• Personalresurser		0,000	0,000	0,000	0,000	**0,000**
• Övriga administrativa utgifter		0,000	0,000	0,000	0,000	**0,000**
TOTALT GD <…….>	Anslag	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

GD: <…….>		År **2024**	År **2025**	År **2026**	År **2027**	**TOTALT Budgetram 2021–2027**
• Personalresurser		0,000	0,000	0,000	0,000	**0,000**
• Övriga administrativa utgifter		0,000	0,000	0,000	0,000	**0,000**
TOTALT GD <…….>	Anslag	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

TOTALA anslag för RUBRIK 7 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

Miljoner EUR (avrundat till tre decimaler)

	År	År	År	År	**TOTALT**

[45] Om du rapporterar användningen av anslag under rubrik 7 är det obligatoriskt att fylla i bilaga 5.

		2024	2025	2026	2027	Budgetram 2021–2027
TOTALA anslag för RUBRIKERNA 1–7	Åtaganden	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
i den fleråriga budgetramen	Betalningar	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

3.2.1.2 Anslag från externa inkomster avsatta för särskilda ändamål

Miljoner EUR (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	Nummer	

GD: <…….>			År	År	År	År	TOTALT Budgetram
			2024	**2025**	**2026**	**2027**	**2021–2027**
Driftsanslag							
Budgetpost	Åtaganden	(1a)					**0,000**
	Betalningar	(2a)					**0,000**
Budgetpost	Åtaganden	(1b)					**0,000**
	Betalningar	(2b)					**0,000**
Anslag av administrativ natur som finansieras genom ramanslagen för särskilda program[46]							
Budgetpost		(3)					**0,000**
TOTALA anslag för GD <…….>	Åtaganden	=1a+1b+3	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
	Betalningar	=2a+2b+3	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

[46] Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

Rubrik i den fleråriga budgetramen	**7**	”Administrativa utgifter”[47]

Miljoner EUR (avrundat till tre decimaler)

GD: <…….>		År **2024**	År **2025**	År **2026**	År **2027**	**TOTALT Budgetram 2021–2027**
• Personalresurser		0,000	0,000	0,000	0,000	**0,000**
• Övriga administrativa utgifter		0,000	0,000	0,000	0,000	**0,000**
TOTALT GD <…….>	Anslag	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

GD: <…….>		År **2024**	År **2025**	År **2026**	År **2027**	**TOTALT Budgetram 2021–2027**
• Personalresurser		0,000	0,000	0,000	0,000	**0,000**
• Övriga administrativa utgifter		0,000	0,000	0,000	0,000	**0,000**
TOTALT GD <…….>	Anslag	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

TOTALA anslag för RUBRIK 7 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

Miljoner EUR (avrundat till tre decimaler)

	År **2024**	År **2025**	År **2026**	År **2027**	**TOTALT Budgetram 2021–2027**

[47] Nödvändiga anslag bör beräknas med hjälp av årsmedelkostnaderna på tillämplig webbsida i BUDGpedia.

TOTALA anslag för RUBRIKERNA 1–7	Åtaganden	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
i den fleråriga budgetramen	Betalningar	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

3.2.2 Beräknad output som finansierats med driftsanslag (ska inte fyllas i för decentraliserade byråer)

Åtagandebemyndiganden i miljoner EUR (avrundat till tre decimaler)

Ange mål och output ⇩			År **2024**		År **2025**		År **2026**		År **2027**		För in så många år som behövs för att redovisa hur länge resursanvändningen påverkas (jfr avsnitt 1.6)						**TOTALT**	
	OUTPUT																	
	Typ[48]	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 1[49]…																		
- Output																		
- Output																		
- Output																		
Delsumma för specifikt mål nr 1																		
SPECIFIKT MÅL nr 2…																		

[48] Output som ska anges är de produkter eller tjänster som levererats (t.ex. antal studentutbyten som har finansierats eller antal kilometer väg som har byggts).
[49] Mål som redovisats under avsnitt 1.3.2: ”Specifikt/specifika mål”

- Output																		
Delsumma för specifikt mål nr 2																		
TOTALT																		

3.2.3 Sammanfattning av beräknad inverkan på de administrativa anslagen

☒ Förslaget/initiativet kräver inte att anslag av administrativ natur tas i anspråk

☐ Förslaget/initiativet kräver att anslag av administrativ natur tas i anspråk enligt följande:

3.2.3.1 Anslag i den antagna budgeten

ANTAGNA ANSLAG	År **2024**	År **2025**	År **2026**	År **2027**	**TOTALT 2021–2027**
RUBRIK 7					
Personalresurser	0,000	0,000	0,000	0,000	**0,000**
Övriga administrativa utgifter	0,000	0,000	0,000	0,000	**0,000**
Delsumma för RUBRIK 7	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
Utanför RUBRIK 7					
Personalresurser	0,000	0,000	0,000	0,000	**0,000**
Andra utgifter av administrativ natur	0,000	0,000	0,000	0,000	**0,000**
Delsumma utanför RUBRIK 7	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
TOTALT	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

Personalbehov och andra utgifter av administrativ natur ska täckas genom anslag inom generaldirektoratet som redan har avdelats för att förvalta åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, samt vid behov kompletterat med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

3.2.4 Beräknat personalbehov

☒ Förslaget/initiativet kräver inte att personalresurser tas i anspråk

☐ Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

3.2.4.1 Finansierat med den antagna budgeten

Beräkningarna ska anges i heltidsekvivalenter[50]

17.

ANTAGNA ANSLAG	År **2024**	År **2025**	År **2026**	År **2027**
• Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)				
20 01 02 01 (vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna)	0	0	0	0
20 01 02 03 (EU:s delegationer)	0	0	0	0
01 01 01 01 (indirekta forskningsåtgärder)	0	0	0	0
01 01 01 11 (direkta forskningsåtgärder)	0	0	0	0

[50] Ange i tabellen nedan hur många heltidsekvivalenter av det angivna antalet som redan är avdelade för förvaltning av åtgärden och/eller kan omfördelas inom ditt GD och vad ditt nettobehov är.

Andra budgetposter (ange vilka)		0	0	0	0
• Extern personal (heltidsekvivalenter)					
20 02 01 (kontraktsanställda och nationella experter finansierade genom ramanslaget)		0	0	0	0
20 02 03 (kontraktsanställda, lokalanställda, nationella experter och unga experter som tjänstgör vid EU:s delegationer)		0	0	0	0
Post för admin. stöd	- vid huvudkontoret	0	0	0	0
[XX.01.YY.YY]	- vid EU:s delegationer	0	0	0	0
01 01 01 02 (kontraktsanställda och nationella experter – indirekta forskningsåtgärder)		0	0	0	0
01 01 01 12 (kontraktsanställda och nationella experter – direkta forskningsåtgärder)		0	0	0	0
Andra budgetposter (ange vilka) – rubrik 7		0	0	0	0
Andra budgetposter (ange vilka) – utanför rubrik 7		0	0	0	0
TOTALT		**0**	**0**	**0**	**0**

3.2.5 Översikt över beräknad inverkan på it-relaterade investeringar

18. Obligatoriskt: Bästa tillgängliga skattning av de it-relaterade investeringar som förslaget/initiativet medför ska anges i tabellen nedan.

19. När så krävs för genomförandet av förslaget/initiativet ska i undantagsfall anslag under rubrik 7 anges på därför avsedd rad.

20. Anslagen under rubrikerna 1–6 ska redovisas som ”It-utgifter inom operativa program som inte omfattas av kommissionens administrativa självständighet och institutionella befogenheter" Dessa utgifter avser den driftsbudget som tas i anspråk för att återanvända/köpa in/utveckla it-plattformar och it-verktyg med direkt koppling till initiativets genomförande med tillhörande investeringar (t.ex. licenser, undersökningar och datalagring). Uppgifterna i den här tabellen bör vara förenliga med uppgifterna i avsnitt 4, ”Digitala inslag”.

TOTALT Anslag för digital teknik och it	År **2024**	År **2025**	År **2026**	År **2027**	**TOTALT Budgetram 2021–2027**
RUBRIK 7					
It-utgifter (centralt)	0,000	0,000	0,000	0,000	**0,000**
Delsumma för RUBRIK 7	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
Utanför RUBRIK 7					
It-utgifter inom operativa program som inte omfattas av kommissionens administrativa självständighet och institutionella befogenheter	0,000	0,000	0,000	0,000	**0,000**
Delsumma utanför RUBRIK 7	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
TOTALT	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

3.2.6 Förenlighet med den gällande fleråriga budgetramen

21. Förslaget/initiativet

☒ kan finansieras fullständigt genom omfördelningar inom den berörda rubriken i den fleråriga budgetramen

☐ kräver användning av den outnyttjade marginalen under den relevanta rubriken i den fleråriga budgetramen och/eller användning av särskilda instrument enligt definitionen i förordningen om den fleråriga budgetramen

☐ kräver en översyn av den fleråriga budgetramen

3.2.7 Bidrag från tredje part

22. Förslaget/initiativet

☒ innehåller inga bestämmelser om samfinansiering från tredje parter

☐ innehåller bestämmelser om samfinansiering från tredje parter enligt följande uppskattning:

Anslag i miljoner euro (avrundat till tre decimaler)

	År **2024**	År **2025**	År **2026**	År **2027**	Totalt
Ange vilket organ som deltar i samfinansieringen					
TOTALA anslag som tillförs genom samfinansiering					

3.3 Beräknad inverkan på inkomsterna

☒ Förslaget/initiativet påverkar inte inkomsterna.

