EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2018/1725

av den 23 oktober 2018

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

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

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

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 ([1]),

i enlighet med det ordinarie lagstiftningsförfarandet ([2]), och

av följande skäl:

(1) Skyddet för fysiska personer med avseende på behandling av personuppgifter är en grundläggande rättighet. I artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) och artikel 16.1 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) föreskrivs att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Denna rättighet garanteras även i artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

(2) Europaparlamentets och rådets förordning (EG) nr 45/2001 ([3]) föreskriver verkställbara rättigheter för fysiska personer, anger de skyldigheter avseende 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 unionsorgan. 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 ([4]) och Europaparlamentets och rådets direktiv (EU) 2016/680 ([5]) antogs den 27 april 2016. Medan förordningen fastställer allmänna regler som syftar till att skydda fysiska personer med avseende på 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 med avseende på behandlingen av personuppgifter och att säkerställa det fria flödet av personuppgifter inom unionen på området för straffrättsligt samarbete och polissamarbete.

(4) I förordning (EU) 2016/679 föreskrivs anpassningar av förordning (EG) nr 45/2001 för att säkerställa en stark och sammanhängande ram för dataskyddet inom unionen och för att göra det möjligt att tillämpa den parallellt med 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 unionens institutioner, organ och byråer till de regler om skydd för personuppgifter som har antagits för den offentliga sektorn i medlemsstaterna. När en bestämmelse i denna förordning följer samma principer som en

([1]) EUT C 288, 31.8.2017, s. 107.
([2]) Europaparlamentets ståndpunkt av den 13 september 2018 (ännu ej offentliggjord i EUT) och rådets beslut av den 11 oktober 2018.
([3]) 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).
([4]) 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).
([5]) 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).

bestämmelse i förordning (EU) 2016/679 bör dessa båda bestämmelser, enligt rättspraxis från Europeiska unionens domstol (nedan kallad *domstolen*), 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 unionsinstitutioner och unionsorgan bör skyddas, oavsett i vilket sammanhang behandlingen sker, till exempel därför att dessa personer 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 rörande 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.

(8) Denna förordning bör vara tillämplig på behandling av personuppgifter som utförs av alla unionens institutioner, organ och byråer. Den bör 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. Akter eller grupper av akter samt omslag till dessa, som inte är ordnade enligt särskilda kriterier, bör inte omfattas av denna förordning.

(9) 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 detta områdes särart kan komma att bli nödvändigt att anta särskilda regler om skydd av personuppgifter och om det fria flödet av personuppgifter på området för straffrättsligt samarbete och polissamarbete med stöd av artikel 16 i EUF-fördraget. Ett särskilt kapitel med allmänna regler i denna förordning bör därför vara tillämpligt på behandlingen av operativa personuppgifter, t.ex. sådana personuppgifter som unionens organ eller byråer behandlar i samband med brottsutredningar när de utövar verksamhet på området för straffrättsligt samarbete och polissamarbete.

(10) I direktiv (EU) 2016/680 fastställs 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 säkerställa en enhetlig skyddsnivå för skyddet av fysiska personer genom rättsligt verkställbara rättigheter i hela unionen och undvika avvikelser som hämmar utbytet av personuppgifter mellan unionens organ eller byråer som utövar verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget och behöriga myndigheter, bör reglerna om skyddet av och den fria rörligheten för operativa personuppgifter som behandlas av sådana unionsorgan eller unionsbyråer vara förenliga med direktiv (EU) 2016/680.

(11) De allmänna reglerna i kapitlet om behandling av operativa personuppgifter i denna förordning bör inte påverka tillämpningen av de särskilda regler som är tillämpliga på behandlingen av operativa personuppgifter som utförs av unionens organ och byråer när dessa utövar verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget. Sådana särskilda regler bör betraktas som *lex specialis* till bestämmelserna i kapitlet i denna förordning om behandling av operativa personuppgifter (*lex specialis derogat generali*, dvs. en speciallag äger företräde framför en allmän lag). För att minska den rättsliga fragmenteringen bör de särskilda regler om skydd för personuppgifter som är tillämpliga på behandlingen av operativa personuppgifter som utförs av unionens organ eller byråer när dessa utövar verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget vara förenliga med de principer som ligger till grund för kapitlet om behandling av operativa personuppgifter i denna förordning och med de bestämmelser i denna förordning som rör oberoende tillsyn, rättsmedel, ansvar och sanktioner.

(12) Kapitlet om behandling av operativa personuppgifter i denna förordning bör tillämpas på unionens organ och byråer när dessa utövar verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget, oavsett om de utövar denna verksamhet som sin huvuduppgift eller tilläggsuppgift i syfte att förebygga, förhindra, avslöja, utreda eller lagföra brott. Kapitlet bör emellertid inte tillämpas på Europol eller på Europeiska åklagarmyndigheten förrän rättsakterna om inrättande av Europol och Europeiska åklagarmyndigheten har ändrats så att kapitlet om behandling av operativa personuppgifter i denna förordning, i dess anpassade lydelse, är tillämpligt på dem.

(13) Kommissionen bör se över denna förordning, särskilt kapitlet om behandling av operativa personuppgifter i denna förordning. Kommissionen bör också se över andra rättsakter som har antagits på grundval av fördragen och som reglerar den behandling av operativa personuppgifter som utförs av unionens organ eller byråer när de utövar

verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget. Efter en sådan översyn bör kommissionen ha möjlighet att lägga fram lämpliga lagstiftningsförslag, bland annat nödvändiga anpassningar av kapitlet om behandling av operativa personuppgifter i denna förordning för att säkerställa ett enhetligt och konsekvent skydd för fysiska personer med avseende på behandlingen av personuppgifter och i syfte att tillämpa det på Europol och Europeiska åklagarmyndigheten. Anpassningarna bör bland annat ta hänsyn till bestämmelserna om oberoende tillsyn, rättsmedel, ansvar och sanktioner.

(14) Behandlingen av administrativa personuppgifter, t.ex. personaluppgifter, som utförs av unionens organ eller byråer som utövar verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget bör omfattas av denna förordning.

(15) Denna förordning bör vara tillämplig på behandling av personuppgifter som utförs av unionens institutioner, organ eller byråer som utövar verksamhet som omfattas av avdelning V kapitel 2 i fördraget om Europeiska unionen (EU-fördraget). Denna förordning bör inte tillämpas på sådan behandling av personuppgifter som utförs av de uppdrag som avses i artiklarna 42.1, 43 och 44 i EU-fördraget och som genomför den gemensamma säkerhets- och försvarspolitiken. Vid behov bör relevanta förslag läggas fram för att ytterligare reglera behandlingen av personuppgifter inom den gemensamma säkerhets- och försvarspolitiken.

(16) 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, dvs. 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.

(17) 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.

(18) 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.

(19) Samtycke bör lämnas genom en entydig bekräftande handling som innebär ett frivilligt, specifikt, informerat och otvetydigt medgivande från den registrerades sida om att denna godkänner behandling av personuppgifter rörande honom eller henne, som t.ex. genom en skriftlig, inklusive elektronisk, eller muntlig förklaring. Detta kan t.ex. ske genom 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 sker för flera olika ändamål, bör samtycke ges för samtliga ändamål. Om den registrerade ska lämna sitt samtycke efter en elektronisk begäran, måste denna begäran vara tydlig och koncis och får inte onödigtvis störa användningen av den tjänst som den avser. Samtidigt bör den registrerade ha rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandling som grundar sig på samtycket innan detta återkallades. För att säkerställa att samtycket lämnas frivilligt bör det inte utgöra giltig rättslig grund för behandling av personuppgifter i särskilda fall där det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, och det därför är osannolikt att samtycket har lämnats frivilligt när det gäller alla

förhållanden som denna särskilda situation omfattar. Det är ofta inte möjligt att fullt ut identifiera syftet med en behandling av personuppgifter för vetenskapliga forskningsändamål i samband med insamlingen av uppgifter. Därför bör registrerade kunna ge sitt samtycke till vissa områden för vetenskaplig forskning, när vedertagna etiska standarder för vetenskaplig forskning iakttas. Registrerade bör ha möjlighet att lämna sitt samtycke endast till vissa forskningsområden eller delar av forskningsprojekt i den utsträckning det avsedda syftet medger detta.

(20) Varje behandling av personuppgifter måste vara laglig och rättvis. Det bör vara klart och tydligt för fysiska personer hur personuppgifter som rör dem samlas in, 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 säkerställs 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 säkerställa att felaktiga uppgifter rättas eller raderas. Personuppgifter bör behandlas på ett sätt som säkerställer lämplig säkerhet och konfidentialitet för personuppgifterna samt förhindrar obehörigt tillträde till, eller obehörig användning av, personuppgifter och den utrustning som används för behandlingen samt för att förhindra obehörigt utlämnande i samband med överföring.

(21) I enlighet med principen om ansvarsskyldighet bör unionsinstitutioner och unionsorgan, i samband med att de överför personuppgifter inom samma unionsinstitution eller unionsorgan, och mottagaren inte är en del av den personuppgiftsansvarige, eller till andra av unionsinstitutioner eller unionsorgan, kontrollera om sådana personuppgifter är nödvändiga för det legitima utförandet av uppgifter som omfattas av mottagarens behörighet. 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 det senare kan kontrolleras att överföringen av uppgifterna var nödvändig.

(22) 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 sin myndighetsutövning, nödvändigheten av att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller någon annan legitim grund i denna förordning, inbegripet samtycke från den registrerade, en nödvändighet som hänför sig till fullgörandet av 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 uppgifter 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 äga rum endast 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.

(23) Den unionsrätt som avses i denna förordning bör vara tydlig och precis, och dess tillämpning bör vara förutsägbar för personer som omfattas av den, i enlighet med kraven i stadgan och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

(24) De interna regler som det hänvisas till i denna förordning bör vara tydliga och precisa akter med allmän giltighet som är avsedda att ha rättsverkan gentemot registrerade. De bör antas på unionsinstitutionernas och unionsorganens högsta administrativa nivå inom ramen för deras behörighet när det gäller frågor rörande deras funktion. De bör offentliggöras i *Europeiska unionens officiella tidning*. Tillämpningen av dessa regler bör vara förutsägbar för personer som omfattas av dem, i enlighet med kraven i stadgan och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Interna regler kan vara utformade som beslut, särskilt om de har antagits av unionsinstitutioner.

(25) Behandling av personuppgifter för andra ändamål än de för vilka de ursprungligen samlades in bör vara tillåten endast 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 utföra 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 samlades in bör den personuppgiftsansvarige, efter att ha uppfyllt alla krav vad beträffar den ursprungliga behandlingens laglighet, bland annat beakta alla kopplingar mellan dessa ändamål och ändamålen med den avsedda ytterligare behandlingen, det sammanhang inom vilket personuppgifterna samlats in, särskilt de registrerades rimliga förväntningar till följd av förhållandet till den personuppgiftsansvarige när det gäller den fortsatta behandlingen, personuppgifternas art, konsekvenserna för de registrerade av den planerade fortsatta behandlingen samt förekomsten av lämpliga skyddsåtgärder för både den ursprungliga och den planerade ytterligare behandlingen.

(26) När behandling sker efter samtycke från registrerade, bör personuppgiftsansvariga kunna visa att de registrerade har lämnat sitt samtycke till behandlingen. I synnerhet vid skriftliga förklaringar som rör andra frågor bör det finnas skyddsåtgärder som säkerställer att de registrerade är medvetna om att samtycke ges och om hur långt samtycket sträcker sig. I enlighet med rådets direktiv 93/13/EEG ([1]) bör en förklaring om samtycke som den personuppgiftsansvarige i förväg formulerat tillhandahållas i en begriplig och lättillgänglig 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.

(27) 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 på insamlingen av personuppgifter med avseende på barn i samband med tjänster som erbjuds direkt till barn på webbplatser som tillhör unionsinstitutioner och unionsorgan, såsom interpersonella kommunikationstjänster eller internetförsäljning av biljetter, och behandlingen av personuppgifter grundar sig på samtycke.

