

Europeiska unionens officiella tidning

L 119



Svensk utgåva

Lagstiftning

femtionionde årgången

4 maj 2016

Innehållsförteckning

I Lagstiftningsakter

FÖRORDNINGAR

- ★ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) ⁽¹⁾ 1

DIREKTIV

- ★ Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF 89
- ★ Europaparlamentets och rådets direktiv (EU) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet 132

⁽¹⁾ Text av betydelse för EES

SV

De rättsakter vilkas titlar är tryckta med fin stil är sådana rättsakter som har avseende på den löpande handläggningen av jordbrukspolitiska frågor. De har normalt begränsad giltighetstid.

Beträffande alla övriga rättsakter gäller att titlarna är tryckta med fet stil och föregås av en asterisk.

I

(Lagstiftningsakter)

FÖRORDNINGAR

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679

av den 27 april 2016

om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ⁽¹⁾,med beaktande av Regionkommitténs yttrande ⁽²⁾,i enlighet med det ordinarie lagstiftningsförfarandet ⁽³⁾, och

av följande skäl:

- (1) Skyddet för fysiska personer vid behandling av personuppgifter är en grundläggande rättighet. Artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) och artikel 16.1 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) föreskriver att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.
- (2) Principerna och reglerna för skyddet för fysiska personer vid behandling av deras personuppgifter bör, oavsett deras medborgarskap eller hemvist, respektera deras grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Avsikten med denna förordning är att bidra till att skapa ett område med frihet, säkerhet och rättvisa och en ekonomisk union, till ekonomiska och sociala framsteg, till förstärkning och konvergens av ekonomierna inom den inre marknaden samt till fysiska personers välbefinnande.
- (3) Europaparlamentets och rådets direktiv 95/46/EG ⁽⁴⁾ syftar till att harmonisera skyddet av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter och att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna.

⁽¹⁾ EUT C 229, 31.7.2012, s. 90.⁽²⁾ EUT C 391, 18.12.2012, s. 127.⁽³⁾ Europaparlamentets ståndpunkt av den 12 mars 2014 (ännu ej offentliggjord i EUT) och rådets ståndpunkt vid första behandlingen av den 8 april 2016 (ännu ej offentliggjord i EUT). Europaparlamentets ståndpunkt av den 14 april 2016.⁽⁴⁾ Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).

- (4) Behandlingen av personuppgifter bör utformas så att den tjänar människor. Rätten till skydd av personuppgifter är inte en absolut rättighet; den måste förstås utifrån sin uppgift i samhället och vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen. Denna förordning respekterar alla grundläggande rättigheter och iakttar de friheter och principer som erkänns i stadgan, såsom de fastställts i fördragen, särskilt skydd för privat- och familjeliv, bostad och kommunikationer, skydd av personuppgifter, tankefrihet, samvetsfrihet och religionsfrihet, yttrande- och informationsfrihet, näringsfrihet, rätten till ett effektivt rättsmedel och en opartisk domstol samt kulturell, religiös och språklig mångfald.
- (5) Den ekonomiska och sociala integration som uppstått tack vare den inre marknaden har lett till en betydande ökning av de gränsöverskridande flödena av personuppgifter. Utbytet av personuppgifter mellan offentliga och privata aktörer, inbegripet fysiska personer, sammanslutningar och företag, över hela unionen har ökat. Nationella myndigheter i medlemsstaterna uppmanas i unionsrätten att samarbeta och utbyta personuppgifter för att vara i stånd att fullgöra sina uppdrag eller utföra arbetsuppgifter för en myndighet som finns i en annan medlemsstat.
- (6) Den snabba tekniska utvecklingen och globaliseringen har skapat nya utmaningar vad gäller skyddet av personuppgifter. Omfattningen av insamling och delning av personuppgifter har ökat avsevärt. Tekniken gör det möjligt för både privata företag och offentliga myndigheter att i sitt arbete använda sig av personuppgifter i en helt ny omfattning. Allt fler fysiska personer gör sina personliga uppgifter allmänt tillgängliga, världen över. Tekniken har omvandlat både ekonomin och det sociala livet, och bör ytterligare underlätta det fria flödet av personuppgifter inom unionen samt överföringar till tredjeländer och internationella organisationer, samtidigt som en hög skyddsnivå säkerställs för personuppgifter.
- (7) Dessa förändringar kräver en stark och mer sammanhängande ram för dataskyddet inom unionen, uppbackad av kraftfullt tillsynsarbete, eftersom det är viktigt att skapa den tillit som behövs för att utveckla den digitala ekonomin över hela den inre marknaden. Fysiska personer bör ha kontroll över sina egna personuppgifter. Den rättsliga säkerheten och smidigheten för fysiska personer, ekonomiska operatörer och myndigheter bör stärkas.
- (8) Om denna förordning föreskriver förtydliganden eller begränsningar av dess bestämmelser genom medlemsstaternas nationella rätt, kan medlemsstaterna, i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga för de personer som de tillämpas på, införliva delar av denna förordning i nationell rätt.
- (9) Målen och principerna för direktiv 95/46/EG är fortfarande giltiga, men det har inte kunnat förhindra bristande enhetlighet i genomförandet av dataskyddet i olika delar av unionen, rättsosäkerhet eller allmänt spridda uppfattningar om att betydande risker kvarstår för fysiska personer, särskilt med avseende på användning av internet. Skillnader i nivån på skyddet av fysiska personers rättigheter och friheter, särskilt rätten till skydd av personuppgifter, vid behandling av personuppgifter i olika medlemsstater kan förhindra det fria flödet av personuppgifter över hela unionen. Dessa skillnader kan därför utgöra ett hinder för att bedriva ekonomisk verksamhet på unionsnivå, de kan snedvrida konkurrensen och hindra myndigheterna att fullgöra sina skyldigheter enligt unionsrätten. De varierande skyddsnivåerna beror på skillnader i genomförandet och tillämpningen av direktiv 95/46/EG.
- (10) För att säkra en enhetlig och hög skyddsnivå för fysiska personer och för att undanröja hindren för flödena av personuppgifter inom unionen bör nivån på skyddet av fysiska personers rättigheter och friheter vid behandling av personuppgifter vara likvärdig i alla medlemsstater. En konsekvent och enhetlig tillämpning av bestämmelserna om skydd av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter bör säkerställas i hela unionen. Vad gäller behandlingen av personuppgifter för att fullgöra en rättslig förpliktelse, för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som utförs av den personuppgiftsansvarige, bör medlemsstaterna tillåtas att behålla eller införa nationella bestämmelser för att närmare fastställa hur bestämmelserna i denna förordning ska tillämpas. Jämte den allmänna och övergripande lagstiftning om dataskydd varigenom direktiv 95/46/EG genomförs har medlemsstaterna flera sektorsspecifika lagar på områden som kräver mer specifika bestämmelser. Denna förordning ger dessutom medlemsstaterna handlingsutrymme att specificera sina bestämmelser, även för behandlingen av särskilda kategorier av personuppgifter (nedan kallade *känsliga uppgifter*). Denna förordning utesluter inte att det i medlemsstaternas nationella rätt fastställs närmare omständigheter för specifika situationer där uppgifter behandlas, inbegripet mer exakta villkor för laglig behandling av personuppgifter.

- (11) Ett effektivt skydd av personuppgifter över hela unionen förutsätter att de registrerades rättigheter förstärks och specificeras och att de personuppgiftsansvarigas och personuppgiftsbiträdenas skyldigheter vid behandling av personuppgifter klargörs, samt att det finns likvärdiga befogenheter för övervakning och att det säkerställs att reglerna för skyddet av personuppgifter efterlevs och att sanktionerna för överträdelser är likvärdiga i medlemsstaterna.
- (12) I artikel 16.2 i EUF-fördraget bemyndigas Europaparlamentet och rådet att fastställa bestämmelser om skydd för fysiska personer när det gäller behandling av personuppgifter och bestämmelser om den fria rörligheten för personuppgifter.
- (13) För att säkerställa en enhetlig nivå för skyddet av fysiska personer över hela unionen och undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden behövs en förordning som skapar rättslig säkerhet och öppenhet för ekonomiska aktörer, däribland mikroföretag samt små och medelstora företag, och som ger fysiska personer i alla medlemsstater samma rättsligt verkställbara rättigheter och skyldigheter samt ålägger personuppgiftsansvariga och personuppgiftsbiträden samma ansvar, så att övervakningen av behandling av personuppgifter blir enhetlig, sanktionerna i alla medlemsstater likvärdiga och samarbetet mellan tillsynsmyndigheterna i olika medlemsstater effektivt. För att den inre marknaden ska fungera väl krävs att det fria flödet av personuppgifter inom unionen inte begränsas eller förbjuds av skäl som har anknytning till skydd för fysiska personer med avseende på behandling av personuppgifter. För att ta hänsyn till mikroföretagens samt de små och medelstora företagens särskilda situation innehåller denna förordning ett undantag för organisationer som sysselsätter färre än 250 personer med avseende på registerföring. Dessutom uppmanas unionens institutioner och organ samt medlemsstaterna och deras tillsynsmyndigheter att vid tillämpningen av denna förordning ta hänsyn till mikroföretagens samt de små och medelstora företagens särskilda behov. Begreppen mikroföretag samt små och medelstora företag bör bygga på artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG⁽¹⁾.
- (14) Det skydd som ska tillhandahållas enligt denna förordning bör tillämpas på fysiska personer, oavsett medborgarskap eller hemvist, med avseende på behandling av deras personuppgifter. Denna förordning omfattar inte behandling av personuppgifter rörande juridiska personer, särskilt företag som bildats som juridiska personer, exempelvis uppgifter om namn på och typ av juridisk person samt kontaktuppgifter.
- (15) För att förhindra att det uppstår en allvarlig risk för att reglerna kringgås bör skyddet för fysiska personer vara teknikneutralt och inte vara beroende av den teknik som används. Skyddet för fysiska personer bör vara tillämpligt på både automatiserad och manuell behandling av personuppgifter, om personuppgifterna ingår i eller är avsedda att ingå i ett register. Akter eller grupper av akter samt omslag till dessa, som inte är ordnade enligt särskilda kriterier, bör inte omfattas av denna förordning.
- (16) Denna förordning är inte tillämplig på frågor som rör skyddet av grundläggande rättigheter och friheter eller det fria flödet av personuppgifter på områden som inte omfattas av unionsrätten, såsom verksamhet rörande nationell säkerhet. Denna förordning är inte tillämplig på medlemsstaternas behandling av personuppgifter när de agerar inom ramen för unionens gemensamma utrikes- och säkerhetspolitik.
- (17) Europaparlamentets och rådets förordning (EG) nr 45/2001⁽²⁾ är tillämplig på den behandling av personuppgifter som sker i unionens institutioner, organ och byråer. Förordning (EG) nr 45/2001 och de av unionens övriga rättsakter som är tillämpliga på sådan behandling av personuppgifter bör anpassas till principerna och bestämmelserna i den här förordningen och tillämpas mot bakgrund av den här förordningen. För att tillhandahålla en stark och sammanhängande ram för dataskyddet inom unionen bör nödvändiga anpassningar av förordning (EG) nr 45/2001 göras när den här förordningen har antagits, så att de båda förordningarna kan tillämpas samtidigt.
- (18) Denna förordning är inte tillämplig på fysiska personers behandling av personuppgifter som ett led i verksamhet som är helt och hållet privat eller har samband med personens hushåll och därmed saknar koppling till yrkes- eller affärsmässig verksamhet. Privat verksamhet eller verksamhet som har samband med hushållet kan omfatta

⁽¹⁾ Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (K(2003) 1422) (EUT L 124, 20.5.2003, s. 36).

⁽²⁾ Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

korrespondens och innehav av adresser, aktivitet i sociala nätverk och internetverksamhet i samband med sådan verksamhet. Denna förordning är dock tillämplig på personuppgiftsansvariga eller personuppgiftsbiträden som tillhandahåller utrustning för behandling av personuppgifter för sådan privat verksamhet eller hushållsverksamhet.

- (19) Skyddet för fysiska personer när det gäller behöriga myndigheters behandling av personuppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten och det fria flödet av sådana uppgifter, säkerställs på unionsnivå av en särskild unionsrättsakt. Därför bör denna förordning inte vara tillämplig på behandling av personuppgifter för dessa ändamål. Personuppgifter som myndigheter behandlar enligt denna förordning och som används för de ändamålen bör emellertid regleras genom en mer specifik unionsrättsakt, nämligen Europaparlamentets och rådets direktiv (EU) 2016/680⁽¹⁾. Medlemsstaterna får anförtro behöriga myndigheter i den mening som avses i direktiv (EU) 2016/680 uppgifter som inte nödvändigtvis utförs för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, så att behandlingen av personuppgifter för dessa andra ändamål, i den mån den omfattas av unionsrätten, omfattas av tillämpningsområdet för denna förordning.

Vad gäller dessa behöriga myndigheters behandling av personuppgifter för ändamål som omfattas av tillämpningsområdet för denna förordning, bör medlemsstaterna kunna bibehålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning. I sådana bestämmelser får det fastställas mer specifika krav för dessa behöriga myndigheters behandling av personuppgifter för dessa andra ändamål, med beaktande av respektive medlemsstats konstitutionella, organisatoriska och administrativa struktur. När privata organs behandling av personuppgifter omfattas av tillämpningsområdet för denna förordning, bör denna förordning ge medlemsstaterna möjlighet att, under särskilda villkor, i lag begränsa vissa skyldigheter och rättigheter, om en sådan begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda särskilda viktiga intressen, däribland allmän säkerhet samt förebyggande, förhindrande, utredning, avslöjande och lagföring av brott eller verkställande av straffrättsliga påföljder eller skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten. Detta är exempelvis relevant i samband med bekämpning av penningtvätt eller verksamhet vid kriminaltekniska laboratorier.

- (20) Eftersom denna förordning bland annat gäller för verksamhet inom domstolar och andra rättsliga myndigheter, skulle det i unionsrätt eller medlemsstaternas nationella rätt kunna anges vilken behandling och vilka förfaranden för behandling som berörs när det gäller domstolars och andra rättsliga myndigheters behandling av personuppgifter. Tillsynsmyndigheternas behörighet bör inte omfatta domstolars behandling av personuppgifter när detta sker inom ramen för domstolarnas dömande verksamhet, i syfte att säkerställa domstolsväsendets oberoende när det utför sin rättsskipande verksamhet, inbegripet när det fattar beslut. Det bör vara möjligt att anförtro tillsynen över sådan behandling av uppgifter till särskilda organ inom medlemsstaternas rättsväsen, vilka framför allt bör säkerställa efterlevnaden av bestämmelserna i denna förordning, främja domstolsväsendets medvetenhet om sina skyldigheter enligt denna förordning och hantera klagomål relaterade till sådan behandling av uppgifter.
- (21) Denna förordning påverkar inte tillämpningen av Europaparlamentets och rådets direktiv 2000/31/EG⁽²⁾, särskilt bestämmelserna om tjänsteleverande mellanhanders ansvar i artiklarna 12–15 i det direktivet. Syftet med det direktivet är att bidra till att den inre marknaden fungerar väl genom att säkerställa fri rörlighet för informations-samhällets tjänster mellan medlemsstaterna.
- (22) All behandling av personuppgifter som sker inom ramen för arbetet på personuppgiftsansvarigas eller personuppgiftsbiträdens verksamhetsställen inom unionen bör ske i överensstämmelse med denna förordning, oavsett om behandlingen i sig äger rum inom unionen. Verksamhetsställe innebär det faktiska och reella utförandet av verksamhet med hjälp av en stabil struktur. Den rättsliga formen för en sådan struktur, oavsett om det är en filial eller ett dotterföretag med status som juridisk person, bör inte vara den avgörande faktorn i detta avseende.

⁽¹⁾ Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (se sidan 89 i detta nummer av EUT).

⁽²⁾ Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden ("Direktiv om elektronisk handel") (EGT L 178, 17.7.2000, s. 1).

- (23) För att fysiska personer inte ska frångå det skydd som denna förordning ger dem bör sådan behandling av personuppgifter om registrerade personer som befinner sig i unionen vilken utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad inom unionen omfattas av denna förordning, om behandlingen avser utbudande av varor eller tjänster inom unionen till de registrerade, oavsett om detta är kopplat till en betalning. I syfte att avgöra om en personuppgiftsansvarig eller ett personuppgiftsbiträde erbjuder varor eller tjänster till registrerade som befinner sig i unionen bör man fastställa om det är uppenbart att den personuppgiftsansvarige eller personuppgiftsbiträdet avser att erbjuda tjänster till registrerade i en eller flera av unionens medlemsstater. Medan enbart åtkomlighet till den personuppgiftsansvariges, personuppgiftsbiträdets eller en mellanhands webbplats i unionen, till en e-postadress eller andra kontaktuppgifter eller användning av ett språk som allmänt används i det tredjeland där den personuppgiftsansvarige är etablerad inte är tillräckligt för att fastställa en sådan avsikt, kan faktorer som användning av ett språk eller en valuta som allmänt används i en eller flera medlemsstater med möjlighet att beställa varor och tjänster på detta andra språk, eller omnämnande av kunder eller användare som befinner sig i unionen, göra det uppenbart att den personuppgiftsansvarige avser att erbjuda varor eller tjänster till registrerade inom unionen.
- (24) Den behandling av personuppgifter som avser registrerade som befinner sig i unionen som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen bör också omfattas av denna förordning, om den hör samman med övervakningen av de registrerade personernas beteende när de befinner sig i unionen. För att avgöra huruvida en viss behandling kan anses övervaka beteendet hos registrerade, bör det fastställas om fysiska personer spåras på internet, och om personuppgifterna därefter behandlas med hjälp av teknik som profilerar fysiska personer, i synnerhet för att fatta beslut rörande honom eller henne eller för att analysera eller förutsäga hans eller hennes personliga preferenser, beteende och attityder.
- (25) Om medlemsstaternas nationella rätt är tillämplig i kraft av folkrätten, bör denna förordning också vara tillämplig på personuppgiftsansvariga som inte är etablerade inom unionen, exempelvis i en medlemsstats diplomatiska beskickning eller konsulat.
- (26) Principerna för dataskyddet bör gälla all information som rör en identifierad eller identifierbar fysisk person. Personuppgifter som har pseudonymiserats och som skulle kunna tillskrivas en fysisk person genom att kompletterande uppgifter används bör anses som uppgifter om en identifierbar fysisk person. För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel, som t.ex. utgallring, som, antingen av den personuppgiftsansvarige eller av en annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen. Principerna för dataskyddet bör därför inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar. Denna förordning berör därför inte behandling av sådan anonym information, vilket inbegriper information för statistiska ändamål eller forskningsändamål.
- (27) Denna förordning gäller inte behandling av personuppgifter rörande avlidna personer. Medlemsstaterna får fastställa bestämmelser för behandlingen av personuppgifter rörande avlidna personer.
- (28) Tillämpningen av pseudonymisering av personuppgifter kan minska riskerna för de registrerade som berörs och hjälpa personuppgiftsansvariga och personuppgiftsbiträden att fullgöra sina skyldigheter i fråga om dataskydd. Ett uttryckligt införande av *pseudonymisering* i denna förordning är inte avsett att utesluta andra åtgärder för dataskydd.
- (29) För att skapa incitament för tillämpning av pseudonymisering vid behandling av personuppgifter bör åtgärder för pseudonymisering som samtidigt medger en allmän analys vara möjliga inom samma personuppgiftsansvarigs verksamhet, när den personuppgiftsansvarige har vidtagit de tekniska och organisatoriska åtgärder som är nödvändiga för att se till att denna förordning genomförs för berörd uppgiftsbehandling och att kompletterande uppgifter för tillskrivning av personuppgifterna till en specifik registrerad person förvaras separat. Den personuppgiftsansvarige som behandlar personuppgifterna bör ange behöriga personer inom samma personuppgiftsansvarigs verksamhet.

- (30) Fysiska personer kan knytas till nätidentifikatorer som lämnas av deras utrustning, applikationer, verktyg och protokoll, t.ex. ip-adresser, kakor eller andra identifikatorer, som radiofrekvensetiketter. Detta kan efterlämna spår som, särskilt i kombination med unika identifikatorer och andra uppgifter som tas emot av serverna, kan användas för att skapa profiler för fysiska personer och identifiera dem.
- (31) Offentliga myndigheter som för sin myndighetsutövning mottar personuppgifter i enlighet med en rättslig förpliktelse, t.ex. skatte- och tullmyndigheter, finansutredningsgrupper, oberoende administrativa myndigheter eller finansmarknadsmyndigheter med ansvar för reglering och övervakning av värdepappersmarknader, bör inte betraktas som mottagare om de tar emot personuppgifter som är nödvändiga för utförandet av en särskild utredning av allmänt intresse, i enlighet med unionsrätten eller medlemstaternas nationella rätt. Offentliga myndigheters begäranden om att uppgifter ska lämnas ut ska alltid vara skriftliga och motiverade, läggas fram i enskilda fall och inte gälla hela register eller leda till att register kopplas samman. Dessa offentliga myndigheters behandling av personuppgifter bör ske i överensstämmelse med de bestämmelser för dataskydd som är tillämpliga på behandlingens ändamål.
- (32) Samtycke bör lämnas genom en entydig bekräftande handling som innebär ett frivilligt, specifikt, informerat och otvetydigt medgivande från den registrerade sida om att denne godkänner behandling av personuppgifter rörande honom eller henne, som t.ex. genom en skriftlig, inklusive elektronisk, eller muntlig förklaring. Detta kan innebära att en ruta kryssas i vid besök på en internetsida, genom val av inställningsalternativ för tjänster på informationssamhällets område eller genom någon annan förklaring eller något annat beteende som i sammanhanget tydligt visar att den registrerade godtar den avsedda behandlingen av sina personuppgifter. Tystnad, på förhand ikryssade rutor eller inaktivitet bör därför inte utgöra samtycke. Samtycket bör gälla all behandling som utförs för samma ändamål. Om behandlingen tjänar flera olika syften, bör samtycke ges för samtliga syften. Om den registrerade ska lämna sitt samtycke efter en elektronisk begäran, måste denna vara tydlig och koncis och får inte onödigtvis störa användningen av den tjänst som den avser.
- (33) Det är ofta inte möjligt att fullt ut identifiera syftet med en behandling av personuppgifter för vetenskapliga forskningsändamål i samband med insamlingen av uppgifter. Därför bör registrerade kunna ge sitt samtycke till vissa områden för vetenskaplig forskning, när vedertagna etiska standarder för vetenskaplig forskning iakttas. Registrerade bör ha möjlighet att endast lämna sitt samtycke till vissa forskningsområden eller delar av forskningsprojekt i den utsträckning det avsedda syftet medger detta.
- (34) Genetiska uppgifter bör definieras som personuppgifter som rör en fysisk persons nedärvda eller förvärvade genetiska kännetecken, vilka framgår av en analys av ett biologiskt prov från den fysiska personen i fråga, framför allt kromosom-, DNA- eller RNA-analys eller av en annan form av analys som gör det möjligt att inhämta motsvarande information.
- (35) Personuppgifter om hälsa bör innefatta alla de uppgifter som hänför sig till en registrerad persons hälsotillstånd som ger information om den registrerades tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd. Detta inkluderar uppgifter om den fysiska personen som insamlats i samband med registrering för eller tillhandahållande av hälso- och sjukvårdstjänster till den fysiska personen enligt Europaparlamentets och rådets direktiv 2011/24/EU ⁽¹⁾, ett nummer, en symbol eller ett kännetecken som den fysiska personen tilldelats för att identifiera denne för hälso- och sjukvårdsändamål, uppgifter som härrör från tester eller undersökning av en kroppsdelen eller kroppssubstans, däribland genetiska uppgifter och biologiska prov, och andra uppgifter om exempelvis sjukdom, funktionshinder, sjukdomsrisk, sjukdomshistoria, klinisk behandling eller den registrerades fysiologiska eller biomedicinska tillstånd, oberoende av källan, exempelvis från en läkare eller från annan sjukvårdspersonal, ett sjukhus, en medicinteknisk produkt eller ett diagnostiskt in vitro-test.
- (36) Den personuppgiftsansvariges huvudsakliga verksamhetsställe i unionen bör vara den plats i unionen där den personuppgiftsansvarige har sin centrala förvaltning, såvida inte beslut om ändamålen och medlen för behandling av personuppgifter fattas vid ett annat av den personuppgiftsansvariges verksamhetsställen i unionen; i sådant fall

⁽¹⁾ Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).

bör det andra verksamhetsstället anses vara det huvudsakliga verksamhetsstället. En personuppgiftsansvarigs huvudsakliga verksamhetsställe inom unionen bör avgöras med beaktande av objektiva kriterier och bör inbegripa den faktiska och reella ledning som fattar de huvudsakliga besluten vad avser ändamål och medel för behandlingen med hjälp av en stabil struktur. Detta kriterium bör inte vara avhängigt av om behandlingen av personuppgifter utförs på detta ställe. Att tekniska medel och teknik för behandling av personuppgifter eller behandlingsverksamhet finns och används visar i sig inte att det rör sig om ett huvudsakligt verksamhetsställe och utgör därför inte avgörande kriterier för ett huvudsakligt verksamhetsställe. Personuppgiftsbiträdets huvudsakliga verksamhetsställe bör vara den plats i unionen där denne har sin centrala förvaltning eller, om denne inte har någon central förvaltning inom unionen, den plats inom unionen där den huvudsakliga behandlingen sker. I fall som omfattar både en personuppgiftsansvarig och ett personuppgiftsbiträde bör den behöriga ansvariga tillsynsmyndigheten fortfarande vara tillsynsmyndigheten i den medlemsstat där den personuppgiftsansvarige har sitt huvudsakliga verksamhetsställe, men den tillsynsmyndighet som gäller för personuppgiftsbiträdet bör betraktas som en berörd tillsynsmyndighet och den tillsynsmyndigheten bör delta i det samarbetsförfarande som föreskrivs i denna förordning. Om utkastet till beslut endast gäller den personuppgiftsansvarige, bör tillsynsmyndigheterna i den eller de medlemsstater där personuppgiftsbiträdet har ett eller flera verksamhetsställen inte under några omständigheter betraktas som berörda tillsynsmyndigheter. Om behandlingen utförs av en koncern bör det kontrollerande företagets huvudsakliga verksamhetsställe betraktas som koncernens huvudsakliga verksamhetsställe, utom då behandlingens ändamål och de medel med vilka den utförs fastställs av ett annat företag.

- (37) En koncern bör innefatta ett kontrollerande företag och de företag som detta företag kontrollerar (kontrollerade företag), varvid det kontrollerande företaget bör vara det företag som kan utöva ett dominerande inflytande på de övriga företagen i kraft av exempelvis ägarskap, finansiellt deltagande eller de bestämmelser som det regleras av eller befogenheten att införa regler som rör personuppgiftsskyddet. Ett företag med kontroll över behandlingen av personuppgifter vid företag som är underställda detta företag bör, tillsammans med dessa företag, anses utgöra en koncern.
- (38) Barns personuppgifter förtjänar särskilt skydd, eftersom barn kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder samt om sina rättigheter när det gäller behandling av personuppgifter. Sådant särskilt skydd bör i synnerhet gälla användningen av barns personuppgifter i marknadsföringssyfte eller för att skapa personlighets- eller användarprofiler samt insamling av personuppgifter med avseende på barn när tjänster som erbjuds direkt till barn utnyttjas. Samtycke från den person som har föräldraansvar över ett barn bör inte krävas för förebyggande eller rådgivande tjänster som erbjuds direkt till barn.
- (39) Varje behandling av personuppgifter måste vara laglig och rättvis. Det bör vara klart och tydligt för fysiska personer hur personuppgifter som rör dem insamlas, används, konsulteras eller på annat sätt behandlas samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas. Öppenhetsprincipen kräver att all information och kommunikation i samband med behandlingen av dessa personuppgifter är lättillgänglig och lättbegriplig samt att ett klart och tydligt språk används. Den principen gäller framför allt informationen till registrerade om den personuppgiftsansvariges identitet och syftet med behandlingen samt ytterligare information för att sörja för en rättvis och öppen behandling för berörda fysiska personer och deras rätt att erhålla bekräftelse på och meddelande om vilka personuppgifter rörande dem som behandlas. Fysiska personer bör göras medvetna om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter och om hur de kan utöva sina rättigheter med avseende på behandlingen. De specifika ändamål som personuppgifterna behandlas för bör vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in. Personuppgifterna bör vara adekvata, relevanta och begränsade till vad som är nödvändigt för de ändamål som de behandlas för. Detta kräver i synnerhet att det tillses att den period under vilken personuppgifterna lagras är begränsad till ett strikt minimum. Personuppgifter bör endast behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel. För att säkerställa att personuppgifter inte sparas längre än nödvändigt bör den personuppgiftsansvarige införa tidsfrister för radering eller för regelbunden kontroll. Alla rimliga åtgärder bör vidtas för att rätta eller radera felaktiga uppgifter. Personuppgifter bör behandlas på ett sätt som säkerställer lämplig säkerhet och konfidentialitet för personuppgifterna samt förhindrar obehörigt tillträde till och obehörig användning av personuppgifter och den utrustning som används för behandlingen.
- (40) För att behandling ska vara laglig bör personuppgifterna behandlas efter samtycke från den berörda registrerade eller på någon annan legitim grund som fastställts i lag, antingen i denna förordning eller i annan unionsrätt eller

medlemsstaternas nationella rätt enligt denna förordning, vilket inbegriper att de rättsliga skyldigheter som åligger den personuppgiftsansvarige måste fullgöras eller att ett avtal i vilket den registrerade är part måste genomföras eller att åtgärder på begäran av den registrerade måste vidtas innan avtalet ingås.

- (41) När det i denna förordning hänvisas till en rättslig grund eller lagstiftningsåtgärd, innebär detta inte nödvändigtvis en lagstiftningsakt antagen av ett parlament, utan att detta påverkar krav som uppställs i den konstitutionella ordningen i den berörda medlemsstaten. En sådan rättslig grund eller lagstiftningsåtgärd bör dock vara tydlig och precis och dess tillämpning bör vara förutsägbar för personer som omfattas av den, i enlighet med rättspraxis vid Europeiska unionens domstol (nedan kallad *domstolen*) och Europeiska domstolen för de mänskliga rättigheterna.
- (42) När behandling sker efter samtycke från registrerade, bör personuppgiftsansvariga kunna visa att de registrerade har lämnat sitt samtycke till behandlingen. I synnerhet vid skriftliga förklaringar som rör andra frågor bör det finnas skyddsåtgärder som säkerställer att de registrerade är medvetna om att samtycke ges och om hur långt samtycket sträcker sig. I enlighet med rådets direktiv 93/13/EEG ⁽¹⁾ bör en förklaring om samtycke som den personuppgiftsansvarige i förväg formulerat tillhandahållas i en begriplig och lätt tillgänglig form, med användning av ett klart och tydligt språk och utan oskäligen villkor. För att samtycket ska vara informerat bör den registrerade känna till åtminstone den personuppgiftsansvariges identitet och syftet med den behandling för vilken personuppgifterna är avsedda. Samtycke bör inte betraktas som frivilligt om den registrerade inte har någon genuin eller fri valmöjlighet eller inte utan problem kan vägra eller ta tillbaka sitt samtycke.
- (43) För att säkerställa att samtycket lämnas frivilligt bör det inte utgöra giltig rättslig grund för behandling av personuppgifter i ett särskilt fall där det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet och det därför är osannolikt att samtycket har lämnats frivilligt när det gäller alla förhållanden som denna särskilda situation omfattar. Samtycke antas inte vara frivilligt om det inte medger att separata samtycken lämnas för olika behandlingar av personuppgifter, trots att detta är lämpligt i det enskilda fallet, eller om genomförandet av ett avtal – inbegripet tillhandahållandet av en tjänst – är avhängigt av samtycket, trots att samtycket inte är nödvändigt för ett sådant genomförande.
- (44) Behandling bör vara laglig när den är nödvändig i samband med avtal eller när det finns en avsikt att ingå ett avtal.
- (45) Behandling som grundar sig på en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller behandling som krävs för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning, bör ha en grund i unionsrätten eller i en medlemsstats nationella rätt. Denna förordning medför inte något krav på en särskild lag för varje enskild behandling. Det kan räcka med en lag som grund för flera behandlingar som bygger på en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller om behandlingen krävs för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Behandlingens syfte bör också fastställas i unionsrätten eller i medlemsstaternas nationella rätt. Därtill skulle man genom denna grund kunna ange denna förordnings allmänna villkor för laglig personuppgiftsbehandling och precisera kraven för att fastställa vem den personuppgiftsansvarige är, vilken typ av personuppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut, ändamålsbegränsningar, lagringstid samt andra åtgärder för att tillförsäkra en laglig och rättvis behandling. Unionsrätten eller medlemsstaternas nationella rätt bör också reglera frågan huruvida en personuppgiftsansvarig som utför en uppgift av allmänt intresse eller som ett led i myndighetsutövning ska vara en offentlig myndighet eller någon annan fysisk eller juridisk person som omfattas av offentlig-rättslig lagstiftning eller, om detta motiveras av allmänintresset, vilket inbegriper hälso- och sjukvårdsändamål, såsom folkhälsa och socialt skydd och förvaltning av hälso- och sjukvårdstjänster, av civilrättslig lagstiftning, exempelvis en yrkesorganisation.
- (46) Behandling av personuppgifter bör även anses laglig när den är nödvändig för att skydda ett intresse som är av avgörande betydelse för den registrerades eller en annan fysisk persons liv. Behandling av personuppgifter på

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

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

- (47) En personuppgiftsansvarigs berättigade intressen, inklusive intressena för en personuppgiftsansvarig till vilken personuppgifter får lämnas ut, eller för en tredje part, kan utgöra rättslig grund för behandling, på villkor att de registrerades intressen eller grundläggande rättigheter och friheter inte väger tyngre, med beaktande av de registrerades rimliga förväntningar till följd av förhållandet till den personuppgiftsansvarige. Ett sådant berättigat intresse kan till exempel finnas när det föreligger ett relevant och lämpligt förhållande mellan den registrerade och den personuppgiftsansvarige i sådana situationer som att den registrerade är kund hos eller arbetar för den personuppgiftsansvarige. Ett berättigat intresse kräver under alla omständigheter en noggrann bedömning, som inbegriper huruvida den registrerade vid tidpunkten för inhämtandet av personuppgifter och i samband med detta rimligen kan förvänta sig att en uppgiftsbehandling för detta ändamål kan komma att ske. Den registrerades intressen och grundläggande rättigheter skulle i synnerhet kunna väga tyngre än den personuppgiftsansvariges intressen, om personuppgifter behandlas under omständigheter där den registrerade inte rimligen kan förvänta sig någon ytterligare behandling. Med tanke på att det är lagstiftarens sak att genom lagstiftning tillhandahålla den rättsliga grunden för de offentliga myndigheternas behandling av personuppgifter, bör den rättsliga grunden inte gälla den behandling de utför som ett led i fullgörandet av sina uppgifter. Sådan behandling av personuppgifter som är absolut nödvändig för att förhindra bedrägerier utgör också ett berättigat intresse för berörd personuppgiftsansvarig. Behandling av personuppgifter för direktmarknadsföring kan betraktas som ett berättigat intresse.
- (48) Personuppgiftsansvariga som ingår i en koncern eller institutioner som är underställda ett centralt organ kan ha ett berättigat intresse att överföra personuppgifter inom koncernen för interna administrativa ändamål, bland annat för behandling av kunders eller anställdas personuppgifter. De allmänna principerna för överföring av personuppgifter, inom en koncern, till företag i tredjeland påverkas inte.
- (49) Behandling av personuppgifter utgör ett berättigat intresse för berörd personuppgiftsansvarig i den mån den är absolut nödvändig och proportionell för att säkerställa nät- och informationssäkerhet, dvs. förmågan hos ett nät eller ett informationssystem att vid en viss tillförlitlighetsnivå tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande som äventyrar tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda personuppgifter och säkerheten hos besläktade tjänster som tillhandahålls av – eller är tillgängliga via – dessa nät och system, av myndigheter, incidenthanteringsorganisationer (Cert), enheter för hantering av datasäkerhetsincidenter, tillhandahållare av elektroniska kommunikationsnät och kommunikationstjänster och tillhandahållare av säkerhetsteknik och säkerhetstjänster. Detta skulle t.ex. kunna innefatta att förhindra obehörigt tillträde till elektroniska kommunikationsnät och felaktig kodfördelning och att sätta stopp för överbelastningsattacker och skador på datasystem och elektroniska kommunikationssystem.
- (50) Behandling av personuppgifter för andra ändamål än de för vilka de ursprungligen samlades in bör endast vara tillåten, när detta är förenligt med de ändamål för vilka personuppgifterna ursprungligen samlades in. I dessa fall krävs det inte någon annan separat rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs. Om behandlingen är nödvändig för att fullgöra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som den personuppgiftsansvarige har fått i uppgift att utföra, kan unionsrätten eller medlemsstaternas nationella rätt fastställa och närmare ange för vilka uppgifter och syften ytterligare behandling bör betraktas som förenlig och laglig. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör betraktas som förenlig och laglig behandling av uppgifter. Den rättsliga grund för behandling av personuppgifter som återfinns i unionsrätten eller i medlemsstaternas nationella rätt kan också utgöra en rättslig grund för ytterligare behandling. För att fastställa om ett ändamål med den ytterligare behandlingen är förenligt med det ändamål för vilket personuppgifterna ursprungligen insamlades bör den personuppgiftsansvarige, efter att ha uppfyllt alla krav vad beträffar den ursprungliga behandlingens lagenlighet, bland annat beakta alla kopplingar mellan dessa ändamål och ändamålen med den avsedda ytterligare behandlingen, det sammanhang inom vilket personuppgifterna insamlats, särskilt de registrerades rimliga förväntningar till följd av förhållandet till den personuppgiftsansvarige i fråga om den

art, den planerade ytterligare behandlingens konsekvenser för de registrerade samt förekomsten av lämpliga skyddsåtgärder för både den ursprungliga och den planerade ytterligare behandlingen.

Om den registrerade har gett sitt medgivande eller behandlingen grundar sig på unionsrätten eller på medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa i synnerhet viktiga mål av allmänt intresse, bör den personuppgiftsansvarige tillåtas att behandla personuppgifterna ytterligare, oavsett om detta är förenligt med ändamålen eller inte. Under alla omständigheter bör tillämpningen av principerna i denna förordning, särskilt informationen till den registrerade om dessa andra ändamål och om dennes rättigheter, inbegripet rätten att göra invändningar, säkerställas. Om den personuppgiftsansvarige anmäler möjliga brott eller hot mot den allmänna säkerheten och i enskilda fall eller i flera fall som rör samma brott eller hot mot den allmänna säkerheten överför dessa personuppgifter till en behörig myndighet, ska detta betraktas som att den personuppgiftsansvarige agerar i ett berättigat intresse. Sådan överföring i den personuppgiftsansvariges berättigade intresse eller ytterligare behandling av personuppgifter bör emellertid vara förbjuden, om behandlingen inte är förenlig med lagstadgad eller yrkesmässig tystnadsplikt eller annan bindande tystnadsplikt.

- (51) Personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheterna och friheter bör åtnjuta särskilt skydd, eftersom behandling av sådana uppgifter kan innebära betydande risker för de grundläggande rättigheterna och friheterna. Dessa personuppgifter bör även inbegripa personuppgifter som avslöjar ras eller etniskt ursprung, varvid användningen av termen *ras* i denna förordning inte innebär att unionen godtar teorier som söker fastställa förekomsten av skilda människoraser. Behandling av foton bör inte systematiskt anses utgöra behandling av särskilda kategorier av personuppgifter, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person. Sådana personuppgifter bör inte behandlas, såvida inte behandling medges i särskilda fall som fastställs i denna förordning, med beaktande av att det i medlemsstaternas lagstiftning får införas särskilda bestämmelser om dataskydd för att anpassa tillämpningen av bestämmelserna i denna förordning i syfte att fullgöra en rättslig skyldighet eller en uppgift av allmänt intresse eller som ett led i myndighetsutövning som den personuppgiftsansvarige har fått i uppgift att utföra. Utöver de särskilda kraven för sådan behandling, bör de allmänna principerna och andra bestämmelser i denna förordning tillämpas, särskilt när det gäller villkoren för laglig behandling. Undantag från det allmänna förbudet att behandla sådana särskilda kategorier av personuppgifter bör uttryckligen fastställas, bland annat om den registrerade lämnar sitt uttryckliga samtycke eller för att tillgodose specifika behov, i synnerhet när behandlingen utförs inom ramen för legitima verksamheter som bedrivs av vissa sammanslutningar eller stiftelser i syfte att göra det möjligt att utöva grundläggande friheter.
- (52) Undantag från förbudet att behandla särskilda kategorier av personuppgifter bör även tillåtas om de föreskrivs i unionsrätten eller i medlemsstaternas nationella rätt och underkastas lämpliga skyddsåtgärder för att skydda personuppgifter och övriga grundläggande rättigheter, när allmänintresset motiverar detta, i synnerhet i fråga om behandling av personuppgifter inom ramen för arbetsrätt och sociallagstiftning, däribland pensioner, och för hälsosäkerhetsändamål, övervaknings- och varningssyften, förebyggande eller kontroll av smittsamma sjukdomar och andra allvarliga hot mot hälsan. Detta undantag får göras för hälsoändamål, inbegripet folkhälsa och förvaltningen av hälso- och sjukvårdstjänster, särskilt för att säkerställa kvalitet och kostnadseffektivitet i de förfaranden som används vid prövningen av ansökningar om förmåner och tjänster inom sjukförsäkringssystemet, eller för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Genom undantag bör man även tillåta behandling av sådana personuppgifter där så krävs för fastställande, utövande eller försvar av rättsliga anspråk, oavsett om detta sker inom ett domstolsförfarande eller inom ett administrativt eller ett utomrättsligt förfarande.
- (53) Särskilda kategorier av personuppgifter som förtjänar ett mer omfattande skydd bör endast behandlas i hälsorelaterade syften om detta krävs för att uppnå dessa syften och gagnar fysiska personer och samhället i stort, särskilt inom ramen för förvaltningen av tjänster för hälso- och sjukvård och social omsorg och deras system, inbegripet behandling som utförs av förvaltningen och centrala nationella hälsovårdsmyndigheter av sådana uppgifter för syften som hör samman med kvalitetskontroll, information om förvaltningen samt allmän nationell och lokal tillsyn över hälso- och sjukvårdssystemet och systemet för social omsorg och säkerställande av kontinuitet inom hälso- och sjukvård och social omsorg samt gränsöverskridande hälso- och sjukvård eller hälsosäkerhet, syften som hör samman med övervakning samt varningssyften eller för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål som baseras på unionsrätten eller på medlemsstaternas nationella rätt, vilka måste ha ett syfte av allmänt intresse, samt studier som genomförs av allmänt intresse på folkhälsoområdet. Denna förordning bör därför innehålla harmoniserade villkor för behandling av särskilda kategorier av personuppgifter om hälsa, vad gäller särskilda behov, i synnerhet när behandlingen av uppgifterna utförs för vissa hälsorelaterade syften av personer som enligt lag är underkastade

yrkesmässig tystnadsplikt. Unionsrätten eller medlemsstaternas nationella rätt bör föreskriva särskilda och lämpliga åtgärder som skyddar fysiska personers grundläggande rättigheter och personuppgifter. Medlemsstaterna bör få behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriskt uppgifter eller uppgifter om hälsa. Detta bör emellertid inte hindra det fria flödet av personuppgifter inom unionen, när villkoren tillämpas på gränsöverskridande behandling av sådana uppgifter.