– ☐ Förslaget/initiativet påverkar inkomsterna på följande sätt:

– ☐ Påverkan på egna medel

– ☐ Påverkan på andra inkomster

– ☐ Ange om inkomsterna är avsatta för särskilda utgiftsposter

Miljoner EUR (avrundat till tre decimaler)

Inkomstposter i den årliga budgeten:	Belopp som förts in för det innevarande budgetåret	Förslagets/initiativets inverkan på inkomsterna[51]			
		År **2024**	År **2025**	År **2026**	År **2027**
Artikel …….					

23. För inkomster avsatta för särskilda ändamål, ange vilka utgiftsposter i budgeten som berörs.

24. […]

[51] Vad gäller traditionella egna medel (tullar, sockeravgifter) ska nettobeloppen anges, dvs. bruttobeloppen minus 20 % avdrag för uppbördskostnader.

25. Övriga anmärkningar (t.ex. vilken metod/formel som har använts för att beräkna inverkan på inkomsterna eller andra relevanta uppgifter).

26. […]

27. 4. DIGITALA INSLAG

4.1 Krav med digital relevans

Beskriv på ett övergripande sätt kraven med digital relevans och relevanta kategorier (data, processdigitalisering och processautomatisering, digitala lösningar och/eller digitala offentliga tjänster)

Hänvisning till kravet	**Beskrivning av kravet**	**Aktörer som påverkas eller berörs av kravet**	**Övergripande processer**	**Kategorier**
Artikel 1	Ändring av artikel 1.1 i dataförordningen, genom att utvidga dess tillämpningsområde till att omfatta följande: • En ram för registrering av dataförmedlingstjänster. • En ram för frivillig registrering av enheter som samlar in och behandlar data som tillhandahålls för altruistiska ändamål. • En ram för inrättandet av en europeisk datainnovationsstyrelse.	Europeiska kommissionen Dataförmedlingstjänster Enheter som samlar in och behandlar data	Utvidgning av dataförordningens tillämpningsområde	Digitala offentliga tjänster
Artikel 1	Ändring av artiklarna 4.8 och 5.11 i dataförordningen. Datahållare som vägrar att dela data enligt undantaget för företagshemligheter ska på lämpligt sätt meddela ett sådant beslut.	Datahållare (innehavare av företagshemlighet) Aktörer som begärt tillgång	Anmälan	Data

Artikel 1	Införande av artikel 15a i dataförordningen. Skyldighet att göra data tillgängliga i ett allmänt nödläge.	Offentligt organ Europeiska kommissionen Europeiska centralbanken Unionsorgan Datahållare	Göra data tillgängliga	Data
Artikel 1	Ändring av artikel 21.5 i dataförordningen. Krav avseende delning av data som erhållits i samband med ett allmänt nödläge med forskningsorganisationer eller statistikorgan. Införande av artikel 22a i dataförordningen om inlämning av klagomål avseende kapitel V (*”Göra data tillgängliga för offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan på grundval av ett exceptionellt behov”*).	Offentligt organ Europeiska kommissionen Europeiska centralbanken Unionsorgan Datahållare Nationell behörig myndighet	Datadelning Klagomål	Data

Artikel 1	Ändringar av artikel 32.1–32.5 i dataförordningen om tredje lands tillgång till andra data än personuppgifter.	Leverantörer av databehandlingstjänster Leverantörer av dataförmedlingstjänster Dataaltruismorganisationer Nationella organ eller myndigheter	Internationell statlig åtkomst och överföring av data	Data Digitala offentliga tjänster
Artikel 1	Ändring av artikel 35.5 i dataförordningen för att göra det möjligt för kommissionen att anta gemensamma specifikationer för interoperabla databehandlingstjänster.	Leverantörer av databehandlingstjänster Europeiska kommissionen	Antagande av gemensamma specifikationer	Digitala offentliga tjänster
Artikel 1	Ändringar av artiklarna 32a–32e i dataförordningen för att införa kapitel VIIa om regelverket för en europeisk märkning för dataförmedlingstjänster, inbegripet anmälan, upprättande av ett offentligt register, villkor för tillhandahållande av tjänster, utnämning av behöriga myndigheter samt övervakning av efterlevnaden Ändringar av artikel 32h i dataförordningen för att införa kapitel VIIb om det fria flödet av data inom unionen, inbegripet förbud	Leverantörer av dataförmedlingstjänster Registrerade, datahållare, dataanvändare Medlemsstaterna Behöriga myndigheter Europeiska kommissionen	Inrättande av en europeisk märkning för dataförmedlingstjänster Inrättande av fri rörlighet för data inom Europeiska unionen	Data Digital lösning Digitalisering av processer Digitala offentliga tjänster

	mot datalokaliseringskrav, krav på anmälan till kommissionen och offentliggörande av en konsoliderad förteckning.			
Artikel 1	Ändringar av artikel 32h i dataförordningen för att införa kapitel VIIb om det fria flödet av data inom unionen, inbegripet förbud mot datalokaliseringskrav, krav på anmälan till kommissionen och offentliggörande av en konsoliderad förteckning.	Medlemsstaterna Europeiska kommissionen	Inrättande av fri rörlighet för data inom Europeiska unionen	Data Digitalisering av processer Digitala offentliga tjänster
Artikel 1	Införande av artikel 32i i dataförordningen för att fastställa tillämpningsområdet för kapitel VIIc. I kapitlet fastställs en uppsättning minimiregler för vidareutnyttjande och praktiska arrangemang för att underlätta vidareutnyttjande av data. Införande av artikel 32j i dataförordningen. Bestämmelser om	Medlemsstaterna Datahållare Dataanvändare	Fastställande av syfte och tillämpningsområde Icke-diskriminering	Digitala offentliga tjänster

	icke-diskriminering vad gäller vidareutnyttjande av data och handlingar.			
Artikel 1	Införande av artikel 32k i dataförordningen. Regler om exklusiva avtal för vidareutnyttjande av data. Inbegriper skyldigheten att offentliggöra de slutgiltiga villkoren för avtalen.	Potentiella aktörer på marknaden Offentliga organ Avtalsslutande parter		Digitala offentliga tjänster Data
Artikel 1	Ändringar av dataförordningen: • (41): Införande av artikel 32n om den allmänna principen för vidareutnyttjande av öppna offentliga data • (42): Införande av artikel 32o om behandling av begäranden om vidareutnyttjande av data • (43): Införande artikel 32p om format för vidareutnyttjande av data • (46): Införande av artikel 32s om praktiska arrangemang för att underlätta sökningen efter data eller handlingar som är tillgängliga för vidareutnyttjande	Datahållare Dataanvändare Medlemsstater (offentliga organ) Europeiska kommissionen	Regler för vidareutnyttjande av data	Digitala offentliga tjänster Data Digitalisering av processer

Artikel 1	Införande av artikel 32t i dataförordningen. Krav på att stödja tillgången till forskningsdata.	Medlemsstaterna Forskningsorganisationer Dataanvändare	Regler för vidareutnyttjande av data	Digitala offentliga tjänster Data
Artikel 1	Införande av artikel 32u i dataförordningen. Fastställande av arrangemang för offentliggörande och vidareutnyttjande av särskilda värdefulla dataset.	Europeiska kommissionen Offentliga organ, offentliga företag	Regler för vidareutnyttjande av data	Digitala offentliga tjänster Data
Artikel 1	Införande av artikel 32w i dataförordningen. Fastställande av villkor för vidareutnyttjande av vissa kategorier av data. Förfarandena för att begära och villkoren för att tillåta sådant vidareutnyttjande ska göras tillgängliga för allmänheten via den gemensamma informationspunkten.	Offentliga organ Dataanvändare	Regler för vidareutnyttjande av data	Digitala offentliga tjänster Data
Artikel 1	Införande av artikel 32x i dataförordningen. Krav för vidareutnyttjares överföring av icke-personuppgifter till tredjeländer.	Aktörer som vidareutnyttjar data Offentliga organ Fysiska/juridiska personer vars rättigheter kan påverkas	Överföring av data till tredjeländer	Digitala offentliga tjänster Data
Artikel 1	Ändringar av dataförordningen: • (55): Införande av artikel 32z. Organisatoriska åtgärder som rör behöriga organ.	Behöriga organ Medlemsstaterna Offentliga organ	Inrättande av behöriga organ Förfaranden för	Digitala offentliga tjänster Data

	• (57): Införande av artikel 32ab om förfaranden för begäranden om vidareutnyttjande av data. • (58): Ersättning av artikel 38.1–38.2 om rätten att inge ett klagomål.		begäranden Klagomål	
Artikel 1	Införande av artikel 32aa i dataförordningen. Föreskrifter för användningen av en gemensam informationspunkt för att underlätta vidareutnyttjande av data.	Medlemsstaterna Datahållare Dataanvändare Europeiska kommissionen.	Inrättande av en gemensam åtkomstpunkt	Digitala lösningar Digitala offentliga tjänster Digitalisering av processer Data