(28) När mottagare som är etablerade i unionen och som inte är unionsinstitutioner och unionsorgan vill få personuppgifter överförda till sig av unionsinstitutioner och unionsorgan, bör dessa mottagare visa att överföringen är nödvändig för att de ska kunna utföra en uppgift som antingen är av allmänt intresse eller är ett led i deras myndighetsutövning. Alternativt bör dessa mottagare visa att överföringen är nödvändig för ett specifikt ändamål av allmänt intresse, och den personuppgiftsansvarige bör fastställa om det finns skäl att anta att den registrerades legitima intressen skulle kunna skadas. Om så är fallet bör den personuppgiftsansvarige på ett påvisbart sätt väga de olika konkurrerande intressena mot varandra för att bedöma om den begärda överföringen av personuppgifter är

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

proportionell. Det specifika ändamålet av allmänt intresse kan vara kopplat till öppenheten inom unionsinstitutioner och unionsorgan. Unionens institutioner och organ bör dessutom visa att det föreligger en sådan nödvändighet när de själva initierar en överföring, i överensstämmelse med principen om öppenhet och god förvaltningssed. De krav som fastställs i denna förordning för överföring till mottagare som är etablerade i unionen och som inte är unionsinstitutioner och unionsorgan bör uppfattas som kompletterande till villkoren för laglig behandling.

(29) 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. Sådana personuppgifter bör inte behandlas om inte villkoren i denna förordning är uppfyllda. 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 definieras som biometriska uppgifter endast 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.

(30) Särskilda kategorier av personuppgifter som förtjänar ett mer omfattande skydd bör behandlas endast i hälsorelaterade syften om detta krävs för att uppnå dessa syften och gagnar fysiska personer och samhället i stort, särskilt inom ramen för förvaltningen av tjänster för hälso- och sjukvård eller social omsorg och deras system. Denna förordning bör därför innehålla harmoniserade villkor för behandling av särskilda kategorier av personuppgifter som rör hälsa, vad gäller särskilda behov, i synnerhet när behandlingen av uppgifterna utförs för vissa hälsorelaterade syften av personer som enligt lag är underkastade tystnadsplikt. Unionsrätten bör föreskriva särskilda och lämpliga åtgärder som skyddar fysiska personers grundläggande rättigheter och personuppgifter.

(31) På folkhälsoområdet kan det bli nödvändigt att med hänsyn till ett allmänt intresse behandla särskilda kategorier av personuppgifter utan att den registrerades samtycke inhämtas. Sådan behandling bör förutsätta lämpliga och särskilda åtgärder för att skydda fysiska personers rättigheter och friheter. I detta sammanhang bör folkhälsa tolkas enligt definitionen i Europaparlamentets och rådets förordning (EG) nr 1338/2008 ([1]), nämligen alla aspekter som rör hälsosituationen, dvs. allmänhetens hälsotillstånd, inbegripet sjuklighet och funktionshinder, hälsans bestämningsfaktorer, hälso- och sjukvårdsbehov, resurser inom hälso- och sjukvården, tillhandahållande av och allmän tillgång till hälso- och sjukvård, utgifter för och finansiering av hälso- och sjukvården samt dödsorsaker. Sådan behandling av uppgifter om hälsa av allmänt intresse bör inte innebära att personuppgifter behandlas för andra ändamål.

(32) Om de personuppgifter som behandlas av en personuppgiftsansvarig inte gör det möjligt för denna 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.

(33) 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

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

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). Unionsinstitutioner och unionsorgan 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 som har antagits av unionsinstitutioner och unionsorgan när det gäller frågor rörande deras funktion.

(34) 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 ingivande av elektroniska framställningar, särskilt i fall då personuppgifter behandlas elektroniskt. Den personuppgiftsansvarige bör utan onödigt dröjsmål och senast inom en månad vara skyldig att besvara registrerades önskemål och lämna en motivering, om den inte avser att uppfylla sådana önskemål.

(35) 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 den registrerade 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.

(36) 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 samlades in, bör denna 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.

(37) Den registrerade bör ha rätt att få tillgång till personuppgifter som samlats in om honom eller henne 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 för vilka ändamål 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 begäran avser, innan informationen lämnas ut.

(38) Den registrerade bör ha rätt att få sina personuppgifter rättade och ha en rätt att bli bortglömd, 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 återkallat 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 ett 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 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.

(39) För att stärka ”rätten att bli bortglömd” i nätmiljön bör rätten till radering utvidgas genom att en personuppgiftsansvarig som offentliggjort personuppgifter är förpliktigad att informera de personuppgiftsansvariga som behandlar dessa personuppgifter om att den registrerade har begärt radering av alla länkar till och kopior eller reproduktioner av dessa personuppgifter. I samband med detta bör den personuppgiftsansvarige vidta rimliga åtgärder, med beaktande av tillgänglig teknik och de hjälpmedel som står den personuppgiftsansvarige till buds, däribland tekniska åtgärder, för att informera de personuppgiftsansvariga som behandlar personuppgifterna om den registrerades begäran.

(40) 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.

(41) 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 i enlighet med 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.

(42) 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.

(43) 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 personlig kontakt, 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 de specifika 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 samt förhindra 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 behandling som leder till åtgärder som får sådana effekter. Automatiserat beslutsfattande och profilering baserat på särskilda kategorier av personuppgifter bör tillåtas endast på särskilda villkor.

(44) Rättsakter som antagits på grundval av fördragen eller interna regler som antagits av unionsinstitutioner och unionsorgan när det gäller frågor rörande deras funktion 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 från elektronisk kommunikation, underrättelse om en personuppgiftsincident till den registrerade och vissa därmed sammanhängande skyldigheter för personuppgiftsansvariga, i den utsträckning åtgärden är nödvändig och proportionell i ett demokratiskt samhälle för att upprätthålla den allmänna säkerheten och för att förebygga, förhindra, utreda och lagföra brott eller verkställa straffrättsliga sanktioner. Detta inbegriper skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten, skydd av människoliv, särskilt vid naturkatastrofer eller katastrofer orsakade av människan, inre säkerhet för unionsinstitutioner och unionsorgan, andra viktiga mål av allmänt intresse för hela unionen eller en medlemsstat, i synnerhet målen för unionens gemensamma utrikes- och säkerhetspolitik eller ett viktigt ekonomiskt eller finansiellt intresse för unionen eller en medlemsstat samt förande av offentliga register av hänsyn till ett allmänt intresse eller skydd av den registrerade eller andras rättigheter och friheter, inklusive socialt skydd, folkhälsa och humanitära skäl.

(45) 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.

(46) 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 som innefattar brott 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.

(47) 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.

(48) Skyddet av fysiska personers rättigheter och friheter med avseende på 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.

(49) I förordning (EU) 2016/679 föreskrivs att personuppgiftsansvariga får styrka efterlevnad genom anslutning till godkända certifieringsmekanismer. På liknande sätt bör unionsinstitutioner och unionsorgan kunna styrka efterlevnad av denna förordning genom att certifieras i enlighet med artikel 42 i förordning (EU) 2016/679.

(50) 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.

(51) För att säkerställa 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 andra personuppgiftsbiträden än unionsinstitutioner och unionsorgan bör hanteringen regleras genom ett avtal eller, om unionsinstitutioner och unionsorgan är personuppgiftsbiträden, genom ett avtal eller en annan rättsakt enligt unionsrätten 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.

(52) För att påvisa 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 göra sina register tillgängliga på begäran, så att de kan tjäna som grund för övervakningen av behandlingen. Såvida det inte är olämpligt, med hänsyn tagen till en unionsinstitutions eller ett unionsorgans storlek, bör unionens institutioner och organ ha möjlighet att inrätta ett centralt register över sin uppgiftsbehandling. Av öppenhetsskäl bör de också kunna göra ett sådant register offentligt.

(53) 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 oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt utlämnande 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.

(54) Unionens institutioner och unionsorgan bör säkerställa konfidentiell behandling av elektronisk kommunikation, som anges i artikel 7 i stadgan. I synnerhet bör unionsinstitutioner och unionsorgan säkerställa säkerheten i sina elektroniska kommunikationsnät. De bör skydda information som rör användares terminalutrustning som används för att få tillgång till unionsinstitutionernas och unionsorganens allmänt tillgängliga webbplatser och mobila applikationer i enlighet med Europaparlamentets och rådets direktiv 2002/58/EG ([1]). De bör även skydda personuppgifter som förvaras i kataloger över användare.

(55) 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.

(56) 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.

(57) I förordning (EG) nr 45/2001 föreskrivs en allmän skyldighet för en personuppgiftsansvarig att anmäla behandling av personuppgifter till dataskyddsombudet. Såvida det inte är olämpligt, med hänsyn tagen till unionsinstitutionens eller unionsorganets storlek, bör dataskyddsombudet föra ett register över sådana anmälda behandlingar. Utöver denna allmänna skyldighet bör effektiva förfaranden och mekanismer inrättas för att övervaka behandlingar som sannolikt innebär en hög risk för fysiska personers rättigheter och friheter, i kraft av deras art, omfattning, sammanhang och ändamål. Dessa förfaranden bör, i synnerhet, också finnas på plats när behandlingstyper inbegriper användning av ny teknik eller är av en ny typ, för vilken konsekvensbedömning avseende uppgiftsskydd inte tidigare har genomförts av den personuppgiftsansvarige, eller om de 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. Konsekvensbedömningen bör främst innefatta de planerade åtgärder, skyddsåtgärder och mekanismer som ska minska denna risk, säkerställa personuppgiftskyddet och visa att denna förordning efterlevs.

(58) 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

([1]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

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 Europeiska datatillsynsmannen, framför allt de åtgärder som planeras för att minska risken för fysiska personers rättigheter och friheter.

(59) Europeiska datatillsynsmannen bör informeras om administrativa åtgärder och höras om interna bestämmelser som antas av unionsinstitutioner och unionsorgan när det gäller frågor avseende deras funktion som rör deras behandling av personuppgifter, föreskriver villkor för begränsning av de registrerades rättigheter eller inför lämpligt skydd för de registrerades rättigheter, i syfte att säkerställa att den avsedda behandlingen överensstämmer med denna förordning, framför allt när det gäller att minska riskerna för den registrerade.

(60) 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 (EU) 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 unionsinstitutioner och unionsorgan, på eget initiativ eller på begäran. I syfte att säkerställa överensstämmelse mellan regler om skydd av personuppgifter inom hela unionen bör kommissionen vid utarbetande av förslag eller rekommendationer sträva efter att samråda med Europeiska datatillsynsmannen. Samråd med kommissionen bör vara obligatoriskt efter antagandet av lagstiftningsakter eller vid utarbetandet av delegerade akter och genomförandeakter som anges i artiklarna 289, 290 och 291 i EUF-fördraget och efter antagandet av rekommendationer och förslag som rör avtal med tredjeländer och internationella organisationer som anges i 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 fysiska personers rättigheter och friheter 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 sina skriftliga råd inom åtta veckor. Denna tidsfrist bör förkortas i brådskande fall eller när det annars är lämpligt, t.ex. när kommissionen utarbetar delegerade akter och genomförandeakter.

(61) I enlighet med artikel 75 i förordning (EU) 2016/679 bör Europeiska datatillsynsmannen tillhandahålla ett sekretariat för Europeiska dataskyddsstyrelsen.

(62) Inom varje unionsinstitution eller unionsorgan bör ett dataskyddsombud säkerställa att bestämmelserna i denna förordning tillämpas och ge råd åt personuppgiftsansvariga och personuppgiftsbiträden då de fullgör sina åligganden. Dataskyddsombudet bör vara en person med expertkunskap om lagstiftning och praxis på området för uppgiftsskydd, vilket bör bedömas med särskild hänsyn till den uppgiftsbehandling som utförs av den personuppgiftsansvarige eller det personuppgiftsbiträdet och det skydd som krävs för de inblandade personuppgifterna. Denna typ av dataskyddsombud bör kunna fullgöra sina uppdrag och utföra sina uppgifter på ett oberoende sätt.

(63) Den skyddsnivå som säkerställs för fysiska personer inom unionen genom denna förordning bör garanteras när personuppgifter överförs från unionsinstitutioner och unionsorgan till personuppgiftsansvariga, personuppgiftsbiträden eller andra mottagare i tredjeland eller till internationella organisationer. Samma garantier bör tillämpas när personuppgifter vidarebefordras 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 och med respekt för de grundläggande rättigheter och friheter som föreskrivs i stadgan. En överföring kan ske endast 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.

(64) Kommissionen får, enligt artikel 45 i förordning (EU) 2016/679 eller artikel 36 i direktiv (EU) 2016/680, besluta att ett tredjeland, ett territorium eller en viss specificerad sektor i ett tredjeland, eller en internationell organisation, 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.

(65) 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 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.

(66) 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.

(67) Vissa tredjeländer antar lagar och andra författningar som syftar till att direkt reglera behandling som utförs av unionsinstitutioner och unionsorgan. Detta kan inkludera rättsliga avgöranden eller beslut av administrativa myndigheter i tredjeländer där det krävs att personuppgiftsansvariga eller personuppgiftsbiträden överför eller lämnar ut 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 tillåtas endast 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.