- (54) På folkhälsoområdet kan det bli nödvändigt att med hänsyn till ett allmänt intresse behandla särskilda kategorier av personuppgifter utan att den registrerades samtycke inhämtas. Sådan behandling bör förutsätta lämpliga och särskilda åtgärder för att skydda fysiska personers rättigheter och friheter. I detta sammanhang bör *folkhälsa* tolkas enligt definitionen i Europaparlamentets och rådets förordning (EG) nr 1338/2008 ⁽¹⁾, nämligen alla aspekter som rör hälsosituationen, dvs. allmänhetens hälsotillstånd, inbegripet sjuklighet och funktionshinder, hälsans bestämningsskriterier, hälso- och sjukvårdsbehov, resurser inom hälso- och sjukvården, tillhandahållande av och allmän tillgång till hälso- och sjukvård, utgifter för och finansiering av hälso- och sjukvården samt dödsorsaker. Sådan behandling av uppgifter om hälsa av allmänt intresse bör inte innebära att personuppgifter behandlas för andra ändamål av tredje part, exempelvis arbetsgivare eller försäkrings- och bankföretag.
- (55) Myndigheters behandling av personuppgifter på officiellt erkända religiösa sammanslutningars vägnar i syften som fastställs i grundlag eller i folkrätten anses också grunda sig på ett allmänt intresse.
- (56) Om det för att det demokratiska systemet ska fungera i samband med allmänna val är nödvändigt att politiska partier i vissa medlemsstater samlar in personuppgifter om fysiska personers politiska uppfattningar, får behandling av sådana uppgifter tillåtas med hänsyn till ett allmänt intresse, på villkor att lämpliga skyddsåtgärder fastställs.
- (57) Om de personuppgifter som behandlas av en personuppgiftsansvarig inte gör det möjligt för denne att identifiera en fysisk person, bör den personuppgiftsansvarige inte vara tvungen att skaffa ytterligare information för att kunna identifiera den registrerade, om ändamålet endast är att följa någon av bestämmelserna i denna förordning. Den personuppgiftsansvarige bör dock inte vägra att ta emot kompletterande uppgifter som den registrerade lämnat som stöd för utövandet av sina rättigheter. Identifiering bör omfatta digital identifiering av en registrerad, till exempel genom en autentiseringsmekanism, exempelvis samma identifieringsinformation som används av den registrerade för att logga in på den nättjänst som tillhandahålls av den personuppgiftsansvarige.
- (58) Öppenhetsprincipen kräver att all information som riktar sig till allmänheten eller till registrerade är kortfattad, lättåtkomlig och lättbegriplig samt utformad på ett tydligt och enkelt språk samt att man vid behov använder visualisering. Denna information kan ges elektroniskt, exempelvis på en webbplats, när den rikts till allmänheten. Detta är särskilt relevant i situationer där mängden olika aktörer och den tekniska komplexiteten gör det svårt för den registrerade att veta och förstå om personuppgifter som rör honom eller henne samlas in, vem som gör det och för vilket syfte, exempelvis i fråga om reklam på nätet. Eftersom barn förtjänar särskilt skydd, bör all information och kommunikation som riktar sig till barn utformas på ett tydligt och enkelt språk som barnet lätt kan förstå.
- (59) Förfaranden bör fastställas som gör det lättare för registrerade att utöva sina rättigheter enligt denna förordning, inklusive mekanismer för att begära och i förekommande fall kostnadsfritt få tillgång till och erhålla rättelse eller radering av personuppgifter samt för att utöva rätten att göra invändningar. Den personuppgiftsansvarige bör också tillhandahålla hjälpmedel för elektroniskt ingivna framställningar, särskilt i fall då personuppgifter behandlas elektroniskt. Personuppgiftsansvariga bör utan onödigt dröjsmål och senast inom en månad vara skyldiga att besvara registrerades önskemål och lämna en motivering, om de inte avser att uppfylla sådana önskemål.

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

- (60) Principerna om rättvis och öppen behandling fordrar att den registrerade informeras om att behandling sker och syftet med den. Den personuppgiftsansvarige bör till den registrerade lämna all ytterligare information som krävs för att säkerställa en rättvis och öppen behandling, med beaktande av personuppgiftsbehandlings specifika omständigheter och sammanhang. Dessutom bör den registrerade informeras om förekomsten av profilering samt om konsekvenserna av sådan profilering. Om personuppgifterna samlas in från den registrerade, bör denne även informeras om huruvida han eller hon är skyldig att tillhandahålla personuppgifterna och om konsekvenserna om han eller hon inte lämnar dem. Denna information får tillhandahållas kombinerad med standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över den planerade behandlingen. Om sådana symboler visas elektroniskt bör de vara maskinläsbara.
- (61) Information om behandling av personuppgifter som rör den registrerade bör lämnas till honom eller henne vid den tidpunkt då personuppgifterna samlas in från den registrerade eller, om personuppgifterna erhålls direkt från en annan källa, inom en rimlig period, beroende på omständigheterna i fallet. Om personuppgifter legitimt kan lämnas ut till en annan mottagare, bör de registrerade informeras första gången personuppgifterna lämnas ut till denna mottagare. Om den personuppgiftsansvarige avser att behandla personuppgifter för ett annat ändamål än det för vilket uppgifterna insamlades, bör denne före ytterligare behandling informera den registrerade om detta andra syfte och lämna annan nödvändig information. Om personuppgifternas ursprung inte kan meddelas den registrerade på grund av att olika källor har använts, bör allmän information ges.
- (62) Det är dock inte nödvändigt att införa någon skyldighet att tillhandahålla information, om den registrerade redan innehar denna information, om registreringen eller utlämnandet av personuppgifterna uttryckligen föreskrivs i lag eller om det visar sig vara omöjligt eller skulle medföra orimliga ansträngningar att tillhandahålla den registrerade informationen. Det sistnämnda skulle särskilt kunna vara fallet om behandlingen sker för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. I detta avseende bör antalet registrerade, uppgifternas ålder och lämpliga skyddsåtgärder beaktas.
- (63) Den registrerade bör ha rätt att få tillgång till personuppgifter som insamlats om denne samt på enkelt sätt och med rimliga intervall kunna utöva denna rätt, för att vara medveten om att behandling sker och kunna kontrollera att den är laglig. Detta innefattar rätten för registrerade att få tillgång till uppgifter om sin hälsa, exempelvis uppgifter i läkarjournaler med t.ex. diagnoser, undersökningsresultat, bedömningar av behandlande läkare och eventuella vårdbehandlingar eller interventioner. Alla registrerade bör därför ha rätt att få kännedom och underrättelse om framför allt orsaken till att personuppgifterna behandlas, om möjligt vilken tidsperiod behandlingen pågår, vilka som mottar personuppgifterna, bakomliggande logik i samband med automatisk behandling av personuppgifter och, åtminstone när behandlingen bygger på profilering, konsekvenserna av sådan behandling. Om möjligt bör den personuppgiftsansvarige kunna ge fjärråtkomst till ett säkert system genom vilket den registrerade kan få direkt åtkomst till sina personuppgifter. Denna rätt bör inte inverka menligt på andras rättigheter eller friheter, t.ex. affärshemligheter eller immateriell äganderätt och särskilt inte på upphovsrätt som skyddar programvaran. Resultatet av dessa överväganden bör dock inte bli att den registrerade förvägras all information. Om den personuppgiftsansvarige behandlar en stor mängd uppgifter om den registrerade, bör den personuppgiftsansvarige kunna begära att den registrerade lämnar uppgift om vilken information eller vilken behandling en framställan avser, innan informationen lämnas ut.
- (64) Personuppgiftsansvariga bör vidta alla rimliga åtgärder för att kontrollera identiteten på en registrerad som begär tillgång, särskilt inom ramen för nättjänster och i fråga om nätidentifierare. Personuppgiftsansvariga bör inte behålla personuppgifter enbart för att kunna agera vid en potentiell begäran.
- (65) Den registrerade bör ha rätt att få sina personuppgifter rättade och en rätt att bli bortglömd, om lagringen av uppgifterna strider mot denna förordning eller unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av. En registrerad bör särskilt ha rätt att få sina personuppgifter raderade och kunna begära att dessa personuppgifter inte behandlas, om de inte längre behövs med tanke på de ändamål för vilka de samlats in eller på annat sätt behandlats, om en registrerad har återtagit sitt samtycke till behandling eller invänder mot behandling av personuppgifter som rör honom eller henne, eller om behandlingen av hans eller

hennes personuppgifter på annat sätt inte överensstämmer med denna förordning. Denna rättighet är särskilt relevant när den registrerade har gett sitt samtycke som barn, utan att vara fullständigt medveten om riskerna med behandlingen, och senare vill ta bort dessa personuppgifter, särskilt på internet. Den registrerade bör kunna utöva denna rätt även när han eller hon inte längre är barn. Ytterligare lagring av personuppgifterna bör dock vara laglig, om detta krävs för att utöva yttrandefrihet och informationsfrihet, för att uppfylla en rättslig förpliktelse, för att utföra en uppgift i av allmänt intresse eller som ett led i myndighetsutövning som anförtrots den personuppgiftsansvarige, med anledning av ett allmänt intresse inom folkhälsoområdet, för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål eller för fastställande, utövande eller försvar av rättsliga anspråk.

- (66) För att stärka "rätten att bli bortglömd" i nätmiljön bör rätten till radering utvidgas genom att personuppgiftsansvariga som offentliggjort personuppgifter är förpliktigade att vidta rimliga åtgärder, däribland tekniska åtgärder, för att informera de personuppgiftsansvariga som behandlar dessa personuppgifter om att den registrerade har begärt radering av alla länkar till och kopior eller reproduktioner av dessa personuppgifter. I samband med detta bör den personuppgiftsansvarige vidta rimliga åtgärder, med beaktande av tillgänglig teknik och de hjälpmedel som står den personuppgiftsansvarige till buds, däribland tekniska åtgärder, för att informera de personuppgiftsansvariga som behandlar personuppgifterna om den registrerades begäran.
- (67) Sätten att begränsa behandlingen av personuppgifter kan bland annat innebära att man tillfälligt flyttar de valda personuppgifterna till ett annat databehandlingssystem, gör de valda uppgifterna otillgängliga för användare eller tillfälligt avlägsnar offentliggjorda uppgifter från en webbplats. I automatiserade register bör begränsningen av behandlingen i princip ske med tekniska medel på ett sådant sätt att personuppgifterna inte blir föremål för ytterligare behandling och inte kan ändras. Det förhållande att behandlingen av personuppgifter är begränsad bör klart anges inom systemet.
- (68) För att ytterligare förbättra kontrollen över sina egna uppgifter bör den registrerade, om personuppgifterna behandlas automatiskt, också tillåtas att motta de personuppgifter som rör honom eller henne, som han eller hon har tillhandahållit den personuppgiftsansvarige, i ett strukturerat, allmänt använt, maskinläsbart och kompatibelt format och överföra dessa till en annan personuppgiftsansvarig. Personuppgiftsansvariga bör uppmuntras att utveckla kompatibla format som möjliggör dataportabilitet. Denna rättighet bör vara tillämplig om den registrerade har tillhandahållit uppgifterna efter att ha lämnat sitt samtycke eller om behandlingen är nödvändig för att ett avtal ska kunna genomföras. Den bör inte vara tillämplig om behandlingen utgår från en annan rättslig grund än samtycke eller avtal. På grund av sin art bör denna rättighet inte utövas mot personuppgiftsansvariga som behandlar personuppgifter som ett led i myndighetsutövning. Därför bör den inte vara tillämplig när behandlingen av personuppgifterna är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som utförs av den personuppgiftsansvarige. Den registrerades rätt att överföra eller motta personuppgifter som rör honom eller henne innebär inte någon skyldighet för de personuppgiftsansvariga att införa eller upprätthålla behandlingssystem som är tekniskt kompatibla. Om mer än en registrerad berörs inom en viss uppsättning personuppgifter, bör rätten att motta personuppgifterna inte inverka på andra registrerades rättigheter och friheter enligt denna förordning. Denna rättighet bör inte heller påverka den registrerades rätt att få till stånd radering av personuppgifter och de inskränkningar av denna rättighet vilka anges i denna förordning och bör i synnerhet inte medföra radering av personuppgifter om den registrerade som denne har lämnat för genomförande av ett avtal, i den utsträckning och så länge som personuppgifterna krävs för genomförande av avtalet. Om det är tekniskt möjligt, bör den registrerade ha rätt till direkt överföring av personuppgifterna från en personuppgiftsansvarig till en annan.
- (69) När personuppgifter lagligen får behandlas, eftersom behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i en myndighetsutövning som utförs av den personuppgiftsansvarige, eller på grund av en personuppgiftsansvarigs eller en tredje parts berättigade intressen, bör alla registrerade ändå ha rätt att göra invändningar mot behandling av personuppgifter som rör de registrerades särskilda situation. Det bör ankomma på den personuppgiftsansvarige att visa att dennes tvingande berättigade intressen väger tyngre än den registrerades intressen eller grundläggande rättigheter och friheter.
- (70) Om personuppgifter behandlas för direktmarknadsföring, bör den registrerade, oavsett om det handlar om inledande eller ytterligare behandling, ha rätt att när som helst kostnadsfritt invända mot sådan behandling, inbegripet profilering, i den mån denna är kopplad till direktmarknadsföring. Denna rättighet bör uttryckligen meddelas den registrerade och redovisas tydligt, klart och åtskilt från annan information.

- (71) Den registrerade bör ha rätt att inte bli föremål för ett beslut, vilket kan innebära en åtgärd, med bedömning av personliga aspekter rörande honom eller henne, vilket enbart grundas på automatiserad behandling och medför rättsverkan för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne, såsom ett automatiserat avslag på en kreditansökan online eller e-rekrytering utan personlig kontakt. Sådan behandling omfattar "profilering" i form av automatisk behandling av personuppgifter med bedömning av personliga aspekter rörande en fysisk person, särskilt för att analysera eller förutse aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar, i den mån dessa har rättsverkan rörande honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. Beslutsfattande grundat på sådan behandling, inbegripet profilering, bör dock tillåtas när det uttryckligen beviljas genom unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av, inbegripet för sådan övervakning och sådant förebyggande av bedrägerier och skatteundandragande som genomförs i enlighet med unionsinstitutionernas eller de nationella tillsynsorganens bestämmelser, standarder och rekommendationer samt för att sörja för tillförlitlighet hos en tjänst som tillhandahålls av den personuppgiftsansvarige, eller när det krävs för ingående eller genomförande av ett avtal mellan den registrerade och en personuppgiftsansvarig eller den registrerade har gett sitt uttryckliga samtycke. Denna form av uppgiftsbehandling bör under alla omständigheter omgärdas av lämpliga skyddsåtgärder, som bör inkludera specifik information till den registrerade och rätt till mänskligt ingripande, att framföra sina synpunkter, att erhålla en förklaring till det beslut som fattas efter sådan bedömning och att överklaga beslutet. Sådana åtgärder bör inte gälla barn.

I syfte att sörja för rättvis och transparent behandling med avseende på den registrerade, med beaktande av omständigheterna och det sammanhang i vilket personuppgifterna behandlas, bör den personuppgiftsansvarige använda adekvata matematiska eller statistiska förfaranden för profilering, genomföra tekniska och organisatoriska åtgärder som framför allt säkerställer att faktorer som kan medföra felaktigheter i personuppgifter korrigeras och att risken för fel minimeras samt säkra personuppgifterna på sådant sätt att man beaktar potentiella risker för den registrerades intressen och rättigheter och förhindrar bland annat diskriminerande effekter för fysiska personer, på grund av ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse, medlemskap i fackföreningar, genetisk status eller hälsostatus eller sexuell läggning, eller som leder till åtgärder som får sådana effekter. Automatiserat beslutsfattande och profilering baserat på särskilda kategorier av personuppgifter bör endast tillåtas på särskilda villkor.

- (72) Profilering omfattas av denna förordnings bestämmelser om behandling av personuppgifter, såsom de rättsliga grunderna för behandlingen och principer för dataskydd. Europeiska dataskyddsstyrelsen som inrättas genom denna förordning (nedan kallad *styrelsen*) bör kunna utfärda riktlinjer i detta avseende.
- (73) Begränsningar med avseende på specifika principer och rätten till information, tillgång till och rättelse eller radering av personuppgifter, rätten till dataportabilitet, rätten att göra invändningar, profileringsbaserade beslut samt information till den registrerade om personuppgiftsincidenter och vissa av den personuppgiftsansvariges relaterade skyldigheter kan införas genom unionsrätten eller medlemsstaternas nationella rätt, i den mån de är nödvändiga och proportionella i ett demokratiskt samhälle för att upprätthålla den allmänna säkerheten, exempelvis för att skydda människoliv, särskilt vid naturkatastrofer eller katastrofer framkallade av människan, vid förebyggande, förhindrande, utredning och lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten eller överträdelser av etiska principer för reglerade yrken, vad gäller unionens eller en medlemsstats övriga viktiga mål av allmänt intresse, särskilt om de är av stort ekonomiskt eller finansiellt intresse för unionen eller en medlemsstat, förande av offentliga register som förs av hänsyn till ett allmänt intresse, ytterligare behandling av arkiverade personuppgifter för att tillhandahålla specifik information om politiskt beteende under tidigare totalitära regimer eller skydd av den registrerade eller andras rättigheter och friheter, inklusive socialt skydd, folkhälsa och humanitära skäl. Dessa begränsningar bör överensstämma med kraven i stadgan och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.
- (74) Personuppgiftsansvariga bör åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar. Personuppgiftsansvariga bör särskilt vara skyldiga att vidta lämpliga och effektiva åtgärder och kunna visa att behandlingen är förenlig med denna förordning, även vad gäller åtgärdernas effektivitet. Man bör inom dessa åtgärder beakta behandlingens art, omfattning, sammanhang och ändamål samt risken för fysiska personers rättigheter och friheter.

- (75) Risken för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av personuppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering eller annan betydande ekonomisk eller social nackdel, om registrerade kan berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter, om personuppgifter behandlas som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i fackförening, om genetiska uppgifter, uppgifter om hälsa eller sexualliv eller fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder behandlas, om personliga aspekter bedöms, framför allt analyser eller förutsägelser beträffande sådant som rör arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlitlighet eller beteende, vistelseort eller förflyttningar, i syfte att skapa eller använda personliga profiler, om det sker behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.
- (76) Hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen inbegriper en risk eller en hög risk.
- (77) Vägledning för den personuppgiftsansvariges eller personuppgiftsbiträdets genomförande av lämpliga åtgärder och för påvisande av att behandlingen är förenlig med denna förordning, särskilt när det gäller att kartlägga den risk som är förknippad med behandlingen och bedöma dess ursprung, art, sannolikhetsgrad och allvar samt fastställa bästa praxis för att minska risken, kan framför allt ges genom godkända uppförandekoder, godkänd certifiering, riktlinjer från styrelsen eller genom anvisningar från ett dataskyddsombud. Styrelsen kan också utfärda riktlinjer för uppgiftsbehandling som inte bedöms medföra någon hög risk för fysiska personers rättigheter och friheter samt ange vilka åtgärder som i sådana fall kan vara tillräckliga för att bemöta en sådan risk.
- (78) Skyddet av fysiska personers rättigheter och friheter i samband med behandling av personuppgifter förutsätter att lämpliga tekniska och organisatoriska åtgärder vidtas, så att kraven i denna förordning uppfylls. För att kunna visa att denna förordning följs bör den personuppgiftsansvarige anta interna strategier och vidta åtgärder, särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard. Sådana åtgärder kan bland annat bestå av att uppgiftsbehandlingen minimeras, att personuppgifter snarast möjligt pseudonymiseras, att öppenhet om personuppgifternas syfte och behandling iakttas, att den registrerade får möjlighet att övervaka uppgiftsbehandlingen och att den personuppgiftsansvarige får möjlighet att skapa och förbättra säkerhetsanordningar. Vid utveckling, utformning, urval och användning av applikationer, tjänster och produkter som är baserade på behandling av personuppgifter eller behandlar personuppgifter för att uppfylla sitt syfte bör producenterna av dessa produkter, tjänster och applikationer uppmanas att beakta rätten till dataskydd när sådana produkter, tjänster och applikationer utvecklas och utformas och att, med tillbörlig hänsyn till den tekniska utvecklingen, säkerställa att personuppgiftsansvariga och personuppgiftsbiträden kan fullgöra sina skyldigheter avseende dataskydd. Principerna om inbyggt dataskydd och dataskydd som standard bör också beaktas vid offentliga upphandlingar.
- (79) Skyddet av de registrerades rättigheter och friheter samt de personuppgiftsansvarigas och personuppgiftsbiträdenas ansvar, även i förhållande till tillsynsmyndigheternas övervakning och åtgärder, kräver ett tydligt fastställande av vem som bär ansvaret enligt denna förordning, bl.a. när personuppgiftsansvariga gemensamt fastställer ändamål och medel för en behandling tillsammans med andra personuppgiftsansvariga eller när en behandling utförs på en personuppgiftsansvarigs vägnar.
- (80) När personuppgiftsansvariga eller personuppgiftsbiträden som inte är etablerade inom unionen behandlar personuppgifter om registrerade som befinner sig inom unionen och det bakomliggande syftet med uppgiftsbehandlingen är att erbjuda de registrerade personerna i unionen varor eller tjänster, oberoende av om de registrerade personerna måste betala för dem, eller att övervaka deras beteende i den mån beteendet äger rum i unionen, bör de personuppgiftsansvariga eller personuppgiftsbiträdena utnämna en företrädare, såvida inte behandlingen endast är tillfällig, inte omfattar behandling i särskilda kategorier av särskilda kategorier av personuppgifter eller behandling av personuppgifter om fällande domar i brottmål samt överträdelser och det är

osannolikt att den inbegriper en risk för fysiska personers rättigheter och friheter, med beaktande av behandlingens art, sammanhang, omfattning och ändamål eller om den personuppgiftsansvarige är en myndighet eller ett organ. Företrädaren bör agera på den personuppgiftsansvariges eller på personuppgiftsbitrådets vägnar och kan kontaktas av samtliga tillsynsmyndigheter. Företrädaren bör uttryckligen utses genom en skriftlig fullmakt från den personuppgiftsansvarige eller från personuppgiftsbitrådet att agera på dennes vägnar med avseende på dennes skyldigheter enligt denna förordning. Utnämningen av företrädaren inverkar inte på den personuppgiftsansvariges eller på personuppgiftsbitrådets ansvar enligt denna förordning. Företrädaren bör utföra sina uppgifter i enlighet med erhållen fullmakt från den personuppgiftsansvarige eller från personuppgiftsbitrådet, vilket inbegriper samarbete med de behöriga tillsynsmyndigheterna i fråga om alla åtgärder som vidtas för att sörja för efterlevnad av denna förordning. Den utsedda företrädaren bör underkastas verkställighetsförfaranden i händelse den personuppgiftsansvarige eller personuppgiftsbitrådet inte uppfyller sina skyldigheter.

- (81) För att se till att kraven i denna förordning uppfylls vad gäller behandling som av ett personuppgiftsbiträde ska utföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige, när denne anförtror behandling åt ett personuppgiftsbiträde, endast använda personuppgiftsbiträden som ger tillräckliga garantier, i synnerhet i fråga om 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. Personuppgiftsbitrådets anslutning till en godkänd uppförandekod eller en godkänd certifieringsmekanism kan användas som ett sätt att påvisa att den personuppgiftsansvarige fullgör sina skyldigheter. När uppgifter behandlas av ett personuppgiftsbiträde, bör hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt mellan personuppgiftsbitrådet och den personuppgiftsansvarige, där föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade anges, med beaktande av personuppgiftsbitrådets specifika arbets- och ansvarsuppgifter inom ramen för den behandling som ska utföras och risken med avseende på den registrerades rättigheter och friheter. Den personuppgiftsansvarige och personuppgiftsbitrådet får välja att använda sig av ett enskilt avtal eller standardavtalsklausuler som antingen antas direkt av kommissionen eller av en tillsynsmyndighet i enlighet med mekanismen för enhetlighet och därefter antas av kommissionen. Efter det att behandlingen på den personuppgiftsansvariges vägnar har avslutats, bör personuppgiftsbitrådet återlämna eller radera personuppgifterna, beroende på vad den personuppgiftsansvarige väljer, såvida inte lagring av personuppgifterna krävs enligt den unionsrätt eller medlemsstaternas nationella rätt som personuppgiftsbitrådet omfattas av.
- (82) För att påvisa att denna förordning följs bör de personuppgiftsansvariga eller personuppgiftsbiträdena föra register över behandling som sker under deras ansvar. Alla personuppgiftsansvariga och personuppgiftsbiträden bör vara skyldiga att samarbeta med tillsynsmyndigheten och på dennas begäran göra detta register tillgängligt, så att det kan tjäna som grund för övervakningen av behandlingen.
- (83) För att upprätthålla säkerheten och förhindra behandling som bryter mot denna förordning bör personuppgiftsansvariga eller personuppgiftsbiträden utvärdera riskerna med behandlingen och vidta åtgärder, såsom kryptering, för att minska dem. Åtgärderna bör säkerställa en lämplig säkerhetsnivå, inbegripet konfidentialitet, med beaktande av den senaste utvecklingen och genomförandekostnader i förhållande till riskerna och vilken typ av personuppgifter som ska skyddas. Vid bedömningen av datasäkerhetsrisken bör man även beakta de risker som personuppgiftsbehandling medför, såsom förstörelse, förlust eller ändringar genom olyckshändelse eller otillåtna handlingar eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, framför allt när denna kan medföra fysisk, materiell eller immateriell skada.
- (84) I syfte att sörja för bättre efterlevnad av denna förordning när behandlingen sannolikt kan innebära en hög risk för fysiska personers rättigheter och friheter, bör den personuppgiftsansvarige vara ansvarig för att en konsekvensbedömning utförs avseende dataskydd för att bedöma framför allt riskens ursprung, art, särdrag och allvar. Resultatet av denna bedömning bör beaktas vid fastställandet av de lämpliga åtgärder som ska vidtas för att visa att behandlingen av personuppgifter är förenlig med denna förordning. I de fall en konsekvensbedömning avseende dataskydd ger vid handen att uppgiftsbehandlingen medför en hög risk, som den personuppgiftsansvarige inte kan begränsa genom lämpliga åtgärder med avseende på tillgänglig teknik och genomförandekostnader, bör ett samråd med tillsynsmyndigheten ske före behandlingen.
- (85) En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan för fysiska personer leda till fysisk, materiell eller immateriell skada, såsom förlust av kontrollen över de egna personuppgifterna eller till begränsning av deras rättigheter, diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, obehörigt hävande av pseudonymisering, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, eller till annan ekonomisk eller social nackdel för den berörda fysiska personen. Så

snart en personuppgiftsansvarig blir medveten om att en personuppgiftsincident har inträffat, bör den personuppgiftsansvarige därför anmäla personuppgiftsincidenten till tillsynsmyndigheten utan onödigt dröjsmål och, om så är möjligt, inom 72 timmar efter att ha blivit medveten om denna, om inte den personuppgiftsansvarige, i enlighet med ansvarsprincipen, kan påvisa att det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter. Om en sådan anmälan inte kan ske inom 72 timmar, bör skälen till fördröjningen åtfölja anmälan och information får lämnas i omgångar utan otillbörligt vidare dröjsmål.

- (86) Den personuppgiftsansvarige bör utan onödigt dröjsmål underrätta den registrerade om en personuppgiftsincident, om personuppgiftsincidenten sannolikt kommer att medföra en hög risk för den fysiska personens rättigheter och friheter, så att denne kan vidta nödvändiga försiktighetsåtgärder. Denna underrättelse bör beskriva personuppgiftsincidentens art samt innehålla rekommendationer för den berörda fysiska personen om hur de potentiella negativa effekterna kan mildras. De registrerade bör underrättas så snart detta rimligtvis är möjligt, i nära samarbete med tillsynsmyndigheten och i enlighet med den vägledning som lämnats av den eller andra relevanta myndigheter, exempelvis brottsbekämpande myndigheter. Till exempel kräver behovet av att mildra en omedelbar skaderisk att de registrerade underrättas omedelbart, medan behovet av att vidta lämpliga åtgärder vid fortlopande eller likartade personuppgiftsincidenter däremot kan motivera längre tid för underrättelsen.
- (87) Det bör undersökas huruvida alla lämpliga tekniska skyddsåtgärder och alla lämpliga organisatoriska åtgärder har vidtagits för att omedelbart fastställa om en personuppgiftsincident har ägt rum och skyndsamt informera tillsynsmyndigheten och den registrerade. Att en anmälan gjordes utan onödigt dröjsmål bör fastställas med hänsyn tagen bl.a. till personuppgiftsincidentens art och svårighetsgrad och dess följder och negativa effekter för den registrerade. En sådan anmälan kan leda till ett ingripande från tillsynsmyndighetens sida i enlighet med dess uppgifter och befogenheter enligt denna förordning.
- (88) När ingående regler fastställs för format och förfaranden för anmälan av personuppgiftsincidenter, bör vederbörlig hänsyn tas till omständigheterna kring incidenten, däribland om personuppgifterna var skyddade av lämpliga tekniska skyddsåtgärder, som betydligt begränsar sannolikheten för identitetsbedrägeri eller andra former av missbruk. Dessutom bör sådana regler och förfaranden beakta brottsbekämpande myndigheters berättigade intressen, där en för tidig redovisning kan riskera att i onödan hämma utredning av omständigheterna kring en personuppgiftsincident.
- (89) Direktiv 95/46/EG föreskrev en allmän skyldighet att anmäla behandling av personuppgifter till tillsynsmyndigheterna. Denna skyldighet medförde administrativa och ekonomiska bördor, men förbättrade inte alltid personuppgiftsskyddet. Sådana övergripande och allmänna anmälningsskyldigheter bör därför avskaffas och ersättas av effektiva förfaranden och mekanismer som i stället inriktas på de typer av behandlingar som sannolikt innebär en hög risk för fysiska personers rättigheter och friheter, i kraft av deras art, omfattning, sammanhang och ändamål. Dessa behandlingar kan vara sådana som särskilt inbegriper användning av ny teknik eller är av en ny typ, för vilken konsekvensbedömning avseende uppgiftsskydd inte tidigare har genomförts av den personuppgiftsansvarige, eller som blir nödvändiga på grund av den tid som har förflutit sedan den ursprungliga behandlingen.
- (90) I sådana fall bör den personuppgiftsansvarige före behandlingen, med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt upphovet till risken, göra en konsekvensbedömning avseende dataskydd i syfte att bedöma den höga riskens specifika sannolikhetsgrad och allvar samt dess ursprung. Konsekvensbedömningen bör främst innefatta de planerade åtgärder, skyddsåtgärder och mekanismer som ska minska denna risk, säkerställa personuppgiftsskyddet och visa att denna förordning efterlevs.
- (91) Detta bör särskilt vara tillämpligt på storskalig uppgiftsbehandling med syftet att behandla betydande mängder personuppgifter på regional, nationell eller övernationell nivå, vilket skulle kunna påverka ett stort antal registrerade och sannolikt kommer att innebära en hög risk, exempelvis till följd av uppgifternas känsliga natur, där i enlighet med den uppnådda nivån av teknisk kunskap en ny teknik används storskaligt, samt på annan behandling som innebär en hög risk för registrerades rättigheter och friheter, framför allt när denna behandling gör det svårare för de registrerade att utöva sina rättigheter. En konsekvensbedömning avseende dataskydd bör

också göras, där personuppgifter behandlas i syfte att fatta beslut om specifika fysiska personer efter en systematisk och omfattande bedömning av fysiska personers personliga aspekter på grundval av profilering av dessa uppgifter eller efter behandling av särskilda kategorier av personuppgifter, biometriska uppgifter eller uppgifter om fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder. Likaså krävs en konsekvensbedömning avseende dataskydd för övervakning av allmän plats i stor omfattning, särskilt vid användning av optisk-elektroniska anordningar, eller för all annan behandling där den behöriga tillsynsmyndigheten anser att behandlingen sannolikt kommer att innebära en hög risk för de registrerades rättigheter och friheter, framför allt på grund av att den hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal eller på grund av att den systematiskt genomförs i stor omfattning. Behandling av personuppgifter bör inte anses vara storskalig, om det är fråga om personuppgifter från patienter eller klienter som behandlas av enskilda läkare, andra yrkesverksamma på hälsoområdet eller juridiska ombud. I dessa fall bör en konsekvensbedömning avseende dataskydd inte vara obligatorisk.

- (92) Ibland kan det vara förnuftigt och ekonomiskt att en konsekvensbedömning avseende dataskydd inriktar sig på ett vidare område än ett enda projekt, exempelvis när myndigheter eller organ avser att skapa en gemensam tillämpnings- eller behandlingsplattform eller när flera personuppgiftsansvariga planerar att införa en gemensam tillämpnings- eller behandlingsmiljö för en hel bransch eller ett helt segment eller för en allmänt utnyttjad horisontell verksamhet.
- (93) Medlemsstaterna kan anse det nödvändigt att genomföra en sådan bedömning före behandlingen i samband med antagandet av medlemsstaters nationella rätt som ligger till grund för utförandet av myndighetens eller det offentliga organets uppgifter och reglerar den aktuella specifika behandlingsåtgärden eller serien av åtgärder.
- (94) Om det av en konsekvensbedömning avseende dataskydd framgår att behandlingen utan skyddsåtgärder, säkerhetsåtgärder och mekanismer för att minska risken kommer att innebära en hög risk för fysiska personers rättigheter och friheter, och den personuppgiftsansvarige anser att risken inte kan begränsas genom åtgärder som är rimliga med avseende på tillgänglig teknik och genomförandekostnader, bör samråd hållas med tillsynsmyndigheten innan behandlingen inleds. En sådan hög risk kommer sannolikt att orsakas av vissa typer av behandling samt av en viss omfattning och frekvens för behandlingen, vilket även kan leda till skador för eller kränkningar av fysiska personers rättigheter och friheter. Tillsynsmyndigheten bör inom en fastställd tid svara på en begäran om samråd. Ett uteblivet svar från tillsynsmyndigheten inom denna tid bör dock inte hindra ett eventuellt ingripande från tillsynsmyndighetens sida i enlighet med dess uppgifter och befogenheter enligt denna förordning, inbegripet befogenheten att förbjuda behandling. Som en del av denna samrådsprocess får resultatet av en konsekvensbedömning avseende dataskydd som utförs med avseende på behandlingen i fråga överlämnas till tillsynsmyndigheten, framför allt de åtgärder som planeras för att minska risken för fysiska personers rättigheter och friheter.
- (95) Personuppgiftsbiträdet bör vid behov och på begäran bistå den personuppgiftsansvarige med fullgörande av de skyldigheter som härrör från utförandet av konsekvensbedömningar avseende dataskydd och förhandssamråd med tillsynsmyndigheten.
- (96) Ett samråd med tillsynsmyndigheten bör även ske som ett led i det förberedande arbetet med en lagstiftningsåtgärd som stadgar om behandling av personuppgifter i syfte att säkerställa att den avsedda behandlingen överensstämmer med denna förordning och framför allt för att minska den risk den medför för den registrerade.
- (97) När en behandling utförs av en myndighet, med undantag av domstolar eller oberoende rättsliga myndigheter som en del av deras dömande verksamhet, eller när en behandling utförs i den privata sektorn av en personuppgiftsansvarig vars kärnverksamhet består av behandlingsverksamhet som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller när den personuppgiftsansvariges eller personuppgiftsbitrådets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av personuppgifter och uppgifter som rör fällande domar i brottmål och överträdelser, bör en person med sakkunskap i fråga om dataskyddslagstiftning och -förfaranden bistå den personuppgiftsansvarige eller personuppgiftsbiträdet för att övervaka den interna efterlevnaden av denna förordning. I den privata sektorn avser personuppgiftsansvarigas kärnverksamhet deras primära verksamhet och inte behandling av personuppgifter som kompletterande verksamhet. Den nödvändiga nivån på sakkunskapen bör fastställas särskilt i enlighet med den uppgiftsbehandling

som utförs och det skydd som krävs för de personuppgifter som behandlas av den personuppgiftsansvarige eller personuppgiftsbiträdet. Denna typ av dataskyddsbud bör, oavsett om de är anställda av den personuppgiftsansvarige eller ej, kunna fullgöra sitt uppdrag och utföra sina uppgifter på ett oberoende sätt.

- (98) Sammanslutningar eller andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden bör uppmuntras att utarbeta uppförandekoder inom gränserna för denna förordning, så att tillämpningen av denna förordning effektiviseras, med beaktande av särdragen hos den behandling som sker inom vissa sektorer och de särskilda behov som finns inom mikroföretag samt inom små och medelstora företag. I synnerhet skulle man genom sådana uppförandekoder kunna anpassa personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter, med beaktande av den risk som behandlingen sannolikt innebär för fysiska personers rättigheter och friheter.
- (99) Vid utformningen av en uppförandekod eller vid ändring eller utvidgning av en befintlig sådan kod bör sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden samråda med berörda intressenter, i möjligaste mån inbegripet registrerade, och beakta de inlagor som mottas och de åsikter som framförs som svar på samråden.
- (100) För att förbättra öppenheten och efterlevnaden av denna förordning bör införandet av certifieringsmekanismer och dataskyddsförsegling och dataskyddsmärkning uppmuntras, så att registrerade snabbt kan bedöma nivån på relevanta produkters och tjänsters dataskydd.
- (101) Flöden av personuppgifter till och från länder utanför unionen och till och från internationella organisationer är nödvändiga för utvecklingen av internationell handel och internationellt samarbete. Ökningen av dessa flöden har medfört nya utmaningar och nya farhågor när det gäller skyddet av personuppgifter. Det är viktigt att den skyddsnivå som fysiska personer säkerställs inom unionen genom denna förordning inte undergrävs när personuppgifter överförs från unionen till personuppgiftsansvariga, personuppgiftsbiträden eller andra mottagare i tredjeland eller till internationella organisationer, vilket inbegriper vidarebefordran av personuppgifter från tredjelandet eller den internationella organisationen till personuppgiftsansvariga, personuppgiftsbiträden i samma eller ett annat tredjeland eller en annan internationell organisation. Överföringar till tredjeländer och internationella organisationer får under alla omständigheter endast utföras i full överensstämmelse med denna förordning. En överföring kan endast ske, om de villkor som fastställs i bestämmelserna i denna förordning om överföring av personuppgifter till tredjeländer eller internationella organisationer har uppfyllts av den personuppgiftsansvarige eller personuppgiftsbiträdet, med förbehåll för de övriga bestämmelserna i denna förordning.
- (102) Denna förordning påverkar inte internationella avtal mellan unionen och tredjeländer som reglerar överföring av personuppgifter, däribland lämpliga skyddsåtgärder för de registrerade. Medlemsstaterna får ingå internationella avtal som innefattar överföring av personuppgifter till tredjeländer eller internationella organisationer i den mån sådana avtal inte påverkar denna förordning eller andra bestämmelser i unionsrätten och innehåller en skälig nivå av skydd för de registrerades grundläggande rättigheter.
- (103) Kommissionen kan med verkan för hela unionen fastställa att ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation erbjuder en adekvat dataskyddsnivå och på så sätt skapa rättslig säkerhet och enhetlighet i hela unionen vad gäller tredjelandet eller den internationella organisationen som anses tillhandahålla en sådan skyddsnivå. I dessa fall får överföringar av personuppgifter till det tredjelandet eller den internationella organisationen ske utan ytterligare tillstånd. Kommissionen kan också, efter att ha underrättat tredjelandet eller den internationella organisationen och lämnat en fullständig motivering, besluta att ett sådant beslut ska återkallas.
- (104) I enlighet med de grundläggande värderingar som unionen bygger på, bl.a. skyddet av mänskliga rättigheter, bör kommissionen i sin bedömning av tredjelandet eller ett territorium eller en specificerad sektor i ett tredjeland beakta hur ett visst tredjeland respekterar rättsstatsprincipen, tillgången till rättslig prövning samt internationella människorättsnormer och -standarder samt landets allmänna lagstiftning och sektorslagstiftning, inklusive lagstiftning om allmän säkerhet, försvar och nationell säkerhet samt allmän ordning och straffrätt. Vid antagandet av ett beslut om adekvat skyddsnivå avseende ett territorium eller en specificerad sektor i ett tredjeland bör hänsyn tas till tydliga och objektiva kriterier, t.ex. specifik behandling och tillämpningsområdet för tillämpliga rättsliga standarder och gällande lagstiftning i tredjelandet. Tredjelandet bör erbjuda garantier som säkerställer en

tillfredsställande skyddsnivå som i huvudsak motsvarar den som säkerställs i unionen, i synnerhet när personuppgifter behandlas inom en eller flera specifika sektorer. Tredjelandet bör framför allt säkerställa en effektiv oberoende dataskyddsövervakning och sörja för samarbetsmekanismer med medlemsstaternas dataskyddsmyndigheter, och de registrerade bör tillförsäkras effektiva och lagstadgade rättigheter samt effektiv administrativ och rättslig prövning.

- (105) Utöver de internationella åtaganden som tredjelandet eller den internationella organisationen har gjort bör kommissionen beakta de skyldigheter som följer av tredjelandets eller den internationella organisationens deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter och genomförandet av dessa skyldigheter. Framför allt bör tredjelandets anslutning till Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk behandling av personuppgifter och dess tilläggsprotokoll beaktas. Kommissionen bör samråda med styrelsen vid bedömningen av skyddsnivån i tredjeländer eller internationella organisationer.
- (106) Kommissionen bör övervaka hur beslut om skyddsnivå i ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation fungerar, och övervaka hur beslut som antas på grundval av artikel 25.6 eller 26.4 i direktiv 95/46/EG fungerar. Kommissionen bör i sina beslut om adekvat skyddsnivå föreskriva en mekanism för periodisk översyn av hur de fungerar. Denna periodiska översyn bör genomföras i samråd med det berörda tredjelandet eller den berörda internationella organisationen, med beaktande av all relevant utveckling i tredjelandet eller den internationella organisationen. Vid övervakningen och genomförandet av den periodiska översynen bör kommissionen ta hänsyn till synpunkter och resultat från Europaparlamentet och rådet samt andra relevanta organ och källor. Kommissionen bör inom rimlig tid utvärdera hur de sistnämnda besluten fungerar och rapportera alla relevanta resultat till den kommitté, i den mening som avses i Europaparlamentets och rådets förordning (EU) nr 182/2011 ⁽¹⁾, som inrättats enligt denna förordning och till Europaparlamentet och rådet.
- (107) Kommissionen kan konstatera att ett tredjeland, ett territorium eller en viss specificerad sektor i ett tredjeland eller en internationell organisation inte längre säkerställer en adekvat dataskyddsnivå. Överföring av personuppgifter till detta tredjeland eller till denna internationella organisation bör då förbjudas, såvida inte kraven i denna förordning avseende överföring med stöd av lämpliga skyddsåtgärder, inbegripet bindande företagsbestämmelser och undantag för särskilda situationer, är uppfyllda. I så fall bör det finnas möjlighet till samråd mellan kommissionen och dessa tredjeländer eller internationella organisationer. Kommissionen bör i god tid informera tredjelandet eller den internationella organisationen om skälen och inleda samråd med tredjelandet eller organisationen för att avhjälpa situationen.
- (108) Saknas beslut om adekvat skyddsnivå bör den personuppgiftsansvarige eller personuppgiftsbiträdet vidta åtgärder för att kompensera för det bristande dataskyddet i ett tredjeland med hjälp av lämpliga skyddsåtgärder för den registrerade. Sådana lämpliga skyddsåtgärder kan bestå i tillämpning av bindande företagsbestämmelser, standardbestämmelser om dataskydd som antagits av kommissionen, standardbestämmelser om dataskydd som antagits av en tillsynsmyndighet eller avtalsbestämmelser som godkänts av en tillsynsmyndighet. Dessa skyddsåtgärder bör säkerställa iakttagande av de krav i fråga om dataskydd och registrerades rättigheter som är lämpliga för behandling inom unionen, inbegripet huruvida bindande rättigheter för de registrerade och effektiva rättsmedel är tillgängliga, inbegripet en faktisk rätt att föra talan på administrativ väg eller inför domstol och att kräva kompensation i unionen eller i ett tredjeland. De bör särskilt gälla överensstämmelse med allmänna principer för behandling av personuppgifter samt principerna om inbyggt dataskydd och dataskydd som standard. Överföring av uppgifter kan också utföras av offentliga myndigheter eller organ till offentliga myndigheter eller organ i tredjeländer eller internationella organisationer med motsvarande skyldigheter eller uppgifter, inbegripet på grundval av bestämmelser som ska införas i administrativa överenskommelser, t.ex. samförståndsavtal, som föreskriver verkställbara och faktiska rättigheter för de registrerade. Tillstånd från den behöriga tillsynsmyndigheten bör erhållas när skyddsåtgärder föreskrivs i icke rättsligt bindande administrativa arrangemang.
- (109) Personuppgiftsansvarigas eller personuppgiftsbiträdens möjlighet att använda standardiserade dataskyddsbestämmelser som antagits av kommissionen eller av en tillsynsmyndighet bör inte hindra att de infogar

⁽¹⁾ Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

standardiserade dataskyddsbestämmelser i ett vidare avtal, såsom ett avtal mellan personuppgiftsbiträdet och ett annat personuppgiftsbiträde, eller lägger till andra bestämmelser eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt står i strid med standardavtalsklausuler som antagits av kommissionen eller av en tillsynsmyndighet eller påverkar de registrerades grundläggande rättigheter eller friheter. Personuppgiftsansvariga och personuppgiftsbiträden bör uppmuntras att tillhandahålla ytterligare skyddsåtgärder via avtalsmässiga åtaganden som kompletterar de standardiserade skyddsbestämmelserna.