Artikel 1	Ändringar av artiklarna 41a, 42, 45, 46, 48a, 49 och 49a i dataförordningen för att införa kapitel IXa om inrättande av Europeiska datainnovationsstyrelsen (EDIB) som en expertgrupp för att samordna tillämpningen och underlätta utvecklingen av en europeisk dataekonomi, inbegripet krav på sammansättning, roll, samarbete mellan behöriga myndigheter och stöd till en konsekvent tillämpning av rättsliga krav.	Europeiska kommissionen, Europeiska datainnovationsstyrelsen (EDIB) Företrädare för medlemsstaterna med behörighet inom politiken för dataekonomi Behöriga myndigheter för tillämpningen av kapitlen II, III och V Behöriga myndigheter för vidareutnyttjande av information från den offentliga sektorn (direktivet om öppna data) Behöriga myndigheter för dataförmedlingstjänster Behöriga myndigheter för registrering av dataaltruismorganisationer Europeiska dataskyddsstyrelsen (EDPB), Europeiska datatillsynsmannen (EDPS) Enisa (Europeiska unionens cybersäkerhetsbyrå) EU-företrädaren för små och	Inrättande av Europeiska datainnovationsstyrelsen (EDIB)	Digitala offentliga tjänster Data

		medelstora företag eller en representant från nätverket av företrädare för små och medelstora företag Andra företrädare för relevanta organ inom specifika sektorer Organ med specifik sakkunskap Standardiseringsorganisationer Europaparlamentet, Europeiska unionens råd, Europeiska ekonomiska och sociala kommittén Leverantörer av dataförmedlingstjänster Erkända dataaltruismorganisationer		
Artikel 3	Ändring av artikel 33 i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) vad gäller anmälningar om personuppgiftsincidenter. Föreskriver bland annat användningen av den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555 och användning av anmälningsmallar.	Registrerade Personuppgiftsansvariga Tillsynsmyndigheter Europeiska dataskyddsstyrelsen Europeiska kommissionen	Anmälan	Data

Artikel 3	Ändring av artiklarna 35 och 70.1 i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen). Krav på att Europeiska dataskyddsstyrelsen ska överlämna förslag till kommissionen om att omsätta vissa aspekter av konsekvensbedömningen avseende dataskydd i praktiken. Dessa omfattar en gemensam mall för sådana bedömningar.	Europeiska dataskyddsstyrelsen Europeiska kommissionen	Förslag från styrelsen som översänts till kommissionen	Data
Artikel 3	Införande av artikel 88b i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen). De registrerade ska kunna ge sitt samtycke eller utöva rätten att göra invändningar genom automatiserade och maskinläsbara metoder. Standarder ska utarbetas av en eller flera europeiska standardiseringsorganisationer.	Registrerade Personuppgiftsansvariga Europeiska standardiseringsorganisationer. Europeiska kommissionen	Automatiserade och maskinläsbara upplysningar om den registrerades val	Digitala lösningar Processautomatisering

Artikel 6	Ändring av direktiv (EU) 2022/2555 (NIS2-direktivet): • (1): Införande av artikel 23a om utarbetande och upprätthållande av en gemensam kontaktpunkt för incidentrapportering. • (3): Ändring av artikel 23.4 för att föreskriva användningen av en gemensam kontaktpunkt för anmälningar om allvarliga incidenter. • (4): Införande av artikel 23.12, vilket säkerställer att allvarliga incidenter endast rapporteras en gång (antingen enligt NIS2-direktivet eller enligt cyberresiliensförordningen). • (5): Ändring av artikel 30.1 för att säkerställa att den gemensamma kontaktpunkten kan användas på frivillig basis för anmälningar från olika entiteter.	Anmälare (väsentliga och viktiga entiteter) CSIRT-enheter/behöriga myndigheter (i tillämpliga fall) Europeiska kommissionen Enisa	Anmälan	Data Digitala lösningar Digitala offentliga tjänster
Artikel 7	Ändring av förordning (EU) 910/2014 (om den europeiska digitala identitetsplånboken) angående krav på användningen av	Anmälare (icke-kvalificerade tillhandahållare av betrodda tjänster, kvalificerade tillhandahållare av betrodda	Anmälan	Data

	en gemensam kontaktpunkt, i enlighet med artikel 23a i direktiv (EU) 2022/2555, för: • Artikel 19a.1a: Anmälningar som avses i punkt 1 b. • Artikel 24.2a: Anmälningar som avses i punkt 2 fb. Artikel 45a.3a: Anmälningar som avses i punkt 3.	tjänster, leverantörer av webbläsare) Tillsynsorgan Andra relevanta behöriga organ eller myndigheter Europeiska kommissionen		
Artikel 8	Ändring av förordning (EU) 2022/2554 (DORA-förordningen) angående krav på användning av en gemensam kontaktpunkt, i enlighet med artikel 23a i direktiv (EU) 2022/2555, för: • Artikel 19.1: Allvarliga IKT-relaterade incidenter • Artikel 19.2: Frivilliga anmälningar av betydande cyberhot.	Anmälare (finansiella enheter) Tillsynsorgan Andra relevanta behöriga organ eller myndigheter Europeiska kommissionen Enisa	Anmälan	Data

Artikel 9	Ändring av direktiv (EU) 2022/2557 (CER-direktivet) angående krav på användning av en gemensam kontaktpunkt, i enlighet med artikel 23a i direktiv (EU) 2022/2555, för: • Artikel 15.1: Incidenter som medför en betydande störning eller kan medföra en betydande störning av tillhandahållandet av samhällsviktiga tjänster.	Anmälare (kritiska entiteter) Tillsynsorgan Andra relevanta behöriga organ eller myndigheter Europeiska kommissionen Enisa	Anmälan	Data

4.2 Data

Övergripande beskrivning av data som omfattas

Typ av data	**Hänvisning till kravet/kraven**	**Standard och/eller specifikation (i tillämpliga fall)**
Avslag på en begäran om tillgång till data på grundval av undantaget avseende företagshemligheter (*och anmälan om detta till den behöriga myndigheten*)	Artikel 1	Ska vara vederbörligen underbyggt på grundval av objektiva faktorer.
Data som ska göras tillgängliga i samband med ett allmänt nödläge	Artikel 1	Inbegriper de metadata som krävs för att tolka och använda data. När det gäller personuppgifter ska de om möjligt pseudonymiseras.
Anmälan av avsikt att göra data tillgängliga i ett allmänt nödläge	Artikel 1	Uppgift om identitet och kontaktuppgifter för den organisation eller enskilda person som tar emot data, syftet med överföringen eller tillhandahållandet av data, den period under vilken datauppgifterna ska användas samt de tekniska skyddsåtgärder och organisatoriska åtgärder som vidtagits.
Klagomål enligt kapitel V (”*Göra data tillgängliga för offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan på grundval av ett exceptionellt behov*”)	Artikel 1	//
Icke-personuppgifter som innehas i Europeiska unionen	Artikel 1	//

Data som ska tillhandahållas som svar på en begäran om vidareutnyttjande	Artikel 1	Att tillhandahålla minsta tillåtna datamängd
Meddelande om begäran om vidareutnyttjande av data som ska beviljas inom kort	Artikel 1	//
Data för vilka förmedlingstjänster tillhandahålls (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1	Format som tagits emot från den registrerade/datahållaren. Omvandlingar endast för att förbättra interoperabiliteten eller uppfylla internationella/europeiska datastandarder
Information om dataanvändning och datatermer (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1	Ska tillhandahållas på ett kortfattat, transparent, begripligt och lättåtkomligt sätt
Ansökningar om registrering i det offentliga unionsregistret och ändringar av anmälda uppgifter (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1	De behöriga myndigheterna ska ta fram nödvändiga ansökningsblanketter.
Godkända ansökningar om registrering som ska läggas till i det offentliga unionsregistret (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1	//
Meddelande om senare ändringar av den information som lämnats under ansökningsprocessen (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1	//
Mottagande av meddelande om senare ändringar (europeisk märkning för dataförmedlingstjänster	Artikel 1	//

och dataaltruismorganisationer)		
Information som lämnats till registrerade/datahållare före behandling (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1	//
Samtycke (eller återkallande av samtycke) till databehandling av en erkänd dataaltruismorganisation (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1	Ska inhämtas på elektronisk väg
Information om den jurisdiktion i tredjeland där dataanvändningen är avsedd att äga rum	Artikel 1	//
Anmälan av obehörig överföring, åtkomst eller användning av icke-personuppgifter (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1	//
Information för övervakning av efterlevnaden (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1	Begärandena måste vara proportionerliga och motiverade
Anmälan av bristande efterlevnad (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1	//
Beslut att återkalla rätten att använda märkningen (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1	//