(68) 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 unionsrätten, och överföringen bör göras endast 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.

(69) 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 unionsinstitutioner och unionsorgan och 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.

(70) Om kommissionen inte har fattat beslut om adekvat dataskyddsnivå i ett tredjeland, bör den personuppgiftsansvarige eller personuppgiftsbiträdet under alla omständigheter använda sig av lösningar som ger de registrerade verkställbara och faktiska 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.

(71) 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 nationella tillsynsmyndigheter och Europeiska datatillsynsmannen, vara ur stånd att handlägga klagomål eller göra utredningar som gäller verksamheter utanför deras jurisdiktion. Deras strävan att arbeta tillsammans över gränserna kan också hindras av otillräckliga preventiva eller korrigerande befogenheter, inkonsekventa rättsliga regelverk och praktiska hinder, som exempelvis bristande resurser. Därför bör ett närmare samarbete mellan Europeiska datatillsynsmannen och nationella tillsynsmyndigheter främjas för att bidra till informationsutbytet med deras internationella motparter.

(72) Inrättandet av Europeiska datatillsynsmannen i förordning (EG) nr 45/2001, som är bemyndigad att utföra sina uppgifter och utöva sina befogenheter under fullständigt oberoende, är ett väsentligt inslag i skyddet av fysiska personer med avseende på behandlingen av personuppgifter. Denna förordning bör ytterligare stärka och klargöra dess roll och oberoende. Europeiska datatillsynsmannen bör vara en person 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 personen har tillhört någon av de tillsynsmyndigheter som har inrättats i enlighet med artikel 51 i förordning (EU) 2016/679.

(73) För att säkerställa en enhetlig tillsyn över och ett enhetligt upprätthållande av regler om skydd av personuppgifter i hela unionen bör Europeiska datatillsynsmannen ha samma uppgifter och faktiska befogenheter som de nationella tillsynsmyndigheterna, inbegripet undersökningsbefogenheter, korrigerande befogenheter och befogenheter att påföra sanktioner samt befogenheter att utfärda tillstånd och ge råd, särskilt vid klagomål från fysiska personer, befogenheter att uppmärksamma domstolen 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 proportionell för att säkerställa 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.

(74) Europeiska datatillsynsmannens tillsynsbehörighet bör inte omfatta domstolens behandling av personuppgifter när detta sker inom ramen för domstolens dömande verksamhet, i syfte att säkerställa domstolens oberoende när den utför sin rättsskipande verksamhet, inbegripet när den fattar beslut. För sådan behandling bör domstolen inrätta en oberoende tillsyn, i enlighet med artikel 8.3 i stadgan, exempelvis genom en intern mekanism.

(75) Europeiska datatillsynsmannens beslut om undantag, garantier, 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.

(76) Europeiska datatillsynsmannen bör följa Europaparlamentets och rådets förordning (EG) nr 1049/2001 ([1]).

(77) 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.

(78) I vissa fall föreskriver unionsrätten en modell för samordnad tillsyn som delas mellan Europeiska datatillsynsmannen och de nationella tillsynsmyndigheterna. Europeiska datatillsynsmannen är även tillsynsmyndighet för Europol, och av den anledningen har en särskild modell för samarbete med de nationella tillsynsmyndigheterna inrättats 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 lägga fram lagstiftningsförslag när så är lämpligt, 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 alla områden.

(79) Alla registrerade bör ha rätt att lämna in ett klagomål till Europeiska datatillsynsmannen och ha rätt till ett effektivt rättsmedel inför domstolen 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.

(80) 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 fördragen.

(81) För att stärka Europeiska datatillsynsmannens tillsynsroll och främja ett effektivt upprätthållande av denna förordning bör Europeiska datatillsynsmannen ha befogenhet att påföra administrativa sanktionsavgifter, som en sanktion att använda i sista hand. Sanktionsavgifterna bör syfta till att bestraffa unionsinstitutioner eller unionsorgan – 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 unionsinstitutioner och unionsorgan. Denna förordning bör ange överträdelser som är föremål för administrativa sanktionsavgifter och de övre gränserna och kriterierna för fastställande av sådana 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, dess följder och de åtgärder som vidtas för att sörja för fullgörandet av skyldigheterna enligt denna förordning och för att förebygga eller lindra konsekvenserna av överträdelsen. Vid påförande av en administrativ sanktionsavgift till en unionsinstitution eller ett unionsorgan bör Europeiska datatillsynsmannen bedöma huruvida sanktionsavgiftsbeloppet är proportionellt. Det administrativa förfarandet för att påföra sanktionsavgifter för unionsinstitutioner och unionsorgan bör följa de allmänna unionsrättsliga principerna, såsom dessa har tolkats av domstolen.

(82) 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 rätt, som har stadgeenliga mål av allmänt intresse och

([1]) Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43).

utövar 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.

(83) Tjänstemän eller övriga anställda i unionen som inte följer 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 och anställningsvillkoren för övriga anställda i unionen som fastställs i rådets förordning (EEG, Euratom, EKSG) nr 259/68 ([1]) (nedan kallade *tjänsteföreskrifterna*).

(84) För att säkerställa enhetliga villkor för genomförandet av denna förordning bör kommissionen tilldelas genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([2]). Granskningsförfarandet bör användas för att anta standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden och mellan personuppgiftsbiträden, för att anta en förteckning över sådan behandling som kräver förhandssamråd med Europeiska datatillsynsmannen av personuppgiftsansvariga som behandlar personuppgifter för att utföra en uppgift av allmänt intresse, och för att anta standardavtalsklausuler om lämpliga skyddsåtgärder vid internationella överföringar.

(85) 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 enligt artikel 338.2 i EUF-fördraget. Europaparlamentets och rådets förordning (EG) nr 223/2009 ([3]) innehåller ytterligare preciseringar om statistisk konfidentialitet för europeisk statistik.

(86) Förordning (EG) nr 45/2001 och Europaparlamentets, rådets och kommissionens beslut nr 1247/2002/EG ([4]) bör upphöra att gälla. Hänvisningar till den upphävda förordningen och det upphävda beslutet bör anses som hänvisningar till den här förordningen.

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

(88) I enlighet med proportionalitetsprincipen är det nödvändigt och lämpligt, för att förverkliga det grundläggande målet att säkerställa en likvärdig nivå för skyddet av fysiska personer med avseende på behandling av personuppgifter och det fria flödet av personuppgifter över hela unionen, att fastställa bestämmelser om behandling av personuppgifter i unionsinstitutioner och unionsorgan. Denna förordning går inte utöver vad som är nödvändigt för att uppnå de eftersträvade målen i enlighet med artikel 5.4 i EU-fördraget.

(89) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 och avgav ett yttrande den 15 mars 2017 ([5]).

([1]) EGT L 56, 4.3.1968, s. 1.

([2]) 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).

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

([4]) Europaparlamentets, rådets och kommissionens 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).

([5]) EUT C 164, 24.5.2017, s. 2.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte och mål

1. I denna förordning fastställs bestämmelser om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionsinstitutioner och unionsorgan samt bestämmelser om det fria flödet av personuppgifter mellan dem eller till andra mottagare som är etablerade i unionen.

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 unionsorgan.

Artikel 2

Tillämpningsområde

1. Denna förordning är tillämplig på alla unionsinstitutioners och unionsorgans behandling av personuppgifter.

2. Endast artikel 3 och kapitel IX i denna förordning är tillämpliga på behandling av operativa personuppgifter som utförs av unionens organ och byråer när dessa utövar verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget.

3. Fram till dess att Europaparlamentets och rådets förordning (EU) 2016/794 ([1]) och rådets förordning (EU) 2017/1939 ([2]) har anpassats i enlighet med artikel 98 i den här förordningen, är denna förordning inte tillämplig på behandling av operativa personuppgifter som utförs av Europol och Europeiska åklagarmyndigheten.

4. Denna förordning är inte tillämplig på behandling av personuppgifter som utförs inom ramen för sådana uppdrag som avses i artiklarna 42.1, 43 och 44 i EU-fördraget.

5. Denna förordning ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

Artikel 3

Definitioner

I denna förordning avses med

1. *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad *den registrerade*); varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

2. *operativa personuppgifter*: alla personuppgifter som behandlas av unionens organ eller byråer när dessa utövar verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget för att uppfylla de mål och fullgöra de uppgifter som fastställs i rättsakterna om inrättande av dessa organ och byråer.

([1]) Europaparlamentets och rådets förordning (EU) 2016/794 av den 11 maj 2016 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF (EUT L 135, 24.5.2016, s. 53).

([2]) Rådets förordning (EU) 2017/1939 av den 12 oktober 2017 om genomförande av fördjupat samarbete om inrättande av Europeiska åklagarmyndigheten (EUT L 283, 31.10.2017, s. 1).

3. *behandling*: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

4. *begränsning av behandling*: markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden.

5. *profilering*: varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

6. *pseudonymisering*: behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

7. *register*: en strukturerad samling personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.

8. *personuppgiftsansvarig*: den unionsinstitution eller det unionsorgan eller det generaldirektorat eller varje annan organisatorisk enhet som ensam(t) eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för denna behandling bestäms av en särskild unionsakt kan den personuppgiftsansvarige eller de särskilda kriterierna för utnämning av personuppgiftsansvarig föreskrivas i unionsrätten.

9. *andra personuppgiftsansvariga än unionsinstitutioner och unionsorgan*: personuppgiftsansvariga i den mening som avses i artikel 4.7 i förordning (EU) 2016/679 och personuppgiftsansvariga i den mening som avses i artikel 3.8 i direktiv (EU) 2016/680.

10. *unionsinstitutioner och unionsorgan*: unionsinstitutioner, unionsorgan och unionsbyråer som har inrättats genom eller på grundval av EU-fördraget, EUF-fördraget eller Euratomfördraget.

11. *behörig myndighet*: en offentlig myndighet i en medlemsstat som har behörighet att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

12. *personuppgiftsbiträde*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

13. *mottagare*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som personuppgifterna utlämnas till, oavsett om det rör sig om en tredje part eller inte; offentliga myndigheter som kan komma att motta personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare; offentliga myndigheters behandling av dessa uppgifter ska vara förenlig med tillämpliga bestämmelser för dataskydd beroende på behandlingens syfte.

14. *tredje part*: en fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvariga, personuppgiftsbiträdet eller de personer som, under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar, är behöriga att behandla personuppgifterna.

15. *samtycke av den registrerade*: varje slag av frivillig, specifik, informerad och otvetydig viljeyttring genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

16. *personuppgiftsincident*: en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörig utlämning av eller obehörig åtkomst till de personuppgifter som har överförts, lagrats eller på annat sätt behandlats.

17. *genetiska uppgifter*: alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om denna fysiska persons fysiologi eller hälsa och vilka framför allt härrör från en analys av ett biologiskt prov från den fysiska personen i fråga.

18. *biometriska uppgifter*: personuppgifter som har erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar en entydig identifiering av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter.

19. *uppgifter om hälsa*: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om personens hälsostatus.

20. *informationssamhällets tjänster*: alla tjänster enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 ([1]).

21. *internationell organisation*: en organisation och dess underställda organ som lyder under internationell rätt, eller ett annat organ som har inrättats genom eller på grundval av en överenskommelse mellan två eller flera länder.

22. *nationell tillsynsmyndighet*: en oberoende offentlig myndighet som har utsetts av en medlemsstat enligt artikel 51 i förordning (EU) 2016/679 eller enligt artikel 41 i direktiv (EU) 2016/680.

23. *användare*: en fysisk person som använder ett nätverk eller en terminalutrustning som drivs under överinseende av en unionsinstitution eller ett unionsorgan.

24. *katalog*: en allmänt tillgänglig användarförteckning eller en intern användarförteckning som är tillgänglig inom en unionsinstitution eller ett unionsorgan eller som delas mellan unionsinstitutioner och unionsorgan, antingen i tryckt eller i elektroniskt format.

25. *elektroniskt kommunikationsnät*: ett system för överföring, oberoende av om det bygger på en permanent infrastruktur eller centraliserad förvaltningskapacitet eller inte, och i tillämpliga fall utrustning för koppling eller dirigering samt andra resurser, inbegripet nätkomponenter som inte är aktiva, som medger överföring av signaler via tråd, via radio, på optisk väg eller via andra elektromagnetiska överföringsmedier, däribland satellitnät, fasta nät (kretskopplade och paketkopplade, inbegripet internet) och markbundna mobilnät, elnätsystem i den utsträckning dessa används för signalöverföring, rundradionät samt kabel-tv-nät, oberoende av vilken typ av information som överförs.

