Europeiska unionens råd

Bryssel den 12 januari 2017
(OR. en)

5034/17

Interinstitutionellt ärende:
2017/0002 (COD)

DATAPROTECT 2
JAI 2
DAPIX 2
FREMP 1
DIGIT 2
CODEC 4

FÖRSLAG

från:	Jordi AYET PUIGARNAU, direktör, för Europeiska kommissionens generalsekreterare
inkom den:	12 januari 2017
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2017) 8 final
Ärende:	Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om skydd för enskilda personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ, kontor och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut 1247/2002/EG

För delegationerna bifogas dokument – COM(2017) 8 final.

Bilaga: COM(2017) 8 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 10.1.2017
COM(2017) 8 final

2017/0002 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om skydd för enskilda personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ, kontor och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut 1247/2002/EG

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

I artikel 16.1 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), som den infördes genom Lissabonfördraget, fastställs principen att var och en har rätt till skydd av personuppgifter som rör honom eller henne. Vidare infördes i artikel 16.2 i EUF-fördraget en särskild rättslig grund för antagande av regler om skydd av personuppgifter. Artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna tar upp skyddet av personuppgifter som en grundläggande rättighet.

Rätten till skydd av personuppgifter gäller även för behandling av personuppgifter som utförs av EU:s institutioner, organ, kontor och byråer. Förordning (EG) nr 45/2001[1], den viktigaste befintliga EU-lagstiftningen om skydd av personuppgifter inom unionsinstitutionerna, antogs 2001 med två mål i åtanke: att skydda den grundläggande rätten till skydd av personuppgifter och att garantera det fria flödet av personuppgifter i hela unionen. Den kompletterades genom beslut nr 1247/2002/EG[2].

Den 27 april 2016 antog Europaparlamentet och rådet den allmänna dataskyddsförordningen (förordning (EU) 2016/679), som kommer att börja tillämpas den 25 maj 2018. I denna förordning anges att förordning (EG) nr 45/2001 bör anpassas till de principer och regler som fastställs i förordning (EU) 2016/679, i syfte att tillhandahålla en stark och sammanhängande ram för skyddet av personuppgifter inom unionen och möjliggöra samtidig tillämpning av de båda instrumenten[3].

Det ligger i linje med en enhetlig strategi för skyddet av personuppgifter i hela unionen att så långt som möjligt anpassa de regler om skydd av personuppgifter som gäller för unionens institutioner, organ, kontor och byråer till de regler om skydd för personuppgifter som har antagits för medlemsstaterna. När en bestämmelse i förslaget bygger på samma begrepp som en bestämmelse i förordning (EU) 2016/679 bör de båda bestämmelserna tolkas på ett enhetligt sätt, i synnerhet eftersom det system som ligger till grund för förslaget bör förstås som en motsvarighet till det system som inrättats genom förordning (EU) 2016/679[4].

Vid översynen av förordning (EG) nr 45/2001 tas också hänsyn till resultaten av undersökningar och samråd med berörda parter samt utvärderingen av dess tillämpning under de senaste 15 åren.

Det här är inte ett initiativ inom ramen för programmet om lagstiftningens ändamålsenlighet och resultat (Refit-programmet).

---

[1] Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

[2] Beslut 1247/2002/EG av den 1 juli 2002 om tjänsteföreskrifter och allmänna villkor för utövande av funktionen som europeisk datatillsynsman,’EGT L 183, 12.07.2002, s. 1. 1.

[3] Se förordning (EU) nr 2016/679, artikel 98 och skäl 17.

[4] Se domstolens dom av den 9 mars 2010, kommissionen mot Förbundsrepubliken Tyskland, mål C-518/07, ECLI:EU:C:2010:125, punkterna 26 och 28.

- **Förenlighet med befintliga bestämmelser inom området**

Syftet med förslaget är att anpassa bestämmelserna i förordning (EG) nr 45/2001 med de principer och regler som fastställs i förordning (EU) 2016/679 för att tillhandahålla en stark och sammanhängande ram för skyddet av personuppgifter inom unionen. Förslaget införlivar även relevanta bestämmelser i förordning (EG) nr XXXX/XX [förordningen om integritet och elektronisk kommunikation] med avseende på integritet och skyddet av slutanvändares terminalutrustning.

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

Ej tillämpligt

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

- **Rättslig grund**

Skyddet av fysiska personer vid behandling av personuppgifter är en grundläggande rättighet som fastställs i artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna.

Detta förslag grundar sig på artikel 16 i EUF-fördraget, som är den rättsliga grunden för antagandet av regler om skydd av personuppgifter. Denna artikel gör det möjligt att anta bestämmelser om skydd för enskilda personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer när dessa utövar verksamhet som omfattas av unionsrättens tillämpningsområde. Den gör det också möjligt att anta regler om fri rörlighet för personuppgifter, inklusive personuppgifter som behandlas av dessa institutioner, organ, kontor och byråer.

- **Subsidiaritetsprincipen (för icke-exklusiv befogenhet)**

Föremålet för denna förordning faller inom ramen för unionens exklusiva befogenheter, eftersom endast unionen kan anta regler för behandling av personuppgifter som utförs av unionens institutioner.

- **Proportionalitetsprincipen**

För att uppnå de grundläggande målen att säkerställa en lika hög nivå av skydd för fysiska personer med avseende på behandling av personuppgifter och det fria flödet av personuppgifter över hela unionen är det, i överensstämmelse med proportionalitetsprincipen, nödvändigt och lämpligt att fastställa regler om behandling av personuppgifter som utförs av unionens institutioner, organ och byråer. Denna förordning går inte utöver vad som är nödvändigt för att uppnå de eftersträvade målen i enlighet med artikel 5.4 i fördraget om Europeiska unionen.

- **Val av instrument**

En förordning är det lämpliga rättsliga instrumentet för att fastställa ramen för skyddet av enskilda personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och för det fria flödet av sådana uppgifter. Den ger fysiska personer lagstadgade rättigheter och anger de skyldigheter som åligger de personuppgiftsansvariga vid unionens institutioner, organ, kontor och byråer. Den föreskriver också att en oberoende tillsynsmyndighet, Europeiska datatillsynsmannen, ska ansvara för

övervakningen av den behandling av personuppgifter som utförs av unionens institutioner, organ, kontor och byråer.

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

Kommissionen har genomfört samråd med berörda parter under 2010 och 2011 och en konsekvensanalys i samband med utarbetandet av reformpaketet för uppgiftsskydd som informerar om de ändringar som föreslås till förordning (EG) nr 45/2001. I detta sammanhang har kommissionen även genomfört en undersökning av kommissionens uppgiftsskyddssamordnare[5].

När det gäller den praktiska tillämpningen av förordning (EG) nr 45/2001 av unionens institutioner, organ och byråer, har uppgifter hämtats från Europeiska datatillsynsmannen, andra av unionens institutioner, organ, kontor och byråer, andra generaldirektorat inom kommissionen och en extern konsult. Ett frågeformulär sändes till nätverket av dataskyddsombud[6].

Dataskyddsombuden från ett antal av unionens institutioner, organ, kontor och byråer höll seminarier om reformen av förordning 45/2001 den 9 juli 2015, den 22 oktober 2015, den 19 januari 2016 och den 15 mars 2016.

Kommissionen beslutade 2013 att göra en utvärderingsstudie av tillämpningen av förordning (EG) nr 45/2001. Denna utvärdering lades ut på en extern konsult. De slutliga resultaten av utvärderingsstudien (slutlig rapport, fem fallstudier och analys av de enskilda artiklarna) överlämnades till kommissionen den 8 juni 2015[7].

Utvärderingen visade att det styrningssystem som strukturerats kring dataskyddsombuden och Europeiska datatillsynsmannen är effektiva. Det konstaterades att fördelningen av befogenheter mellan dataskyddsombud och Europeiska datatillsynsmannen är tydlig och väl avvägd och att båda har lämpliga befogenheter. Problem kan dock uppstå på grund av att dataskyddsombuden, på grund av otillräckligt stöd från deras ledning, inte kan utöva sina befogenheter på ett ändamålsenligt sätt.

I utvärderingsstudien angavs att förordning (EG) nr 45/2001 skulle kunna genomföras på ett bättre sätt med hjälp av sanktioner från Europeiska datatillsynsmannen. En ökad användning av dess befogenheter som tillsynsmyndighet skulle kunna leda till ett bättre genomförande av reglerna om skydd av personuppgifter. En annan slutsats var att de personuppgiftsansvariga bör anta en strategi för riskhantering och utföra riskbedömningar inför uppgiftsbehandling för att bättre leva upp till lagrings- och säkerhetskrav.

Undersökningen visade också att de befintliga bestämmelserna om telekommunikationssektorn i kapitel IV i förordning (EG) nr 45/2001 är inaktuella och att det

---

5 Se http://ec.europa.eu/justice/data-protection/reform/index_en.htm

6 Se Europeiska datatillsynsmannens allmänna rapport ”Measuring compliance with Regulation (EC) 45/2001 in EU institutions (Survey 2013)” och yttrande 3/2015 ”Europe’s big opportunity: EDPS recommendations on the EU’s options for data protection reform”.

7 JUST/2013/FRAC/FW/0157/A4 in the context of the multiple framework contract JUST/2011/EVAL/01 (RS 2013/05) - Evaluation Study on Regulation (EC) 45/2001, av Ernst and Young, tillgänglig på http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=51087

finns ett behov av att anpassa detta kapitel till direktivet om integritet och elektronisk kommunikation. Enligt utvärderingen finns det även ett behov av att förtydliga vissa viktiga definitioner i förordning (EG) nr 45/2001. Det rör sig bland annat om identifieringen av personuppgiftsansvariga i unionens institutioner, organ, kontor och byråer, om definitionen av mottagare och om en utvidgning av tystnadsplikten till externa personuppgiftsbiträden.

Utvärderingen pekade också på behovet av att förenkla systemet för anmälningar och förhandskontroller i syfte att öka effektiviteten och minska den administrativa bördan.

Utvärderaren genomförde en enkät vid 64 av unionens institutioner, byråer, organ och kontor. 422 tjänstemän med ansvar för personuppgiftsbiträden, 73 dataskyddsombud, 118 dataskyddssamordnare och 109 it-medarbetare besvarade frågorna i enkäten. Utvärderaren genomförde även en rad intervjuer med berörda parter. Den 26 mars 2015 anordnade utvärderaren och kommissionen en slutlig workshop, med deltagande av ett antal uppgiftsskyddsansvariga, dataskyddsombud, dataskyddssamordnare, it-medarbetare och företrädare för Europeiska datatillsynsmannen.

- **Insamling och användning av sakkunnigutlåtanden**

Se hänvisningen till utvärderingen under föregående punkt.

- **Konsekvensbedömning**

Konsekvenserna av föreliggande förslag kommer huvudsakligen att beröra unionens institutioner, organ, kontor och byråer. Detta har bekräftats av uppgifter som inhämtats från Europeiska datatillsynsmannen, andra av unionens institutioner, organ, kontor och byråer, kommissionens generaldirektorat och den externa uppdragstagaren. Dessutom har effekten av de nya skyldigheter som följer av förordning (EU) 2016/679, till vilken den här förordningen ska anpassas, bedömts i samband med det förberedande arbetet för de sistnämnda. Detta innebär att det inte behövs någon särskild konsekvensbedömning för denna förordning.

- **Lagstiftningens ändamålsenlighet och förenkling**

Ej tillämpligt

- **Grundläggande rättigheter**

Rätten till skydd av personuppgifter fastställs i artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan), i artikel 16 i EUF-fördraget och i artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Såsom har framhållits av Europeiska unionens domstol[8] är rätten till skydd av personuppgifter inte en absolut rättighet, utan ska beaktas i förhållande till dess funktion i samhället[9]. Uppgiftsskyddet är nära knutet till respekten för privatlivet och familjelivet som skyddas genom artikel 7 i stadgan.

---

[8] Domstolens dom av den 9 november 2010, Volker och Markus Schecke och Eifert, förenade målen C-92/09 och C-93/09, ECLI:EU:C:2009:284, punkt 48.

[9] I enlighet med artikel 52.1 i stadgan får utövandet av rätten till skydd av personuppgifter begränsas, under förutsättning att begränsningarna har fastställts i lag, är förenliga med det väsentliga innehållet i rättigheten och friheterna och, med beaktande av proportionalitetsprincipen, endast görs om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

Detta förslag föreskriver regler om skydd av enskilda personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och för det fria flödet av sådana uppgifter.

Andra grundläggande rättigheter som fastläggs i stadgan och som skulle kunna påverkas är yttrandefriheten (artikel 11), rätten till egendom och särskilt rätten till skydd av immateriell egendom (artikel 17.2), förbudet mot all diskriminering på grund av bland annat ras, etniskt ursprung, genetiska särdrag, religion eller övertygelse, politisk eller annan åskådning, funktionshinder eller sexuell läggning (artikel 21), barnets rättigheter (artikel 24), rätten till en hög nivå av skydd för människors hälsa (artikel 35), rätt till tillgång till handlingar (artikel 42), och rätt till ett effektivt rättsmedel och till en opartisk domstol (artikel 47)

4. BUDGETKONSEKVENSER

Se den bilagda finansieringsöversikten.

5. ÖVRIGA INSLAG

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

Ej tillämpligt

- **Förklarande dokument (för direktiv)**

Ej tillämpligt

KAPITEL I - ALLMÄNNA BESTÄMMELSER

I artikel 1 definieras förordningens syfte. Liksom i artikel 1 i förordning (EG) nr 45/2001 fastställs också de två målen för förordningen, nämligen att skydda den grundläggande rätten till skydd av personuppgifter och att garantera det fria flödet av personuppgifter i hela unionen. I denna artikel anges också de viktigaste uppgifterna för Europeiska datatillsynsmannen.

I artikel 2 fastställs förordningens tillämpningsområde: den ska vara tillämplig på alla unionsinstitutioners och unionsorgans behandling av personuppgifter, automatiserad eller ej, om denna behandling genomförs för att utföra uppgifter som helt eller delvis omfattas av unionsrätten. Det materiella tillämpningsområdet för denna förordning är tekniskt neutralt. Skyddet för personuppgifter gäller för både automatiserad och manuell behandling, om personuppgifterna ingår i eller är avsedda att ingå i ett register.

Artikel 3 innehåller definitioner av begrepp som används i förordningen. Förutom de definitioner av ”unionens institutioner och organ”, ”personuppgiftsansvarig”, ”användare” och ”register” som är specifika för denna förordning, definieras de termer som används i denna förordning i förordning (EU) 2016/679, förordning (EU) 0000/00 [ny förordning om integritet och elektronisk kommunikation], direktiv 00/0000/EU [direktiv om upprättandet av en europeisk kodex för elektronisk kommunikation] och kommissionens direktiv 2008/63/EG.

KAPITEL II – PRINCIPER

I artikel 4 fastställs principerna rörande behandling av personuppgifter, vilka motsvarar dem som anges i artikel 5 i förordning (EU) 2016/679. Jämfört med förordning (EG) nr 45/2001 tillförs nya principer om öppenhet och integritet och konfidentialitet.

Artikel 5 bygger på artikel 6 i förordning (EU) 2016/679 och anger kriterierna för laglig behandling, med som enda undantag kriteriet avseende den personuppgiftsansvariges berättigade intresse som inte är tillämplig på den offentliga sektorn och således inte bör tillämpas på unionsinstitutioner och unionsorgan. I artikel 5 bibehålls de kriterier som redan har fastställts enligt artikel 5 i förordning (EG) nr 45/2001.

Genom artikel 6 klargörs villkoren för behandling för ett annat jämförbart ändamål i överensstämmelse med artikel 6.4 i förordning (EU) 2016/679. Jämfört med artikel 6 i förordning (EG) nr 45/2001 ger denna nya bestämmelse större flexibilitet och rättssäkerhet när det gäller ytterligare behandling för förenliga ändamål.

I artikel 7 klargörs, i enlighet med artikel 7 i förordning (EU) 2016/679, villkoren för att samtycket ska vara giltigt som rättslig grund för laglig behandling.

I artikel 8 anges, i enlighet med artikel 8 i förordning (EU) 2016/679, ytterligare villkor för när det är lagligt att behandla barns personuppgifter i förhållande till sådana informationssamhällets tjänster som erbjuds direkt till dem. Där fastställs minimiåldern för giltigt samtycke till 13 år.

Artikel 9 innehåller, i överensstämmelse med artikel 8 i förordning (EG) nr 45/2001, regler som föreskriver en viss nivå av skydd för överföring av personuppgifter till mottagare, utöver unionsinstitutioner och unionsorgan, som är etablerade i unionen och som omfattas av förordning (EU) 2016/679 eller direktiv (EU) 2016/680. Det klargörs att om det är den personuppgiftsansvarige som initierar överföringen, bör denne kunna visa på att överföringen är nödvändig och proportionerlig.

I artikel 10 anges ett generellt förbud mot behandling av specifika kategorier av uppgifter samt undantagen från denna allmänna regel. Artikeln baserar sig på artikel 9 i förordning (EU) 2016/679 och är en vidareutveckling av artikel 10 i förordning (EG) nr 45/2001.

I artikel 11 anges, i enlighet med artikel 10 i förordning (EU) 2016/679 och i enlighet med artikel 10.5 i förordning (EG) nr 45/2001, villkoren för behandling av personuppgifter med anknytning till fällande domar i brottmål och lagöverträdelser.

I artikel 12 klargörs att den personuppgiftsansvariges informationsplikt gentemot den registrerade, i överensstämmelse med artikel 11 i förordning (EU) 2016/679. Det anges att om de personuppgifter som behandlas av en personuppgiftsansvarig inte gör det möjligt för denne att identifiera en fysisk person, bör den personuppgiftsansvarige inte vara tvungen att skaffa ytterligare information för att kunna identifiera den registrerade, om ändamålet endast är att följa någon av bestämmelserna i denna förordning. Den personuppgiftsansvarige bör dock inte vägra att ta emot kompletterande uppgifter som den registrerade lämnat till stöd för utövandet av sina rättigheter.

I artikel 13 fastställs, på grundval av artikel 89.1 i förordning (EU) 2016/679, reglerna om skyddsåtgärder för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

KAPITEL III – DEN REGISTRERADES RÄTTIGHETER

Avsnitt 1 – Insyn och villkor

Genom artikel 14 införs, på grundval av artikel 12 i förordning (EU) 2016/679, en skyldighet för personuppgiftsansvariga att tillhandahålla öppen, lättåtkomlig och begriplig information samt förfaranden och en mekanism för utövande av den registrerades rättigheter, inbegripet i förekommande fall hjälpmedel för elektronisk ingivna framställningar, med krav på svar på den registrerades begäran inom en fastställd tidsfrist och motivering av avslag. Eftersom unionsinstitutioner och unionsorgan inte under några förhållanden förväntas ta ut några avgifter med anknytning till de administrativa kostnaderna för att tillhandahålla informationen, har denna möjlighet inte övertagits från förordning (EU) 2016/679.

Avsnitt 2 – Information och tillgång till uppgifter

I artikel 15 fastställs, på grundval av artikel 13 i förordning (EU) 2016/679 och som en vidareutveckling av artikel 11 i förordning (EG) nr 45/2001, den personuppgiftsansvariges skyldighet att informera den registrerade när personuppgifter samlas in från denne. Det handlar om att lämna information till den registrerade om lagringsperioden, rätten att inge ett klagomål samt i samband med internationella överföringar.

I artikel 16 specificeras vidare, på grundval av artikel 14 i förordning (EU) 2016/679 och som en vidareutveckling av artikel 12 i förordning (EG) nr 45/2001, den personuppgiftsansvariges informationsplikt gentemot den registrerade om personuppgifterna inte har erhållits från den registrerade som lämnar information till den källa från vilken uppgifterna härrör. Man bibehåller även de möjliga undantagen i förordning (EU) 2016/679, vilket exempelvis innebär att det inte föreligger någon sådan skyldighet om den registrerade redan förfogar över informationen, tillhandahållandet av sådan information visar sig vara omöjligt eller skulle inbegripa en oproportionell ansträngning för den personuppgiftsansvarige, om personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätten eller om registreringen eller utlämnandet uttryckligen föreskrivs i lag. Detta kan till exempel gälla i förfaranden vid myndigheter som är behöriga med avseende på frågor om social trygghet eller hälso- och sjukvård.

I artikel 17 finns, i överensstämmelse med artikel 15 i förordning (EU) 2016/679 och som en vidareutveckling av artikel 13 i förordning (EG) nr 45/2001, bestämmelser om den registrerades rätt att få tillgång till sina personuppgifter. Vissa nya inslag har tillförts, såsom en skyldighet att informera de registrerade om lagringsperioden och om rätten till begära rättelse och radering och att inge klagomål.

Avsnitt 3 – Rättelse och radering

I artikel 18 anges den registrerades rätt till rättelse. Bestämmelsen baserar sig på artikel 16 i förordning (EU) 2016/679 och är en vidareutveckling av artikel 14 i förordning (EG) nr 45/2001.

I artikel 19 anges, i överensstämmelse med artikel 17 i förordning (EU) 2016/679 och som en vidareutveckling av artikel 16 i förordning (EG) nr 45/2001, den registrerades rätt att bli glömd och få sina uppgifter raderade. Där fastställs villkoren för rätten att bli glömd, inklusive skyldigheten för den personuppgiftsansvarige som har lämnat ut personuppgifterna att underrätta tredje parter om den registrerades begäran att få eventuella länkar till, eller kopior eller reproduktioner av dessa personuppgifter raderade.

Genom artikel 20 införs rätten att begränsa behandlingen i vissa fall, för att undvika det tvetydiga begreppet ”blockering” som används i förordning (EG) nr 45/2001 och för att säkra överensstämmelse med den nya terminologin enligt artikel 18 i förordning (EU) 2016/679.

Artikel 21 innehåller, i överensstämmelse med artikel 19 i förordning (EU) 2016/679 och som en vidareutveckling av artikel 17 i förordning (EG) nr 45/2001, bestämmelser om den personuppgiftsansvariges skyldighet att underrätta mottagare till vilka personuppgifter har lämnats ut om en eventuell rättelse eller radering av personuppgifter eller om en eventuell begränsning, om det inte visar sig vara omöjligt eller innebär en oproportionerligt stor ansträngning. Den personuppgiftsansvarige ska också underrätta den registrerade om dessa mottagare om han eller hon begär det.

Genom artikel 22 införs, i enlighet med artikel 20 i förordning (EU) 2016/679, den registrerades rätt till dataportabilitet, dvs. rätt att erhålla de personuppgifter som rör den registrerade och som den registrerade har tillhandahållit den personuppgiftsansvarige, eller att få sådana personuppgifter överförda direkt till en annan personuppgiftsansvarig, när detta är tekniskt möjligt. Som en förutsättning och för att ytterligare förbättra enskildas tillgång till sina personuppgifter, föreskrivs rätten att från den personuppgiftsansvarige erhålla uppgifterna i ett strukturerat, allmänt använt och maskinläsbart dataformat. Denna rättighet gäller endast om behandlingen grundar sig på den registrerades samtycke eller ett avtal som ingåtts av honom eller henne.

Avsnitt 4 – Rätt att göra invändningar och automatiserat individuellt beslutsfattande

I artikel 23 föreskrivs den registrerades rätt att göra invändningar. Bestämmelsen baserar sig på artikel 21 i förordning (EU) 2016/679 och är en vidareutveckling av artikel 18 i förordning (EG) nr 45/2001.

Artikel 24 rör den registrerades rätt att inte bli föremål för en åtgärd som enbart grundas på automatiserad behandling, inbegripet profilering. Bestämmelsen överensstämmer med artikel 22 i förordning (EU) 2016/679 och är en vidareutveckling av artikel 19 i förordning (EG) nr 45/2001.

Avsnitt 5 – Begränsningar

I artikel 25 ges utrymme för begränsningar av den registrerades rättigheter som fastställs i artiklarna 14–22 och i artiklarna 34 och 38 och av de principer som fastställs i artikel 4 (i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 14–22). Sådana begränsningar bör fastställas i rättsakter som antagits på grundval av fördragen eller unionsinstitutioners och unionsorgans interna regler. Om det inte föreskrivs någon möjlighet till en sådan begränsning i rättsakter som antagits på grundval av fördragen eller i unionsinstitutioners och unionsorgans interna regler, skulle de sistnämnda kunna införa en tillfällig begränsning om den sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna, med avseende på en specifik behandling, och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa ett eller flera av de ändamål som möjliggör begränsningar av den registrerades rättigheter. Denna lösning ligger i linje med artikel 23 i förordning (EU) 2016/679. Till skillnad från artikel 23 i förordning (EU) 2016/679 och i överensstämmelse med artikel 20 i förordning (EG) nr 45/2001 föreskriver denna bestämmelse dock ingen möjlighet att begränsa rätten att göra invändningar och rätten att inte bli föremål för beslut som enbart grundas på automatisk behandling. Kriterierna i fråga om begränsningar ligger i linje med Europeiska unionens stadga om de grundläggande rättigheterna och den europeiska konventionen om de mänskliga rättigheterna, såsom dessa

tolkas av Europeiska unionens domstol respektive Europeiska domstolen för de mänskliga rättigheterna.

KAPITEL IV – PERSONUPPGIFTSANSVARIG OCH PERSONUPPGIFTSBITRÄDE

Avsnitt 1 – Allmänna skyldigheter

Artikel 26 bygger på artikel 24 i förordning (EU) 2016/679 och inför ”principen om ansvarsskyldighet” genom att beskriva den personuppgiftsansvariges ansvar att följa förordningen och visa att så sker, bland annat genom att vidta lämpliga tekniska och organisatoriska åtgärder och, i förekommande fall, interna strategier och mekanismer för att säkerställa sådan efterlevnad. Artikel 24.3 i förordning (EU) 2016/679 behölls inte i denna bestämmelse, eftersom unionsinstitutionerna och unionsorganen inte bör ansluta sig till uppförandekoder eller certifieringsmekanismer.

I artikel 27 anges, i enlighet med artikel 25 i förordning (EU) 2016/679, den personuppgiftsansvariges skyldigheter utifrån principerna om inbyggt uppgiftsskydd och uppgiftsskydd som standard.

Artikel 28 om gemensamt personuppgiftsansvariga bygger på artikel 26 i förordning (EU) 2016/679 för att klargöra de gemensamt personuppgiftsansvarigas ansvar – oavsett om de är unionsinstitutioner eller unionsorgan eller inte – vad gäller förhållandet dem emellan och gentemot den registrerade. Denna bestämmelse tar upp situationen där alla gemensamt personuppgiftsansvariga omfattas av samma regelverk (denna förordning) och situationen där vissa omfattas av denna förordning och andra av en annan rättsakt (förordning (EU) 2016/679, direktiv (EU) 2016/680, direktiv (EU) 2016/681 och andra särskilda ordningar för uppgiftsskydd som rör unionsinstitutioner och unionsorgan).

Artikel 29 bygger på artikel 28 i förordning (EU) 2016/679 och är en vidareutveckling av artikel 23 i förordning (EG) nr 45/2001. Syftet är att förtydliga personuppgiftsbiträdenas ställning och skyldigheter, bland annat genom att ange att ett personuppgiftsbiträde som bryter mot förordningen genom att fastställa ändamålen med och medlen för en behandling ska anses vara en personuppgiftsansvarig med avseende på den behandlingen.

Artikel 30 om behandling under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende grundar sig på artikel 29 i förordning (EU) 2016/679, som föreskriver att personuppgiftsbiträdet eller en person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som har tillgång till personuppgifter, endast får behandla dessa uppgifter på instruktion från den personuppgiftsansvarige, såvida inte han eller hon är ålagd att göra det enligt unionsrätten eller medlemsstaternas nationella rätt.