- (110) En koncern eller en grupp av företag som deltar i en gemensam ekonomisk verksamhet bör kunna använda sig av godkända bindande företagsbestämmelser för sina internationella överföringar från unionen till organisationer inom samma koncern eller grupp av företag som deltar i en gemensam ekonomisk verksamhet, under förutsättning att företagsbestämmelserna inbegriper alla nödvändiga principer och bindande rättigheter som säkerställer lämpliga skyddsåtgärder för överföringar eller kategorier av överföringar av personuppgifter.
- (111) Det bör införas bestämmelser som ger möjlighet att under vissa omständigheter göra överföringar, om den registrerade har lämnat sitt uttryckliga samtycke, när överföringen är tillfällig och nödvändig med hänsyn till ett avtal eller ett rättsligt anspråk, oavsett om detta sker inom ett rättsligt förfarande eller i ett administrativt eller utomrättsligt förfarande, inbegripet förfaranden inför tillsynsorgan. Det bör också införas bestämmelser som ger möjlighet till överföringar om viktiga allmänintressen fastställda genom unionsrätten eller medlemsstaternas nationella rätt så kräver eller när överföringen görs från ett register som inrättats genom lag och är avsett att konsulteras av allmänheten eller av personer med ett berättigat intresse. I sistnämnda fall bör en sådan överföring inte omfatta alla personuppgifter eller hela kategorier av uppgifter i registret, och överföringen bör endast göras när registret är avsett att vara tillgängligt för personer med ett berättigat intresse, på begäran av dessa personer eller om de själva är mottagarna, med full hänsyn till de registrerades intressen och grundläggande rättigheter.
- (112) Dessa undantag bör främst vara tillämpliga på uppgiftsöverföringar som krävs och är nödvändiga med hänsyn till viktiga allmänintressen, exempelvis vid internationella utbyten av uppgifter mellan konkurrensmyndigheter, skatte- eller tullmyndigheter, finanstillsynsmyndigheter, socialförsäkringsmyndigheter eller hälsovårdsmyndigheter, till exempel vid kontaktspårning för smittsamma sjukdomar eller för att minska och/eller undanröja dopning inom idrott. En överföring av personuppgifter bör också betraktas som laglig, om den är nödvändig för att skydda ett intresse som är väsentligt för den registrerade eller en annan persons vitala intressen, inklusive dennes fysiska integritet och liv, om den registrerade är oförmögen att ge sitt samtycke. Saknas beslut om adekvat skyddsnivå får unionsrätten eller medlemsstaternas nationella rätt med hänsyn till viktiga allmänintressen uttryckligen fastställa gränser för överföringen av särskilda kategorier av uppgifter till ett tredjeland eller en internationell organisation. Medlemsstaterna bör underrätta kommissionen om sådana bestämmelser. Varje överföring till en internationell humanitär organisation av personuppgifter rörande en registrerad som är fysiskt eller rättsligt förhindrad att ge sitt samtycke, i syfte att utföra en uppgift inom ramen för Genèvekonventionerna eller vara förenlig med internationell humanitär rätt, vilken är tillämplig vid väpnade konflikter, skulle kunna anses vara nödvändig för ett betydande allmänintresse eller för att den är av vitalt intresse för den registrerade.
- (113) Överföringar som kan anses vara icke återkommande och endast gäller ett begränsat antal registrerade kan också vara möjliga när personuppgiftsansvarigas tvingande berättigade intressen motiverar detta, om inte den registrerades intressen eller rättigheter och friheter väger tyngre än dessa intressen, och den personuppgiftsansvarige har bedömt alla omständigheter kring uppgiftsöverföringen. Den personuppgiftsansvarige bör ta särskild hänsyn till personuppgifternas art, den eller de avsedda behandlingarnas ändamål och varaktighet samt situationen i ursprungslandet, tredjelandet och det slutliga bestämmelselandet och bör tillhandahålla lämpliga åtgärder för att skydda fysiska personers grundläggande rättigheter och friheter vid behandlingen av deras personuppgifter. Sådana överföringar bör endast vara möjliga i vissa fall där inget av de andra skälen till överföring är tillämpligt. För vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör hänsyn tas till samhällets legitima förväntningar i fråga om ökad kunskap. Den personuppgiftsansvarige bör informera tillsynsmyndigheten och den registrerade om överföringen.
- (114) Om kommissionen inte har fattat beslut om adekvat dataskyddsnivå i ett tredjeland, bör den personuppgiftsansvarige eller personuppgiftsbiträdet i alla fall använda sig av lösningar som ger de registrerade verkställbara och effektiva rättigheter vad gäller behandlingen av deras personuppgifter inom unionen när dessa uppgifter väl har överförts, så att de fortsatt kan utöva sina grundläggande rättigheter och att skyddsåtgärder fortsatt gäller i förhållande till dem.

- (115) Vissa tredjeländer antar lagar och andra författningar som syftar till att direkt reglera behandling som genomförs av fysiska och juridiska personer under medlemsstaternas jurisdiktion. Detta kan inkludera rättsliga avgöranden eller beslut av administrativa myndigheter i tredjeländer med krav på att personuppgiftsansvariga eller personuppgiftsbiträden överför eller överlämnar personuppgifter, vilka inte grundar sig på något gällande internationellt avtal, såsom ett fördrag om ömsesidig rättshjälp, mellan det begärande tredjelandet och unionen eller en medlemsstat. Extraterritoriell tillämpning av dessa lagar och andra författningar kan strida mot internationell rätt och inverka menligt på det skydd av fysiska personer som säkerställs inom unionen genom denna förordning. Överföringar bör endast tillåtas om villkoren i denna förordning för en överföring till tredjeländer är uppfyllda. Detta kan vara fallet bl.a. när utlämnande är nödvändigt på grund av ett viktigt allmänintresse som erkänns i unionsrätten eller i medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av.
- (116) När personuppgifter förs över gränser utanför unionen kan detta öka risken för att fysiska personer inte kan utöva sina dataskyddsrättigheter, i synnerhet för att skydda sig från otillåten användning eller otillåtet utlämnande av denna information. Samtidigt kan tillsynsmyndigheter finna att de inte är i stånd att handlägga klagomål eller göra utredningar som gäller verksamheter utanför gränserna för deras land. Deras strävan att arbeta tillsammans över gränserna kan också hindras av otillräckliga preventiva eller korrigerande befogenheter, oenhetliga rättsliga regelverk och praktiska hinder, som exempelvis bristande resurser. Närmare samarbete mellan dataskyddstillsynsmyndigheter bör därför främjas för att hjälpa dem att utbyta information och utföra utredningar med sina internationella motparter. I syfte att bygga upp internationella samarbetsmekanismer för att underlätta och tillhandahålla ömsesidig internationell hjälp med att kontrollera efterlevnaden av lagstiftningen till skydd för personuppgifter, bör kommissionen och tillsynsmyndigheterna utbyta information och samarbeta, inom verksamhet som rör utövandet av deras befogenheter, med behöriga myndigheter i tredjeländer, på grundval av ömsesidighet och i överensstämmelse med denna förordning.
- (117) Ett väsentligt inslag i skyddet av fysiska personer vid behandlingen av personuppgifter är att medlemsstaterna inrättar tillsynsmyndigheter med behörighet att utföra sina uppgifter och utöva sina befogenheter under fullständigt oberoende. Medlemsstaterna bör kunna inrätta fler än en tillsynsmyndighet om det behövs för att ta hänsyn till den egna konstitutionella, organisatoriska och administrativa strukturen.
- (118) Tillsynsmyndigheternas oberoende bör dock inte innebära att deras utgifter inte kan underkastas kontroll- eller övervakningsmekanismer eller bli föremål för domstolsprövning.
- (119) Om en medlemsstat inrättar flera tillsynsmyndigheter, bör den genom lagstiftning säkerställa att dessa tillsynsmyndigheter effektivt deltar i mekanismen för enhetlighet. Medlemsstaten bör i synnerhet utnämna en tillsynsmyndighet som fungerar som samlande kontaktpunkt för dessa myndigheters effektiva deltagande i mekanismen för att säkra ett snabbt och smidigt samarbete med övriga tillsynsmyndigheter, styrelsen och kommissionen.
- (120) Varje tillsynsmyndighet bör tilldelas de ekonomiska och personella resurser och lokalutrymmen samt den infrastruktur som är nödvändig för att den effektivt ska kunna utföra sina uppgifter, däribland de uppgifter som är knutna till ömsesidigt bistånd och samarbete med övriga tillsynsmyndigheter i hela unionen. Varje tillsynsmyndighet bör ha en separat offentlig årlig budget, som kan ingå i den övergripande statsbudgeten eller nationella budgeten.
- (121) De allmänna villkoren för tillsynsmyndighetens ledamot eller ledamöter bör fastställas genom varje medlemsstats lagstiftning och där bör i synnerhet föreskrivas att ledamöterna ska utnämnas genom ett öppet förfarande antingen av medlemsstatens parlament, regering eller statschef, på grundval av ett förslag från regeringen, en ledamot av regeringen, parlamentet eller en av parlamentets kammare eller av ett oberoende organ som enligt medlemsstaternas nationella rätt har anförtratts utnämningen. I syfte att säkerställa tillsynsmyndighetens oberoende bör ledamoten eller ledamöterna handla med integritet, avstå från alla handlingar som står i strid med deras tjänsteutövning och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet som står i strid med deras uppdrag. Tillsynsmyndigheten bör ha egen personal, som valts ut av tillsynsmyndigheten eller ett oberoende organ som fastställs i medlemsstaternas nationella rätt, vilken uteslutande bör vara underställd tillsynsmyndighetens ledamot eller ledamöter.
- (122) Varje tillsynsmyndighet bör ha behörighet att inom sin medlemsstats territorium utöva de befogenheter och utföra de uppgifter som den tilldelats i enlighet med denna förordning. Detta bör framför allt omfatta behandling

inom ramen för verksamhet vid den personuppgiftsansvariges eller personuppgiftsbiträdets verksamhetsställen inom den egna medlemsstatens territorium, behandling av personuppgifter som utförs av myndigheter eller privata organ som agerar i ett allmänt intresse, behandling som påverkar registrerade på dess territorium eller behandling som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen när den rör registrerade som är bosatta på dess territorium. Detta bör inbegripa att hantera klagomål som lämnas in av en registrerad, genomföra undersökningar om tillämpningen av denna förordning samt främja allmänhetens medvetenhet om risker, bestämmelser, skyddsåtgärder och rättigheter när det gäller behandlingen av personuppgifter.

- (123) Tillsynsmyndigheterna bör övervaka tillämpningen av bestämmelserna i denna förordning och bidra till att tillämpningen blir enhetlig över hela unionen, för att skydda fysiska personer vid behandling av deras personuppgifter och för att underlätta det fria flödet av personuppgifter inom den inre marknaden. För detta ändamål bör tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen, utan att det behövs något avtal mellan medlemsstaterna om tillhandahållande av ömsesidigt bistånd eller om sådant samarbete.
- (124) Om behandlingen av personuppgifter sker inom ramen för verksamhet vid en personuppgiftsansvarigs eller ett personuppgiftsbiträdets verksamhetsställe i unionen och den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat, eller om behandling som sker inom ramen för verksamhet vid ett enda verksamhetsställe tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka registrerade i mer än en medlemsstat, bör tillsynsmyndigheten för den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga verksamhetsställe eller för detta enda verksamhetsställe tillhörande den personuppgiftsansvarige eller personuppgiftsbiträdet agera som ansvarig myndighet. Denna bör samarbeta med de övriga myndigheter som berörs, eftersom den personuppgiftsansvarige eller personuppgiftsbiträdet har ett verksamhetsställe inom deras medlemsstats territorium, eftersom registrerade som är bosatta på deras territorium i väsentlig grad påverkas eller eftersom ett klagomål har lämnats in till dem. Även när en registrerad som inte är bosatt i medlemsstaten har lämnat in ett klagomål, bör den tillsynsmyndighet som klagomålet har lämnats in till också vara en berörd tillsynsmyndighet. Styrelsen bör inom ramen för sina uppgifter kunna utfärda riktlinjer för alla frågor som rör tillämpningen av denna förordning, framför allt för vilka kriterier som ska beaktas för att konstatera om behandlingen i fråga i väsentlig grad påverkar registrerade i mer än en medlemsstat och för vad som utgör en relevant och motiverad invändning.
- (125) Den ansvariga myndigheten bör ha behörighet att anta bindande beslut om åtgärder inom ramen för de befogenheter som den tilldelats i enlighet med denna förordning. I egenskap av ansvarig myndighet bör tillsynsmyndigheten nära involvera och samordna de berörda tillsynsmyndigheterna i beslutsfattandet. Om man beslutar att helt eller delvis avslå den registrerades klagomål, bör detta beslut antas av den tillsynsmyndighet som klagomålet har lämnats in till.
- (126) Den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna bör gemensamt enas om beslutet, som bör rikta sig till den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga eller enda verksamhetsställe och vara bindande för den personuppgiftsansvarige och personuppgiftsbiträdet. Den personuppgiftsansvarige eller personuppgiftsbiträdet bör vidta de åtgärder som krävs för att säkerställa efterlevnad av denna förordning och genomförande av det beslut som den ansvariga tillsynsmyndigheten har anmält till den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga verksamhetsställe vad gäller behandling i unionen.
- (127) Varje tillsynsmyndighet som inte agerar som ansvarig tillsynsmyndighet bör vara behörig att behandla lokala fall, om den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat men ärendet för den specifika behandlingen endast avser behandling som utförs i en enda medlemsstat och endast omfattar registrerade i denna enda medlemsstat, till exempel om ärendet avser behandling av anställdas personuppgifter inom ramen för en medlemsstats specifika anställningsförhållanden. I sådana fall bör tillsynsmyndigheten utan dröjsmål underrätta den ansvariga tillsynsmyndigheten om detta ärende. Efter att ha underrättats bör den ansvariga tillsynsmyndigheten besluta huruvida den kommer att hantera ärendet i enlighet med bestämmelsen om samarbete mellan den ansvariga tillsynsmyndigheten och andra berörda tillsynsmyndigheter (nedan kallad *mekanismen för en enda kontaktpunkt*), eller om den tillsynsmyndighet som underrättade den bör behandla ärendet på lokal nivå. När den ansvariga tillsynsmyndigheten beslutar huruvida den kommer att behandla ärendet, bör den ta hänsyn till om den personuppgiftsansvarige eller personuppgiftsbiträdet har ett verksamhetsställe i den medlemsstat där den tillsynsmyndighet som underrättade den ansvariga myndigheten är belägen för att säkerställa ett effektivt genomförande av ett beslut gentemot den personuppgiftsansvarige eller personuppgiftsbiträdet. När den ansvariga tillsynsmyndigheten beslutar att behandla ärendet, bör den tillsynsmyndighet som underrättade den

ha möjlighet att lämna in ett förslag till beslut, som den ansvariga tillsynsmyndigheten bör ta största möjliga hänsyn till när den utarbetar utkastet till beslut inom ramen för mekanismen för en enda kontaktpunkt.

- (128) Bestämmelserna om den ansvariga tillsynsmyndigheten och mekanismen för en enda kontaktpunkt bör inte tillämpas om behandlingen utförs av myndigheter eller privata organ i ett allmänt intresse. I sådana fall bör den enda tillsynsmyndighet som är behörig att utöva de befogenheter som den tilldelas i enlighet med denna förordning vara tillsynsmyndigheten i den medlemsstat där myndigheten eller det privata organet är etablerat.
- (129) För att denna förordning ska övervakas och verkställas på ett enhetligt sätt i hela unionen bör tillsynsmyndigheterna i alla medlemsstater ha samma uppgifter och effektiva befogenheter, bl.a. undersökningsbefogenheter, korrigerande befogenheter och befogenheter att ålägga sanktioner samt befogenheter att utfärda tillstånd och ge råd, särskilt vid klagomål från fysiska personer och, utan att det påverkar åklagarmyndigheternas befogenheter enligt medlemsstaternas nationella rätt, att upplysa de rättsliga myndigheterna om överträdelser av denna förordning och delta i rättsliga förfaranden. Dessa befogenheter bör även omfatta en befogenhet att införa en tillfällig eller definitiv begränsning av, inklusive förbud mot, behandling. Medlemsstaterna får fastställa andra uppgifter med anknytning till skyddet av personuppgifter enligt denna förordning. Tillsynsmyndigheternas befogenheter bör utövas opartiskt, rättvist och inom rimlig tid i överensstämmelse med lämpliga rättssäkerhetsgarantier i unionsrätten och i medlemsstaternas nationella rätt. Framför allt bör varje åtgärd vara lämplig, nödvändig och proportionell för att säkerställa efterlevnad av denna förordning, med beaktande av omständigheterna i varje enskilt fall, samt respektera varje persons rätt att bli hörd innan några enskilda åtgärder som påverkar honom eller henne negativt vidtas och vara utformad så att onödiga kostnader och alltför stora olägenheter för de berörda personerna undviks. Undersökningsbefogenheten när det gäller tillträde till lokaler bör utövas i enlighet med särskilda krav i medlemsstaternas nationella processrätt, såsom kravet på att inhämta förhandstillstånd från rättsliga myndigheter. Varje rättsligt bindande åtgärd som vidtas av tillsynsmyndigheten bör vara skriftlig, klar och entydig, innehålla information om vilken tillsynsmyndighet som har utfärdat åtgärden och datum för utfärdandet, vara undertecknad av tillsynsmyndighetens chef eller en av dess ledamöter efter dennes bemyndigande samt innehålla en motivering till åtgärden och en hänvisning till rätten till ett effektivt rättsmedel. Detta bör inte utesluta ytterligare krav enligt medlemsstaternas nationella processrätt. Antagande av ett rättsligt bindande beslut innebär att det kan bli föremål för domstolsprövning i den medlemsstat till vilken den tillsynsmyndighet som antog beslutet hör.
- (130) Om den tillsynsmyndighet till vilken klagomålet har ingetts inte är den ansvariga tillsynsmyndigheten, bör den ansvariga tillsynsmyndigheten nära samarbeta med den tillsynsmyndighet till vilken klagomålet har ingetts i enlighet med de bestämmelser om samarbete och enhetlighet som fastställs i denna förordning. I sådana fall bör den ansvariga tillsynsmyndigheten när den vidtar åtgärder avsedda att ha rättsverkan, inbegripet utdömandet av administrativa sanktionsavgifter, ta största hänsyn till synpunkter från den tillsynsmyndighet till vilken klagomålet har ingetts, vilken bör kvarstå som behörig för genomförande av utredningar på den egna medlemsstatens territorium i samverkan med den behöriga tillsynsmyndigheten.
- (131) Om en annan tillsynsmyndighet bör agera som ansvarig tillsynsmyndighet för den personuppgiftsansvariges eller personuppgiftsbitrådets behandling men den sakfråga som klagomålet gäller eller den möjliga överträdelsen endast rör den personuppgiftsansvariges eller personuppgiftsbitrådets behandling i den medlemsstat där klagomålet har ingetts eller den eventuella överträdelsen har upptäckts, och frågan inte i väsentlig grad påverkar eller inte sannolikt i väsentlig grad kommer att påverka registrerade i andra medlemsstater, bör den tillsynsmyndighet som mottar ett klagomål eller upptäcker eller på annat sätt informeras om situationer som innebär eventuella överträdelser av denna förordning försöka få till stånd en uppgörelse i godo med den personuppgiftsansvarige och, om detta inte lyckas, utöva sina befogenheter fullt ut. Detta bör omfatta särskild behandling som utförs inom tillsynsmyndighetens medlemsstats territorium eller med avseende på registrerade inom denna medlemsstats territorium, behandling som utförs inom ramen för ett erbjudande om varor eller tjänster som särskilt riktar sig till registrerade inom tillsynsmyndighetens medlemsstats territorium eller behandling som måste bedömas med beaktande av relevanta rättsliga skyldigheter enligt medlemsstaternas nationella rätt.
- (132) Medvetandehöjande kampanjer från tillsynsmyndigheters sida riktade till allmänheten bör innefatta särskilda åtgärder riktade dels till personuppgiftsansvariga och personuppgiftsbitråden, inbegripet mikroföretag samt små och medelstora företag, dels till fysiska personer, särskilt i utbildningssammanhang.

- (133) Tillsynsmyndigheterna bör hjälpa varandra att utföra sina uppgifter och ge ömsesidigt bistånd så att denna förordning tillämpas och verkställs enhetligt på den inre marknaden. En tillsynsmyndighet som begärt ömsesidigt bistånd får anta en provisorisk åtgärd, om den inte har fått något svar på en begäran om ömsesidigt bistånd inom en månad från det att begäran mottogs av den andra tillsynsmyndigheten.
- (134) Alla tillsynsmyndigheter bör om lämpligt delta i gemensamma insatser med andra tillsynsmyndigheter. Den anmodade tillsynsmyndigheten bör vara skyldig att besvara en begäran inom en fastställd tidsperiod.
- (135) För att denna förordning ska tillämpas enhetligt i hela unionen bör en mekanism för enhetlighet när det gäller samarbete mellan tillsynsmyndigheterna skapas. Denna mekanism bör främst tillämpas när en tillsynsmyndighet avser att anta en åtgärd som är avsedd att ha rättsverkan gällande behandlingar som i väsentlig grad påverkar ett betydande antal registrerade i flera medlemsstater. Den bör också tillämpas när en berörd tillsynsmyndighet eller kommissionen begär att ett sådant ärende ska hanteras inom ramen för mekanismen för enhetlighet. Mekanismen bör inte påverka åtgärder som kommissionen kan komma att vidta när den utövar sina befogenheter enligt fördragen.
- (136) Vid tillämpningen av mekanismen för enhetlighet bör styrelsen inom en fastställd tidsperiod avge ett yttrande, om en majoritet av dess ledamöter så beslutar eller om någon berörd tillsynsmyndighet eller kommissionen begär detta. Styrelsen bör också ges befogenhet att anta rättsligt bindande beslut vid tvister mellan tillsynsmyndigheter. För detta ändamål bör den, normalt med två tredjedelars majoritet av sina ledamöter, utfärda rättsligt bindande beslut i tydligt fastställda fall då tillsynsmyndigheter har olika uppfattningar, framför allt när det gäller mekanismen för samarbete mellan den ansvariga tillsynsmyndigheten och berörda tillsynsmyndigheter om sakförhållandena, i synnerhet om huruvida denna förordning har överträtts.
- (137) Det kan uppstå brådskande behov att agera för att skydda registrerades rättigheter och friheter, särskilt när fara föreligger att säkerställandet av en registrerad persons rättighet kan komma att försvåras avsevärt. En tillsynsmyndighet bör därför kunna vidta vederbörligen motiverade provisoriska åtgärder inom sitt territorium med en viss giltighetsperiod, som inte bör överskrida tre månader.
- (138) Tillämpningen av en sådan mekanism bör vara ett villkor för lagligheten av en åtgärd som är avsedd att ha rättsverkan och som vidtas av tillsynsmyndigheten i de fall där denna tillämpning är obligatorisk. I andra ärenden som inbegriper flera länder bör samarbetsmekanismen mellan den ansvariga tillsynsmyndigheten och berörda tillsynsmyndigheter tillämpas, och ömsesidigt bistånd och gemensamma insatser kan utföras mellan de berörda tillsynsmyndigheterna på bilateral eller multilateral basis utan att mekanismen för enhetlighet utlöses.
- (139) I syfte att främja en enhetlig tillämpning av denna förordning bör styrelsen inrättas som ett oberoende unionsorgan. För att styrelsen ska kunna uppfylla sina mål bör den vara en juridisk person. Styrelsen bör företräddas av sin ordförande. Den bör ersätta arbetsgruppen för skydd av fysiska personer med avseende på behandlingen av personuppgifter, som inrättades genom direktiv 95/46/EG. Den bör bestå av chefen för en tillsynsmyndighet i varje medlemsstat och Europeiska datatillsynsmannen eller deras respektive företrädare. Kommissionen bör delta i styrelsens verksamhet utan att ha rösträtt, och Europeiska datatillsynsmannen bör ha specifik rösträtt. Styrelsen bör bidra till denna förordnings enhetliga tillämpning i hela unionen, bl.a. genom att lämna råd till kommissionen, särskilt vad gäller skyddsnivån i tredjeländer eller internationella organisationer, och främja samarbetet mellan tillsynsmyndigheterna i hela unionen. Styrelsen bör agera oberoende när den utför sina uppgifter.
- (140) Styrelsen bör biträddas av ett sekretariat som tillhandahålls av Europeiska datatillsynsmannen. Den personal vid Europeiska datatillsynsmannen som medverkar i utförandet av de uppgifter som enligt denna förordning anförtros styrelsen bör för sina uppgifter uteslutande ta emot instruktioner från styrelsens ordförande och rapportera till denne.
- (141) Alla registrerade bör ha rätt att lämna in ett klagomål till en enda tillsynsmyndighet, särskilt i den medlemsstat där den registrerade har sin hemvist, och ha rätt till ett effektivt rättsmedel i enlighet med artikel 47 i stadgan,

om den registrerade anser att hans eller hennes rättigheter enligt denna förordning har kränkts eller om tillsynsmyndigheten inte reagerar på ett klagomål, helt eller delvis avslår eller avvisar ett klagomål eller inte agerar när så är nödvändigt för att skydda den registrerades rättigheter. Utredningen av ett klagomål bör, med förbehåll för eventuell domstolsprövning, ske i den utsträckning som är lämplig i det enskilda fallet. Tillsynsmyndigheten bör inom rimlig tid informera den registrerade om hur arbetet med klagomålet fortskrider och vad resultatet blir. Om ärendet fordrar ytterligare utredning eller samordning med en annan tillsynsmyndighet, bör den registrerade underrättas även om detta. För att förenkla inlämningen av klagomål bör varje tillsynsmyndighet vidta åtgärder, såsom att tillhandahålla ett formulär för inlämnande av klagomål som även kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.

- (142) Om en registrerad anser att hans eller hennes rättigheter enligt denna förordning har kränkts, bör han eller hon ha rätt att ge mandat till ett organ, en organisation eller en sammanslutning som drivs utan vinstsyfte och som har inrättats i enlighet med en medlemsstats nationella rätt, som har stadgeenliga mål av allmänt intresse och bedriver verksamhet på området skydd av personuppgifter, att på hans eller hennes vägnar lämna in ett klagomål till en tillsynsmyndighet, om detta föreskrivs i medlemsstatens nationella rätt, att på den registrerades vägnar utöva rätten till domstolsprövning eller att på den registrerades vägnar utöva rätten att ta emot ersättning. En medlemsstat får föreskriva att ett sådant organ, en sådan organisation eller en sådan sammanslutning ska ha rätt att lämna in ett klagomål i den medlemsstaten, oberoende av en registrerad persons mandat, och ha rätt till ett effektivt rättsmedel, om det eller den har skäl att anse att en registrerad persons rättigheter har kränkts till följd av behandling av personuppgifter som strider mot denna förordning. Detta organ, denna organisation eller denna sammanslutning får inte ges rätt att kräva ersättning på en registrerad persons vägnar oberoende av den registrerades mandat.
- (143) Varje fysisk eller juridisk person har rätt att väcka ogiltighetstalan mot styrelsens beslut vid domstolen enligt de villkor som föreskrivs i artikel 263 i EUF-fördraget. I sin egenskap av adressater för sådana beslut måste, i enlighet med artikel 263 i EUF-fördraget, de berörda tillsynsmyndigheter som önskar överklaga dessa väcka talan inom två månader efter det att beslutet meddelats dem. Om styrelsens beslut direkt och personligen berör en personuppgiftsansvarig, ett personuppgiftsbiträde eller en enskild, kan den enskilde väcka ogiltighetstalan mot besluten inom två månader efter det att de har offentliggjorts på styrelsens webbplats, i enlighet med artikel 263 i EUF-fördraget. Utan att det påverkar denna rätt inom ramen för artikel 263 i EUF-fördraget bör varje fysisk eller juridisk person ha rätt till ett effektivt rättsmedel vid den behöriga nationella domstolen mot ett beslut av en tillsynsmyndighet som har rättsliga följder för denna person. Sådana beslut avser särskilt tillsynsmyndighetens utövande av utrednings-, korrigerings- och godkännandebefogenheter eller avvisande av eller avslag på klagomål. Rätten till ett effektivt rättsmedel inbegriper dock inte åtgärder som vidtagits av tillsynsmyndigheter när dessa inte är rättsligt bindande, såsom yttranden som avgivits eller rådgivning som tillhandahållits av tillsynsmyndigheten. Talan mot beslut som har fattats av en tillsynsmyndighet bör väckas vid domstolarna i den medlemsstat där tillsynsmyndigheten har sitt säte och bör genomföras i enlighet med den medlemsstatens nationella processrätt. Dessa domstolar bör ha fullständig behörighet, vilket bör omfatta behörighet att pröva alla fakta och rättsliga frågor som rör den tvist som anhängiggjorts vid dem.

Om talan avslås eller avvisas av en tillsynsmyndighet, kan den enskilde väcka talan vid domstolarna i samma medlemsstat. I samband med rättsmedel som avser tillämpningen av denna förordning kan eller, i det fall som anges i artikel 267 i EUF-fördraget, måste nationella domstolar som anser att ett beslut om ett förhandsavgörande är nödvändigt för att de ska kunna döma begära att domstolen meddelar ett förhandsavgörande om tolkningen av unionsrätten, inbegripet denna förordning. Om dessutom ett beslut av en tillsynsmyndighet om genomförande av ett beslut av styrelsen överklagas till en nationell domstol och giltigheten av styrelsens beslut ifrågasätts, har inte den nationella domstolen befogenhet att förklara styrelsens beslut ogiltigt utan måste hänskjuta frågan om giltighet till domstolen i enlighet med artikel 267 i EUF-fördraget såsom den tolkats av domstolen, närhelst den anser att beslutet är ogiltigt. En nationell domstol får dock inte hänskjuta en fråga om giltigheten av styrelsens beslut på begäran av en fysisk eller juridisk person som haft tillfälle att väcka ogiltighetstalan mot beslutet, i synnerhet inte om denna person direkt och personligen berördes av beslutet men inte gjorde detta inom den frist som anges i artikel 263 i EUF-fördraget.

- (144) Om en domstol där ett förfarande inletts mot beslut som har fattats av en tillsynsmyndighet har skäl att tro att ett förfarande rörande samma behandling, såsom samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller samma personuppgiftsbiträde, eller samma händelseförlopp, har inletts vid en annan behörig domstol i en annan medlemsstat, bör den kontakta denna domstol i syfte att bekräfta förekomsten av sådana relaterade förfaranden. Om relaterade förfaranden pågår vid en domstol i en annan medlemsstat får alla andra

domstolar än den domstol där förfarandet först inleddes låta förfarandena vila eller på en av parternas begäran förklara sig obehöriga till förmån för den domstol där förfarandet först inleddes, om den domstolen har behörighet i förfarandet i fråga och dess lagstiftning tillåter förening av sådana relaterade förfaranden. Förfarandena anses vara relaterade, om de är så nära förenade att en gemensam handläggning och dom är påkallad för att undvika att oförenliga domar meddelas som en följd av att förfarandena prövas i olika rättegångar.

- (145) När det gäller ett rättsligt förfarande mot en personuppgiftsansvarig eller ett personuppgiftsbiträde bör käranden kunna välja att väcka talan antingen vid domstolarna i de medlemsstater där den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad eller där den registrerade är bosatt, såvida inte den personuppgiftsansvarige är en myndighet i en medlemsstat som agerar inom ramen för sin myndighetsutövning.
- (146) Den personuppgiftsansvarige eller personuppgiftsbiträdet bör ersätta all skada som en person kan komma att lida till följd av behandling som strider mot denna förordning. Den personuppgiftsansvarige eller personuppgiftsbiträdet bör dock befrias från skadeståndsskyldighet om den kan visa att den inte på något sätt är ansvarig för skadan. Begreppet skada bör tolkas brett mot bakgrund av domstolens rättspraxis på ett sätt som fullt ut återspeglar denna förordnings mål. Detta påverkar inte skadeståndsanspråk till följd av överträdelser av andra bestämmelser i unionsrätten eller i medlemsstaternas nationella rätt. Behandling som strider mot denna förordning omfattar även behandling som strider mot delegerade akter och genomförandekter som antagits i enlighet med denna förordning och medlemsstaternas nationella rätt med närmare specifikation av denna förordnings bestämmelser. Registrerade bör få full och effektiv ersättning för den skada de lidit. Om personuppgiftsansvariga eller personuppgiftsbiträden medverkat vid samma behandling, bör varje personuppgiftsansvarig eller personuppgiftsbiträde hållas ansvarig för hela skadan. Om de är förenade i samma rättsliga förfarande i enlighet med medlemsstaternas nationella rätt, kan ersättningen dock fördelas i enlighet med varje personuppgiftsansvarigs eller personuppgiftsbiträdes ansvar för den genom behandlingen uppkomna skadan, förutsatt att den registrerade som lidit skada tillförsäkras full och effektiv ersättning. Varje personuppgiftsansvarig eller personuppgiftsbiträde som har betalat full ersättning får därefter inleda förfaranden för återkrav mot andra personuppgiftsansvariga eller personuppgiftsbiträden som medverkat vid samma behandling.
- (147) Om särskilda bestämmelser om behörighet fastställs i denna förordning, framför allt vad gäller förfaranden för att begära rättslig prövning som inbegriper ersättning mot en personuppgiftsansvarig eller ett personuppgiftsbiträde, bör inte allmänna bestämmelser om behörighet, såsom bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 1215/2012 ⁽¹⁾, påverka tillämpningen av sådana särskilda bestämmelser.
- (148) För att stärka verkställigheten av denna förordning bör det utdömas sanktioner, inbegripet administrativa sanktionsavgifter, för överträdelser av denna förordning utöver eller i stället för de lämpliga åtgärder som tillsynsmyndigheten vidtar i enlighet med denna förordning. Vid en mindre överträdelse eller om den sanktionsavgift som sannolikt skulle utdömas skulle innebära en oproportionell börda för en fysisk person får en reprimand utfärdas i stället för sanktionsavgifter. Vederbörlig hänsyn bör dock tas till överträdelsens karaktär, svårighetsgrad och varaktighet och huruvida den har skett uppsåtligen, vilka åtgärder som vidtagits för att lindra skadan, graden av ansvar eller eventuella tidigare överträdelser av relevans, det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, efterlevnad av åtgärder som förordnats mot den personuppgiftsansvarige eller personuppgiftsbiträdet, tillämpning av en uppförandekod och eventuella andra försvårande eller förmildrande faktorer. Utdömandet av sanktioner, inbegripet administrativa sanktionsavgifter, bör underkastas adekvata rättssäkerhetsgarantier i överensstämmelse med allmänna principer inom unionsrätten och stadgan, vilket inbegriper ett effektivt rättsligt skydd och korrekt rättsligt förfarande.
- (149) Medlemsstaterna bör kunna fastställa bestämmelser om straffrättsliga påföljder för överträdelser av denna förordning, inbegripet för överträdelser av nationella bestämmelser som antagits i enlighet med och inom ramen för denna förordning. Dessa straffrättsliga påföljder kan även inbegripa en möjlighet att förverka den vinning som gjorts genom överträdelser av denna förordning. Utdömandet av straffrättsliga påföljder för överträdelser av sådana nationella bestämmelser och administrativa sanktioner bör dock inte medföra ett åsidosättande av principen *ne bis in idem* enligt domstolens tolkning.
- (150) För att förstärka och harmonisera de administrativa sanktionerna för överträdelser av denna förordning bör samtliga tillsynsmyndigheter ha befogenhet att utfärda administrativa sanktionsavgifter. Det bör i denna

⁽¹⁾ Europaparlamentets och rådets förordning (EU) nr 1215/2012 av den 12 december 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttens område (EUTL 351, 20.12.2012, s. 1).

förordning anges vilka överträdelseerna är, den övre gränsen för och kriterierna för fastställande av de administrativa sanktionsavgifterna, som i varje enskilt fall bör bestämmas av den behöriga tillsynsmyndigheten med beaktande av alla relevanta omständigheter i det särskilda fallet, med vederbörlig hänsyn bl.a. till överträdelsens karaktär, svårighetsgrad och varaktighet samt till dess följder och till de åtgärder som vidtas för att sörja för fullgörandet av skyldigheterna enligt denna förordning och för att förebygga eller lindra konsekvenserna av överträdelsen. Om de administrativa sanktionsavgifterna åläggs ett företag, bör ett företag i detta syfte anses vara ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget. Om de administrativa sanktionsavgifterna åläggs personer som inte är ett företag, bör tillsynsmyndigheten ta hänsyn till den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation, när den överväger lämplig sanktionsavgift. Mekanismen för enhetlighet kan också tillämpas för att främja en enhetlig tillämpning av administrativa sanktionsavgifter. Medlemsstaterna bör fastställa om och i vilken utsträckning myndigheter ska omfattas av administrativa sanktionsavgifter. Utfärdande av administrativa sanktionsavgifter eller utdelning av en varning påverkar inte tillämpningen av tillsynsmyndigheternas övriga befogenheter eller av andra sanktioner enligt denna förordning.

- (151) Danmarks och Estlands rättssystem tillåter inte administrativa sanktionsavgifter i enlighet med denna förordning. Bestämmelserna om administrativa sanktionsavgifter kan tillämpas så att sanktionsavgiften i Danmark utdöms som en straffrättslig påföljd av en behörig nationell domstol och att den i Estland utdöms av tillsynsmyndigheten inom ramen för ett förseelseförfarande, under förutsättning att en sådan tillämpning av bestämmelserna i dessa medlemsstater har en effekt som är likvärdig med administrativa sanktionsavgifter som utdöms av tillsynsmyndigheter. De behöriga nationella domstolarna bör därför beakta rekommendationen från den tillsynsmyndighet som initierar sanktionsavgiften. De sanktionsavgifter som utdöms bör i alla händelser vara effektiva, proportionella och avskräckande.
- (152) Om denna förordning inte harmoniserar administrativa sanktioner eller om nödvändigt i andra fall, till exempel vid fall av allvarliga överträdelser av denna förordning, bör medlemsstaterna genomföra ett system med effektiva, proportionella och avskräckande sanktioner. Dessa sanktioners art, straffrättsliga eller administrativa, bör fastställas i medlemsstaternas nationella rätt.
- (153) Medlemsstaterna bör i sin lagstiftning sammanjämka bestämmelserna om yttrandefrihet och informationsfrihet, vilket inbegriper journalistiska, akademiska, konstnärliga och/eller litterära uttrycksformer, med rätten till skydd av personuppgifter i enlighet med denna förordning. Behandling av personuppgifter enbart för journalistiska, akademiska, konstnärliga eller litterära ändamål bör undantas från vissa av kraven i denna förordning, så att rätten till skydd av personuppgifter vid behov kan förenas med rätten till yttrandefrihet och informationsfrihet, som följer av artikel 11 i stadgan. Detta bör särskilt gälla vid behandling av personuppgifter inom det audiovisuella området och i nyhetsarkiv och pressbibliotek. Medlemsstaterna bör därför anta lagstiftningsåtgärder som fastställer de olika undantag som behövs för att skapa en balans mellan dessa grundläggande rättigheter. Medlemsstaterna bör fastställa sådana undantag med avseende på allmänna principer, de registrerades rättigheter, personuppgiftsansvariga och personuppgiftsbiträden, överföring av uppgifter till tredjeländer eller internationella organisationer, de oberoende tillsynsmyndigheterna, samarbete och enhetlighet samt specifika situationer där personuppgifter behandlas. Om sådana undantag varierar från en medlemsstat till en annan, ska den nationella rätten i den medlemsstat vars lag den personuppgiftsansvarige omfattas av tillämpas. För att beakta vikten av rätten till yttrandefrihet i varje demokratiskt samhälle måste det göras en bred tolkning av vad som innefattas i denna frihet, som till exempel journalistik.
- (154) Denna förordning gör det möjligt att vid tillämpningen av den ta hänsyn till principen om allmänhetens rätt att få tillgång till allmänna handlingar. Allmänhetens rätt att få tillgång till allmänna handlingar kan betraktas som ett allmänt intresse. Personuppgifter i handlingar som innehas av en myndighet eller ett offentligt organ bör kunna lämnas ut offentligt av denna myndighet eller detta organ, om utlämning stadgas i unionsrätten eller i medlemsstatens nationella rätt som är tillämplig på myndigheten eller det offentliga organet. Denna rätt bör sammanjämka allmänhetens rätt att få tillgång till allmänna handlingar och vidareutnyttjande av information från den offentliga sektorn med rätten till skydd av personuppgifter och får därför innehålla föreskrifter om den nödvändiga sammanjämkningen med rätten till skydd av personuppgifter enligt denna förordning. Hänvisningen till offentliga myndigheter och organ bör i detta sammanhang omfatta samtliga myndigheter eller andra organ som omfattas av medlemsstaternas nationella rätt om allmänhetens tillgång till handlingar. Europaparlamentets och rådets direktiv 2003/98/EG ⁽¹⁾ ska inte på något sätt påverka skyddsnivån för fysiska personer med avseende

⁽¹⁾ Europaparlamentets och rådets direktiv 2003/98/EG av den 17 november 2003 om vidareutnyttjande av information från den offentliga sektorn (EUT L 345, 31.12.2003, s. 90).

på behandling av personuppgifter enligt bestämmelserna i unionsrätten och i medlemsstaternas nationella rätt och i synnerhet ändras inte de skyldigheter och rättigheter som anges i denna förordning genom det direktivet. I synnerhet ska direktivet inte vara tillämpligt på handlingar till vilka, med hänsyn till skyddet av personuppgifter, tillgång enligt tillgångsbestämmelserna är utesluten eller begränsad eller på delar av handlingar som är tillgängliga enligt dessa bestämmelser men som innehåller personuppgifter vilkas vidareutnyttjande i lag har fastställts som oförenligt med lagstiftningen om skydd för fysiska personer vid behandling av personuppgifter.