26. *terminalutrustning*: terminalutrustning enligt definitionen i artikel 1.1 i kommissionens direktiv 2008/63/EG ([2]).

KAPITEL II

ALLMÄNNA 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 ska, i enlighet med artikel 13, inte anses vara oförenlig med de ursprungliga ändamålen (ändamålsbegränsning).

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

d) De ska vara riktiga 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 (riktighet).

([1]) Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

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

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 kommer att 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 är endast laglig 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 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. Den grund för behandlingen som avses i punkt 1 a och b ska fastställas i unionsrätten.

Artikel 6

Behandling för ett annat förenligt ändamål

Om en behandling för ett annat ändamål än det för vilket personuppgifterna har samlats 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 25.1, ska den personuppgiftsansvarige för att fastställa huruvida behandling för annat ändamål är förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in bland annat beakta följande:

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

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

c) Personuppgifternas art, särskilt huruvida särskilda kategorier av personuppgifter behandlas enligt artikel 10, eller huruvida personuppgifter om fällande domar i brottmål och lagöverträdelser som innefattar brott behandlas, enligt artikel 11.

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

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

Artikel 7

Villkor för samtycke

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

2. Om den registrerades samtycke lämnas i 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 lättillgänglig 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 för ett barns samtycke avseende informationssamhällets tjänster

1. Vid erbjudande av informationssamhällets tjänster direkt till ett barn, ska vid tillämpningen av artikel 5.1 d behandling av personuppgifter som rör ett barn vara tillåten om barnet är minst 13 år. Om barnet är under 13 år ska sådan behandling vara tillåten 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 mottagare som är etablerade i unionen och som inte är unionsinstitutioner och unionsorgan

1. Utan att det påverkar tillämpningen av artiklarna 4 – 6 och 10 ska personuppgifter överföras till mottagare som är etablerade i unionen och som inte utgörs av unionsinstitutioner och unionsorgan endast om

a) mottagaren visar att uppgifterna är nödvändiga för att utföra en uppgift av allmänt intresse eller som ett led i mottagarens myndighetsutövning, eller om

b) mottagaren visar att det är nödvändigt att uppgifterna överförs för ett specifikt ändamål av allmänt intresse och, i de fall då det finns skäl att anta att den registrerades legitima intressen skulle kunna skadas, den personuppgiftsansvarige visar att överföringen av personuppgifterna är proportionell i förhållande till det specifika ändamålet, efter en påvisbar avvägning mellan de olika konkurrerande intressena.

2. Om den personuppgiftsansvarige tar initiativ till överföringen enligt denna artikel ska denne visa att överföringen av personuppgifterna är nödvändig och proportionell i förhållande till ändamålet med överföringen med tillämpning av de kriterier som anges i punkt 1 a eller b.

3. Unionsinstitutioner och unionsorgan ska förena rätten till skydd av personuppgifter med rätten till tillgång till handlingar i enlighet med unionsrätten.

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 personuppgifter 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 på områdena om social trygghet och socialt skydd, i den omfattning detta är tillåtet enligt unionsrätten 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 när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.

d) Behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder i 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 organets medlemmar eller före detta medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med det och att uppgifterna inte lämnas ut utanför organet utan den registrerades samtycke.

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

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

g) Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten 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.

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

i) Behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter, på grundval av unionsrätten 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 unionsrätten vilken ska stå i proportion till det eftersträvade syftet, vara förenlig med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

3. Personuppgifter som avses i punkt 1 får behandlas för de ändamål som avses i punkt 2 h när uppgifterna behandlas av eller under ansvar av en yrkesutövare som omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställts av nationella behöriga organ, eller av en annan person som också omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställts av nationella behöriga organ.

Artikel 11

Behandling av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott

Behandling av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott eller därmed sammanhängande säkerhetsåtgärder enligt artikel 5.1 får endast utföras under kontroll av en myndighet eller då behandlingen är tillåten enligt unionsrätten, 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 den 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 identifieringen 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 ändamålen kan uppfyllas på det sättet. När ändamålen kan uppfyllas genom ytterligare behandling av uppgifter som inte medger eller inte längre medger identifiering av de registrerade ska ändamålen uppfyllas på det sättet.

KAPITEL III

DEN REGISTRERADES RÄTTIGHETER

AVSNITT 1

Öppenhet och villkor

Artikel 14

Klar och tydlig information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter

1. Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att tillhandahålla den registrerade all information som avses i artiklarna 15 och 16 och all kommunikation enligt artiklarna 17–24 och 35 vilken avser behandling i en koncis, klar och tydlig, begriplig och lättillgänglig form och på ett klart och tydligt språk, i synnerhet information som är särskilt riktad till barn. Informationen ska tillhandahållas skriftligen, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Om den registrerades begär det får informationen tillhandahållas muntligen, förutsatt att den registrerades identitet bevisats på andra sätt.

2. Den personuppgiftsansvarige ska underlätta utövandet av den registrerades rättigheter enligt 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 enligt artiklarna 17–24, om inte den personuppgiftsansvarige visar att den inte är i stånd att identifiera den registrerade.

3. Den personuppgiftsansvarige ska på begäran utan onödigt dröjsmål och under alla omständigheter senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits enligt artiklarna 17–24. 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 inte den registrerade begär något annat.

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

5. Information som tillhandahålls enligt artiklarna 15 och 16, all kommunikation och samtliga åtgärder som vidtas enligt artiklarna 17–24 och 35 ska tillhandahållas kostnadsfritt. Om begäranden från en registrerad är uppenbart ogrundade eller orimliga, särskilt på grund av deras repetitiva art, får den personuppgiftsansvarige vägra att tillmötesgå dem. Det ska åligga den personuppgiftsansvarige att visa att en begäran är uppenbart ogrundad eller orimlig.

6. Utan att det påverkar tillämpningen av artikel 12 får den personuppgiftsansvarige, om den har rimliga skäl att betvivla identiteten hos den fysiska person som lämnar in 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 den registrerade enligt 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 enligt 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 standardiserade symboler, ska unionsinstitutioner och unionsorgan tillhandahålla de uppgifter som avses i artiklarna 15 och 16 i den här förordningen tillsammans med sådana standardiserade symboler när det är lämpligt.

AVSNITT 2

Information och tillgång till personuppgifter

Artikel 15

Information som ska tillhandahållas när 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, till den registrerade lämna information om följande:

a) Identitet och kontaktuppgifter för den personuppgiftsansvarige.

b) Kontaktuppgifter för dataskyddsombudet.

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 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 48, 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 tillhandahålla 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 av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller, i tillämpliga fall, rätten att invända mot behandling samt rätten 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) Rätten att inge 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 om 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, som avses i 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 tillhandahålla den registrerade följande information:

a) Identitet och kontaktuppgifter för den personuppgiftsansvarige.

b) Kontaktuppgifter för dataskyddsombudet.

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 48, 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) Förekomsten av rätten att av 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, rätten att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket innan detta återkallades.

d) Rätten att inge klagomål till 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 tillhandahålla 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 som fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen, eller

d) personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätten, inbegripet andra lagstadgade sekretessförpliktelser.

6. I de fall som avses i punkt 5 b ska den personuppgiftsansvarige vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen, däribland göra informationen allmänt tillgänglig.

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) Rätten 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 åtminstone i dessa fall 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 48 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 bortglömd”)

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 något av följande gäller:

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

b) Den registrerade återkallar det samtycke på vilket behandlingen grundar sig enligt artikel 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, eller andra personuppgiftsansvariga än unionsinstitutioner och unionsorgan, 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 ett led i myndighetsutövning som utförs av den personuppgiftsansvarige.

c) För skäl som rör ett 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 riktighet, under en tid som ger den personuppgiftsansvarige möjlighet att kontrollera om personuppgifterna är riktiga och fullständiga.

b) Behandlingen är olaglig, och den registrerade motsätter sig att personuppgifterna raderas och begär i stället 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, behandlas endast 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 ske 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 eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling som skett 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, eller till andra personuppgiftsansvariga än unionsinstitutioner och unionsorgan, 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 påverka andras rättigheter och friheter på ett ogynnsamt sätt.

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 denna inte kan påvisa avgörande 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 tydligt, 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 36 och 37, utöva sin rätt att göra invändningar på automatiserat sätt med 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, och som 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 berättigade 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 i denna artikel 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 som ska skydda 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 unionsinstitutioners och unionsorgans funktion, interna regler som införts av de sistnämnda får föreskriva begränsningar i tillämpningen av artiklarna 14–22, 35 och 36, 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 målen för unionens gemensamma utrikes- och säkerhetspolitik eller 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 unionsinstitutioner och unionsorgan, 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 leden a–c,

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

i) verkställighet av civilrättsliga krav.

2. Framför allt ska alla rättsakter eller interna regler som avses i punkt 1 innehålla specifika bestämmelser, när så är relevant, avseende

a) ändamålen med behandlingen eller kategorierna av behandling,

b) kategorierna av personuppgifter,

c) omfattningen av de införda begränsningarna,

d) skyddsåtgärder för att förhindra missbruk eller olaglig tillgång eller överföring,

e) specificeringen av den personuppgiftsansvarige eller kategorierna av personuppgiftsansvarige,

f) lagringsperioderna samt tillämpliga skyddsåtgärder med beaktande av behandlingens art, omfattning och ändamål eller kategorierna av behandling, och

g) riskerna för de registrerades rättigheter och friheter.

3. Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål får det i unionsrätten, som kan inkludera interna regler som antagits av unionsinstitutioner och unionsorgan när det gäller frågor rörande deras funktion, 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, som kan inkludera interna regler som antagits av unionsinstitutioner och unionsorgan när det gäller frågor rörande deras funktion, 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 mycket 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 klara och precisa akter med allmän giltighet som är avsedda att ha rättsverkan gentemot registrerade och som har antagits på unionsinstitutionernas och unionsorganens högsta administrativa nivå och ska offentliggöras i *Europeiska unionens officiella tidning*.

6. Om en begränsning införs i enlighet med punkt 1, 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 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 i den här artikeln samt i artikel 45.2 får skjutas upp, utelämnas eller nekas om det skulle upphäva verkan av en begränsning som införts i enlighet med punkt 1 i den här artikeln.

KAPITEL IV

PERSONUPPGIFTSANSVARIGA OCH PERSONUPPGIFTSBITRÄDEN

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.

3. Tillämpningen av godkända certifieringsmekanismer som avses i artikel 42 i förordning (EU) 2016/679 får användas för att visa att den personuppgiftsansvarige fullgör sina skyldigheter.

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, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter som standard inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

3. En godkänd certifieringsmekanism i enlighet med artikel 42 i förordning (EU) 2016/679 får användas för att visa att kraven i punkterna 1 och 2 i den här artikeln följs.

Artikel 28

Gemensamt personuppgiftsansvariga

1. Om två eller flera personuppgiftsansvariga eller en eller flera personuppgiftsansvariga tillsammans med en eller flera personuppgiftsansvariga som inte är unionsinstitutioner och unionsorgantillsammans 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 gemensamt personuppgiftsansvarigas respektive skyldigheter fastställs genom unionsrätten eller en medlemsstats nationella rätt som de gemensamt personuppgiftsansvariga omfattas av. Inom ramen för arrangemanget får en gemensam kontaktpunkt för de personuppgiftsansvariga utses.

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

3. Oavsett formerna för det arrangemang som avses i punkt 1 får den registrerade utöva sina rättigheter enligt denna förordning med avseende på och gentemot var och en av de personuppgiftsansvariga.

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. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.

3. När uppgifter behandlas av ett personuppgiftsbiträde ska 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) ska säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt,

c) ska vidta alla åtgärder som krävs enligt artikel 33,

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

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

f) ska bistå den personuppgiftsansvarige med att säkerställa att skyldigheterna enligt artiklarna 33–41 fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå,

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

h) ska ge 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 personuppgiftsbiträdet 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 i 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 beviljats det personuppgiftsbiträde 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 96.2.

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 eller personuppgiftsbiträdets överinseende

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

Artikel 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 personuppgiftsansvarige.

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 omfattar 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. Unionsinstitutioner och unionsorgan ska på begäran göra registret tillgängligt för Europeiska datatillsynsmannen.

5. Såvida det inte är olämpligt med hänsyn till unionsinstitutionens eller unionsorganets storlek, ska unionsinstitutioner och unionsorgan bevara sina register över behandling i ett centralt register. De ska göra registret allmänt tillgängligt.