Utkast till rättsakter om datalokaliseringskrav	Artikel 1	//
De slutgiltiga villkoren för exklusiva avtal	Artikel 1	//
Data (och/eller anmälningar) som rör en begäran om vidareutnyttjande	Artikel 1	I alla befintliga format eller språk och, där så är möjligt och lämpligt, på elektronisk väg, i format som är öppna, maskinläsbara, tillgängliga, sökbara och möjliga att vidareutnyttja, tillsammans med deras metadata.
Offentligt finansierade forskningsdata	Artikel 1	Öppet tillgängliga enligt principen ”öppenhet som standard” och förenliga med Fair-principerna.
Särskilda värdefulla dataset	Artikel 1	Tillgängliga utan kostnad, maskinläsbara, utlämnade via API:er och som en bulknedladdning (i förekommande fall). Genomförandeakter som ska följas, dessa kan omfatta format för data och metadata.
Villkor för att tillåta vidareutnyttjande av data eller handlingar som avses i artikel 2.54	Artikel 1	Tillgängliga för allmänheten.
Meddelande om obehörigt vidareutnyttjande av icke-personuppgifter	Artikel 1	//
Anmälan om avsikt att överföra icke-personuppgifter till ett tredjeland och syftet med en denna överföring (*till det offentliga organet*)	Artikel 1	//
Anmälan om avsikt att överföra icke-	Artikel 1	//

personuppgifter till ett tredjeland, syftet med denna överföring och lämpliga skyddsåtgärder (*till den fysiska eller juridiska person vars rättigheter och intressen kan påverkas*)		
All relevant information om tillämpningen av artiklarna 32z [villkor för vidareutnyttjande], 32aa [tredjeländer] och 32ab [avgifter] i dataförordningen	Artikel 1	Tillgängliga och lättåtkomliga via en gemensam informationspunkt.
Klagomål från fysiska eller juridiska personer om deras rättigheter enligt dataförordningen har överträtts eller andra relevanta frågor	Artikel 1	//
Information om hur förfarandet eller tillämpningen av rättsmedel fortskrider i samband med klagomål enligt dataförordningen	Artikel 1	//
Data om erfarenheter och god praxis (EDIB)	Artikel 1	//
Utvärdering av kapitlen II, III, IV, V, VI, VII och VIII i dataförordningen Utvärdering av kapitlen VIIa, VIIb och VIIc i dataförordningen	Artikel 1 Artikel 1	Minimikrav för innehållet i rapporter anges.
Anmälningar om personuppgiftsincidenter	Artikel 3	Via (och därmed i enlighet med specifikationerna för) den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555. Europeiska dataskyddsstyrelsen ska utarbeta ett förslag till en gemensam mall (*se nästa post*).

Europeiska dataskyddsstyrelsens förslag till en gemensam mall för anmälan av uppgiftsincidenter	Artikel 3	//
Europeiska dataskyddsstyrelsens förslag om konsekvensbedömning av dataskydd	Artikel 3	//
Rapporter om allvarliga incidenter i enlighet med NIS2-direktivet	Artikel 6	Via (och därmed i enlighet med specifikationerna för) den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555.
Anmälningar om personuppgiftsincidenter	Artikel 3	Via (och därmed i enlighet med specifikationerna för) den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555
Anmälningar om allvarliga IKT-relaterade incidenter i enlighet med DORA-förordningen. Frivilliga anmälningar om betydande cyberhot i enlighet med DORA-förordningen	Artikel 8	Via (och därmed i enlighet med specifikationerna för) den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555
Anmälningar om incidenter som medför en betydande störning eller kan medföra en betydande störning av tillhandahållandet av samhällsviktiga tjänster, enligt CER-direktivet	Artikel 9	Via (och därmed i enlighet med specifikationerna för) den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555

Överensstämmelse med EU:s datastrategi

Förklara hur kravet/kraven överensstämmer med EU:s datastrategi

Genom dessa ändringar av dataförordningen införs Europeiska datainnovationsstyrelsen (EDIB) (kapitel IXa), som ska samordna tillämpningen av regler och utarbeta riktlinjer för sektorsvisa gemensamma europeiska dataområden. Den europeiska märkningen för dataförmedlingstjänster och dataaltruismorganisationer (kapitel VIIa) skapar ett tillförlitligt ekosystem för datadelning och skydd av rättigheter. Genom kapitel VIIb genomförs det fria flödet av andra data än personuppgifter genom att förbjuda omotiverade

datalokaliseringskrav. I kapitel VIIc anpassas reglerna för vidareutnyttjande av data från den offentliga sektorn genom att slå samman bestämmelserna i direktivet om öppna data och dataförvaltningsakten. Reglerna för internationella överföringar av data stärker den europeiska digitala suveräniteten genom att skydda data från obehörig åtkomst av tredjeländer. Slutligen säkerställer undantagen för små och medelstora företag och deltagandet av EU:s företrädare för små och medelstora företag i EDIB att dataekonomin är mer tillgänglig även för små företag.

Överensstämmelse med engångsprincipen

Förklara hur engångsprincipen har beaktats och hur möjligheten att återanvända befintliga data har utforskats

Dessa ändringar stöder engångsprincipen genom att skapa en infrastruktur för effektivt vidareutnyttjande av data: EDIB utarbetar interoperabilitetsstandarder för gemensamma europeiska dataområden för att minska tillhandahållandet av dubblerade data. Dataförmedlingstjänster fungerar som betrodda mellanhänder som möjliggör säker delning av befintliga data och eliminerar överflödig insamling. Dataaltruismorganisationer underlättar frivillig datadelning för allmännyttiga ändamål och gör data tillgängliga för forskning och offentliga tjänster. Bestämmelser om fritt flöde undanröjer hinder som kräver samtidig lagring på flera platser. Skyddsåtgärder för internationella överföringar säkerställer gränsöverskridande tillgång till data samtidigt som skyddet upprätthålls, vilket gör det möjligt för både enskilda personer och företag att tillhandahålla sina data vid ett tillfälle med vetskapen om att senare behov tillgodoses genom säkra rättighetsbaserade delningsmekanismer. Samtidigt gör bestämmelserna om den gemensamma kontaktpunkten att engångsprincipen även tillämpas när det gäller incidentrapportering.

Förklara hur nyskapade data är sökbara, tillgängliga, kompatibla och återanvändbara samt uppfyller standarder för hög kvalitet

Dessa ändringar säkerställer att nyskapade data uppfyller Fair-principerna och kvalitetsnormerna genom samordnade mekanismer: EDIB utarbetar gemensamma tekniska specifikationer och tillgängliga protokoll för interoperabilitet mellan sektorsspecifika dataområden. Bestämmelser om fritt flöde förhindrar fragmentering som undergräver datakvaliteten. EDIB:s samordningsroll kan möjliggöra ett harmoniserat genomförande av standarder, tekniska krav och kvalitetsriktmärken för metadata i medlemsstaterna.

Dataflöden

Övergripande beskrivning av dataflöden

Anmärkning: De flesta av de dataflöden som beskrivs nedan är befintliga flöden som flyttas från en förordning till en annan. Närmare bestämt överförs bestämmelser i dataförvaltningsakten till dataförordningen.

Typ av data	**Hänvisning/hänvisningar till kravet/kraven**	**Aktör som tillhandahåller data**	**Aktör som tar emot data**	**Utlösande faktor för datautbyte**	**Frekvens (i tillämpliga fall)**
Avslag på en begäran om tillgång till data på grundval av undantaget avseende företagshemligheter (*och anmälan om detta till den behöriga myndigheten*)	Artikel 1 *Ändring av artiklarna 4.8 och 5.11 i dataförordningen*	Datahållare	Dataanvändare (som framställer begäran). Behörig myndighet som utsetts enligt artikel 37	Avslag på en begäran om åtkomst till data på grundval av undantaget för företagshemligheter	Beroende på ändamålet
Data som ska göras tillgängliga i samband med ett allmänt nödläge	Artikel 1 *Införande av artikel 15a i dataförordningen*	Datahållare	Offentligt organ, Europeiska kommissionen, Europeiska centralbanken, Unionsorgan	Allmänt nödläge + begäran om tillgång till data som uppfyller de nödvändiga villkoren	Beroende på ändamålet
Anmälan av avsikt att göra data tillgängliga i ett allmänt nödläge	Artikel 1 *Ändring av artikel 21.5 i dataförordningen*	Offentligt organ, Europeiska kommissionen, Europeiska centralbanken, Unionsorgan	Datahållare från vilken data mottogs	Allmänt nödläge + avsikt att överföra data eller göra dem tillgängliga	Beroende på ändamålet
Klagomål enligt kapitel V (”Göra data tillgängliga för offentliga organ, kommissionen, Europeiska centralbanken och unionsorgan på	Artikel 1 *Införande av artikel 22a i dataförordningen*	Datahållare, offentliga organ, Europeiska kommissionen, Europeiska centralbanken,	Behörig myndighet i den medlemsstat där datahållaren är etablerad	Om en tvist uppstår om en begäran om data enligt artikel 15a i dataförordningen	Beroende på ändamålet