- (155) En medlemsstatsnationella rätt eller kollektivavtal, inbegripet "verksamhetsöverenskommelser", får föreskriva särskilda bestämmelser om behandling av anställdas personuppgifter i anställningsförhållanden, särskilt när det gäller villkoren för hur personuppgifter i anställningsförhållanden får behandlas på grundval av samtycke från den anställde, rekrytering, genomförande av anställningsavtalet, inklusive befrielse från i lag eller kollektivavtal stadgade skyldigheter, ledning, planering och organisering av arbetet samt hälsa och säkerhet på arbetsplatsen, men också när det gäller att såväl kollektivt som individuellt utöva och komma i åtnjutande av rättigheter och förmåner som är knutna till anställningen samt att avsluta anställningsförhållandet.
- (156) Behandlingen av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör omfattas av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt denna förordning. Skyddsåtgärderna bör säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt principen om uppgiftsminimering iakttas. Ytterligare behandling av personuppgifter för arkivändamål av allmänintresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör genomföras, när den personuppgiftsansvarige har bedömt möjligheten att uppnå dessa ändamål genom behandling av personuppgifter som inte medger eller inte längre medger identifiering av de registrerade, förutsatt att det finns lämpliga skyddsåtgärder (t. ex. pseudonymisering av personuppgifter). Medlemsstaterna bör införa lämpliga skyddsåtgärder för behandlingen av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Medlemsstaterna bör på särskilda villkor med förbehåll för lämpliga skyddsåtgärder för de registrerade ha rätt att specificera och göra undantag från kraven på information, rätten till rättelse eller radering av personuppgifter, rätten att bli bortglömd, rätten till begränsning av behandlingen, rätten till dataportabilitet och rätten att göra invändning i samband med behandling av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Villkoren och säkerhetsåtgärderna i fråga kan medföra att de registrerade måste följa särskilda förfaranden för att utöva dessa rättigheter, om det är lämpligt med hänsyn till den särskilda behandlingens syfte tillsammans med tekniska och organisatoriska åtgärder som syftar till att minimera behandlingen av personuppgifter i enlighet med principerna om proportionalitet och nödvändighet. Behandling av personuppgifter för vetenskapliga ändamål bör även vara förenlig med annan relevant lagstiftning, exempelvis om kliniska prövningar.
- (157) Genom att koppla samman information från olika register kan forskare erhålla ny kunskap av stort värde med avseende på medicinska tillstånd som exempelvis hjärt-kärlsjukdomar, cancer och depression. På grundval av registren kan forskningsresultaten förbättras, eftersom de bygger på en större befolkningsgrupp. Forskning inom samhällsvetenskap som bedrivs på grundval av register gör det möjligt för forskare att få grundläggande kunskaper om sambandet på lång sikt mellan ett antal sociala villkor, exempelvis arbetslöshet och utbildning, och andra livsförhållanden. Forskningsresultat som erhållits på grundval av register utgör en stabil, högkvalitativ kunskap, som kan ligga till grund för utformningen och genomförandet av kunskapsbaserad politik, förbättra livskvaliteten för ett antal personer och förbättra de sociala tjänsternas effektivitet. För att underlätta vetenskaplig forskning får personuppgifter behandlas för vetenskapliga forskningsändamål, med förbehåll för lämpliga villkor och skyddsåtgärder i unionsrätten eller i medlemsstaternas nationella rätt.
- (158) Om personuppgifter behandlas för arkivändamål, bör denna förordning också gälla denna behandling, med beaktande av att denna förordning inte bör gälla för avlidna personer. Offentliga myndigheter eller offentliga eller privata organ som innehar uppgifter av allmänt intresse bör vara tillhandahållare som, i enlighet med unionsrätten eller medlemsstaternas nationella rätt, har en rättslig skyldighet att förvärva, bevara, bedöma, organisera, beskriva, kommunicera, främja, sprida och ge tillgång till uppgifter av bestående värde för allmänintresset. Medlemsstaterna bör också ha rätt att föreskriva att personuppgifter får vidarebehandlas för arkivering, exempelvis i syfte att tillhandahålla specifik information om politiskt beteende under tidigare totalitära regimer, folkmord, brott mot mänskligheten, särskilt Förintelsen, eller krigsförbrytelser.

- (159) Om personuppgifter behandlas för vetenskapliga forskningsändamål, bör denna förordning också gälla denna behandling. Behandling av personuppgifter för vetenskapliga forskningsändamål bör i denna förordning ges en vid tolkning och omfatta till exempel teknisk utveckling och demonstration, grundforskning, tillämpad forskning och privatfinansierad forskning. Behandlingen av personuppgifter bör dessutom ta hänsyn till unionens mål enligt artikel 179.1 i EUF-fördraget angående åstadkommandet av ett europeiskt forskningsområde. Vetenskapliga forskningsändamål bör också omfatta studier som utförs av ett allmänt intresse inom folkhälsoområdet. För att tillgodose de särskilda kraven i samband med behandling av personuppgifter för vetenskapliga forskningsändamål bör särskilda villkor gälla, särskilt vad avser offentliggörande eller annat utlämnande av personuppgifter inom ramen för vetenskapliga forskningsändamål. Om resultatet av vetenskaplig forskning, särskilt för hälso- och sjukvårdsändamål, ger anledning till ytterligare åtgärder i den registrerades intresse, bör de allmänna reglerna i denna förordning tillämpas på dessa åtgärder.
- (160) Om personuppgifter behandlas för historiska forskningsändamål, bör denna förordning också gälla denna behandling. Detta bör även omfatta forskning för historiska och genealogiska ändamål, med beaktande av att denna förordning inte bör gälla för avlidna personer.
- (161) När det gäller samtycke till deltagande i vetenskaplig forskning inom ramen för kliniska prövningar, bör de relevanta bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 536/2014 ⁽¹⁾ tillämpas.
- (162) Om personuppgifter behandlas för statistiska ändamål, bör denna förordning gälla denna behandling. Unionsrätten eller medlemsstaternas nationella rätt bör, inom ramen för denna förordning, fastställa statistiskt innehåll, kontroll av tillgång, specifikationer för behandling av personuppgifter för statistiska ändamål och lämpliga åtgärder till skydd för den registrerades rättigheter och friheter och för att säkerställa insynsskydd för statistiska uppgifter. Med statistiska ändamål avses varje åtgärd som vidtas för den insamling och behandling av personuppgifter som är nödvändig för statistiska undersökningar eller för framställning av statistiska resultat. Dessa statistiska resultat kan vidare användas för olika ändamål, inbegripet vetenskapliga forskningsändamål. Ett statistiskt ändamål innebär att resultatet av behandlingen för statistiska ändamål inte består av personuppgifter, utan av aggregerade personuppgifter, och att resultatet eller uppgifterna inte används till stöd för åtgärder eller beslut som avser en särskild fysiskperson.
- (163) De konfidentiella uppgifter som unionens myndigheter och nationella statistikansvariga myndigheter samlar in för att framställa officiell europeisk och officiell nationell statistik bör skyddas. Europeisk statistik bör utvecklas, framställas och spridas i enlighet med de statistiska principerna i artikel 338.2 i EUF-fördraget, medan hanteringen av nationell statistik även bör överensstämma med medlemsstaternas nationella rätt. Europaparlamentets och rådets förordning (EG) nr 223/2009 ⁽²⁾ innehåller ytterligare preciseringar om statistisk konfidentialitet för europeisk statistik.
- (164) Vad beträffar tillsynsmyndigheternas befogenheter att från personuppgiftsansvariga eller personuppgiftsbiträden få tillgång till personuppgifter och tillträde till lokaler, får medlemsstaterna, inom gränserna för denna förordning, genom lagstiftning anta särskilda regler för att skydda yrkesmässig eller annan motsvarande tystnadsplikt, i den mån detta är nödvändigt för att jämka samman rätten till skydd av personuppgifter med tystnadsplikten. Detta påverkar inte tillämpningen av medlemsstaternas befintliga skyldigheter att anta bestämmelser om tystnadsplikt, där detta krävs enligt unionsrätten.
- (165) Denna förordning är förenlig med kravet på att respektera och inte påverka den ställning som kyrkor och religiösa sammanslutningar eller samfund har i medlemsstaterna enligt gällande grundlag i enlighet med artikel 17 i EUF-fördraget.
- (166) I syfte att uppnå målen för denna förordning, nämligen att skydda fysiska personers grundläggande rättigheter och friheter och i synnerhet deras rätt till skydd av personuppgifter och för att säkra det fria flödet av

⁽¹⁾ Europaparlamentets och rådets förordning (EU) nr 536/2014 av den 16 april 2014 om kliniska prövningar av humanläkemedel och om upphävande av direktiv 2001/20/EG (EUT L 158, 27.5.2014, s. 1).

⁽²⁾ Europaparlamentets och rådets förordning (EG) nr 223/2009 av den 11 mars 2009 om europeisk statistik och om upphävande av Europaparlamentets och rådets förordning (EG, Euratom) nr 1101/2008 om utlämnande av insynsskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor, rådets förordning (EG) nr 322/97 om gemenskapsstatistik och rådets beslut 89/382/EEG, Euratom om inrättande av en kommitté för Europeiska gemenskapernas statistiska program (EUT L 87, 31.3.2009, s. 164).

personuppgifter inom unionen, bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen. Delegerade akter bör framför allt antas när det gäller kriterier och krav vad gäller certifieringsmekanismer, information som ska ges med användning av standardiserade symboler och förfaranden för att tillhandahålla sådana symboler. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå. När kommissionen förbereder och utarbetar delegerade akter bör den se till att relevanta handlingar översänds samtidigt till Europaparlamentet och rådet och att detta sker så snabbt som möjligt och på lämpligt sätt.

- (167) För att säkerställa enhetliga villkor för tillämpningen av denna förordning bör kommissionen ges genomförandebefogenheter i enlighet med denna förordning. Dessa befogenheter bör utövas i enlighet med förordning (EU) nr 182/2011. Kommissionen bör därvid överväga särskilda åtgärder för mikroföretag och små och medelstora företag.
- (168) Granskningsförfarandet bör användas vid antagande av genomförandekter om standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden och mellan personuppgiftsbiträden, uppförandekoder, tekniska standarder och mekanismer för certifiering, adekvat nivå på det skydd som lämnas av ett tredjeland, ett territorium eller av en specificerad sektor inom det tredjelandet eller en internationell organisation, standardiserade skyddsbestämmelser, format och förfaranden för elektroniskt utbyte av information mellan personuppgiftsansvariga, personuppgiftsbiträden och tillsynsmyndigheter för bindande företagsbestämmelser, ömsesidigt bistånd och tillvägagångssätt för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen.
- (169) Kommissionen bör när det föreligger tvingande skäl till skyndsamhet anta omedelbart tillämpliga genomförandekter, när tillgängliga bevis visar att ett tredjeland, ett territorium eller en specificerad sektor inom det tredjelandet eller en internationell organisation inte upprätthåller en adekvat skyddsnivå.
- (170) Eftersom målet för denna förordning, nämligen att säkerställa en likvärdig nivå för skyddet av fysiska personer och det fria flödet av personuppgifter inom hela unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning eller verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen (EU-fördraget). I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.
- (171) Direktiv 95/46/EG bör upphävas genom denna förordning. Behandling som redan pågår den dag då denna förordning börjar tillämpas bör bringas i överensstämmelse med denna förordning inom en period av två år från det att denna förordning träder i kraft. Om behandlingen grundar sig på samtycke enligt direktiv 95/46/EG, är det inte nödvändigt att den registrerade på nytt ger sitt samtycke för att den personuppgiftsansvarige ska kunna fortsätta med behandlingen i fråga efter det att denna förordning börjar tillämpas, om det sätt på vilket samtycket gavs överensstämmer med villkoren i denna förordning. Beslut av kommissionen som antagits och tillstånd från tillsynsmyndigheterna som utfärdats på grundval av direktiv 95/46/EG ska fortsatt vara giltiga tills de ändras, ersätts eller upphävs.
- (172) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 och avgav ett yttrande den 7 mars 2012 ⁽¹⁾.
- (173) Denna förordning bör vara tillämplig på alla frågor som gäller skyddet av grundläggande rättigheter och friheter i förhållande till behandlingen av personuppgifter, vilka inte omfattas av särskilda skyldigheter med samma mål som anges i Europaparlamentets och rådets direktiv 2002/58/EG ⁽²⁾, däribland den personuppgiftsansvariges skyldigheter och fysiska personers rättigheter. För att klargöra förhållandet mellan denna förordning och direktiv 2002/58/EG bör det direktivet ändras. När denna förordning har antagits, bör direktiv 2002/58/EG ses över, framför allt för att säkerställa konsekvens med denna förordning.

⁽¹⁾ EUT C 192, 30.6.2012, s. 7.

⁽²⁾ Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Syfte

1. I denna förordning fastställs bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och om det fria flödet av personuppgifter.
2. Denna förordning skyddar fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.
3. Det fria flödet av personuppgifter inom unionen får varken begränsas eller förbjudas av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter.

Artikel 2

Materiellt tillämpningsområde

1. Denna förordning ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.
2. Denna förordning ska inte tillämpas på behandling av personuppgifter som
 - a) utgör ett led i en verksamhet som inte omfattas av unionsrätten,
 - b) medlemsstaterna utför när de bedriver verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget,
 - c) en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,
 - d) behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.
3. Förordning (EG) nr 45/2001 är tillämplig på den behandling av personuppgifter som sker i EU:s institutioner, organ och byråer. Förordning (EG) nr 45/2001 och de av unionens övriga rättsakter som är tillämpliga på sådan behandling av personuppgifter ska anpassas till principerna och bestämmelserna i denna förordning i enlighet med artikel 98.
4. Denna förordning påverkar inte tillämpningen av direktiv 2000/31/EG, särskilt bestämmelserna om tjänsteleverande mellanhänders ansvar i artiklarna 12–15 i det direktivet.

Artikel 3

Territoriellt tillämpningsområde

1. Denna förordning ska tillämpas på behandlingen av personuppgifter inom ramen för den verksamhet som bedrivs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i unionen, oavsett om behandlingen utförs i unionen eller inte.

2. Denna förordning ska tillämpas på behandling av personuppgifter som avser registrerade som befinner sig i unionen och som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen, om behandlingen har anknytning till

a) utbudande av varor eller tjänster till sådana registrerade i unionen, oavsett om dessa varor eller tjänster erbjuds kostnadsfritt eller inte, eller

b) övervakning av deras beteende så länge beteendet sker inom unionen.

3. Denna förordning ska tillämpas på behandling av personuppgifter som utförs av en personuppgiftsansvarig som inte är etablerad i unionen, men på en plats där en medlemsstats nationella rätt gäller enligt folkrätten.

Artikel 4

Definitioner

I denna förordning avses med

1. *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad *en registrerad*), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,
2. *behandling*: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,
3. *begränsning av behandling*: markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden,
4. *profilering*: varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar,
5. *pseudonymisering*: behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person,
6. *register*: en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,
7. *personuppgiftsansvarig*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt,
8. *personuppgiftsbiträde*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,
9. *mottagare*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte; offentliga myndigheter som kan komma att motta

personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare; offentliga myndigheters behandling av dessa uppgifter ska vara förenlig med tillämpliga bestämmelser för dataskydd beroende på behandlingens syfte,

10. *tredje part*: en fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbitrådets direkta ansvar är behöriga att behandla personuppgifterna,
11. *samtycke* av den registrerade: varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne,
12. *personuppgiftsincident*: en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,
13. *genetiska uppgifter*: alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om denna fysiska persons fysiologi eller hälsa och vilka framför allt härrör från en analys av ett biologiskt prov från den fysiska personen i fråga,
14. *biometriska uppgifter*: personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter,
15. *uppgifter om hälsa*: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus,
16. *huvudsakligt verksamhetsställe*:
 - a) när det gäller en personuppgiftsansvarig med verksamhetsställen i mer än en medlemsstat, den plats i unionen där vederbörande har sin centrala förvaltning, om inte besluten om ändamålen och medlen för behandlingen av personuppgifter fattas vid ett annat av den personuppgiftsansvariges verksamhetsställen i unionen och det sistnämnda verksamhetsstället har befogenhet att få sådana beslut genomförda, i vilket fall det verksamhetsställe som har fattat sådana beslut ska betraktas som det huvudsakliga verksamhetsstället,
 - b) när det gäller ett personuppgiftsbiträde med verksamhetsställen i mer än en medlemsstat, den plats i unionen där vederbörande har sin centrala förvaltning eller, om personuppgiftsbiträdet inte har någon central förvaltning i unionen, det av personuppgiftsbitrådets verksamhetsställen i unionen där den huvudsakliga behandlingen inom ramen för verksamheten vid ett av personuppgiftsbitrådets verksamhetsställen sker, i den utsträckning som personuppgiftsbiträdet omfattas av särskilda skyldigheter enligt denna förordning,
17. *företrädare*: en i unionen etablerad fysisk eller juridisk person som skriftligen har utsetts av den personuppgiftsansvarige eller personuppgiftsbiträdet i enlighet med artikel 27 och företräder denne i frågor som gäller dennes skyldigheter enligt denna förordning,
18. *företag*: en fysisk eller juridisk person som bedriver ekonomisk verksamhet, oavsett dess juridiska form, vilket inbegriper partnerskap eller föreningar som regelbundet bedriver ekonomisk verksamhet,
19. *koncern*: ett kontrollerande företag och dess kontrollerade företag,
20. *bindande företagsbestämmelser*: strategier för skydd av personuppgifter som en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad på en medlemsstats territorium använder sig av vid överföringar eller en uppsättning av överföringar av personuppgifter till en personuppgiftsansvarig eller ett personuppgiftsbiträde i ett eller flera tredjeländer inom en koncern eller en grupp av företag som deltar i gemensam ekonomisk verksamhet,
21. *tillsynsmyndighet*: en oberoende offentlig myndighet som är utsedd av en medlemsstat i enlighet med artikel 51,

22. *berörd tillsynsmyndighet*: en tillsynsmyndighet som berörs av behandlingen av personuppgifter på grund av att
- a) den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad på tillsynsmyndighetens medlemsstats territorium,
 - b) registrerade som är bosatta i den tillsynsmyndighetens medlemsstat i väsentlig grad påverkas eller sannolikt i väsentlig grad kommer att påverkas av behandlingen, eller
 - c) ett klagomål har lämnats in till denna tillsynsmyndighet,
23. *gränsöverskridande behandling*:
- a) behandling av personuppgifter som äger rum inom ramen för verksamhet vid verksamhetsställen i mer än en medlemsstat tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen, när den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat, eller
 - b) behandling av personuppgifter som äger rum inom ramen för verksamhet vid ett enda verksamhetsställe tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen men som i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka registrerade i mer än en medlemsstat,
24. *relevant och motiverad invändning*: en invändning mot ett förslag till beslut avseende frågan huruvida det föreligger en överträdelse av denna förordning eller huruvida den planerade åtgärden i förhållande till den personuppgiftsansvarige eller personuppgiftsbiträdet är förenlig med denna förordning, av vilken invändning det tydligt framgår hur stora risker utkastet till beslut medför när det gäller registrerades grundläggande rättigheter och friheter samt i tillämpliga fall det fria flödet av personuppgifter inom unionen,
25. *informationssamhällets tjänster*: alla tjänster enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 ⁽¹⁾,
26. *internationell organisation*: en organisation och dess underställda organ som lyder under folkrätten, eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera länder.

KAPITEL II

Principer

Artikel 5

Principer för behandling av personuppgifter

1. Vid behandling av personuppgifter ska följande gälla:
- a) Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (*laglighet, korrekthet och öppenhet*).
 - b) De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenligt med de ursprungliga ändamålen (*ändamålsbegränsning*).
 - c) De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (*uppgiftsminimering*).
 - d) De ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (*korrekthet*).

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

- e) De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (*lagringsminimering*).
 - f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstörelse eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (*integritet och konfidentialitet*).
2. Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs (*ansvarsskyldighet*).

Artikel 6

Laglig behandling av personuppgifter

1. Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:
- a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
 - b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
 - c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
 - d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
 - e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
 - f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Led f i första stycket ska inte gälla för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

2. Medlemsstaterna får behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning med hänsyn till behandling för att efterleva punkt 1 c och e genom att närmare fastställa specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling, inbegripet för andra specifika situationer då uppgifter behandlas i enlighet med kapitel IX.

3. Den grund för behandlingen som avses i punkt 1 c och e ska fastställas i enlighet med

- a) unionsrätten, eller
- b) en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av.

Syftet med behandlingen ska fastställas i den rättsliga grunden eller, i fråga om behandling enligt punkt 1 e, ska vara nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Den rättsliga grunden kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning, bland annat: de allmänna villkor som ska gälla för den personuppgiftsansvariges behandling, vilken typ av uppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål, ändamålsbegränsningar, lagringstid samt typer av behandling och förfaranden för behandling, inbegripet åtgärder för att tillförsäkra en laglig och rättvis behandling, däribland för behandling i andra särskilda

situationer enligt kapitel IX. Unionsrätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas.

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

- a) Kopplingar mellan de ändamål för vilka personuppgifterna har samlats in och ändamålen med den avsedda ytterligare behandlingen.
- b) Det sammanhang inom vilket personuppgifterna har samlats in, särskilt förhållandet mellan de registrerade och den personuppgiftsansvarige.
- c) Personuppgifternas art, särskilt huruvida särskilda kategorier av personuppgifter behandlas i enlighet med artikel 9 eller huruvida personuppgifter om fällande domar i brottmål och överträdelser behandlas i enlighet med artikel 10.
- d) Eventuella konsekvenser för registrerade av den planerade fortsatta behandlingen.
- e) Förekomsten av lämpliga skyddsåtgärder, vilket kan inbegripa kryptering eller pseudonymisering.

Artikel 7

Villkor för samtycke

1. Om behandlingen grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter.
2. Om den registrerades samtycke lämnas i en skriftlig förklaring som också rör andra frågor, ska begäran om samtycke läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Om en del av förklaringen innebär en överträdelse av denna förordning, ska denna del inte vara bindande.
3. De registrerade ska ha rätt att när som helst återkalla sitt samtycke. Återkallandet av samtycket ska inte påverka lagligheten av behandling som grundar sig på samtycke, innan detta återkallas. Innan samtycke lämnas ska den registrerade informeras om detta. Det ska vara lika lätt att återkalla som att ge sitt samtycke.
4. Vid bedömning av huruvida samtycke är frivilligt ska största hänsyn bland annat tas till huruvida genomförandet av ett avtal, inbegripet tillhandahållandet av en tjänst, har gjorts beroende av samtycke till sådan behandling av personuppgifter som inte är nödvändig för genomförandet av det avtalet.

Artikel 8

Villkor som gäller barns samtycke avseende informationssamhällets tjänster

1. Vid erbjudande av informationssamhällets tjänster direkt till ett barn, ska vid tillämpningen av artikel 6.1 a behandling av personuppgifter som rör ett barn vara tillåten om barnet är minst 16 år. Om barnet är under 16 år ska sådan behandling vara tillåten endast om och i den mån samtycke ges eller godkänns av den person som har föräldraansvar för barnet.

Medlemsstaterna får i sin nationella rätt föreskriva en lägre ålder i detta syfte, under förutsättning att denna lägre ålder inte är under 13 år.

2. Den personuppgiftsansvarige ska göra rimliga ansträngningar för att i sådana fall kontrollera att samtycke ges eller godkänns av den person som har föräldraansvar för barnet, med hänsyn tagen till tillgänglig teknik.
3. Punkt 1 ska inte påverka tillämpningen av allmän avtalsrätt i medlemsstaterna, såsom bestämmelser om giltigheten, upprättandet eller effekten av ett avtal som gäller ett barn.

Artikel 9

Behandling av särskilda kategorier av personuppgifter

1. Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden.
2. Punkt 1 ska inte tillämpas om något av följande gäller:
 - a) Den registrerade har uttryckligen lämnat sitt samtycke till behandlingen av dessa personuppgifter för ett eller flera specifika ändamål, utom då unionsrätten eller medlemsstaternas nationella rätt föreskriver att förbudet i punkt 1 inte kan upphävas av den registrerade.
 - b) Behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd, i den omfattning detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt eller ett kollektivavtal som antagits med stöd av medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställs.
 - c) Behandlingen är nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.
 - d) Behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att behandlingen enbart rör sådana organs medlemmar eller tidigare medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta och personuppgifterna inte lämnas ut utanför det organet utan den registrerades samtycke.
 - e) Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.
 - f) Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet.
 - g) Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträfvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.
 - h) Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system, på grundval av unionsrätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet och under förutsättning att de villkor och skyddsåtgärder som avses i punkt 3 är uppfyllda.
 - i) Behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter, på grundval av unionsrätten eller medlemsstaternas nationella rätt, där lämpliga och specifika åtgärder för att skydda den registrerades rättigheter och friheter fastställs, särskilt tystnadsplikt.

- j) Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträfvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.
3. Personuppgifter som avses i punkt 1 får behandlas för de ändamål som avses i punkt 2 h, när uppgifterna behandlas av eller under ansvar av en yrkesutövare som omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ eller av en annan person som också omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ.
4. Medlemsstaterna får behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om hälsa.

Artikel 10

Behandling av personuppgifter som rör fällande domar i brottmål samt överträdelser

Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder enligt artikel 6.1 får endast utföras under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet.

Artikel 11

Behandling som inte kräver identifiering

1. Om de ändamål för vilka den personuppgiftsansvarige behandlar personuppgifter inte kräver eller inte längre kräver att den registrerade identifieras av den personuppgiftsansvarige, ska den personuppgiftsansvarige inte vara tvungen att bevara, förvärva eller behandla ytterligare information för att identifiera den registrerade endast i syfte att följa denna förordning.
2. Om den personuppgiftsansvarige, i de fall som avses i punkt 1 i denna artikel, kan visa att denne inte är i stånd att identifiera den registrerade, ska den personuppgiftsansvarige om möjligt informera den registrerade om detta. I sådana fall ska artiklarna 15–20 inte gälla, förutom när den registrerade för utövande av sina rättigheter i enlighet med dessa artiklar tillhandahåller ytterligare information som gör identifieringen möjlig.

KAPITEL III

Den registrerades rättigheter

Avsnitt 1

Insyn och villkor

Artikel 12

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

1. Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att till den registrerade tillhandahålla all information som avses i artiklarna 13 och 14 och all kommunikation enligt artiklarna 15–22 och 34 vilken avser behandling i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn. Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt.

2. Den personuppgiftsansvarige ska underlätta utövandet av den registrerades rättigheter i enlighet med artiklarna 15–22. I de fall som avses i artikel 11.2 får den personuppgiftsansvarige inte vägra att tillmötesgå den registrerades begäran om att utöva sina rättigheter enligt artiklarna 15–22, om inte den personuppgiftsansvarige visar att han eller hon inte är i stånd att identifiera den registrerade.

3. Den personuppgiftsansvarige ska på begäran utan onödigt dröjsmål och under alla omständigheter senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits enligt artiklarna 15–22. Denna period får vid behov förlängas med ytterligare två månader, med beaktande av hur komplicerad begäran är och antalet inkomna begäranden. Den personuppgiftsansvarige ska underrätta den registrerade om en sådan förlängning inom en månad från det att begäran mottagits samt ange orsakerna till förseningen. Om den registrerade lämnar begäran i elektronisk form, ska informationen om möjligt tillhandahållas i elektronisk form, om den registrerade inte begär något annat.

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

5. Information som tillhandahållits enligt artiklarna 13 och 14, all kommunikation och samtliga åtgärder som vidtas enligt artiklarna 15–22 och 34 ska tillhandahållas kostnadsfritt. Om begäranden från en registrerad är uppenbart ogrundade eller orimliga, särskilt på grund av deras repetitiva art, får den personuppgiftsansvarige antingen

- a) ta ut en rimlig avgift som täcker de administrativa kostnaderna för att tillhandahålla den information eller vidta den åtgärd som begärts, eller
- b) vägra att tillmötesgå begäran.

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

6. Utan att det påverkar tillämpningen av artikel 11 får den personuppgiftsansvarige, om denne har rimliga skäl att betvivla identiteten hos den fysiska person som lämnar in en begäran enligt artiklarna 15–21, begära att ytterligare information som är nödvändig för att bekräfta den registrerades identitet tillhandahålls.

7. Den information som ska tillhandahållas de registrerade i enlighet med artiklarna 13 och 14 får tillhandahållas kombinerad med standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över den planerade behandlingen. Om sådana symboler visas elektroniskt ska de vara maskinläsbara.

8. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 92 för att fastställa vilken information som ska visas med hjälp av symboler och förfaranden för att tillhandahålla sådana symboler.

Avsnitt 2

Information och tillgång till personuppgifter

Artikel 13

Information som ska tillhandahållas om personuppgifterna samlas in från den registrerade

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

- a) Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.
- b) Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall.
- c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.

- d) Om behandlingen är baserad på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen.
 - e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.
 - f) I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artikel 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.
2. Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige vid insamlingen av personuppgifterna lämna den registrerade följande ytterligare information, vilken krävs för att säkerställa rättvis och transparent behandling:
- a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
 - b) Att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.
 - c) Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, att det föreligger en rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.
 - d) Rätten att inge klagomål till en tillsynsmyndighet.
 - e) Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav eller ett krav som är nödvändigt för att ingå ett avtal samt huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att sådana uppgifter inte lämnas.
 - f) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.
3. Om den personuppgiftsansvarige avser att ytterligare behandla personuppgifterna för ett annat syfte än det för vilket de insamlades, ska den personuppgiftsansvarige före denna ytterligare behandling ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt punkt 2.
4. Punkterna 1, 2 och 3 ska inte tillämpas om och i den mån den registrerade redan förfogar över informationen.

Artikel 14

Information som ska tillhandahållas om personuppgifterna inte har erhållits från den registrerade

1. Om personuppgifterna inte har erhållits från den registrerade, ska den personuppgiftsansvarige förse den registrerade med följande information:
- a) Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.
 - b) Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall.
 - c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.
 - d) De kategorier av personuppgifter som behandlingen gäller.
 - e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.

- f) I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till en mottagare i ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artiklarna 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.
2. Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige lämna den registrerade följande information, vilken krävs för att säkerställa rättvis och transparent behandling när det gäller den registrerade:
- a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
 - b) Om behandlingen grundar sig på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen.
 - c) Förekomsten av rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade och att invända mot behandling samt rätten till dataportabilitet.
 - d) Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, rätten att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.
 - e) Rätten att inge klagomål till en tillsynsmyndighet.
 - f) Varifrån personuppgifterna kommer och i förekommande fall huruvida de har sitt ursprung i allmänt tillgängliga källor.
 - g) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.
3. Den personuppgiftsansvarige ska lämna den information som anges i punkterna 1 och 2
- a) inom en rimlig period efter det att personuppgifterna har erhållits, dock senast inom en månad, med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas,
 - b) om personuppgifterna ska användas för kommunikation med den registrerade, senast vid tidpunkten för den första kommunikationen med den registrerade, eller
 - c) om ett utlämnande till en annan mottagare förutses, senast när personuppgifterna lämnas ut för första gången.
4. Om den personuppgiftsansvarige avser att ytterligare behandla personuppgifterna för ett annat syfte än det för vilket de insamlades, ska den personuppgiftsansvarige före denna ytterligare behandling ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt punkt 2.
5. Punkterna 1–4 ska inte tillämpas i följande fall och i den mån
- a) den registrerade redan förfogar över informationen,
 - b) tillhandahållandet av sådan information visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning, särskilt för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, eller i den mån den skyldighet som avses i punkt 1 i den här artikeln sannolikt kommer att göra det omöjligt eller avsevärt försvåra uppfyllandet av målen med den behandlingen; i sådana fall ska den personuppgiftsansvarige vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen, inbegripet göra uppgifterna tillgängliga för allmänheten,
 - c) erhållande eller utlämnande av uppgifter uttryckligen föreskrivs genom unionsrätten eller genom en medlemsstats nationella rätt som den registrerade omfattas av och som fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen, eller
 - d) personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt, inbegripet andra lagstadgade sekretessförpliktelser.

*Artikel 15***Den registrerades rätt till tillgång**

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

- a) Ändamålen med behandlingen.
- b) De kategorier av personuppgifter som behandlingen gäller.
- c) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer.
- d) Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
- e) Förekomsten av rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifterna eller begränsningar av behandling av personuppgifter som rör den registrerade eller att invända mot sådan behandling.
- f) Rätten att inge klagomål till en tillsynsmyndighet.
- g) Om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån dessa uppgifter kommer.
- h) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

2. Om personuppgifterna överförs till ett tredjeland eller till en internationell organisation, ska den registrerade ha rätt till information om de lämpliga skyddsåtgärder som i enlighet med artikel 46 har vidtagits vid överföringen.

3. Den personuppgiftsansvarige ska förse den registrerade med en kopia av de personuppgifter som är under behandling. För eventuella ytterligare kopior som den registrerade begär får den personuppgiftsansvarige ta ut en rimlig avgift på grundval av de administrativa kostnaderna. Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat.

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

*Avsnitt 3***Rättelse och radering***Artikel 16***Rätt till rättelse**

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

*Artikel 17***Rätt till radering ("rätten att bli bortglömd")**

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

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

- b) Den registrerade återkallar det samtycke på vilket behandlingen grundar sig enligt artikel 6.1 a eller artikel 9.2 a och det finns inte någon annan rättslig grund för behandlingen.
- c) Den registrerade invänder mot behandlingen i enlighet med artikel 21.1 och det saknas berättigade skäl för behandlingen som väger tyngre, eller den registrerade invänder mot behandlingen i enlighet med artikel 21.2.
- d) Personuppgifterna har behandlats på olagligt sätt.
- e) Personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse i unionsrätten eller i medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av.
- f) Personuppgifterna har samlats in i samband med erbjudande av informationssamhällets tjänster, i de fall som avses i artikel 8.1.

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

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

- a) För att utöva rätten till yttrande- och informationsfrihet.
- b) För att uppfylla en rättslig förpliktelse som kräver behandling enligt unionsrätten eller enligt en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av eller för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige.
- c) För skäl som rör ett viktigt allmänt intresse på folkhälsoområdet enligt artikel 9.2 h och i samt artikel 9.3.
- d) För arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål enligt artikel 89.1, i den utsträckning som den rätt som avses i punkt 1 sannolikt omöjliggör eller avsevärt försvårar uppnåendet av syftet med den behandlingen.
- e) För att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

Artikel 18

Rätt till begränsning av behandling

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

- a) Den registrerade bestrider personuppgifternas korrekthet, under en tid som ger den personuppgiftsansvarige möjlighet att kontrollera om personuppgifterna är korrekta.
- b) Behandlingen är olaglig och den registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning.
- c) Den personuppgiftsansvarige behöver inte längre personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.
- d) Den registrerade har invänt mot behandling i enlighet med artikel 21.1 i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.

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

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

Artikel 19

Anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling

Den personuppgiftsansvarige ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling som skett i enlighet med artiklarna 16, 17.1 och 18, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Artikel 20

Rätt till dataportabilitet

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

- a) behandlingen grundar sig på samtycke enligt artikel 6.1 a eller artikel 9.2 a eller på ett avtal enligt artikel 6.1 b, och
- b) behandlingen sker automatiserat.

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

3. Utövandet av den rätt som avses i punkt 1 i den här artikeln ska inte påverka tillämpningen av artikel 17. Den rätten ska inte gälla i fråga om en behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige.

4. Den rätt som avses i punkt 1 får inte påverka andras rättigheter och friheter på ett ogynnsamt sätt.

Avsnitt 4

Rätt att göra invändningar och automatiserat individuellt beslutsfattande

Artikel 21

Rätt att göra invändningar

1. Den registrerade ska, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på artikel 6.1 e eller f, inbegripet profilering som grundar sig på dessa bestämmelser. Den personuppgiftsansvarige får inte längre behandla personuppgifterna såvida denne inte kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.

2. Om personuppgifterna behandlas för direkt marknadsföring ska den registrerade ha rätt att när som helst invända mot behandling av personuppgifter som avser honom eller henne för sådan marknadsföring, vilket inkluderar profilering i den utsträckning som denna har ett samband med sådan direkt marknadsföring.

3. Om den registrerade invänder mot behandling för direkt marknadsföring ska personuppgifterna inte längre behandlas för sådana ändamål.

4. Senast vid den första kommunikationen med den registrerade ska den rätt som avses i punkterna 1 och 2 uttryckligen meddelas den registrerade och redovisas tydligt, klart och åtskilt från eventuell annan information.
5. När det gäller användningen av informationssamhällets tjänster, och trots vad som sägs i direktiv 2002/58/EG, får den registrerade utöva sin rätt att göra invändningar på automatiserat sätt med användning av tekniska specifikationer.
6. Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska den registrerade, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att göra invändningar mot behandling av personuppgifter avseende honom eller henne om inte behandlingen är nödvändig för att utföra en uppgift av allmänt intresse.

Artikel 22

Automatiserat individuellt beslutsfattande, inbegripet profilering

1. Den registrerade ska ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne.
2. Punkt 1 ska inte tillämpas om beslutet
 - a) är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige,
 - b) tillåts enligt unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av och som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen, eller
 - c) grundar sig på den registrerades uttryckliga samtycke.
3. I fall som avses i punkt 2 a och c ska den personuppgiftsansvarige genomföra lämpliga åtgärder för att säkerställa den registrerades rättigheter, friheter och rättsliga intressen, åtminstone rätten till personlig kontakt med den personuppgiftsansvarige för att kunna uttrycka sin åsikt och bestrida beslutet.
4. Beslut enligt punkt 2 får inte grunda sig på de särskilda kategorier av personuppgifter som avses i artikel 9.1, såvida inte artikel 9.2 a eller g gäller och lämpliga åtgärder som ska skydda den registrerades berättigade intressen har vidtagits.

Avsnitt 5

Begränsningar

Artikel 23

Begränsningar

1. Det ska vara möjligt att i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige eller personuppgiftsbiträdet omfattas av införa en lagstiftningsåtgärd som begränsar tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i artiklarna 12–22 och 34, samt artikel 5 i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 12–22, om en sådan begränsning sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa
 - a) den nationella säkerheten,
 - b) försvaret,
 - c) den allmänna säkerheten,

- d) förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten,
 - e) andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet,
 - f) skydd av rättsväsendets oberoende och rättsliga åtgärder,
 - g) förebyggande, förhindrande, utredning, avslöjande och lagföring av överträdelser av etiska regler som gäller för lagreglerade yrken,
 - h) en tillsyns-, inspektions- eller regleringsfunktion som, även i enstaka fall, har samband med myndighetsutövning i fall som nämns i a–e och g,
 - i) skydd av den registrerade eller andras rättigheter och friheter,
 - j) verkställighet av civilrättsliga krav.
2. Framför allt ska alla lagstiftningsåtgärder som avses i punkt 1 innehålla specifika bestämmelser åtminstone, när så är relevant, avseende
- a) ändamålen med behandlingen eller kategorierna av behandling,
 - b) kategorierna av personuppgifter,
 - c) omfattningen av de införda begränsningarna,
 - d) skyddsåtgärder för att förhindra missbruk eller olaglig tillgång eller överföring,
 - e) specificeringen av den personuppgiftsansvarige eller kategorierna av personuppgiftsansvariga,
 - f) lagringstiden samt tillämpliga skyddsåtgärder med beaktande av behandlingens art, omfattning och ändamål eller kategorierna av behandling,
 - g) riskerna för de registrerades rättigheter och friheter, och
 - h) de registrerades rätt att bli informerade om begränsningen, såvida detta inte kan inverka menligt på begränsningen.

KAPITEL IV

Personuppgiftsansvarig och personuppgiftsbiträde

Avsnitt 1

Allmänna skyldigheter

Artikel 24

Den personuppgiftsansvariges ansvar

1. Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.
2. Om det står i proportion till behandlingen, ska de åtgärder som avses i punkt 1 omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.
3. Tillämpningen av godkända uppförandekoder som avses i artikel 40 eller godkända certifieringsmekanismer som avses i artikel 42 får användas för att visa att den personuppgiftsansvarige fullgör sina skyldigheter.

*Artikel 25***Inbyggt dataskydd och dataskydd som standard**

1. Med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder – såsom pseudonymisering – vilka är utformade för ett effektivt genomförande av dataskyddsprinciper – såsom uppgiftsminimering – och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i denna förordning uppfylls och den registrerades rättigheter skyddas.
2. Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.
3. En godkänd certifieringsmekanism i enlighet med artikel 42 får användas för att visa att kraven i punkterna 1 och 2 i den här artikeln följs.

*Artikel 26***Gemensamt personuppgiftsansvariga**

1. Om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. Gemensamt personuppgiftsansvariga ska under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt denna förordning, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artiklarna 13 och 14, genom ett inbördes arrangemang, såvida inte de personuppgiftsansvarigas respektive skyldigheter fastställs genom unionsrätten eller en medlemsstats nationella rätt som de personuppgiftsansvariga omfattas av. Inom ramen för arrangemanget får en gemensam kontaktpunkt för de personuppgiftsansvariga utses.
2. Det arrangemang som avses i punkt 1 ska på lämpligt sätt återspegla de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade. Det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade.
3. Oavsett formerna för det arrangemang som avses i punkt 1 får den registrerade utöva sina rättigheter enligt denna förordning med avseende på och emot var och en av de personuppgiftsansvariga.

*Artikel 27***Företrädare för personuppgiftsansvariga eller personuppgiftsbiträden som inte är etablerade i unionen**

1. Om artikel 3.2 tillämpas ska den personuppgiftsansvarige eller personuppgiftsbiträdet skriftligen utse en företrädare i unionen.
2. Skyldigheten enligt punkt 1 i denna artikel ska inte gälla
 - a) tillfällig behandling som inte omfattar behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller behandling av personuppgifter avseende fällande domar i brottmål samt överträdelser, som avses i artikel 10, och som sannolikt inte kommer att medföra en risk för fysiska personers rättigheter och friheter, med hänsyn till behandlingens art, sammanhang, omfattning och ändamål, eller
 - b) en offentlig myndighet eller ett offentligt organ.

3. Företrädaren ska vara etablerad i en av de medlemsstater där de registrerade, vars personuppgifter behandlas i samband med att de erbjuds varor eller tjänster, eller vars beteende övervakas, befinner sig.
4. Företrädaren ska på den personuppgiftsansvariges eller personuppgiftsbiträdets uppdrag, utöver eller i stället för den personuppgiftsansvarige eller personuppgiftsbiträdet, fungera som kontaktperson för i synnerhet tillsynsmyndigheter och registrerade, i alla frågor som har anknytning till behandlingen, i syfte att säkerställa efterlevnad av denna förordning.
5. Att den personuppgiftsansvarige eller personuppgiftsbiträdet utser en företrädare ska inte påverka de rättsliga åtgärder som skulle kunna inledas mot den personuppgiftsansvarige eller personuppgiftsbiträdet.

Artikel 28

Personuppgiftsbiträden

1. Om en behandling ska genomföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas.
2. Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.
3. När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige och i vilken föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges. I det avtalet eller den rättsakten ska det särskilt föreskrivas att personuppgiftsbiträdet
 - a) endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av, och i så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt,
 - b) säkerställer att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt,
 - c) ska vidta alla åtgärder som krävs enligt artikel 32,
 - d) ska respektera de villkor som avses i punkterna 2 och 4 för anlitandet av ett annat personuppgiftsbiträde,
 - e) med tanke på behandlingens art, ska hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter i enlighet med kapitel III,
 - f) ska bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå,
 - g) beroende på vad den personuppgiftsansvarige väljer, ska radera eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av behandlingstjänster har avslutats, och radera befintliga kopior såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt, och
 - h) ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i denna artikel har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige.

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

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

5. Ett personuppgiftsbiträdes anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att tillräckliga garantier tillhandahålls, så som avses punkterna 1 och 4 i den här artikeln.

6. Det avtal eller den andra rättsakt som avses i punkterna 3 och 4 i den här artikeln får, utan att det påverkar tillämpningen av ett enskilt avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet, helt eller delvis baseras på sådana standardavtalsklausuler som avses i punkterna 7 och 8 i den här artikeln, inbegripet när de ingår i en certifiering som i enlighet med artiklarna 42 och 43 beviljats den personuppgiftsansvarige eller personuppgiftsbiträdet.