Artikel 31 bygger på artikel 30 i förordning (EU) 2016/679 och inför en skyldighet för personuppgiftsansvariga och personuppgiftsbiträden att bevara dokumentation om all behandling som de ansvarar för, i stället för krav på förhandsanmälan till Europeiska datatillsynsmannen i enlighet med artikel 25 i förordning (EG) nr 45/2001 och till dataskyddsombudets register. I motsats till vad som gäller enligt förordning (EU) 2016/679 görs i denna bestämmelse inte någon hänvisning till företrädare, eftersom unionsinstitutioner inte kommer att ha företrädare, utan alltid kommer att ha dataskyddsombud. Hänvisningar till överföringar grundade på undantag för särskilda situationer i den mening som avses i förordning (EU) 2016/679 har inte bibehållits, eftersom dessa typer av överföringar inte tas upp i den här förordningen. Skyldigheten att föra ett register över behandling som utförts kan centraliseras till en unionsinstitution eller ett unionsorgan. I sådana fall har unionsinstitutioner

och unionsorgan möjlighet att bevara sina register över behandling i form av ett offentligt register.

I artikel 32 klargörs, på grundval av artikel 31 i förordning (EU) 2016/679, unionsinstitutioners och unionsorgans skyldighet att samarbeta med Europeiska datatillsynsmannen.

Avsnitt 2 – Säkerhet för personuppgifter och konfidentialitet för elektronisk kommunikation

Genom artikel 33 åläggs den personuppgiftsansvarige, i överensstämmelse med artikel 32 i förordning (EU) 2016/679 och som en vidareutveckling av artikel 22 i förordning (EG) nr 45/2001, att vidta lämpliga åtgärder för att säkerställa säkerheten vid behandling. Denna skyldighet utsträcks även till att omfatta personuppgiftsbiträden, oavsett avtal med den personuppgiftsansvarige.

Artikel 34 bygger på artikel 36 i förordning (EG) nr 45/2001 och säkerställer konfidentialitet vid elektronisk kommunikation inom unionens institutioner och organ.

Artikel 35 bygger på befintlig praxis vid unionsinstitutioner och unionsorgan och syftar till att skydda information rörande terminalutrustning för slutanvändare som går in på allmänt tillgängliga webbplatser och mobila applikationer som tillhandahålls av unionens institutioner och organ, i överensstämmelse med förordning (EU) nr XX/XXXX [ny förordning om integritet och elektronisk kommunikation], särskilt artikel 8 i denna.

Artikel 36 bygger på artikel 38 i förordning (EG) nr 45/2001 och syftar till att skydda personuppgifter i offentliga och interna register vid unionens institutioner och organ.

I artiklarna 37 och 38 införs en skyldighet att anmäla personuppgiftsincidenter, i överensstämmelse med artiklarna 33 och 34 i förordning (EU) 2016/679.

Avsnitt 3 – Konsekvensbedömning avseende dataskydd samt föregående samråd

Artikel 39 bygger på artikel 35 i förordning (EU) 2016/679 och inför en skyldighet för personuppgiftsansvariga och personuppgiftsbiträden att göra en konsekvensbedömning avseende dataskydd inför behandlingar som sannolikt kommer att utsätta fysiska personers rättigheter och friheter för hög risk. Denna skyldighet kommer särskilt att vara tillämplig vid systematisk och omfattande bedömning av personliga aspekter rörande fysiska personer på grundval automatisk behandling, inbegripet profilering, omfattande behandling av särskilda kategorier av uppgifter eller systematisk och storskalig övervakning av allmän plats.

Artikel 40 bygger på artikel 36 i förordning (EU) 2016/679 och rör de fall där tillstånd av, och samråd med, Europeiska datatillsynsmannen är obligatoriskt inför behandlingen. Första stycket i artikel 40 återger emellertid skäl 94 i förordning (EU) 2016/679 och syftar till att förtydliga omfattningen av skyldigheten att samråda.

Avsnitt 4 – Information och samråd i lagstiftningsprocessen

I artikel 41 föreskrivs en skyldighet för unionens institutioner och organ att informera Europeiska datatillsynsmannen vid utarbetandet av administrativa åtgärder och interna regler för behandling av personuppgifter.

I artikel 42 föreskrivs en skyldighet för kommissionen att samråda med Europeiska datatillsynsmannen efter antagandet av förslag till en rättsakt och av rekommendationer eller

förslag till rådet i enlighet med artikel 218 i EUF-fördraget och när den utarbetar delegerade akter eller genomförandeakter som inverkar på skyddet av enskilda personers rättigheter och friheter med avseende på behandlingen av personuppgifter. Om dessa akter är av särskild vikt för skyddet av enskilda personers fri- och rättigheter med avseende på behandlingen av personuppgifter, kan kommissionen också samråda med Europeiska dataskyddsstyrelsen. I sådana fall bör båda organen samordna sitt arbete i syfte att utfärda ett gemensamt yttrande. Det fastställs en tidsfrist på åtta veckor för utfärdande av råden i ovannämnda fall, med möjliga undantag för brådskande fall och i övrigt när så är lämpligt, t.ex. när kommissionen utarbetar delegerade akter och genomförandeakter.

Avsnitt 5 – Skyldighet att reagera på anmärkningar

I artikel 43 fastställs en skyldighet för personuppgiftsansvariga och personuppgiftsbiträden att reagera på anmärkningar efter det att Europeiska datatillsynsmannen beslutat att hänskjuta ett ärende till dem.

Avsnitt 6 – Dataskyddsombud

Artikel 44 bygger på artikel 37.1 a i förordning (EU) 2016/679 och artikel 24 i förordning (EG) nr 45/2001 och gör det obligatoriskt för unionens institutioner och organ att ha ett dataskyddsombud.

Artikel 45 bygger på artikel 38 i förordning (EU) 2016/679 och artikel 24 i förordning (EG) nr 45/2001 och anger dataskyddsombudets ställning.

Artikel 46 bygger på artikel 39 i förordning (EU) 2016/679 samt artikel 24 i, och andra och tredje punkterna i bilagan till, förordning (EG) nr 45/2001. Syftet är att ange dataskyddsombudets viktigaste uppgifter.

KAPITEL V – ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJELAND ELLER INTERNATIONELLA ORGANISATIONER

Artikel 47 bygger på artikel 9 i förordning (EG) nr 45/2001 och tar upp den allmänna principen, i enlighet med artikel 44 i förordning (EU) 2016/679, att överensstämmelse med andra bestämmelser i denna förordning och de villkor som fastställs i kapitel V är ett obligatoriskt krav vid varje överföring av personuppgifter till tredjeländer eller internationella organisationer, inbegripet vid vidareöverföring av personuppgifter från tredjelandet i fråga eller en internationell organisation till ett annat tredjeland eller till en annan internationell organisation.

I artikel 48 fastställs att en överföring av personuppgifter till ett tredjeland eller en internationell organisation får äga rum om kommissionen i enlighet med artikel 45.3 i förordning (EU) 2016/679 har beslutat att en adekvat nivå av skydd säkerställs i det berörda tredjelandet, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller inom den internationella organisationen, och personuppgifter överförs uteslutande för att möjliggöra utförandet av de uppgifter som omfattas av den personuppgiftsansvariges befogenheter. Punkterna 2 och 3 i denna artikel har hämtats från artikel 9 i förordning (EG) nr 45/2001, eftersom de är värdefulla inslag vad gäller övervakningen av skyddsnivån i tredje länder och i internationella organisationer.

Artikel 49 bygger på artikel 46 i förordning (EU) 2016/679 och föreskriver krav på vidtagande av lämpliga skyddsåtgärder vid överföringar till tredjeländer, om inget beslut vad gäller adekvat skydd har antagits av kommissionen. Det handlar i första hand om

standardiserade uppgiftsskyddsbestämmelser och avtalsklausuler. Bindande företagsregler, uppförandekoder och certifieringsmekanismer skulle kunna användas, i enlighet med förordning (EU) 2016/679, av andra personuppgiftsbiträden än unionens institutioner och organ. Punkt 4 i denna artikel, som tar upp unionsinstitutioners och unionsorgans skyldighet att informera Europeiska datatillsynsmannen om kategorier av fall där de har tillämpat denna artikel, motsvarar artikel 9.8 i förordning (EG) nr 45/2001 och bibehålls på grund av dess specifika karaktär. Punkt 5 bygger på skyddsklausulen för befintliga tillstånd i artikel 46.5 i förordning (EU) 2016/679.

I artikel 50 klargörs, i överensstämmelse med artikel 48 i förordning (EU) 2016/679, att ett domstolsbeslut eller beslut från myndigheter i tredjeland som kräver överföring eller utlämnande av personuppgifter får erkännas eller genomföras på något som helst sätt endast om det grundar sig på en internationell överenskommelse, såsom ett avtal om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen, utan att detta påverkar andra grunder för överföring enligt detta kapitel.

Artikel 51 bygger på artikel 49 i förordning (EU) 2016/679 och redogör för och förtydligar undantagen när det gäller överföring av uppgifter. Det handlar särskilt om uppgiftsöverföringar som krävs och är nödvändiga med hänsyn till skyddet av viktiga allmänintressen, exempelvis vid internationella uppgiftsöverföringar som involverar konkurrensmyndigheter eller skatte- eller tullmyndigheter, eller som görs mellan socialförsäkringsmyndigheter eller myndigheter med ansvar för fiskeriförvaltning. Punkt 5 om skyldigheten att informera Europeiska datatillsynsmannen om kategorier av fall där undantag har åberopats vid en överföring motsvarar den nuvarande artikel 9.8 i förordning (EG) nr 45/2001.

Artikel 52 bygger på artikel 50 i förordning (EU) 2016/679 och föreskriver uttryckligen internationella samarbetsmekanismer för skydd av personuppgifter mellan Europeiska datatillsynsmannen, i samarbete med kommissionen och Europeiska dataskyddsstyrelsen, och tillsynsmyndigheterna i tredjeländer.

KAPITEL VI – EUROPEISKA DATATILLSYNSMANNEN

Artikel 53 bygger på artikel 41 i förordning (EG) nr 45/2001 och rör inrättandet av Europeiska datatillsynsmannen.

Artikel 54 bygger på artikel 42 i förordning (EG) nr 45/2001 och artikel 3 i beslut 1247/2002/EG och fastställer reglerna för Europaparlamentets och rådets utnämning av Europeiska datatillsynsmannen. I denna artikel anges också Europeiska datatillsynsmannens mandattid: fem år.

Artikel 55 bygger på artikel 43 i förordning (EG) nr 45/2001 och artikel 1 i beslut 1247/2002/EG och innehåller regler och allmänna villkor för Europeiska datatillsynsmannens fullgörande av sina uppgifter samt om personal och finansiella resurser.

Artikel 56 bygger på artikel 52 i förordning (EU) 2016/679 och artikel 44 i förordning (EG) nr 45/2001 och förtydligar villkoren för Europeiska datatillsynsmannens oberoende, med hänsyn till rättspraxis från Europeiska unionens domstol.

I artikel 57 fastställs, på grundval av artikel 45 i förordning (EG) nr 45/2001, Europeiska datatillsynsmannens tystnadsplikt under och efter sin ämbetstid vad avser konfidentiell information som har kommit till hans eller hennes kännedom under tjänsteutövningen.

Artikel 58 bygger på artikel 57 i förordning (EU) 2016/679 och artikel 46 i förordning (EG) nr 45/2001 och anger Europeiska datatillsynsmannens uppgifter, bland annat att höra och utreda klagomål och främja medvetenheten om risker, regler, skyddsåtgärder och rättigheter.

Artikel 59 bygger på artikel 58 i förordning (EU) 2016/679 och artikel 47 i förordning (EG) nr 45/2001 och anger Europeiska datatillsynsmannens befogenheter.

Artikel 60 bygger på artikel 59 i förordning (EU) 2016/679 och artikel 48 i förordning (EG) nr 45/2001 och anger Europeiska datatillsynsmannens skyldighet att upprätta en årlig verksamhetsrapport.

KAPITEL VII – SAMARBETE OCH ENHETLIGHET

Artikel 61 bygger på artikel 61 i förordning (EU) 2016/679 och artikel 46 f i förordning (EG) nr 45/2001 och inför uttryckliga bestämmelser om samarbete mellan Europeiska datatillsynsmannen och nationella tillsynsmyndigheter.

I artikel 62 anges Europeiska datatillsynsmannens skyldigheter när andra unionsakter hänvisar till denna artikel inom ramen för samordnad tillsyn tillsammans med nationella tillsynsmyndigheter. Syftet är att införa en gemensam modell för samordnad tillsyn. Denna modell skulle kunna användas för samordnad tillsyn över stora it-system såsom Eurodac, Schengens informationssystem II, informationssystemet för viseringar, tullinformationssystemet eller informationssystemet för den inre marknaden, men också för tillsyn över vissa unionsbyråer, i sådana fall där en särskild modell för samarbete mellan Europeiska datatillsynsmannen och nationella myndigheter har införts, t.ex. Europol. Europeiska dataskyddsstyrelsen bör fungera som ett gemensamt forum för att säkerställa en effektiv samordnad tillsyn på ett övergripande plan.

KAPITEL VIII – RÄTTSMEDEL, ANSVAR OCH SANKTIONER

Artikel 63 bygger på artikel 77 i förordning (EU) 2016/679 och artikel 32 i förordning (EG) nr 45/2001 och föreskriver en rätt för alla registrerade att ge in klagomål till Europeiska datatillsynsmannen. Det fastställs också en skyldighet för Europeiska datatillsynsmannen att handlägga klagomålet och informera den registrerade om hur ärendet fortskrider och resultatet av klagomålet inom en tidsfrist på tre månader, varefter klagomålet ska anses ha avslagits.

I artikel 64 motsvarar artikel 32.1 i förordning (EG) nr 45/2001, som fastställer behörigheten för Europeiska unionens domstol att pröva tvister med anknytning till bestämmelserna i denna förordning, inklusive skadeståndsanspråk.

I artikel 65 fastställs rätten till ersättning, både för ekonomisk och för immateriell skada, med förbehåll för de villkor, bland annat rörande skadeståndsansvar, som föreskrivs i fördragen.

Artikel 66 bygger på artikel 83 i förordning (EU) 2016/679 och ger Europeiska datatillsynsmannen befogenhet att utfärda administrativa sanktionsavgifter till unionsinstitutioner och unionsorgan, som en sanktion att tillgripa i sista hand och endast om unionsinstitutionen eller unionsorganet har underlåtit att följa ett sådant beslut av Europeiska datatillsynsmannen som avses i artikel 59.2 a–h och j. I artikeln fastställs också kriterier för att besluta om beloppet för de administrativa sanktionsavgifterna i varje enskilt fall, medan de maximala årliga taken har inspirerats av storleken på de avgifter som tillämpas i vissa medlemsstater.

Artikel 67 ger möjlighet, i överensstämmelse med artikel 80.1 i förordning (EU) 2016/679, för vissa organ, organisationer eller sammanslutningar att ge in klagomål på en registrerad persons vägnar.

I artikel 68 föreskrivs, i överensstämmelse med artikel 33 i förordning (EG) nr 45/2001, särskilda regler som syftar till att skydda unionsanställda som framför klagomål till Europeiska datatillsynsmannen om en påstådd överträdelse av bestämmelserna i denna förordning utan att gå den officiella vägen.

Artikel 69 bygger på artikel 49 i förordning (EG) nr 45/2001 och anger vilka sanktioner som är tillämpliga om tjänstemän eller andra anställda i Europeiska unionen underlåter att uppfylla skyldigheterna enligt denna förordning.

KAPITEL IX – GENOMFÖRANDEAKTER

Artikel 70 innehåller en bestämmelse om det kommittéförfarande som behövs för att tilldela kommissionen genomförandebefogenheter i sådana fall där det, i enlighet med artikel 291 i EUF-fördraget, är nödvändigt med enhetliga villkor för genomförandet av unionens rättsligt bindande akter. Granskningsförfarandet är tillämpligt.

KAPITEL X – SLUTBESTÄMMELSER

Artikel 71 upphäver förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG och föreskriver att hänvisningar till de båda upphävda rättsakterna ska tolkas som hänvisningar till den här förordningen.

I artikel 72 klargörs att det nuvarande mandatet för Europeiska datatillsynsmannen och den biträdande datatillsynsmannen inte ska påverkas av denna förordning och att artiklarna 54.4, 54.5 och 54.7 samt artiklarna 56 och 57 i förordningen tillämpas på den nuvarande biträdande datatillsynsmannen fram till slutet av mandatperioden, dvs. till och med den 5 december 2019.

I artikel 73 fastställs ikraftträdandedagen för denna förordning till den 25 maj 2018, för att säkerställa överensstämmelse med den dag då förordning (EU) 2016/679 börjar tillämpas.

2017/0002 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om skydd för enskilda personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ, kontor och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut 1247/2002/EG

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16.2,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[10],

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) Skyddet för fysiska personer vid behandling av personuppgifter är en grundläggande rättighet. Artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) och artikel 16.1 i fördraget om Europeiska unionens funktionssätt (nedan kallat *EUF-fördraget*) föreskriver att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

(2) Europaparlamentets och rådets förordning (EG) nr 45/2001[11] föreskriver verkställbara rättigheter för fysiska personer, anger de skyldigheter i fråga om behandling av personuppgifter som åligger personuppgiftsansvariga inom gemenskapsinstitutionerna och gemenskapsorganen, och inrättar en oberoende tillsynsmyndighet, Europeiska datatillsynsmannen, vars uppgift är att övervaka behandlingen av personuppgifter vid unionens institutioner och organ. Den är emellertid inte tillämplig på behandling av personuppgifter som utgör ett led i sådan verksamhet vid unionsinstitutioner eller unionsorgan vilken inte omfattas av unionsrätten.

(3) Europaparlamentets och rådets förordning (EU) 2016/679[12] och Europaparlamentets och rådets direktiv (EU) 2016/680[13] antogs den 27 april 2016. Medan förordningen fastställer allmänna regler som syftar till att skydda fysiska personer vid behandling av personuppgifter och att säkerställa det fria flödet av personuppgifter inom unionen, fastställs i direktivet särskilda regler som syftar till att skydda fysiska personer i samband med behandlingen av personuppgifter och att säkerställa det fria flödet av personuppgifter inom unionen på områdena för straffrättsligt samarbete och polissamarbete.

(4) I förordning (EU) 2016/679 betonas behovet av nödvändiga anpassningar av förordning (EG) nr 45/2001 för att tillhandahålla en stark och sammanhängande ram för dataskyddet inom unionen och möjliggöra samtidig tillämpning av förordning (EU) 2016/679.

(5) För att främja en konsekvent strategi för skyddet av personuppgifter i hela unionen och för det fria flödet av personuppgifter inom unionen, är det viktigt att så långt som möjligt anpassa de regler om skydd av personuppgifter som gäller för

---

10 EUT C , , s. .

11 Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

12 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.

13 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).

unionsinstitutioner och unionsorgan till de regler om skydd för personuppgifter som har antagits för den offentliga sektorn i medlemsstaterna. När en bestämmelse i denna förordning bygger på samma koncept som en bestämmelse i förordning (EU) 2016/679 bör dessa båda bestämmelser tolkas enhetligt, särskilt eftersom den systematik som denna förordning bygger på bör uppfattas som en motsvarighet till systematiken bakom förordning (EU) 2016/679.

(6) Personer vars personuppgifter behandlas av unionens institutioner och organ bör skyddas, oavsett i vilket sammanhang behandlingen sker, exempelvis på grund av att de är anställda av dessa institutioner och organ. Denna förordning bör inte vara tillämplig på behandling av personuppgifter som rör avlidna personer. Denna förordning omfattar inte behandling av personuppgifter som rör juridiska personer, särskilt företag som bildats som juridiska personer, exempelvis uppgifter om namn på och typ av juridisk person samt kontaktuppgifter.

(7) För att förhindra att det uppstår en allvarlig risk för att reglerna kringgås bör skyddet för fysiska personer vara teknikneutralt och inte vara beroende av den teknik som används. Skyddet för fysiska personer bör vara tillämpligt på både automatiserad och manuell behandling av personuppgifter, om personuppgifterna ingår i eller är avsedda att ingå i ett register. Akter eller grupper av akter samt omslag till dessa, som inte är ordnade enligt särskilda kriterier, bör inte omfattas av denna förordning.

(8) I förklaring nr 21 om skydd av personuppgifter på området för straffrättsligt samarbete och polissamarbete, fogad till slutakten från den regeringskonferens som antog Lissabonfördraget, bekräftade konferensen att det med hänsyn till dessa områdens särart kan komma att bli nödvändigt att anta särskilda regler om skydd av personuppgifter och om det fria flödet av personuppgifter på områdena för straffrättsligt samarbete och polissamarbete med stöd av artikel 16 i EUF-fördraget. Denna förordning bör därför tillämpas på unionsbyråer som bedriver verksamhet på området för straffrättsligt samarbete och polissamarbete endast i den utsträckning som unionslagstiftning som är tillämplig på sådana byråer inte innehåller några särskilda regler om behandling av personuppgifter.

(9) Direktiv (EU) 2016/680 innehåller harmoniserade regler om skydd och fri rörlighet för personuppgifter som behandlas i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. I syfte att främja en enhetlig skyddsnivå för skyddet av fysiska personer genom rättsligt verkställbara rättigheter i hela unionen och undvika avvikelser som hämmar utbytet av personuppgifter mellan å ena sidan unionsbyråer som bedriver verksamhet inom områdena rättsligt samarbete i straffrättsliga frågor och polissamarbete, å andra sidan medlemsstaternas behöriga myndigheter, bör reglerna om skyddet av och den fria rörligheten för operativa personuppgifter som behandlas av sådana unionsbyråer bygga på de principer som ligger till grund för denna förordning och vara förenliga med direktiv (EU) 2016/680.

(10) Om grundakten för ett unionsorgan som bedriver verksamhet som omfattas av tillämpningsområdet för kapitlen 4 och 5 i avdelning V i fördraget föreskriver ett fristående system för uppgiftsskydd vad avser behandlingen av operativa personuppgifter, bör detta system inte påverkas av denna förordning. Kommissionen bör dock, i enlighet med artikel 62 i direktiv (EU) 2016/680, senast den 6 maj 2019 se över unionsakter som reglerar behandling som utförs av behöriga myndigheter i syfte

att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot samt förebygga hot mot den allmänna säkerheten och, när så är lämpligt, lägga fram nödvändiga förslag till ändring av dessa rättsakter för att säkerställa ett enhetligt tillvägagångssätt för att skydda personuppgifter inom området för straffrättsligt samarbete och polissamarbete.

(11) Principerna för dataskyddet bör gälla all information som rör en identifierad eller identifierbar fysisk person. Personuppgifter som har pseudonymiserats och som skulle kunna tillskrivas en fysisk person genom att kompletterande uppgifter används bör anses som uppgifter om en identifierbar fysisk person. För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel, som t.ex. utgallring, som, antingen av den personuppgiftsansvarige eller av en annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen. Principerna för dataskyddet bör därför inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar. Denna förordning berör därför inte behandling av sådan anonym information, vilket inbegriper information för statistiska ändamål eller forskningsändamål.

(12) Tillämpningen av pseudonymisering av personuppgifter kan minska riskerna för de registrerade som berörs och hjälpa personuppgiftsansvariga och personuppgiftsbiträden att fullgöra sina skyldigheter i fråga om dataskydd. Ett uttryckligt införande av pseudonymisering i denna förordning är inte avsett att utesluta andra åtgärder för dataskydd.

(13) Fysiska personer kan knytas till nätidentifierare som lämnas av deras utrustning, applikationer, verktyg och protokoll, t.ex. ip-adresser, kakor eller andra identifierare, som radiofrekvensetiketter. Detta kan efterlämna spår som, särskilt i kombination med unika identifierare och andra uppgifter som tas emot av servrarna, kan användas för att skapa profiler för fysiska personer och identifiera dem.

(14) Samtycke bör lämnas genom en entydig bekräftande handling som innebär ett frivilligt, specifikt, informerat och otvetydigt medgivande från den registrerades sida om att denne godkänner behandling av personuppgifter rörande honom eller henne, som t.ex. genom en skriftlig, inklusive elektronisk, eller muntlig förklaring. Detta kan inbegripa att en ruta kryssas i vid besök på en internetsida, genom val av inställningsalternativ för tjänster på informationssamhällets område eller genom någon annan förklaring eller något annat beteende som i sammanhanget tydligt visar att den registrerade godtar den avsedda behandlingen av sina personuppgifter. Tystnad, på förhand ikryssade rutor eller inaktivitet bör därför inte utgöra samtycke. Samtycket bör gälla all behandling som utförs för samma ändamål. Om behandlingen tjänar flera olika syften, bör samtycke ges för samtliga syften. Om den registrerade ska lämna sitt samtycke efter en elektronisk begäran, måste denna vara tydlig och koncis och får inte onödigtvis störa användningen av den tjänst som den avser.

(15) Varje behandling av personuppgifter måste vara laglig och rättvis. Det bör vara klart och tydligt för fysiska personer hur personuppgifter som rör dem insamlas, används,

konsulteras eller på annat sätt behandlas samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas. Öppenhetsprincipen kräver att all information och kommunikation i samband med behandlingen av dessa personuppgifter är lättillgänglig och lättbegriplig samt att ett klart och tydligt språk används. Den principen gäller framför allt informationen till registrerade om den personuppgiftsansvariges identitet och syftet med behandlingen samt ytterligare information för att sörja för en rättvis och öppen behandling för berörda fysiska personer och deras rätt att erhålla bekräftelse på och meddelande om vilka personuppgifter rörande dem som behandlas. Fysiska personer bör göras medvetna om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter och om hur de kan utöva sina rättigheter med avseende på behandlingen. De specifika ändamål som personuppgifterna behandlas för bör vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in. Personuppgifterna bör vara adekvata, relevanta och begränsade till vad som är nödvändigt för de ändamål som de behandlas för. Detta kräver i synnerhet att det tillses att den period under vilken personuppgifterna lagras är begränsad till ett strikt minimum. Personuppgifter bör endast behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel. För att säkerställa att personuppgifter inte sparas längre än nödvändigt bör den personuppgiftsansvarige införa tidsfrister för radering eller för regelbunden kontroll. Alla rimliga åtgärder bör vidtas för att rätta eller radera felaktiga uppgifter. Personuppgifter bör behandlas på ett sätt som säkerställer lämplig säkerhet och konfidentialitet för personuppgifterna samt förhindrar obehörigt tillträde till och obehörig användning av personuppgifter och den utrustning som används för behandlingen.

(16) I enlighet med principen om ansvarsskyldighet bör unionens institutioner och organ, i samband med att de överför personuppgifter internt eller till andra av unionens institutioner och organ, kontrollera om sådana personuppgifter är nödvändiga för det legitima utförandet av uppgifter som omfattas av mottagarens befogenheter, om mottagaren är inte en del av den personuppgiftsansvarige. Efter en mottagares begäran om överföring av uppgifter bör den personuppgiftsansvarige kontrollera att det föreligger en relevant grund för laglig behandling av personuppgifter och att mottagaren är behörig. Den personuppgiftsansvarige bör också göra en preliminär bedömning av om överföringen av uppgifterna är nödvändig. Om det uppstår tveksamhet om nödvändigheten bör den personuppgiftsansvarige begära ytterligare förklaringar från mottagaren. Mottagaren bör se till att man senare kan kontrollera att överföringen av uppgifterna var nödvändig.