grundval av ett exceptionellt behov”)		Unionsorgan			
Icke-personuppgifter som innehas i Europeiska unionen	Artikel 1 *Ändring av följande artiklar i dataförordningen:* *artikel 32.1, 32.3 och 32.4*	Leverantörer av databehandlingstjänster, leverantörer av dataförmedlingstjänster, dataaltruismorganisationer	Domstolar i tredjeländer. Administrativa myndigheter i tredjeländer, kunder (datahållare/registrerade)	Begäran från tredjeland baserad på internationellt avtal, begäran från tredjeland som uppfyller villkoren i artikel 32.3, begäran från kunden om åtkomst till egna data	Beroende på ändamålet
Data som ska tillhandahållas som svar på en begäran om vidareutnyttjande	Artikel 1 *Ändring av artikel 32.4–32.5 i dataförordningen*	Leverantör av dataförmedlingstjänster eller en erkänd dataaltruismorganisation	Aktör som lämnat in en begäran om vidareutnyttjande av data (myndigheten i tredjeland)	Datum för beviljande av begäran om vidareutnyttjande	Beroende på ändamålet
Meddelande om begäran om vidareutnyttjande av data som ska beviljas inom kort	Artikel 1 *Ändring av artikel 32.4–32.5 i dataförordningen*	Leverantör av dataförmedlingstjänster eller en erkänd dataaltruismorganisation	Kund	Datum för beviljande av begäran om vidareutnyttjande från myndigheter i tredjeland (*utom vid en begäran för brottsbekämpande ändamål*)	Beroende på ändamålet
Information som ska offentliggöras i offentliga register (europeisk	Artikel 1 *Införande av artikel 32a i dataförordningen*	Europeiska kommissionen	Offentlig	Information om erkända dataförmedlingstjänster eller	Pågående (registret uppdateras

märkning för dataförmedlingstjänster och dataaltruismorganisationer)				dataaltruismorganisationer blir tillgänglig eller behöver ändras	regelbundet)
Data för vilka förmedlingstjänster tillhandahålls (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1 *Införande av artikel 32c i dataförordningen*	Registrerade Datahållare	Dataanvändare (via leverantören av dataförmedlingstjänster)	Den registrerades samtycke Tillstånd från datahållaren Begäran av dataanvändaren	Enligt avtal/kontrakt mellan parter
Information om dataanvändning och datatermer (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1 *Införande av artikel 32c i dataförordningen*	Leverantör av dataförmedlingstjänster	Registrerade	Innan den registrerade ger sitt samtycke till dataanvändning	Varje gång innan samtycke begärs
Ansökningar om registrering i det offentliga unionsregistret och ändringar av anmälda uppgifter (europeisk	Artikel 1 *Införande av artikel 32e i dataförordningen*	Leverantörer av dataförmedlingstjänster Dataaltruismorganisationer	Behörig myndighet i den medlemsstat där det huvudsakliga verksamhetsstället	Ansökan	Beroende på ändamålet

märkning för dataförmedlingstjänster och dataaltruismorganisationer)			finns		
Godkända ansökningar om registrering som ska läggas till i det offentliga unionsregistret (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1 *Införande av artikel 32e i dataförordningen*	Behörig myndighet	Europeiska kommissionen	Ansökan godkänd	Beroende på ändamålet (inom tolv veckor efter mottagandet av en ansökan, förutsatt att beslutet är positivt)
Meddelande om senare ändringar av den information som lämnats under ansökningsprocessen (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1 *Införande av artikel 32e i dataförordningen*	Registrerade enheter	Behörig myndighet	Ändringar av den information som lämnats eller om entiteterna upphör med sin verksamhet i unionen	Beroende på ändamålet
Mottagande av meddelande om senare ändringar (europeisk märkning för	Artikel 1 *Införande av artikel 32e i dataförordningen*	Behörig myndighet	Europeiska kommissionen	Registrerade enheter meddelar ändringen (se posten ovan)	Beroende på ändamålet, utan dröjsmål

dataförmedlingstjänster och dataaltruismorganisationer)					
Information som lämnats till registrerade/datahållare före behandling (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1 *Införande av artikel 32f i dataförordningen*	Erkänd dataaltruismorganisation	Registrerade Datahållare	Före eventuell behandling av deras data	Före varje bearbetning (måste vara tydlig och lättbegriplig)
Samtycke (eller återkallande av samtycke) till databehandling av en erkänd dataaltruismorganisation (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1 *Införande av artikel 32f i dataförordningen*	Registrerade Datahållare (om icke-personuppgifter)	Dataaltruismorganisation	Den registrerades samtycke eller tillstånd från datahållaren som krävs för behandlingen	Enligt samtycke eller beviljat tillstånd, med möjlighet till återkallelse när som helst
Information om den jurisdiktion i tredjeland där dataanvändningen är avsedd att äga rum	Artikel 1 *Införande av artikel 32f i dataförordningen*	Dataaltruismorganisation	Datahållare	Om dataaltruismorganisationen underlättar databehandlingen för	Beroende på ändamålet

				tredje part	
Anmälan av obehörig överföring, åtkomst eller användning av icke-personuppgifter (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1 *Införande av artikel 32f i dataförordningen*	Dataaltruismorganisation	Datahållare	Otillåten åtgärd	Beroende på ändamålet, utan dröjsmål
Information för övervakning av efterlevnaden (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1 *Införande av artikel 32g i dataförordningen*	Leverantörer av dataförmedlingstjänster Dataaltruismorganisationer	Behöriga myndigheter	Begäran från behörig myndighet Begäran från fysisk eller juridisk person	Beroende på ändamålet (på begäran, vilken måste vara proportionell och motiverad)
Anmälan av bristande efterlevnad (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1 *Införande av artikel 32g i dataförordningen*	Behörig myndighet	Enhet som inte uppfyller kraven	Den behöriga myndigheten konstaterar att en erkänd leverantör av dataförmedlingstjänster eller en erkänd dataaltruismorganisation inte uppfyller kraven	Beroende på ändamålet (följt av möjligheten för enheten att framföra sina synpunkter inom 30

					dagar)
Beslut att återkalla rätten att använda märkningen (europeisk märkning för dataförmedlingstjänster och dataaltruismorganisationer)	Artikel 1 *Införande av artikel 32g i dataförordningen*	Behörig myndighet	Offentlig	Efter beslut om återkallande av märkningen	Beroende på ändamålet
Utkast till rättsakter om datalokaliseringskrav	Artikel 1	Medlemsstaterna	Europeiska kommissionen	Skapande av utkast till rättsakt som inför ett nytt datalokaliseringskrav eller ändrar ett befintligt datalokaliseringskrav	Beroende på ändamålet, omedelbart
De slutgiltiga villkoren för exklusiva avtal	Artikel 1	Parter i arrangemanget	Offentlig	Exklusiva avtal som upprättades den 16 juli 2019 eller senare	Beroende på ändamålet, minst två månader innan ett avtal träder i kraft
Data (och/eller anmälningar) som rör en begäran om vidareutnyttjande	Artikel 1 *Införande av artikel 32p i dataförordningen*	Offentliga organ	Aktör som lämnat in en begäran om vidareutnyttjande av data	Om någon av följande handlingar ska tillhandahållas: begärda data/handlingar, utlysning av licens, meddelanden om	Beroende på ändamålet

				dröjsmål, meddelande om ett negativt beslut.	
De slutgiltiga villkoren för exklusiva avtal	Artikel 1 *Införande av artikel 32k i dataförordningen*	Parterna i ett exklusivt avtal	Allmänheten	Slutliga villkor för att ett exklusivt avtal ska kunna ingås	Beroende på ändamålet
Villkor för att tillåta vidareutnyttjande av data eller handlingar som avses i artikel 2.54	Artikel 1 *Införande av artikel 32z i dataförordningen*	Offentliga organ (med behörighet att bevilja eller avslå ansökningar om tillgång)	Allmänheten	När de beviljar vidareutnyttjande av data eller handlingar	Beroende på ändamålet
Meddelande om obehörigt vidareutnyttjande av icke-personuppgifter	Artikel 1 *Införande av artikel 32z i dataförordningen*	Vidareutnyttjare (eventuellt med bistånd av det offentliga organet)	Fysiska eller juridiska personer vars rättigheter och intressen kan påverkas	Otillåtet vidareutnyttjande har ägt rum	Beroende på ändamålet
Anmälan om avsikt att överföra icke-personuppgifter till ett tredjeland och syftet med en denna överföring (till det offentliga organet)	Artikel 1 *Införande av artikel 32aa i dataförordningen*	Vidareutnyttjare	Offentligt organ	Avsikt att överföra data till ett tredjeland	Beroende på ändamålet
Anmälan om avsikt att överföra icke-personuppgifter till ett tredjeland, syftet med denna överföring och lämpliga skyddsåtgärder (till den fysiska eller	Artikel 1 *Införande av artikel 32aa i dataförordningen*	Vidareutnyttjare (eventuellt med bistånd av det offentliga organet)	Fysisk eller juridisk person vars rättigheter och intressen kan påverkas	Avsikt att överföra data till ett tredjeland	Beroende på ändamålet

juridiska person vars rättigheter och intressen kan påverkas)					
All relevant information om tillämpningen av artiklarna 32z [villkor för vidareutnyttjande], 32aa [tredjeländer] och 32ab [avgifter] i dataförordningen	Artikel 1 *Införande av artikel 32ad i dataförordningen*	Medlemsstaterna	Tillgängliga för användare av den gemensamma informationspunkten	Relevant information måste tillhandahållas	Beroende på ändamålet
Klagomål från fysiska eller juridiska personer om deras rättigheter enligt dataförordningen har överträtts eller andra relevanta frågor	Artikel 1 *Ändring av artikel 38.1–38.2 i dataförordningen*	Fysiska eller juridiska personer	Relevant behörig myndighet i den berörda medlemsstaten	Klagomål som ska lämnas in	Beroende på ändamålet
Information om hur förfarandet eller tillämpningen av rättsmedel fortskrider i samband med klagomål enligt dataförordningen	Artikel 1 *Ändring av artikel 38.1–38.2 i dataförordningen*	Relevant behörig myndighet	Fysiska eller juridiska personer som ligger bakom klagomålet	Klagomålet som lämnats in	Beroende på ändamålet
Data om erfarenheter och god praxis (EDIB)	Artikel 1 *Införande av kapitel IXa i dataförordningen*	Europeiska datainnovationsstyrelsen	Kommissionen, Behöriga myndigheter	Indata som ska tillhandahållas	Beroende på ändamålet
Utvärdering av kapitlen	Artikel 1	Europeiska	Europaparlamentet,	Utvärdering av	Senast den 12