7. Kommissionen får fastställa standardavtalsklausuler för de frågor som avses i punkterna 3 och 4 i den här artikeln, i enlighet med det granskningsförfarande som avses i artikel 93.2.

8. En tillsynsmyndighet får fastställa standardavtalsklausuler för de frågor som avses i punkterna 3 och 4 i den här artikeln, i enlighet med den mekanism för enhetlighet som avses i artikel 63.

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

10. Om ett personuppgiftsbiträde överträder denna förordning genom att fastställa ändamålen med och medlen för behandlingen, ska personuppgiftsbiträdet anses vara personuppgiftsansvarig med avseende på den behandlingen, utan att det påverkar tillämpningen av artiklarna 82, 83 och 84.

Artikel 29

Behandling under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende

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

Artikel 30

Register över behandling

1. Varje personuppgiftsansvarig och, i tillämpliga fall, dennes företrädare ska föra ett register över behandling som utförts under dess ansvar. Detta register ska innehålla samtliga följande uppgifter:

- a) Namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet.
- b) Ändamålen med behandlingen.
- c) En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.

- d) De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer.
 - e) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentationen av lämpliga skyddsåtgärder.
 - f) Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
 - g) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1.
2. Varje personuppgiftsbiträde och, i tillämpliga fall, dennes företrädare ska föra ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning, som omfattar följande:
- a) Namn och kontaktuppgifter för personuppgiftsbiträdet eller personuppgiftsbiträdena och för varje personuppgiftsansvarig för vars räkning personuppgiftsbiträdet agerar, och, i tillämpliga fall, för den personuppgiftsansvariges eller personuppgiftsbiträdets företrädare samt dataskyddsombudet.
 - b) De kategorier av behandling som har utförts för varje personuppgiftsansvariges räkning.
 - c) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentationen av lämpliga skyddsåtgärder.
 - d) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1.
3. De register som avses i punkterna 1 och 2 ska upprättas skriftligen, inbegripet i elektronisk form.
4. På begäran ska den personuppgiftsansvarige eller personuppgiftsbiträdet samt, i tillämpliga fall, den personuppgiftsansvariges eller personuppgiftsbiträdets företrädare göra registret tillgängligt för tillsynsmyndigheten.
5. De skyldigheter som anges i punkterna 1 och 2 ska inte gälla för ett företag eller en organisation som sysselsätter färre än 250 personer såvida inte den behandling som utförs sannolikt kommer att medföra en risk för registrerades rättigheter och friheter, behandlingen inte är tillfällig eller behandlingen omfattar särskilda kategorier av uppgifter som avses i artikel 9.1 eller personuppgifter om fällande domar i brottmål samt överträdelser som avses i artikel 10.

Artikel 31

Samarbete med tillsynsmyndigheten

Den personuppgiftsansvarige och personuppgiftsbiträdet samt, i tillämpliga fall, deras företrädare ska på begäran samarbeta med tillsynsmyndigheten vid utförandet av dennes uppgifter.

Avsnitt 2

Säkerhet för personuppgifter

Artikel 32

Säkerhet i samband med behandlingen

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

- a) pseudonymisering och kryptering av personuppgifter,

- b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlings-systemen och -tjänsterna,
 - c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
 - d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.
2. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförs, lagrats eller på annat sätt behandlats.
3. Anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att kraven i punkt 1 i den här artikeln följs.
4. Den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbitrådets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det.

Artikel 33

Anmälan av en personuppgiftsincident till tillsynsmyndigheten

1. Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig i enlighet med artikel 55, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.
2. Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident.
3. Den anmälan som avses i punkt 1 ska åtminstone
 - a) beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,
 - b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,
 - c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och
 - d) beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.
4. Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.
5. Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av denna artikel.

Artikel 34

Information till den registrerade om en personuppgiftsincident

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

2. Den information till den registrerade som avses i punkt 1 i denna artikel ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone de upplysningar och åtgärder som avses i artikel 33.3 b, c och d.
3. Information till den registrerade i enlighet med punkt 1 krävs inte om något av följande villkor är uppfyllt:
 - a) Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som ska göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna, såsom kryptering.
 - b) Den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter som avses i punkt 1 sannolikt inte längre kommer att uppstå.
 - c) Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.
4. Om den personuppgiftsansvarige inte redan har informerat den registrerade om personuppgiftsincidenten får tillsynsmyndigheten, efter att ha bedömt sannolikheten för att personuppgiftsincidenten medför en hög risk, kräva att personuppgiftsbiträdet gör det eller får besluta att något av de villkor som avses i punkt 3 uppfylls.

Avsnitt 3

Konsekvensbedömning avseende dataskydd samt föregående samråd

Artikel 35

Konsekvensbedömning avseende dataskydd

1. Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.
2. Den personuppgiftsansvarige ska rådfråga dataskyddsombudet, om ett sådant utsetts, vid genomförande av en konsekvensbedömning avseende dataskydd.
3. En konsekvensbedömning avseende dataskydd som avses i punkt 1 ska särskilt krävas i följande fall:
 - a) En systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer.
 - b) Behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller av personuppgifter som rör fällande domar i brottmål och överträdelse som avses i artikel 10.
 - c) Systematisk övervakning av en allmän plats i stor omfattning.
4. Tillsynsmyndigheten ska upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd i enlighet med punkt 1. Tillsynsmyndigheten ska översända dessa förteckningar till den styrelse som avses i artikel 68.
5. Tillsynsmyndigheten får också upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som inte kräver någon konsekvensbedömning avseende dataskydd. Tillsynsmyndigheten ska översända dessa förteckningar till styrelsen.
6. Innan de förteckningar som avses i punkterna 4 och 5 antas ska den behöriga tillsynsmyndigheten tillämpa den mekanism för enhetlighet som avses i artikel 63 om en sådan förteckning inbegriper behandling som rör erbjudandet av varor eller tjänster till registrerade, eller övervakning av deras beteende i flera medlemsstater, eller som väsentligt kan påverka den fria rörligheten för personuppgifter i unionen.

7. Bedömningen ska innehålla åtminstone
- a) en systematisk beskrivning av den planerade behandlingen och behandlingens syften, inbegripet, när det är lämpligt, den personuppgiftsansvariges berättigade intresse,
 - b) en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,
 - c) en bedömning av de risker för de registrerades rättigheter och friheter som avses i punkt 1, och
 - d) de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att denna förordning efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.
8. De berörda personuppgiftsansvarigas eller personuppgiftsbiträdenas efterlevnad av godkända uppförandekoder enligt artikel 40 ska på lämpligt sätt beaktas vid bedömningen av konsekvenserna av de behandlingar som utförs av dessa personuppgiftsansvariga eller personuppgiftsbiträden, framför allt när det gäller att ta fram en konsekvensbedömning avseende dataskydd.
9. Den personuppgiftsansvarige ska, när det är lämpligt, inhämta synpunkter från de registrerade eller deras företrädare om den avsedda behandlingen, utan att det påverkar skyddet av kommersiella eller allmänna intressen eller behandlingens säkerhet.
10. Om behandling enligt artikel 6.1 c eller e har en rättslig grund i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av, reglerar den rätten den aktuella specifika behandlingsåtgärden eller serien av åtgärder i fråga och en konsekvensbedömning avseende dataskydd redan har genomförts som en del av en allmän konsekvensbedömning i samband med antagandet av denna rättsliga grund, ska punkterna 1–7 inte gälla, om inte medlemsstaterna anser det nödvändigt att utföra en sådan bedömning före behandlingen.
11. Den personuppgiftsansvarige ska vid behov genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen avseende dataskydd åtminstone när den risk som behandlingen medför förändras.

Artikel 36

Förhandssamråd

1. Den personuppgiftsansvarige ska samråda med tillsynsmyndigheten före behandling om en konsekvensbedömning avseende dataskydd enligt artikel 35 visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken.
2. Om tillsynsmyndigheten anser att den planerade behandling som avses i punkt 1 skulle strida mot denna förordning, särskilt om den personuppgiftsansvarige inte i tillräcklig mån har fastställt eller reducerat risken, ska tillsynsmyndigheten inom en period på högst åtta veckor från det att begäran om samråd mottagits, ge den personuppgiftsansvarige och i tillämpliga fall personuppgiftsbiträdet skriftliga råd och får utnyttja alla de befogenheter som den har enligt artikel 58. Denna period får förlängas med sex veckor beroende på hur komplicerad den planerade behandlingen är. Tillsynsmyndigheten ska informera den personuppgiftsansvarige och, i tillämpliga fall, personuppgiftsbiträdet om en sådan förlängning inom en månad från det att begäran om samråd mottagits, tillsammans med orsakerna till förseningen. Dessa perioder får tillfälligt upphöra att löpa i avvaktan på att tillsynsmyndigheten erhåller den information som den har begärt med tanke på samrådet.
3. Vid samråd med tillsynsmyndigheten enligt punkt 1 ska den personuppgiftsansvarige till tillsynsmyndigheten lämna
- a) i tillämpliga fall de respektive ansvarsområdena för de personuppgiftsansvariga, gemensamt personuppgiftsansvariga och personuppgiftsbiträden som medverkar vid behandlingen, framför allt vid behandling inom en koncern,
 - b) ändamålen med och medlen för den avsedda behandlingen,
 - c) de åtgärder som vidtas och de garantier som lämnas för att skydda de registrerades rättigheter och friheter enligt denna förordning,
 - d) i tillämpliga fall kontaktuppgifter till dataskyddsombudet,

- e) konsekvensbedömningen avseende dataskydd enligt artikel 35, och
- f) all annan information som begärs av tillsynsmyndigheten.

4. Medlemsstaterna ska samråda med tillsynsmyndigheten vid utarbetandet av ett förslag till lagstiftningsåtgärd som ska antas av ett nationellt parlament eller av en regleringsåtgärd som grundar sig på en sådan lagstiftningsåtgärd som rör behandling.

5. Trots vad som sägs i punkt 1 får det i medlemsstaternas nationella rätt krävas att personuppgiftsansvariga ska samråda med, och erhålla förhandstillstånd av, tillsynsmyndigheten när det gäller en personuppgiftsansvarigs behandling för utförandet av en uppgift som den personuppgiftsansvarige utför av allmänt intresse, inbegripet behandling avseende social trygghet och folkhälsa.

Avsnitt 4

Dataskyddsombud

Artikel 37

Utnämning av dataskyddsombudet

1. Den personuppgiftsansvarige och personuppgiftsbiträdet ska under alla omständigheter utnämna ett dataskyddsombud om
 - a) behandlingen genomförs av en myndighet eller ett offentligt organ, förutom när detta sker som en del av domstolarnas dömande verksamhet,
 - b) den personuppgiftsansvariges eller personuppgiftsbitrådets kärnverksamhet består av behandling som, på grund av sin karaktär, sin omfattning och/eller sina ändamål, kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller
 - c) den personuppgiftsansvariges eller personuppgiftsbitrådets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter i enlighet med artikel 9 och personuppgifter som rör fällande domar i brottmål och överträdelse, som avses i artikel 10.
2. En koncern får utnämna ett enda dataskyddsombud om det på varje etableringsort är lätt att nå ett dataskyddsombud.
3. Om den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet eller ett offentligt organ, får ett enda dataskyddsombud utnämnas för flera sådana myndigheter eller organ, med hänsyn till deras organisationsstruktur och storlek.
4. I andra fall än de som avses i punkt 1 får eller, om så krävs enligt unionsrätten eller medlemsstaternas nationella rätt, ska den personuppgiftsansvarige eller personuppgiftsbiträdet eller sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden utnämna ett dataskyddsombud. Dataskyddsombudet får agera för sådana sammanslutningar och andra organ som företräder personuppgiftsansvariga eller personuppgiftsbiträden.
5. Dataskyddsombudet ska utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i artikel 39.
6. Dataskyddsombudet får ingå i den personuppgiftsansvariges eller personuppgiftsbitrådets personal, eller utföra uppgifterna på grundval av ett tjänsteavtal.
7. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.

Artikel 38

Dataskyddsombudets ställning

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

2. Den personuppgiftsansvarige och personuppgiftsbiträdet ska stödja dataskyddsombudet i utförandet av de uppgifter som avses i artikel 39 genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap.
3. Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att uppgiftskyddsombudet inte tar emot instruktioner som gäller utförandet av dessa uppgifter. Han eller hon får inte avsättas eller bli föremål för sanktioner av den personuppgiftsansvarige eller personuppgiftsbiträdet för att ha utfört sina uppgifter. Dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbitrådets högsta förvaltningsnivå.
4. Den registrerade får kontakta dataskyddsombudet med avseende på alla frågor som rör behandlingen av dennes personuppgifter och utövandet av dennes rättigheter enligt denna förordning.
5. Dataskyddsombudet ska, när det gäller dennes genomförande av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt.
6. Dataskyddsombudet får fullgöra andra uppgifter och uppdrag. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska se till att sådana uppgifter och uppdrag inte leder till en intressekonflikt.

Artikel 39

Dataskyddsombudets uppgifter

1. Dataskyddsombudet ska ha minst följande uppgifter:
 - a) Att informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar om deras skyldigheter enligt denna förordning och andra av unionens eller medlemsstaternas dataskyddsbestämmelser.
 - b) Att övervaka efterlevnaden av denna förordning, av andra av unionens eller medlemsstaternas dataskyddsbestämmelser och av den personuppgiftsansvariges eller personuppgiftsbitrådets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.
 - c) Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den enligt artikel 35.
 - d) Att samarbeta med tillsynsmyndigheten.
 - e) Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, inbegripet det förhandssamråd som avses i artikel 36, och vid behov samråda i alla andra frågor.
2. Dataskyddsombudet ska vid utförandet av sina uppgifter ta vederbörlig hänsyn till de risker som är förknippade med behandling, med beaktande av behandlingens art, omfattning, sammanhang och syften.

Avsnitt 5

Uppförandekod och certifiering

Artikel 40

Uppförandekoder

1. Medlemsstaterna, tillsynsmyndigheterna, styrelsen och kommissionen ska uppmuntra utarbetandet av uppförandekoder avsedda att bidra till att denna förordning genomförs korrekt, med hänsyn till särdragen hos de olika sektorer där behandling sker, och de särskilda behoven hos mikroföretag samt små och medelstora företag.
2. Sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden får utarbeta uppförandekoder, eller ändra eller utöka sådana koder, i syfte att specificera tillämpningen av denna förordning, till exempel när det gäller
 - a) rättvis och öppen behandling,

- b) personuppgiftsansvarigas berättigade intressen i särskilda sammanhang,
- c) insamling av personuppgifter,
- d) pseudonymisering av personuppgifter,
- e) information till allmänheten och de registrerade,
- f) utövande av registrerades rättigheter,
- g) information till och skydd av barn samt metoderna för att erhålla samtycke från de personer som har föräldraansvar för barn,
- h) åtgärder och förfaranden som avses i artiklarna 24 och 25 samt åtgärder för att säkerställa säkerhet vid behandling i enlighet med artikel 32,
- i) anmälan av personuppgiftsincidenter till tillsynsmyndigheter och meddelande av sådana personuppgiftsincidenter till registrerade,
- j) överföring av personuppgifter till tredjeländer eller internationella organisationer,
- k) utomrättsliga förfaranden och andra tvistlösningsförfaranden för lösande av tvister mellan personuppgiftsansvariga och registrerade när det gäller behandling, utan att detta påverkar registrerades rättigheter enligt artiklarna 77 och 79.

3. Uppförandekoder som är godkända i enlighet med punkt 5 i denna artikel och som har allmän giltighet enligt punkt 9 i denna artikel får, förutom att de iakttas av personuppgiftsansvariga eller personuppgiftsbiträden som omfattas av denna förordning, även iakttas av personuppgiftsansvariga eller personuppgiftsbiträden som inte omfattas av denna förordning enligt artikel 3, för att tillhandahålla lämpliga garantier inom ramen för överföringar av personuppgifter till tredjeländer eller internationella organisationer enligt villkoren i artikel 46.2 e. Sådana personuppgiftsansvariga eller personuppgiftsbiträden ska göra bindande och verkställbara åtaganden, genom avtal eller andra rättsligt bindande instrument, att tillämpa dessa lämpliga garantier inbegripet när det gäller registrerades rättigheter.

4. Den uppförandekod som avses i punkt 2 i den här artikeln ska innehålla mekanismer som gör det möjligt för det organ som avses i artikel 41.1 att utföra den obligatoriska övervakningen av att dess bestämmelser efterlevs av personuppgiftsansvariga och personuppgiftsbiträden som tillämpar den, utan att det påverkar uppgifter eller befogenheter för de tillsynsmyndigheter som är behöriga enligt artikel 55 eller 56.

5. Sammanslutningar och andra organ som avses i punkt 2 i den här artikeln som avser att utarbeta en uppförandekod eller ändra eller utöka befintliga uppförandekoder ska inte utkastet till uppförandekod, ändringen eller utökningen till den tillsynsmyndighet som är behörig enligt artikel 55. Tillsynsmyndigheten ska yttra sig om huruvida utkastet till uppförandekod, ändring eller utökning överensstämmer med denna förordning och ska godkänna ett det utkastet till kod, ändring eller utökning om den finner att tillräckliga garantier tillhandahålls.

6. Om utkastet till kod, eller en ändring eller utökning, godkänns i enlighet med punkt 5, och om den berörda uppförandekoden inte avser behandling i flera medlemsstater, ska tillsynsmyndigheten registrera och offentliggöra uppförandekoden.

7. Om ett utkast till uppförandekod avser behandling i flera medlemsstater ska den tillsynsmyndighet som är behörig enligt artikel 55 innan den godkänner utkastet till kod, ändring eller utökning, inom ramen för det förfarande som avses i artikel 63 överlämna det till styrelsen som ska avge ett yttrande om huruvida utkastet till kod, ändring eller utökning är förenligt med denna förordning eller, i de fall som avses i punkt 3 i den här artikeln, tillhandahåller lämpliga garantier.

8. Om det i det yttrande som avses i punkt 7 bekräftas att utkastet till kod, ändring eller utökning är förenligt med denna förordning, eller, i de fall som avses i punkt 3, tillhandahåller lämpliga garantier, ska styrelsen inlämna sitt yttrande till kommissionen.

9. Kommissionen får, genom genomförandeakter, besluta att den godkända koden, ändringen eller utökningen som getts in till den enligt punkt 8 i den här artikeln har allmän giltighet inom unionen. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

10. Kommissionen ska se till att de godkända koder om vilka det har beslutats att de har allmän giltighet enligt punkt 9 offentliggörs på lämpligt sätt.

11. Styrelsen ska samla alla godkända uppförandekoder, ändringar och utökningar i ett register och offentliggöra dem på lämpligt sätt.

Artikel 41

Övervakning av godkända uppförandekoder

1. Utan att det påverkar den berörda tillsynsmyndighetens uppgifter och befogenheter enligt artiklarna 57 och 58 får övervakningen av efterlevnaden av en uppförandekod i enlighet med artikel 40 utföras av ett organ som har en lämplig expertnivå i förhållande till kodens syfte och som ackrediteras för detta ändamål av den behöriga tillsynsmyndigheten.

2. Ett organ som avses i punkt 1 får ackrediteras för att övervaka efterlevnaden av en uppförandekod om detta organ har

a) visat sitt oberoende och sin expertis i förhållande till uppförandekodens syfte på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande,

b) upprättat förfaranden varigenom det kan bedöma de berörda personuppgiftsansvarigas och personuppgiftsbiträdenas lämplighet för att tillämpa uppförandekoden, övervaka att de efterlever dess bestämmelser och regelbundet se över hur den fungerar,

c) upprättat förfaranden och strukturer för att hantera klagomål om överträdelser av uppförandekoden eller det sätt på vilket uppförandekoden har tillämpats, eller tillämpas, av en personuppgiftsansvarig eller ett personuppgiftsbiträde, och för att göra dessa förfaranden och strukturer synliga för registrerade och för allmänheten, och

d) på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande visat att dess uppgifter och uppdrag inte leder till en intressekonflikt.

3. Den behöriga tillsynsmyndigheten ska inlämna utkastet till kriterier för ackreditering av ett organ som avses i punkt 1 i den här artikeln till styrelsen i enlighet med den mekanism för enhetlighet som avses i artikel 63.

4. Utan att det påverkar den behöriga tillsynsmyndighetens uppgifter och befogenheter och tillämpningen av bestämmelserna i kapitel VIII ska ett organ som avses i punkt 1 i denna artikel, med förbehåll för tillräckliga skyddsåtgärder, vidta lämpliga åtgärder i fall av en personuppgiftsansvarigs eller ett personuppgiftsbiträdes överträdelse av uppförandekoden, inbegripet avstängning eller uteslutande av den personuppgiftsansvarige eller personuppgiftsbiträdet från uppförandekoden. Det ska informera den behöriga tillsynsmyndigheten om sådana åtgärder och skälen för att de vidtagits.

5. Den behöriga tillsynsmyndigheten ska återkalla ackrediteringen av ett organ som avses i punkt 1 om villkoren för ackrediteringen inte, eller inte längre, uppfylls eller om åtgärder som vidtagits av organet strider mot denna förordning.

6. Denna artikel ska inte gälla behandling som utförs av offentliga myndigheter och organ.

Artikel 42

Certifiering

1. Medlemsstaterna, tillsynsmyndigheterna, styrelsen och kommissionen ska uppmuntra, särskilt på unionsnivå, införandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som syftar till att visa att personuppgiftsansvarigas eller personuppgiftsbiträdens behandling är förenlig med denna förordning. De särskilda behoven hos mikroföretag samt små och medelstora företag ska beaktas.

2. Certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som är godkända enligt punkt 5 i denna artikel får, förutom att de iakttas av personuppgiftsansvariga eller personuppgiftsbiträden som omfattas av denna förordning, inrättas för att visa att det föreligger lämpliga garantier som tillhandahålls av personuppgiftsansvariga och personuppgiftsbiträden som inte omfattas av denna förordning enligt artikel 3, inom ramen för överföringar av personuppgifter till tredjeländer eller internationella organisationer enligt villkoren i artikel 46.2 f. Sådana personuppgiftsansvariga eller personuppgiftsbiträden ska göra bindande och verkställbara åtaganden, genom avtal eller andra rättsligt bindande instrument, att tillämpa dessa lämpliga garantier, inbegripet när det gäller registrerades rättigheter.
3. Certifieringen ska vara frivillig och tillgänglig via ett öppet förfarande.
4. En certifiering i enlighet med denna artikel minskar inte den personuppgiftsansvariges eller personuppgiftsbiträdets ansvar för att denna förordning efterlevs och påverkar inte uppgifter och befogenheter för de tillsynsmyndigheter som är behöriga enligt artikel 55 eller 56.
5. En certifiering i enlighet med denna artikel ska utfärdas av de certifieringsorgan som avses i artikel 43 eller av den behöriga tillsynsmyndigheten på grundval av kriterier som godkänts av den behöriga myndigheten enligt artikel 58.3 eller av styrelsen enligt artikel 63. Om kriterierna har godkänts av styrelsen får detta leda till en gemensam certifiering, det europeiska sigillet för dataskydd.
6. Den personuppgiftsansvarige eller det personuppgiftsbiträde som låter sin behandling av uppgifter omfattas av certifieringsmekanismen ska förse det certifieringsorgan som avses i artikel 43 eller, i tillämpliga fall, den behöriga tillsynsmyndigheten, med all information och tillgång till behandlingsförfaranden som krävs för att genomföra certifieringsförfarandet.
7. Certifiering ska utfärdas till en personuppgiftsansvarig eller ett personuppgiftsbiträde för en period på högst tre år och får förnyas på samma villkor under förutsättning att kraven fortsätter att vara uppfyllda. Certifiering ska, i tillämpliga fall, återkallas av de certifieringsorgan som avses i artikel 43 eller av den behöriga tillsynsmyndigheten om kraven för certifieringen inte eller inte längre uppfylls.
8. Styrelsen ska samla alla certifieringsmekanismer och sigill och märkningar för dataskydd i ett register och offentliggöra dem på lämpligt sätt.

Artikel 43

Certifieringsorgan

1. Utan att det påverkar den behöriga tillsynsmyndighetens uppgifter och befogenheter enligt artiklarna 57 och 58 ska certifieringsorgan som har lämplig nivå av expertis i fråga om dataskydd, efter att ha informerat tillsynsmyndigheten för att den ska kunna utöva sina befogenheter enligt artikel 58.2 h när så är nödvändigt, utfärda och förnya certifiering. Medlemsstat ska säkerställa att dessa certifieringsorgan är ackrediterade av en av eller båda följande:
 - a) Den tillsynsmyndighet som är behörig enligt artikel 55 eller 56,
 - b) det nationella ackrediteringsorgan som utsetts i enlighet med Europaparlamentets och rådets förordning (EG) nr 765/2008 ⁽¹⁾ i enlighet med EN-ISO/IEC 17065/2012 och med de ytterligare krav som fastställts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56.
2. Certifieringsorgan som avses i punkt 1 får ackrediteras i enlighet med den punkten endast om de har
 - a) visat oberoende och expertis i förhållande till certifieringens syfte på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande,

⁽¹⁾ Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

- b) förbundit sig att respektera de kriterier som avses i artikel 42.5 och godkänts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56, eller av styrelsen enligt artikel 63,
- c) upprättat förfaranden för utfärdande, periodisk översyn och återkallande av certifiering, sigill och märkningar för dataskydd,
- d) upprättat förfaranden och strukturer för att hantera klagomål om överträdelser av certifieringen eller det sätt på vilket certifieringen har tillämpats, eller tillämpas, av en personuppgiftsansvarig eller ett personuppgiftsbiträde, och för att göra dessa förfaranden och strukturer synliga för registrerade och för allmänheten, och
- e) på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande visat att deras uppgifter och uppdrag inte leder till en intressekonflikt.

3. Ackrediteringen av certifieringsorgan som avses i punkterna 1 och 2 i denna artikel ska ske på grundval av kriterier som godkänts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56, eller av styrelsen enligt artikel 63. I händelse av ackreditering enligt punkt 1 b i den här artikeln ska dessa krav komplettera dem som föreskrivs i förordning (EG) nr 765/2008 och de tekniska regler som beskriver certifieringsorganens metoder och förfaranden.

4. De certifieringsorgan som avses i punkt 1 ska ansvara för den korrekta bedömning som leder till certifieringen eller återkallelsen av certifieringen, utan att det påverkar den personuppgiftsansvariges eller personuppgiftsbitrådets ansvar att efterleva denna förordning. Ackrediteringen ska utfärdas för en period på högst fem år och får förnyas på samma villkor under förutsättning att certifieringsorganet uppfyller de krav som anges i denna artikel.

5. De certifieringsorgan som avses i punkt 1 ska informera de behöriga tillsynsmyndigheterna om orsakerna till beviljandet eller återkallelsen av den begärda certifieringen.

6. De krav som avses i punkt 3 i den här artikeln och de kriterier som avses i artikel 42.5 ska offentliggöras av tillsynsmyndigheten i ett lättillgängligt format. Tillsynsmyndigheterna ska också översända dessa krav och kriterier till styrelsen. Styrelsen ska samla alla certifieringsmekanismer och sigill för dataskydd i ett register och offentliggöra dem på lämpligt sätt.

7. Utan att det påverkar tillämpningen av kapitel VIII ska den behöriga tillsynsmyndigheten eller det nationella ackrediteringsorganet återkalla ett certifieringsorgans ackreditering enligt punkt 1 i denna artikel om villkoren för ackrediteringen inte, eller inte längre, uppfylls eller om åtgärder som vidtagits av certifieringsorganet strider mot denna förordning.

8. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 92 i syfte att närmare ange de krav som ska tas i beaktande för de certifieringsmekanismer för dataskydd som avses i artikel 42.1.

9. Kommissionen får anta genomförandeakter för att fastställa tekniska standarder för certifieringsmekanismer och sigill och märkningar för dataskydd samt rutiner för att främja och erkänna dessa certifieringsmekanismer, sigill och märkningar. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

KAPITEL V

Överföring av personuppgifter till tredjeländer eller internationella organisationer

Artikel 44

Allmän princip för överföring av uppgifter

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

Artikel 45

Överföring på grundval av ett beslut om adekvat skyddsnivå

1. Personuppgifter får överföras till ett tredjeland eller en internationell organisation om kommissionen har beslutat att tredjelandet, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå. En sådan överföring ska inte kräva något särskilt tillstånd.
 2. När kommissionen bedömer om en adekvat skyddsnivå föreligger ska den särskilt beakta
 - a) rättsstatsprincipen, respekten för de mänskliga rättigheterna och de grundläggande friheterna, relevant lagstiftning, både allmän lagstiftning och sektorslagstiftning, inklusive avseende allmän säkerhet, försvar, nationell säkerhet och straffrätt och offentliga myndigheters tillgång till personuppgifter samt tillämpningen av sådan lagstiftning, dataskyddsregler, yrkesregler och säkerhetsbestämmelser, inbegripet regler för vidare överföring av personuppgifter till ett annat tredjeland eller en annan internationell organisation, som ska följas i det landet eller den internationella organisationen, rättspraxis samt faktiska och verkställbara rättigheter för registrerade och effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs,
 - b) huruvida det finns en eller flera effektivt fungerande oberoende tillsynsmyndigheter i tredjelandet, eller som utövar tillsyn över den internationella organisationen, som har ansvar för att säkerställa och kontrollera att dataskyddsregler följs, inklusive lämpliga verkställighetsbefogenheter, ge de registrerade råd och assistans när det gäller utövandet av deras rättigheter och samarbeta med medlemsstaternas tillsynsmyndigheter, och
 - c) vilka internationella åtaganden det berörda tredjelandet eller den berörda internationella organisationen har gjort, eller andra skyldigheter som följer av rättsligt bindande konventioner eller instrument samt av dess deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter.
 3. Kommissionen får, efter att ha bedömt om det föreligger en adekvat skyddsnivå, genom en genomförandeakt besluta att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland, eller en internationell organisation säkerställer en adekvat skyddsnivå i den mening som avses i punkt 2 i den här artikeln. Genomförandeakten ska inrätta en mekanism för regelbunden översyn, minst vart fjärde år, som ska beakta all relevant utveckling i det tredjelandet eller den internationella organisationen. Beslutets territoriella och sektorsmässiga tillämpning ska regleras i genomförandeakten, där det också i förekommande fall ska anges vilken eller vilka myndigheter som är tillsynsmyndighet(er) enligt punkt 2 b i den här artikeln. Genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.
 4. Kommissionen ska fortlöpande övervaka utveckling i tredjeländer och internationella organisationer vilken kan påverka hur beslut som antagits enligt punkt 3 i den här artikeln och beslut som antagits på grundval av artikel 25.6 i direktiv 95/46/EG fungerar.
 5. Kommissionen ska, när tillgänglig information visar, i synnerhet efter den översyn som avses i punkt 3 i den här artikeln, att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom tredjelandet i fråga eller en internationell organisation inte längre säkerställer adekvat skydd i den mening som avses i punkt 2 i den här artikeln och, i den mån det behövs, genom genomförandeakter återkalla, ändra eller upphäva det beslut som avses i punkt 3 i den här artikeln utan retroaktiv verkan. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.
- När det föreligger vederbörligen motiverade och tvingande skäl till skyndsamhet ska kommissionen anta omedelbart tillämpliga genomförandeakter i enlighet med det förfarande som avses i artikel 93.3.
6. Kommissionen ska samråda med tredjelandet eller den internationella organisationen i fråga för att lösa den situation som lett till beslutet enligt punkt 5.
 7. Beslut enligt punkt 5 i den här artikeln ska inte påverka överföring av personuppgifter till tredjelandet, ett territorium eller en eller flera specificerade sektorer inom tredjelandet, eller den internationella organisationen i fråga enligt artiklarna 46–49.
 8. Kommissionen ska i *Europeiska unionens officiella tidning* och på sin webbplats offentliggöra en förteckning över de tredjeländer och de territorier och specificerade sektorer i ett givet tredjeland samt de internationella organisationer för vilka den har fastställt att en adekvat skyddsnivå inte eller inte längre säkerställs.

9. De beslut som antas av kommissionen på grundval av artikel 25.6 i direktiv 95/46/EG ska förbli i kraft tills de ändrats, ersatts eller upphävts av ett kommissionsbeslut som antagits i enlighet med punkt 3 eller 5 i den här artikeln.

Artikel 46

Överföring som omfattas av lämpliga skyddsåtgärder

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

2. Lämpliga skyddsåtgärder enligt punkt 1 får, utan att det krävs särskilt tillstånd från en övervakningsmyndighet, ta formen av

- a) ett rättsligt bindande och verkställbart instrument mellan offentliga myndigheter eller organ,
- b) bindande företagsbestämmelser i enlighet med artikel 47,
- c) standardiserade dataskyddsbestämmelser som antas av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2,
- d) standardiserade dataskyddsbestämmelser som antagits av en tillsynsmyndighet och godkänts av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2,
- e) en godkänd uppförandekod enligt artikel 40 tillsammans med rättsligt bindande och verkställbara åtaganden för den personuppgiftsansvarige eller personuppgiftsbiträdet i tredjelandet att tillämpa lämpliga skyddsåtgärder, även när det gäller registrerades rättigheter, eller
- f) en godkänd certifieringsmekanism enligt artikel 42 tillsammans med rättsligt bindande och verkställbara åtaganden för den personuppgiftsansvarige, personuppgiftsbiträdet i tredjelandet att tillämpa lämpliga skyddsåtgärder, även när det gäller de registrerades rättigheter.

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

- a) avtalsklausuler mellan den personuppgiftsansvarige eller personuppgiftsbiträdet och den personuppgiftsansvarige, personuppgiftsbiträdet eller mottagaren av personuppgifterna i tredjelandet eller den internationella organisationen, eller
- b) bestämmelser som ska införas i administrativa överenskommelser mellan offentliga myndigheter eller organ vilka inbegriper verkställbara och faktiska rättigheter för registrerade.

4. Tillsynsmyndigheten ska tillämpa den mekanism för enhetlighet som avses i artikel 63 i de fall som avses i punkt 3 i den här artikeln.

5. Tillstånd från en medlemsstat eller tillsynsmyndighet på grundval av artikel 26.2 i direktiv 95/46/EG ska förbli giltigt tills det, vid behov, ändrats, ersatts eller upphävts av den tillsynsmyndigheten. De beslut som fattas av kommissionen på grundval av artikel 26.4 i direktiv 95/46/EG ska förbli i kraft tills de, vid behov, ändrats, ersatts eller upphävts av ett kommissionsbeslut som antagits i enlighet med punkt 2 i den här artikeln.

Artikel 47

Bindande företagsbestämmelser

1. Den behöriga tillsynsmyndigheten ska godkänna bindande företagsbestämmelser i enlighet med den mekanism för enhetlighet som föreskrivs i artikel 63 under förutsättning att de

- a) är rättslig bindande, tillämpas på, och verkställs av alla delar som berörs inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet, inklusive deras anställda,

- b) innehåller uttryckliga bestämmelser om de registrerades lagstadgade rättigheter när det gäller behandlingen av deras personuppgifter, och
 - c) uppfyller villkoren i punkt 2.
2. De bindande företagsbestämmelser som avses i punkt 1 ska närmare ange åtminstone följande:
- a) struktur och kontaktuppgifter för den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet och för var och en av dess medlemmar,
 - b) vilka överföringar eller uppsättningar av överföringar av uppgifter som omfattas, inklusive kategorierna av personuppgifter, typen av behandling och dess ändamål, den typ av registrerade som berörs samt vilket eller vilka tredjeländer som avses,
 - c) bestämmelsernas rättsligt bindande natur, såväl internt som externt,
 - d) tillämpningen av allmänna principer för dataskydd, särskilt avgränsning av syften, uppgiftsminimering, begränsade lagringsperioder, datakvalitet, inbyggt dataskydd och dataskydd som standard, rättslig grund för behandling, behandling av särskilda kategorier av personuppgifter, åtgärder för att säkerställa datasäkerhet och villkoren när det gäller vidare överföring av uppgifter till organ som inte är bundna av bindande företagsbestämmelser,
 - e) de registrerades rättigheter avseende behandling och medlen för att utöva dessa rättigheter, inklusive rätten att inte bli föremål för beslut grundade enbart på automatisk behandling, inklusive profilering, enligt artikel 22, rätten att inge klagomål till den behöriga tillsynsmyndigheten och till behöriga domstolar i medlemsstaterna enligt artikel 79, rätten till prövning samt i förekommande fall rätten till kompensation för överträdelse av de bindande företagsbestämmelserna,
 - f) att den personuppgiftsansvarige eller personuppgiftsbiträdet som är etablerad inom en medlemsstats territorium tar på sig ansvaret om en berörd enhet som inte är etablerad inom unionen bryter mot de bindande företagsbestämmelserna; den personuppgiftsansvarige eller personuppgiftsbiträdet får helt eller delvis undantas från denna skyldighet endast på villkor att det kan visas att den berörda enheten i företagsgruppen inte kan hållas ansvarig för den skada som har uppkommit,
 - g) hur de registrerade ska informeras om innehållet i de bindande företagsbestämmelserna, särskilt de bestämmelser som avses i leden d, e och f i denna punkt utöver den information som avses i artiklarna 13 och 14,
 - h) uppgifterna för varje dataskyddsombud som utsetts i enlighet med artikel 37, eller varje annan person eller enhet med ansvar för kontrollen av att de bindande företagsbestämmelserna följs inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet, samt i fråga om utbildning och hantering av klagomål,
 - i) förfaranden för klagomål,
 - j) rutinerna inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet för att kontrollera att de bindande företagsreglerna följs; sådana rutiner ska inbegripa dataskyddstillsyn och metoder för att säkerställa korrigering åtgärder för att skydda de registrerades rättigheter; resultaten av sådana kontroller bör meddelas den person eller enhet som avses i led h och styrelsen i det kontrollerande företaget i koncernen eller gruppen av företag som deltar i gemensam ekonomisk verksamhet, och bör på begäran vara tillgänglig för den behöriga tillsynsmyndigheten,
 - k) rutinerna för att rapportera och dokumentera ändringar i bestämmelserna, samt rutinerna för att rapportera dessa ändringar till tillsynsmyndigheten,
 - l) rutinerna för att samarbeta med tillsynsmyndigheten i syfte att se till att alla medlemmar i den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet följer reglerna, särskilt genom att meddela tillsynsmyndigheten resultaten av kontroller av de åtgärder som avses i led j,
 - m) rutinerna för att till den behöriga tillsynsmyndigheten rapportera alla rättsliga krav som en medlem i koncernen eller gruppen av företag som deltar i gemensam ekonomisk verksamhet är underkastad i ett tredjeland och som sannolikt kommer att ha en avsevärd negativ inverkan på de garantier som ges genom de bindande företagsbestämmelserna, och
 - n) lämplig utbildning om dataskydd för personal som har ständig eller regelbunden tillgång till personuppgifter.

3. Kommissionen får närmare ange vilket format och vilka rutiner som ska användas för de personuppgiftsansvarigas, personuppgiftsbiträdenas och tillsynsmyndigheternas utbyte av information om bindande företagsbestämmelser i den mening som avses i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

Artikel 48

Överföringar och utlämnanden som inte är tillåtna enligt unionsrätten

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

Artikel 49

Undantag i särskilda situationer

1. Om det inte föreligger något beslut om adekvat skyddsnivå enligt artikel 45.3, eller om lämpliga skyddsåtgärder enligt artikel 46, inbegripet bindande företagsbestämmelser, får en överföring eller uppsättning av överföringar av personuppgifter till ett tredjeland eller en internationell organisation endast ske om något av följande villkor är uppfyllt:

- a) Den registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med sådana överföringar för den registrerade när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder.
- b) Överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den personuppgiftsansvarige eller för att genomföra åtgärder som föregår ett sådant avtal på den registrerades begäran.
- c) Överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den personuppgiftsansvarige och en annan fysisk eller juridisk person i den registrerades intresse.
- d) Överföringen är nödvändig av viktiga skäl som rör allmänintresset.
- e) Överföringen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.
- f) Överföringen är nödvändig för att skydda den registrerades eller andra personers grundläggande intressen, när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.
- g) Överföringen görs från ett register som enligt unionsrätten eller medlemsstaternas nationella rätt är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse, men endast i den utsträckning som de i unionsrätten eller i medlemsstaternas nationella rätt angivna villkoren för tillgänglighet uppfylls i det enskilda fallet.

När en överföring inte skulle kunna grundas på en bestämmelse i artikel 45 eller 46, inklusive bestämmelserna om bindande företagsbestämmelser, och inget av undantagen för en särskild situation som avses i första stycket i den här punkten är tillämpligt, får en överföring till ett tredjeland eller en internationell organisation äga rum endast om överföringen inte är repetitiv, endast gäller ett begränsat antal registrerade, är nödvändig för ändamål som rör den personuppgiftsansvariges tvingande berättigade intressen och den registrerades intressen eller rättigheter och friheter inte väger tyngre, och den personuppgiftsansvarige har bedömt samtliga omständigheter kring överföringen av uppgifter och på grundval av denna bedömning vidtagit lämpliga skyddsåtgärder för att skydda personuppgifter. Den personuppgiftsansvarige ska informera tillsynsmyndigheten om överföringen. Den personuppgiftsansvarige ska utöver tillhandahållande av den information som avses i artiklarna 13 och 14 informera den registrerade om överföringen och om de tvingande berättigade intressen som eftersträvas.

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

3. Leden a, b och c i punkt 1 första stycket samt andra stycket i samma punkt ska inte gälla åtgärder som vidtas av offentliga myndigheter som ett led i myndighetsutövning.
4. Det allmänintresse som avses i led d i punkt 1 första stycket ska vara erkänt i unionsrätten eller i den nationella rätt som den personuppgiftsansvarige omfattas av.
5. Saknas beslut om adekvat skyddsnivå, får unionsrätten eller medlemsstaternas nationella rätt med hänsyn till viktiga allmänintressen uttryckligen fastställa gränser för överföringen av specifika kategorier av personuppgifter till ett tredjeland eller en internationell organisation. Medlemsstaterna ska underrätta kommissionen om sådana bestämmelser.
6. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska bevara uppgifter både om bedömningen och om de lämpliga skyddsåtgärder som avses i punkt 1 andra stycket i den här artikeln i det register som avses i artikel 30.

Artikel 50

Internationellt samarbete för skydd av personuppgifter

När det gäller tredjeländer och internationella organisationer ska kommissionen och tillsynsmyndigheterna vidta lämpliga åtgärder för att

- a) utveckla rutiner för det internationella samarbetet för att underlätta en effektiv tillämpning av lagstiftningen om skydd av personuppgifter,
- b) på internationell nivå erbjuda ömsesidigt bistånd för en effektiv tillämpning av lagstiftningen om skydd av personuppgifter, bland annat genom underrättelse, hänskjutande av klagomål, bistånd vid utredningar samt informationsutbyte, med iakttagande av lämpliga skyddsåtgärder för personuppgifter samt skyddet av andra grundläggande rättigheter och friheter,
- c) involvera berörda aktörer i diskussioner och åtgärder som syftar till att öka det internationella samarbetet när det gäller tillämpningen av lagstiftningen om skydd av personuppgifter,
- d) främja utbyte och dokumentation om lagstiftning och praxis för skydd av personuppgifter, inklusive avseende behörighetskonflikter med tredjeländer.

KAPITEL VI

Oberoende tillsynsmyndigheter

Avsnitt 1

Oberoende ställning

Artikel 51

Tillsynsmyndighet

1. Varje medlemsstat ska föreskriva att en eller flera offentliga myndigheter ska vara ansvariga för att övervaka tillämpningen av denna förordning, i syfte att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling samt att underlätta det fria flödet av sådana uppgifter inom unionen (nedan kallad *tillsynsmyndighet*).
2. Varje tillsynsmyndighet ska bidra till en enhetlig tillämpning av denna förordning i hela unionen. För detta ändamål ska tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen i enlighet med kapitel VII.
3. Om det finns fler än en tillsynsmyndighet i en medlemsstat ska medlemsstaten utse den tillsynsmyndighet som ska företräda dessa myndigheter i styrelsen; medlemsstaten ska också upprätta en rutin för att se till att övriga myndigheter följer reglerna för den mekanism för enhetlighet som avses i artikel 63.
4. Varje medlemsstat ska senast den 25 maj 2018 anmäla till kommissionen vilka nationella bestämmelser den antar i enlighet med detta kapitel, och alla framtida ändringar som rör dessa bestämmelser ska anmälas utan dröjsmål.