Artikel 32

Samarbete med Europeiska datatillsynsmannen

Unionsinstitutioner och unionsorgan ska på begäran samarbeta med Europeiska datatillsynsmannen vid fullgörandet av dess uppgifter.

AVSNITT 2

Säkerhet för personuppgifter

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 fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och behandlingstjänsterna,

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

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

2. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt utlämnande 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, behandlar dessa endast på instruktion från den personuppgiftsansvarige, om inte unionsrätten ålägger honom eller henne att göra det.

4. Anslutning till en godkänd certifieringsmekanism som avses i artikel 42 i förordning (EU) 2016/679 får användas för att visa att kraven i punkt 1 i den här artikeln följs.

Artikel 34

Anmälan av en personuppgiftsincident till Europeiska datatillsynsmannen

1. Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till 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 35

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 34.3 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 har tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som ska göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna, såsom kryptering.

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

c) Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade underrättas 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 den personuppgiftsansvarige gör det eller får besluta att något av de villkor som avses i punkt 3 uppfylls.

AVSNITT 3

Konfidentialitet för elektronisk kommunikation

Artikel 36

Konfidentialitet för elektronisk kommunikation

Unionsinstitutioner och unionsorgan ska säkerställa konfidentiell behandling av uppgifter inom elektronisk kommunikation, särskilt genom att säkra sina elektroniska kommunikationsnät.

Artikel 37

Skydd av information som sänds till, lagras i, avser, behandlas av eller samlas in från användares terminalutrustning

Unionsinstitutioner och unionsorgan ska skydda information som sänds till, lagras i, avser, behandlas av eller samlas in från användares terminalutrustning som används för att få tillgång till unionsinstitutionernas och unionsorganens allmänt tillgängliga webbplatser och mobila applikationer i enlighet med artikel 5.3 i direktiv 2002/58/EG.

Artikel 38

Kataloger över användare

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

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

AVSNITT 4

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 följande fall:

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

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

c) 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. Innan de förteckningar som avses i punkterna 4 och 5 i denna artikel antas ska Europeiska datatillsynsmannen begära att Europeiska dataskyddsstyrelsen, som inrättats genom artikel 68 i förordning (EU) 2016/679, undersöker dem i enlighet med artikel 70.1 e i den förordningen, om de avser behandling som utförs av en personuppgiftsansvarig gemensamt med en eller flera andra personuppgiftsansvariga än unionsinstitutioner och unionsorgan.

7. 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.

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

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

10. Om behandlingen enligt 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 i den här artikeln inte vara tillämpliga, såvida inte den rättsakten föreskriver något annat.

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

Artikel 40

Förhandssamråd

1. Den personuppgiftsansvarige ska samråda med Europeiska datatillsynsmannen före behandling om en konsekvensbedömning avseende dataskydd enligt artikel 39 visar 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 reducerat risken, ska Europeiska datatillsynsmannen inom en period på högst åtta veckor från det att begäran om samråd mottagits, ge den personuppgiftsansvarige och i tillämpliga fall personuppgiftsbiträdet skriftliga råd och får utnyttja alla de befogenheter som denne har enligt artikel 58. 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 tillfälligt upphöra att löpa 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 den personuppgiftsansvarige, de gemensamt personuppgiftsansvariga och de 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 en genomförandeakt fastställa en förteckning över de fall där de personuppgiftsansvarige ska samråda med, och erhålla förhandstillstånd av, Europeiska datatillsynsmannen i samband med behandling av personuppgifter för att utföra en arbetsuppgift som den personuppgiftsansvarige utför i allmänhetens intresse, inbegripet behandling av sådana uppgifter i samband med social trygghet och folkhälsa.

AVSNITT 5

Information och samråd i lagstiftningsprocessen

Artikel 41

Information och samråd

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

2. Unionsinstitutioner och unionsorgan ska samråda med Europeiska datatillsynsmannen när de utarbetar de interna regler som avses i artikel 25.

Artikel 42

Samråd i lagstiftningsprocessen

1. Kommissionen ska, efter antagandet av förslag till en lagstiftningsakt, av rekommendationer eller av förslag till rådet i enlighet med artikel 218 i EUF-fördraget eller 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, 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 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 6

Dataskyddsombud

Artikel 43

Utnämning av dataskyddsombudet

1. Varje unionsinstitution eller unionsorgan ska utnämna ett dataskyddsombud.

2. Unionsinstitutioner och unionsorgan får utnämna ett enda dataskyddsombud för flera av dem, med hänsyn till deras organisationsstruktur och storlek.

3. Dataskyddsombudet ska utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i artikel 45.

4. Dataskyddsombudet ska ingå i unionsinstitutionens eller unionsorganets personal. Med hänsyn tagen till deras storlek och om det alternativ som anges i punkt 2 inte har utnyttjats, får unionsinstitutioner och unionsorgan utse ett dataskyddsombud som utför sina uppgifter på grundval av ett tjänsteavtal.

5. Unionsinstitutioner och unionsorgan ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till Europeiska datatillsynsmannen.

Artikel 44

Dataskyddsombudets ställning

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

2. Unionsinstitutioner och unionsorgan ska stödja dataskyddsombudet i utförandet av de uppgifter som avses i artikel 45 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. Unionsinstitutioner och unionsorgan ska säkerställa att dataskyddsombudet inte tar emot instruktioner som gäller utförandet av dessa 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 dennes personal ska, när det gäller genomförandet av sina uppgifter, vara bundna 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, i alla frågor som rör tolkningen eller tillämpningen av denna förordning, utan att dessa personer behöver gå den officiella vägen. 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 honom eller henne om han eller hon inte längre uppfyller de krav som ställs för att han eller hon ska kunna utföra sina uppgifter endast efter medgivande av Europeiska datatillsynsmannen.

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 45

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, samt 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 av eller ett meddelande om en personuppgiftsincident enligt artiklarna 34 och 35.

e) På begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet 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 föregående samråd med Europeiska datatillsynsmannen enligt artikel 40 och samråda med Europeiska datatillsynsmannen vid eventuellt tvivel om behovet av ett föregående samråd.

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

h) Säkerställa att de registrerades rättigheter och friheter inte påverkas negativt av behandlingen.

2. Dataskyddsombudet får ge rekommendationer till den personuppgiftsansvarige och personuppgiftsbiträdet för den praktiska förbättringen av uppgiftsskyddet 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 utredningen eller till den personuppgiftsansvarige eller personuppgiftsbiträdet.

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

KAPITEL V

ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJELÄNDER ELLER INTERNATIONELLA ORGANISATIONER

Artikel 46

Allmän princip för överföring av uppgifter

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

Artikel 47

Överföring på grundval av ett beslut om adekvat skyddsnivå

1. Personuppgifter får överföras till ett tredjeland eller en internationell organisation om kommissionen enligt artikel 45.3 i förordning (EU) 2016/679 eller artikel 36.3 i direktiv (EU) 2016/680 har beslutat att ett tredjeland, ett territorium eller en eller flera specificerade sektorer i det tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå, och personuppgifter överförs uteslutande för att göra det möjligt att utföra uppgifter som omfattas av den personuppgiftsansvariges behörighet.

2. Unionsinstitutioner och unionsorgan ska informera kommissionen och Europeiska datatillsynsmannen då de anser att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredje land, eller en internationell organisation i fråga inte säkerställer en adekvat skyddsnivå enligt punkt 1.

3. Unionsinstitutioner och unionsorgan ska vidta de åtgärder som är nödvändiga för att följa de beslut kommissionen fattat enligt artikel 45.3 eller 45.5 i förordning (EU) 2016/679 eller med artikel 36.3 eller 36.5 i direktiv (EU) 2016/680, i vilka den konstaterat att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredje land, eller en internationell organisation säkerställer eller inte längre säkerställer en adekvat skyddsnivå.

Artikel 48

Överföring som omfattas av lämpliga skyddsåtgärder

1. I avsaknad av ett beslut i enlighet med artikel 45.3 i förordning (EU) 2016/679 eller artikel 36.3 i direktiv (EU) 2016/680 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 antagits av kommissionen i enlighet med det granskningsförfarande som avses i artikel 96.2,

c) standardiserade dataskyddsbestämmelser som antas av Europeiska datatillsynsmannen och godkänts av kommissionen enligt det granskningsförfarande som avses i artikel 96.2,

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

3. Med förbehåll för tillstånd från Europeiska datatillsynsmannen, får lämpliga skyddsåtgärder enligt punkt 1 också i synnerhet ta formen av

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

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

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

5. Unionsinstitutioner och unionsorgan ska informera Europeiska datatillsynsmannen om kategorier av fall där denna artikel har tillämpats.

Artikel 49

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 50

Undantag i särskilda situationer

1. Om det inte föreligger något beslut om adekvat skyddsnivå enligt artikel 45.3 i förordning (EU) 2016/679 eller artikel 36.3 i direktiv (EU) 2016/680 eller lämpliga skyddsåtgärder enligt artikel 48 i den här förordningen 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 berättigat intresse, men endast i den utsträckning som de i unionsrätten angivna villkoren för tillgänglighet uppfylls i det särskilda fallet.

2. Punkt 1 a, b och c ska inte tillämpas på åtgärder som vidtas av unionsinstitutioner och unionsorgan som ett led i utövandet av deras offentliga befogenheter.

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

4. 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 göras endast på begäran av dessa personer eller om de själva är mottagarna.

5. Saknas 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.

6. Unionsinstitutioner och unionsorgan ska informera Europeiska datatillsynsmannen om kategorierna av fall där denna artikel har tillämpats.

Artikel 51

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 en effektiv tillämpning av lagstiftningen om skydd av personuppgifter,

b) på internationell nivå erbjuda ömsesidigt bistånd för en effektiv tillämpning av lagstiftningen om skydd av personuppgifter, bland annat genom underrättelse, hänskjutande av klagomål, bistånd vid utredningar samt informationsutbyte, med iakttagande av lämpliga skyddsåtgärder för personuppgifter samt 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 52

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 unionsinstitutioner och unionsorgan.

3. Europeiska datatillsynsmannen ska ha i uppdrag att övervaka och säkerställa 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 unionsinstitutioner och unionsorgan och de registrerade i alla frågor som rör behandling av personuppgifter. För dessa ändamål ska Europeiska datatillsynsmannen fullgöra de uppgifter som fastställs i artikel 57 och utöva de befogenheter som anges i artikel 58.

4. Förordning (EG) nr 1049/2001 ska vara tillämplig på handlingar som innehas av Europeiska datatillsynsmannen. Europeiska datatillsynsmannen ska anta föreskrifter för tillämpningen av förordning (EG) nr 1049/2001 när det gäller dessa handlingar.

Artikel 53

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 och bestå av minst tre kandidater. 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 av kandidater som avses i punkt 1 ska bestå av personer vars oberoende är ställt utom alla tvivel och som har expertkunskap inom dataskydd och den erfarenhet och sakkunskap som krävs för att utöva uppdraget som Europeisk datatillsynsman.

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 domstolen, 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 unionens immunitet och privilegier ska vara tillämpliga på Europeiska datatillsynsmannen.

Artikel 54

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 domstolen när det gäller fastställande av löner, ersättningar, ålderspension och all annan ersättning utöver lön.

2. Budgetmyndigheten ska säkerställa 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 avsnittet om administrativa utgifter i 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. Artikel 75.2 i förordning (EU) 2016/679 ska tillämpas på dem bland Europeiska datatillsynsmannens personal som deltar i att utföra de uppgifter som tilldelats Europeiska dataskyddsstyrelsen i unionsrätten.

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

6. Europeiska datatillsynsmannen ska ha sitt säte i Bryssel.

Artikel 55

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 fria från utomstående påverkan, direkt såväl som indirekt, och får varken begära eller ta emot instruktioner av någon.

3. Europeiska datatillsynsmannen ska avhålla sig från alla handlingar som är oförenliga med hans eller hennes skyldigheter och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet.

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

Artikel 56

Tystnadsplikt

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

Artikel 57

Uppgifter

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

a) Övervaka och upprätthålla unionsinstitutioner och unionsorgans tillämpning av denna förordning, med undantag av behandling av personuppgifter som utförs av domstolen 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 de nationella tillsynsmyndigheterna 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) På eget initiativ eller på begäran ge rådgivning åt alla unionsinstitutioner och unionsorgan om lagstiftningsåtgärder och administrativa åtgärder rörande skyddet av fysiska personers rättigheter och friheter med avseende på 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 48.2 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.

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 48.3.

o) Föra interna register över överträdelser av denna förordning och åtgärder som vidtagits i enlighet med artikel 58.2.