II, III, IV, V, VI, VII och VIII i dataförordningen Utvärdering av kapitlen VIIa, VIIb och VIIc i dataförordningen	*Ändring av artikel 49.1 i dataförordningen* Artikel 1 *Ändring av artikel 49.2 i dataförordningen*	kommissionen	rådet, Europeiska ekonomiska och sociala kommittén	dataförordningen utförd	september 2028 Senast den [dagen för ikraftträdande plus fem år]
Anmälningar om personuppgiftsincidenter	Artikel 3 *Ändring av artikel 33.1 i den allmänna dataskyddsförordningen*	Personuppgiftsansvarig	Tillsynsmyndighet	Dataincident har inträffat	Beroende på ändamålet
Europeiska dataskyddsstyrelsens förslag till en gemensam mall för anmälan av uppgiftsincidenter	Artikel 3 *Ändring av artikel 33.1 i den allmänna dataskyddsförordningen*	Europeiska dataskyddsstyrelsen	Kommissionen	Förslag som ska lämnas in	Inom [månader] efter ikraftträdandet av denna förordning Vart tredje år
Europeiska dataskyddsstyrelsens förslag om konsekvensbedömning av dataskydd	Artikel 3 *Ändring av artikel 70.1 i den allmänna dataskyddsförordningen*	Europeiska dataskyddsstyrelsen	Kommissionen	Förslag som ska lämnas in	Beroende på ändamålet
Rapporter om allvarliga incidenter i enlighet med NIS2-direktivet	Artikel 6 *Införande av artiklarna 23a och 23b, ändring av*	Väsentliga och viktiga entiteter	CSIRT-enheter/behöriga myndigheter (i	Omständigheter som beskrivs i artikel 23.3 i NIS2-direktivet	Beroende på ändamålet

	artiklarna 23 och 30.1 i NIS2-direktivet		tillämpliga fall)		
Anmälningar om personuppgiftsincidenter	Artikel 3 *Ändring av artikel 33 i den allmänna dataskyddsförordningen*	Personuppgiftsansvariga	Tillsynsmyndighet	Personuppgiftsincident	Beroende på ändamålet
Anmälningar om allvarliga IKT-relaterade incidenter i enlighet med DORA-förordningen. Frivilliga anmälningar om betydande cyberhot i enlighet med DORA-förordningen	Artikel 8 *Ändring av artikel 19 i DORA-förordningen*	Finansiella enheter	Relevant behörig myndighet	Allvarliga IKT-relaterade incidenter, betydande cyberhot	Beroende på ändamålet
Anmälningar om incidenter som medför en betydande störning eller kan medföra en betydande störning av tillhandahållandet av samhällsviktiga tjänster enligt CER-direktivet	Artikel 9 *Ändring av artikel 15 i CER-direktivet*	Kritiska entiteter	Behörig myndighet	Incidenter som medför en betydande störning eller kan medföra en betydande störning av tillhandahållandet av samhällsviktiga tjänster	Beroende på ändamålet

4.3 Digitala lösningar

Övergripande beskrivning av digitala lösningar

Anmärkning: Alla de digitala lösningar som beskrivs nedan är befintliga lösningar vars rättsliga grund ska flyttas från en förordning till en annan. Närmare bestämt överförs bestämmelser i dataförvaltningsakten till dataförordningen.

Digital lösning	**Hänvisning/hänvisningar till kravet/kraven**	**Huvudsakliga föreskrivna funktioner**	**Ansvarigt organ**	**Hur tillgodoses tillgängligheten?**	**Hur övervägs möjligheten till återanvändning?**	**Användning av AI-teknik (i tillämpliga fall)**
Offentligt unionsregister över dataförmedlingstjänster och dataaltruismorganisationer	*Införande av artikel 32a i dataförordningen*	Lagring och offentliggörande av obligatorisk information	Europeiska kommissionen	//	//	Ej tillämpligt
Gemensam informationspunkt (enligt dataförordningen)	Artikel 1 *Införande av artikel 32ad i dataförordningen*	Information som ska göras tillgänglig och tillgänglig Behörighet att ta emot förfrågningar eller begäranden om vidareutnyttjande av kategorierna av skyddade data Begäranden om	Europeiska kommissionen	En gemensam åtkomstpunkt med ett sökbart elektroniskt register över tillgängliga data i nationella gemensamma informationspunkter och ytterligare information om hur man begär data via dessa nationella gemensamma	Tillgång på elektronisk väg till en sökbar tillgångsförteckning med en översikt över alla tillgängliga dataresurser [...] och villkoren för deras vidareutnyttjande.	Ej tillämpligt

		överföring, om möjligt och lämpligt genom automatiserade metoder, till behöriga offentliga organ Tillhandahållande på elektronisk väg av en sökbar tillgångsförteckning med en översikt över alla tillgängliga dokumentresurser		informationspunkter		
En gemensam kontaktpunkt för anmälan av incidenter	Artikel 6 *Införande av artikel 23a i NIS2-direktivet*	Möjlighet till rapportering av incidenter i enlighet med relevanta akter på unionsnivå Säkerställande av interoperabilitet och kompatibilitet med europeiska företagsplånböcker	Europeiska kommissionen, Enisa	Interoperabilitet och kompatibilitet med europeiska företagsplånböcker och deras egna tillgänglighetsmetoder	Möjlighet att hantera rapportering av incidenter enligt olika rättsakter, möjlighet att införa ytterligare rättsliga grunder i lösningen med en gemensam kontaktpunkt i framtiden	Ej tillämpligt

Förklara, för varje digital lösning, hur den digitala lösningen uppfyller tillämplig digital politik och lagstiftning.

Offentligt unionsregister över dataförmedlingstjänster och dataaltruismorganisationer

Digital och/eller sektoriell politik (i tillämpliga fall)	**Beskrivning av överensstämmelse**
Förordningen om artificiell intelligens	Ej tillämpligt
EU:s cybersäkerhetsram	Ej tillämpligt
eIDA	Ej tillämpligt
Den gemensamma digitala ingången och IMI	Ändring av förordning (EU) 2018/1724 för att lägga till ”Registrering som leverantör av dataförmedlingstjänster” och ”Registrering som dataaltruismorganisation som är erkänd i unionen” i bilaga II.
Övriga	Ej tillämpligt

Gemensam informationspunkt (enligt dataförordningen)

Digital och/eller sektoriell politik (i tillämpliga fall)	**Beskrivning av överensstämmelse**
Förordningen om artificiell intelligens	Ej tillämpligt
EU:s cybersäkerhetsram	Offentliga organ får införa krav på att tillgång till och vidareutnyttjande av data eller handlingar på distans ska ske i en säker behandlingsmiljö som tillhandahålls eller kontrolleras av det offentliga organet. I sådana fall ska de offentliga organen införa villkor som bevarar integriteten hos de

	tekniska systemens funktionssätt i den säkra behandlingsmiljön.
eIDA	Ej tillämpligt
Den gemensamma digitala ingången och IMI	Ej tillämpligt
Övriga	Den gemensamma informationspunkten ska vara förenlig med förordning (EU) 2016/679 (den allmänna dataskyddsförordningen). Offentliga organ får införa krav på att tillgång för vidareutnyttjande av data eller handlingar endast ska beviljas om dessa har anonymiserats och/eller under förutsättning att andra relevanta förberedelser har gjorts. Dessutom ska vidareutnyttjaren vid otillåtet vidareutnyttjande av icke-personuppgifter vara skyldig att informera de fysiska personer vars rättigheter och intressen kan påverkas.