*Artikel 52***Oberoende**

1. Varje tillsynsmyndighet ska vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med denna förordning.
2. Varje tillsynsmyndighets ledamot eller ledamöter ska i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med denna förordning stå fria från utomstående påverkan, direkt såväl som indirekt, och får varken begära eller ta emot instruktioner av någon.
3. Tillsynsmyndighetens ledamöter ska avhålla sig från alla handlingar som är oförenliga med deras skyldigheter och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet som står i strid med deras tjänsteutövning.
4. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet förfogar över de personella, tekniska och finansiella resurser samt de lokaler och den infrastruktur som behövs för att myndigheten ska kunna utföra sina uppgifter och utöva sina befogenheter, inklusive inom ramen för det ömsesidiga biståndet, samarbetet och deltagandet i styrelsens verksamhet.
5. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet väljer och förfogar över egen personal, som ska ta instruktioner uteslutande från den berörda tillsynsmyndighetens ledamot eller ledamöter.
6. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet blir föremål för finansiell kontroll, utan att detta påverkar tillsynsmyndighetens oberoende och att de förfogar över en separat, offentlig årsbudget som kan ingå i den övergripande statsbudgeten eller nationella budgeten.

*Artikel 53***Allmänna villkor för tillsynsmyndighetens ledamöter**

1. Medlemsstaterna ska föreskriva att varje ledamot av deras tillsynsmyndigheter ska utnämnas genom ett genom ett öppet förfarande med insyn av
 - deras parlament,
 - deras regering,
 - deras statschef, eller
 - ett oberoende organ som genom medlemsstatens nationella rätt anförtratts utnämningen.
2. Varje ledamot ska ha de kvalifikationer, den erfarenhet och den kompetens, särskilt på området skydd av personuppgifter, som krävs för att ledamoten ska kunna utföra sitt uppdrag och utöva sina befogenheter.
3. En ledamots uppdrag ska upphöra då mandattiden löper ut eller om ledamoten avgår eller avsätts från sin tjänst i enlighet med den berörda medlemsstatens nationella rätt.
4. En ledamot får avsättas endast på grund av grov försummelse eller när ledamoten inte längre uppfyller de villkor som krävs för att utföra uppdraget.

*Artikel 54***Regler för inrättandet av en tillsynsmyndighet**

1. Varje medlemsstat ska fastställa följande i lag:
 - a) Varje tillsynsmyndighets inrättande.

- b) De kvalifikationer och de villkor för lämplighet som krävs för att någon ska kunna utnämnas till ledamot av en tillsynsmyndighet.
- c) Regler och förfaranden för att utse varje tillsynsmyndighets ledamot eller ledamöter.
- d) Mandattiden för varje tillsynsmyndighets ledamot eller ledamöter, vilken inte får understiga fyra år, utom vid tillsättandet av de första ledamöterna efter den 24 maj 2016, då ett stegvis tillsättningsförfarande med kortare perioder för några av ledamöterna får tillämpas om detta är nödvändigt för att säkerställa myndighetens oberoende.
- e) Huruvida varje tillsynsmyndighets ledamot eller ledamöter får ges förnyat mandat, och om så är fallet, för hur många perioder.
- f) Vilka villkor som gäller för de skyldigheter som varje tillsynsmyndighets ledamot eller ledamöter och personal har, förbud mot handlingar, yrkesverksamhet och förmåner som står i strid därmed under och efter mandattiden och vilka bestämmelser som gäller för anställningens upphörande.

2. Varje tillsynsmyndighets ledamot eller ledamöter och personal ska i enlighet med unionsrätten eller medlemsstaternas nationella rätt omfattas av tystnadsplikt både under och efter sin mandattid vad avser konfidentiell information som de fått kunskap om under utförandet av deras uppgifter eller utövandet av deras befogenheter. Under mandatperioden ska denna tystnadsplikt i synnerhet gälla rapportering från fysiska personer om överträdelse av denna förordning.

Avsnitt 2

Behörighet, uppgifter och befogenheter

Artikel 55

Behörighet

1. Varje tillsynsmyndighet ska vara behörig att utföra de uppgifter och utöva de befogenheter som tilldelas den enligt denna förordning inom sin egen medlemsstats territorium.
2. Om behandling utförs av myndigheter eller privata organ som agerar på grundval av artikel 6.1 c eller e ska tillsynsmyndigheten i den berörda medlemsstaten vara behörig. I sådana fall ska artikel 56 inte tillämpas.
3. Tillsynsmyndigheterna ska inte vara behöriga att utöva tillsyn över domstolar som behandlar personuppgifter i sin dömande verksamhet.

Artikel 56

Den ansvariga tillsynsmyndighetens behörighet

1. Utan att det påverkar tillämpningen av artikel 55 ska tillsynsmyndigheten för den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga verksamhetsställe eller enda verksamhetsställe vara behörig att agera som ansvarig tillsynsmyndighet för den personuppgiftsansvariges eller personuppgiftsbiträdets gränsöverskridande behandling i enlighet med det förfarande som föreskrivs i artikel 60.
2. Genom undantag från punkt 1 ska varje tillsynsmyndighet vara behörig att behandla ett klagomål som lämnats in till denna eller en eventuell överträdelse av denna förordning, om sakfrågan i ärendet endast rör ett verksamhetsställe i medlemsstaten eller i väsentlig grad påverkar registrerade endast i medlemsstaten.
3. I de fall som avses i punkt 2 i den här artikeln ska tillsynsmyndigheten utan dröjsmål informera den ansvariga tillsynsmyndigheten om detta ärende. Inom tre veckor från det att den underrättats ska den ansvariga tillsynsmyndigheten besluta huruvida den kommer att behandla ärendet i enlighet med det förfarande som föreskrivs i artikel 60, med hänsyn till huruvida den personuppgiftsansvarige eller personuppgiftsbiträdet har eller inte har ett verksamhetsställe som är beläget i den medlemsstat där den tillsynsmyndighet som lämnat informationen är belägen.

4. Om den ansvariga tillsynsmyndigheten beslutar att behandla ärendet ska det ske i enlighet med det förfarande som föreskrivs i artikel 60. Den tillsynsmyndighet som underrättade den ansvariga tillsynsmyndigheten får lämna in ett utkast till beslut till den ansvariga tillsynsmyndigheten. Den ansvariga tillsynsmyndigheten ska ta största möjliga hänsyn till detta utkast till beslut när det utarbetar det utkast till beslut som avses i artikel 60.3.
5. Om den ansvariga tillsynsmyndigheten beslutar att inte behandla ärendet ska den tillsynsmyndighet som underrättade den ansvariga tillsynsmyndigheten behandla ärendet i enlighet med artiklarna 61 och 62.
6. Den ansvariga tillsynsmyndigheten ska vara den personuppgiftsansvariges eller personuppgiftsbitrådets enda motpart när det gäller den registreringsansvariges eller den personuppgiftsbitrådets gränsöverskridande behandling.

Artikel 57

Uppgifter

1. Utan att det påverkar de andra uppgifter som föreskrivs i denna förordning ska varje tillsynsmyndighet på sitt territorium ansvara för följande:
 - a) Övervaka och verkställa tillämpningen av denna förordning.
 - b) Öka allmänhetens medvetenhet om och förståelse för risker, regler, skyddsåtgärder och rättigheter i fråga om behandling. Särskild uppmärksamhet ska ägnas åt insatser som riktar sig till barn.
 - c) I enlighet med medlemsstatens nationella rätt ge rådgivning åt det nationella parlamentet, regeringen och andra institutioner och organ om lagstiftningsåtgärder och administrativa åtgärder rörande skyddet av fysiska personers rättigheter och friheter när det gäller behandling.
 - d) Öka personuppgiftsansvarigas och personuppgiftsbitrådets medvetenhet om sina skyldigheter enligt denna förordning.
 - e) På begäran tillhandahålla information till registrerade om hur de ska utöva sina rättigheter enligt denna förordning, och om så krävs samarbeta med tillsynsmyndigheter i andra medlemsstater för detta ändamål.
 - f) Behandla klagomål från en registrerad eller från ett organ, en organisation eller en sammanslutning enligt artikel 80, och där så är lämpligt undersöka den sakfråga som klagomålet gäller och inom rimlig tid underrätta den enskilde om hur undersökningen fortskrider och om resultatet, i synnerhet om det krävs ytterligare undersökningar eller samordning med en annan tillsynsmyndighet.
 - g) Samarbeta, inbegripet utbyta information, med och ge ömsesidigt bistånd till andra tillsynsmyndigheter för att se till att denna förordning tillämpas och verkställs på ett enhetligt sätt.
 - h) Utföra undersökningar om tillämpningen av denna förordning, inbegripet på grundval av information som erhålls från en annan tillsynsmyndighet eller annan myndighet.
 - i) Följa sådan utveckling som påverkar skyddet av personuppgifter, bland annat inom informations- och kommunikationsteknik och affärspraxis.
 - j) Anta sådana standardavtalsklausuler som avses i artiklarna 28.8 och 46.2 d.
 - k) Upprätta och föra en förteckning när det gäller kravet på en konsekvensbedömning avseende dataskydd enligt artikel 35.4.
 - l) Ge råd om behandling av personuppgifter enligt artikel 36.2.
 - m) Främja framtagande av uppförandekoder enligt artikel 40.1 samt yttra sig över och godkänna sådana uppförandekoder som tillhandahåller tillräckliga garantier, i enlighet med artikel 40.5.
 - n) Uppmuntra till inrättandet av certifieringsmekanismer för dataskydd och av sigill och märkningar för dataskydd i enlighet med artikel 42.1 samt godkänna certifieringskriterierna i enlighet med artikel 42.5.
 - o) I tillämpliga fall genomföra en periodisk översyn av certifieringar som utfärdats i enlighet med artikel 42.7.

- p) Utarbeta och offentliggöra kriterier för ackreditering av ett organ för övervakning av uppförandekoder enligt artikel 41 och ett certifieringsorgan enligt artikel 43.
 - q) Ackreditera ett organ för övervakning av uppförandekoder enligt artikel 41 och ett certifieringsorgan enligt artikel 43.
 - r) Godkänna sådana avtalsklausuler och bestämmelser som avses i artikel 46.3.
 - s) Godkänna sådana bindande företagsbestämmelser som avses i artikel 47.
 - t) Bidra till styrelsens verksamhet.
 - u) Hålla arkiv över överträdelser av denna förordning och åtgärder som vidtagits i enlighet med artikel 58.2.
 - v) Utföra eventuella andra uppgifter som rör skyddet av personuppgifter.
2. Varje tillsynsmyndighet ska underlätta inlämningen av klagomål enligt punkt 1 f genom åtgärder såsom ett särskilt formulär för ändamålet, vilket också kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.
3. Utförandet av alla tillsynsmyndigheters uppgifter ska vara avgiftsfritt för den registrerade och, i tillämpliga fall, för dataskyddsombudet.
4. Om en begäran är uppenbart ogrundad eller orimlig, särskilt på grund av dess repetitiva karaktär, får tillsynsmyndigheten ta ut en rimlig avgift grundad på de administrativa kostnaderna eller vägra att tillmötesgå begäran. Det åligger tillsynsmyndigheten att visa att begäran är uppenbart ogrundad eller orimlig.

Artikel 58

Befogenheter

1. Varje tillsynsmyndighet ska ha samtliga följande utredningsbefogenheter
- a) Beordra den personuppgiftsansvarige eller personuppgiftsbiträdet, och i tillämpliga fall den personuppgiftsansvariges eller personuppgiftsbiträdets företrädare, att lämna all information som myndigheten behöver för att kunna fullgöra sina uppgifter.
 - b) Genomföra undersökningar i form av dataskyddstillsyn.
 - c) Genomföra en översyn av certifieringar som utfärdats i enlighet med artikel 42.7.
 - d) Meddela den personuppgiftsansvarige eller personuppgiftsbiträdet om en påstådd överträdelse av denna förordning.
 - e) Från den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter och all information som tillsynsmyndigheten behöver för att kunna fullgöra sina uppgifter.
 - f) Få tillträde till alla lokaler som tillhör den personuppgiftsansvarige och personuppgiftsbiträdet, inbegripet tillgång till all utrustning och alla andra medel för behandling av personuppgifter i överensstämmelse med unionens processrätt eller medlemsstaternas nationella processrätt.
2. Varje tillsynsmyndighet ska ha samtliga följande korrigerande befogenheter
- a) Utfärda varningar till en personuppgiftsansvarig eller personuppgiftsbiträdet om att planerade behandlingar sannolikt kommer att bryta mot bestämmelserna i denna förordning.
 - b) Utfärda reprimander till en personuppgiftsansvarig eller personuppgiftsbiträdet om behandling bryter mot bestämmelserna i denna förordning.
 - c) Förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att tillmötesgå den registrerades begäran att få utöva sina rättigheter enligt denna förordning.

- d) Förelägga en personuppgiftsansvarig eller ett personuppgiftsbiträde att se till att behandlingen sker i enlighet med bestämmelserna i denna förordning och om så krävs på ett specifikt sätt och inom en specifik period,
 - e) Förelägga den personuppgiftsansvarige att meddela den registrerade att en personuppgiftsincident har inträffat.
 - f) Införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, behandling.
 - g) Förelägga om rättelse eller radering av personuppgifter samt begränsning av behandling enligt artiklarna 16, 17 och 18 och underrätta mottagare till vilka personuppgifterna har lämnats ut om dessa åtgärder enligt artiklarna 17.2 och 19.
 - h) Återkalla en certifiering eller beordra certifieringsorganet att återkalla en certifiering som utfärdats enligt artikel 42 eller 43, eller beordra certifieringsorganet att inte utfärda certifiering om kraven för certifiering inte eller inte längre uppfylls.
 - i) Påföra administrativa sanktionsavgifter i enlighet med artikel 83 utöver eller i stället för de åtgärder som avses i detta stycke, beroende på omständigheterna i varje enskilt fall.
 - j) Förelägga om att flödet av uppgifter till en mottagare i tredje land eller en internationell organisation ska avbrytas.
3. Varje tillsynsmyndighet ska ha samtliga följande befogenheter att utfärda tillstånd och att ge råd:
- a) Ge råd till den personuppgiftsansvarige i enlighet med det förfarande för förhandssamråd som avses i artikel 36.
 - b) På eget initiativ eller på begäran avge yttranden till det nationella parlamentet, medlemsstatens regering eller, i enlighet med medlemsstatens nationella rätt, till andra institutioner och organ samt till allmänheten, i frågor som rör skydd av personuppgifter.
 - c) Ge tillstånd till behandling enligt artikel 36.5 om medlemsstatens rätt kräver ett sådant förhandstillstånd.
 - d) Avge ett yttrande om och godkänna utkast till uppförandekoder enligt artikel 40.5.
 - e) Ackreditera certifieringsorgan i enlighet med artikel 43.
 - f) Utfärda certifieringar och godkänna kriterier för certifiering i enlighet med artikel 42.5.
 - g) Anta standardiserade dataskyddsbestämmelser enligt artiklarna 28.8 och 46.2 d.
 - h) Godkänna avtalsklausuler enligt artikel 46.3 a.
 - i) Godkänna administrativa överenskommelser enligt artikel 46.3 b.
 - j) Godkänna bindande företagsbestämmelser enligt artikel 47.
4. Utövandet av de befogenheter som tillsynsmyndigheten tilldelas enligt denna artikel ska omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel och rättssäkerhet, som fastställs i unionsrätten och i medlemsstaternas nationella rätt i enlighet med stadgan.
5. Varje medlemsstat ska i lagstiftning fastställa att dess tillsynsmyndighet ska ha befogenhet att upplysa de rättsliga myndigheterna om överträdelser av denna förordning och vid behov att inleda eller på övrigt vis delta i rättsliga förfaranden, för att verkställa bestämmelserna i denna förordning.
6. Varje medlemsstat får i lagstiftning föreskriva att dess tillsynsmyndighet ska ha ytterligare befogenheter utöver dem som avses i punkterna 1, 2 och 3. Utövandet av dessa befogenheter ska inte påverka den effektiva tillämpningen av kapitel VII.

Artikel 59

Verksamhetsrapporter

Varje tillsynsmyndighet ska upprätta en årlig rapport om sin verksamhet, vilken kan omfatta en förteckning över typer av anmälda överträdelser och typer av åtgärder som vidtagits i enlighet med artikel 58.2. Rapporterna ska översändas till det nationella parlamentet, regeringen och andra myndigheter som utsetts genom medlemsstatens nationella rätt. De ska göras tillgängliga för allmänheten, kommissionen och styrelsen.

KAPITEL VII

Samarbete och enhetlighet

Avsnitt 1

Samarbete

Artikel 60

Samarbete mellan den ansvariga tillsynsmyndigheten och de andra berörda tillsynsmyndigheterna

1. Den ansvariga tillsynsmyndigheten ska samarbeta med de andra berörda tillsynsmyndigheterna i enlighet med denna artikel i en strävan att uppnå samförstånd. Den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna ska utbyta all relevant information med varandra.
2. Den ansvariga tillsynsmyndigheten får när som helst begära att andra berörda tillsynsmyndigheter ger ömsesidigt bistånd i enlighet med artikel 61 och får genomföra gemensamma insatser i enlighet med artikel 62, i synnerhet för att utföra utredningar eller övervaka genomförandet av en åtgärd som avser en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i en annan medlemsstat.
3. Den ansvariga tillsynsmyndigheten ska utan dröjsmål meddela de andra berörda tillsynsmyndigheterna den relevanta informationen i ärendet. Den ska utan dröjsmål lägga fram ett utkast till beslut för de andra berörda tillsynsmyndigheterna så att de kan avge ett yttrande och ta vederbörlig hänsyn till deras synpunkter.
4. Om någon av de andra berörda tillsynsmyndigheterna inom en period av fyra veckor efter att de har rådfrågats i enlighet med punkt 3 i den här artikeln uttrycker en relevant och motiverad invändning mot utkastet till beslut ska den ansvariga tillsynsmyndigheten, om den inte instämmer i den relevanta och motiverade invändningen eller anser att invändningen inte är relevant eller motiverad, överlämna ärendet till den mekanism för enhetlighet som avses i artikel 63.
5. Om den ansvariga tillsynsmyndigheten avser att följa den relevanta och motiverade invändningen ska den till de andra berörda tillsynsmyndigheterna överlämna ett reviderat utkast till beslut så att de kan avge ett yttrande. Detta reviderade utkast till beslut ska omfattas av det förfarande som avses i punkt 4 inom en period av två veckor.
6. Om ingen av de andra berörda tillsynsmyndigheterna har gjort invändningar mot det utkast till beslut som den ansvariga tillsynsmyndigheten har lagt fram inom den period som avses i punkterna 4 och 5 ska den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna anses samtycka till detta utkast till beslut och ska vara bundna av det.
7. Den ansvariga tillsynsmyndigheten ska anta och meddela beslutet till den personuppgiftsansvariges eller personuppgiftsbitrådets huvudsakliga eller enda verksamhetsställe, allt efter omständigheterna, och underrätta de andra berörda tillsynsmyndigheterna och styrelsen om beslutet i fråga, inbegripet en sammanfattning av relevanta fakta och en relevant motivering. Den tillsynsmyndighet till vilken ett klagomål har lämnats in ska underrätta den enskilde om beslutet.
8. Om ett klagomål avvisas eller avslås ska den tillsynsmyndighet till vilken klagomålet lämnades in, genom undantag från punkt 7, anta beslutet och meddela den enskilde samt informera den personuppgiftsansvarige.
9. Om den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna är överens om att avvisa eller avslå delar av ett klagomål och att vidta åtgärder beträffande andra delar av klagomålet ska ett separat beslut antas för var och en av dessa delar av frågan. Den ansvariga tillsynsmyndigheten ska anta beslutet om den del som gäller åtgärder som avser den personuppgiftsansvarige och meddela det till den personuppgiftsansvariges eller personuppgiftsbitrådets huvudsakliga eller enda verksamhetsställe på medlemsstatens territorium och underrätta den enskilde om detta, medan den enskildes tillsynsmyndighet ska anta beslutet för den del som gäller avvisande av eller avslag på klagomålet och meddela det till den enskilde och underrätta den personuppgiftsansvarige eller personuppgiftsbiträdet om detta.
10. Efter att den personuppgiftsansvarige eller personuppgiftsbiträdet har meddelats om den ansvariga myndighetens beslut i enlighet med punkterna 7 och 9 ska den personuppgiftsansvarige eller personuppgiftsbiträdet vidta nödvändiga åtgärder för att se till att beslutet efterlevs vad gäller behandling med koppling till alla deras verksamhetsställen i unionen. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska meddela den ansvariga tillsynsmyndigheten vilka åtgärder som har vidtagits för att efterleva beslutet, och den ansvariga tillsynsmyndigheten ska informera de andra berörda tillsynsmyndigheterna.

11. Om en berörd tillsynsmyndighet under exceptionella omständigheter har skäl att anse att det finns ett brådskande behov av att agera för att skydda registrerades intressen ska det skyndsamma förfarande som avses i artikel 66 tillämpas.

12. Den ansvariga tillsynsmyndigheten och de andra berörda tillsynsmyndigheterna ska förse varandra med den information som krävs enligt denna artikel på elektronisk väg med användning av ett standardiserat format.

Artikel 61

Ömsesidigt bistånd

1. Tillsynsmyndigheterna ska utbyta relevant information och ge ömsesidigt bistånd i arbetet för att genomföra och tillämpa denna förordning på ett enhetligt sätt, och ska införa åtgärder som bidrar till ett verkningsfullt samarbete. Det ömsesidiga biståndet ska i synnerhet omfatta begäranden om information och tillsynsåtgärder, till exempel begäranden om utförande av förhandstillstånd och förhandssamråd, inspektioner och utredningar.

2. Varje tillsynsmyndighet ska vidta lämpliga åtgärder som krävs för att besvara en begäran från en annan tillsynsmyndighet utan onödigt dröjsmål och inte senare än en månad efter det att den tagit emot begäran. Till sådana åtgärder hör bland annat att översända relevant information om genomförandet av en pågående utredning.

3. En begäran om bistånd ska innehålla all nödvändig information, inklusive syftet med begäran och skälen till denna. Information som utbyts får endast användas för det syfte för vilket den har begärts.

4. Den tillsynsmyndighet som tar emot en begäran får endast vägra att tillmötesgå begäran om

- a) den inte är behörig att behandla den sakfråga som begäran avser eller de åtgärder som det begärs att den ska utföra, eller
- b) det skulle stå i strid med denna förordning eller unionsrätten eller den nationella rätt i en medlemsstat som tillsynsmyndigheten omfattas av att tillmötesgå begäran.

5. Den tillsynsmyndighet som tagit emot begäran ska meddela den myndighet som begäran kommer ifrån om resultatet eller, allt efter omständigheterna, om hur de åtgärder som vidtagits för att tillmötesgå begäran fortskrider. Den tillsynsmyndighet som tagit emot begäran ska redogöra för sina skäl för att vägra tillmötesgå begäran i enlighet med punkt 4.

6. Den tillsynsmyndighet som tar emot en begäran ska som regel tillhandahålla den information som begärts av andra tillsynsmyndigheter på elektronisk väg med användning av ett standardiserat format.

7. Tillsynsmyndigheter som tar emot en begäran får inte ta ut någon avgift för åtgärder som vidtagits av dem till följd av en begäran om ömsesidigt bistånd. Tillsynsmyndigheter får i undantagsfall komma överens med andra tillsynsmyndigheter om regler för ersättning från varandra för vissa utgifter i samband med tillhandahållande av ömsesidigt bistånd.

8. Om en tillsynsmyndighet inte tillhandahåller den information som avses i punkt 5 i denna artikel inom en månad efter det att den erhållit begäran från en annan tillsynsmyndighet får den begärande myndigheten anta en provisorisk åtgärd på sin medlemsstats territorium i enlighet med artikel 55.1. I detta fall ska det brådskande behov av att agera enligt artikel 66.1 anses vara uppfyllt och kräva ett brådskande bindande beslut från styrelsen i enlighet med artikel 66.2.

9. Kommissionen får genom genomförandeakter närmare ange format och förfaranden för sådant ömsesidigt bistånd som avses i denna artikel samt formerna för elektronisk överföring av information tillsynsmyndigheter emellan, samt mellan tillsynsmyndigheter och styrelsen, i synnerhet det standardiserade format som avses i punkt 6 i den här artikeln. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

Artikel 62

Tillsynsmyndigheters gemensamma insatser

1. Tillsynsmyndigheter ska vid behov genomföra gemensamma insatser, inbegripet gemensamma utredningar och gemensamma verkställighetsåtgärder i vilka ledamöter eller personal från andra medlemsstaters tillsynsmyndigheter deltar.

2. Om den personuppgiftsansvarige eller personuppgiftsbiträdet har verksamhetsställen i flera medlemsstater eller om ett betydande antal registrerade personer i mer än en medlemsstat sannolikt kommer att påverkas i väsentlig grad av att uppgifter behandlas, ska tillsynsmyndigheterna i var och en av dessa medlemsstater ha rätt att delta i de gemensamma insatserna. Den tillsynsmyndighet som är behörig enligt artikel 56.1 eller 56.4 ska bjuda in tillsynsmyndigheterna i var och en av de berörda medlemsstaterna att delta i de gemensamma insatserna och ska utan dröjsmål svara på en annan tillsynsmyndighets begäran att få delta.

3. En tillsynsmyndighet får, i enlighet med medlemsstatens nationella rätt och efter godkännande från ursprungslandets tillsynsmyndighet, tilldela befogenheter, inklusive utredningsbefogenheter, till ledamöter eller personal från ursprungslandets tillsynsmyndighet som deltar i gemensamma insatser eller, i den mån lagstiftningen i den medlemsstat som är värdland för tillsynsmyndigheten tillåter detta, medge att ursprungslandets tillsynsmyndighets ledamöter eller personal utövar utredningsbefogenheter enligt lagstiftningen i ursprungslandets tillsynsmyndighets medlemsstat. Sådana utredningsbefogenheter får endast utövas under vägledning och i närvaro av ledamöter eller personal från värdlandets tillsynsmyndighet. Ledamöter och personal från ursprungslandets tillsynsmyndighet ska omfattas av den medlemsstats nationella rätt som gäller för värdlandets tillsynsmyndighet.

4. Om personal från ursprungslandets tillsynsmyndighet verkar i en annan medlemsstat i enlighet med punkt 1 ska värdtillsynsmyndighetens medlemsstat ansvara för deras handlingar, vilket inbegriper ansvar för skador som personalen vållar i samband med insatserna, i enlighet med rätten i den medlemsstat på vars territorium personalen verkar.

5. Den medlemsstat på vars territorium skadorna förorsakades ska ersätta sådana skador enligt de villkor som gäller för skador som förorsakas av dess egen personal. Den medlemsstat vars tillsynsmyndighets tjänstemän har orsakat en person skada på någon annan medlemsstats territorium ska fullt ut ersätta den andra medlemsstaten för det belopp som denna har betalat ut till den personens rättsinnehavare.

6. Utan att det påverkar rättigheterna gentemot tredje man och tillämpningen av punkt 5, ska varje medlemsstat i de fall som nämns i punkt 1 avstå från att kräva ersättning från en annan medlemsstat för skador som avses i punkt 4.

7. Om en gemensam insats planeras och en tillsynsmyndighet inte inom en månad har uppfyllt sin skyldighet enligt punkt 2 i den här artikeln, andra meningen får övriga tillsynsmyndigheter anta provisoriska åtgärder på sina respektive medlemsstaters territorium i enlighet med artikel 55. I detta fall ska det brådskande behov av att agera enligt artikel 66.1 anses vara uppfyllt och kräva ett yttrande eller ett brådskande bindande beslut från styrelsen i enlighet med artikel 66.2.

Avsnitt 2

Enhetlighet

Artikel 63

Mekanism för enhetlighet

För att bidra till en enhetlig tillämpning av denna förordning i hela unionen ska tillsynsmyndigheterna samarbeta med varandra och, i förekommande fall, med kommissionen, genom den mekanism för enhetlighet som föreskrivs i detta avsnitt.

Artikel 64

Yttrande från Styrelsen

1. Styrelsen ska avge ett yttrande när en behörig tillsynsmyndighet avser att anta någon av åtgärderna nedan. I detta syfte ska den behöriga tillsynsmyndigheten skicka utkastet till beslut till styrelsen när det

a) syftar till att anta en förteckning över behandling som omfattas av kravet på en konsekvensbedömning avseende dataskydd enligt artikel 35.4,

b) rör ett ärende i enlighet med artikel 40.7 om huruvida ett utkast till uppförandekoder eller en ändring eller förlängning av en uppförandekod är förenlig med denna förordning,

- c) syftar till att godkänna kriterierna för ackreditering av ett organ enligt artikel 41.3 eller ett certifieringsorgan enligt artikel 43.3,
- d) syftar till att fastställa standardiserade dataskyddsbestämmelser enligt artiklarna 46.2 d och 28.8,
- e) syftar till att godkänna sådana avtalsklausuler som avses i artikel 46.3 a, eller
- f) syftar till att godkänna bindande företagsbestämmelser enligt artikel 47.

2. Varje tillsynsmyndighet, styrelsens ordförande eller kommissionen får i syfte att erhålla ett yttrande begära att styrelsen granskar en fråga med allmän räckvidd eller som har följder i mer än en medlemsstat, i synnerhet om en behörig myndighet inte uppfyller sina skyldigheter i fråga om ömsesidigt bistånd i enlighet med artikel 61 eller i fråga om gemensamma insatser i enlighet med artikel 62.

3. I de fall som avses i punkterna 1 och 2 ska styrelsen avge ett yttrande i den fråga som ingivits till den, förutsatt att den inte redan har avgett ett yttrande i samma fråga. Detta yttrande ska antas med enkel majoritet av styrelsens ledamöter inom åtta veckor. Denna period får förlängas med ytterligare sex veckor med hänsyn till sakfrågans komplexitet. Vad gäller det utkast till beslut som avses i punkt 1 som spridits till styrelsens ledamöter i enlighet med punkt 5, ska en ledamot som inte har gjort invändningar inom en rimlig period som ordföranden angett anses samtycka till utkastet till beslut.

4. Tillsynsmyndigheterna och kommissionen ska utan onödigt dröjsmål i ett standardiserat elektroniskt format till styrelsen översända all relevant information, som allt efter omständigheterna får utgöras av en sammanfattning av sakförhållanden, utkastet till beslut, grunden till att en sådan åtgärd är nödvändig och synpunkter från övriga berörda tillsynsmyndigheter.

5. Styrelsens ordförande ska utan onödigt dröjsmål och på elektronisk väg upplysa

- a) styrelsens ledamöter samt kommissionen om all relevant information som meddelats styrelsen i ett standardiserat format; styrelsens sekretariat ska vid behov tillhandahålla översättningar av relevant information; och
- b) den tillsynsmyndighet som, allt efter omständigheterna, avses i punkterna 1 och 2 samt kommissionen om yttrandet, och ska också offentliggöra det.

6. Den behöriga tillsynsmyndigheten får inte anta sitt utkast till beslut enligt punkt 1 inom den period som avses i punkt 3.

7. Den tillsynsmyndighet som avses i punkt 1 ska ta största möjliga hänsyn till styrelsens yttrande och ska, inom två veckor efter att yttrandet inkommit, i ett standardiserat elektroniskt format meddela styrelsens ordförande om huruvida den kommer att hålla fast vid eller ändra sitt utkast till beslut, och i förekommande fall översända det ändrade utkastet till beslut.

8. Om den berörda tillsynsmyndigheten underrättar styrelsens ordförande inom den period som avses i punkt 7 i den här artikeln om att den inte avser att följa styrelsens yttrande, helt eller delvis, och tillhandahåller en relevant motivering, ska artikel 65.1 tillämpas.

Artikel 65

Tvistlösning genom styrelsen

1. För att säkerställa en korrekt och enhetlig tillämpning av denna förordning i enskilda fall ska styrelsen anta ett bindande beslut i följande fall:

- a) Om en berörd tillsynsmyndighet i ett fall som avses i artikel 60.4 har gjort en relevant och motiverad invändning mot ett utkast till beslut av den ansvariga myndigheten, eller om den ansvariga myndigheten har avslagit denna invändning med motiveringen att den inte var relevant eller motiverad. Det bindande beslutet ska avse alla ärenden som är föremål för den relevanta och motiverade invändningen, särskilt frågan om huruvida det föreligger en överträdelse av denna förordning.

- b) Om det finns motstridiga åsikter om vilken av de berörda tillsynsmyndigheterna som är behörig för det huvudsakliga verksamhetsstället.
- c) Om en behörig tillsynsmyndighet inte begär ett yttrande från styrelsen i de fall som avses i artikel 64.1, eller inte följer ett yttrande som styrelsen avger enligt artikel 64. I detta fall får varje berörd tillsynsmyndighet eller kommissionen översända ärendet till styrelsen.
2. Det beslut som avses i punkt 1 ska antas inom en månad efter det att sakfrågan hänskjutits med två tredjedels majoritet av styrelsens ledamöter. Denna period får förlängas med ytterligare en månad med hänsyn till sakfrågans komplexitet. Det beslut som avses i punkt 1 ska vara motiverat och riktat till den ansvariga tillsynsmyndigheten och alla berörda tillsynsmyndigheter och ska vara bindande för dem.
3. Om styrelsen inte har kunnat anta något beslut inom de perioder som avses i punkt 2 ska den anta sitt beslut inom två veckor efter utgången av den andra månad som avses i punkt 2 med enkel majoritet av styrelsens ledamöter. Om styrelsens ledamöter är delade i frågan ska beslutet antas i enlighet med ordförandens röst.
4. De berörda tillsynsmyndigheterna ska inte anta något beslut om den sakfråga som ingivits till styrelsen i enlighet med punkt 1 under de perioder som avses i punkterna 2 och 3.
5. Styrelsens ordförande ska utan onödigt dröjsmål meddela de berörda tillsynsmyndigheterna det beslut som avses i punkt 1. Kommissionen ska informeras om detta. Beslutet ska utan dröjsmål offentliggöras på styrelsens webbplats efter att tillsynsmyndigheten har meddelat det slutliga beslut som avses i punkt 6.
6. Den ansvariga tillsynsmyndigheten eller, allt efter omständigheterna, den tillsynsmyndighet till vilken klagomålet har ingetts ska anta sitt slutliga beslut på grundval av det beslut som avses i punkt 1 i den här artikeln, utan onödigt dröjsmål och senast en månad efter det att styrelsen har meddelat sitt beslut. Den ansvariga tillsynsmyndigheten eller, allt efter omständigheterna, den tillsynsmyndighet till vilken klagomålet har ingetts ska underrätta styrelsen om vilken dag dess slutliga beslut meddelas till den personuppgiftsansvarige respektive personuppgiftsbiträdet och den registrerade. De berörda tillsynsmyndigheternas slutliga beslut ska antas i enlighet med bestämmelserna i artikel 60.7, 60.8 och 60.9. Det slutliga beslutet ska hänvisa till det beslut som avses i punkt 1 i den här artikeln och ska precisera att det beslut som avses i punkt 1 kommer att offentliggöras på styrelsens webbplats i enlighet med punkt 5 i den här artikeln. Det beslut som avses i punkt 1 i den här artikeln ska fogas till det slutliga beslutet.

Artikel 66

Skyndsamt förfarande

1. Under exceptionella omständigheter får en berörd tillsynsmyndighet med avvikelse från den mekanism för enhetlighet som avses i artiklarna 63, 64 och 65 eller det förfarande som avses i artikel 60 omedelbart vidta provisoriska åtgärder avsedda att ha rättsverkan på det egna territoriet och med förutbestämd varaktighet som inte överskrider tre månader, om den anser att det finns ett brådskande behov av att agera för att skydda registrerades rättigheter och friheter. Tillsynsmyndigheten ska utan dröjsmål underrätta de andra berörda tillsynsmyndigheterna, styrelsen och kommissionen om dessa åtgärder och om skälen till att de vidtas.
2. Om en tillsynsmyndighet har vidtagit en åtgärd enligt punkt 1 och anser att definitiva åtgärder skyndsamt måste antas, får den begära ett brådskande yttrande eller ett brådskande bindande beslut från styrelsen; den ska då motivera varför den begär ett sådant yttrande eller beslut.
3. Om en behörig tillsynsmyndighet inte har vidtagit någon lämplig åtgärd i en situation som kräver skyndsamt handling för att skydda registrerades rättigheter och friheter, får vilken tillsynsmyndighet som helst begära ett brådskande yttrande eller, i tillämpliga fall, ett brådskande bindande beslut från styrelsen, varvid den ska motivera varför den begär ett sådant yttrande eller beslut och varför åtgärden måste vidtas skyndsamt.
4. Genom undantag från artiklarna 64.3 och 65.2 ska ett brådskande yttrande eller ett brådskande beslut enligt punkterna 2 och 3 i den här artikeln antas inom två veckor med enkel majoritet av styrelsens ledamöter.

*Artikel 67***Utbyte av information**

Kommissionen får anta genomförandeakter med allmän räckvidd i syfte att närmare ange tillvägagångssätten för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen, särskilt det standardiserade format som avses i artikel 64.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

*Avsnitt 3***Europeiska dataskyddsstyrelsen***Artikel 68***Europeiska dataskyddsstyrelsen**

1. Europeiska dataskyddsstyrelsen (nedan kallad *styrelsen*) inrättas härmed som ett unionsorgan och ska ha ställning som juridisk person.
2. Styrelsen ska företrädas av sin ordförande.
3. Styrelsen ska bestå av chefen för en tillsynsmyndighet per medlemsstat och av Europeiska datatillsynsmannen eller deras respektive företrädare.
4. Om en medlemsstat har mer än en tillsynsmyndighet som ansvarar för att övervaka tillämpningen av bestämmelserna i denna förordning ska en gemensam företrädare utses i enlighet med den medlemsstatens nationella rätt.
5. Kommissionen ska ha rätt att delta i styrelsens verksamhet och möten utan rösträtt. Kommissionen ska utse en egen företrädare. Styrelsens ordförande ska underrätta kommissionen om styrelsens verksamhet.
6. I de fall som avses i artikel 65 ska Europeiska datatillsynsmannen endast ha rösträtt i fråga om beslut som rör principer och regler som är tillämpliga på unionens institutioner, organ och byråer, och som i allt väsentligt motsvarar dem i denna förordning.

*Artikel 69***Oberoende**

1. Styrelsen ska vara oberoende när den fullgör sina uppgifter eller utövar sina befogenheter i enlighet med artiklarna 70 och 71.
2. Utan att detta påverkar kommissionens rätt att lämna en begäran enligt artikel 70.1 b och 70.2 ska styrelsen när den fullgör sina uppgifter eller utövar sina befogenheter varken begära eller ta emot instruktioner av någon.

*Artikel 70***Styrelsens uppgifter**

1. Styrelsen ska se till att denna förordning tillämpas enhetligt. För detta ändamål ska styrelsen, på eget initiativ eller i förekommande fall på begäran av kommissionen, i synnerhet
 - a) övervaka och säkerställa korrekt tillämpning av denna förordning i de fall som avses i artiklarna 64 och 65 utan att det påverkar de nationella tillsynsmyndigheternas uppgifter,

- b) ge kommissionen råd i alla frågor som gäller skydd av personuppgifter inom unionen, inklusive om eventuella förslag till ändring av denna förordning,
- c) ge kommissionen råd om format och förfaranden för informationsutbyte mellan personuppgiftsansvariga, personuppgiftsbiträden och tillsynsmyndigheter för bindande företagsbestämmelser,
- d) utfärda riktlinjer, rekommendationer och bästa praxis beträffande förfaranden för att radera länkar, kopior eller reproduktioner av personuppgifter från allmänt tillgängliga kommunikationstjänster enligt artikel 17.2,
- e) på eget initiativ eller på begäran av en av sina ledamöter eller av kommissionen behandla frågor om tillämpningen av denna förordning och utfärda riktlinjer, rekommendationer och bästa praxis i syfte att främja en enhetlig tillämpning av denna förordning,
- f) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och villkoren för profileringsbaserade beslut enligt artikel 22.2,
- g) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att konstatera sådana personuppgiftsincidenter och fastställa sådant onödigt dröjsmål som avses i artikel 33.1 och 33.2 och för de särskilda omständigheter under vilka en personuppgiftsansvarig eller ett personuppgiftsbiträde är skyldig att anmäla personuppgiftsincidenten,
- h) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt angående de omständigheter under vilka en personuppgiftsincident sannolikt kommer att leda till hög risk för rättigheterna och friheterna för de fysiska personer som avses i artikel 34.1,
- i) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och kraven för överföringar av personuppgifter på grundval av bindande företagsbestämmelser som personuppgiftsansvariga eller personuppgiftsbiträden följer samt ytterligare nödvändiga krav för att säkerställa skyddet för personuppgifter för berörda registrerade enligt artikel 47,
- j) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och villkoren för överföring av personuppgifter på grundval av artikel 49.1,
- k) utforma riktlinjer för tillsynsmyndigheterna i fråga om tillämpningen av de åtgärder som avses i artikel 58.1, 58.2 och 58.3 och fastställandet av administrativa sanktionsavgifter i enlighet med artikel 83,
- l) se över den praktiska tillämpningen av de riktlinjer och rekommendationer samt den bästa praxis som avses i leden e och f,
- m) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att fastställa gemensamma förfaranden för fysiska personers rapportering av överträdelser av denna förordning enligt artikel 54.2,
- n) främja utarbetandet av uppförandekoder och införandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd i enlighet med artiklarna 40 och 42,
- o) ackreditera certifieringsorgan och utföra sin periodiska översyn i enlighet med artikel 43 och föra ett offentligt register över ackrediterade organ i enlighet med artikel 43.6 och över de ackrediterade personuppgiftsansvariga eller personuppgiftsbiträdena som är etablerade i tredjeländer i enlighet med artikel 42.7,
- p) närmare ange de krav som avses i artikel 43.3 i syfte att ackreditera certifieringsorgan enligt artikel 42,
- q) avge ett yttrande till kommissionen om de certifieringskrav som avses i artikel 43.8,
- r) avge ett yttrande till kommissionen om de symboler som avses i artikel 12.7,
- s) avge ett yttrande till kommissionen för bedömningen av adekvat skyddsnivå i ett tredjeland eller en internationell organisation, inklusive för bedömningen av huruvida ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom det tredjelandet, eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå; i detta syfte ska kommissionen lämna all nödvändig dokumentation till styrelsen, inklusive korrespondens med regeringen i tredjelandet, med avseende på tredjelandet, territoriet eller den specificerade sektorn, eller till databehandlingssektorn i tredjelandet eller den internationella organisationen,

- t) avge yttranden om utkast till beslut som läggs fram av tillsynsmyndigheter inom den mekanism för enhetlighet som avses i artikel 64.1, i ärenden som ingivits i enlighet med artikel 64.2 och anta bindande beslut i enlighet med artikel 65, inbegripet de fall som avses i artikel 66,
 - u) främja samarbete och effektivt bilateralt och multilateralt utbyte av bästa praxis och information mellan tillsynsmyndigheterna,
 - v) främja gemensamma utbildningsprogram och underlätta personalutbyte mellan tillsynsmyndigheterna och där så är lämpligt även med tillsynsmyndigheter i tredjeländer eller internationella organisationer,
 - w) främja utbyte av kunskap och dokumentation om lagstiftning om och praxis för dataskydd med tillsynsmyndigheter för dataskydd i hela världen.
 - x) avge yttranden över de uppförandekoder som utarbetas på unionsnivå i enlighet med artikel 40.9, och
 - y) föra ett offentligt elektroniskt register över tillsynsmyndigheters beslut och domstolars avgöranden i frågor som hanteras inom mekanismen för enhetlighet.
2. När kommissionen begär rådgivning från styrelsen får den ange en tidsfrist med hänsyn till hur brådskande ärendet är.
3. Styrelsen ska vidarebefordra sina yttranden, riktlinjer, rekommendationer och bästa praxis till kommissionen och till den kommitté som avses i artikel 93, samt offentliggöra dem.
4. När så är lämpligt ska styrelsen samråda med berörda parter och ge dem möjlighet att yttra sig inom rimlig tid. Styrelsen ska, utan att det påverkar tillämpningen av artikel 76, offentliggöra resultatet av samrådsförfarandet.