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 kostnadsfritt 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 58

Befogenheter

1. Europeiska datatillsynsmannen ska ha samtliga följande utredningsbefogenheter:

a) Att beordra den personuppgiftsansvarige eller personuppgiftsbiträdet att tillhandahålla all information som Europeiska datatillsynsmannen behöver för att kunna fullgöra sina uppgifter.

b) Att genomföra undersökningar i form av dataskyddstillsyn.

c) Att underrätta den personuppgiftsansvarige eller personuppgiftsbiträdet om en påstådd överträdelse av denna förordning.

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

e) Att 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 unionsrätten.

2. Europeiska datatillsynsmannen ska ha samtliga följande korrigerande befogenheter:

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

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

c) Att rapportera ärenden till den personuppgiftsansvarige eller det personuppgiftsbiträde som berörs och vid behov till Europaparlamentet, rådet och kommissionen.

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

e) Att 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) Att förelägga den personuppgiftsansvarige att meddela den registrerade att en personuppgiftsincident har inträffat.

g) Att införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, behandling.

h) Att 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) Att påföra administrativa sanktionsavgifter i enlighet med artikel 66, om en unionsinstitution eller ett unionsorgan inte har efterlevt en av de åtgärder som avses i leden d–h och j i denna punkt, med hänsyn till omständigheterna i det enskilda fallet.

j) Att förelägga om att flödet av uppgifter till en mottagare i en medlemsstat, ett tredjeland 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 och i enlighet med artikel 41.2.

c) På eget initiativ eller på begäran avge yttranden till unionsinstitutioner och unionsorgan samt till allmänheten, i frågor som rör skydd av personuppgifter.

d) Anta standardiserade dataskyddsbestämmelser enligt artiklarna 29.8 och 48.2 c.

e) Godkänna avtalsklausuler enligt artikel 48.3 a.

f) Godkänna administrativa överenskommelser enligt artikel 48.3 b.

g) Godkänna behandling enligt genomförandeakter som antagits enligt artikel 40.4.

4. Europeiska datatillsynsmannen ska ha befogenhet att hänskjuta ärendet till domstolen på de villkor som anges i fördragen och att intervenera i ärenden som anhängiggjorts vid domstolen.

5. 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.

Artikel 59

Skyldighet för personuppgiftsansvariga och personuppgiftsbiträden att reagera på anmärkningar

När Europeiska datatillsynsmannen utövar de befogenheter som föreskrivs i artikel 58.2 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 också innehålla en beskrivning av de eventuella åtgärder som har vidtagits med anledning av anmärkningar från Europeiska datatillsynsmannen.

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 den rapport som avses i punkt 1 till övriga unionsinstitutioner och unionsorgan, som får lämna kommentarer inför en eventuell granskning av rapporten av Europaparlamentet.

KAPITEL VII

SAMARBETE OCH ENHETLIGHET

Artikel 61

Samarbete mellan Europeiska datatillsynsmannen och nationella tillsynsmyndigheter

Europeiska datatillsynsmannen ska samarbeta med nationella tillsynsmyndigheter samt med den gemensamma tillsynsmyndighet som inrättats enligt artikel 25 i rådets beslut 2009/917/RIF ([1]) i den utsträckning som krävs för att de ska kunna fullgöra sina respektive uppgifter, särskilt genom att ge varandra relevant information, efterfråga av varandra att utöva respektive befogenheter och svara på varandras begäranden.

Artikel 62

En samordnad tillsyn av Europeiska datatillsynsmannen och de nationella tillsynsmyndigheterna

1. Om en unionsakt hänvisar till denna artikel ska Europeiska datatillsynsmannen och de nationella tillsynsmyndigheterna, inom ramen för sina respektive behörigheter, samarbeta aktivt inom sina ansvarsområden för att säkerställa en effektiv tillsyn över stora it-system och unionsorgan eller unionsbyråer.

2. De ska, om så behövs, inom ramen för sina respektive behörigheter och inom sina ansvarsområden utbyta relevant information, bistå varandra 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 utöva sina rättigheter, upprätta harmoniserade förslag till lösningar på eventuella problem och främja medvetenheten om dataskyddsrättigheterna.

3. För de ändamål som anges i punkt 2 ska Europeiska datatillsynsmannen och de nationella tillsynsmyndigheterna sammanträda minst två gånger om året inom ramen för Europeiska dataskyddsstyrelsen. För dessa ändamål får Europeiska dataskyddsstyrelsen utarbeta ytterligare arbetsmetoder efter behov.

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

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

KAPITEL VIII

RÄTTSMEDEL, ANSVAR OCH SANKTIONER

Artikel 63

Rätt att lämna 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 underrätta den enskilde om hur arbetet med klagomålet fortskrider och vad resultatet blir, inbegripet möjligheten till rättslig prövning enligt artikel 64.

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

Artikel 64

Rätten till ett effektivt rättsmedel

1. Domstolen ska vara behörig att pröva tvister som hänför sig till denna förordnings bestämmelser, inklusive skadeståndsanspråk.

2. Talan mot Europeiska datatillsynsmannens beslut, inbegripet beslut enligt artikel 63.3, ska väckas vid domstolen.

3. Domstolen ska ha obegränsad behörighet att pröva de administrativa sanktionsavgifter som avses i artikel 66. Den får upphäva, sänka eller höja avgifterna inom ramen för artikel 66.

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 unionsinstitutionen eller unionsorganet för den uppkomna skadan, med förbehåll för de villkor som anges i fördragen.

Artikel 66

Administrativa sanktionsavgifter

1. Europeiska datatillsynsmannen får påföra unionsinstitutioner och unionsorgan administrativa sanktionsavgifter, beroende på omständigheterna i det enskilda fallet, om en unionsinstitution eller ett unionsorgan inte rättar sig efter ett beslut av Europeiska datatillsynsmannen enligt artikel 58.2 d–h och j. Vid beslut om huruvida administrativa sanktionsavgifter ska påföras och om beloppet för de administrativa sanktionsavgifterna i varje enskilt fall ska vederbörlig hänsyn tas till följande:

a) Överträdelsens karaktär, 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 enligt 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) Efterlevnad av någon av de åtgärder som avses i artikel 58 som tidigare förordnats mot den berörda unionsinstitutionen eller det berörda unionsorganet vad gäller samma sakfråga. De förfaranden som leder fram till åläggandet av dessa avgifter ska 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, 27–35, 39, 40, 43, 44 och 45 ska, i enlighet med punkt 1 i den här artikeln, medföra administrativa sanktionsavgifter på upp till 25 000 EUR per överträdelse och upp till ett totalt belopp på 250 000 EUR per år.

3. Vid överträdelser av följande bestämmelser från unionsinstitutionens eller unionsorganets sida ska det i enlighet med punkt 1 påföras administrativa sanktionsavgifter på upp till 50 000 EUR per överträdelse och upp till ett totalt belopp på 500 000 EUR per år:

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

b) Registrerades rättigheter enligt artiklarna 4–24.

c) Överföring av personuppgifter till en mottagare i ett tredjeland eller en internationell organisation enligt artiklarna 46–50.

4. Om en unionsinstitution eller ett unionsorgan, med avseende på en och samma sammankopplade eller fortlöpande uppgiftsbehandlingar, överträder flera av bestämmelserna i denna förordning eller samma bestämmelse i denna förordning 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 förfarandet som genomförs av Europeiska datatillsynsmannen möjlighet att höras om de frågor med avseende på vilka Europeiska 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 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 lämpligt sätt i enlighet med unionsrätten eller rätten 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 artiklarna 63 och 64 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 om en påstådd överträdelse av bestämmelserna i denna förordning om behandling av personuppgifter till Europeiska datatillsynsmannen, även utan att gå den officiella vägen. Ingen ska lida förfång på grund av att ett klagomål lämnats in till Europeiska datatillsynsmannen angående en sådan överträdelse.

Artikel 69

Sanktioner

Om en tjänsteman eller annan anställd vid 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.

KAPITEL IX

BEHANDLING AV OPERATIVA PERSONUPPGIFTER SOM UTFÖRS AV UNIONENS ORGAN OCH BYRÅER NÄR DESSA UTÖVAR VERKSAMHET SOM OMFATTAS AV TREDJE DELEN AVDELNING V KAPITEL 4 ELLER KAPITEL 5 I EUF-FÖRDRAGET

Artikel 70

Kapitlets tillämpningsområde

Detta kapitel ska endast tillämpas på behandlingen av operativa personuppgifter som utförs av unionens organ och byråer när dessa utövar verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget, utan att det påverkar särskilda dataskyddsbestämmelser som är tillämpliga på dessa unionsorgan och unionsbyråer.

Artikel 71

Principer för behandling av operativa personuppgifter

1. Vid behandling av operativa personuppgifter ska följande gälla:

a) Uppgifterna ska behandlas på ett lagligt och korrekt sätt (laglighet och korrekthet).

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

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

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

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 de operativa personuppgifterna behandlas (lagringsminimering).

f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för de operativa 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. Behandling som utförs av samma eller en annan personuppgiftsansvarig för något annat ändamål, som anges i rättsakten om inrättande av unionsorganet eller unionsbyrån, än det för vilket de operativa personuppgifterna samlas in ska tillåtas om

a) den personuppgiftsansvarige är bemyndigad att behandla sådana operativa personuppgifter för ett sådant ändamål i enlighet med unionsrätten,

b) behandlingen är nödvändig och står i proportion till detta andra ändamål i enlighet med unionsrätten.

3. Behandling som utförs av samma eller en annan personuppgiftsansvarig kan inbegripa arkivering av allmänt intresse och vetenskaplig, statistisk eller historisk användning för de ändamål som anges i rättsakten om inrättande av unionsorganet eller unionsbyrån, under förutsättning att det finns lämpliga skyddsåtgärder för de registrerades rättigheter och friheter.

4. Den personuppgiftsansvarige ska ansvara för, och kunna visa efterlevnad av, punkterna 1, 2 och 3.

Artikel 72

Laglig behandling av operativa personuppgifter

1. Behandling av operativa personuppgifter ska vara laglig endast om och i den mån som behandling är nödvändig för att utföra en uppgift som utförs av unionens organ, och byråer när dessa utövar verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget, och som grundas på unionsrätten.

2. Särskilda unionsrättsakter som reglerar behandling inom tillämpningsområdet för detta kapitel ska åtminstone ange målen för behandlingen, vilka operativa personuppgifter som ska behandlas, syftet med behandlingen och tidsgränserna för lagring av de operativa personuppgifterna eller för periodisk översyn av behovet av ytterligare lagring av de operativa personuppgifterna.

Artikel 73

Åtskillnad mellan olika kategorier av registrerade

Den personuppgiftsansvarige ska i tillämpliga fall och i möjligaste mån göra en tydlig åtskillnad mellan operativa personuppgifter som rör olika kategorier av registrerade, såsom de kategorier som förtecknas i rättsakten om inrättande av unionens organ eller byråer.

Artikel 74

Åtskillnad mellan operativa personuppgifter och kontroll av kvaliteten på de operativa personuppgifterna

1. Den personuppgiftsansvarige ska i möjligaste mån skilja mellan operativa personuppgifter som grundar sig på fakta och operativa personuppgifter som grundar sig på personliga bedömningar.

2. Den personuppgiftsansvarige ska vidta alla rimliga åtgärder för att säkerställa att operativa personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. Den personuppgiftsansvarige ska därför i den mån det är praktiskt möjligt och i tillämpliga fall kontrollera kvaliteten på de operativa personuppgifterna innan dessa överförs eller görs tillgängliga, exempelvis genom att samråda med den behöriga myndighet som uppgifterna kommer ifrån. Vid all överföring av operativa personuppgifter ska den personuppgiftsansvarige i möjligaste mån lägga till sådan nödvändig information som gör det möjligt för mottagaren att bedöma i vilken grad de operativa personuppgifterna är riktiga, fullständiga och tillförlitliga samt i vilken utsträckning de är aktuella.

3. Om det visar sig att felaktiga operativa personuppgifter har överförts eller att operativa personuppgifter olagligen har överförts, ska mottagaren omedelbart underrättas om detta. I sådana fall ska de operativa personuppgifterna i fråga rättas eller raderas eller behandlingen begränsas i enlighet med artikel 82.

Artikel 75

Särskilda villkor för uppgiftsbehandling

1. När den unionsrätt som är tillämplig på den personuppgiftsansvarige som överför uppgifter fastställer särskilda villkor för behandling, ska den personuppgiftsansvarige informera mottagaren av de operativa personuppgifterna om dessa särskilda villkor och om kravet att uppfylla dem.