En gemensam kontaktpunkt för anmälan av incidenter

Digital och/eller sektoriell politik (i tillämpliga fall)	**Beskrivning av överensstämmelse**
Förordningen om artificiell intelligens	Ej tillämpligt
EU:s cybersäkerhetsram	Som en ändring av NIS2-direktivet införs ett övergripande fokus på cybersäkerhet. Mer allmänt ska den gemensamma kontaktpunkten fungera som en ingång för att kanalisera alla cybersäkerhetsrelaterade incidentrapporter till respektive behöriga myndigheter, i enlighet med ett flertal unionsrättsakter.
eIDA	Den gemensamma kontaktpunkten föreskrivs även för incidentrapportering enligt förordning (EU) nr 910/2014 (eIDA-förordningen). Enisa ska se till att den gemensamma kontaktpunkten är förenlig och kompatibel med de europeiska företagsplånböckerna och att de europeiska företagsplånböckerna åtminstone kan användas för att

	identifiera och autentisera entiteter som använder den gemensamma kontaktpunkten. Initiativet för en europeisk företagsplånbok kommer att bygga på regelverket i eIDA-förordningen.
Den gemensamma digitala ingången och IMI	Ej tillämpligt
Övriga	I förslaget beaktades hela det digitala regelverket, inklusive de politiska åtgärderna för data, cybersäkerhet och telekommunikationer.

4.4 Interoperabilitetsbedömning

Övergripande beskrivning av den digitala offentliga tjänst/de digitala offentliga tjänster som påverkas av kravet

Digital offentlig tjänst eller kategori av digitala offentliga tjänster	**Beskrivning**	**Hänvisning/hänvisningar till kravet/kraven**	**Lösning(ar) för ett interoperabelt Europa** **(EJ TILLÄMPLIGT)**	**Andra interoperabilitetslösningar**
Europeisk infrastruktur för dataförvaltning och transparens	Digitala offentliga tjänster som möjliggör en infrastruktur för dataförvaltning och transparens och som bland annat utnyttjar ett offentligt EU-register över dataförmedlingstjänster och dataaltruismorganisationer, samt en gemensam informationspunkt som hjälper vidareutnyttjare att hitta information om vidareutnyttjande av vissa kategorier av skyddade data. Kategori av digitala offentliga tjänster enligt COFOG 04.9.0 – Övriga ekonomiska frågor (CS)	Artikel 1	//	//
Incidentrapportering	Digital offentlig tjänst som möjliggör incidentrapportering via den gemensamma kontaktpunkten. Kategori av digitala offentliga	Artikel 6	//	Europeiska företagsplånböcker

	tjänster enligt COFOG 03.6.0 Övrigt samhällsskydd och rättskipning			

Kravets/kravens inverkan på gränsöverskridande interoperabilitet vad gäller digitala offentliga tjänster

Anmärkning: I följande analys hänvisar numren på artiklarna i avsnittet ”Åtgärder” till den eller de rättsakter som ska ändras. Kartläggningen av kraven i omnibuspaketet görs en gång, högst upp i varje cell.

Digital offentlig tjänst #1 – Europeisk infrastruktur för dataförvaltning och transparens

Bedömning	**Åtgärd/åtgärder**	**Potentiella återstående hinder (i tillämpliga fall)**
Överensstämmelse med befintlig digital och sektoriell politik. **Ange tillämplig digital och sektoriell politik som identifierats**	Artikel 1 Anpassningen till befintlig digital och sektoriell politik återspeglas i skälen till dataförvaltningsakten: Gemensam digital ingång (förordning (EU) 2018/1724) (skäl 56): Anmälningsförfarandena för dataförmedlingstjänster och registreringsförfarandena för dataaltruismorganisationer måste göras tillgängliga via den gemensamma digitala ingången för att säkerställa gränsöverskridande onlineåtkomst. Den europeiska interoperabilitetsramen (skäl 54): Den digitala infrastrukturen måste följa principerna i den europeiska interoperabilitetsramen för att säkerställa gränsöverskridande och sektorsöverskridande dataanvändning. FSE-byggstenar (Infrastruktur för digitala tjänster inom ramen för Fonden för ett sammanlänkat Europa) (skäl 54): Hänvisningar till ”basvokabulärerna och FSE-byggstenarna”. Den digitala tjänsten bör utnyttja FSE-byggstenar (t.ex. eDelivery, e-ID, e-signatur) för det tekniska genomförandet. Tillgänglighetskrav (direktiven (EU) 2016/2102 och (EU) 2019/882) (skäl 62). Direktiv (EU) 2016/2102 (direktivet om webbtillgänglighet): Offentliga register och digitala	

	tjänster ska vara tillgängliga för personer med funktionsnedsättning. Direktiv (EU) 2019/882 (det europeiska tillgänglighetsdirektivet): Digitala tjänster ska uppfylla tillgänglighetskraven. Den allmänna dataskyddsförordningen (förordning (EU) 2016/679) (skälen 4 och 35): Alla digitala tjänster för hantering av personuppgifter ska uppfylla kraven i den allmänna dataskyddsförordningen avseende dataskydd, integritet och säkerhet. Förordning (EU) 2018/1725 (skäl 4): Om EU-institutionerna behandlar uppgifter genom dessa register ska de följa den här förordningen. Direktivet om öppna data (direktiv (EU) 2019/1024) (skälen 6 och 10): ”Genom direktiv (EU) 2019/1024 och sektorsspecifik unionsrätt säkerställs att de offentliga organen gör en större del av de data de producerar lättillgängliga för användning och vidareutnyttjande”: Den digitala tjänsten kompletterar direktivet om öppna data genom att hantera kategorier av skyddade data som inte omfattas av dess tillämpningsområde, samtidigt som den säkerställer att offentliga organ följer principerna om ”inbyggd öppenhet och öppenhet som standard” i tillämpliga fall. Sektorspolitik för europeiska dataområden och sektorsvisa data, inbegripet det europeiska hälsodataområdet, det gemensamma europeiska dataområdet för mobilitet, den europeiska gröna given, klimat- och energidata, tillverknings- och industridata, data om finansiella tjänster, jordbruksdata, dataområdet för offentlig förvaltning och dataområdet för kompetens.	

Organisatoriska åtgärder för ett smidigt tillhandahållande av gränsöverskridande digitala offentliga tjänster **Ange planerade förvaltningsåtgärder**	Artikel 1 **Utnämning och samordning av behöriga myndigheter** - Artikel 32b: Varje medlemsstat ska utse en eller flera behöriga myndigheter som ska ansvara för registreringen av leverantörer av dataförmedlingstjänster och dataaltruismorganisationer. Dessa behöriga myndigheter ska upprätthålla sitt oberoende av alla erkända leverantörer av dataförmedlingstjänster eller erkända dataaltruismorganisationer. Artikel 32ac: Varje medlemsstat ska utse ett eller flera behöriga organ som ska bistå de offentliga organ som beviljar eller vägrar åtkomst för vidareutnyttjande av kategorier av skyddade data. Artikel 32g: De behöriga myndigheterna ska övervaka och kontrollera att erkända leverantörer av dataförmedlingstjänster och erkända dataaltruismorganisationer följer bestämmelserna i dataförordningen. **Mekanism för gränsöverskridande behörighet** Artikel 32e: Dataförmedlingstjänster omfattas av den behöriga myndighetens behörighet i den medlemsstat där de har sitt huvudsakliga verksamhetsställe. Samma princip gäller för dataaltruismorganisationer. **Ömsesidigt erkännande och en enda registrering** Artikel 32e: Registreringen som en dataförmedlingstjänst eller en dataaltruismorganisation ska vara giltig i alla medlemsstater. Artikel 32a: Användning av en gemensam logotyp **Centraliserade register på EU-nivå för datainsamling och transparens** Artikel 32 a: Offentliga unionsregister över alla erkända leverantörer av dataförmedlingstjänster och dataaltruismorganisationer. Artikel 32 e: Behöriga myndigheter ska utan dröjsmål och på elektronisk väg underrätta	

	kommissionen om nya registreringar, ändringar och raderingar, varefter kommissionen ska uppdatera EU-registren i enlighet med detta. **Samordning av övervakning och tillämpning** Nationella behöriga myndigheter Europeiska datainnovationsstyrelsen **Styrning av dataöverföring till tredjeländer** Artikel 32aa: Krav för vidareutnyttjares överföring av icke-personuppgifter till tredjeländer. **Exklusiva avtal** Artikel 32k: Fastställer lagligheten av exklusiva avtal om vidareutnyttjande av data eller handlingar som innehas av offentliga organ. Kräver insyn i de slutgiltiga villkoren.	
Åtgärder som vidtagits för att säkerställa en samstämmig förståelse av data **Ange dessa åtgärder**	Artikel 1 **Gemensamma standarder och interoperabla ramar** - EDIB ger Europeiska kommissionen råd om standardisering när det gäller sektorsövergripande aspekter av datadelning, bland annat när det gäller framväxten av gemensamma europeiska dataområden, med beaktande av sektorsspecifik standardiseringsverksamhet. o Artikel 42: EDIB bistår i antagandet av riktlinjer för inrättandet av interoperabla ramar och gemensam praxis för hur gemensamma europeiska dataområden ska fungera. - Gemensam logotyp för identifiering av dataförmedlingstjänster och dataaltruismorganisationer.	