Artikel 71

Rapporter

1. Styrelsen ska sammanställa en årsrapport om skydd av fysiska personer vid behandling inom unionen och, i förekommande fall, i tredjeländer och internationella organisationer. Rapporten ska offentliggöras och översändas till Europaparlamentet, rådet och kommissionen.
2. Årsrapporten ska också innehålla en översikt över den praktiska tillämpningen av de riktlinjer och rekommendationer och den bästa praxis som avses i artikel 70.1 liksom de bindande beslut som avses i artikel 65.

Artikel 72

Förfarande

1. Styrelsen ska fatta beslut med enkel majoritet av dess ledamöter, om inte annat anges i denna förordning.
2. Styrelsen ska själv anta sin arbetsordning med två tredjedels majoritet av sina ledamöter och fastställa sina arbetsformer.

Artikel 73

Ordförande

1. Styrelsen ska med enkel majoritet välja en ordförande och två vice ordförande bland sina ledamöter.
2. Ordförandens och de vice ordförandenas mandattid ska vara fem år och kunna förnyas en gång.

*Artikel 74***Ordförandens uppgifter**

1. Ordföranden ska ha i uppgift att
 - a) sammankalla till styrelsens möten och planera dagordningen,
 - b) meddela beslut som antas av styrelsen i enlighet med artikel 65 till den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna,
 - c) se till att styrelsens uppgifter fullgörs i tid, särskilt i fråga om den mekanism för enhetlighet som avses i artikel 63.
2. Fördelningen av uppgifter mellan ordföranden och de vice ordförandena ska fastställas i styrelsens arbetsordning.

*Artikel 75***Sekretariatet**

1. Styrelsen ska förfoga över ett sekretariat som ska tillhandahållas av Europeiska datatillsynsmannen.
2. Sekretariatet ska utföra sina uppgifter enbart under ledning av ordföranden för styrelsen.
3. Den personal vid Europeiska datatillsynsmannen som utför de uppgifter som styrelsen tilldelas genom denna förordning ska följa separata rapporteringsvägar från den personal som utför de uppgifter som Europeiska datatillsynsmannen tilldelas.
4. När så är lämpligt ska styrelsen och Europeiska datatillsynsmannen fastställa och offentliggöra ett samförståndsavtal för genomförande av denna artikel, som fastställer villkoren för deras samarbete, och som ska tillämpas på den personal vid Europeiska datatillsynsmannen som utför de uppgifter som styrelsen tilldelas genom denna förordning.
5. Sekretariatet ska förse styrelsen med analysstöd samt administrativt och logistiskt stöd.
6. Sekretariatet ska särskilt ansvara för
 - a) styrelsens löpande arbete,
 - b) kommunikationen mellan styrelsens ledamöter, dess ordförande och kommissionen,
 - c) kommunikationen med andra institutioner och med allmänheten,
 - d) användningen av elektroniska medel för intern och extern kommunikation,
 - e) översättning av relevant information,
 - f) förberedelser och uppföljning av styrelsens möten,
 - g) förberedelse, sammanställning och offentliggörande av yttranden, beslut om lösning av tvister mellan tillsynsmyndigheter och andra texter som antas av styrelsen.

*Artikel 76***Konfidentialitet**

1. Styrelsens överläggningar ska vara konfidentiella i de fall som styrelsen bedömer detta vara nödvändigt, i enlighet med vad som anges i dess arbetsordning.

2. Tillgången till handlingar som skickas till styrelsens ledamöter, till experter eller till företrädare för tredje part ska regleras av Europaparlamentets och rådets förordning (EG) nr 1049/2001 ⁽¹⁾.

KAPITEL VIII

Rättsmedel, ansvar och sanktioner

Artikel 77

Rätt att lämna in klagomål till en tillsynsmyndighet

1. Utan att det påverkar något annat administrativt prövningsförfarande eller rättsmedel, ska varje registrerad som anser att behandlingen av personuppgifter som avser henne eller honom strider mot denna förordning ha rätt att lämna in ett klagomål till en tillsynsmyndighet, särskilt i den medlemsstat där han eller hon har sin hemvist eller sin arbetsplats eller där det påstådda intrånget begicks.

2. Den tillsynsmyndighet till vilken klagomålet har ingetts ska underrätta den enskilde om hur arbetet med klagomålet fortskrider och vad resultatet blir, inbegripet möjligheten till rättslig prövning enligt artikel 78.

Artikel 78

Rätt till ett effektivt rättsmedel mot tillsynsmyndighetens beslut

1. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol ska varje fysisk eller juridisk person ha rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut rörande dem som meddelats av en tillsynsmyndighet.

2. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol, ska varje registrerad person ha rätt till ett effektivt rättsmedel om den tillsynsmyndighet som är behörig i enlighet med artiklarna 55 och 56 underlåter att behandla ett klagomål eller att informera den registrerade inom tre månader om hur det fortskrider med det klagomål som ingetts med stöd av artikel 77 eller vilket beslut som har fattats med anledning av det.

3. Talan mot en tillsynsmyndighet ska väckas vid domstolarna i den medlemsstat där tillsynsmyndigheten har sitt säte.

4. Om talan väcks mot ett beslut som fattats av en tillsynsmyndighet och som föregicks av ett yttrande från eller beslut av styrelsen inom ramen för mekanismen för enhetlighet ska tillsynsmyndigheten vidarebefordra detta yttrande eller beslut till domstolen.

Artikel 79

Rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde

1. Utan att det påverkar tillgängliga administrativa prövningsförfaranden eller prövningsförfaranden utanför domstol, inbegripet rätten att lämna in ett klagomål till en tillsynsmyndighet i enlighet med artikel 77, ska varje registrerad som anser att hans eller hennes rättigheter enligt denna förordning har åsidosatts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med denna förordning ha rätt till ett effektivt rättsmedel.

2. Talan mot en personuppgiftsansvarig eller ett personuppgiftsbiträde ska väckas vid domstolarna i den medlemsstat där den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad. Alternativt får sådan talan väckas vid domstolarna i den medlemsstat där den registrerade har sin hemvist, såvida inte den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet i en medlemsstat som agerar inom ramen för sin myndighetsutövning.

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

*Artikel 80***Företrädande av registrerade**

1. Den registrerade ska ha rätt att ge ett organ, en organisation eller sammanslutning utan vinstsyfte, som har inrättats på lämpligt sätt i enlighet med lagen i en medlemsstat, vars stadgeenliga mål är av allmänt intresse och som är verksam inom området skydd av registrerades rättigheter och friheter när det gäller skyddet av deras personuppgifter, i uppdrag att lämna in ett klagomål för hans eller hennes räkning, att utöva de rättigheter som avses i artiklarna 77, 78 och 79 för hans eller hennes räkning samt att för hans eller hennes räkning utöva den rätt till ersättning som avses i artikel 82 om så föreskrivs i medlemsstatens nationella rätt.

2. Medlemsstaterna får föreskriva att ett organ, en organisation eller en sammanslutning enligt punkt 1 i den här artikeln, oberoende av en registrerads mandat, har rätt att i den medlemsstaten inge klagomål till den tillsynsmyndighet som är behörig enligt artikel 77 och utöva de rättigheter som avses i artiklarna 78 och 79 om organet, organisationen eller sammanslutningen anser att den registrerades rättigheter enligt den här förordningen har kränkts som en följd av behandlingen.

*Artikel 81***Vilandeförklaring av förfaranden**

1. Om en behörig domstol i en medlemsstat har information om att förfaranden som rör samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller personuppgiftsbiträde pågår i en domstol i en annan medlemsstat ska den kontakta denna domstol i den andra medlemsstaten för att bekräfta förekomsten av sådana förfaranden.

2. Om förfaranden som rör samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller personuppgiftsbiträde pågår i en domstol i en annan medlemsstat får alla andra behöriga domstolar än den där förfarandena först inleddes vilandeförklara förfarandena.

3. Om dessa förfaranden prövas i första instans får varje domstol, utom den vid vilken förfarandena först inleddes, också förklara sig obehörig på begäran av en av parterna, om den domstol vid vilken förfarandena först inleddes är behörig att pröva de berörda förfarandena och dess lagstiftning tillåter förening av dessa.

*Artikel 82***Ansvar och rätt till ersättning**

1. Varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av denna förordning ska ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan.

2. Varje personuppgiftsansvarig som medverkat vid behandlingen ska ansvara för skada som orsakats av behandling som strider mot denna förordning. Ett personuppgiftsbiträde ska ansvara för skada uppkommen till följd av behandlingen endast om denne inte har fullgjort de skyldigheter i denna förordning som specifikt riktar sig till personuppgiftsbiträden eller agerat utanför eller i strid med den personuppgiftsansvariges lagenliga anvisningar.

3. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska undgå ansvar enligt punkt 2 om den visar att den inte på något sätt är ansvarig för den händelse som orsakade skadan.

4. Om mer än en personuppgiftsansvarig eller ett personuppgiftsbiträde, eller både en personuppgiftsansvarig och ett personuppgiftsbiträde, har medverkat vid samma behandling, och om de enligt punkterna 2 och 3 är ansvariga för eventuell skada som behandlingen orsakat ska varje personuppgiftsansvarig eller personuppgiftsbiträde hållas ansvarig för hela skadan för att säkerställa att den registrerade får effektiv ersättning.

5. Om en personuppgiftsansvarig eller ett personuppgiftsbiträde, i enlighet med punkt 4, har betalat full ersättning för den skada som orsakats ska den personuppgiftsansvarige eller personuppgiftsbiträdet ha rätt att från de andra personuppgiftsansvariga eller personuppgiftsbiträdena som medverkat vid samma behandling återkräva den del av ersättningen som motsvarar deras del av ansvaret för skadan i enlighet med de villkor som fastställs i punkt 2.

6. Domstolsförfaranden för utövande av rätten till ersättning ska tas upp vid de domstolar som är behöriga enligt den nationella rätten i den medlemsstat som avses i artikel 79.2.

Artikel 83

Allmänna villkor för påförande av administrativa sanktionsavgifter

1. Varje tillsynsmyndighet ska säkerställa att påförande av administrativa sanktionsavgifter i enlighet med denna artikel för sådana överträdelser av denna förordning som avses i punkterna 4, 5 och 6 i varje enskilt fall är effektivt, proportionellt och avskräckande.

2. Administrativa sanktionsavgifter ska, beroende på omständigheterna i det enskilda fallet, påföras utöver eller i stället för de åtgärder som avses i artikel 58.2 a–h och j. Vid beslut om huruvida administrativa sanktionsavgifter ska påföras och om beloppet för de administrativa sanktionsavgifterna i varje enskilt fall ska vederbörlig hänsyn tas till följande:

- a) Överträdelsens karaktär, svårighetsgrad och varaktighet med beaktande av den aktuella uppgiftsbehandlings karaktär, omfattning eller syfte samt antalet berörda registrerade och den skada som de har lidit.
- b) Om överträdelsen skett med uppsåt eller genom oaktsamhet.
- c) De åtgärder som den personuppgiftsansvarige eller personuppgiftsbiträdet har vidtagit för att lindra den skada som de registrerade har lidit.
- d) Graden av ansvar hos den personuppgiftsansvarige eller personuppgiftsbiträdet med beaktande av de tekniska och organisatoriska åtgärder som genomförts av dem i enlighet med artiklarna 25 och 32.
- e) Eventuella relevanta tidigare överträdelser som den personuppgiftsansvarige eller personuppgiftsbiträdet gjort sig skyldig till.
- f) Graden av samarbete med tillsynsmyndigheten för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter.
- g) De kategorier av personuppgifter som påverkas av överträdelsen.
- h) Det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, särskilt huruvida och i vilken omfattning den personuppgiftsansvarige eller personuppgiftsbiträdet anmälde överträdelsen.
- i) När åtgärder enligt artikel 58.2 tidigare har förordnats mot den berörda personuppgiftsansvarige eller personuppgiftsbiträdet vad gäller samma sakfråga, efterlevnad av dessa åtgärder.
- j) Tillämpandet av godkända uppförandekoder i enlighet med artikel 40 eller godkända certifieringsmekanismer i enlighet med artikel 42.
- k) Eventuell annan försvårande eller förmildrande faktor som är tillämplig på omständigheterna i fallet, såsom ekonomisk vinst som görs eller förlust som undviks, direkt eller indirekt, genom överträdelsen.

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

4. Vid överträdelser av följande bestämmelser ska det i enlighet med punkt 2 påföras administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om det gäller ett företag, på upp till 2 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

- a) Personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter enligt artiklarna 8, 11, 25–39, 42 och 43.
- b) Certifieringsorganets skyldigheter enligt artiklarna 42 och 43.
- c) Övervakningsorganets skyldigheter enligt artikel 41.4.

5. Vid överträdelser av följande bestämmelser ska det i enlighet med punkt 2 påföras administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

- a) De grundläggande principerna för behandling, inklusive villkoren för samtycke, enligt artiklarna 5, 6, 7 och 9.
- b) Registrerades rättigheter enligt artiklarna 12–22.
- c) Överföring av personuppgifter till en mottagare i ett tredjeland eller en internationell organisation enligt artiklarna 44–49.
- d) Alla skyldigheter som följer av medlemsstaternas lagstiftning som antagits på grundval av kapitel IX.
- e) Underlåtenhet att rätta sig efter ett föreläggande eller en tillfällig eller permanent begränsning av behandling av uppgifter eller ett beslut om att avbryta uppgiftsflödena som meddelats av tillsynsmyndigheten i enlighet med artikel 58.2 eller underlåtelse att ge tillgång till uppgifter i strid med artikel 58.1.

6. Vid underlåtenhet att rätta sig efter ett föreläggande från tillsynsmyndigheten i enlighet med artikel 58.2 ska det i enlighet med punkt 2 i den här artikeln påföras administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

7. Utan att det påverkar tillsynsmyndigheternas korrigerande befogenheter enligt artikel 58.2 får varje medlemsstat fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och organ som är inrättade i medlemsstaten.

8. Tillsynsmyndighetens utövande av sina befogenheter enligt denna artikel ska omfattas av lämpliga rättssäkerhetsgarantier i enlighet med unionsrätten och medlemsstaternas nationella rätt, inbegripet effektiva rättsmedel och rättssäkerhet.

9. Om det i medlemsstatens rättssystem inte finns några föreskrifter om administrativa sanktionsavgifter får den här artikeln tillämpas så att förfarandet inleds av den behöriga tillsynsmyndigheten och sanktionsavgifterna sedan utdöms av behörig nationell domstol, varvid det säkerställs att rättsmedlen är effektiva och har motsvarande verkan som de administrativa sanktionsavgifter som påförs av tillsynsmyndigheter. De sanktionsavgifter som påförs ska i alla händelser vara effektiva, proportionella och avskräckande. Dessa medlemsstater ska till kommissionen anmäla de bestämmelser i deras lagstiftning som de antar i enlighet med denna punkt senast den 25 maj 2018, samt utan dröjsmål anmäla eventuell senare ändringslagstiftning eller ändringar som berör dem.

Artikel 84

Sanktioner

1. Medlemsstaterna ska fastställa regler om andra sanktioner för överträdelser av denna förordning, särskilt för överträdelser som inte är föremål för administrativa sanktionsavgifter enligt artikel 83, och vidta alla nödvändiga åtgärder för att säkerställa att de genomförs. Dessa sanktioner ska vara effektiva, proportionella och avskräckande.

2. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antar i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella senare ändringar som berör dem.

KAPITEL IX

Bestämmelser om särskilda behandlingssituationer

Artikel 85

Behandling och yttrande- och informationsfriheten

1. Medlemsstaterna ska i lag förena rätten till integritet i enlighet med denna förordning med yttrande- och informationsfriheten, inbegripet behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

2. Medlemsstaterna ska, för behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande, fastställa undantag eller avvikelser från kapitel II (principer), kapitel III (den registrerades rättigheter), kapitel IV (personuppgiftsansvarig och personuppgiftsbiträde), kapitel V (överföring av personuppgifter till tredjeländer eller internationella organisationer), kapitel VI (oberoende tillsynsmyndigheter), kapitel VII (samarbete och enhetlighet) och kapitel IX (särskilda situationer vid behandling av personuppgifter) om dessa är nödvändiga för att förena rätten till integritet med yttrande- och informationsfriheten.

3. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antagit i enlighet med punkt 2, samt utan dröjsmål anmäla eventuell senare ändringslagstiftning eller ändringar som berör dem.

Artikel 86

Behandling och allmänhetens tillgång till allmänna handlingar

Personuppgifter i allmänna handlingar som förvaras av en myndighet eller ett offentligt organ eller ett privat organ för utförande av en uppgift av allmänt intresse får lämnas ut av myndigheten eller organet i enlighet med den unionsrätt eller den medlemsstats nationella rätt som myndigheten eller det offentliga organet omfattas av, för att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd av personuppgifter i enlighet med denna förordning.

Artikel 87

Behandling av nationella identifikationsnummer

Medlemsstaterna får närmare bestämma på vilka särskilda villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas. Ett nationellt identifikationsnummer eller ett annat vedertaget sätt för identifiering ska i sådana fall endast användas med iakttagande av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt denna förordning.

Artikel 88

Behandling i anställningsförhållanden

1. Medlemsstaterna får i lag eller i kollektivavtal fastställa mer specifika regler för att säkerställa skyddet av rättigheter och friheter vid behandling av anställdas personuppgifter i anställningsförhållanden, särskilt när det gäller rekrytering, genomförande av anställningsavtalet inklusive befrielse från i lag eller kollektivavtal stadgade skyldigheter, ledning, planering och organisering av arbetet, jämställdhet och mångfald i arbetslivet, hälsa och säkerhet på arbetsplatsen samt skydd av arbetsgivarens eller kundens egendom men också när det gäller att såväl kollektivt som individuellt utöva och komma i åtnjutande av rättigheter och förmåner som är knutna till anställningen samt att avsluta anställningsförhållandet.

2. Dessa regler ska innehålla lämpliga och specifika åtgärder för att skydda den registrerades mänskliga värdighet, berättigade intressen och grundläggande rättigheter, varvid hänsyn särskilt ska tas till insyn i behandlingen, överföring av personuppgifter inom en koncern eller en grupp av företag som deltar i gemensam ekonomisk verksamhet samt övervakningssystem på arbetsplatsen.

3. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antar i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella senare ändringar som berör dem.

Artikel 89

Skyddsåtgärder och undantag för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål

1. Behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ska omfattas av lämpliga skyddsåtgärder i enlighet med denna förordning för den registrerades rättigheter och friheter. Skyddsåtgärderna ska säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt

principen om uppgiftsminimering iakttas. Dessa åtgärder får inbegripa pseudonymisering, under förutsättning att dessa ändamål kan uppfyllas på det sättet. När dessa ändamål kan uppfyllas genom vidare behandling av uppgifter som inte medger eller inte längre medger identifiering av de registrerade ska dessa ändamål uppfyllas på det sättet.

2. Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål får det i unionsrätten eller i medlemsstaternas nationella rätt föreskrivas undantag från de rättigheter som avses i artiklarna 15, 16, 18 och 21 med förbehåll för de villkor och skyddsåtgärder som avses i punkt 1 i den här artikeln i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla de särskilda ändamålen, och sådana undantag krävs för att uppnå dessa ändamål.

3. Om personuppgifter behandlas för arkivändamål av allmänt intresse får det i unionsrätten eller i medlemsstaternas nationella rätt föreskrivas om undantag från de rättigheter som avses i artiklarna 15, 16, 18, 19, 20 och 21 med förbehåll för de villkor och skyddsåtgärder som avses i punkt 1 i den här artikeln i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla de särskilda ändamålen, och sådana undantag krävs för att uppnå dessa ändamål.

4. Om behandling enligt punkterna 2 och 3 samtidigt har andra ändamål, ska undantagen endast tillämpas på behandling för de ändamål som avses i dessa punkter.

Artikel 90

Tystnadsplikt

1. Medlemsstaterna får anta särskilda bestämmelser för att fastställa tillsynsmyndigheternas befogenheter enligt artikel 58.1 e och f gentemot personuppgiftsansvariga eller personuppgiftsbiträden som enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställts av behöriga nationella organ omfattas av tystnadsplikt eller andra motsvarande former av förbud mot att lämna ut uppgifter, om det är nödvändigt och står i proportion till vad som behövs för att förena rätten till skydd för personuppgifter och tystnadsplikten. Dessa bestämmelser ska endast tillämpas med avseende på personuppgifter som den personuppgiftsansvarige eller personuppgiftsbiträdet har erhållit i samband med en verksamhet som omfattas av denna tystnadsplikt.

2. Varje medlemsstat ska till kommissionen anmäla de bestämmelser den har antagit i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella ändringar som berör dem.

Artikel 91

Befintliga bestämmelser om dataskydd inom kyrkor och religiösa samfund

1. Om kyrkor och religiösa samfund eller gemenskaper i en medlemsstat vid tidpunkten för ikraftträdandet av denna förordning tillämpar övergripande bestämmelser om skyddet av fysiska personer i samband med behandling, får sådana befintliga bestämmelser fortsätta att tillämpas under förutsättning att de görs förenliga med denna förordning.

2. Kyrkor och religiösa samfund som tillämpar övergripande bestämmelser i enlighet med punkt 1 i denna artikel ska vara föremål för kontroll av en oberoende tillsynsmyndighet som kan vara specifik, förutsatt att den uppfyller de villkor som fastställs i kapitel VI i denna förordning.

KAPITEL X

Delegerade akter och genomförandeakter

Artikel 92

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 12.8 och artikel 43.8 ska ges till kommissionen tills vidare från och med den 24 maj 2016.
3. Den delegering av befogenhet som avses i artikel 12.8 och artikel 43.8 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.
4. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.
5. En delegerad akt som antas enligt artikel 12.8 och artikel 43.8 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av tre månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med tre månader på Europaparlamentets eller rådets initiativ.

Artikel 93

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.
2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.
3. När det hänvisas till denna punkt ska artikel 8 i förordning (EU) nr 182/2011, jämförd med artikel 5 i samma förordning, tillämpas.

KAPITEL XI

Slutbestämmelser

Artikel 94

Upphävande av direktiv 95/46/EG

1. Direktiv 95/46/EG ska upphöra att gälla med verkan från och med den 25 maj 2018.
2. Hänvisningar till det upphävda direktivet ska anses som hänvisningar till denna förordning. Hänvisningar till arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, som inrättades genom artikel 29 i direktiv 95/46/EG, ska anses som hänvisningar till Europeiska dataskyddsstyrelsen, som inrättas genom denna förordning.

Artikel 95

Förhållande till direktiv 2002/58/EG

Denna förordning ska inte innebära några ytterligare förpliktelser för fysiska eller juridiska personer som behandlar personuppgifter inom ramen för tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät i unionen, när det gäller områden inom vilka de redan omfattas av särskilda skyldigheter för samma ändamål i enlighet med direktiv 2002/58/EG.

*Artikel 96***Förhållande till tidigare ingångna avtal**

De internationella avtal som rör överföring av personuppgifter till tredjeländer eller internationella organisationer som ingicks av medlemsstaterna före den 24 maj 2016 och som är förenliga med unionsrätten i dess lydelse innan detta datum, ska fortsätta att gälla tills de ändras, ersätts eller återkallas.

*Artikel 97***Kommissionsrapporter**

1. Senast den 25 maj 2020 och därefter vart fjärde år ska kommissionen överlämna en rapport om tillämpningen och översynen av denna förordning till Europaparlamentet och rådet.
2. Inom ramen för de utvärderingar och översyner som avses i punkt 1 ska kommissionen särskilt undersöka hur följande bestämmelser tillämpas och fungerar:
 - a) Kapitel V om överföring av personuppgifter till tredjeländer och internationella organisationer, särskilt när det gäller beslut som antagits enligt artikel 45.3 i den här förordningen och beslut som antagits på grundval av artikel 25.6 i direktiv 95/46/EG.
 - b) Kapitel VII om samarbete och enhetlighet.
3. Med avseende på tillämpningen av punkt 1 får kommissionen begära information från medlemsstaterna och tillsynsmyndigheterna.
4. Kommissionen ska när den utför de utvärderingar och översyner som avses i punkterna 1 och 2 ta hänsyn till ståndpunkter och slutsatser från Europaparlamentet, rådet och andra relevanta organ och källor.
5. Kommissionen ska om nödvändigt överlämna lämpliga förslag om ändring av denna förordning, med särskild hänsyn till informationsteknikens utveckling och mot bakgrund av tendenserna inom informationssamhället.

*Artikel 98***Översyn av andra unionsrättsakter om dataskydd**

Kommissionen ska, om så är lämpligt, lägga fram lagstiftningsförslag i syfte att ändra andra unionsrättsakter om skydd av personuppgifter, för att säkerställa ett enhetligt och konsekvent skydd för fysiska personer med avseende på behandling. Detta gäller i synnerhet bestämmelserna om skyddet för fysiska personer i samband med behandling som utförs av unionens institutioner, organ och byråer samt om det fria flödet av sådana uppgifter.

*Artikel 99***Ikraftträdande och tillämpning**

1. Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.
2. Den ska tillämpas från och med den 25 maj 2018.

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

Utfärdad i Bryssel den 27 april 2016.

På Europaparlamentets vägnar

M. SCHULZ

Ordförande

På rådets vägnar

J.A. HENNIS-PLASSCHAERT

Ordförande

DIREKTIV

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2016/680

av den 27 april 2016

om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

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

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Regionkommitténs yttrande ⁽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.
- (2) Principerna och reglerna för skyddet för fysiska personer med avseende på behandling av deras personuppgifter bör, oavsett deras medborgarskap eller hemvist, respektera deras rättigheter och grundläggande friheter, särskilt deras rätt till skydd av personuppgifter. Detta direktiv är avsett att bidra till att skapa ett område med frihet, säkerhet och rättvisa.
- (3) Den snabba tekniska utvecklingen och globaliseringen har skapat nya utmaningar vad gäller skyddet av personuppgifter. Omfattningen av insamlingen och delningen av personuppgifter har ökat avsevärt. Tekniken gör det möjligt att i en aldrig tidigare skådad omfattning behandla personuppgifter i verksamheter såsom förebyggande, förhindrande, utredning, avslöjande och lagföring av brott eller verkställighet av straffrättsliga påföljder.
- (4) Det fria flödet av personuppgifter mellan behöriga myndigheter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten inom unionen, samt överföringar av sådana personuppgifter till tredjeländer och internationella organisationer, bör underlättas samtidigt som en hög skyddsnivå för personuppgifter säkerställs. Denna utveckling kräver en stark och mer sammanhängande ram för skyddet av personuppgifter inom unionen, uppbackad av kraftfullt tillsynsarbete.
- (5) Europaparlamentets och rådets direktiv 95/46/EG ⁽³⁾ är tillämpligt på all behandling av personuppgifter i medlemsstaterna, såväl inom den offentliga som inom den privata sektorn. Det är emellertid inte tillämpligt på behandling av personuppgifter "som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten", t.ex. verksamhet på områdena för straffrättsligt samarbete och polissamarbete.

⁽¹⁾ EUT C 391, 18.12.2012, s. 127.

⁽²⁾ Europaparlamentets ståndpunkt av den 12 mars 2014 (ännu ej offentliggjord i EUT) och rådets ståndpunkt vid första behandlingen av den 8 april 2016 (ännu ej offentliggjord i EUT). Europaparlamentets ståndpunkt av den 14 april 2016.

⁽³⁾ Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).

- (6) Rådets rambeslut 2008/977/RIF ⁽¹⁾ är tillämpligt på områdena för straffrättsligt samarbete och polissamarbete. Tillämpningsområdet för det rambeslutet begränsas till behandling av sådana personuppgifter som överförs eller görs tillgängliga mellan medlemsstaterna.
- (7) Att säkerställa en enhetlig och hög skyddsnivå för fysiska personers personuppgifter och underlätta utbytet av personuppgifter mellan behöriga myndigheter i medlemsstaterna är av avgörande betydelse för att säkerställa ett effektivt straffrättsligt samarbete och polissamarbete. Därför bör skyddet för fysiska personers rättigheter och friheter i samband med behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, vara likvärdigt i alla medlemsstater. Ett effektivt skydd av personuppgifter i hela unionen förutsätter att de registrerades rättigheter stärks och att skyldigheterna för dem som behandlar personuppgifter, ökar, samt likvärdiga befogenheter för att övervaka och säkerställa efterlevnaden av bestämmelserna om skydd av personuppgifter i medlemsstaterna.
- (8) I artikel 16.2 i EUF-fördraget bemyndigas Europaparlamentet och rådet att fastställa bestämmelser om skydd för fysiska personer när det gäller behandling av personuppgifter samt om det fria flödet för personuppgifter.
- (9) Med stöd av denna grund fastställs i Europaparlamentets och rådets förordning (EU) 2016/679 ⁽²⁾ allmänna bestämmelser om skydd av fysiska personer i samband med behandling av personuppgifter och om det fria flödet för sådana uppgifter inom unionen.
- (10) I förklaring nr 21 om skydd av personuppgifter på området för straffrättsligt samarbete och polissamarbete, fogad till slutakten från den regeringskonferens som antog Lissabonfördraget, bekräftade konferensen att det med hänsyn till dessa områdens särart kan komma att bli nödvändigt att anta särskilda regler om skydd av personuppgifter och om det fria flödet av personuppgifter på områdena för straffrättsligt samarbete och polissamarbete med stöd av artikel 16 i EUF-fördraget.
- (11) Det är därför lämpligt att dessa områden behandlas i ett direktiv som fastställer särskilda regler om skydd för fysiska personer i samband med behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, med respekt för den särskilda karaktären hos denna verksamhet. Sådana behöriga myndigheter kan omfatta inte bara offentliga myndigheter såsom rättsliga myndigheter, polis eller andra brottsbekämpande myndigheter, utan också alla andra organ eller enheter som genom medlemsstaternas nationella rätt har anförtratts myndighetsutövning enligt detta direktiv. Förordning (EU) 2016/679 bör tillämpas när ett sådant organ eller en sådan enhet behandlar personuppgifter för andra ändamål än de som avses i detta direktiv. Förordning (EU) 2016/679 är därför tillämplig i fall då ett organ eller en enhet samlar in personuppgifter för andra ändamål och behandlar dessa personuppgifter ytterligare för att iakttä sina rättsliga skyldigheter. Exempelvis behåller finansinstitut vissa personuppgifter som de behandlar i syfte att utreda, avslöja eller lagföra brott, och tillhandahåller dessa personuppgifter för behöriga nationella myndigheter endast i särskilda fall och i enlighet med medlemsstaternas nationella rätt. Ett organ eller en enhet som behandlar personuppgifter för sådana myndigheters räkning inom detta direktivs tillämpningsområde bör vara bundet av ett avtal eller annan rättsakt och de bestämmelser som är tillämpliga på personuppgiftsbiträden enligt detta direktiv, medan tillämpningen av förordning (EU) 2016/679 förblir opåverkad när det gäller personuppgiftsbitrådets behandling av personuppgifter som inte omfattas av detta direktivs tillämpningsområde.
- (12) Polisens och andra brottsbekämpande myndigheters verksamhet är främst inriktad på att förebygga, förhindra, utreda, avslöja och lagföra brott, inbegripet polisverksamhet där man inte på förhand vet om det inträffade utgör ett brott eller inte. Sådan verksamhet kan också innefatta myndighetsutövning genom vidtagande av tvångsåtgärder vid demonstrationer, större idrottsevenemang och upplopp. Denna verksamhet omfattar också upprätthållande av lag och ordning som en uppgift som anförtros åt polisen eller andra brottsbekämpande

⁽¹⁾ Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (EUT L 350, 30.12.2008, s. 60).

⁽²⁾ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (se sidan 1 i detta nummer av EUT).

myndigheter när det är nödvändigt för att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten och mot i lag skyddade grundläggande allmänna intressen som kan leda till ett brott. Medlemsstaterna får åt behöriga myndigheter anförtro andra uppgifter som inte nödvändigtvis utförs för att förebygga, förhindra, utreda, avslöja eller lagföra brott, inklusive att skydda mot och förebygga hot mot den allmänna säkerheten, så att behandlingen av personuppgifter för dessa andra ändamål, i den mån den omfattas av unionsrätten, omfattas av tillämpningsområdet för förordning (EU) 2016/679.

- (13) Ett brott i den mening som avses i detta direktiv bör utgöra ett självständigt begrepp i unionsrätten enligt Europeiska unionens domstols (nedan kallad *domstolen*) tolkning.
- (14) Eftersom detta direktiv inte bör tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten, bör verksamhet som rör nationell säkerhet, verksamhet som utförs av byråer och organ som hanterar nationella säkerhetsfrågor och medlemsstaternas behandling av personuppgifter när de utför verksamhet som omfattas av del V kapitel 2 i fördraget om Europeiska unionen (EU-fördraget) inte betraktas som verksamhet som omfattas av detta direktivs tillämpningsområde.
- (15) För att säkerställa en enhetlig skyddsnivå för fysiska personer genom rättsligt verkställbara rättigheter i hela unionen och undvika avvikelser som hämmar utbytet av personuppgifter mellan behöriga myndigheter, bör detta direktiv innehålla harmoniserade bestämmelser om skydd och fri rörlighet för personuppgifter som behandlas för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Tillnärmningen av medlemsstaternas nationella rätt bör inte leda till försämringar i det personuppgiftsskydd de tillhandahåller, utan i stället ha till syfte att säkerställa en hög skyddsnivå inom unionen. Inget ska hindra medlemsstaterna från att föreskriva starkare skyddsåtgärder än dem som fastställs i detta direktiv för skyddet av den registrerades rättigheter och friheter med avseende på behöriga myndigheters behandling av personuppgifter.
- (16) Detta direktiv påverkar inte tillämpningen av principen om allmänhetens rätt att få tillgång till allmänna handlingar. Enligt förordning (EU) 2016/679 får personuppgifter i allmänna handlingar som förvaras av en offentlig myndighet eller ett offentligt eller privat organ för utförande av en uppgift av allmänt intresse lämnas ut av myndigheten eller organet i enlighet med unionsrätten eller medlemsstatens nationella lagstiftning som den offentliga myndigheten eller det offentliga organet omfattas av, för att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd av personuppgifter.
- (17) Det skydd som ska tillhandahållas enligt detta direktiv bör tillämpas på fysiska personer, oavsett medborgarskap eller hemvist, med avseende på behandling av deras personuppgifter.
- (18) För att förhindra att det uppstår en allvarlig risk för att reglerna kringgås bör skyddet för fysiska personer vara teknikneutralt och inte vara beroende av den teknik som används. Skyddet för fysiska personer bör vara tillämpligt på både automatiserad och manuell behandling av personuppgifter, om personuppgifterna ingår i eller är avsedda att ingå i ett register. Akter eller grupper av akter samt omslag till dessa, som inte är ordnade enligt särskilda kriterier, bör inte omfattas av detta direktiv.
- (19) Europaparlamentets och rådets förordning (EG) nr 45/2001⁽¹⁾ är tillämplig på den behandling av personuppgifter som sker i unionens institutioner, organ och byråer. Förordning (EG) nr 45/2001 och de av unionens övriga rättsakter som är tillämpliga på sådan behandling av personuppgifter bör anpassas till principerna och bestämmelserna i förordning (EU) 2016/679.
- (20) Detta direktiv bör inte hindra medlemsstaterna från att i nationell straffprocesslagstiftning ange vilken behandling och vilka förfaranden för behandling som berörs när det gäller domstolars och andra rättsliga myndigheters behandling av personuppgifter, särskilt när det gäller personuppgifter som ingår i ett domstolsbeslut eller i protokoll avseende straffrättsliga förfaranden.

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

- (21) Principerna för dataskydd bör gälla all information som rör en identifierad eller identifierbar fysisk person. För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel, som t.ex. utgallring, som, antingen av den personuppgiftsansvarige eller av någon annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva faktorer som kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen. Principerna för dataskydd bör därför inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte längre är identifierbar.
- (22) Offentliga myndigheter som för sin myndighetsutövning mottar personuppgifter i enlighet med en rättslig förpliktelse, t.ex. skatte- och tullmyndigheter, finansutredningsgrupper, oberoende administrativa myndigheter eller finansmarknadsmyndigheter med ansvar för reglering och övervakning av värdepappersmarknader, bör inte betraktas som mottagare om de tar emot personuppgifter som är nödvändiga för utförandet av en särskild utredning i allmänhetens intresse, i enlighet med unionsrätten eller medlemstaternas nationella rätt. Offentliga myndigheters begäranden om att uppgifter ska lämnas ut bör alltid vara skriftliga och motiverade, läggas fram i enskilda fall och inte gälla hela register eller leda till att register kopplas samman. Dessa offentliga myndigheters behandling av personuppgifter bör ske i överensstämmelse med de bestämmelser om dataskydd som är tillämpliga på behandlingens ändamål.
- (23) Genetiska uppgifter bör definieras som personuppgifter som rör en fysisk persons nedärvda eller förvärvade genetiska kännetecken som ger unik information om denna enskilda persons fysiologi eller hälsa och vilka framgår av en analys av ett biologiskt prov från den fysiska personen i fråga, framför allt kromosom-, DNA- eller RNA-analys eller av en annan form av analys som gör det möjligt att inhämta motsvarande information. Eftersom genetiska uppgifter är komplexa och känsliga finns det en stor risk för att den personuppgiftsansvarige missbrukar och återanvänder dem för olika ändamål. All diskriminering på grundval av genetiska särdrag bör i princip vara förbjuden.
- (24) Personuppgifter om hälsa bör innefatta alla uppgifter som hänför sig till en registrerad persons hälsotillstånd som ger information om den registrerades tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd. Detta innebär uppgifter om den enskilda personen som samlats in i samband med registrering för eller tillhandahållande av hälso- och sjukvårdstjänster till den fysiska personen enligt Europaparlamentets och rådets direktiv 2011/24/EU ⁽¹⁾, ett nummer, en symbol eller ett kännetecken som personen tilldelats för att unikt identifiera den fysiska personen för hälso- och sjukvårdsändamål, uppgifter som härrör från tester eller undersökningar av en kroppsdelen eller kroppssubstans, däribland genetiska uppgifter och biologiska prover, och andra uppgifter om exempelvis sjukdom, funktionshinder, sjukdomsrisk, sjukdomshistoria, klinisk behandling, eller den registrerades fysiologiska eller biomedicinska tillstånd oberoende av källan, exempelvis från en läkare eller från annan sjukvårdspersonal, ett sjukhus, en medicinteknisk produkt eller ett diagnostiskt in vitro-test.
- (25) Samtliga medlemsstater är anslutna till Internationella kriminalpolisorganisationen (Interpol). För att kunna fullgöra sitt uppdrag mottar, lagrar och cirkulerar Interpol personuppgifter i syfte att hjälpa behöriga myndigheter att förebygga, förhindra och bekämpa internationell brottslighet. Därför är det lämpligt att stärka samarbetet mellan unionen och Interpol genom att främja ett effektivt utbyte av personuppgifter med respekt för de grundläggande rättigheterna och friheterna vid automatiserad behandling av personuppgifter. När personuppgifter överförs från unionen till Interpol samt till länder som har delegerade medlemmar i Interpol bör detta direktiv, framför allt bestämmelserna om internationella överföringar, gälla. Detta direktiv bör inte påverka de särskilda bestämmelserna i rådets gemensamma ståndpunkt 2005/69/RIF ⁽²⁾ och rådets beslut 2007/533/RIF ⁽³⁾.
- (26) Varje behandling av personuppgifter måste vara laglig, korrekt och öppen i förhållande till berörda fysiska personer och endast genomföras för särskilda lagstadgade ändamål. Detta hindrar i sig inte brottsbekämpande myndigheter från att genomföra verksamhet såsom hemliga utredningar eller videoövervakning. Sådan verksamhet kan genomföras i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa

⁽¹⁾ Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).

⁽²⁾ Rådets gemensamma ståndpunkt 2005/69/RIF av den 24 januari 2005 om utbyte av vissa uppgifter med Interpol (EUT L 27, 29.1.2005, s. 61).

⁽³⁾ Rådets beslut 2007/533/RIF av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) (EUT L 205, 7.8.2007, s. 63).

straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, förutsatt att verksamheten har fastställts i lag och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den fysiska personens berättigade intressen. Dataskyddsprincipen om korrekt behandling är ett begrepp som är skilt från rätten till en opartisk domstol enligt artikel 47 i stadgan och rätten till en rättvis rättegång enligt artikel 6 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Fysiska personer bör göras medvetna om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter och om hur de kan utöva sina rättigheter med avseende på behandlingen. De specifika ändamål som personuppgifterna behandlas för bör vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in. Personuppgifterna bör vara adekvata och relevanta för de ändamål som de behandlas för. Det bör i synnerhet säkerställas att de uppgifter som insamlats inte är orimligt omfattande och att de inte sparas längre än vad som är nödvändigt för det ändamål för vilket uppgifterna behandlas. Personuppgifter bör endast behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel. För att säkerställa att uppgifter inte sparas längre än nödvändigt bör den personuppgiftsansvarige införa tidsfrister för radering eller för regelbunden kontroll. Medlemsstaterna bör inrätta lämpliga skyddsåtgärder för personuppgifter som lagras under längre perioder, för arkivändamål av allmänt intresse, för vetenskapliga, statistiska eller historiska ändamål.