(17) För att behandling ska vara laglig bör personuppgifterna behandlas med hänsyn till nödvändigheten av att unionsinstitutioner och unionsorgan utför en uppgift av allmänt intresse eller som ett led i deras myndighetsutövning, nödvändigheten av att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller någon annan legitim grund som anges i denna förordning, inbegripet samtycke från den registrerade eller en nödvändighet som hänför sig till fullgörandet ett avtal i vilket den registrerade är part eller vidtagandet av åtgärder på begäran av den registrerade innan ett sådant avtal ingås. Behandling av personuppgifter för utförandet av de arbetsuppgifter av allmänt intresse som unionsinstitutionerna och unionsorganen utför inbegriper sådan behandling av personuppgifter som är nödvändig för förvaltningen av dessa institutioner och organ för att de ska fungera. Behandling av personuppgifter bör även anses laglig när den är nödvändig för att skydda ett intresse som är av avgörande betydelse för den registrerades eller en annan fysisk persons liv. Behandling av personuppgifter på grundval av en annan fysisk persons grundläggande intressen bör i

princip endast äga rum om behandlingen inte uppenbart kan ha en annan rättslig grund. Vissa typer av behandling kan tjäna både viktiga allmänintressen och intressen som är av grundläggande betydelse för den registrerade, till exempel när behandlingen är nödvändig av humanitära skäl, bland annat för att övervaka epidemier och deras spridning eller i humanitära nödsituationer, särskilt vid naturkatastrofer eller katastrofer orsakade av människan.

(18) De unionsrättsliga och de interna regler som det hänvisas till i denna förordning bör vara tydliga och precisa och deras tillämpning bör vara förutsägbar för personer som omfattas av dem, i enlighet med rättspraxis från Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna.

(19) Behandling av personuppgifter för andra ändamål än de för vilka de ursprungligen samlades in bör endast vara tillåten när detta är förenligt med de ändamål för vilka personuppgifterna ursprungligen samlades in. I dessa fall krävs det inte någon annan separat rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs. Om behandlingen är nödvändig för att fullgöra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som den personuppgiftsansvarige har fått i uppgift att utföra, kan unionsrätten fastställa och närmare ange för vilka uppgifter och syften ytterligare behandling bör betraktas som förenlig och laglig. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör betraktas som förenlig och laglig behandling av uppgifter. Den rättsliga grund för behandling av personuppgifter som återfinns i unionsrätten kan också utgöra en rättslig grund för ytterligare behandling. För att fastställa om ett ändamål med den ytterligare behandlingen är förenligt med det ändamål för vilket personuppgifterna ursprungligen insamlades bör den personuppgiftsansvarige, efter att ha uppfyllt alla krav vad beträffar den ursprungliga behandlingens lagenlighet, bland annat beakta alla kopplingar mellan dessa ändamål och ändamålen med den avsedda ytterligare behandlingen, det sammanhang inom vilket personuppgifterna insamlats, särskilt de registrerades rimliga förväntningar till följd av förhållandet till den personuppgiftsansvarige i fråga om den framtida användningen, personuppgifternas art, den planerade ytterligare behandlingens konsekvenser för de registrerade, samt förekomsten av lämpliga skyddsåtgärder för både den ursprungliga och den planerade ytterligare behandlingen.

(20) När behandling sker efter samtycke från registrerade, bör personuppgiftsansvariga kunna visa att de registrerade har lämnat sitt samtycke till behandlingen. I synnerhet vid skriftliga förklaringar som rör andra frågor bör det finnas skyddsåtgärder som säkerställer att de registrerade är medvetna om att samtycke ges och om hur långt samtycket sträcker sig. I enlighet med rådets direktiv 93/13/EEG[14] bör en förklaring om samtycke som den personuppgiftsansvarige i förväg formulerat tillhandahållas i en begriplig och lätt tillgänglig form, med användning av ett klart och tydligt språk och utan oskäliga villkor. För att samtycket ska vara informerat bör den registrerade känna till åtminstone den personuppgiftsansvariges identitet och syftet med den behandling för vilken personuppgifterna är avsedda. Samtycke bör inte betraktas som frivilligt om den registrerade inte har någon genuin eller fri valmöjlighet eller inte utan problem kan vägra eller ta tillbaka sitt samtycke.

---

[14] Rådets direktiv 93/13/EEG av den 5 april 1993 om oskäliga villkor i konsumentavtal (EGT L 95, 21.4.1993, s. 29).

(21) Barns personuppgifter förtjänar särskilt skydd, eftersom barn kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder samt om sina rättigheter när det gäller behandling av personuppgifter. Sådant särskilt skydd bör i synnerhet vara tillämpligt på skapande av personlighetsprofiler samt insamling av personuppgifter med avseende på barn i samband med användning av tjänster som erbjuds direkt till barn på webbplatser som tillhör unionsinstitutioner och unionsorgan, såsom interpersonella kommunikationstjänster eller internetförsäljning av biljetter, och när behandlingen av personuppgifter grundar sig på samtycke.

(22) När mottagare som är etablerade i unionen och som omfattas av förordning (EU) 2016/679 eller direktiv (EU) 2016/680 vill få personuppgifter överförda till sig av unionsinstitutioner och unionsorgan, bör dessa mottagare visa att överföringen är nödvändig för att de ska kunna uppnå sin målsättning samt är proportionerlig och inte går utöver vad som är nödvändigt för att uppnå denna målsättning. Unionens institutioner och organ bör visa att det föreligger en sådan nödvändighet när de själva initierar överföringen, i överensstämmelse med principen om öppenhet.

(23) Personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheter och friheter bör åtnjuta särskilt skydd, eftersom behandling av sådana uppgifter kan innebära betydande risker för de grundläggande rättigheterna och friheterna. Dessa personuppgifter bör även inbegripa personuppgifter som avslöjar ras eller etniskt ursprung, varvid användningen av termen ras i denna förordning inte innebär att unionen godtar teorier som söker fastställa förekomsten av skilda människoraser. Behandling av foton bör inte systematiskt anses utgöra behandling av särskilda kategorier av personuppgifter, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person. Utöver de särskilda kraven för behandling av känsliga uppgifter, bör de allmänna principerna och andra bestämmelser i denna förordning tillämpas, särskilt när det gäller villkoren för laglig behandling. Undantag från det allmänna förbudet att behandla sådana särskilda kategorier av personuppgifter bör uttryckligen fastställas, bland annat om den registrerade lämnar sitt uttryckliga samtycke eller för att tillgodose specifika behov, i synnerhet när behandlingen utförs inom ramen för legitima verksamheter som bedrivs av vissa sammanslutningar eller stiftelser i syfte att göra det möjligt att utöva grundläggande friheter.

(24) På folkhälsoområdet kan det bli nödvändigt att med hänsyn till ett allmänt intresse behandla särskilda kategorier av personuppgifter utan att den registrerades samtycke inhämtas. Sådan behandling bör förutsätta lämpliga och särskilda åtgärder för att skydda fysiska personers rättigheter och friheter. I detta sammanhang bör folkhälsa tolkas enligt definitionen i Europaparlamentets och rådets förordning (EG) nr 1338/2008[15], nämligen alla aspekter som rör hälsosituationen, dvs. allmänhetens hälsotillstånd, inbegripet sjuklighet och funktionshinder, hälsans bestämningsfaktorer, hälso- och sjukvårdsbehov, resurser inom hälso- och sjukvården, tillhandahållande av och allmän tillgång till hälso- och sjukvård, utgifter för och finansiering av hälso- och sjukvården samt dödsorsaker. Sådan behandling av uppgifter om hälsa av allmänt intresse bör inte innebära att personuppgifter behandlas för andra ändamål av tredje part.

---

[15] Europaparlamentets och rådets förordning (EG) nr 1338/2008 av den 16 december 2008 om gemenskapsstatistik om folkhälsa och hälsa och säkerhet i arbetet (EUT L 354, 31.12.2008, s. 70).

(25) Om de personuppgifter som behandlas av en personuppgiftsansvarig inte gör det möjligt för denne att identifiera en fysisk person, bör den personuppgiftsansvarige inte vara tvungen att skaffa ytterligare information för att kunna identifiera den registrerade, om ändamålet endast är att följa någon av bestämmelserna i denna förordning. Den personuppgiftsansvarige bör dock inte vägra att ta emot kompletterande uppgifter som den registrerade lämnat till stöd för utövandet av sina rättigheter. Identifiering bör omfatta digital identifiering av en registrerad, till exempel genom en autentiseringsmekanism, exempelvis samma identifieringsinformation som används av den registrerade för att logga in på den nättjänst som tillhandahålls av den personuppgiftsansvarige.

(26) Behandlingen av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör omfattas av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt denna förordning. Skyddsåtgärderna bör säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt principen om uppgiftsminimering iakttas. Ytterligare behandling av personuppgifter för arkivändamål av allmänintresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör genomföras, när den personuppgiftsansvarige har bedömt möjligheten att uppnå dessa ändamål genom behandling av personuppgifter som inte medger eller inte längre medger identifiering av de registrerade, förutsatt att det finns lämpliga skyddsåtgärder (t.ex. pseudonymisering av personuppgifter). Unionens institutioner och organ bör införa lämpliga skyddsåtgärder för behandlingen av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i unionsrätten, vilket kan inbegripa interna regler.

(27) Förfaranden bör fastställas som gör det lättare för registrerade att utöva sina rättigheter enligt denna förordning, inklusive mekanismer för att begära och i förekommande fall kostnadsfritt få tillgång till och erhålla rättelse eller radering av personuppgifter samt för att utöva rätten att göra invändningar. Den personuppgiftsansvarige bör också tillhandahålla hjälpmedel för elektroniskt ingivna framställningar, särskilt i fall då personuppgifter behandlas elektroniskt. Personuppgiftsansvariga bör utan onödigt dröjsmål och senast inom en månad vara skyldiga att besvara registrerades önskemål och lämna en motivering, om de inte avser att uppfylla sådana önskemål.

(28) Principerna om rättvis och öppen behandling fordrar att den registrerade informeras om att behandling sker och syftet med den. Den personuppgiftsansvarige bör till den registrerade lämna all ytterligare information som krävs för att säkerställa en rättvis och öppen behandling, med beaktande av personuppgiftsbehandlingens specifika omständigheter och sammanhang. Dessutom bör den registrerade informeras om förekomsten av profilering samt om konsekvenserna av sådan profilering. Om personuppgifterna samlas in från den registrerade, bör denne även informeras om huruvida han eller hon är skyldig att tillhandahålla personuppgifterna och om konsekvenserna om han eller hon inte lämnar dem. Denna information får tillhandahållas tillsammans med standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över den planerade behandlingen. Om sådana symboler visas elektroniskt bör de vara maskinläsbara.

(29) Information om behandling av personuppgifter som rör den registrerade bör lämnas till honom eller henne vid den tidpunkt då personuppgifterna samlas in från den registrerade eller, om personuppgifterna erhålls direkt från en annan källa, inom en rimlig period, beroende på omständigheterna i fallet. Om personuppgifter legitimt kan

lämnas ut till en annan mottagare, bör de registrerade informeras första gången personuppgifterna lämnas ut till denna mottagare. Om den personuppgiftsansvarige avser att behandla personuppgifter för ett annat ändamål än det för vilket uppgifterna insamlades, bör denne före denna ytterligare behandling informera den registrerade om detta andra syfte och lämna annan nödvändig information. Om personuppgifternas ursprung inte kan meddelas den registrerade på grund av att olika källor har använts, bör allmän information ges.

(30) Den registrerade bör ha rätt att få tillgång till personuppgifter som insamlats om denne samt på enkelt sätt och med rimliga intervall kunna utöva denna rätt, för att vara medveten om att behandling sker och kunna kontrollera att den är laglig. Detta innefattar rätten för registrerade att få tillgång till uppgifter om sin hälsa, exempelvis uppgifter i läkarjournaler med t.ex. diagnoser, undersökningsresultat, bedömningar av behandlande läkare och eventuella vårdbehandlingar eller interventioner. Alla registrerade bör därför ha rätt att få kännedom och underrättelse om framför allt orsaken till att personuppgifterna behandlas, om möjligt vilken tidsperiod behandlingen pågår, vilka som mottar personuppgifterna, bakomliggande logik i samband med automatisk behandling av personuppgifter och, åtminstone när behandlingen bygger på profilering, konsekvenserna av sådan behandling. Denna rätt bör inte inverka menligt på andras rättigheter eller friheter, t.ex. affärshemligheter eller immateriell äganderätt och särskilt inte på upphovsrätt som skyddar programvaran. Resultatet av dessa överväganden bör dock inte bli att den registrerade förvägras all information. Om den personuppgiftsansvarige behandlar en stor mängd uppgifter om den registrerade, bör den personuppgiftsansvarige kunna begära att den registrerade lämnar uppgift om vilken information eller vilken behandling en framställan avser, innan informationen lämnas ut.

(31) Den registrerade bör ha rätt att få sina personuppgifter rättade och rätt att bli ”glömd”, om lagringen av uppgifterna strider mot denna förordning eller unionsrätt som den personuppgiftsansvarige omfattas av. En registrerad bör ha rätt att få sina personuppgifter raderade och kunna begära att dessa personuppgifter inte behandlas, om de inte längre behövs med tanke på de ändamål för vilka de samlats in eller på annat sätt behandlats, om en registrerad har återtagit sitt samtycke till behandling eller invänder mot behandling av personuppgifter som rör honom eller henne, eller om behandlingen av hans eller hennes personuppgifter på annat sätt inte överensstämmer med denna förordning. Denna rättighet är särskilt relevant när den registrerade har gett sitt samtycke som barn, utan att vara fullständigt medveten om riskerna med behandlingen, och senare vill ta bort dessa personuppgifter, särskilt på internet. Den registrerade bör kunna utöva denna rätt även när han eller hon inte längre är barn. Ytterligare lagring av personuppgifterna bör dock vara laglig, om detta krävs för att utöva yttrandefrihet och informationsfrihet, för att uppfylla en rättslig förpliktelse, för att utföra en uppgift i av allmänt intresse eller som ett led i myndighetsutövning som anförtrotts den personuppgiftsansvarige, med anledning av ett allmänt intresse inom folkhälsoområdet, för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål eller för fastställande, utövande eller försvar av rättsliga anspråk.

(32) För att stärka rätten att bli ”glömd” i nätmiljön bör rätten till radering utvidgas på så sätt att en personuppgiftsansvarig som har offentliggjort personuppgifter bör vara skyldig instruera de personuppgiftsansvariga som behandlar dessa personuppgifter att radera alla länkar till eller kopior eller reproduktioner av dessa personuppgifter. I samband med detta bör den personuppgiftsansvarige vidta rimliga åtgärder, med

beaktande av tillgänglig teknik och de hjälpmedel som står den personuppgiftsansvarige till buds, däribland tekniska åtgärder, för att informera de personuppgiftsansvariga som behandlar personuppgifterna om den registrerades begäran.

(33) Sätten att begränsa behandlingen av personuppgifter kan bland annat inbegripa att man tillfälligt flyttar de valda personuppgifterna till ett annat databehandlingssystem, gör de valda uppgifterna otillgängliga för användare eller tillfälligt avlägsnar offentliggjorda uppgifter från en webbplats. I automatiserade register bör begränsningen av behandlingen i princip ske med tekniska medel på ett sådant sätt att personuppgifterna inte blir föremål för ytterligare behandling och inte kan ändras. Det förhållandet att behandlingen av personuppgifter är begränsad bör klart anges inom systemet.

(34) För att ytterligare förbättra kontrollen över sina egna uppgifter bör den registrerade, om personuppgifterna behandlas automatiskt, också tillåtas att motta de personuppgifter som rör honom eller henne, som han eller hon har tillhandahållit den personuppgiftsansvarige, i ett strukturerat, allmänt använt, maskinläsbart och kompatibelt format och överföra dessa till en annan personuppgiftsansvarig. Personuppgiftsansvariga bör uppmuntras att utveckla kompatibla format som möjliggör dataportabilitet. Denna rättighet bör vara tillämplig om den registrerade har tillhandahållit uppgifterna efter att ha lämnat sitt samtycke eller om behandlingen är nödvändig för att ett avtal ska kunna genomföras. Därför bör den inte vara tillämplig när behandlingen av personuppgifterna är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som utförs av den personuppgiftsansvarige. Den registrerades rätt att överföra eller motta personuppgifter som rör honom eller henne innebär inte någon skyldighet för de personuppgiftsansvariga att införa eller upprätthålla behandlingssystem som är tekniskt kompatibla. Om mer än en registrerad berörs inom en viss uppsättning personuppgifter, bör rätten att motta personuppgifterna inte inverka på andra registrerades rättigheter och friheter enligt denna förordning. Denna rättighet bör inte heller påverka den registrerades rätt att få till stånd radering av personuppgifter och de inskränkningar av denna rättighet vilka anges i denna förordning och bör i synnerhet inte medföra radering av personuppgifter om den registrerade som denne har lämnat för genomförande av ett avtal, i den utsträckning och så länge som personuppgifterna krävs för genomförande av avtalet. Om det är tekniskt möjligt, bör den registrerade ha rätt till direkt överföring av personuppgifterna från en personuppgiftsansvarig till en annan.

(35) När personuppgifter lagligen får behandlas, eftersom behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i en myndighetsutövning som utförs av den personuppgiftsansvarige, bör alla registrerade ändå ha rätt att göra invändningar mot behandling av personuppgifter som rör de registrerades särskilda situation. Det bör ankomma på den personuppgiftsansvarige att visa att dennes tvingande berättigade intressen väger tyngre än den registrerades intressen eller grundläggande rättigheter och friheter.

(36) Den registrerade bör ha rätt att inte bli föremål för ett beslut, vilket kan inbegripa en åtgärd, med bedömning av personliga aspekter rörande honom eller henne, vilket enbart grundas på automatiserad behandling och medför rättsverkan för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne, såsom e-

rekrytering utan personlig kontakt. Sådan behandling omfattar ”profilering” i form av automatisk behandling av personuppgifter med bedömning av personliga aspekter rörande en fysisk person, särskilt för att analysera eller förutse aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar, i den mån dessa har rättsverkan rörande honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. Beslutsfattande grundat på sådan behandling, inbegripet profilering, bör dock tillåtas när det uttryckligen är tillåtet enligt unionsrätten. Denna form av uppgiftsbehandling bör under alla omständigheter omgärdas av lämpliga skyddsåtgärder, som bör inkludera specifik information till den registrerade och rätt till mänskligt ingripande, att framföra sina synpunkter, att erhålla en förklaring till det beslut som fattas efter sådan bedömning och att överklaga beslutet. Sådana åtgärder bör inte gälla barn. I syfte att sörja för rättvis och öppen behandling med avseende på den registrerade, med beaktande av omständigheterna och det sammanhang i vilket personuppgifterna behandlas, bör den personuppgiftsansvarige använda adekvata matematiska eller statistiska förfaranden för profilering, genomföra tekniska och organisatoriska åtgärder som framför allt säkerställer att faktorer som kan medföra felaktigheter i personuppgifter korrigeras och att risken för fel minimeras samt säkra personuppgifterna på sådant sätt att man beaktar potentiella risker för den registrerades intressen och rättigheter och förhindrar bland annat diskriminerande effekter för fysiska personer, på grund av ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse, medlemskap i fackföreningar, genetisk status eller hälsostatus eller sexuell läggning, eller som leder till åtgärder som får sådana effekter. Automatiserat beslutsfattande och profilering baserat på särskilda kategorier av personuppgifter bör endast tillåtas på särskilda villkor.

(37) Rättsakter som antagits på grundval av fördragen eller interna regler vid unionens institutioner och organ får föreskriva begränsningar med avseende på specifika principer och med avseende på rätt till information, tillgång till och rättelse eller radering av personuppgifter, rätt till dataportabilitet, konfidentiell behandling av uppgifter inom elektronisk kommunikation, underrättelse om en personuppgiftsincident till den registrerade och vissa därmed sammanhängande skyldigheter för personuppgiftsansvariga, i den utsträckning åtgärden är nödvändig och proportionerlig i ett demokratiskt samhälle för att upprätthålla den allmänna säkerheten, förebygga, utreda och lagföra brott eller verkställa straffrättsliga påföljder, inbegripet skydd mot samt förebyggande av hot mot den allmänna säkerheten, däribland skydd av människoliv, särskilt vid naturkatastrofer eller katastrofer orsakade av människan, den inre säkerheten för unionsinstitutioner och unionsorgan, andra viktiga mål av allmänt intresse för hela unionen eller en medlemsstat, i synnerhet ett viktigt ekonomiskt eller finansiellt intresse för unionen eller en medlemsstat, förande av offentliga register som förs av hänsyn till ett allmänt intresse eller skydd av den registrerade eller andras rättigheter och friheter, inklusive socialt skydd, folkhälsa och humanitära skäl.

Även om en begränsning inte föreskrivs i rättsakter som antagits på grundval av fördragen eller i interna regler vid unionens institutioner och organ, får unionsinstitutioner och unionsorgan i specifika fall införa en tillfällig begränsning avseende särskilda principer och den registrerades rättigheter om begränsningen sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och, med avseende på en specifik behandling, utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa ett eller flera av de ändamål som anges i punkt 1. Begränsningen bör anmälas till dataskyddsombudet. Alla begränsningar bör överensstämma med kraven i stadgan och den

europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

(38) Personuppgiftsansvariga bör åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar. Personuppgiftsansvariga bör särskilt vara skyldiga att vidta lämpliga och effektiva åtgärder och kunna visa att behandlingen är förenlig med denna förordning, även vad gäller åtgärdernas effektivitet. Man bör inom dessa åtgärder beakta behandlingens art, omfattning, sammanhang och ändamål samt risken för fysiska personers rättigheter och friheter. Risken för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av personuppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering, eller annan betydande ekonomisk eller social nackdel, om registrerade kan berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter, om personuppgifter behandlas som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i fackförening, om genetiska uppgifter, uppgifter om hälsa eller sexualliv eller fällande domar i brottmål samt lagöverträdelser eller därmed sammanhängande säkerhetsåtgärder behandlas, om personliga aspekter bedöms, framför allt analyser eller förutsägelser beträffande sådant som rör arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar, i syfte att skapa eller använda personliga profiler, om det sker behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade. Hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen inbegriper en risk eller en hög risk.

(39) Skyddet av fysiska personers rättigheter och friheter i samband med behandling av personuppgifter förutsätter att lämpliga tekniska och organisatoriska åtgärder vidtas, så att kraven i denna förordning uppfylls. För att kunna visa att denna förordning följs bör den personuppgiftsansvarige anta interna strategier och vidta åtgärder, särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard. Sådana åtgärder kan bland annat bestå av att uppgiftsbehandlingen minimeras, att personuppgifter snarast möjligt pseudonymiseras, att öppenhet om personuppgifternas syfte och behandling iakttas, att den registrerade får möjlighet att övervaka uppgiftsbehandlingen och att den personuppgiftsansvarige får möjlighet att skapa och förbättra säkerhetsanordningar. Principerna om inbyggt dataskydd och dataskydd som standard bör också beaktas vid offentliga upphandlingar.

(40) Skyddet av de registrerades rättigheter och friheter samt de personuppgiftsansvarigas och personuppgiftsbiträdenas ansvar kräver ett tydligt fastställande av vem som bär ansvaret enligt denna förordning, bl.a. när personuppgiftsansvariga gemensamt fastställer ändamål och medel för en behandling tillsammans med andra personuppgiftsansvariga eller när en behandling utförs på en personuppgiftsansvarigs vägnar.

(41) För att se till att kraven i denna förordning uppfylls vad gäller behandling som av ett personuppgiftsbiträde ska utföras på en personuppgiftsansvarigs vägnar ska den

personuppgiftsansvarige, när denne anförtror behandling åt ett personuppgiftsbiträde, endast använda personuppgiftsbiträden som ger tillräckliga garantier, i synnerhet i fråga om sakkunskap, tillförlitlighet och resurser, för att genomföra tekniska och organisatoriska åtgärder som uppfyller kraven i denna förordning, bl.a. vad gäller säkerhet i samband med behandlingen av uppgifter. Anslutning av andra personuppgiftsbiträden än unionsinstitutioner och unionsorgan till en godkänd uppförandekod eller en godkänd certifieringsmekanism kan användas som ett sätt att påvisa att den personuppgiftsansvarige fullgör sina skyldigheter. När uppgifter behandlas av ett personuppgiftsbiträde, bör hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt mellan personuppgiftsbiträdet och den personuppgiftsansvarige, där föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade anges, med beaktande av personuppgiftsbiträdets specifika arbets- och ansvarsuppgifter inom ramen för den behandling som ska utföras och risken med avseende på den registrerades rättigheter och friheter. Den personuppgiftsansvarige och personuppgiftsbiträdet bör kunna välja att använda sig av ett enskilt avtal eller standardavtalsklausuler som antingen antas direkt av kommissionen eller av Europeiska datatillsynsmannen och därefter av kommissionen. Efter det att behandlingen på den personuppgiftsansvariges vägnar har avslutats, bör personuppgiftsbiträdet återlämna eller radera personuppgifterna, beroende på vad den personuppgiftsansvarige väljer, såvida inte lagring av personuppgifterna krävs enligt den unionsrätt eller medlemsstaternas nationella rätt som personuppgiftsbiträdet omfattas av.

(42) För att visa att denna förordning följs bör personuppgiftsansvariga föra register över sådan uppgiftsbehandling som de ansvarar för och personuppgiftsbiträden bör föra register över kategorier av uppgiftsbehandling som de ansvarar för. Unionsinstitutioner och unionsorgan bör vara skyldiga att samarbeta med Europeiska datatillsynsmannen och på dennas begäran göra sina register tillgängliga, så att de kan tjäna som grund för övervakningen av behandlingen. Unionens institutioner och organ bör ha möjlighet att inrätta ett centralt register över sin uppgiftsbehandling. Av öppenhetsskäl bör de också kunna göra ett sådant register offentligt.

(43) För att upprätthålla säkerheten och förhindra behandling som bryter mot denna förordning bör personuppgiftsansvariga eller personuppgiftsbiträden utvärdera riskerna med behandlingen och vidta åtgärder, såsom kryptering, för att minska dem. Åtgärderna bör säkerställa en lämplig säkerhetsnivå, inbegripet konfidentialitet, med beaktande av den senaste utvecklingen och genomförandekostnader i förhållande till riskerna och vilken typ av personuppgifter som ska skyddas. Vid bedömningen av datasäkerhetsrisken bör man även beakta de risker som personuppgiftsbehandling medför, såsom förstöring, förlust eller ändringar genom olyckshändelse eller otillåtna handlingar eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, framför allt när denna kan medföra fysisk, materiell eller immateriell skada.

(44) Unionens institutioner och organ bör säkerställa konfidentiell behandling av uppgifter inom elektronisk kommunikation, i enlighet med artikel 7 i stadgan. I synnerhet bör unionens institutioner och organ säkerställa säkerheten i sina elektroniska kommunikationsnät, skydda information som rör terminalutrustning som slutanvändarna använder för att få tillgång till unionsinstitutionernas och unionsorganens allmänt tillgängliga webbplatser och mobila applikationer i enlighet

med förordning (EU) nr XX/XXXX [ny förordning om integritet och elektronisk kommunikation] samt skydda personuppgifter i kataloger över användare.