2. Den personuppgiftsansvarige ska rätta sig efter de särskilda behandlingsvillkor för behandlingen som anges av en överförande behörig myndighet i enlighet med artikel 9.3 och 9.4 i direktiv (EU) 2016/680.

Artikel 76

Behandling av särskilda kategorier av operativa personuppgifter

1. Behandling av operativa personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt behandling av genetiska uppgifter, biometriska uppgifter för att unikt identifiera en fysisk person, operativa personuppgifter om hälsa eller om en fysisk persons sexualliv eller sexuella läggning ska vara tillåten endast om det är absolut nödvändigt för operativa ändamål inom ramen för de berörda unionsorganens eller unionsbyråernas uppdrag samt under förutsättning att det finns lämpliga skyddsåtgärder för den registrerades rättigheter och friheter. Det ska vara förbjudet att diskriminera fysiska personer på grundval av sådana personuppgifter.

2. Dataskyddsombudet ska utan onödigt dröjsmål informeras ifall denna artikel tillämpas.

Artikel 77

Automatiserat individuellt beslutsfattande, inbegripet profilering

1. Beslut som enbart grundas på automatiserad behandling, inbegripet profilering, som har negativa rättsliga följder för den registrerade eller i betydande grad påverkar honom eller henne, ska förbjudas om de inte är tillåtna enligt unionsrätten som den personuppgiftsansvarige lyder under och som föreskriver lämpliga skyddsåtgärder för den registrerades rättigheter och friheter, åtminstone rätten till mänskligt ingripande från den personuppgiftsansvariges sida.

2. Beslut som avses i punkt 1 i den här artikeln får inte grundas på de särskilda kategorier av personuppgifter som avses i artikel 76, såvida inte lämpliga åtgärder för att skydda den registrerades rättigheter, friheter och berättigade intressen har vidtagits.

3. Profilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter enligt artikel 76 ska förbjudas i enlighet med unionsrätten.

Artikel 78

Information om och villkor för utövandet av den registrerades rättigheter

1. Den personuppgiftsansvarige ska vidta rimliga åtgärder för att tillhandahålla den registrerade all information som avses i artikel 79 och alla meddelanden enligt artiklarna 80–84 och 92 som avser behandling i en koncis, begriplig och lättillgänglig form och på ett klart och tydligt språk. Informationen ska tillhandahållas på lämpligt sätt, t.ex. elektroniskt. Som en allmän regel ska den personuppgiftsansvarige tillhandahålla informationen i samma format som begäran.

2. Den personuppgiftsansvarige ska underlätta utövandet av den registrerades rättigheter enligt artiklarna 79–84.

3. Den personuppgiftsansvarige ska utan onödigt dröjsmål skriftligen informera den registrerade om uppföljningen av hans eller hennes begäran och under alla omständigheter senast tre månader efter mottagandet av den registrerades begäran.

4. Den personuppgiftsansvarige ska tillhandahålla informationen enligt artikel 79 och alla meddelanden eller åtgärder som vidtas enligt artiklarna 80–84 och 92 kostnadsfritt. Om en registrerads begäranden är uppenbart ogrundade eller orimliga, särskilt på grund av deras repetitiva karaktär, får den personuppgiftsansvarige vägra att tillmötesgå begäran. Det ska åligga den personuppgiftsansvarige att visa att begäran är uppenbart ogrundad eller orimlig.

5. Om den personuppgiftsansvarige har rimliga skäl att betvivla identiteten hos den fysiska person som lämnar in en begäran enligt artikel 80 eller 82, får den personuppgiftsansvarige begära att ytterligare information som är nödvändig för att bekräfta den registrerades identitet ska tillhandahållas.

Artikel 79

Information som ska göras tillgänglig för eller lämnas till den registrerade

1. Den personuppgiftsansvarige ska göra åtminstone följande information tillgänglig för den registrerade:

a) Unionsorganets eller unionsbyråns identitet och kontaktuppgifter.

b) Dataskyddsombudets kontaktuppgifter.

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

d) Rätten att lämna in ett klagomål till Europeiska datatillsynsmannen samt dennes kontaktuppgifter.

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

2. Utöver den information som avses i punkt 1, ska den personuppgiftsansvarige, i specifika fall som fastställs i unionsrätten, lämna följande information till den registrerade, för att göra det möjligt för honom eller henne att utöva sina rättigheter:

a) Behandlingens rättsliga grund.

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

c) I tillämpliga fall, kategorierna av mottagare av de operativa personuppgifterna, inbegripet i tredjeländer eller internationella organisationer.

d) Vid behov ytterligare information, i synnerhet om de operativa personuppgifterna samlas in utan den registrerades vetskap.

3. Den personuppgiftsansvarige får senarelägga, begränsa eller utelämna tillhandahållandet av informationen till den registrerade enligt punkt 2, i den utsträckning och så länge en sådan åtgärd är nödvändig och proportionell i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att

a) undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden,

b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,

c) skydda medlemsstaternas allmänna säkerhet,

d) skydda medlemsstaternas nationella säkerhet,

e) skydda andra personers rättigheter och friheter, till exempel brottsoffer och vittnen.

Artikel 80

Den registrerades rätt till tillgång

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

a) Ändamålen med behandlingen och dess rättsliga grund.

b) De kategorier av operativa personuppgifter som behandlingen avser.

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

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

e) Förekomsten av rätten att av den personuppgiftsansvarige begära rättelse eller radering av operativa personuppgifter eller begränsning av behandling av operativa personuppgifter som rör den registrerade.

f) Rätten att lämna in ett klagomål till Europeiska datatillsynsmannen och dennes kontaktuppgifter.

g) Meddelande om vilka operativa personuppgifter som håller på att behandlas och all tillgänglig information om varifrån dessa uppgifter härstammar.

Artikel 81

Begränsningar av rätten till tillgång

1. Den personuppgiftsansvarige får helt eller delvis begränsa den registrerades rätt till tillgång i den utsträckning och så länge en sådan partiell eller fullständig begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att

a) undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden,

b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,

c) skydda medlemsstaternas allmänna säkerhet,

d) skydda medlemsstaternas nationella säkerhet,

e) skydda andra personers rättigheter och friheter, till exempel brottsoffer och vittnen.

2. I de fall som avses i punkt 1 ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade skriftligen om varje vägran eller begränsning av tillgång och om skälen för vägran eller begränsningen. Denna information kan utelämnas om tillhandahållandet skulle undergräva ett ändamål enligt punkt 1. Den personuppgiftsansvarige ska underrätta den registrerade om möjligheten att lämna in ett klagomål till Europeiska datatillsynsmannen eller begära rättslig prövning vid domstolen. Den personuppgiftsansvarige ska dokumentera de sakliga och rättsliga grunderna för beslutet. Denna information ska på begäran göras tillgänglig för Europeiska datatillsynsmannen.

Artikel 82

Rätt till rättelse eller radering av operativa personuppgifter och begränsning av behandling

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få felaktiga operativa personuppgifter som rör honom eller henne rättade. Med beaktande av ändamålen med behandlingen ska den registrerade ha rätt att få ofullständiga operativa personuppgifter kompletterade, inbegripet genom att tillhandahålla en kompletterande inlaga.

2. Den personuppgiftsansvarige ska radera operativa personuppgifter utan onödigt dröjsmål, och ge den registrerade rätt att få till stånd radering av operativa personuppgifter som rör honom eller henne om behandlingen står i strid med artiklarna 71, 72.1 eller 76 eller om de operativa personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

3. I stället för radering ska den personuppgiftsansvarige begränsa behandling om

a) den registrerade bestrider personuppgifternas riktighet och riktigheten eller felaktigheten inte kan fastställas, eller

b) personuppgifterna måste sparas som bevisning.

Om behandlingen begränsas enligt första stycket led a ska den personuppgiftsansvarige underrätta den registrerade innan begränsningen av behandlingen upphävs.

Begränsade uppgifter får endast behandlas för det syfte som hindrade att de raderades.

4. Den personuppgiftsansvarige ska underrätta den registrerade skriftligen om eventuell vägran att rätta eller radera operativa personuppgifter eller begränsa behandlingen och om skälen till vägran. Den personuppgiftsansvarige får helt eller delvis begränsa tillhandahållandet av sådan information i den utsträckning som en sådan begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att

a) undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden,

b) undvika menlig inverkan på förebyggande, förhindrande, utredning, upptäckt eller lagföring av brott eller verkställighet av straffrättsliga påföljder,

c) skydda medlemsstaternas allmänna säkerhet,

d) skydda medlemsstaternas nationella säkerhet,

e) skydda andra personers rättigheter och friheter, till exempel brottsoffer och vittnen.

Den personuppgiftsansvarige ska underrätta den registrerade om möjligheten att lämna in ett klagomål till Europeiska datatillsynsmannen eller begära rättslig prövning vid domstolen.

5. Den personuppgiftsansvarige ska meddela varje rättelse av oriktiga operativa personuppgifter till den behöriga myndighet från vilken de oriktiga operativa personuppgifterna kommer.

6. Den personuppgiftsansvarige ska, när operativa personuppgifter har rättats, raderats eller deras begränsats i enlighet med punkterna 1, 2 eller 3, underrätta mottagarna att mottagarna ska rätta eller radera de operativa personuppgifterna eller begränsa den behandling av de operativa personuppgifterna som utförs under deras ansvar.

Artikel 83

Rätt till tillgång inom brottsutredningar och straffrättsliga förfaranden

Om operativa personuppgifter kommer från en behörig myndighet ska unionens organ och byråer, innan beslut fattas om registrerades rätt till tillgång, kontrollera med behörig myndighet om dessa personuppgifter ingår i ett domstolsbeslut eller ett rättsligt protokoll eller ärende som behandlas i samband med brottsutredningar och straffrättsliga förfaranden i den behöriga myndighetens medlemsstat. Om så är fallet ska ett beslut om rätt till tillgång fattas i samråd och nära samarbete med den berörda behöriga myndigheten.

Artikel 84

Den registrerades utövande av rättigheter och kontroll genom Europeiska datatillsynsmannen

1. I de fall som avses i artiklarna 79.3, 81 och 82.4 får den registrerades rättigheter också utövas genom Europeiska datatillsynsmannen.

2. Den personuppgiftsansvarige ska underrätta den registrerade om hans eller hennes möjlighet att utöva sina rättigheter genom Europeiska datatillsynsmannen enligt punkt 1.

3. Om den rättighet som avses i punkt 1 utövas ska Europeiska datatillsynsmannen åtminstone underrätta den registrerade om att alla nödvändiga kontroller eller en översyn genom Europeiska datatillsynsmannen har ägt rum. Europeiska datatillsynsmannen ska även underrätta den registrerade om hans eller hennes rätt att begära rättslig prövning vid domstolen.

Artikel 85

Inbyggt dataskydd och dataskydd som standard

1. Den personuppgiftsansvarige ska, med beaktande av den senaste utvecklingen, och genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt de risker, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter som behandlingen utgör, både vid tidpunkten för beslut om vilka medel behandlingen ska utföras med och vid tidpunkten för själva behandlingen, ska genomföra lämpliga tekniska och organisatoriska åtgärder, såsom pseudonymisering, vilka är utformade för genomförande av dataskyddsprinciper, såsom uppgiftsminimering, på ett effektivt sätt och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, för att uppfylla kraven i denna förordning och rättsakten om dess inrättande och skydda de registrerades rättigheter.

2. Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast operativa personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade operativa personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att operativa personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

Artikel 86

Gemensamt personuppgiftsansvariga

1. Om två eller flera personuppgiftsansvariga eller en eller flera personuppgiftsansvariga tillsammans med en eller flera personuppgiftsansvariga som inte är unionsinstitutioner och unionsorgan, tillsammans fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. De 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 artikel 79, genom ett inbördes arrangemang, såvida inte och i den mån som de personuppgiftsansvarigas respektive skyldigheter fastställs i unionsrätten eller en medlemsstats nationella rätt som de gemensamt 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 den registrerade. Det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade.

3. Oavsett formerna för det arrangemang som avses i punkt 1 får den registrerade utöva sina rättigheter enligt denna förordning med avseende på var och en av de personuppgiftsansvariga.

Artikel 87

Personuppgiftsbiträden

1. Om 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 rättsakten om inrättande av den personuppgiftsansvarige och säkerställer att den registrerades rättigheter skyddas.