	- Artikel 32q: Offentliga organ och offentliga företag ska göra sina data eller handlingar tillgängliga, om möjligt och lämpligt på elektronisk väg, i format som är öppna, maskinläsbara, tillgängliga, sökbara och möjliga att vidareutnyttja, tillsammans med tillhörande metadata. Både format och metadata ska, när så är möjligt, vara förenliga med formella öppna standarder. **Andra relevanta åtgärder:** - Artikel 32t: Medlemsstaterna ska, i samarbete med kommissionen, fortsätta ansträngningarna för att förenkla tillgången till dataset och göra lämpliga dataset tillgängliga i format som är åtkomliga, lättillgängliga och möjliga att vidareutnyttja på elektronisk väg. - Artikel 32u: Medlemsstaterna ska underlätta tillgången till forskningsdata på ett sätt som är förenligt med Fair-principerna.	
Användning av gemensamt överenskomna öppna tekniska specifikationer och standarder **Ange dessa åtgärder**	Artikel 1 **Åtgärder för maskinläsbara data:** - Artikel 32a: Maskinläsbart EU-register över leverantörer av dataförmedlingstjänster. - Artikel 32a: Maskinläsbart EU-register över dataaltruismorganisationer. - Artikel 32q: Offentliga organ ska göra sina data eller handlingar tillgängliga, om möjligt i format som är öppna, maskinläsbara, tillgängliga, sökbara och möjliga att vidareutnyttja, tillsammans med tillhörande metadata. Både format och metadata ska, när så är möjligt, vara förenliga med formella öppna standarder. - Artikel 32q: Värdefulla dataset ska göras tillgängliga för vidareutnyttjande i maskinläsbart format via lämpliga API:er och, i förekommande fall, som en bulknedladdning. - Artikel 32t: Medlemsstaterna ska inrätta praktiska arrangemang för att underlätta sökning efter data eller handlingar som finns tillgängliga för vidareutnyttjande, till	

	exempel i form av tillgångsförteckningar över viktiga data eller handlingar med relevanta metadata, om möjligt och lämpligt tillgängliga online och i maskinläsbart format, och i form av portaler som är kopplade till tillgångsförteckningarna. Om möjligt ska medlemsstaterna underlätta sökning på flera språk efter data eller handlingar. - Artikel 32w: Särskilda värdefulla dataset ska vara maskinläsbara. Genomförandeakter får innehålla bestämmelser om format för data och metadata samt tekniska arrangemang för spridning. **Åtgärder för interaktioner från maskin till maskin:** - Artikel 32ad: Föreskrift om användningen av den gemensamma informationspunkten. Den gemensamma informationspunkten ska vara behörig att ta emot förfrågningar eller framställningar och ska, om möjligt och lämpligt på ett automatiserat sätt, översända dem till behöriga offentliga organ eller behöriga organ. **Andra relevanta åtgärder:** - Artikel 48a: Ändring av bilaga II till förordning (EU) 2018/1724 (Gemensam digital ingång). Utredning av synergier. - Skäl 52 i omnibuspaketet: I den mån det är genomförbart bör Enisa ta hänsyn till befintliga nationella tekniska lösningar som underlättar incidentrapportering, däribland nationella plattformar, vid utarbetandet av specifikationerna för tekniska, operativa och organisatoriska åtgärder avseende inrättande, underhåll och säker drift av den gemensamma kontaktpunkten. Enisa bör även överväga att använda tekniska protokoll och verktyg, däribland gränssnitt för tillämpningsprogram och maskinläsbara standarder, som gör att entiteterna kan underlätta integreringen av rapporteringskraven i sina affärsprocesser och att myndigheterna kan ansluta den gemensamma kontaktpunkten till sina nationella rapporteringssystem.	

Digital offentlig tjänst #2 – Incidentrapportering

Bedömning	Åtgärd/åtgärder	Potentiella återstående hinder (i tillämpliga fall)
Överensstämmelse med befintlig digital och sektoriell politik. **Ange tillämplig digital och sektoriell politik som identifierats**	Artikel 6 En allmän anpassning till befintlig digital politik och sektorspolitik föreskrivs genom direktiv (EU) 2022/2555 (NIS2-direktivet), vilket nu ändras genom det digitala omnibuspaketet. Dessutom möjliggör omnibuspaketet synergier med den europeiska företagsplånboken och förordning (EU) 2024/2847 (cyberresiliensförordningen). Särskilt gäller följande: • I artikel 23.4 föreskrivs att den gemensamma kontaktpunkten ska användas vid en anmälan enligt NIS2-direktivet. • I artikel 23.1 fastställs att en anmälan om en allvarlig incident enligt artikel 14.3 i förordning (EU) 2024/2847 (cyberresiliensförordningen) även ska utgöra rapportering av information enligt direktiv (EU) 2022/2555 (NIS2-direktivet). Detta är i överensstämmelse med engångsprincipen. • I artikel 23a.3 d föreskrivs kopplingen till de europeiska företagsplånböckerna.	
Organisatoriska åtgärder för ett smidigt tillhandahållande av gränsöverskridande digitala offentliga tjänster **Ange planerade förvaltningsåtgärder**	Artikel 6 I artikel 23a fastställs roller och ansvarsområden. Närmare bestämt ska Enisa göra följande: • Utveckla och upprätthålla en gemensam kontaktpunkt för att stödja skyldigheten att rapportera incidenter och relaterade händelser enligt unionsrättsakterna. • Vidta tekniska, operativa och organisatoriska åtgärder för att hantera riskerna med den gemensamma kontaktpunktens säkerhet och den information som lämnas eller sprids. Byrån ska därvid samråda med kommissionen, CSIRT-nätverket och relevanta behöriga myndigheter.	

Åtgärder som vidtagits för att säkerställa en samstämmig förståelse av data **Ange dessa åtgärder**	Artikel 6 Genom artikel 23a åläggs Enisa att utarbeta specifikationer som ska säkerställa den nödvändiga kapaciteten för interoperabilitet när det gäller andra relevanta rapporteringsskyldigheter. *Anmärkning: Ytterligare innehållskrav för incidentrapportering fastställs i de relevanta unionsrättsakterna, däribland direktiv (EU) 2022/2555 (NIS2-direktivet). I artikel 23a.3 c i omnibuspaketet klargörs att Enisa ska se till att dessa beaktas i vederbörlig ordning.*	

Användning av gemensamt överenskomna öppna tekniska specifikationer och standarder
 	
Ange dessa åtgärder
	Artikel 6
	
	I artikel 23a uppmanas till utarbetande av specifikationer:
	• Enisa ska tillhandahålla och genomföra specifikationer för tekniska åtgärder avseende inrättande, underhåll och säker drift av den gemensamma kontaktpunkten. Dessa specifikationer ska bland annat omfatta
	  ○ den nödvändiga kapaciteten för interoperabilitet med andra relevanta rapporteringsskyldigheter,
	  ○ tekniska arrangemang för de relevanta entiteterna och myndigheterna för att få tillgång till, lämna in, inhämta, överföra eller på annat sätt behandla information från den gemensamma kontaktpunkten, samt tekniska protokoll och verktyg som gör det möjligt för entiteterna och myndigheterna att vidarebehandla den mottagna informationen inom sina system.
	• Den gemensamma kontaktpunkten ska i förekommande fall vara förenlig och kompatibel med de europeiska företagsplånböckerna.	

4.5 Åtgärder till stöd för digitalt genomförande

Övergripande beskrivning av åtgärder till stöd för digitalt genomförande

Beskrivning av åtgärden	**Hänvisning/hänvisningar till kravet/kraven**	**Kommissionens roll** (i tillämpliga fall)	**Aktörer som ska involveras** (i tillämpliga fall)	**Förväntad tidsplan** (i tillämpliga fall)
Genomförandeakt: Gemensam logotyp för leverantörer av dataförmedlingstjänster	Artikel 1	Fastställer egenskaperna hos den gemensamma logotypen, inbegripet utformning och användning.	Kommittén för granskningsförfarandet	//
Genomförandeakt: Gemensam logotyp för erkänd dataaltruism	Artikel 1	Fastställer egenskaperna hos den gemensamma logotypen, inbegripet utformning och användning.	Kommittén för granskningsförfarandet	//
Övervakning och efterlevnad: Behöriga myndigheter får övervaka efterlevnaden antingen på eget initiativ eller på begäran av fysiska eller juridiska personer.	Artikel 1	//	Behöriga myndigheter, dataförmedlingstjänster, dataaltruismorganisationer	//

Genomförandeakt: Särskilda värdefulla dataset	Artikel 1	Utarbetande av en förteckning över särskilda värdefulla dataset. Får ange arrangemangen för offentliggörande och vidareutnyttjande av värdefulla dataset.	Kommittén för granskningsförfarandet	//
Riktlinjer: • EDIB ska ge råd om riktlinjer för gemensamma europeiska dataområden • EDIB att anta riktlinjer om interoperabla ramar	Artikel 1	Stöd från EDIB	EDIB	//
Genomförandeakt: Gemensam mall för anmälan av personuppgiftsincidenter	Artikel 3	Anta en gemensam mall baserad på EDPB:s förslag.	Kommittén för granskningsförfarandet	//
Delegerad akt: Automatiserade och maskinläsbara upplysningar om den registrerades val	Artikel 3	Fastställa skyldigheter för webbläsare och leverantörer av terminalutrustning	Kommittén för granskningsförfarandet	//

Genomförandeakt: Incidentrapportering enligt CER-direktivet	Artikel 9	Ytterligare specificera typ och format av information som anmälts i enlighet med artikel 15.1 i direktiv (EU) 2022/2557 (CER-direktivet).	//	//