(45) Ett personuppgiftsincident kan, om den inte snabbt åtgärdas på lämpligt sätt, leda till fysisk, materiell eller immateriell skada för fysiska personer. Så snart en personuppgiftsansvarig blir medveten om att en personuppgiftsincident har inträffat, bör den personuppgiftsansvarige därför anmäla personuppgiftsincidenten till Europeiska datatillsynsmannen utan onödigt dröjsmål och, om så är möjligt, inom 72 timmar efter att ha blivit medveten om denna, om inte den personuppgiftsansvarige, i enlighet med principen om ansvarsskyldighet, kan påvisa att det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter. Om en sådan anmälan inte kan ske inom 72 timmar, bör den åtföljas av skälen till fördröjningen och information kan lämnas i omgångar utan otillbörligt vidare dröjsmål. Om en sådan fördröjning är motiverad, av mindre känslig natur eller mindre specifik bör information om incidenten lämnas så tidigt som möjligt, i stället för att man väntar med att lämna information till dess att den underliggande incidenten har avhjälpts fullt ut.

(46) Den personuppgiftsansvarige bör utan onödigt dröjsmål underrätta den registrerade om en personuppgiftsincident, om personuppgiftsincidenten sannolikt kommer att medföra en hög risk för den fysiska personens rättigheter och friheter, så att denne kan vidta nödvändiga försiktighetsåtgärder. Denna underrättelse bör beskriva personuppgiftsincidentens art samt innehålla rekommendationer för den berörda fysiska personen om hur de potentiella negativa effekterna kan mildras. De registrerade bör underrättas så snart detta rimligtvis är möjligt, i nära samarbete med Europeiska datatillsynsmannen och i enlighet med den vägledning som lämnats av den eller av andra relevanta myndigheter, exempelvis brottsbekämpande myndigheter.

(47) I förordning (EG) nr 45/2001 föreskrivs en allmän skyldighet för den personuppgiftsansvarige att anmäla behandling av personuppgifter till dataskyddsombudet, som i sin tur ska föra ett register över sådana behandlingar som har anmälts. Denna skyldighet medförde administrativa och ekonomiska bördor, men förbättrade inte alltid personuppgiftsskyddet. Sådana övergripande och allmänna anmälningsskyldigheter bör därför avskaffas och ersättas av effektiva förfaranden och mekanismer som i stället inriktas på de typer av behandlingar som sannolikt innebär en hög risk för fysiska personers rättigheter och friheter, i kraft av deras art, omfattning, sammanhang och ändamål. Dessa behandlingar kan vara sådana som särskilt inbegriper användning av ny teknik eller är av en ny typ, för vilken konsekvensbedömning avseende uppgiftsskydd inte tidigare har genomförts av den personuppgiftsansvarige, eller som blir nödvändiga på grund av den tid som har förflutit sedan den ursprungliga behandlingen. I sådana fall bör den personuppgiftsansvarige före behandlingen, med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt upphovet till risken, göra en konsekvensbedömning avseende dataskydd i syfte att bedöma den höga riskens specifika sannolikhetsgrad och allvar samt dess ursprung. Konsekvensbedömningen bör främst innefatta de planerade åtgärder, skyddsåtgärder och mekanismer som ska minska denna risk, säkerställa personuppgiftskyddet och visa att denna förordning efterlevs.

(48) Om det av en konsekvensbedömning avseende dataskydd framgår att behandlingen utan skyddsåtgärder, säkerhetsåtgärder och mekanismer för att minska risken kommer att innebära en hög risk för fysiska personers rättigheter och friheter, och den

personuppgiftsansvarige anser att risken inte kan begränsas genom åtgärder som är rimliga med avseende på tillgänglig teknik och genomförandekostnader, bör samråd hållas med Europeiska datatillsynsmannen innan behandlingen inleds. En sådan hög risk kommer sannolikt att orsakas av vissa typer av behandling samt av en viss omfattning och frekvens för behandlingen, vilket även kan leda till skador för eller kränkningar av fysiska personers rättigheter och friheter. Europeiska datatillsynsmannen bör inom en fastställd tid svara på en begäran om samråd. Ett uteblivet svar från Europeiska datatillsynsmannen inom denna tid bör dock inte hindra ett eventuellt ingripande från Europeiska datatillsynsmannens sida i enlighet med dess uppgifter och befogenheter enligt denna förordning, inbegripet befogenheten att förbjuda behandling. Som en del av denna samrådsprocess bör det vara möjligt att överlämna resultatet av en konsekvensbedömning avseende dataskydd som utförs med avseende på behandlingen i fråga till tillsynsmyndigheten, framför allt de åtgärder som planeras för att minska risken för fysiska personers rättigheter och friheter.

(49) Europeiska datatillsynsmannen bör informeras om administrativa åtgärder och interna bestämmelser vid unionens institutioner och organ som rör behandling av personuppgifter, föreskriver villkor för begränsningar av den registrerades rättigheter eller inför lämpligt skydd för den registrerades rättigheter, i syfte att se till att den avsedda behandlingen överensstämmer med denna förordning och framför allt för att minska risken för den registrerade.

(50) Genom förordning (EU) 2016/679 inrättades Europeiska dataskyddsstyrelsen som ett oberoende unionsorgan med ställning som juridisk person. Styrelsen bör bidra till en enhetlig tillämpning av förordning (EU) 2016/679 och direktiv 2016/680 i hela unionen, bl.a. genom att lämna råd till kommissionen. Samtidigt bör Europeiska datatillsynsmannen fortsätta att utöva sina övervakande och rådgivande funktioner med avseende på alla unionens institutioner och organ, även på eget initiativ eller på begäran. I syfte att säkerställa överensstämmelse mellan bestämmelserna om skydd av personuppgifter inom hela unionen, bör samråd med kommissionen vara obligatoriskt efter antagandet av lagstiftningsakter eller vid utarbetandet av delegerade akter och genomförandeakter som anges i artikel 289, 290 och 291 i EUF-fördraget och efter antagandet av rekommendationer och förslag som rör avtal med tredjeländer och internationella organisationer i enlighet med artikel 218 i EUF-fördraget vilka har en inverkan på rätten till skydd av personuppgifter. I sådana fall bör kommissionen vara skyldig att samråda med Europeiska datatillsynsmannen, utom i de fall då det i förordning (EU) 2016/679 föreskrivs obligatoriskt samråd med Europeiska dataskyddsstyrelsen, exempelvis vad gäller beslut om adekvat skyddsnivå eller delegerade akter om standardiserade symboler och krav för certifieringsmekanismer. Om akten i fråga är av särskild vikt för skyddet av enskilda personers fri- och rättigheter med avseende på behandlingen av personuppgifter, bör kommissionen dessutom ha möjlighet att samråda med Europeiska dataskyddsstyrelsen. I sådana fall bör Europeiska datatillsynsmannen, i egenskap av medlem i Europeiska dataskyddsstyrelsen, samordna sitt arbete med den senare i syfte att utfärda ett gemensamt yttrande. Europeiska datatillsynsmannen och, i tillämpliga fall, Europeiska dataskyddsstyrelsen, bör lämna sitt skriftliga råd inom åtta veckor. Denna tidsfrist bör förkortas i brådskande fall eller när det annars är lämpligt, t.ex. när kommissionen förbereder delegerade akter och genomförandeakter.

(51) Ett dataskyddsombud bör inom varje unionsinstitution eller unionsorgan övervaka tillämpningen av bestämmelserna i denna förordning och ge råd åt personuppgiftsansvariga och personuppgiftsbiträden då de fullgör sina åligganden.

Dataskyddsombudet bör vara en person med sakkunskap om lagstiftning och praxis på området för uppgiftsskydd, vilket bör bedömas med särskild hänsyn till den uppgiftsbehandling som utförs och det skydd som krävs för de personuppgifter som behandlas av den personuppgiftsansvarige eller personuppgiftsbiträdet. Denna typ av dataskyddsombud bör kunna fullgöra sitt uppdrag och utföra sina uppgifter på ett oberoende sätt.

(52) Det är viktigt att den skyddsnivå som fysiska personer säkerställs inom unionen genom denna förordning inte undergrävs när personuppgifter överförs från unionsinstitutioner och unionsorgan till personuppgiftsansvariga, personuppgiftsbiträden eller andra mottagare i tredjeland eller till internationella organisationer, vilket inbegriper vidarebefordran av personuppgifter från tredjelandet eller den internationella organisationen till personuppgiftsansvariga, personuppgiftsbiträden i samma eller ett annat tredjeland eller en annan internationell organisation. Överföringar till tredjeländer och internationella organisationer får under alla omständigheter endast utföras i full överensstämmelse med denna förordning. En överföring kan endast ske, om de villkor som fastställs i bestämmelserna i denna förordning om överföring av personuppgifter till tredjeländer eller internationella organisationer har uppfyllts av den personuppgiftsansvarige eller personuppgiftsbiträdet, med förbehåll för de övriga bestämmelserna i denna förordning.

(53) Kommissionen får, i enlighet med artikel 45 i förordning (EU) 2016/679, besluta att ett tredjeland, ett territorium eller en viss specificerad sektor i ett tredjeland, eller en internationell organisation, inte längre erbjuder en adekvat dataskyddsnivå. I dessa fall får överföringar av personuppgifter till det tredjelandet eller den internationella organisationen av en unionsinstitution eller ett unionsorgan ske utan ytterligare tillstånd.

(54) Saknas beslut om adekvat skyddsnivå bör den personuppgiftsansvarige eller personuppgiftsbiträdet vidta åtgärder för att kompensera för det bristande dataskyddet i ett tredjeland med hjälp av lämpliga skyddsåtgärder för den registrerade. Sådana lämpliga skyddsåtgärder kan bestå i tillämpning av standardbestämmelser om dataskydd som antagits av kommissionen, standardbestämmelser om dataskydd som antagits av Europeiska datatillsynsmannen eller avtalsbestämmelser som godkänts av Europeiska datatillsynsmannen. Om personuppgiftsbiträdet inte är en unionsinstitution eller ett unionsorgan kan dessa lämpliga skyddsåtgärder också bestå av bindande företagsregler, uppförandekoder och certifieringsmekanismer som används för internationella överföringar enligt förordning (EU) 2016/679. Dessa skyddsåtgärder bör säkerställa iakttagande av de krav i fråga om dataskydd och registrerades rättigheter som är lämpliga för behandling inom unionen, inbegripet huruvida bindande rättigheter för de registrerade och effektiva rättsmedel är tillgängliga, inbegripet en faktisk rätt att föra talan på administrativ väg eller inför domstol och att kräva kompensation i unionen eller i ett tredjeland. De bör särskilt gälla överensstämmelse med allmänna principer för behandling av personuppgifter samt principerna om inbyggt dataskydd och dataskydd som standard. Uppgifter kan också överföras av unionsinstitutioner och unionsorgan eller organ till offentliga myndigheter eller organ i tredjeländer eller internationella organisationer med motsvarande skyldigheter eller uppgifter, inbegripet på grundval av bestämmelser som ska införas i administrativa överenskommelser, t.ex. samförståndsavtal, som föreskriver verkställbara och faktiska rättigheter för de registrerade. Tillstånd från

Europeiska datatillsynsmannen bör erhållas när skyddsåtgärder föreskrivs i icke rättsligt bindande administrativa arrangemang.

(55) Personuppgiftsansvarigas eller personuppgiftsbiträdens möjlighet att använda standardiserade dataskyddsbestämmelser som antagits av kommissionen eller av Europeiska datatillsynsmannen bör inte hindra att de infogar standardiserade dataskyddsbestämmelser i ett vidare avtal, såsom ett avtal mellan personuppgiftsbiträdet och ett annat personuppgiftsbiträde, eller lägger till andra bestämmelser eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt står i strid med standardavtalsklausuler som antagits av kommissionen eller av Europeiska datatillsynsmannen eller påverkar de registrerades grundläggande rättigheter eller friheter. Personuppgiftsansvariga och personuppgiftsbiträden bör uppmuntras att tillhandahålla ytterligare skyddsåtgärder via avtalsmässiga åtaganden som kompletterar de standardiserade dataskyddsbestämmelserna.

(56) Vissa tredjeländer antar lagar och andra författningar som syftar till att direkt reglera behandling som utförs av unionens institutioner och organ. Detta kan inkludera rättsliga avgöranden eller beslut av administrativa myndigheter i tredjeländer där det krävs att personuppgiftsansvariga eller personuppgiftsbiträden överför eller överlämnar personuppgifter, utan grund i ett gällande internationellt avtal mellan det begärande tredjelandet och unionen. Extraterritoriell tillämpning av dessa lagar och andra författningar kan strida mot internationell rätt och inverka menligt på det skydd av fysiska personer som säkerställs inom unionen genom denna förordning. Överföringar bör endast tillåtas om villkoren i denna förordning för en överföring till tredjeländer är uppfyllda. Detta kan vara fallet bl.a. när utlämnande är nödvändigt på grund av ett viktigt allmänintresse som erkänns i unionsrätten.

(57) Det bör införas bestämmelser som i särskilda situationer ger möjlighet att under vissa omständigheter göra överföringar, om den registrerade har lämnat sitt uttryckliga samtycke, när överföringen är tillfällig och nödvändig med hänsyn till ett avtal eller ett rättsligt anspråk, oavsett om detta sker inom ett rättsligt förfarande eller i ett administrativt eller utomrättsligt förfarande, inbegripet förfaranden inför tillsynsorgan. Det bör också införas bestämmelser som ger möjlighet till överföringar om viktiga allmänintressen fastställda genom unionsrätten så kräver eller när överföringen görs från ett register som inrättats genom lag och är avsett att konsulteras av allmänheten eller av personer med ett berättigat intresse. I sistnämnda fall bör en sådan överföring inte omfatta alla personuppgifter eller hela kategorier av uppgifter i registret, om detta inte tillåts i unionslagstiftningen, och överföringen bör endast göras när registret är avsett att vara tillgängligt för personer med ett berättigat intresse, på begäran av dessa personer eller om de själva är mottagarna, med full hänsyn till de registrerades intressen och grundläggande rättigheter.

(58) Dessa undantag bör främst vara tillämpliga på uppgiftsöverföringar som krävs och är nödvändiga med hänsyn till viktiga allmänintressen, exempelvis vid internationella utbyten av uppgifter mellan konkurrensmyndigheter, skatte- eller tullmyndigheter, finanstillsynsmyndigheter, socialförsäkringsmyndigheter eller hälsovårdsmyndigheter, till exempel vid kontaktspårning för smittsamma sjukdomar eller för att minska och/eller undanröja dopning inom idrott. En överföring av personuppgifter bör också betraktas som laglig, om den är nödvändig för att skydda ett intresse som är väsentligt för den registrerades eller en annan persons vitala intressen, inklusive dennes fysiska integritet och liv, om den registrerade är oförmögen att ge sitt samtycke. Saknas beslut om adekvat skyddsnivå, får unionsrätten med hänsyn till viktiga allmänintressen

uttryckligen fastställa gränser för överföringen av specifika kategorier av uppgifter till ett tredjeland eller en internationell organisation. Varje överföring till en internationell humanitär organisation av personuppgifter rörande en registrerad som är fysiskt eller rättsligt förhindrad att ge sitt samtycke, i syfte att utföra en uppgift inom ramen för Genèvekonventionerna eller för att följa internationell humanitär rätt som är tillämplig vid väpnade konflikter, kan ses som nödvändig av skäl som rör ett betydande allmänintresse eller för att den är av grundläggande intresse för den registrerade.

(59) Om kommissionen inte har fattat beslut om adekvat dataskyddsnivå i ett tredjeland, bör den personuppgiftsansvarige eller personuppgiftsbiträdet i alla fall använda sig av lösningar som ger de registrerade verkställbara och effektiva rättigheter vad gäller behandlingen av deras personuppgifter inom unionen när dessa uppgifter väl har överförts, så att de fortsatt kan utöva sina grundläggande rättigheter och att skyddsåtgärder fortsatt gäller i förhållande till dem.

(60) När personuppgifter förs över gränser utanför unionen kan detta öka risken för att fysiska personer inte kan utöva sina dataskyddsrättigheter, i synnerhet för att skydda sig från otillåten användning eller otillåtet utlämnande av denna information. Samtidigt kan tillsynsmyndigheter i unionen, inklusive Europeiska datatillsynsmannen, vara ur stånd att handlägga klagomål eller göra utredningar som gäller verksamheter utanför gränserna för deras land. Deras strävan att arbeta tillsammans över gränserna kan också hindras av otillräckliga preventiva eller korrigerande befogenheter, oenhetliga rättsliga regelverk och praktiska hinder, som exempelvis bristande resurser. Därför bör ett närmare samarbete mellan Europeiska datatillsynsmannen och andra tillsynsmyndigheter för uppgiftsskydd främjas för att bidra till informationsutbytet med deras internationella motparter.

(61) Inrättandet av Europeiska datatillsynsmannen i förordning (EG) nr 45/2001, med behörighet att utföra sina uppgifter och utöva sina befogenheter under fullständigt oberoende, är ett väsentligt inslag i skyddet av fysiska personer vid behandlingen av personuppgifter. Denna förordning bör ytterligare stärka och klargöra dess roll och oberoende.

(62) För att säkerställa en enhetlig tillsyn över och ett enhetligt upprätthållande av denna förordning i hela unionen bör Europeiska datatillsynsmannen ha samma uppgifter och faktiska befogenheter som tillsynsmyndigheterna i medlemsstaterna, inbegripet undersökningsbefogenheter, korrigerande befogenheter och befogenheter att ålägga sanktioner samt befogenheter att utfärda tillstånd och ge råd, särskilt vid klagomål från fysiska personer, och att uppmärksamma Europeiska unionens domstol på överträdelser av denna förordning och delta i rättsliga förfaranden i enlighet med primärrätten. Dessa befogenheter bör även omfatta en befogenhet att införa en tillfällig eller definitiv begränsning av, inklusive förbud mot, behandling. För att undvika onödiga kostnader och alltför stora nackdelar för de berörda personer som kan komma att påverkas negativt, bör var och en av de åtgärder som Europeiska datatillsynsmannen vidtar vara lämplig, nödvändig och proportionerlig för att garantera efterlevnad av denna förordning och ta hänsyn till omständigheterna i varje enskilt fall samt respektera varje persons rätt att bli hörd innan någon enskild åtgärd vidtas. Varje rättsligt bindande åtgärd som vidtas av Europeiska datatillsynsmannen bör vara skriftlig, klar och entydig, innehålla uppgift om datum för utfärdandet, vara undertecknad av Europeiska datatillsynsmannen samt innehålla en motivering till åtgärden och en hänvisning till rätten till ett effektivt rättsmedel.

(63) Europeiska datatillsynsmannens beslut om undantag, skyddsåtgärder, tillstånd och villkor när det gäller behandling av uppgifter, såsom de fastställs i denna förordning, bör offentliggöras i verksamhetsrapporten. Förutom det årliga offentliggörandet av verksamhetsrapporten kan Europeiska datatillsynsmannen offentliggöra rapporter om särskilda ämnen.

(64) De nationella tillsynsmyndigheterna övervakar tillämpningen av förordning (EU) 2016/679 och bidrar till att den tillämpas enhetligt över hela unionen, för att skydda fysiska personer vid behandling av deras personuppgifter och för att underlätta det fria flödet av personuppgifter inom den inre marknaden. För att skapa större enhetlighet vid tillämpningen av regler om skydd av personuppgifter som är tillämpliga i medlemsstaterna och av regler om skydd av personuppgifter som är tillämpliga för unionsinstitutioner och unionsorgan bör Europeiska datatillsynsmannen samarbeta effektivt med de nationella tillsynsmyndigheterna.

(65) I vissa fall föreskriver unionsrätten en modell för samordnad tillsyn som delas mellan Europeiska datatillsynsmannen och de nationella tillsynsmyndigheterna. Dessutom är Europeiska datatillsynsmannen tillsynsmyndighet för Europol och en särskild modell för samarbete med de nationella tillsynsmyndigheterna inrättas genom en samarbetsnämnd med en rådgivande funktion. I syfte att förbättra tillsynen och upprätthållandet av materiella regler om uppgiftsskydd i praktiken bör en gemensam, enhetlig modell för samordnad tillsyn införas i unionen. Kommissionen bör därför, när så är lämpligt, lägga fram lagstiftningsförslag i syfte att ändra unionsrättsakter som föreskriver en modell för samordnad tillsyn, för att anpassa dessa till den samordnade tillsynsmodellen i denna förordning. Europeiska dataskyddsstyrelsen bör fungera som ett gemensamt forum för att säkerställa en effektiv samordnad tillsyn på ett övergripande plan.

(66) Alla registrerade bör ha rätt att lämna in ett klagomål till Europeiska datatillsynsmannen och ha rätt till ett effektivt rättsmedel inför Europeiska unionens domstol i enlighet med fördragen, om den registrerade anser att hans eller hennes rättigheter enligt denna förordning har kränkts eller om Europeiska datatillsynsmannen inte reagerar på ett klagomål, helt eller delvis avslår eller avvisar ett klagomål eller inte agerar när så är nödvändigt för att skydda den registrerades rättigheter. Utredningen av ett klagomål bör, med förbehåll för eventuell domstolsprövning, ske i den utsträckning som är lämplig i det enskilda fallet. Europeiska datatillsynsmannen bör i rimlig tid informera den registrerade om hur arbetet med klagomålet fortskrider och vad resultatet blir. Om ärendet fordrar ytterligare samordning med en nationell tillsynsmyndighet, bör den registrerade underrättas även om detta. För att förenkla inlämningen av klagomål bör Europeiska datatillsynsmannen vidta åtgärder, såsom att tillhandahålla ett formulär för inlämnande av klagomål som även kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.

(67) Varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av denna förordning bör ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan, med förbehåll för de villkor som föreskrivs i fördraget.

(68) För att stärka Europeiska datatillsynsmannens tillsynsroll och främja ett effektivt upprätthållande av denna förordning bör Europeiska datatillsynsmannen ha befogenhet att utfärda administrativa sanktionsavgifter, som en sanktion att använda i sista hand. Sanktionsavgifterna bör syfta till att bestraffa institutioner eller organ – snarare än

fysiska personer – för bristande efterlevnad av denna förordning, för att avskräcka från framtida överträdelser av denna förordning och för att främja en kultur av skydd för personuppgifter inom Europeiska unionens institutioner och organ. Denna förordning bör ange överträdelser och de övre gränserna och kriterierna för fastställande av administrativa sanktionsavgifter. Europeiska datatillsynsmannen bör fastställa avgiftsbeloppen i varje enskilt fall, med beaktande av alla relevanta omständigheter i det särskilda fallet, med vederbörlig hänsyn till överträdelsens karaktär, svårhetsgrad och varaktighet samt till dess följder och till de åtgärder som vidtas för att sörja för fullgörandet av skyldigheterna enligt denna förordning och för att förebygga eller lindra konsekvenserna av överträdelsen. Vid utfärdandet av en administrativ sanktionsavgift till ett unionsorgan bör Europeiska datatillsynsmannen bedöma huruvida sanktionsavgiftsbeloppet är proportionerligt. Det administrativa förfarandet för att besluta om sanktionsavgifter för unionsinstitutioner och unionsorgan bör följa de allmänna unionsrättsliga principerna, såsom dessa har tolkats av Europeiska unionens domstol.

(69) Om en registrerad anser att hans eller hennes rättigheter enligt denna förordning har kränkts, bör han eller hon ha rätt att ge mandat till ett organ, en organisation eller en sammanslutning som drivs utan vinstsyfte och som har inrättats i enlighet med unionsrätten eller en medlemsstats nationella rätt, som har stadgeenliga mål av allmänt intresse och bedriver verksamhet på området skydd av personuppgifter, att på hans eller hennes vägnar lämna in ett klagomål till Europeiska datatillsynsmannen. Detta organ, denna organisation eller denna sammanslutning bör också kunna utöva rätten till ett rättsmedel på registrerades vägnar eller utöva rätten att ta emot ersättning för registrerades räkning.

(70) Tjänstemän eller övriga anställda i unionen som underlåter att uppfylla de skyldigheter som anges i denna förordning bör bli föremål för disciplinära eller andra åtgärder, i enlighet med de regler och förfaranden som föreskrivs i tjänsteföreskrifterna för tjänstemän i Europeiska unionen eller anställningsvillkoren för övriga anställda i Europeiska unionen.

(71) För att säkerställa enhetliga villkor för tillämpningen av denna förordning bör kommissionen ges genomförandebefogenheter i enlighet med denna förordning. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011[16]. Granskningsförfarandet bör användas för att anta standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden och mellan personuppgiftsbiträden, för att anta förteckningen över sådan behandling om föregående samråd med Europeiska datatillsynsmannen är ett krav för personuppgiftsansvariga som behandlar uppgifter för att fullgöra en arbetsuppgift som utförs i allmänt intresse, och för att anta standardavtalsklausuler om lämpliga skyddsåtgärder vid internationella överföringar.

(72) De konfidentiella uppgifter som unionens myndigheter och nationella statistikansvariga myndigheter samlar in för att framställa officiell europeisk och officiell nationell statistik bör skyddas. Europeisk statistik bör utvecklas, framställas och spridas i enlighet med de statistiska principerna i artikel 338.2 i EUF-fördraget.

---

[16] Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

Europaparlamentets och rådets förordning (EG) nr 223/2009[17] innehåller ytterligare preciseringar om statistisk konfidentialitet för europeisk statistik.

(73) Förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG bör upphävas. Hänvisningar till den upphävda förordningen och det upphävda beslutet bör ses som hänvisningar till den här förordningen.

(74) För att garantera fullständigt oberoende för ledamöterna av den oberoende tillsynsmyndigheten, bör mandattiden för den nuvarande Europeiska datatillsynsmannen och biträdande datatillsynsmannen inte påverkas av denna förordning. Den nuvarande biträdande datatillsynsmannen bör förbli på sin post fram till slutet av sin ämbetstid, såvida inte något av villkoren för ett förtida avslutande av Europeiska datatillsynsmannens ämbetstid enligt denna förordning är uppfyllda. De relevanta bestämmelserna i denna förordning bör tillämpas på den biträdande datatillsynsmannen fram till slutet av hans eller hennes ämbetstid.

(75) I enlighet med proportionalitetsprincipen är det nödvändigt och lämpligt för uppnåendet av det grundläggande målet att säkerställa en likvärdig nivå för skyddet av fysiska personer och det fria flödet av personuppgifter över hela unionen att fastställa bestämmelser om behandling av personuppgifter hos unionens institutioner och organ. Denna förordning går inte utöver vad som är nödvändigt för att uppnå de eftersträvade målen i enlighet med artikel 5.4 i fördraget om Europeiska unionen.

(76) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 och avgav ett yttrande den XX/XX/XXXX.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1
Syfte och mål

1. I denna förordning fastställs regler om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ, kontor och byråer samt om det fria flödet av personuppgifter dem emellan eller till mottagare som är etablerade i unionen och omfattas av förordning (EU) 2016/679[18]

---

17 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(OJ L 87, 31.3.2009, p. 164).

18 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.

eller de bestämmelser i nationell rätt som antagits i enlighet med direktiv (EU) 2016/680[19].

2. Denna förordning skyddar fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.

3. Europeiska datatillsynsmannen ska övervaka att bestämmelserna i denna förordning tillämpas vid all behandling som utförs av en unionsinstitution eller ett unionsorgan.

Artikel 2
Tillämpningsområde

1. Denna förordning ska vara tillämplig på alla unionsinstitutioners och unionsorgans behandling av personuppgifter, om denna behandling genomförs för att utföra uppgifter som helt eller delvis omfattas av unionsrätten.

2. Denna förordning ska vara tillämplig på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av sådana personuppgifter som ingår i eller är avsedda att ingå i ett register.