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

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

a) endast ska handla enligt instruktioner från den personuppgiftsansvarige,

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

c) på lämpligt sätt ska bistå den personuppgiftsansvarige att säkerställa efterlevnad av bestämmelserna om den registrerades rättigheter,

d) beroende på vad den personuppgiftsansvarige väljer, ska radera eller återlämna alla operativa personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av behandlingstjänsterna har avslutats, och radera befintliga kopior, såvida inte lagring av de operativa personuppgifterna krävs enligt unionsrätten eller en medlemsstats rätt,

e) ska ge den personuppgiftsansvarige tillgång till all information som krävs för att påvisa fullgörandet av de skyldigheter som fastställs i denna artikel,

f) ska respektera de villkor som avses i punkt 2 och i denna punkt för anlitande av ett annat personuppgiftsbiträde.

4. Det avtal eller den andra rättsakt som avses i punkt 3 ska vara skriftligt, även i elektronisk form.

5. Om ett personuppgiftsbiträde i strid med denna förordning eller rättsakten om inrättande av den personuppgiftsansvarige fastställer ändamålen och medlen för behandlingen ska personuppgiftsbiträdet anses vara personuppgiftsansvarig med avseende på den behandlingen.

Artikel 88

Loggning

1. Den personuppgiftsansvarige ska föra loggar över följande typer av behandling i automatiserade behandlingssystem: insamling, ändring, åtkomst, läsning, utlämning inbegripet överföringar, sammanförande och radering av operativa personuppgifter. Loggarna över läsning och utlämning ska göra det möjligt att fastställa motivering, datum och tidpunkt för sådana åtgärder, vem som har läst eller lämnat ut operativa personuppgifter samt, i möjligaste mån, vilka som har fått tillgång till de operativa personuppgifterna.

2. Loggarna ska endast användas för att kontrollera om behandlingen är tillåten, för egenkontroll, för att säkerställa de operativa personuppgifternas integritet och säkerhet, samt inom ramen för straffrättsliga förfaranden. Sådana loggar ska raderas efter tre år, om de inte krävs för en pågående kontroll.

3. Den personuppgiftsansvarige ska på begäran göra loggarna tillgängliga för sitt dataskyddsombud och för Europeiska datatillsynsmannen.

Artikel 89

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, 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 operativa personuppgifter.

2. Den bedömning som avses i punkt 1 ska åtminstone innehålla en allmän beskrivning av den planerade behandlingen, en bedömning av riskerna för de registrerades rättigheter och friheter, de åtgärder som planeras för att hantera dessa risker, skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av operativa personuppgifter och för att visa att denna förordning efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

Artikel 90

Förhandssamråd med Europeiska datatillsynsmannen

1. Den personuppgiftsansvarige ska samråda med Europeiska datatillsynsmannen före behandling av uppgifter som kommer att ingå i ett nytt register som ska inrättas, om

a) en konsekvensbedömning avseende dataskydd enligt artikel 89 visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken, eller

b) typen av behandling, särskilt vid användning av ny teknik eller nya rutiner eller förfaranden, medför en hög risk för de registrerades rättigheter och friheter.

2. Europeiska datatillsynsmannen får upprätta en förteckning över de olika typer av uppgiftsbehandling som omfattas av förhandssamråd enligt punkt 1.

3. Den personuppgiftsansvarige ska förse Europeiska datatillsynsmannen med den konsekvensbedömning avseende dataskydd som avses i artikel 89 och, på begäran, eventuell övrig information som gör att Europeiska datatillsynsmannen kan göra en bedömning av behandlingens överensstämmelse och särskilt av riskerna för skyddet av den registrerades operativa personuppgifter och av därmed sammanhängande skyddsåtgärder.

4. Om Europeiska datatillsynsmannen anser att den planerade behandling som avses i punkt 1 skulle stå i strid med denna förordning eller rättsakten om inrättande av unionsorganet eller unionsbyrån, särskilt om den personuppgiftsansvarige inte i tillräcklig mån har fastställt eller reducerat risken, ska Europeiska datatillsynsmannen ge den personuppgiftsansvarige skriftliga råd inom en period på upp till sex veckor från det att begäran om samråd har mottagits. Denna period får förlängas med en månad beroende på hur komplicerad den planerade behandlingen är. Europeiska datatillsynsmannen ska informera den personuppgiftsansvarige om en sådan förlängning inom en månad från det att begäran om samråd har mottagits, tillsammans med orsakerna till förseningen.

Artikel 91

Säkerhet i samband med behandling av operativa personuppgifter

1. Den personuppgiftsansvarige och personuppgiftsbiträdet ska, med beaktande av den senaste utvecklingen, kostnaden för genomförande, behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, i synnerhet när det gäller behandling av särskilda kategorier av operativa personuppgifter.

2. När det gäller automatiserad behandling ska den personuppgiftsansvarige och personuppgiftsbiträdet efter en utvärdering av riskerna genomföra åtgärder som är avsedda att

a) vägra varje obehörig person åtkomst till utrustning för databehandling som används för behandling (åtkomstskydd för utrustning),

b) förhindra att databärare läses, kopieras, ändras eller avlägsnas av obehöriga (kontroll av datamedier),

c) förhindra obehörig registrering av operativa personuppgifter och obehörig åtkomst till, ändring av eller radering av lagrade operativa personuppgifter (lagringskontroll),

d) förhindra att obehöriga kan använda automatiserade behandlingssystem med hjälp av utrustning för dataöverföring (användarkontroll),

e) säkerställa att personer som är behöriga att använda ett automatiserat behandlingssystem endast har tillgång till operativa personuppgifter som omfattas av deras behörighet (åtkomstkontroll),

f) säkerställa att det kan kontrolleras och fastställas till vilka organ operativa personuppgifter har överförts eller kan överföras respektive kan göras tillgängliga med hjälp av dataöverföring (kommunikationskontroll),

g) säkerställa att det är möjligt att i efterhand kontrollera och fastställa vilka operativa personuppgifter som har förts in i ett automatiserat databehandlingssystem samt när och av vem de operativa personuppgifterna infördes (indatakontroll),

h) förhindra obehörig läsning, kopiering, ändring eller radering av operativa personuppgifter vid överföring i samband med överföring av sådana uppgifter eller under transport av databärare (transportkontroll),

i) säkerställa att de system som används kan återställas vid störningar (återställande),

j) säkerställa att system fungerar, att funktionsfel rapporteras (driftssäkerhet) och att de lagrade operativa personuppgifterna inte kan förvanskas genom funktionsfel i systemet (dataintegritet).

Artikel 92

Anmälan av en personuppgiftsincident till Europeiska datatillsynsmannen

1. Den personuppgiftsansvarige ska vid en personuppgiftsincident utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om incidenten, 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. Den anmälan som avses i punkt 1 ska åtminstone

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

3. Om och i den utsträckning som det inte är möjligt att tillhandahålla den information som avses i punkt 2 samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

4. Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter som avses i punkt 1, 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.

5. Om personuppgiftsincidenten rör operativa personuppgifter som har överförts av eller till de behöriga myndigheterna ska den personuppgiftsansvarige förmedla den information som avses i punkt 2 till de berörda behöriga myndigheterna utan onödigt dröjsmål.

Artikel 93

Information till den registrerade om en personuppgiftsincident

1. Om personuppgiftsincidenten sannolikt kommer att leda 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 de rekommendationer som anges i artikel 92.2 b, c och d.

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

a) Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder, och dessa åtgärder har tillämpats på de operativa personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som gör de operativa personuppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till dem, såsom kryptering.

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

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

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

5. Den information till den registrerade som avses i punkt 1 i denna artikel får senareläggas, begränsas eller utelämnas på de villkor och av de skäl som avses i artikel 79.3.

Artikel 94

Överföring av operativa personuppgifter till tredjeländer och internationella organisationer

1. Med förbehåll för begränsningar och villkor som fastställs i rättsakterna om inrättande av unionsorganet eller unionsbyrån får den personuppgiftsansvarige överföra operativa personuppgifter till myndigheter i tredjeland eller till internationella organisationer i den mån överföringen är nödvändig för utförandet av uppdragen för den personuppgiftsansvarige och endast då villkoren i denna artikel är uppfyllda:

a) Ett kommissionsbeslut har antagit ett beslut om adekvat skyddsnivå enligt med artikel 36.3 i direktiv (EU) 2016/680, i vilket det konstateras att tredjelandet eller ett territorium eller en behandlande enhet i det tredjelandet eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå.

b) Om det inte finns något kommissionsbeslut enligt led a: En internationell överenskommelse har ingåtts mellan unionen och tredjelandet eller den internationella organisationen i enlighet med artikel 218 i EUF-fördraget, med hänsyn till lämpliga skyddsåtgärder avseende skyddet av den personliga integriteten och enskildas grundläggande fri- och rättigheter.

c) Om det inte finns något kommissionsbeslut om adekvat skyddsnivå enligt led a eller något internationellt avtal enligt led b: Ett samarbetsavtal som medger utbyte av operativa personuppgifter har ingåtts före datumet för tillämpning av rättsakten om inrättande av unionsorganet eller unionsbyrån i fråga, mellan det unionsorganet eller den unionsbyrån och det berörda tredjelandet.

2. Rättsakterna om inrättande av unionens organ och byråer får behålla eller införa mer specifika bestämmelser om villkoren för internationella överföringar av operativa personuppgifter, särskilt överföringar genom lämpliga skyddsåtgärder och undantag för specifika situationer.

3. Den personuppgiftsansvarige ska på sin webbplats offentliggöra och uppdatera en förteckning över beslut om adekvat skyddsnivå som avses i punkt 1 a, avtal, administrativa överenskommelser och andra instrument som rör överföring av operativa personuppgifter i enlighet med punkt 1.

4. Den personuppgiftsansvarige ska utförligt registrera alla överföringar som gjorts i enlighet med denna artikel.

Artikel 95

Sekretesskraven i samband med rättsliga utredningar och straffrättsliga förfaranden

Rättsakterna om inrättande av unionens organ eller byråer, när dessa utför verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget, får ålägga Europiska datatillsynsmannen att vid utövandet av sin tillsyn ta maximal hänsyn till sekretesskraven i samband med rättsliga utredningar och straffrättsliga förfaranden, i enlighet med unionsrätten eller medlemsstaternas rätt.

KAPITEL X

GENOMFÖRANDEAKTER

Artikel 96

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 XI

ÖVERSYN

Artikel 97

Översynsklausul

Senast den 30 april 2022 och vart femte år därefter ska kommissionen lägga fram en rapport för Europaparlamentet och rådet om tillämpningen av denna förordning, vid behov åtföljd av lämpliga lagstiftningsförslag.

Artikel 98

Översyn av unionsrättsakter

1. Senast den 30 april 2022 ska kommissionen se över rättsakter som antagits på grundval av de fördrag som reglerar den behandling av operativa personuppgifter som utförs av unionens organ eller byråer när de utövar verksamhet som omfattas av tredje delen avdelning V kapitel 4 eller kapitel 5 i EUF-fördraget, i syfte att:

a) bedöma deras överensstämmelse med direktiv (EU) 2016/680 och kapitel IX i denna förordning,

b) identifiera eventuella skillnader som kan hindra utbyte av operativa personuppgifter mellan å ena sidan unionens organ eller byråer när dessa utövar verksamhet på dessa områden och å andra sidan behöriga myndigheter, och

c) identifiera alla skillnader som kan skapa rättslig fragmentering av dataskyddslagstiftningen i unionen.

2. För att säkerställa enhetligt och konsekvent skydd för fysiska personer vad gäller behandling av personuppgifter, kan kommissionen på grundval av översynen lägga fram lämpliga lagstiftningsförslag särskilt, i syfte att tillämpa kapitel IX i denna förordning på Europol och Europeiska åklagarmyndigheten, inbegripet anpassningar av kapitel IX i denna förordning, vid behov.

KAPITEL XII

SLUTBESTÄMMELSER

Artikel 99

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

Förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG upphör att gälla med verkan från och med den 11 december 2018. Hänvisningar till den upphävda förordningen och det upphävda beslutet ska anses som hänvisningar till den här förordningen.

Artikel 100

Övergångsbestämmelser

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

([1]) 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).

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

3. Artikel 53.4, 53.5 och 53.7 samt artiklarna 55 och 56 i denna förordning ska tillämpas på den nuvarande biträdande datatillsynsmannen fram till utgången av dennes mandatperiod.

4. Den biträdande datatillsynsmannen ska biträda datatillsynsmannen i fullgörandet av 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.

Artikel 101

Ikraftträdande och tillämpning

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

2. Denna förordning ska dock tillämpas på Eurojusts behandling av personuppgifter från och med den 12 december 2019.

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

Utfärdad i Strasbourg den 23 oktober 2018.

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*
A. TAJANI	K. EDTSTADLER