Artikel 3
Definitioner

1. I denna förordning gäller följande definitioner:

   (a) de definitioner som fastställs i förordning (EU) 2016/679, med undantag av definitionen av *personuppgiftsansvarig* i artikel 4.7 i den förordningen.

   (b) definitionen av *elektronisk kommunikation* i artikel 4.2 a i förordning (EU) nr XX/XXXX [förordningen om integritet och elektronisk kommunikation].

   (c) definitionerna av *elektroniska kommunikationsnät* och *slutanvändare* i artikel 2.1 respektive 2.14 i direktiv 00/0000/EU [direktiv om inrättandet av en europeisk kodex för elektronisk kommunikation].

   (d) definitionen av *terminalutrustning* i artikel 1.1 i kommissionens direktiv 2008/63/EG[20].

2. I denna förordning gäller dessutom följande definitioner:

   (a) *unionens institutioner och organ*: unionens institutioner, organ, kontor och byråer som inrättats genom eller på grundval av fördraget om Europeiska unionen, fördraget om Europeiska unionens funktionssätt eller Euratomfördraget.

---

[19] 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.

[20] Kommissionens direktiv 2008/63/EG av den 20 juni 2008 om konkurrens på marknaderna för teleterminalutrustning (EUT L 162, 21.6.2008, s. 20).

(b) *personuppgiftsansvarig*: den unionsinstitution, det unionsorgan, det unionskontor, den unionsbyrå eller det generaldirektorat eller varje annan organisatorisk enhet som ensam(t) eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter; om ändamålen med och medlen för behandlingen fastställs i en särskild unionsakt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten.

(c) *användare*: en fysisk person som använder ett nät eller en terminalutrustning som drivs under överinseende av en unionsinstitution eller ett unionsorgan.

(d) *katalog*: en allmänt tillgänglig abonnentförteckning eller en intern förteckning över användare som är tillgänglig inom en unionsinstitution eller ett unionsorgan eller delas mellan unionsinstitutioner och unionsorgan, oavsett om den föreligger på papper eller i elektronisk form.

KAPITEL II

PRINCIPER

Artikel 4
Principer för behandling av personuppgifter

1. Vid behandling av personuppgifter ska följande gälla:

a) Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (laglighet, korrekthet och öppenhet).

b) De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 13 ska inte anses vara oförenlig med de ursprungliga ändamålen (ändamålsbegränsning).

c) De ska vara adekvata, relevanta och begränsade till vad som är nödvändigt i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering).

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

e) De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 13, under förutsättning att de lämpliga tekniska

och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (lagringsminimering).

f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet).

2. Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs (ansvarsskyldighet).

Artikel 5
Laglig behandling av personuppgifter

1. Behandling ska vara laglig endast om och i den mån som åtminstone ett av följande villkor är uppfyllt:

a) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse på grundval av eller som ett led i unionsinstitutionens eller unionsorganets myndighetsutövning.

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

c) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

d) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.

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

2. De uppgifter som avses i punkt 1 a ska vara fastställda i unionsrätt.

Artikel 6
Behandling för ett annat förenligt ändamål

Om en behandling för ett annat ändamål än det för vilket personuppgifterna samlades in inte grundar sig på den registrerades samtycke eller på unionsrätten, men utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda de mål som avses i artikel 23.1, ska den personuppgiftsansvarige för att fastställa huruvida behandling för annat ändamål är förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in beakta bland annat följande:

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

b) Det sammanhang i vilket personuppgifterna har samlats in, särskilt förhållandet mellan de registrerade och den personuppgiftsansvarige.

c) Personuppgifternas art, särskilt huruvida särskilda kategorier av personuppgifter behandlas, i enlighet med artikel 10, eller huruvida personuppgifter som rör fällande domar i brottmål och lagöverträdelser behandlas, i enlighet med artikel 11.

d) Eventuella konsekvenser för registrerade av den planerade ytterligare behandlingen.

e) Förekomsten av lämpliga skyddsåtgärder, vilket kan inbegripa kryptering eller pseudonymisering.

Artikel 7
Villkor för samtycke

1. Om behandlingen grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter.

2. Om den registrerades samtycke lämnas i samband med en skriftlig förklaring som också rör andra frågor, ska begäran om samtycke läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Om en del av förklaringen innebär en överträdelse av denna förordning, ska denna del inte vara bindande.

3. Den registrerade ska ha rätt att när som helst återkalla sitt samtycke. Återkallandet av samtycket ska inte påverka lagligheten av behandling som grundar sig på samtycket innan detta återkallades. Innan samtycke lämnas ska den registrerade informeras om detta. Det ska vara lika lätt att återkalla som att ge sitt samtycke.

4. Vid bedömning av huruvida samtycke är frivilligt ska största hänsyn tas till bland annat huruvida genomförandet av ett avtal, inbegripet tillhandahållandet av en tjänst, har gjorts beroende av samtycke till sådan behandling av personuppgifter som inte är nödvändig för genomförandet av det avtalet.

Artikel 8
Villkor som gäller barns samtycke avseende informationssamhällets tjänster

1. Vid erbjudande av informationssamhällets tjänster direkt till ett barn ska, om artikel 5.1 d är tillämplig, behandling av personuppgifter som rör ett barn vara laglig om barnet är minst 13 år. Om barnet är under 13 år ska sådan behandling vara laglig endast om och i den mån samtycke ges eller godkänns av den person som har föräldraansvar för barnet.

2. Den personuppgiftsansvarige ska göra rimliga ansträngningar för att i sådana fall kontrollera att samtycke ges eller godkänns av den person som har föräldraansvar för barnet, med hänsyn tagen till tillgänglig teknik.

3. Punkt 1 ska inte påverka tillämpningen av allmän avtalsrätt i medlemsstaterna, såsom bestämmelser om giltigheten, upprättandet eller verkan av ett avtal som gäller ett barn.

Artikel 9

Överföring av personuppgifter till andra mottagare än unionens institutioner och organ vilka är etablerade i unionen och omfattas av förordning (EU) 2016/679 eller direktiv (EU) 2016/680

1. Utan att det påverkar tillämpningen av artiklarna 4, 5, 6 och 10 ska personuppgifter endast överföras till mottagare som är etablerade i unionen och som omfattas av förordning (EU) 2016/679 eller den nationella lagstiftning som har antagits i enlighet med direktiv (EU) 2016/680, om mottagaren visar

   a) att uppgifterna är nödvändiga för att utföra ett uppdrag som är av allmänt intresse eller är förenat med myndighetsutövning, eller

   b) att det är nödvändigt att uppgifterna överförs, det råder proportionalitet i förhållande till syftet med överföringen och det saknas skäl att anta att den registrerades legitima intressen skulle kunna skadas.

2. Om överföringen enligt denna artikel äger rum på den personuppgiftsansvariges initiativ, ska den personuppgiftsansvarige visa att överföringen av personuppgifterna är nödvändig och proportionell i förhållande till syftet med överföringen, med tillämpning av de kriterier som anges punkt 1 a eller b.

Artikel 10

Behandling av särskilda kategorier av personuppgifter

1. Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden.

2. Punkt 1 ska inte tillämpas om något av följande gäller:

   a) Den registrerade har uttryckligen lämnat sitt samtycke till behandlingen av dessa uppgifter för ett eller flera specifika ändamål, utom då unionsrätten föreskriver att förbudet i punkt 1 inte får upphävas av den registrerade.

   b) Behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och lagstiftning om social trygghet och socialt skydd, i den omfattning detta är tillåtet enligt unionsrätt där lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställs.

   c) Behandlingen är nödvändig för att skydda den registrerades eller någon annan persons grundläggande intressen om den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.

   d) Behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder hos ett icke vinstdrivande organ som utgör en enhet som är integrerad i en unionsinstitution eller ett unionsorgan och som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att behandlingen endast rör

sådana organs medlemmar eller tidigare medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta och uppgifterna inte lämnas ut utanför det organet utan den registrerades samtycke.

e) Behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

f) Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av Europeiska unionens domstols dömande verksamhet.

g) Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätt som ska stå i proportion till det eftersträvade syftet, vara förenlig med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

h) Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård eller yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system, på grundval av unionsrätten eller enligt avtal med yrkesverksamma på hälsoområdet och under förutsättning att de villkor och skyddsåtgärder som avses i punkt 3 är uppfyllda.

i) Behandlingen är nödvändig av hänsyn till ett allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter, på grundval av unionsrätt som föreskriver lämpliga och specifika åtgärder för att skydda den registrerades rättigheter och friheter, särskilt tystnadsplikt.

j) Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål, på grundval av unionsrätt som ska stå i proportion till det eftersträvade syftet, vara förenlig med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och specifika åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

3. Personuppgifter som avses i punkt 1 får behandlas för de ändamål som avses i punkt 2 h, om uppgifterna behandlas av eller under ansvar av en yrkesutövare som omfattas av tystnadsplikt enligt unionsrätten.

Artikel 11

Behandling av personuppgifter som rör fällande domar i brottmål samt lagöverträdelser

Behandling av personuppgifter som rör fällande domar i brottmål och lagöverträdelser eller därmed sammanhängande säkerhetsåtgärder enligt artikel 5.1 får endast utföras om behandlingen är tillåten enligt unionsrätten, vilket kan inbegripa interna regler, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs.

Artikel 12
Behandling som inte kräver identifiering

1. Om de ändamål för vilka den personuppgiftsansvarige behandlar personuppgifter inte kräver eller inte längre kräver att den registrerade identifieras av den personuppgiftsansvarige, ska den personuppgiftsansvarige inte vara skyldig att bevara, förvärva eller behandla ytterligare information för att identifiera den registrerade endast i syfte att följa denna förordning.

2. Om den personuppgiftsansvarige, i de fall som avses i punkt 1 i denna artikel, kan visa att denne inte är i stånd att identifiera den registrerade, ska den personuppgiftsansvarige om möjligt informera den registrerade om detta. I sådana fall ska artiklarna 17–22 inte gälla, förutom om den registrerade i syfte att utöva sina rättigheter i enlighet med dessa artiklar tillhandahåller ytterligare information som gör dess identifiering möjlig.

Artikel 13
Skyddsåtgärder vid behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål

Behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ska omfattas av lämpliga skyddsåtgärder i enlighet med denna förordning för den registrerades rättigheter och friheter. Skyddsåtgärderna ska säkerställa att tekniska och organisatoriska åtgärder har införts för att särskilt se till att principen om uppgiftsminimering iakttas. Dessa åtgärder får inbegripa pseudonymisering, under förutsättning att dessa ändamål kan uppfyllas på det sättet. När dessa ändamål kan uppfyllas genom ytterligare behandling av uppgifter som inte medger eller inte längre medger identifiering av de registrerade ska dessa ändamål uppfyllas på det sättet.

KAPITEL III

DEN REGISTRERADES RÄTTIGHETER

AVSNITT 1

ÖPPENHET OCH VILLKOR

Artikel 14
Öppen information och kommunikation samt villkor för utövandet av den registrerades rättigheter

1. Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att till den registrerade tillhandahålla all information som avses i artiklarna 15 och 16 och all kommunikation enligt artiklarna 17–24 och 38 vilken avser behandling i en koncis, öppen, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet information som är särskilt riktad till barn. Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i

elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt.

2. Den personuppgiftsansvarige ska underlätta utövandet av den registrerades rättigheter i enlighet med artiklarna 17–24 I de fall som avses i artikel 12.2 får den personuppgiftsansvarige inte vägra att tillmötesgå den registrerades begäran om att utöva sina rättigheter i enlighet med artiklarna 17–24, om inte den personuppgiftsansvarige visar att den inte är i stånd att identifiera den registrerade.

3. Den personuppgiftsansvarige ska utan onödigt dröjsmål och under alla omständigheter inom en månad från mottagandet av en begäran enligt artiklarna 17–24 tillhandahålla den registrerade information om de åtgärder som vidtagits till följd av begäran. Denna period får vid behov förlängas med ytterligare två månader, med beaktande av hur komplicerad begäran är och antalet inkomna begäranden. Den personuppgiftsansvarige ska underrätta den registrerade om en sådan förlängning inom en månad från mottagandet av begäran och ange orsakerna till förseningen. Om den registrerade lämnar begäran i elektronisk form, ska informationen om möjligt tillhandahållas i elektronisk form, om den registrerade inte begär något annat.

4. Om den personuppgiftsansvarige inte vidtar åtgärder till följd av den registrerades begäran, ska den personuppgiftsansvarige utan dröjsmål och senast inom en månad från mottagandet av begäran informera den registrerade om orsaken till att åtgärder inte vidtagits och om möjligheten att lämna in ett klagomål till Europeiska datatillsynsmannen och begära rättslig prövning.

5. Information som tillhandahållits enligt artiklarna 15 och 16, all kommunikation och samtliga åtgärder som vidtas enligt artiklarna 17–24 och 38 ska tillhandahållas kostnadsfritt. Om begäranden från en registrerad är uppenbart ogrundade eller orimliga, särskilt på grund av deras repetitiva art, får den personuppgiftsansvarige vägra att tillmötesgå begäran.

Det ska åligga den personuppgiftsansvarige att visa att begäran är uppenbart ogrundad eller orimlig.

6. Utan att det påverkar tillämpningen av artikel 12 får den personuppgiftsansvarige, om denne har rimliga skäl att betvivla identiteten hos den fysiska person som gör en begäran enligt artiklarna 17–23, begära att ytterligare information som är nödvändig för att bekräfta den registrerades identitet tillhandahålls.

7. Den information som ska tillhandahållas de registrerade i enlighet med artiklarna 15 och 16 får tillhandahållas tillsammans med standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över den planerade behandlingen. Om sådana symboler visas elektroniskt ska de vara maskinläsbara.

8. Om kommissionen antar delegerade akter i enlighet med artikel 12.8 i förordning (EU) 2016/679 för att fastställa vilken information som ska visas med hjälp av symboler och förfarandena för att tillhandahålla sådana symboler, ska unionens institutioner och organ, i tillämpliga fall, lämna de uppgifter som avses i artiklarna 15 och 16, tillsammans med sådana standardiserade symboler.

AVSNITT 2

INFORMATION OCH TILLGÅNG TILL PERSONUPPGIFTER

Artikel 15
Information som ska tillhandahållas om personuppgifter samlas in från den registrerade

1. Om personuppgifter som rör en registrerad person samlas in från den registrerade, ska den personuppgiftsansvarige, vid den tidpunkt då personuppgifterna erhålls, lämna följande information till den registrerade:

   a) Den personuppgiftsansvariges identitet och kontaktuppgifter.

   b) Dataskyddsombudets kontaktuppgifter.

   c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.

   d) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.

   e) I tillämpliga fall uppgift om att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artikel 49, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

2. Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige vid insamlingen av personuppgifterna lämna den registrerade följande ytterligare information, vilken krävs för att säkerställa rättvis och öppen behandling:

   a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

   b) Att det föreligger en rätt att hos den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller, i tillämpliga fall, rätt att invända mot behandling eller rätt till dataportabilitet.

   c) Om behandlingen grundar sig på artikel 5.1 d eller artikel 10.2 a, att det föreligger en rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket innan detta återkallades.

   d) Rätt att lämna in ett klagomål till Europeiska datatillsynsmannen.

   e) Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav eller ett krav som är nödvändigt för att ingå ett avtal samt

huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att sådana uppgifter inte lämnas.

f) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 24.1 och 24.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

3. Om den personuppgiftsansvarige avser att ytterligare behandla personuppgifterna för ett annat syfte än det för vilket de insamlades, ska den personuppgiftsansvarige före denna ytterligare behandling ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt punkt 2.

4. Punkterna 1, 2 och 3 ska inte tillämpas om och i den mån den registrerade redan förfogar över informationen.

Artikel 16
Information som ska tillhandahållas om personuppgifter inte har erhållits från den registrerade

1. Om personuppgifterna inte har erhållits från den registrerade, ska den personuppgiftsansvarige lämna följande information till den registrerade:

a) Den personuppgiftsansvariges identitet och kontaktuppgifter.

b) Dataskyddsombudets kontaktuppgifter.

c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.

d) De kategorier av personuppgifter som behandlingen gäller.

e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.

f) I tillämpliga fall uppgift om att den personuppgiftsansvarige avser att överföra personuppgifter till en mottagare i ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artikel 49, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

2. Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige lämna den registrerade följande ytterligare information, vilken krävs för att säkerställa rättvis och öppen behandling när det gäller den registrerade:

a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

b) Att det föreligger en rätt att hos den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller, i tillämpliga fall, rätt att invända mot behandling eller rätt till dataportabilitet.

c) Om behandlingen grundar sig på artikel 5.1 d eller artikel 10.2 a, att det föreligger en rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket innan detta återkallades.

d) Rätt att lämna in ett klagomål till Europeiska datatillsynsmannen.

e) Varifrån personuppgifterna kommer och i förekommande fall huruvida de har sitt ursprung i allmänt tillgängliga källor.

f) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 24.1 och 24.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

3. Den personuppgiftsansvarige ska lämna den information som anges i punkterna 1 och 2

(a) inom en rimlig period efter det att personuppgifterna har erhållits, dock senast inom en månad, med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas,

(b) om personuppgifterna ska användas för kommunikation med den registrerade, senast vid tidpunkten för den första kommunikationen med den registrerade, eller

(c) om ett utlämnande till en annan mottagare förutses, senast när personuppgifterna lämnas ut för första gången.

4. Om den personuppgiftsansvarige avser att ytterligare behandla personuppgifterna för ett annat syfte än det för vilket de insamlades, ska den personuppgiftsansvarige före denna ytterligare behandling ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt punkt 2.

5. Punkterna 1–4 ska inte tillämpas i följande fall och i den mån

a) den registrerade redan förfogar över informationen,

b) tillhandahållandet av sådan information visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning, särskilt för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål, eller i den mån den skyldighet som avses i punkt 1 i denna artikel sannolikt kommer att göra det omöjligt eller avsevärt försvårar uppfyllandet av målen med den behandlingen,

c) erhållande eller utlämnande av uppgifter uttryckligen föreskrivs genom unionsrätten, eller

d) personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätten.

Artikel 17
Den registrerades rätt till tillgång

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna och följande information:

   a) Ändamålen med behandlingen.

   b) De kategorier av personuppgifter som behandlingen gäller.

   c) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer.

   d) Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

   e) Förekomsten av rätten att hos den personuppgiftsansvarige begära rättelse eller radering av personuppgifterna eller begränsningar av behandling av personuppgifter som rör den registrerade eller att invända mot sådan behandling.

   f) Rätt att lämna in ett klagomål till Europeiska datatillsynsmannen.

   g) Om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån dessa uppgifter kommer.

   h) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 24.1 och 24.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

2. Om personuppgifter överförs till ett tredjeland eller till en internationell organisation, ska den registrerade ha rätt till information om de lämpliga skyddsåtgärder som i enlighet med artikel 49 har vidtagits vid överföringen.

3. Den personuppgiftsansvarige ska förse den registrerade med en kopia av de personuppgifter som är under behandling. Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat.

4. Den rätt till en kopia som avses i punkt 3 ska inte inverka menligt på andras rättigheter och friheter.

AVSNITT 3

RÄTTELSE OCH RADERING

Artikel 18
Rätt till rättelse

Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få felaktiga personuppgifter som rör honom eller henne rättade. Med beaktande av ändamålen med behandlingen, ska den registrerade ha rätt att komplettera ofullständiga personuppgifter, bland annat genom att tillhandahålla ett kompletterande utlåtande.

Artikel 19
Rätt till radering (”rätten att bli glömd”)

1. Den registrerade ska ha rätt att hos den personuppgiftsansvarige utan onödigt dröjsmål få sina personuppgifter raderade och den personuppgiftsansvarige ska vara skyldig att utan onödigt dröjsmål radera personuppgifter om någon av följande grunder föreligger:

   a) Personuppgifterna är inte längre nödvändiga för de ändamål för vilka de samlades in eller på annat sätt behandlades.

   b) Den registrerade återkallar det samtycke på vilket behandlingen grundar sig enligt artikel 5.1 d eller artikel 10.2 a och det finns inte någon annan rättslig grund för behandlingen.

   c) Den registrerade invänder mot behandlingen i enlighet med artikel 23.1 och det saknas berättigade skäl för behandlingen som väger tyngre.

   d) Personuppgifterna har behandlats på olagligt sätt.

   e) Personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse som den personuppgiftsansvarige omfattas av.

   f) Personuppgifterna har samlats in i samband med erbjudande av informationssamhällets tjänster, som avses i artikel 8.1.

2. Om den personuppgiftsansvarige har offentliggjort personuppgifterna och enligt punkt 1 är skyldig att radera personuppgifterna, ska den personuppgiftsansvarige med beaktande av tillgänglig teknik och kostnaden för genomförandet vidta rimliga åtgärder, inbegripet tekniska åtgärder, för att underrätta personuppgiftsansvariga som behandlar personuppgifterna om att den registrerade har begärt att de ska radera eventuella länkar till, eller kopior eller reproduktioner av, dessa personuppgifter.

3. Punkterna 1 och 2 ska inte gälla i den utsträckning som behandlingen är nödvändig av följande skäl:

   a) För att utöva rätten till yttrande- och informationsfrihet.

b) För att uppfylla en rättslig förpliktelse som den personuppgiftsansvarige omfattas av eller för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige.

c) Av skäl som rör ett viktigt allmänt intresse på folkhälsoområdet enligt artikel 10.2 h och i samt artikel 10.3.

d) För arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål, i den utsträckning som den rätt som avses i punkt 1 sannolikt omöjliggör eller avsevärt försvårar uppnåendet av syftet med den behandlingen.

e) För att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

Artikel 20
Rätt till begränsning av behandling

1. Den registrerade ska ha rätt att hos den personuppgiftsansvarige kräva att behandlingen begränsas om något av följande är tillämpligt:

a) Den registrerade bestrider personuppgifternas korrekthet, för en tidsperiod som ger den personuppgiftsansvarige möjlighet att kontrollera om personuppgifterna är korrekta och fullständiga.

b) Behandlingen är olaglig och den registrerade motsätter sig att de raderas och i stället begär en begränsning av deras användning.

c) Den personuppgiftsansvarige behöver inte längre personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

d) Den registrerade har invänt mot behandling i enlighet med artikel 23.1 i avvaktan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.

2. Om behandlingen har begränsats i enlighet med punkt 1 får sådana personuppgifter, med undantag för lagring, endast behandlas med den registrerades samtycke eller för att fastställa, göra gällande eller försvara rättsliga anspråk eller för att skydda någon annan fysisk eller juridisk persons rättigheter eller av skäl som rör ett viktigt allmänintresse för unionen eller för en medlemsstat.

3. En registrerad som har fått behandling begränsad i enlighet med punkt 1 ska underrättas av den personuppgiftsansvarige innan begränsningen av behandlingen upphör.

4. I automatiserade register ska begränsningar av behandlingen i princip säkerställas med tekniska medel. Det förhållandet att personuppgifter omfattas av begränsningar ska anges i systemet på ett sådant sätt att det är tydligt att personuppgifterna inte får användas.

Artikel 21
Anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling

Den personuppgiftsansvarige ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om varje rättelse eller radering av personuppgifter eller begränsning av behandling som utförts i enlighet med artiklarna 18, 19.1 och 20, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Artikel 22
Rätt till dataportabilitet

1. Den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits personuppgifterna hindrar detta, om

   a) behandlingen grundar sig på samtycke enligt artikel 5.1 d eller artikel 10.2 a eller på ett avtal enligt artikel 5.1 c, och

   b) behandlingen sker automatiserat.

2. Vid utövandet av sin rätt till dataportabilitet i enlighet med punkt 1 ska den registrerade ha rätt till överföring av personuppgifterna direkt från en personuppgiftsansvarig till en annan, när detta är tekniskt möjligt.

3. Utövandet av den rätt som avses i punkt 1 i denna artikel ska inte påverka tillämpningen av artikel 19. Den rätten ska inte gälla i fråga om en behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige.

4. Den rätt som avses i punkt 1 får inte inverka menligt på andras rättigheter och friheter.

AVSNITT 4

RÄTT ATT GÖRA INVÄNDNINGAR OCH AUTOMATISERAT INDIVIDUELLT BESLUTSFATTANDE

Artikel 23
Rätt att göra invändningar

1. Den registrerade ska, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på artikel 5.1 a, inbegripet profilering som grundar sig på den bestämmelsen. Den personuppgiftsansvarige får inte längre behandla personuppgifterna såvida denne inte kan påvisa tvingande berättigade skäl

för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.

2. Senast vid den första kommunikationen med den registrerade ska den rätt som avses i punkt 1 uttryckligen meddelas den registrerade och redovisas klart och åtskilt från eventuell annan information.

3. I samband med användningen av informationssamhällets tjänster får den registrerade, utan att det påverkar tillämpningen av artiklarna 34 och 35, utöva sin rätt att göra invändningar genom automatiserad användning av tekniska specifikationer.

4. Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ska den registrerade, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att göra invändningar mot behandling av personuppgifter avseende honom eller henne om inte behandlingen är nödvändig för att utföra en uppgift av allmänt intresse.

Artikel 24
Automatiserat individuellt beslutsfattande, inbegripet profilering

1. Den registrerade ska ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne.

2. Punkt 1 ska inte tillämpas om beslutet

   a) är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige,

   b) tillåts enligt unionsrätten, som även fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen, eller

   c) grundar sig på den registrerades uttryckliga samtycke.

3. I fall som avses i punkt 2 a och c ska den personuppgiftsansvarige genomföra lämpliga åtgärder för att säkerställa den registrerades rättigheter, friheter och rättsliga intressen, åtminstone rätten till personlig kontakt med den personuppgiftsansvarige för att kunna utrycka sin åsikt och bestrida beslutet.

4. Beslut som avses i punkt 2 får inte grunda sig på de särskilda kategorier av personuppgifter som avses i artikel 10.1, såvida inte artikel 10.2 a eller g är tillämplig och lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen har inrättats.

AVSNITT 5

BEGRÄNSNINGAR

Artikel 25
Begränsningar

1. Rättsakter som antas på grundval av fördragen eller, när det gäller frågor rörande unionens institutioners och organs funktion, interna regler som införts av de sistnämnda får föreskriva begränsningar i tillämpningen av artiklarna 14–22, 34 och 38, samt artikel 4 i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 14–22, om en sådan begränsning sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa

   (a) den nationella säkerheten, den allmänna säkerheten eller försvaret i medlemsstaterna,

   (b) förebyggande, förhindrande, utredning, avslöjande och lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten,

   (c) andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet,

   (d) den inre säkerheten i unionens institutioner och organ, inbegripet deras elektroniska kommunikationsnät,

   (e) skydd av rättsväsendets oberoende och rättsliga åtgärder,

   (f) förebyggande, förhindrande, utredning, avslöjande och lagföring av överträdelser av etiska regler som gäller för lagreglerade yrken,

   (g) en tillsyns-, inspektions- eller regleringsfunktion som, även i enstaka fall, har samband med myndighetsutövning i fall som avses i a–c,

   (h) skydd av den registrerade eller andras rättigheter och friheter,

   (i) verkställighet av civilrättsliga krav.

2. Om en begränsning som inte föreskrivs i en rättsakt som antagits på grundval av fördragen eller genom en intern regel i enlighet med punkt 1, får unionens institutioner och organ begränsa tillämpningen av artiklarna 14–22, 34 och 38, samt artikel 4 i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 14–22, om en sådan begränsning sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna, i samband med en specifik behandling, och utgör en nödvändig och proportionell åtgärd i ett

demokratiskt samhälle för att skydda ett eller flera av de syften som avses i punkt 1. Begränsningen ska anmälas till det behöriga dataskyddsombudet.

3. Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål får det i unionsrätten, vilket kan inkludera interna regler, föreskrivas undantag från de rättigheter som avses i artiklarna 17, 18, 20 och 23 med förbehåll för de villkor och skyddsåtgärder som avses i artikel 13 i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller avsevärt svårare att uppfylla de särskilda ändamålen, och sådana undantag krävs för att uppnå dessa ändamål.

4. Om personuppgifter behandlas för arkivändamål av allmänt intresse får det i unionsrätten, vilket kan inkludera interna regler, föreskrivas undantag från de rättigheter som avses i artiklarna 17, 18, 20, 21, 22 och 23 med förbehåll för de villkor och skyddsåtgärder som avses i artikel 13 i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller avsevärt svårare att uppfylla de särskilda ändamålen, och sådana undantag krävs för att uppnå dessa ändamål.

5. Sådana interna regler som avses i punkterna 1, 3 och 4 ska vara tillräckligt klara och precisa och offentliggöras på lämpligt sätt.

6. Om en begränsning införs i enlighet med punkt 1 eller 2, ska den registrerade i enlighet med unionsrätten informeras om de huvudsakliga skälen till begränsningen och om att han eller hon har rätt att ge in ett klagomål till Europeiska datatillsynsmannen.

7. Om en begränsning som införts i enlighet med punkt 1 eller 2 åberopas för att vägra den registrerade tillgång, ska Europeiska datatillsynsmannen vid utredning av klagomålet endast informera honom eller henne om huruvida uppgifterna har behandlats korrekt och, om så inte är fallet, huruvida alla nödvändiga korrigeringar har gjorts.

8. Tillhandahållande av den information som avses i punkterna 6 och 7 samt i artikel 46.2 får skjutas upp, utelämnas eller nekas om det skulle upphäva verkan av en begränsning som införts i enlighet med punkt 1 eller 2.

KAPITEL IV

PERSONUPPGIFTSANSVARIG OCH PERSONUPPGIFTSBITRÄDE

AVSNITT 1

ALLMÄNNA SKYLDIGHETER

Artikel 26
Den personuppgiftsansvariges ansvar

1. Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.

2. Om det står i proportion till behandlingen, ska de åtgärder som avses i punkt 1 omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.

Artikel 27
Inbyggt dataskydd och dataskydd som standard

1. Med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder, såsom pseudonymisering, vilka är utformade för ett effektivt genomförande av dataskyddsprinciper, såsom uppgiftsminimering, och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i denna förordning uppfylls och den registrerades rättigheter skyddas.

2. Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att som standard säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, den tid de lagras och deras tillgänglighet. Särskilt ska dessa åtgärder säkerställa att personuppgifter som standard inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

Artikel 28
Gemensamt personuppgiftsansvariga

1. Om en unionsinstitution eller ett unionsorgan tillsammans med en eller flera personuppgiftsansvariga, som kan vara unionsinstitutioner eller unionsorgan eller inte, gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. Gemensamt personuppgiftsansvariga ska under öppna former fastställa sitt respektive ansvar för att fullgöra sina skyldigheter i fråga om dataskydd, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artiklarna 15 och 16, genom ett inbördes arrangemang, såvida inte de personuppgiftsansvarigas respektive skyldigheter fastställs genom unionsrätten eller en medlemsstats nationella rätt som de personuppgiftsansvariga omfattas av. Inom ramen för arrangemanget får en gemensam kontaktpunkt för de personuppgiftsansvariga utses.

2. Det arrangemang som avses i punkt 1 ska på lämpligt sätt återspegla de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade. Det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade.

3. Den registrerade får utöva sina rättigheter enligt denna förordning med avseende på och gentemot en eller flera av de gemensamt personuppgiftsansvariga, med beaktande av deras roller såsom dessa fastställs i villkoren i det arrangemang som avses i punkt 1.

Artikel 29
Personuppgiftsbiträden

1. Om en behandling ska genomföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas.

2. Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde utan särskilt eller allmänt skriftligt förhandstillstånd från den personuppgiftsansvarige. Vid ett allmänt skriftligt tillstånd , ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.

3. När uppgifter behandlas av ett personuppgiftsbiträde ska behandlingen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige och i vilken föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges. I det avtalet eller den rättsakten ska det särskilt föreskrivas att personuppgiftsbiträdet

   a) endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av

personuppgifter till ett tredjeland eller en internationell organisation, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av; i så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt,

b) säkerställer att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt,

c) vidtar alla åtgärder som krävs enligt artikel 33,

d) respekterar de villkor som avses i punkterna 2 och 4 för anlitandet av ett annat personuppgiftsbiträde,

e) med tanke på behandlingens art, hjälper den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter i enlighet med kapitel III,

f) bistår den personuppgiftsansvarige med att säkerställa att skyldigheterna enligt artiklarna 33–40 iakttas, med beaktande av arten av behandling och den information som personuppgiftsbiträdet har att tillgå,

g) beroende på vad den personuppgiftsansvarige väljer, raderar eller återlämnar alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av behandlingstjänster har avslutats, och raderar befintliga kopior såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt, och

h) ger den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i denna artikel iakttas samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige.

Med avseende på första stycket led h ska personuppgiftsbiträdet omedelbart informera den personuppgiftsansvarige om denne anser att en instruktion strider mot denna förordning eller mot andra av unionens eller medlemsstaternas dataskyddsbestämmelser.

4. I de fall där ett personuppgiftsbiträde anlitar ett annat personuppgiftsbiträde för utförande av specifik behandling på den personuppgiftsansvariges vägnar ska det andra personuppgiftsbiträdet, genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt, åläggas samma skyldigheter i fråga om dataskydd som de som fastställs i avtalet eller den andra rättsakten mellan den personuppgiftsansvarige och personuppgiftsbiträdet enligt punkt 3, och särskilt att ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning. Om det andra personuppgiftsbiträdet inte fullgör sina skyldigheter i fråga om dataskydd ska det ursprungliga personuppgiftsbiträdet vara fullt ansvarigt gentemot den personuppgiftsansvarige för utförandet av det andra personuppgiftsbiträdets skyldigheter.

5. Om ett personuppgiftsbiträde inte är en unionsinstitution eller ett unionsorgan får dess anslutning till en godkänd uppförandekod som avses i artikel 40.5 i förordning (EU) 2016/679 eller en godkänd certifieringsmekanism som avses i artikel 42 i förordning (EU) 2016/679 användas för att visa att tillräckliga garantier tillhandahålls, så som avses punkterna 1 och 4 i denna artikel.

6. Det avtal eller den andra rättsakt som avses i punkterna 3 och 4 i denna artikel får, utan att det påverkar tillämpningen av ett enskilt avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet, helt eller delvis baseras på sådana standardavtalsklausuler som avses i punkterna 7 och 8 i denna artikel, inbegripet när de ingår i en certifiering som i enlighet med artikel 42 i förordning (EU) 2016/679 beviljats den personuppgiftsansvarige som inte är en unionsinstitution eller ett unionsorgan enligt artikel 42 i förordning (EU) 2016/679.

7. Kommissionen får fastställa standardavtalsklausuler för de frågor som avses i punkterna 3 och 4 i denna artikel, i enlighet med det granskningsförfarande som avses i artikel 70.2.

8. Europeiska datatillsynsmannen får fastställa standardavtalsklausuler för de frågor som avses i punkterna 3 och 4.

9. Det avtal eller den andra rättsakt som avses i punkterna 3 och 4 ska upprättas skriftligen, inbegripet i ett elektroniskt format.

10. Om ett personuppgiftsbiträde överträder denna förordning genom att fastställa ändamålen med och medlen för behandlingen, ska personuppgiftsbiträdet anses vara en personuppgiftsansvarig med avseende på den behandlingen, utan att det påverkar tillämpningen av artiklarna 65 och 66.

Artikel 30
Behandling under den personuppgiftsansvariges och personuppgiftsbiträdets överinseende

Personuppgiftsbiträdet och personer som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, får endast behandla dessa på instruktion från den personuppgiftsansvarige, såvida de inte är skyldiga att göra det enligt unionsrätten eller medlemsstaternas nationella rätt.

Artikel 31
Register över behandling

1. Varje personuppgiftsansvarig ska föra ett register över behandling som utförts under dess ansvar. Detta register ska innehålla samtliga följande uppgifter:

   a) Namn och kontaktuppgifter för den personuppgiftsansvarige, dataskyddsombudet samt, i tillämpliga fall, personuppgiftsbiträdet och den gemensamt personuppgiftsansvariga.

   b) Ändamålen med behandlingen.

   c) En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.

d) De kategorier av mottagare till vilka personuppgifterna har lämnats ut eller ska lämnas ut, inbegripet mottagare i medlemsstater, tredjeländer eller internationella organisationer.

e) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och dokumentation av lämpliga skyddsåtgärder.

f) Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.

g) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 33.

2. Varje personuppgiftsbiträde ska föra ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning, som ska omfatta följande:

a) Namn och kontaktuppgifter för personuppgiftsbiträdet eller personuppgiftsbiträdena, för varje personuppgiftsansvarig för vars räkning personuppgiftsbiträdet agerar samt för dataskyddsombudet.

b) De kategorier av behandling som har utförts för varje personuppgiftsansvariges räkning.

c) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och dokumentation av lämpliga skyddsåtgärder.

d) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 33.

3. De register som avses i punkterna 1 och 2 ska upprättas skriftligen, inbegripet i elektronisk form.

4. Unionens institutioner och organ ska göra registret tillgängligt för Europeiska datatillsynsmannen på begäran.

5. Unionens institutioner och organ får besluta att bevara sina register över behandling i ett centralt register. I detta fall får de också besluta att göra registret allmänt tillgängligt.

Artikel 32
Samarbete med Europeiska datatillsynsmannen

Unionens institutioner och organ ska på begäran samarbeta med Europeiska datatillsynsmannen vid fullgörandet av dess uppgifter.

AVSNITT 2

SÄKERHET FÖR PERSONUPPGIFTER OCH KONFIDENTIALITET FÖR ELEKTRONISK KOMMUNIKATION

Artikel 33
Säkerhet i samband med behandlingen

1. Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet när det är lämpligt

   (a) pseudonymisering och kryptering av personuppgifter,

   (b) förmågan att säkerställa fortlöpande konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,

   (c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,

   (d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

2. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, särskilt från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

3. Den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige, om inte unionsrätten ålägger honom eller henne att göra det.

Artikel 34
Konfidentialitet för elektronisk kommunikation

Unionens institutioner och organ ska säkerställa konfidentiell behandling av uppgifter inom elektronisk kommunikation, särskilt genom att säkra sina elektroniska kommunikationsnät.

Artikel 35
Skydd av information som rör slutanvändarnas terminalutrustning

Unionens institutioner och organ ska skydda information som rör slutanvändares terminalutrustning som används för att få tillgång till deras offentligt tillgängliga webbplatser och mobilapplikationer i enlighet med förordning (EU) nr XX/XXXX [nya förordningen om integritet och elektronisk kommunikation], särskilt artikel 8.

Artikel 36
Kataloger över användare

1. Personuppgifter i kataloger och tillgång till sådana kataloger ska begränsas till vad som krävs för de specifika ändamålen med katalogen.

2. Unionens institutioner och organ ska vidta alla nödvändiga åtgärder för att förhindra att personuppgifter i dessa kataloger, oavsett om de är tillgängliga för allmänheten eller inte, används för direkt marknadsföring.

Artikel 37
Anmälan av en personuppgiftsincident till Europeiska datatillsynsmannen

1. Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, senast 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till Europeiska datatillsynsmannen, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till Europeiska datatillsynsmannen inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.

2. Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident.

3. Den anmälan som avses i punkt 1 ska åtminstone

   a) beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,

   b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet,

   c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten,

   d) beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

4. Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

5. Den personuppgiftsansvarige ska underrätta dataskyddsombudet om personuppgiftsincidenten.

6. Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för Europeiska datatillsynsmannen att kontrollera efterlevnaden av denna artikel.

Artikel 38
Information till den registrerade om en personuppgiftsincident

1. Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.

2. Den information till den registrerade som avses i punkt 1 i denna artikel ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone de upplysningar och åtgärder som avses i artikel 37.3 b, c och d.

3. Information till den registrerade i enlighet med punkt 1 ska inte krävas om något av följande villkor är uppfyllt:

   a) Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder tillämpades på de personuppgifter som påverkades av personuppgiftsincidenten, särskilt sådana som ska göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna, såsom kryptering.

   b) Den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter som avses i punkt 1 sannolikt inte längre kommer att uppstå.

   c) Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället en information till allmänheten göras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.

4. Om den personuppgiftsansvarige inte redan har informerat den registrerade om personuppgiftsincidenten får Europeiska datatillsynsmannen, efter att ha bedömt sannolikheten för att personuppgiftsincidenten medför en hög risk, kräva att personuppgiftsbiträdet gör det eller får besluta att något av de villkor som avses i punkt 3 uppfylls.

AVSNITT 3

KONSEKVENSBEDÖMNING AVSEENDE DATASKYDD SAMT FÖREGÅENDE SAMRÅD

Artikel 39
Konsekvensbedömning avseende dataskydd

1. Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för

fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning får omfatta en serie liknande behandlingar som medför liknande höga risker.

2. Den personuppgiftsansvarige ska rådfråga dataskyddsombudet vid genomförande av en konsekvensbedömning avseende dataskydd.

3. En konsekvensbedömning avseende dataskydd som avses i punkt 1 ska särskilt krävas i vid

   a) en systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer,

   b) behandling i stor omfattning av särskilda kategorier av uppgifter som avses i artikel 10 eller av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som avses i artikel 11, eller

   c) en systematisk övervakning av en allmän plats i stor omfattning.

4. Europeiska datatillsynsmannen ska upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd i enlighet med punkt 1.

5. Europeiska datatillsynsmannen får också upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som inte kräver någon konsekvensbedömning avseende dataskydd.

6. Bedömningen ska innehålla åtminstone

   a) en systematisk beskrivning av den planerade behandlingen och behandlingens syften,

   b) en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,

   c) en bedömning av de risker för de registrerades rättigheter och friheter som avses i punkt 1, och

   d) de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att denna förordning efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

7. Efterlevnaden av godkända uppförandekoder enligt artikel 40 i förordning (EU) 2016/679 från andra personuppgiftsbiträden än unionens institutioner och organ ska på lämpligt sätt beaktas vid bedömningen av konsekvenserna av de behandlingar som utförs av dessa personuppgiftsbiträden, särskilt när det gäller att ta fram en konsekvensbedömning avseende dataskydd.

8. Den personuppgiftsansvarige ska, när det är lämpligt, inhämta synpunkter från de registrerade eller deras företrädare om den avsedda behandlingen, utan att det påverkar skyddet av allmänna intressen eller behandlingens säkerhet.

9. Om behandlingen i enlighet med artikel 5.1 a eller b har en rättslig grund i en rättsakt som antagits på grundval av fördragen och som reglerar den särskilda behandlingen eller serien av behandlingar i fråga, och om en konsekvensbedömning avseende dataskydd redan har genomförts som en del av en allmän konsekvensbedömning som föregick antagandet av den rättsakten, ska punkterna 1–6 inte vara tillämpliga, såvida inte unionsrätten föreskriver något annat.

10. Den personuppgiftsansvarige ska vid behov genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen avseende dataskydd åtminstone när den risk som behandlingen medför förändras.

Artikel 40
Föregående samråd

1. Den personuppgiftsansvarige ska samråda med Europeiska datatillsynsmannen inför uppgiftsbehandling där det av en konsekvensbedömning avseende dataskydd i enlighet med artikel 39 framgår att behandlingen utan skyddsåtgärder, säkerhetsåtgärder och mekanismer för att minska risken kommer att innebära en hög risk för fysiska personers rättigheter och friheter, och den personuppgiftsansvarige anser att risken inte kan minskas genom åtgärder som är rimliga med avseende på tillgänglig teknik och genomförandekostnader. Den personuppgiftsansvarige ska rådfråga dataskyddsombudet om behovet av föregående samråd.

2. Om Europeiska datatillsynsmannen anser att den planerade behandling som avses i punkt 1 skulle strida mot denna förordning, särskilt om den personuppgiftsansvarige inte i tillräcklig mån har fastställt eller minskat risken, ska Europeiska datatillsynsmannen inom en period på högst åtta veckor från det att begäran om samråd mottogs, ge den personuppgiftsansvarige och i tillämpliga fall personuppgiftsbiträdet skriftliga råd och får utnyttja alla de befogenheter som den har enligt artikel 59. Denna period får förlängas med sex veckor med beaktande av hur komplicerad den planerade behandlingen är. Europeiska datatillsynsmannen ska informera den personuppgiftsansvarige och, i tillämpliga fall, personuppgiftsbiträdet om en sådan förlängning inom en månad från det att begäran om samråd mottagits, tillsammans med orsakerna till förseningen. Dessa perioder får avbrytas tillfälligt i avvaktan på att Europeiska datatillsynsmannen erhåller den information som den har begärt med tanke på samrådet.

3. Vid samråd med Europeiska datatillsynsmannen enligt punkt 1 ska den personuppgiftsansvarige till Europeiska datatillsynsmannen lämna

   a) i tillämpliga fall, uppgift om de respektive ansvarsområdena för de personuppgiftsansvariga, gemensamt personuppgiftsansvariga och personuppgiftsbiträden som medverkar vid behandlingen,

   b) ändamålen med och medlen för den avsedda behandlingen,

   c) de åtgärder som vidtas och de garantier som lämnas för att skydda de registrerades rättigheter och friheter enligt denna förordning,

d) kontaktuppgifter till dataskyddsombudet,

e) konsekvensbedömningen avseende dataskydd enligt artikel 39, och

f) all annan information som begärs av Europeiska datatillsynsmannen.

4. Kommissionen får genom genomförandeakter fastställa en förteckning över de fall där de personuppgiftsansvariga ska samråda med, och erhålla förhandstillstånd av, Europeiska datatillsynsmannen i samband med behandling av uppgifter med anknytning till en arbetsuppgift som den personuppgiftsansvarige utför i allmänhetens intresse, inbegripet behandling av sådana uppgifter i samband med social trygghet och folkhälsa.

AVSNITT 4

INFORMATION OCH SAMRÅD I LAGSTIFTNINGSPROCESSEN

Artikel 41
Information

Unionens institutioner och organ ska underrätta Europeiska datatillsynsmannen när de utarbetar administrativa åtgärder och interna regler som rör behandling av personuppgifter där en unionsinstitution eller ett unionsorgan deltar, ensamt eller tillsammans med andra.

Artikel 42
Samråd i lagstiftningsprocessen

1. Efter antagandet av förslag till en lagstiftningsakt och av rekommendationer eller förslag till rådet i enlighet med artikel 218 i EUF-fördraget och i samband med utarbetandet av delegerade akter eller genomförandeakter vilka har en inverkan på skyddet av enskilda personers rättigheter och friheter med avseende på behandling av personuppgifter, ska kommissionen samråda med Europeiska datatillsynsmannen.

2. När en akt som avses i punkt 1 är av särskild betydelse för skyddet av enskilda personers rättigheter och friheter med avseende på behandling av personuppgifter, får kommissionen även samråda med Europeiska dataskyddsstyrelsen. I sådana fall ska Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen samordna sitt arbete i syfte att utfärda ett gemensamt yttrande.

3. Den rådgivning som avses i punkterna 1 och 2 ska tillhandahållas skriftligen inom en period på högst åtta veckor från mottagandet av begäran om samråd i som avses i punkterna 1 och 2. I brådskande fall, eller där det i övrigt är lämpligt, får kommissionen förkorta tidsfristen.

4. Denna artikel ska inte tillämpas i de fall då kommissionen i enlighet med förordning (EU) 2016/679 är skyldig att samråda med Europeiska dataskyddsstyrelsen.

AVSNITT 5

SKYLDIGHET ATT REAGERA PÅ ANMÄRKNINGAR

Artikel 43
Skyldighet att reagera på anmärkningar

När Europeiska datatillsynsmannen utövar de befogenheter som föreskrivs i artikel 59.2 a b och c, ska den berörda personuppgiftsansvarige eller det berörda personuppgiftsbiträdet informera Europeiska datatillsynsmannen om sina synpunkter inom en rimlig period, som ska fastställas av Europeiska datatillsynsmannen med beaktande av omständigheterna i varje enskilt fall. Dessa synpunkter ska i förekommande fall också innehålla en beskrivning av de eventuella åtgärder som har vidtagits med anledning av anmärkningar från Europeiska datatillsynsmannen.

AVSNITT 6

DATASKYDDSOMBUD

Artikel 44
Utnämning av dataskyddsombudet

1. Varje unionsinstitution eller unionsorgan ska utse ett dataskyddsombud.

2. Unionens institutioner och organ får utse ett enda dataskyddsombud för flera av dem, med hänsyn till deras organisationsstruktur och storlek.

3. Dataskyddsombudet ska utses på grundval av yrkesmässiga kvalifikationer och, särskilt, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i artikel 46.

4. Dataskyddsombudet får ingå i unionsinstitutionens eller unionsorganets personal, eller utföra uppgifterna på grundval av ett tjänsteavtal.

5. Unionens institutioner och organ ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till Europeiska datatillsynsmannen.

Artikel 45
Dataskyddsombudets ställning

1. Unionens institutioner och organ ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

2. Unionens institutioner och organ ska stödja dataskyddsombudet i utförandet av de uppgifter som avses i artikel 46 genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av hans eller hennes sakkunskap.

3. Unionens institutioner och organ ska säkerställa att uppgiftskyddsombudet inte tar emot instruktioner som gäller utförandet av hans eller hennes uppgifter. Dataskyddsombudet får inte avsättas eller bli föremål för sanktioner av den personuppgiftsansvarige eller personuppgiftsbiträdet för att ha utfört sina uppgifter. Dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta ledningsnivå.

4. Den registrerade får kontakta dataskyddsombudet med avseende på alla frågor som rör behandlingen av dennes personuppgifter och utövandet av dennes rättigheter enligt denna förordning.

5. Dataskyddsombudet och hans eller hennes personal ska, när det gäller genomförandet av hans eller hennes uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten.

6. Dataskyddsombudet får fullgöra andra uppgifter och uppdrag. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska se till att sådana uppgifter och uppdrag inte leder till en intressekonflikt.

7. Dataskyddsombudet får rådfrågas av den personuppgiftsansvarige och personuppgiftsbiträdet, av den berörda personalkommittén och av enskilda personer, utan att dessa behöver gå den officiella vägen, i alla frågor som rör tolkningen eller tillämpningen av denna förordning. Ingen ska lida förfång för att ha gjort det behöriga dataskyddsombudet uppmärksamt på att en händelse som påstås utgöra en överträdelse av bestämmelserna i denna förordning har ägt rum.

8. Dataskyddsombudet ska utses för en period på tre till fem år och ska kunna ges förnyat mandat. Dataskyddsombudet får avsättas från sitt uppdrag av den unionsinstitution eller det unionsorgan som utsett henne eller honom endast efter medgivande av Europeiska datatillsynsmannen, om han eller hon inte längre uppfyller de krav som ställs för att han eller hon ska kunna utföra sina uppgifter.

9. Efter det att dataskyddsombudet har utsetts ska han eller hon registreras hos Europeiska datatillsynsmannen av den unionsinstitution eller det unionsorgan som utsåg vederbörande.

Artikel 46
Dataskyddsombudets uppgifter

1. Dataskyddsombudet ska ha följande uppgifter:

   (a) Informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar om deras skyldigheter enligt denna förordning och andra av unionens dataskyddsbestämmelser.

   (b) På ett oberoende sätt säkerställa den interna tillämpningen av denna förordning och övervaka efterlevnaden av denna förordning, av annan tillämplig unionsrätt som innehåller dataskyddsbestämmelser och av den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.

(c) Säkerställa att registrerade informeras om sina rättigheter och skyldigheter enligt denna förordning.

(d) På begäran ge råd vad gäller behovet av en anmälan eller ett meddelande om personuppgiftsincidenter i enlighet med artiklarna 37 och 38.

(e) På begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka dess genomförande enligt artikel 39 och samråda med Europeiska datatillsynsmannen vid eventuellt tvivel om behovet av en konsekvensbedömning avseende dataskydd.

(f) På begäran ge råd vad gäller behovet av förhandssamråd med Europeiska datatillsynsmannen i enlighet med artikel 40 och samråda med Europeiska datatillsynsmannen vid eventuellt tvivel om behovet av ett förhandssamråd.

(g) Besvara framställningar från Europeiska datatillsynsmannen och, inom ramen för sin behörighet, samarbeta och samråda med denne på Europeiska datatillsynsmannens begäran eller på eget initiativ.

2. Dataskyddsombudet får ge rekommendationer för den praktiska förbättringen av uppgiftsskyddet till den personuppgiftsansvarige och personuppgiftsbiträdet och ge dem råd i frågor som rör tillämpningen av bestämmelserna om uppgiftsskydd. Dessutom får han eller hon, på eget initiativ eller på begäran av den personuppgiftsansvarige eller personuppgiftsbiträdet, den berörda personalkommittén eller varje enskild person, utreda frågor och händelser som har direkt samband med hans eller hennes uppgifter och som kommer till hans eller hennes kännedom och rapportera tillbaka till den person som beställde undersökningen eller till den personuppgiftsansvarige eller personuppgiftsbiträdet.

3. Ytterligare genomföranderegler rörande dataskyddsombudet ska antas av varje unionsinstitution eller unionsorgan. Genomföranderegleрna ska i synnerhet avse dataskyddsombudets arbetsuppgifter, åligganden och befogenheter.

KAPITEL V

Överföring av personuppgifter till tredjeländer eller internationella organisationer

Artikel 47
Allmän princip för överföring av uppgifter

Överföring av personuppgifter som är under behandling eller är avsedda att behandlas efter det att de överförts till ett tredjeland eller en internationell organisation får endast ske om, med förbehåll för övriga bestämmelser i denna förordning, den personuppgiftsansvarige och personuppgiftsbiträdet uppfyller villkoren i detta kapitel, inklusive för vidare överföring av personuppgifter från det tredjelandet eller den internationella organisationen till ett annat tredjeland eller en annan internationell organisation. Alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den nivå på skyddet av fysiska personer som säkerställs genom denna förordning inte undergrävs.

Artikel 48
Överföring på grundval av ett beslut om adekvat skyddsnivå

1. En överföring av personuppgifter till ett tredjeland eller en internationell organisation får ske om kommissionen enligt artikel 45.3 i förordning (EU) 2016/679 har beslutat att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom det tredjelandet, eller inom den internationella organisationen säkerställer en adekvat skyddsnivå, och personuppgifter överförs uteslutande för att göra det möjligt att utföra uppgifter som omfattas av den personuppgiftsansvariges behörighet.

2. Unionens institutioner och organ ska informera kommissionen och Europeiska datatillsynsmannen om de anser att ifrågavarande tredjeland eller internationella organisation inte säkerställer en adekvat skyddsnivå enligt punkt 1.

3. Unionens institutioner och organ ska vidta de åtgärder som är nödvändiga för att följa de beslut kommissionen fattat när den i enlighet med artikel 45.3 och 45.5 i förordning (EU) 2016/679 fastställer att ett tredjeland eller en internationell organisation säkerställer eller inte längre säkerställer en lämplig skyddsnivå.

Artikel 49
Överföring som omfattas av lämpliga skyddsåtgärder

1. I avsaknad av ett beslut i enlighet med artikel 45.3 i förordning (EU) 2016/679, får en personuppgiftsansvarig eller ett personuppgiftsbiträde överföra personuppgifter till ett tredjeland eller en internationell organisation endast efter att ha vidtagit lämpliga skyddsåtgärder, och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga.

2. Lämpliga skyddsåtgärder enligt punkt 1 får, utan att det krävs särskilt tillstånd från Europeiska datatillsynsmannen, införas genom

   (a) ett rättsligt bindande och verkställbart instrument mellan offentliga myndigheter eller organ,

   (b) standardiserade dataskyddsbestämmelser som antas av kommissionen i enlighet med det granskningsförfarande som avses i artikel 70.2,

   (c) standardiserade dataskyddsbestämmelser som antags av Europeiska datatillsynsmannen och godkänns av kommissionen i enlighet med det granskningsförfarande som avses i artikel 70.2,

   (d) bindande företagsbestämmelser, uppförandekoder och certifieringsmekanismer som avses i artikel 46.2 b, e och f i förordning (EU) 2016/679, i de fall där personuppgiftsbiträdet inte är en unionsinstitution eller ett unionsorgan.

3. Med förbehåll för tillstånd från Europeiska datatillsynsmannen, får lämpliga skyddsåtgärder enligt punkt 1 också i synnerhet införas genom

   (a) avtalsklausuler mellan den personuppgiftsansvarige eller personuppgiftsbiträdet och den personuppgiftsansvarige, personuppgiftsbiträdet eller mottagaren av personuppgifterna i tredjelandet eller den internationella organisationen, eller

(b) bestämmelser som ska införas i administrativa överenskommelser mellan offentliga myndigheter eller organ vilka inbegriper verkställbara och faktiska rättigheter för registrerade.

4. Unionens institutioner och organ ska informera Europeiska datatillsynsmannen om kategorier av fall där denna artikel har tillämpats.

5. Tillstånd från Europeiska datatillsynsmannen på grundval av artikel 9.7 i förordning (EG) 45/2001 ska förbli giltiga till dess att de, vid behov, har ändrats, ersatts eller upphävts av Europeiska datatillsynsmannen.

Artikel 50
Överföringar och utlämnanden som inte är tillåtna enligt unionsrätten

Domstolsbeslut eller beslut från myndigheter i tredjeland där det krävs att en personuppgiftsansvarig eller ett personuppgiftsbiträde överför eller lämnar ut personuppgifter får erkännas eller verkställas på något som helst sätt endast om det grundar sig på en internationell överenskommelse, såsom ett avtal om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen, utan att detta påverkar andra grunder för överföring enligt detta kapitel.

Artikel 51
Undantag i särskilda situationer

1. Om det inte föreligger något beslut om enligt artikel 45.3 i förordning (EU) 2016/679 eller lämpliga skyddsåtgärder enligt artikel 49 ska en överföring eller en uppsättning av överföringar av personuppgifter till ett tredjeland eller en internationell organisation ske endast om något av följande villkor är uppfyllt:

(a) Den registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med sådana överföringar för den registrerade med hänsyn till att det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder.

(b) Överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den personuppgiftsansvarige eller för att genomföra åtgärder som föregår ett sådant avtal på den registrerades begäran.

(c) Överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den personuppgiftsansvarige och en annan fysisk eller juridisk person som ingåtts i den registrerades intresse.

(d) Överföringen är nödvändig av viktiga skäl som rör allmänintresset.

(e) Överföringen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

(f) Överföringen är nödvändig för att skydda den registrerades eller andra personers grundläggande intressen, när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.

(g) Överföringen görs från ett register som enligt unionsrätten är avsett att ge information till allmänheten och som är tillgängligt antingen för allmänheten eller för varje person som kan påvisa ett legitimt intresse, men endast i den utsträckning som villkoren i unionsrätten om tillgång för allmänheten är uppfyllda i det särskilda fallet.

2. En överföring enligt punkt 1 g får inte omfatta alla personuppgifter eller hela kategorier av personuppgifter som finns i registret, såvida inte unionsrätten tillåter det. Om registret är avsett att vara tillgängligt för personer med ett berättigat intresse ska överföringen endast göras på begäran av dessa personer eller om de själva är mottagarna.

3. Det allmänintresse som avses i punkt 1 d ska vara erkänt i unionsrätten.

4. Om det saknas ett beslut om adekvat skyddsnivå, får unionsrätten med hänsyn till viktiga allmänintressen uttryckligen fastställa gränser för överföringen av specifika kategorier av personuppgifter till ett tredjeland eller en internationell organisation.

5. Unionens institutioner och organ ska informera Europeiska datatillsynsmannen om kategorier av fall där denna artikel har tillämpats.

Artikel 52
Internationellt samarbete för skydd av personuppgifter

När det gäller tredjeländer och internationella organisationer ska Europeiska datatillsynsmannen, i samarbete med kommissionen och Europeiska dataskyddsstyrelsen, vidta lämpliga åtgärder för att

(a) utveckla rutiner för det internationella samarbetet för att underlätta ett effektivt upprätthållande av lagstiftningen om skydd av personuppgifter,

(b) tillhandahålla internationellt ömsesidigt bistånd för ett effektivt upprätthållande av lagstiftningen om skydd av personuppgifter, bland annat genom anmälan, hänskjutande av klagomål, assistans vid utredningar samt informationsutbyte, med iakttagande av lämpliga åtgärder till skydd för personuppgifter samt andra grundläggande rättigheter och friheter,

(c) involvera berörda aktörer i diskussioner och åtgärder som syftar till att öka det internationella samarbetet när det gäller tillämpningen av lagstiftningen om skydd av personuppgifter,

(d) främja utbyte och dokumentation om lagstiftning och praxis för skydd av personuppgifter, inklusive avseende behörighetskonflikter med tredjeländer.

KAPITEL VI

EUROPEISKA DATATILLSYNSMANNEN

Artikel 53
Europeiska datatillsynsmannen

1. Härmed inrättas Europeiska datatillsynsmannen.

2. Vad gäller behandling av personuppgifter ska Europeiska datatillsynsmannen ha i uppdrag att säkerställa att fysiska personers grundläggande fri- och rättigheter, särskilt deras rätt till dataskydd, respekteras av unionens institutioner och organ.

3. Europeiska datatillsynsmannen ska ha i uppdrag att övervaka och garantera tillämpningen av bestämmelserna i denna förordning och andra unionsrättsakter om skyddet för fysiska personers grundläggande fri- och rättigheter då en unionsinstitution eller ett unionsorgan behandlar personuppgifter och för att ge råd till unionens institutioner och organ och de registrerade i alla frågor som rör behandling av personuppgifter. För dessa ändamål ska Europeiska datatillsynsmannen fullgöra de uppgifter som anges i artikel 58 och utöva de befogenheter som anges i artikel 59.

Artikel 54
Utnämning av Europeiska datatillsynsmannen

1. Europaparlamentet och rådet ska i samförstånd utnämna Europeiska datatillsynsmannen för en period av fem år, på grundval av en förteckning som kommissionen upprättat efter en offentlig infordran av intresseanmälningar. Infordran av intresseanmälningar ska göra det möjligt för alla intresserade parter i hela unionen att lämna in sina ansökningar. Den förteckning över kandidater som upprättats av kommissionen ska vara offentlig. På grundval av den förteckning som upprättats av kommissionen får Europaparlamentets behöriga utskott besluta att hålla en utfrågning för att kunna yttra sig om vilken kandidat det föredrar.

2. Den förteckning som upprättats av kommissionen och från vilken Europeiska datatillsynsmannen ska utses ska bestå av personer vars oberoende är ställt utom varje tvivel och som har den erfarenhet och sakkunskap som krävs för att utöva uppdraget som Europeisk datatillsynsman, exempelvis genom att de tillhör eller har tillhört de tillsynsmyndigheter som har inrättats i enlighet med artikel 41 i förordning (EU) 2016/679.

3. Europeiska datatillsynsmannens mandattid ska kunna förnyas en gång.

4. Europeiska datatillsynsmannens skyldigheter ska upphöra i följande fall:

   (a) Om Europeiska datatillsynsmannen byts ut.

   (b) Om Europeiska datatillsynsmannen avgår.

(c) Om Europeiska datatillsynsmannen entledigas eller avsätts.

5. Europeiska datatillsynsmannen kan på begäran av Europaparlamentet, rådet eller kommissionen entledigas eller fråntas sina pensionsrättigheter eller andra förmåner av Europeiska gemenskapernas domstol, om han eller hon inte längre uppfyller de krav som ställs för att han eller hon ska kunna utföra sina uppgifter eller om han eller hon gjort sig skyldig till allvarlig försummelse.

6. Vid normal nytillsättning eller frivillig avgång ska Europeiska datatillsynsmannen emellertid kvarstå i tjänst till dess att han eller hon har fått en ersättare.

7. Artiklarna 11–14 och 17 i protokollet om Europeiska gemenskapernas immunitet och privilegier ska vara tillämpliga på Europeiska datatillsynsmannen.

Artikel 55
Föreskrifter och allmänna villkor för hur Europeiska datatillsynsmannen ska utöva sitt ämbete samt om personal och finansiella medel

1. Europeiska datatillsynsmannen ska anses likställd med en domare vid Europeiska unionens domstol när det gäller fastställande av löner, ersättningar, ålderspension och all annan ersättning utöver lön.

2. Budgetmyndigheten ska se till att Europeiska datatillsynsmannen erhåller den personal och de finansiella medel som behövs för att han eller hon ska kunna fullgöra sina uppgifter.

3. Budgeten för Europeiska datatillsynsmannen ska finnas under en särskild budgetpost i avsnitt IX i Europeiska unionens allmänna budget.

4. Europeiska datatillsynsmannen ska biträdas av ett sekretariat. Tjänstemän och övriga anställda vid sekretariatet ska utses av Europeiska datatillsynsmannen, som ska vara deras överordnade. De ska endast stå under hans eller hennes ledning. Deras antal ska fastställas varje år inom ramen för budgetförfarandet.

5. Tjänstemän och övriga anställda vid Europeiska datatillsynsmannens sekretariat ska omfattas av de förordningar och regler som tillämpas på tjänstemän och övriga anställda i Europeiska unionen.

6. Europeiska datatillsynsmannen ska ha sitt säte i Bryssel.

Artikel 56
Oberoende

1. Europeiska datatillsynsmannen ska vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med denna förordning.

2. Europeiska datatillsynsmannen ska i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med denna förordning stå fri från utomstående påverkan, direkt såväl som indirekt, och får varken begära eller ta emot instruktioner av någon.

3. Europeiska datatillsynsmannen ska avstå från alla handlingar som står i strid med hans eller hennes tjänsteutövning och under sin ämbetstid avstå från all annan avlönad eller oavlönad yrkesverksamhet.

4. Efter sin ämbetstid ska Europeiska datatillsynsmannen visa integritet och omdöme i fråga om att acceptera utnämningar och ta emot förmåner.

Artikel 57
Tystnadsplikt

Både under och efter sin ämbetstid ska Europeiska datatillsynsmannen och hans eller hennes personal omfattas av tystnadsplikt vad avser konfidentiell information som har kommit till deras kännedom under tjänsteutövningen.

Artikel 58
Uppgifter

1. Utan att det påverkar de andra uppgifter som föreskrivs i denna förordning ska Europeiska datatillsynsmannen ansvara för följande:

   (a) Övervaka och upprätthålla tillämpningen av denna förordning och andra unionsrättsakter som rör skydd av fysiska personer i samband med en unionsinstitutions eller ett unionsorgans behandling av personuppgifter, med undantag av behandling av personuppgifter som utförs av Europeiska unionens domstol i dess rättskipande funktion.

   (b) Öka allmänhetens medvetenhet om och förståelse för risker, regler, skyddsåtgärder och rättigheter i fråga om behandling. Särskild uppmärksamhet ska ägnas åt insatser som riktar sig till barn.

   (c) Öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter enligt denna förordning.

   (d) På begäran tillhandahålla information till registrerade om hur de ska utöva sina rättigheter enligt denna förordning, och om så krävs samarbeta med tillsynsmyndigheter i medlemsstater för detta ändamål.

   (e) Behandla klagomål som lämnats in av en registrerad eller av ett organ, en organisation eller en sammanslutning i enlighet med artikel 67, och där så är lämpligt undersöka den sakfråga som klagomålet gäller och inom rimlig tid underrätta klaganden om hur undersökningen fortskrider och om resultatet, särskilt om det krävs ytterligare undersökningar eller samordning med en annan tillsynsmyndighet.

   (f) Utföra undersökningar om tillämpningen av denna förordning, inbegripet på grundval av information som erhålls från en annan tillsynsmyndighet eller annan myndighet.

   (g) Ge rådgivning åt alla unionens institutioner och organ om lagstiftningsåtgärder och administrativa åtgärder rörande skyddet av fysiska personers rättigheter och friheter när det gäller behandling av personuppgifter.

(h) Övervaka relevant utveckling i den mån den påverkar skyddet av personuppgifter, särskilt inom informations- och kommunikationsteknik.

(i) Anta sådana standardavtalsklausuler som avses i artiklarna 29.8 och 49.2 c.

(j) Upprätta och föra en förteckning när det gäller kravet på en konsekvensbedömning avseende dataskydd enligt artikel 39.4.

(k) Delta i den verksamhet som bedrivs av Europeiska dataskyddsstyrelsen, som inrättats genom artikel 68 i förordning (EU) 2016/679.

(l) Tillhandahålla Europeiska dataskyddsstyrelsens sekretariat, i enlighet med artikel 75 i förordning (EU) 2016/679.

(m) Ge råd om behandling som avses i artikel 40.2.

(n) Godkänna sådana avtalsklausuler och bestämmelser som avses i artikel 49.3.

(o) Hålla arkiv över överträdelser av denna förordning och åtgärder som vidtagits i enlighet med artikel 59.2.

(p) Utföra eventuella andra uppgifter som rör skyddet av personuppgifter.

(q) Anta sin arbetsordning.

2. Europeiska datatillsynsmannen ska underlätta inlämnandet av klagomål enligt punkt 1 e genom ett särskilt formulär för det ändamålet, vilket också kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.

3. Utförandet av Europeiska datatillsynsmannens uppgifter ska vara avgiftsfritt för den registrerade.

4. Om en begäran är uppenbart ogrundad eller orimlig, särskilt på grund av dess repetitiva karaktär, får Europeiska datatillsynsmannen vägra att tillmötesgå begäran. Det åligger Europeiska datatillsynsmannen att visa att begäran är uppenbart ogrundad eller orimlig.

Artikel 59
Befogenheter

1. Europeiska datatillsynsmannen ska ha följande utredningsbefogenheter:

(a) Beordra den personuppgiftsansvarige eller personuppgiftsbiträdet att lämna all information som Europeiska datatillsynsmannen behöver för att kunna fullgöra sina uppgifter.

(b) Genomföra undersökningar i form av dataskyddstillsyn.

(c) Meddela den personuppgiftsansvarige eller personuppgiftsbiträdet om en påstådd överträdelse av denna förordning.

(d) Från den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter och all information som tillsynsmyndigheten behöver för att kunna fullgöra sina uppgifter.

(e) Få tillträde till alla lokaler som tillhör den personuppgiftsansvarige och personuppgiftsbiträdet, inbegripet tillgång till all utrustning och alla andra medel för behandling av personuppgifter i överensstämmelse med unionens processrätt eller medlemsstaternas nationella processrätt.

2. Europeiska datatillsynsmannen ska ha följande korrigerande befogenheter:

(a) Utfärda varningar till en personuppgiftsansvarig eller ett personuppgiftsbiträde om att planerade behandlingar sannolikt kommer att bryta mot bestämmelserna i denna förordning.

(b) Utfärda reprimander till en personuppgiftsansvarig eller ett personuppgiftsbiträde om behandling bryter mot bestämmelserna i denna förordning.

(c) Rapportera ärendet till den personuppgiftsansvarige eller det personuppgiftsbiträde som berörs och vid behov till Europaparlamentet, rådet och kommissionen.

(d) Förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att tillmötesgå den registrerades begäran att få utöva sina rättigheter enligt denna förordning.

(e) Förelägga en personuppgiftsansvarig eller ett personuppgiftsbiträde att se till att behandlingen sker i enlighet med bestämmelserna i denna förordning och om så krävs på ett specifikt sätt och inom en specifik period,

(f) Förelägga den personuppgiftsansvarige att meddela den registrerade att en personuppgiftsincident har inträffat.

(g) Införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, behandling.

(h) Förelägga om rättelse eller radering av personuppgifter eller begränsning av behandling enligt artiklarna 18, 19 och 20 och underrätta mottagare till vilka personuppgifterna har lämnats ut om dessa åtgärder enligt artiklarna 19.2 och 21.

(i) Påföra administrativa sanktionsavgifter i enlighet med artikel 66, om unionsinstitutionen eller institutionsorganet inte har efterlevt en av de åtgärder som avses i denna punkt, och beroende på omständigheterna i varje enskilt fall.

(j) Förelägga om att flödet av uppgifter till en mottagare i en medlemsstat, ett tredje land eller en internationell organisation ska avbrytas.

3. Europeiska datatillsynsmannen ska ha följande befogenheter att utfärda tillstånd och att ge råd:

(a) Ge råd till registrerade när de utövar sina rättigheter.

(b) Ge råd till den personuppgiftsansvarige i enlighet med det förfarande för föregående samråd som avses i artikel 40.

(c) På eget initiativ eller på begäran avge yttranden till unionens institutioner och organ samt till allmänheten, i frågor som rör skydd av personuppgifter.

(d) Anta standardiserade dataskyddsbestämmelser enligt artiklarna 29.8 och 49.2 c.

(e) Godkänna avtalsklausuler enligt artikel 49.3 a.

(f) Godkänna administrativa överenskommelser enligt artikel 49.3 b.

4. Utövandet av de befogenheter som Europeiska datatillsynsmannen tilldelas enligt denna artikel ska omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel och rättssäkerhet, som fastställs i unionsrätten.

5. Europeiska datatillsynsmannen ska ha befogenhet att hänskjuta ärendet till Europeiska unionens domstol på de villkor som anges i fördraget och att intervenera i ärenden som anhängiggjorts vid Europeiska unionens domstol.

Artikel 60
Verksamhetsrapport

1. Europeiska datatillsynsmannen ska lämna en årlig rapport om sin verksamhet till Europaparlamentet, rådet och kommissionen och samtidigt offentliggöra rapporten.

2. Europeiska datatillsynsmannen ska vidarebefordra verksamhetsrapporten till unionens övriga institutioner och organ, som får lämna kommentarer inför en eventuell granskning av rapporten i Europaparlamentet.

KAPITEL VII

SAMARBETE OCH ENHETLIGHET

Artikel 61
Samarbete med nationella tillsynsmyndigheter

Europeiska datatillsynsmannen ska samarbeta med de tillsynsmyndigheter som har inrättats i enlighet med artikel 41 i förordning (EU) 2016/679 och artikel 51 i direktiv (EU) 2016/680 (nedan kallad *nationella tillsynsmyndigheter*) samt med den gemensamma tillsynsmyndighet som inrättats genom artikel 25 i rådets beslut 2009/917/RIF[21] i den utsträckning som krävs för att de ska kunna fullgöra sina respektive uppgifter, särskilt genom att ge varandra relevant information, begära att de nationella tillsynsmyndigheterna utövar sina befogenheter eller svara på en begäran från dessa myndigheter.

[21] Rådets beslut 2009/917/RIF av den 30 november 2009 om användning av informationsteknik för tulländamål, EUT L 323, 10.12.2009, s. 20.

Artikel 62
En samordnad tillsyn av Europeiska datatillsynsmannen och de nationella tillsynsmyndigheterna

1. Om en unionsakt hänvisar till denna artikel ska Europeiska datatillsynsmannen aktivt samarbeta med de nationella tillsynsmyndigheterna för att säkerställa en effektiv tillsyn över stora it-system eller unionsbyråer.

2. Europeiska datatillsynsmannen ska inom ramen för sina respektive befogenheter och inom ramen för sitt ansvarsområde utbyta relevant information, bistå i samband med revision och kontroller, utreda problem med tolkningen eller tillämpningen av denna förordning och andra tillämpliga unionsakter, studera problem med att utöva oberoende tillsyn eller problem med de registrerades möjligheter att hävda sina rättigheter, upprätta harmoniserade förslag till lösningar på eventuella problem och främja medvetenheten om dataskyddsrättigheterna, om så behövs, tillsammans med de nationella tillsynsmyndigheterna.

3. För de ändamål som anges i punkt 2 ska Europeiska datatillsynsmannen sammanträda med de nationella tillsynsmyndigheterna minst två gånger om året inom ramen för Europeiska dataskyddsstyrelsen. Europeiska dataskyddsstyrelsen ska stå för kostnaderna för och tillhandahållandet av tjänster i samband med sådana möten. En arbetsordning ska antas vid det första mötet. Ytterligare arbetsmetoder ska utvecklas gemensamt efter behov.

4. Vartannat år ska Europeiska dataskyddsstyrelsen översända en gemensam verksamhetsrapport vad gäller samordnad tillsyn till Europaparlamentet, rådet och kommissionen.

KAPITEL VIII

RÄTTSMEDEL, ANSVAR OCH SANKTIONER

Artikel 63
Rätt att ge in klagomål till Europeiska datatillsynsmannen

1. Utan att det påverkar något rättsmedel, administrativt prövningsförfarande eller prövningsförfarande utanför domstol, ska varje registrerad som anser att behandlingen av personuppgifter som avser henne eller honom strider mot denna förordning ha rätt att lämna in ett klagomål till Europeiska datatillsynsmannen.

2. Europeiska datatillsynsmannen ska i rimlig tid informera den registrerade om hur arbetet med klagomålet fortskrider och vad resultatet blir, inbegripet möjligheten till rättslig prövning enligt artikel 64.

3. Om Europeiska datatillsynsmannen inte behandlar ett klagomål eller inte informerar den registrerade inom tre månader om hur arbetet fortskrider eller om resultatet av klagomålet, ska klagomålet anses ha avslagits.

Artikel 64
Rätten till ett effektivt rättsmedel

Europeiska unionens domstol ska vara behörig att pröva tvister som hänför sig till denna förordnings bestämmelser, inklusive skadeståndsanspråk.

Artikel 65
Rätt till ersättning

Varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av denna förordning ska ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan, med förbehåll för de villkor som anges i fördragen.

Artikel 66
Administrativa sanktionsavgifter

1. Europeiska datatillsynsmannen får ålägga unionsinstitutioner och unionsorgan administrativa sanktionsavgifter, med hänsyn till omständigheterna i det enskilda fallet, om en unionsinstitution eller ett unionsorgan inte rättar sig efter ett beslut av Europeiska datatillsynsmannen i enlighet med artikel 59.2 d-h och j. Vid beslut om huruvida administrativa sanktionsavgifter ska åläggas och om avgiftsbeloppet i varje enskilt fall ska vederbörlig hänsyn tas till följande:

   (a) Överträdelsens karaktär, svårhetsgrad och varaktighet med beaktande av den aktuella uppgiftsbehandlingens karaktär, omfattning eller syfte samt antalet berörda registrerade och den skada som de har lidit.

   (b) De åtgärder som unionsinstitutionen eller unionsorganet har vidtagit för att lindra den skada som de registrerade har lidit.

   (c) Graden av ansvar hos unionsinstitutionen eller unionsorganet med beaktande av de tekniska och organisatoriska åtgärder som de genomfört i enlighet med artiklarna 27 och 33.

   (d) Eventuella liknande tidigare överträdelser som begåtts av unionsinstitutionen eller unionsorganet.

   (e) Graden av samarbete med Europeiska datatillsynsmannen för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter.

   (f) De kategorier av personuppgifter som påverkas av överträdelsen.

   (g) Det sätt på vilket överträdelsen kom till Europeiska datatillsynsmannens kännedom, särskilt huruvida och i vilken omfattning unionsinstitutionen eller unionsorganet anmälde överträdelsen.

   (h) När åtgärder enligt artikel 59 tidigare har förordnats mot den berörda unionsinstitutionen eller unionsorganet vad gäller samma sakfråga, efterlevnad av dessa åtgärder.

De förfaranden som leder fram till åläggandet av dessa avgifter bör genomföras inom en tidsram som är rimlig med hänsyn till omständigheterna i fallet och med hänsyn tagen till de åtgärder och förfaranden som avses i artikel 69.

2. Överträdelser av de skyldigheter som åligger unionsinstitutionen eller unionsorganet enligt artiklarna 8, 12, 27, 28, 29, 30, 31, 32, 33, 37, 38, 39, 40, 44, 45 och 46 ska, i enlighet med punkt 1 medföra administrativa sanktionsavgifter på upp till 25 000 euro per överträdelse och upp till ett totalt belopp på 250 000 euro per år.

3. Överträdelser av följande bestämmelser från unionsinstitutionens eller unionsorganets sida ska, i enlighet med punkt 1 medföra administrativa sanktionsavgifter på upp till 50 000 euro per överträdelse och upp till ett totalt belopp på 500 000 euro per år:

   (a) De grundläggande principerna för behandling, inklusive villkoren för samtycke, enligt artiklarna 4, 5, 7 och 10.

   (b) Registrerades rättigheter enligt artiklarna 14–24.

   (c) Överföring av personuppgifter till en mottagare i ett tredjeland eller en internationell organisation enligt artiklarna 47–51.

4. Om en unionsinstitution eller ett unionsorgan, med avseende på en och samma sammankopplade eller fortlöpande uppgiftsbehandlingar, uppsåtligen eller av oaktsamhet överträder flera av bestämmelserna i denna förordning eller samma bestämmelse flera gånger får den administrativa sanktionsavgiftens totala belopp inte överstiga det belopp som fastställs för den allvarligaste överträdelsen.

5. Innan ett beslut fattas enligt denna artikel ska Europeiska datatillsynsmannen ge den unionsinstitution eller det unionsorgan som är föremål för ett förfarande som genomförs av datatillsynsmannen möjlighet att bli hörd om de frågor med avseende på vilka datatillsynsmannen har gjort invändningar. Europeiska datatillsynsmannen ska grunda sina beslut endast på invändningar som de berörda parterna har getts möjlighet att yttra sig om. De klagande ska vara nära knutna till förfarandet.

6. Berörda parters rätt till försvar ska iakttas fullt ut under förfarandet. De ska ha rätt att få tillgång till Europeiska datatillsynsmannens akt, med förbehåll för enskildas eller företags berättigade intresse av skydd av deras personuppgifter eller affärshemligheter.

7. De medel som samlats in genom åläggande av avgifter i denna artikel ska utgöra intäkter i Europeiska unionens allmänna budget.

Artikel 67
Företrädande av registrerade

Den registrerade ska ha rätt att ge ett organ, en organisation eller en sammanslutning utan vinstsyfte, som har inrättats på vederbörligt sätt i enlighet med unionslagstiftning eller lagstiftning i en medlemsstat, vars stadgeenliga mål är av allmänt intresse och som är verksam inom området skydd av registrerades rättigheter och friheter när det gäller skyddet av deras personuppgifter, i uppdrag att lämna in ett klagomål till Europeiska datatillsynsmannen för hans eller hennes räkning, att utöva de rättigheter som avses i artikel 63 för hans eller hennes

räkning samt att för hans eller hennes räkning utöva den rätt till ersättning som avses i artikel 65.

Artikel 68
Klagomål från anställda vid Europeiska unionen

Varje person som är anställd vid en unionsinstitution eller ett unionsorgan får framföra klagomål till Europeiska datatillsynsmannen om en påstådd överträdelse av bestämmelserna i denna förordning, utan att gå den officiella vägen. Ingen ska lida förfång på grund av att ett klagomål framförts till Europeiska datatillsynsmannen angående en sådan överträdelse.

Artikel 69
Sanktioner

Om en tjänsteman eller annan anställd vid Europeiska unionen inte uppfyller de förpliktelser som föreskrivs i denna förordning, avsiktligt eller på grund av försumlighet, ska denne bli föremål för disciplinära eller andra åtgärder enligt de regler och förfaranden som föreskrivs i tjänsteföreskrifterna för tjänstemännen vid Europeiska unionen eller i anställningsvillkoren för övriga anställda vid Europeiska unionen.

KAPITEL IX

GENOMFÖRANDEAKTER

Artikel 70
Kommittéförfarande

1. Kommissionen ska biträdas av den kommitté som inrättats genom artikel 93 i förordning (EU) 2016/679. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

KAPITEL X

SLUTBESTÄMMELSER

Artikel 71
Upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG

Förordning (EG) nr 45/2001[22] och beslut nr 1247/2002/EG[23] ska upphävas med verkan från och med den 25 maj 2018. Hänvisningar till den upphävda förordningen och det upphävda beslutet ska anses som hänvisningar till den här förordningen.

Artikel 72
Övergångsbestämmelser

1. Europaparlamentets och rådets beslut 2014/886/EU[24] och de nuvarande mandaten för Europeiska datatillsynsmannen och den biträdande datatillsynsmannen ska inte påverkas av denna förordning.

2. Den biträdande tillsynsmannen ska betraktas som likställd med en justitiesekreterare vid Europeiska unionens domstol när det gäller fastställande av löner, ersättningar, ålderspension och all annan ersättning utöver lön.

3. Artikel 54.4, 54.5 och 54.7 samt artiklarna 56 och 57 i denna förordning ska tillämpas på den nuvarande biträdande datatillsynsmannen fram till utgången av dennes mandatperiod den 5 december 2019.

4. Den biträdande datatillsynsmannen ska biträda datatillsynsmannen i alla dennes uppgifter och fungera som ersättare när Europeiska datatillsynsmannen är frånvarande eller förhindrad att fullgöra dessa uppgifter fram till utgången av den biträdande tillsynsmannens mandatperiod den 5 december 2019.

Artikel 73
Ikraftträdande och tillämpning

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

2. Den ska tillämpas från och med den 25 maj 2018.

---

22 Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, EGT L 8, 12.1.2001, s. 1.

23 Beslut nr 1247/2002/EG av den 1 juli 2002 om tjänsteföreskrifter och allmänna villkor för utövande av funktionen som europeisk datatillsynsman, EGT L 183, 12.7.2002, s. 1.

24 Europaparlamentets och rådets beslut 2014/886/EU av den 4 december 2014 om utnämning av Europeiska datatillsynsmannen och den biträdande datatillsynsmannen, EUT L 351, 9.12.2014, s. 9.

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

Utfärdad i Bryssel den

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

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1 Förslagets eller initiativets beteckning

1.2 Berörda politikområden i den verksamhetsbaserade förvaltningen och budgeteringen

1.3 Typ av förslag eller initiativ

1.4 Mål

1.5 Motivering till förslaget eller initiativet

1.6 Tid under vilken åtgärden kommer att pågå respektive påverka resursanvändningen

1.7 Planerad metod för genomförandet

2. FÖRVALTNING

2.1 Bestämmelser om uppföljning och rapportering

2.2 Administrations- och kontrollsystem

2.3 Åtgärder för att förebygga bedrägeri och oegentligheter/oriktigheter

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3,1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

3,2. Beräknad inverkan på utgifterna

3.2.1 Sammanfattning av den beräknade inverkan på utgifterna

3.2.2 Beräknad inverkan på driftsanslagen

3.2.3 Beräknad inverkan på anslag av administrativ natur

3.2.4 Förenlighet med den gällande fleråriga budgetramen

3.2.5 Bidrag från tredje part

3.3 Beräknad inverkan på inkomsterna

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets beteckning

Förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ, kontor och byråer, om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut 1247/2002/EG

1.2. Berörda politikområden i den verksamhetsbaserade förvaltningen och budgeteringen[25]

Rättsliga frågor – skydd av personuppgifter

1.3. Typ av förslag eller initiativ

☐ **Ny åtgärd**

☐ **Ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd**[26]

– **Befintlig åtgärd vars genomförande förlängs i tiden**

☐ **Tidigare åtgärd som omformas till eller ersätts av en ny**

1.4. Mål

1.4.1. Fleråriga strategiska mål för kommissionen som förslaget eller initiativet är avsett att bidra till

Efter ikraftträdandet av Lissabonfördraget, och särskilt efter införandet av en ny rättslig grund (artikel 16 i EUF-fördraget), har det blivit möjligt att inrätta en övergripande ram för skydd av personuppgifter som täcker alla områden.

Den 27 april 2016 antog unionen 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.

Samma dag antog unionen 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,

---

25 Verksamhetsbaserad förvaltning och verksamhetsbaserad budgetering benämns ibland med de interna förkortningarna ABM respektive ABB.

26 I den mening som avses i artikel 54.2 a och b i budgetförordningen.

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.

Detta förslag syftar till att fullborda inrättandet av en övergripande ram för uppgiftsskydd inom unionen, genom att anpassa de regler om skydd av personuppgifter som är tillämpliga på unionens institutioner och organ till bestämmelserna om skydd av personuppgifter i förordning (EU) 2016/679. Av skäl som rör enhetlighet och samstämmighet bör unionens institutioner och organ tillämpa en uppsättning regler om skydd av personuppgifter som liknar de regler som tillämpas inom den offentliga sektorn i medlemsstaterna.

1.4.2. Specifika mål eller verksamheter inom den verksamhetsbaserade förvaltningen och budgeteringen som berörs

Specifikt mål nr 1:

Säkerställa en enhetlig tillämpning av regler om uppgiftsskydd i hela unionen.

Specifikt mål nr 2:

Rationalisera den befintliga styrningsmodellen för uppgiftsskydd i unionens institutioner och organ.

Specifikt mål nr 3:

Säkerställa en bättre efterlevnad och ett effektivare upprätthållande av regler om uppgiftsskydd i unionens institutioner och organ.

1.4.3. Verkan eller resultat som förväntas

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

När det gäller unionens institutioner och organ i egenskap av personuppgiftsansvariga, bör de gynnas av övergången från de nuvarande administrativa förfarandena (förhandskontroll) i samband med uppgiftsskydd i riktning mot en effektiv efterlevnad och en striktare tillämpning av de materiella reglerna om uppgiftsskydd och de nya principer och begrepp med avseende på uppgiftsskydd som infördes genom förordning (EU) 2016/679 (system med efterhandskontroll), som kommer att vara tillämplig i hela unionen.

Enskilda vilkas uppgifter behandlas av unionens institutioner och organ kommer att få bättre kontroll över sina personuppgifter och kunna lita på den digitala miljön. Ansvarsskyldigheten för unionens institutioner och organ kommer också att stärkas.

Europeiska datatillsynsmannen kommer att kunna fokusera mer på sin roll som övervakare. Fördelningen av uppgiften att ge råd till kommissionen mellan Europeiska dataskyddsstyrelsen, som inrättades genom förordning (EU) 2016/679 och Europeiska datatillsynsmannen kommer att klarläggas så att överlappningar kan undvikas.

1.4.4. Indikatorer för bedömning av resultat eller verkan

Ange vilka indikatorer som ska användas för att följa upp hur förslaget eller initiativet genomförs.

Indikatorerna ska omfatta följande:

Antal yttranden från Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen.

Beskrivning (uppdelad) av dataskyddsombudens verksamhet.

Användning av konsekvensbedömningar rörande uppgiftsskydd.

Antal klagomål som lämnats in av registrerade.

Sanktionsavgifter som utfärdas till personuppgiftsansvariga för dataskyddsincidenter.

1.5. Motivering till förslaget eller initiativet

1.5.1. Behov som ska tillgodoses på kort eller lång sikt

I förordning (EU) 2016/679 (artikel 2.3, artikel 98, skäl 17) efterlyste unionens medlagstiftare en anpassning av förordning (EG) nr 45/2001 till principerna och bestämmelserna i förordning (EU) 2016/679 för att tillhandahålla en stark och sammanhängande ram för dataskyddet inom unionen och göra det möjligt att börja tillämpa båda instrumenten samtidigt, dvs. den 25 maj 2018.

1.5.2. Mervärdet av en åtgärd på unionsnivå

De uppgiftsskyddsregler som ska tillämpas på unionens institutioner och organ kan därför endast införas genom en unionsrättsakt.

1.5.3. Huvudsakliga erfarenheter från liknande försök eller åtgärder

Detta förslag bygger vidare på erfarenheterna från förordning (EG) nr 45/2001 och utvärderingen av dess tillämpning (som utfördes av en extern uppdragstagare mellan september 2014 och juni 2015)[27].

1.5.4. Förenlighet med andra finansieringsformer och eventuella synergieffekter

Detta förslag bygger på förordning (EU) 2016/679 och slutför upprättandet av en stark, enhetlig och modern ram för uppgiftsskyddet inom unionen – teknikneutral och framtidssäkrad.

[27] JUST/2013/FRAC/FW/0157/A4 in the context of the multiple framework contract JUST/2011/EVAL/01 (RS 2013/05) - Evaluation Study on Regulation (EC) 45/2001, av Ernst and Young

1.6. Tid under vilken åtgärden kommer att pågå respektive påverka resursanvändningen

☐ Förslag eller initiativ som pågår under **begränsad tid**

– ☐ Förslaget eller initiativet ska gälla från [den DD/MM]ÅÅÅÅ till [den DD/MM]ÅÅÅÅ.

– ☐ Det påverkar resursanvändningen från ÅÅÅÅ till ÅÅÅÅ.

- Förslag eller initiativ som **pågår under en obegränsad tid**
- Efter en inledande period från [2017] till den 25 maj 2018 beräknas genomförandetakten nå en stabil nivå.

1.7. Planerad metod för genomförandet[28]

- **Direkt förvaltning** som sköts av kommissionen

– ☐ inom dess avdelningar, vilket också inbegriper personalen vid unionens delegationer

– ☐ via genomförandeorgan

☐ **Delad förvaltning** med medlemsstaterna

☐ **Indirekt förvaltning** genom att uppgifter som ingår i budgetgenomförandet delegeras till

– ☐ tredjeländer eller organ som de har utsett

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

– ☐ EIB och Europeiska investeringsfonden

– ☐ organ som avses i artiklarna 208 och 209 i budgetförordningen

– ☐ offentligrättsliga organ

– ☐ privaträttsliga organ som anförtrotts uppgifter som faller inom offentlig förvaltning och som lämnat tillräckliga ekonomiska garantier

– ☐ organ som omfattas av privaträtten i en medlemsstat, som anförtrotts genomförandet av ett offentlig-privat partnerskap och som lämnat tillräckliga ekonomiska garantier

– ☐ personer som anförtrotts ansvaret för genomförandet av särskilda åtgärder inom Gusp som följer av avdelning V i fördraget om Europeiska unionen och som anges i den grundläggande rättsakten

---

[28] Närmare förklaringar av de olika metoderna för genomförande med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

– *Vid fler än en metod, ange kompletterande uppgifter under ”Anmärkningar”.*

Anmärkningar

Detta förslag är begränsat till och påverkar alla unionens institutioner och organ.

2. FÖRVALTNING

2.1. Bestämmelser om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder:

Detta förslag är begränsat till unionsinstitutioners och unionsorgans tillämpning av regler om uppgiftsskydd. Tillsynen över och upprättshållandet av dessa regler är en uppgift som utförs av Europeiska datatillsynsmannen. Övervakning och rapportering tillhandahålls därför av Europeiska datatillsynsmannen. Enligt artikel 60 i detta förslag är Europeiska datatillsynsmannen skyldig att lämna en årlig rapport om verksamhet som omfattas av Europeiska datatillsynsmannens behörighetsområde till Europaparlamentet, rådet och kommissionen och samtidigt offentliggöra rapporten.

2.2. Administrations- och kontrollsystem

2.2.1. Risker som identifierats

En utvärdering av tillämpningen av förordning (EG) nr 45/2001 har genomförts av en extern uppdragstagare, mellan september 2014 och juni 2015. Utvärderingen undersöker också verkan av att introducera grundläggande begrepp och principer i förordning (EU) 2016/679 i unionens institutioner och organ.

Den nya uppgiftsskyddsmodellen kommer att fokusera på en effektiv efterlevnad av reglerna om uppgiftsskydd och en effektiv övervakning och ett effektivt upprätthållande av dessa regler. Det kommer att kräva en förändring av uppgiftsskyddskulturen inom unionens institutioner och organ, och medföra en övergång från den administrativa modellen med förhandskontroll till en mer effektiv modell för efterhandskontroll.

2.2.2. Uppgifter om det interna kontrollsystemet:

Befintliga kontrollmetoder som tillämpas av unionens institutioner och organ.

2.2.3. Beräknade kostnader för och fördelar med kontroller – bedömning av förväntad risk för fel

Befintliga kontrollmetoder som tillämpas av unionens institutioner och organ.

2.3. Åtgärder för att förebygga bedrägeri och oegentligheter/oriktigheter

Beskriv förebyggande åtgärder (befintliga eller planerade)

Befintliga metoder för bedrägeribekämpning som tillämpas av unionens institutioner och organ.

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

- Befintliga budgetrubriker (även kallade ”budgetposter”)

Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd

Rubrik i den fleråriga budgetramen	Budgetrubrik	Typ avanslag	Bidrag			
	Nummer [Beteckning……...……]	Diff./Icke-diff.[29]	från Efta-länder[30]	från kandidat-länder[31]	från tredje-länder	enligt artikel 21.2 b i budget-förordningen
	[XX.YY.YY.YY]	Diff./Icke-diff.	JA/NEJ	JA/NEJ	JA/NEJ	JA/NEJ

- Nya budgetrubriker som föreslås

Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd

Rubrik i den fleråriga budgetramen	Budgetrubrik	Typ avanslag	Bidrag			
	Nummer [Beteckning……]	Diff./Icke-diff.	från Efta-länder	från kandidat-länder	från tredje-länder	enligt artikel 21.2 b i budget-förordningen
	[XX.YY.YY.YY]		JA/NEJ	JA/NEJ	JA/NEJ	JA/NEJ

[29] Differentierade respektive icke-differentierade anslag.
[30] Efta: Europeiska frihandelssammanslutningen.
[31] Kandidatländer och i förekommande fall potentiella kandidatländer i västra Balkan.

3.2. Beräknad inverkan på utgifterna

Inverkan på utgifterna av detta förslag är begränsat till utgifter för unionens institutioner och organ. Utvärderingen av kostnaderna i samband med detta förslag visar dock att det inte ger upphov till betydande ytterligare utgifter för unionens institutioner och organ.

När det gäller personuppgiftsansvariga inom unionens institutioner och organ visar utvärderingen av förordning (EG) nr 45/2001 att deras uppgiftsskyddsverksamhet motsvarar cirka 70 heltidsekvivalenter (heltidsekvivalenter), dvs. omkring 9.3 miljoner euro per år. Omkring 20 % av deras uppgiftsskyddsverksamhet utgörs idag av arbete med anmälningar av behandling av uppgifter. Denna verksamhet avskaffas i denna förordning, vilket motsvarar årliga besparingar på 1,922 miljoner euro för personuppgiftsansvariga inom unionens institutioner och organ. Dessa besparingar förväntas neutraliseras av ökade investeringar från de personuppgiftsansvarigas sida i samband med genomförandet av nya principer och begrepp som införs genom den här förordningen.

Närmare bestämt påpekades i den undersökning som genomfördes inom ramen för utvärderingen att

a) principen om uppgiftsminimering skulle ge en mycket liten eller obefintlig inverkan på unionens institutioner och organ,

b) öppenhetsprincipen inte skulle få några betydande konsekvenser för unionens institutioner och organ,

c) den utökade informationsplikten skulle öka arbetsbördan för personuppgiftsansvariga och dataskyddsombud,

d) rätten att bli glömd inte skulle få några betydande konsekvenser för unionens institutioner och organ,

e) principen om dataportabilitet skulle leda till en mycket liten eller obefintlig inverkan på unionens institutioner och organ,

f) konsekvensbedömningar avseende dataskydd skulle få en viss betydelse för de personuppgiftsansvarigas och dataskyddsombudens arbetsbelastning, eftersom vissa unionens institutioner och organ som redan gör konsekvensbedömningar avseende dataskydd och de fall då sådana konsekvensbedömningar skulle behöva göras är begränsade,

g) anmälningar av personuppgiftsincidenter skulle öka arbetsbördan för personuppgiftsansvariga, men sådana incidenter är inte vanligt förekommande,

h) inbyggt dataskydd och dataskydd som standard redan används inom flera unionsinstitutioner och unionsorgan.

I den konsekvensanalys som genomfördes inför antagandet av förslaget till reformpaket på området för uppgiftsskydd drogs slutsatsen att varken offentliga myndigheter eller personuppgiftsansvariga skulle drabbas av någon ytterligare administrativ börda som en följd av införandet av principen om inbyggt dataskydd[32].

Vad gäller dataskyddsombuden beräknades i utvärderingen kostnaderna för det nuvarande nätverket av dataskyddsombud och uppgiftsskyddssamordnare inom unionens institutioner och organ till 82,9 heltidsekvivalenter eller 10,9 miljoner euro per år. De använder 26 % av sin uppgiftsskyddsrelaterade tid på verksamhet som avskaffas genom denna förordning, det vill säga arbetet med att utarbeta anmälningar (i stället för personuppgiftsansvariga), bedöma mottagna anmälningar, hantera uppgifter i registret och göra förhandskontroller. Detta leder till ytterligare besparingar på 2,834 miljoner euro per år för unionens institutioner och organ. Denna förordning ger dessutom utrymme för potentiella ytterligare besparingar genom att göra det möjligt för unionens institutioner och organ att lägga ut verksamhet som utförs av dataskyddsombud, i stället för att anställa egen personal.

Besparingarna inom dataskyddsombudens verksamhet ställs mot att de i större omfattning kommer att beröras av utökad informationsplikt, konsekvensbedömningar avseende uppgiftsskydd (i begränsad omfattning när så krävs) och föregående samråd med Europeiska datatillsynsmannen (som kommer att vara långt mer begränsat i omfattning än den nuvarande skyldigheten att göra förhandskontroller).

När det gäller Europeiska datatillsynsmannen är dess årliga budget är tämligen stabil sedan 2011 och ligger på omkring 8 miljoner euro. För närvarande har dess tillsyns- och genomförandeenhet respektive dess enhet för policyfrågor och samråd jämförbara personalsiffror, som har legat stabilt sedan 2008. Denna förordnings ökade fokusering på Europeiska datatillsynsmannens tillsynsfunktion kommer att balanseras av en mer riktad rådgivande roll och avskaffandet av överlappningar i förhållande till Europeiska dataskyddsstyrelsen. En omfördelning av Europeiska datatillsynsmannens personal kan därför uppnås internt.

Detta förslag inbegriper en möjlighet för Europeiska datatillsynsmannen att ålägga unionens institutioner och organ administrativa sanktionsavgifter. Varje institution eller organ kan åläggas sanktionsavgifter på upp till högst 250 000 euro per år (25 000 euro per överträdelse), eller 500 000 euro per år (50 000 euro per överträdelse) för de allvarligaste överträdelserna enligt denna förordning. Sådana avgifter förväntas tillämpas endast i de allvarligaste fallen, och först efter det att unionsinstitutionen eller unionsorganet i fråga underlåtit att efterleva andra korrigerande befogenheter som utövats av Europeiska datatillsynsmannen. Det kan därför förväntas att de ekonomiska effekterna av sådana sanktionsavgifter blir begränsad.

---

[32] Arbetsdokument från kommissionens avdelningar, konsekvensbedömning, SEC (2012) 72 final, s. 110.

3.2.1. Sammanfattning av den beräknade inverkan på utgifterna

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	Nummer	[Beteckning……...…… ….]

GD: <…….>			År **N**[33]	År**N+1**	År**N+2**	År**N+3**	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)			**TOTALT**
• Driftsanslag										
Budgetrubrik (nr)	Åtaganden	1)								
	Betalningar	2)								
Budgetrubrik (nr)	Åtaganden	1 a)								
	Betalningar	2 a)								
Anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program[34]										
Budgetrubrik (nr)		3)								
TOTALA anslag för GD <…….>	Åtaganden	=1+1a +3								
	Betalningar	=2+2a +3								

33 Med år n avses det år då förslaget eller initiativet ska börja genomföras.

34 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.

• TOTALA driftsanslag	Åtaganden	4)								
	Betalningar	5)								
• TOTALA anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program		6)								
TOTALA anslag för RUBRIK 5 <….> i den fleråriga budgetramen	Åtaganden	=4+ 6								
	Betalningar	=5+ 6								

Följande ska anges om flera rubriker i budgetramen påverkas av förslaget eller initiativet:

• TOTALA driftsanslag	Åtaganden	4)								
	Betalningar	5)								
• TOTALA anslag av administrativ natur som finansieras genom ramanslagen för vissa operativa program		6)								
TOTALA anslag för RUBRIKERNA 1–4 i den fleråriga budgetramen (referensbelopp)	Åtaganden	=4+ 6								
	Betalningar	=5+ 6								

Rubrik i den fleråriga budgetramen	**5**	”Administrativa utgifter”

Miljoner euro (avrundat till tre decimaler)

	År **N**	År **N+1**	År **N+2**	År **N+3**	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)	**TOTALT**
GD: <…….>						
• Personalresurser						
• Övriga administrativa utgifter						

GD <….> TOTALT	Anslag								

TOTALA anslag för RUBRIK 5 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)								

Miljoner euro (avrundat till tre decimaler)

		År**N**[35]	År**N+1**	År**N+2**	År**N+3**	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)			**TOTALT**
TOTALA anslag för RUBRIKERNA 1–5 i den fleråriga budgetramen	Åtaganden								
	Betalningar								

[35] Med år n avses det år då förslaget eller initiativet ska börja genomföras.

3.2.2. Beräknad inverkan på driftsanslagen

- Förslaget/initiativet kräver inte att driftsanslag tas i anspråk

☐ Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler)

Mål- och resultatbeteckning			ÅrN		ÅrN+1		ÅrN+2		ÅrN+3		För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)						**TOTALT**	
	RESULTAT																	
⇩	Typ[36]	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 1[37]…																		
- Resultat																		
- Resultat																		
- Resultat																		
Delsumma för specifikt mål nr 1																		
SPECIFIKT MÅL nr 2…																		
- Resultat																		
Delsumma för specifikt mål nr 2																		
TOTALA KOSTNADER																		

[36] Resultaten är de produkter och tjänster som levererats (t.ex.: antal studentutbyten som har finansierats eller antal kilometer väg som har byggts).

[37] Mål som redovisats under punkt 1.4.2: ”Specifikt/specifika mål…”.

3.2.3. Beräknad inverkan på anslag av administrativ natur

3.2.3.1. Sammanfattning

- 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:

Miljoner euro (avrundat till tre decimaler)

	År N [38]	År N+1	År N+2	År N+3	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)			**TOTALT**
RUBRIK 5 i den fleråriga budgetramen								
Personalresurser								
Övriga administrativa utgifter								
Delsumma RUBRIK 5 i den fleråriga budgetramen								
Belopp utanför RUBRIK 5 [39] i den fleråriga budgetramen								
Personalresurser								
Andra utgifter av administrativ natur								
Delsumma för belopp utanför RUBRIK 5 i den fleråriga budgetramen								
TOTALT								

Personalbehov och andra administrativa kostnader ska täckas genom anslag inom generaldirektoratet som redan har avdelats för att förvalta åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad 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.

[38] Med år n avses det år då förslaget eller initiativet ska börja genomföras.

[39] 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.

3.2.3.2. Beräknat personalbehov

- Förslaget/initiativet kräver inte att personalresurser tas i anspråk

☐ Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

Beräkningarna ska anges i heltidsekvivalenter

	År N	År N +1	År N+2	År N+ 3	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)		
• Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)							
XX 01 01 01 (vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna)							
XX 01 01 02 (vid delegationer)							
XX 01 05 01 (indirekta forskningsåtgärder)							
10 01 05 01 (direkta forskningsåtgärder)							
• Extern personal (i heltidsekvivalenter)[40]							
XX 01 02 01 (kontraktsanställda, nationella experter och vikarier finansierade genom ramanslaget)							
XX 01 02 02 (kontraktsanställda, lokalanställda, nationella experter, vikarier och unga experter som tjänstgör vid delegationerna)							
XX 01 04 **yy** [41] - vid huvudkontoret							
XX 01 04 **yy** [41] - vid delegationer							
XX 01 05 02 (kontraktsanställda, nationella experter och vikarier som arbetar med indirekta forskningsåtgärder)							
10 01 05 02 (kontraktsanställda, nationella experter och vikarier som arbetar med direkta forskningsåtgärder)							
Annan budgetrubrik (ange vilken)							
TOTALT							

XX motsvarar det politikområde eller den avdelning i budgeten som avses.

Personalbehoven ska täckas med personal inom generaldirektoratet som redan har avdelats för att förvalta åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad

40 [Denna fotnot förklarar vissa initialförkortningar som inte används i den svenska versionen].

41 Särskilt tak för finansiering av extern personal genom driftsanslag (tidigare s.k. BA-poster).

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.

Beskrivning av arbetsuppgifter:

Tjänstemän och tillfälligt anställda	
Extern personal	

3.2.4. Förenlighet med den gällande fleråriga budgetramen

- Förslaget/initiativet är förenligt med den gällande fleråriga budgetramen

☐ Förslaget/initiativet kräver omfördelningar under den berörda rubriken i den fleråriga budgetramen

Förklara i förekommande fall vilka ändringar i planeringen som krävs, och ange berörda budgetrubriker och belopp.

☐ Förslaget/initiativet förutsätter att flexibilitetsmekanismen utnyttjas eller att den fleråriga budgetramen revideras.

Beskriv behovet av sådana åtgärder, och ange berörda rubriker i budgetramen, budgetrubriker i den årliga budgeten samt belopp.

3.2.5. Bidrag från tredje part

- Det ingår inga bidrag från tredje part i det aktuella förslaget eller initiativet

Förslaget eller initiativet kommer att medfinansieras enligt följande:

Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler)

	År **N**	År **N+1**	År **N+2**	År **N+3**	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)			Totalt
Ange vilken extern organisation eller annan källa som bidrar till finansieringen								
TOTALA anslag som tillförs genom medfinansiering								

3.3. Beräknad inverkan på inkomsterna

- Förslaget/initiativet påverkar inte budgetens inkomstsida.

☐ Förslaget/initiativet påverkar inkomsterna på följande sätt:

– ☐ Påverkan på egna medel

– ☐ Påverkan på ”diverse inkomster”

Miljoner euro (avrundat till tre decimaler)

Budgetrubrik i den årliga budgetens inkomstdel:	Belopp som förts in för det innevarande budgetåret	Förslagets eller initiativets inverkan på inkomsterna[42]						
		År**N**	År**N+1**	År**N+2**	År**N+3**	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)		
Artikel …….								

Ange vilka budgetrubriker i utgiftsdelen som berörs i de fall där inkomster i diversekategorin kommer att avsättas för särskilda ändamål.

Ange med vilken metod inverkan på inkomsterna har beräknats.

[42] När det gäller traditionella egna medel (tullar och sockeravgifter) ska nettobeloppen anges, dvs. bruttobeloppen minus 25 % avdrag för uppbördskostnader.