- (27) Om behöriga myndigheter ska kunna förebygga, förhindra, utreda och lagföra brott är det nödvändigt att de behandlar personuppgifter som insamlats inom ramen för förebyggande, förhindrande, utredning och lagföring av specifika brott i ett bredare sammanhang för att utveckla förståelsen för kriminell verksamhet och göra kopplingar mellan olika upptäckta brott.
- (28) För att bibehålla behandlingens säkerhet och förhindra behandling som innebär en överträdelse av detta direktiv bör personuppgifter behandlas på ett sätt som säkerställer en lämplig säkerhets- och konfidentialitetsnivå samt förhindrar obehörigt tillträde till eller obehörig användning av personuppgifter och den utrustning som används för behandlingen, med beaktande av tillgänglig teknik och den tekniska utvecklingen samt genomförandekostnader i förhållande till riskerna och den typ av personuppgifter som ska skyddas.
- (29) Personuppgifter bör samlas in för särskilda, uttryckligt angivna och berättigade ändamål som omfattas av detta direktivs tillämpningsområde och bör inte behandlas för andra ändamål än att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Om samma eller en annan personuppgiftsansvarig behandlar personuppgifter för ett ändamål som omfattas av detta direktiv men som inte är det ändamål som uppgifterna insamlades för, bör behandlingen vara tillåten, förutsatt att behandlingen har godkänts i enlighet med tillämpliga rättsliga bestämmelser och är nödvändig och står i proportion till det andra ändamålet.
- (30) Principen om uppgifters korrekthet bör tillämpas med hänsyn till den typ av behandling det är fråga om och syftet med denna. Särskilt i domstolsförfaranden baseras utsagor som innehåller personuppgifter på fysiska personers subjektiva uppfattning, och kan inte alltid verifieras. Följaktligen bör inte korrekthetskravet röra korrektheten i en utsaga, utan endast det faktum att en viss utsaga har gjorts.
- (31) Behandling av personuppgifter på områdena för straffrättsligt samarbete och polissamarbete innebär av naturliga skäl att personuppgifter om olika kategorier av registrerade behandlas. Därför är det viktigt att i tillämpliga fall och i möjligaste mån göra en klar åtskillnad mellan personuppgifter om olika kategorier av registrerade, t.ex. brottsmisstänkta, brottsdömda och brottsoffer samt andra som berörs av ett brottmål, t.ex. vittnen, personer med relevant information eller personer med kontakter eller band till brottsmisstänkta och brottsdömda. Detta bör inte hindra tillämpningen av rätten till oskuldspresumtion som garanteras i stadgan och i Europakonventionen, tolkade enligt rättspraxis från domstolen och Europeiska domstolen för de mänskliga rättigheterna.
- (32) De behöriga myndigheterna bör säkerställa att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. För att säkerställa skydd för fysiska personer, korrekthet, fullständighet eller i vilken grad personuppgifterna är aktuella och tillförlitlighet i de personuppgifter som överförs eller görs tillgängliga, bör de behöriga myndigheterna i möjligaste mån föra in nödvändiga uppgifter vid all överföring av personuppgifter.
- (33) När det i detta direktiv hänvisas till medlemsstaternas nationella rätt, en rättslig grund eller lagstiftningsåtgärd innebär detta inte nödvändigtvis en lagstiftningsakt antagen av ett parlament, med förbehåll för krav i den

berörda medlemsstatens konstitutionella ordning. Medlemsstaternas nationella rätt, den rättsliga grunden eller lagstiftningsåtgärden bör emellertid i dessa fall vara tydlig och precis, och dess tillämpning förutsägbar för dem som omfattas av den i enlighet med rättspraxis från domstolen och Europeiska domstolen för de mänskliga rättigheterna. Medlemsstaternas nationella rätt som reglerar behandlingen av personuppgifter inom tillämpningsområdet för detta direktiv bör åtminstone specificera målen, vilka personuppgifter som ska behandlas, behandlingens ändamål, förfarandena för att bevara personuppgifternas integritet och konfidentialitet samt förfarandena för förstöring av dem så att tillräckliga garantier mot risken för missbruk och godtycklighet ges.

- (34) Behöriga myndigheters behandling av personuppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott, verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, bör omfatta varje åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter som utförs i dessa syften, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, justering eller sammanförande, begränsning av behandlingen, radering eller förstöring. Framför allt bör bestämmelserna i detta direktiv gälla personuppgifter som vid tillämpningen av detta direktiv överförs till en mottagare som inte omfattas av detta direktiv. Med sådana mottagare bör avses fysiska eller juridiska personer, myndigheter, institutioner eller andra organ som den behöriga myndigheten lagligen lämnar ut personuppgifterna till. Om personuppgifter ursprungligen samlats in av en behörig myndighet för något av detta direktivs ändamål, bör förordning (EU) 2016/679 vara tillämplig på behandlingen av dessa uppgifter för andra ändamål än de som anges i detta direktiv om behandlingen är godkänd enligt unionsrätten eller nationell rätt. Framför allt bör bestämmelserna i förordning (EU) 2016/679 gälla överföring av personuppgifter för ändamål som inte omfattas av detta direktiv. Förordning (EU) 2016/679 bör gälla när personuppgifter behandlas av en mottagare som varken är eller agerar i egenskap av behörig myndighet i den mening som avses i detta direktiv och som lagligen mottagit personuppgifter av en behörig myndighet. Vid tillämpningen av detta direktiv bör medlemsstaterna också närmare kunna ange tillämpningen av bestämmelserna i förordning (EU) 2016/679 på de villkor som anges i den förordningen.
- (35) För att vara laglig bör behandlingen av personuppgifter enligt detta direktiv vara nödvändig för att utföra en uppgift av allmänt intresse som en behörig myndighet ansvarar för enligt unionsrätten eller medlemsstaternas nationella rätt för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Denna verksamhet bör omfatta skydd av intressen som är av grundläggande betydelse för den registrerade. Utförandet av uppgifterna att förebygga, förhindra, utreda, avslöja eller lagföra brott, som de behöriga myndigheterna institutionellt har tilldelats enligt lag, gör det möjligt för dem att kräva eller beordra att fysiska personer efterlever de begäranden som gjorts. I detta fall bör den registrerades samtycke, enligt definitionen i förordning (EU) 2016/679, inte utgöra en rättslig grund för behöriga myndigheters behandling av personuppgifter. Om den registrerade är skyldig att fullgöra en rättslig förpliktelse har den registrerade inte någon genuin och fri valmöjlighet, och således är det inte möjligt att betrakta den registrerades reaktion som en frivillig viljeyttring. Detta bör inte hindra medlemsstaterna från att i lag fastställa att den registrerade får tillåta behandling av sina personuppgifter vid tillämpning av detta direktiv, såsom DNA-testning inom ramen för brottsutredningar eller övervakning av var den registrerade befinner sig med elektronisk fotboja för verkställighet av straffrättsliga påföljder.
- (36) Medlemsstaterna bör föreskriva att om det i den unionsrätt eller nationella rätt som är tillämplig på den överförande behöriga myndigheten fastställs särskilda villkor som under särskilda omständigheter är tillämpliga på behandlingen av personuppgifter, såsom användning av hanteringskoder, bör den överförande behöriga myndigheten informera den mottagare till vilken uppgifterna överförs om dessa villkor och om kravet att respektera dem. Sådana villkor kan till exempel innefatta ett förbud mot att överföra personuppgifter till andra mottagare eller använda dem i andra syften än de för vilka de överfördes till mottagaren eller att informera den registrerade vid en begränsning av rätten till information utan förhandsgodkännande från den överförande behöriga myndigheten. Dessa skyldigheter bör även gälla för överföringar från den överförande behöriga myndigheten till mottagare i tredjeländer eller internationella organisationer. Medlemsstaterna bör säkerställa att den överförande behöriga myndigheten inte tillämpar dessa villkor på mottagare i andra medlemsstater eller på byråer och organ som inrättats i enlighet med avdelning V kapitlen 4 och 5 i EUF-fördraget, med undantag för sådana villkor som är tillämpliga på motsvarande överföringar av uppgifter inom den medlemsstat där den behöriga myndigheten är belägen.
- (37) Personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheter och friheter bör åtnjuta ett särskilt skydd eftersom behandling av sådana uppgifter kan innebära betydande risker för de grundläggande rättigheterna och friheterna. Dessa personuppgifter bör även inbegripa personuppgifter som avslöjar ras eller etniskt ursprung, varvid användningen av termen *ras* i detta direktiv inte innebär att unionen

godtar teorier som söker fastställa förekomsten av skilda människoraser. Dessa personuppgifter bör inte behandlas såvida inte behandlingen omfattas av lämpliga skyddsåtgärder för den registrerades lagstadgade rättigheter och friheter och medges i fall som är tillåtna enligt lag, eller behandlingen, om den ännu inte är tillåten enligt lag, är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan person, eller behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade. Lämpliga skyddsåtgärder för den registrerades rättigheter och friheter kan till exempel innebära möjligheten att samla in dessa uppgifter endast i samband med andra uppgifter om den berörda fysiska personen, möjligheten att säkra de insamlade uppgifterna, striktare regler om tillgång till uppgifterna för den behöriga myndighetens personal på lämpligt sätt, och förbud mot att översända sådana uppgifter. Behandling av sådana uppgifter bör även tillåtas enligt lag när den registrerade uttryckligen har gett sitt samtycke i fall där uppgiftsbehandlingen är särskilt inkräktande för honom eller henne. Den registrerades samtycke bör dock inte i sig utgöra någon rättslig grund för behöriga myndigheters behandling av sådana känsliga personuppgifter.

- (38) Den registrerade bör ha rätt att inte bli föremål för ett beslut angående bedömning av personliga aspekter rörande honom eller henne som uteslutande grundas på automatiserad behandling och som har negativa rättsliga följder eller i betydande grad påverkar honom eller henne. Denna form av uppgiftsbehandling bör under alla omständigheter omfattas av lämpliga skyddsåtgärder, inbegripet skild information till den registrerade och rätt till personlig kontakt, särskilt för framförande av egna synpunkter, rätten att erhålla en förklaring för det beslut som fattats efter sådan bedömning och rätten att överklaga beslutet. Profileringsomständigheter som leder till diskriminering av fysiska personer på grundval av personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheter och friheter är förbjuden på de villkor som fastställs i artiklarna 21 och 52 i stadgan.
- (39) För att den registrerade ska kunna utöva sina rättigheter bör all information till denne vara lättåtkomlig, t.ex. via den personuppgiftsansvariges webbplats, och lättbegriplig, på ett klart och tydligt språk. Denna information bör anpassas till de behov som sårbara människor, t.ex. barn, har.
- (40) Det bör finnas arrangemang som underlättar för registrerade att utöva sina rättigheter enligt de bestämmelser som antas i enlighet med detta direktiv, bl.a. rutiner för att kostnadsfritt begära och i tillämpliga fall få, särskilt, kostnadsfri tillgång till och rättelse eller radering av personuppgifter och begränsning av behandlingen. Personuppgiftsansvariga bör vara skyldiga att besvara en begäran från den registrerade utan onödigt dröjsmål, om inte de personuppgiftsansvariga tillämpar begränsningar av den registrerades rättigheter i enlighet med detta direktiv. Om en begäran är uppenbart ogrundad eller orimlig, som i fall då en registrerad utan skäl och vid upprepade tillfällen begär uppgifter eller om denne missbrukar sin rätt till information genom att exempelvis i sin begäran tillhandahålla felaktig eller missvisande information, bör den personuppgiftsansvarige dessutom kunna ta ut en rimlig avgift eller vägra att tillmötesgå begäran.
- (41) När den personuppgiftsansvarige begär att ytterligare information som är nödvändig för att bekräfta den registrerades identitet ska tillhandahållas bör denna information endast behandlas för detta specifika ändamål och bör inte lagras längre än vad som krävs för detta ändamål.
- (42) Åtminstone följande information bör göras tillgänglig för den registrerade: Vem som är personuppgiftsansvarig, att behandling sker, syftena med behandlingen, rätten att lämna in klagomål och rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandlingen. Informationen kan anges på den behöriga myndighetens webbplats. Dessutom bör den registrerade, i specifika fall och för att göra det möjligt för honom eller henne att utöva sina rättigheter, informeras om behandlingens rättsliga grund och om hur länge uppgifterna kommer att lagras, i den utsträckning som den ytterligare informationen är nödvändig, med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas, för att garantera en korrekt behandling när det gäller den registrerade.
- (43) Fysiska personer bör ha rätt att få tillgång till uppgifter som insamlats som rör dem samt att på enkelt sätt och med rimliga intervall kunna utöva denna rätt för att hålla sig underrättade om att behandling sker och kunna kontrollera att den är laglig. Därför bör varje registrerad ha rätt att känna till och underrättas om de ändamål för vilka uppgifterna behandlas, hur länge behandlingen kommer att pågå och vilka som kommer att få del av uppgifterna, inbegripet mottagare i tredjeländer. Om denna underrättelse omfattar information om personuppgifternas ursprung bör denna information inte avslöja fysiska personers identitet, framför allt konfidentiella källor. För att denna rättighet ska respekteras är det tillräckligt att den registrerade innehar en komplett sammanfattning av dessa uppgifter i begripligt format, det vill säga ett format som gör det möjligt för den registrerade att få kännedom om dessa uppgifter och kontrollera att de är korrekta och behandlade i enlighet med detta direktiv så

att den sökande kan utöva de rättigheter som han eller hon tilldelas enligt detta direktiv. En sådan sammanfattning skulle kunna tillhandahållas i form av en kopia av de personuppgifter som håller på att behandlas.

- (44) Medlemsstaterna bör ha möjlighet att genom lagstiftning vidta åtgärder som innebär att informationen till de registrerade senareläggs, begränsas eller utelämnas eller att deras tillgång till sina personuppgifter helt eller delvis begränsas, i den utsträckning och så länge som en sådan åtgärd utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, och syftet är att undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden, undvika menlig inverkan på förebyggande, förhindrande, utredning, upptäckt eller lagföring av brott eller verkställighet av straffrättsliga påföljder, skydd för allmän eller nationell säkerhet eller skydd för andra personers rättigheter och friheter. Den personuppgiftsansvarige bör genom en konkret och individuell granskning i varje enskilt fall bedöma om rätten till tillgång delvis eller helt bör begränsas.
- (45) En vägran eller begränsning av tillgång bör i princip meddelas den registrerade skriftligen och inkludera de faktiska eller rättsliga skäl som beslutet grundar sig på.
- (46) All begränsning av den registrerades rättigheter måste vara förenlig med stadgan och med Europakonventionen, tolkade enligt rättspraxis från domstolen respektive Europeiska domstolen för de mänskliga rättigheterna, och i synnerhet respektera kärnan i dessa rättigheter och friheter.
- (47) Fysiska personer bör ha rätt att få felaktiga personuppgifter som rör dem rättade, särskilt faktauppgifter, samt rätt att få dem raderade om behandlingen av uppgifterna utgör en överträdelse av detta direktiv. Rätten till rättelse bör emellertid inte påverka exempelvis innehållet i ett vittnesmål. En fysisk person bör också ha rätt till begränsning av behandlingen när han eller hon bestrider korrektheten av en personuppgift och det inte kan fastställas huruvida denna är korrekt eller när personuppgiften måste sparas som bevisning. Framför allt bör behandlingen av personuppgifter begränsas snarare än att uppgifterna raderas om det i ett visst fall finns rimliga skäl att anta att en radering skulle kunna påverka den registrerades legitima intressen. I ett sådant fall bör begränsade uppgifter endast behandlas för det ändamål som hindrade att de raderades. Behandling av personuppgifter kan exempelvis begränsas genom att man flyttar de valda uppgifterna till ett annat databehandlingssystem, till exempel för arkivering, eller gör de valda uppgifterna otillgängliga. I automatiserade register bör begränsningen av behandlingen i princip ske med tekniska medel. Att behandlingen av personuppgifter är begränsad bör anges inom systemet på sådant sätt att det tydligt framgår att behandlingen av personuppgifterna är begränsad. Sådant rättelse, radering av personuppgifter eller begränsning av behandlingen bör meddelas till de mottagare till vilka uppgifterna har lämnats ut och till de behöriga myndigheter från vilka de oriktiga uppgifterna härrörde. De personuppgiftsansvariga bör också avstå från vidare spridning av sådana uppgifter.
- (48) Om en personuppgiftsansvarig nekar en registrerad dennes rätt till information, tillgång till, rättelse, eller radering av personuppgifter eller till begränsning av behandlingen bör den registrerade ha rätt att begära att den nationella tillsynsmyndigheten kontrollerar behandlingens laglighet. De registrerade bör informeras om denna rättighet. När en tillsynsmyndighet agerar för de registrerades räkning, bör tillsynsmyndigheten åtminstone informera dem om att tillsynsmyndigheten har utfört alla nödvändiga kontroller eller översyner. Tillsynsmyndigheten bör också informera de registrerade om rätten att begära rättslig prövning.
- (49) När personuppgifter behandlas inom ramen för en brottsutredning eller domstolsförfaranden vid brottmål, bör medlemsstaterna kunna föreskriva att rätten till information, tillgång, rättelse och radering samt till begränsning av behandlingen utövas i enlighet med nationella bestämmelser om rättsliga förfaranden.
- (50) Den personuppgiftsansvarige bör åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar. Personuppgiftsansvariga bör särskilt vara skyldiga att vidta lämpliga och effektiva åtgärder och bör kunna visa att behandlingen är förenlig med detta direktiv. I samband med dessa åtgärder bör behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter beaktas. De åtgärder som den personuppgiftsansvarige vidtar bör omfatta utarbetande och genomförande av särskilda skyddsåtgärder för behandling av personuppgifter om sårbara fysiska personer, t.ex. barn.
- (51) Risker för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av uppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller identitetsbedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller uppgifter som omfattas av tystnadsplikt, obehörigt hävande av

pseudonymisering, eller annan betydande ekonomisk eller social nackdel; eller om registrerade kan komma att berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter; om personuppgifter behandlas som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i fackförening, om genetiska uppgifter eller biometrisk uppgifter behandlas för att unikt identifiera en person eller om uppgifter om hälsa eller uppgifter om sexualliv och sexuell läggning eller fällande domar i brottmål samt brott eller därmed sammanhängande säkerhetsåtgärder behandlas; om det förekommer en bedömning av personliga aspekter, exempelvis analyser och förutsägelser beträffande sådant som rör arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlitlighet eller beteende, vistelseort eller förflyttningar, i syfte att skapa eller använda personliga profiler; eller om personuppgifter rörande sårbara fysiska personer, framför allt barn, behandlas; eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

- (52) Riskens sannolikhetsgrad och allvar bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas enligt en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen medför hög risk. Med hög risk avses en särskild risk för menlig inverkan på registrerades rättigheter och friheter.
- (53) Skyddet för fysiska personers rättigheter och friheter i samband med behandlingen av personuppgifter kräver lämpliga tekniska och organisatoriska åtgärder för att säkerställa att kraven i detta direktiv uppfylls. Genomförandet av sådana åtgärder bör inte enbart bero på ekonomiska hänsyn. För att kunna visa överensstämmelse med detta direktiv bör den personuppgiftsansvarige anta interna strategier och vidta åtgärder, som i synnerhet följer principerna om inbyggt dataskydd och dataskydd som standard. Om den personuppgiftsansvarige har genomfört en konsekvensbedömning avseende dataskydd i enlighet med detta direktiv bör resultatet beaktas vid utarbetandet av dessa åtgärder och förfaranden. Sådana åtgärder kan bland annat bestå av pseudonymisering snarast möjligt. Pseudonymisering vid tillämpning av detta direktiv kan utgöra ett verktyg som kan underlätta det fria flödet av personuppgifter inom området med frihet, säkerhet och rättvisa.
- (54) Skyddet för de registrerades rättigheter och friheter samt de personuppgiftsansvarigas och registerförarnas ansvar, också i förhållande till tillsynsmyndigheternas övervakning och åtgärder, kräver ett tydligt fastställande av vem som bär ansvaret enligt detta direktiv, bl.a. när personuppgiftsansvariga gemensamt fastställer ändamål och medel för en behandling tillsammans med andra personuppgiftsansvariga eller när en behandling utförs på en personuppgiftsansvarigs vägnar.
- (55) Ett personuppgiftsbiträdes behandling bör styras av en rättsakt som omfattar ett avtal som binder personuppgiftsbiträdet till den personuppgiftsansvarige och där det särskilt anges att personuppgiftsbiträdet endast bör agera på instruktion av den personuppgiftsansvarige. Personuppgiftsbiträdet bör beakta principen om inbyggt dataskydd och dataskydd som standard.
- (56) För att visa överensstämmelse med detta direktiv bör de personuppgiftsansvariga eller registerförarna föra register över alla kategorier av behandling som sker under deras ansvar. Alla personuppgiftsansvariga och personuppgiftsbiträden bör vara skyldiga att samarbeta med tillsynsmyndigheten och på dennas begäran göra detta register tillgängligt för myndigheten så att det kan tjäna som grund för övervakningen av behandlingen. Personuppgiftsansvariga eller personuppgiftsbiträden som behandlar personuppgifter i icke-automatiserade behandlingssystem bör ha infört effektiva metoder, t.ex. loggar eller andra typer av register, för att visa att behandlingen är laglig, möjliggöra egenkontroll och säkerställa dataintegritet och datasäkerhet.
- (57) Loggar bör åtminstone föras över behandlingar i automatiserade behandlingssystem såsom insamling, ändring, läsning, utlämning, inklusive överföringar, sammanförande eller radering. Identifieringen av den person som läst eller lämnat ut personuppgifter bör loggas och från denna identifiering skulle det kunna vara möjligt att fastställa motiveringen till behandlingen. Loggarna bör endast användas för att kontrollera om behandlingen av uppgifterna är tillåten, för egenkontroll, för att garantera dataintegritet och datasäkerhet samt för straffrättsliga förfaranden. Egenkontroll omfattar även behöriga myndigheters interna disciplinära förfaranden.
- (58) En konsekvensbedömning avseende dataskydd bör genomföras av den personuppgiftsansvarige om det är sannolikt att uppgiftsbehandlingen, på grund av sin karaktär, sin omfattning eller sina ändamål, medför en hög risk för de registrerades rättigheter och friheter, vilken i synnerhet bör omfatta planerade åtgärder, skyddsåtgärder och mekanismer för att säkerställa skyddet av personuppgifter och för att styrka efterlevnaden av detta direktiv. Konsekvensbedömningarna bör omfatta relevanta system och processer för behandling men inte enskilda fall.

- (59) I syfte att säkerställa ett effektivt skydd av de registrerades rättigheter och friheter bör den personuppgiftsansvarige eller personuppgiftsbiträdet i vissa fall samråda med tillsynsmyndigheten före behandlingen.
- (60) För att upprätthålla säkerheten och förhindra behandling som bryter mot detta direktiv bör personuppgiftsansvariga eller personuppgiftsbiträden utvärdera de risker som behandlingen är förknippad med och bör vidta åtgärder, såsom kryptering, för att mildra dem. Åtgärderna bör leda till en lämplig säkerhetsnivå, inklusive konfidentialitetsnivå, med beaktande av den senaste utvecklingen och till genomförandekostnaderna med hänsyn till riskerna och vilken typ av personuppgifter som ska skyddas. Vid bedömningen av riskerna när det gäller datasäkerhet bör man beakta de risker som uppgiftsbehandling medför, såsom förstörelse, förlust eller ändringar genom olyckshändelse eller olagliga handlingar eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, som framför allt kan leda till fysisk, materiell eller immateriell skada. Den personuppgiftsansvarige och personuppgiftsbiträdet bör säkerställa att behandlingen av personuppgifter inte utförs av obehöriga personer.
- (61) En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan för fysiska personer leda till fysisk, materiell eller immateriell skada, såsom förlust av kontrollen över de egna personuppgifterna eller till begränsning av deras rättigheter, diskriminering, identitetsstöld eller identitetsbedrägeri, ekonomisk förlust, obehörigt hävande av pseudonymisering, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, eller till annan betydande ekonomisk eller social nackdel för den berörda fysiska personen. Så snart en personuppgiftsansvarig blir medveten om en personuppgiftsincident bör den personuppgiftsansvarige därför anmäla personuppgiftsincidenten till tillsynsmyndigheten utan onödigt dröjsmål och, om möjligt, inom 72 timmar efter att ha fått kännedom om denna, om inte den personuppgiftsansvarige, i enlighet med ansvarsprincipen, kan visa att det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter. Om anmälan inte kan göras inom 72 timmar bör skälen till fördröjningen åtfölja anmälan och informationen får lämnas i omgångar utan otillbörligt vidare dröjsmål.
- (62) Fysiska personer bör utan onödigt dröjsmål underrättas om personuppgiftsincidenten sannolikt leder till en högre risk för deras rättigheter och friheter så att de kan vidta nödvändiga försiktighetsåtgärder. Underrättelsen bör innehålla en beskrivning av personuppgiftsincidentens art samt rekommendationer till den berörda fysiska personen om hur de potentiella negativa effekterna kan mildras. De registrerade bör underrättas så snart detta rimligtvis är möjligt, i nära samarbete med tillsynsmyndigheten och i enlighet med den vägledning som lämnats av den eller andra relevanta myndigheter. Exempelvis kräver behovet av att mildra en omedelbar skaderisk att de registrerade underrättas omgående medan behovet att vidta lämpliga åtgärder vid fortlöpande eller likartade uppgiftsincidenter kan motivera längre tid för underrättelsen. Om man inte kan undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden, undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder eller skydda allmän säkerhet, nationell säkerhet eller andra personers rättigheter och friheter genom att senarelägga eller begränsa informationen till den berörda fysiska personen om en personuppgiftsincident skulle denna information under exceptionella omständigheter kunna utelämnas.
- (63) Den personuppgiftsansvarige bör utse en person att hjälpa denne att övervaka den interna efterlevnaden av de bestämmelser som antas i enlighet med detta direktiv, förutom om en medlemsstat beslutar att undanta domstolar och andra oberoende rättsliga myndigheter som behandlar personuppgifter inom ramen för sin dömande verksamhet. Denna person kan vara en av den personuppgiftsansvariges medarbetare som fått särskild utbildning inom dataskyddslagstiftning och praxis i fråga om dataskydd för att förvärva sakkunskap på detta område. Den nödvändiga nivån på sakkunskapen bör särskilt fastställas i enlighet med den uppgiftsbehandling som utförs och det skydd som krävs för de personuppgifter som behandlas av den personuppgiftsansvarige. Hans eller hennes uppgift kan utföras på deltid eller heltid. Flera personuppgiftsansvariga kan, med beaktande av organisationsstruktur och storlek, gemensamt utse ett dataskyddsombud, t.ex. vid gemensamma resurser i centralenheter. Denna person kan också utnämnas till olika befattningar inom de berörda personuppgiftsansvarigas struktur. Denna person bör hjälpa den personuppgiftsansvarige och de anställda som behandlar personuppgifter genom att ge information och råd till dem angående efterlevnaden av deras respektive skyldigheter i fråga om dataskydd. Dataskyddsombudet i fråga bör kunna utföra sina uppdrag och uppgifter på ett oberoende sätt i enlighet med medlemsstaternas nationella rätt.
- (64) Medlemsstaterna bör säkerställa att överföringar till ett tredjeland eller en internationell organisation endast får äga rum om detta är nödvändigt för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller för att verkställa straffrättsliga påföljder, inklusive för att skydda mot samt förebygga och förhindra hot mot den

allmänna säkerheten, och den personuppgiftsansvarige i tredjelandet eller den internationella organisationen är en myndighet som är behörig i den mening som avses i detta direktiv. En överföring bör endast utföras av behöriga myndigheter som agerar som personuppgiftsansvariga, utom när personuppgiftsbiträden uttryckligen har getts i uppdrag att göra en överföring för personuppgiftsansvarigas räkning. En sådan överföring kan äga rum när kommissionen har beslutat att skyddsnivån i ett tredjeland eller en internationell organisation är adekvat eller när lämpliga skyddsåtgärder föreligger, eller när undantag för särskilda situationer gäller. Det är viktigt att den skyddsnivå som fysiska personer garanteras inom unionen genom detta direktiv inte undergrävs när personuppgifter överförs från unionen till personuppgiftsansvariga, personuppgiftsbiträden eller andra mottagare i tredjeländer eller internationella organisationer, vilket inbegriper fall av vidare överföring av personuppgifter från tredjelandet eller den internationella organisationen till personuppgiftsansvariga eller personuppgiftsbiträden i samma eller i ett annat tredjeland eller en annan internationell organisation.

- (65) Om personuppgifter överförs från en medlemsstat till tredjeländer eller internationella organisationer bör en sådan överföring i princip ske först efter det att den medlemsstat från vilken uppgifterna insamlades har gett sitt tillstånd till överföringen. För ett effektivt samarbete i fråga om brottsbekämpning krävs att, om ett hot mot en medlemsstats eller ett tredjelandets allmänna säkerhet eller en medlemsstats väsentliga intressen är så överhängande att det är omöjligt att i tid inhämta ett förhandstillstånd, den behöriga myndigheten bör få överföra de relevanta personuppgifterna till det berörda tredjelandet eller internationella organisationen utan sådant förhandstillstånd. Medlemsstaterna bör föreskriva att eventuella särskilda villkor som rör överföringen bör vidarebefordras till tredjeländer eller internationella organisationer. För vidare överföring av personuppgifter bör det krävas förhandstillstånd från den behöriga myndighet som utförde den ursprungliga överföringen. När den behöriga myndighet som utförde den ursprungliga överföringen fattar beslut om en begäran om tillstånd för vidare överföring bör den vederbörligen beakta alla relevanta faktorer, inklusive hur allvarligt brottet är, de särskilda villkor på vilka, och det ändamål för vilket, uppgifterna ursprungligen överfördes, arten och villkoren för verkställandet av den straffrättsliga påföljden, samt nivån på skyddet av personuppgifter i det tredjeland eller den internationella organisation som personuppgifterna vidare överförs till. Den behöriga myndighet som utförde den ursprungliga överföringen bör också ha möjlighet att tillämpa särskilda villkor för vidare överföring. Dessa särskilda villkor kan beskrivas, t.ex. i hanteringskoder.
- (66) Kommissionen bör med verkan för hela unionen kunna fastställa att vissa tredjeländer, ett visst territorium eller en eller flera specificerade sektorer i ett tredjeland eller en internationell organisation kan erbjuda en adekvat dataskyddsnivå, och på så sätt skapa rättssäkerhet och enhetlighet i hela unionen vad gäller dessa tredjeländer eller internationella organisationer som anses erbjuda en sådan skyddsnivå. I dessa fall bör överföringar av personuppgifter till dessa länder kunna ske utan särskilt tillstånd, utom när en annan medlemsstat från vilken uppgifterna insamlades måste ge tillstånd till överföringen.
- (67) I enlighet med de grundläggande värderingar som unionen vilar på, särskilt skyddet av de mänskliga rättigheterna, bör kommissionen i sin bedömning av ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland beakta i vilken omfattning ett visst tredjeland iakttar rättsstatsprincipen, möjligheten till rättslig prövning samt internationella människorättsliga normer och standarder samt landets allmänna lagstiftning och sektorslagstiftning, vilket inbegriper lagstiftning om allmän säkerhet, försvar och nationell säkerhet samt allmän ordning och straffrätt. Vid antagandet av ett beslut om adekvat skyddsnivå avseende ett territorium eller en specificerad sektor i ett tredjeland bör hänsyn tas till tydliga och objektiva kriterier, t.ex. specifik behandling och tillämpningsområdet för tillämpliga rättsliga standarder och gällande lagstiftning i det tredjelandet. Tredjelandet bör erbjuda garantier som säkerställer en tillfredsställande skyddsnivå, som i huvudsak motsvarar den som säkerställs inom unionen, i synnerhet när uppgifter behandlas inom en eller flera specifika sektorer. Tredjelandet bör framför allt säkerställa en effektiv oberoende dataskyddsövervakning samt sörja för mekanismer för samarbete med medlemsstaternas dataskyddsmyndigheter och de registrerade bör tillförsäkras effektiva och verkställbara rättigheter samt effektiva administrativa och rättsliga rättsmedel.
- (68) Utöver de internationella åtaganden som tredjelandet eller den internationella organisationen har ingått bör kommissionen också beakta de skyldigheter som följer av tredjelandets eller den internationella organisationens deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter, samt genomförandet av dessa skyldigheter. Framför allt bör tredjelandets anslutning till Europarådets konvention av den 28 januari 1981 om skydd för fysiska personer vid automatiserad databehandling av personuppgifter och dess tilläggsprotokoll beaktas. Kommissionen bör samråda med Europeiska dataskyddsstyrelsen, inrättad genom förordning

(EU) 2016/679 (nedan kallad *styrelsen*) vid bedömningen av skyddsnivån i tredjeländer eller internationella organisationer. Kommissionen bör också beakta alla relevanta kommissionsbeslut om adekvat skyddsnivå som antagits i enlighet med artikel 45 i förordning (EU) 2016/679.

- (69) Kommissionen bör övervaka hur beslut om skyddsnivå i ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation fungerar. I sina beslut om adekvat skyddsnivå bör kommissionen föreskriva en mekanism för periodisk översyn av hur de fungerar. Denna periodiska översyn bör göras i samråd med tredjelandet eller den internationella organisationen i fråga och bör beakta all relevant utveckling i tredjelandet eller den internationella organisationen.
- (70) Kommissionen bör även kunna konstatera att ett tredjeland eller ett territorium eller en specificerad sektor inom ett tredjeland, eller en internationell organisation, inte längre säkerställer en adekvat dataskyddsnivå. Följaktligen bör överföringar av personuppgifter till det tredjelandet eller den internationella organisationen förbjudas om inte kraven i detta direktiv rörande överföring som är föremål för lämpliga skyddsåtgärder och undantag i särskilda situationer är uppfyllda. Bestämmelser bör fastställas för förfaranden för samråd mellan kommissionen och dessa tredjeländer eller internationella organisationer. Kommissionen bör i god tid informera tredjelandet eller den internationella organisationen om skälen och inleda samråd med tredjelandet eller organisationen för att avhjälpa situationen.
- (71) Överföringar som inte grundar sig på ett sådant beslut om adekvat skyddsnivå bör endast tillåtas om lämpliga skyddsåtgärder garanteras i ett rättsligt bindande instrument, som säkerställer skyddet av personuppgifterna eller om den personuppgiftsansvarige har gjort en bedömning av alla omständigheter kring en uppgiftsöverföring och på grundval av denna bedömning anser att lämpliga skyddsåtgärder föreligger vad avser skyddet av personuppgifter. Sådana rättsligt bindande instrument kan t.ex. vara rättsligt bindande bilaterala avtal som har ingåtts av medlemsstaterna och genomförts inom deras rättsordning och som kan åberopas av registrerade som omfattas av denna och som sörjer för att kraven i fråga om dataskydd uppfylls och att registrerades rättigheter respekteras, inbegripet rätten till en effektiv administrativ eller rättslig prövning. Den personuppgiftsansvarige bör vid bedömningen av alla omständigheter kring uppgiftsöverföringen kunna beakta samarbetsavtal som ingåtts mellan Europol eller Eurojust och tredjeländer, som medger utbyte av personuppgifter. Den personuppgiftsansvarige bör också kunna beakta att överföringen av personuppgifter kommer att omfattas av tystnadsplikt och principen om specificitet, vilket säkerställer att personuppgifterna inte kommer att behandlas i andra syften än för överföringen. Dessutom bör den personuppgiftsansvarige beakta att personuppgifterna inte kommer att användas för att göra framställningar om, meddela eller verkställa dödsstraff eller någon form av grym och omänsklig behandling. Även om dessa villkor kan betraktas som tillräckliga skyddsåtgärder för överföringen av uppgifter bör den personuppgiftsansvarige kunna begära ytterligare skyddsåtgärder.
- (72) Om det inte finns något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder saknas kan en överföring eller en kategori av överföringar endast äga rum i särskilda situationer om överföringen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan person, eller för att skydda den registrerades berättigade intressen om lagstiftningen i den medlemsstat som överför personuppgifterna föreskriver detta, eller för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en medlemsstat eller i ett tredjeland, eller om det är nödvändigt i ett enskilt fall för att förebygga, förhindra, avslöja, utreda eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive för att skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten, eller i ett enskilt fall för att fastslå, göra gällande eller försvara rättsliga anspråk. Dessa undantag bör tolkas restriktivt och bör inte möjliggöra upprepade, omfattande eller strukturella överföringar av personuppgifter eller storskaliga överföringar av uppgifter, utan begränsas till uppgifter som är absolut nödvändiga. Sådana överföringar bör dokumenteras och på begäran göras tillgängliga för tillsynsmyndigheten så att man kan övervaka om överföringen är laglig.
- (73) Medlemsstaternas behöriga myndigheter tillämpar gällande bilaterala eller multilaterala internationella avtal som ingåtts med tredjeländer på området för straffrättsligt samarbete och polissamarbete för utbyte av relevant information för att de ska kunna fullgöra de uppgifter som de anförtratts enligt lag. Detta sker i princip genom eller åtminstone i samarbete med tredjeländernas berörda myndigheter, i vissa fall även i avsaknad av ett bilateralt eller multilateralt internationellt avtal. I specifika enskilda fall är emellertid de ordinarie förfaranden som kräver kontakt med myndigheten i tredjelandet ineffektiva eller olämpliga, framför allt för att överföringen inte skulle kunna utföras i tid eller för att myndigheten i tredjelandet inte respekterar rättsstatsprincipen eller internationella människorättsliga normer och standarder, så att medlemsstaternas behöriga myndigheter skulle kunna besluta att överföra personuppgifterna direkt till de mottagare som är etablerade i dessa tredjeländer. Detta kan till exempel vara fallet om det finns ett akut behov av att överföra personuppgifter för att rädda livet på en person som riskerar att utsättas för ett brott eller för att förhindra en överhängande fara för brottslighet, inbegripet terrorism. Även om denna överföring mellan behöriga myndigheter och mottagare som är etablerade i tredjeländer endast

äger rum i särskilda enskilda fall bör det i detta direktiv föreskrivas villkor för att reglera sådana fall. Dessa bestämmelser bör inte betraktas som undantag från något befintligt bilateralt eller multilateralt internationellt avtal på området för straffrättsligt samarbete och polissamarbete. Dessa bestämmelser bör vara tillämpliga utöver övriga bestämmelser i detta direktiv, särskilt bestämmelserna om när personuppgifter får behandlas och bestämmelserna i kapitel V.

- (74) När personuppgifter förs över gränserna kan detta öka risken för att fysiska personer inte ska kunna utöva sina dataskyddsrättigheter för att skydda sig mot olaglig användning eller olagligt utlämnande av dessa uppgifter. Samtidigt kan tillsynsmyndigheter finna att de inte är i stånd att handlägga klagomål eller genomföra utredningar avseende verksamheter utanför sina egna gränser. Deras strävan att samarbeta i ett gränsöverskridande sammanhang kan också försvåras på grund av otillräckliga preventiva eller korrigerande befogenheter och oenhetliga rättsliga regelverk. Närmare samarbete mellan tillsynsmyndigheter bör därför främjas för att hjälpa dem att utbyta information med sina utländska motparter.
- (75) För att skydda fysiska personer med avseende på behandling av personuppgifter är det av avgörande betydelse att medlemsstaterna inrättar tillsynsmyndigheter som kan utföra sitt uppdrag fullständigt oberoende. Tillsynsmyndigheterna bör övervaka tillämpningen av detta direktiv och bör bidra till enhetlig tillämpning av dessa i hela unionen, för att skydda fysiska personer när deras personuppgifter behandlas. För detta ändamål bör tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen.
- (76) Medlemsstaterna får anförtro en tillsynsmyndighet som de redan har inrättat i enlighet med förordning (EU) 2016/679 ansvaret för de uppgifter som ska utföras av de nationella tillsynsmyndigheter som ska inrättas i enlighet med detta direktiv.
- (77) Medlemsstaterna bör kunna inrätta mer än en tillsynsmyndighet för att återspegla sin konstitutionella, organisatoriska och administrativa struktur. Varje tillsynsmyndighet bör tilldelas de ekonomiska och personella resurser och lokalutrymmen samt den infrastruktur som krävs för att den effektivt ska kunna utföra sina uppgifter, däribland de uppgifter som är knutna till ömsesidigt bistånd och samarbete med övriga tillsynsmyndigheter i hela unionen. Varje tillsynsmyndighet bör ha en separat offentlig årlig budget, som kan ingå i den övergripande statsbudgeten eller nationella budgeten.
- (78) Tillsynsmyndigheterna bör vara föremål för oberoende kontroll- eller övervakningsmekanismer i fråga om sina utgifter, förutsatt att denna finansiella kontroll inte påverkar deras oberoende.
- (79) De allmänna villkoren för tillsynsmyndighetens ledamot eller ledamöter bör fastställas i medlemsstaternas nationella rätt och bör i synnerhet föreskriva att de ska utnämnas antingen av den berörda medlemsstatens parlament eller dess regering eller dess statschef på grundval av ett förslag från regeringen eller en minister eller parlamentet eller dess kammare eller av ett oberoende organ som enligt medlemsstaternas nationella rätt har anförtrotts utnämningen genom ett öppet förfarande. I syfte att säkerställa tillsynsmyndighetens oberoende bör ledamoten eller ledamöterna handla med integritet, bör avstå från alla handlingar som står i strid med deras tjänsteutövning och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet som står i strid med deras uppdrag. För att säkerställa tillsynsmyndighetens oberoende bör personalurvalet göras av tillsynsmyndigheten, och kunna innefatta ett ingripande från ett oberoende organ som enligt medlemsstaternas nationella rätt har anförtrotts uppgiften.
- (80) Detta direktiv är visserligen tillämpligt på nationella domstolars och andra rättsliga myndigheters verksamheter, men tillsynsmyndigheterna bör inte ha behörighet att övervaka behandling av personuppgifter inom ramen för domstolars dömande verksamhet. Syftet är att garantera domarnas oberoende när de utför sina rättsliga uppgifter. Detta undantag bör vara inskränkt till rättsliga verksamheter i domstolsmål och inte vara tillämpligt på övriga verksamheter där domare i enlighet med medlemsstaternas nationella rätt kan medverka. Medlemsstaterna bör också kunna föreskriva att tillsynsmyndigheten inte ska vara behörig att övervaka andra oberoende rättsliga myndigheter som behandlar personuppgifter inom ramen för sin rättsliga verksamhet, exempelvis allmänna åklagarmyndigheter. Under alla omständigheter är domstolarnas och andra oberoende rättsliga myndigheters efterlevnad av bestämmelserna i detta direktiv alltid föremål för en oberoende kontroll i enlighet med artikel 8.3 i stadgan.

- (81) Tillsynsmyndigheterna bör hantera klagomål som anförts av registrerade och utreda ärendena i fråga eller överföra dem till den behöriga övervakande myndigheten. Utredningen av ett klagomål bör, med förbehåll för eventuell domstolsprövning, ske i den utsträckning som är lämplig i det enskilda fallet. Tillsynsmyndigheten bör i rimlig tid informera den registrerade om hur arbetet med klagomålet fortskrider och vad resultatet blir. Om ärendet kräver ytterligare utredning eller samordning med en annan tillsynsmyndighet bör den registrerade underrättas även om detta.
- (82) För att man ska kunna övervaka efterlevnaden av och verkställa detta direktiv på ett effektivt, tillförlitligt och enhetligt sätt i hela unionen enligt EUF-fördraget, i enlighet med den tolkning som domstolen gjort, bör tillsynsmyndigheterna i alla medlemsstater ha samma uppgifter och effektiva befogenheter, bl.a. undersökningsbefogenheter, korrigerande befogenheter och rådgivande befogenheter, som utgör nödvändiga medel för utförandet av deras uppgifter. Emellertid bör deras befogenheter inte inkräkta på särskilda regler för straffrättsliga förfaranden, inbegripet utredning och lagföring av brott, eller domstolsväsendets oberoende. Utan att det påverkar åklagarmyndigheternas befogenheter enligt medlemsstaternas nationella rätt bör tillsynsmyndigheterna också ha befogenhet att upplysa de rättsliga myndigheterna om överträdelse av detta direktiv eller delta i rättsliga förfaranden. Tillsynsmyndigheternas befogenheter bör utövas i överensstämmelse med lämpliga rättssäkerhetsgarantier som fastställs i unionsrätten och i medlemsstaternas nationella rätt samt opartiskt, korrekt och inom rimlig tid. Framför allt bör varje åtgärd vara lämplig, nödvändig och proportionell för att säkerställa efterlevnaden av detta direktiv, med beaktande av omständigheterna i varje enskilt fall, samt respektera varje persons rätt att bli hörd innan några enskilda åtgärder som påverkar den berörda personen negativt vidtas, och utformas så att onödiga kostnader och alltför stora olägenheter för denne undviks. Undersökningsbefogenheten när det gäller tillträde till lokaler bör utövas i enlighet med särskilda krav i medlemsstaternas nationella rätt, såsom kravet på att inhämta förhandstillstånd från rättsliga myndigheter. Antagande av ett rättsligt bindande beslut bör bli föremål för domstolsprövning i den medlemsstat där den tillsynsmyndighet som antog beslutet är belägen.
- (83) Tillsynsmyndigheterna bör bistå varandra när de utför sina uppgifter och ge ömsesidigt bistånd för att säkerställa att de bestämmelser som antas i enlighet med detta direktiv efterlevs och tillämpas på ett enhetligt sätt.
- (84) Styrelsen bör bidra till detta direktivs enhetliga tillämpning i hela unionen, bl.a. genom att lämna råd till kommissionen och främja samarbetet mellan tillsynsmyndigheterna i hela unionen.
- (85) Alla registrerade bör ha rätt att lämna in ett klagomål till en enda tillsynsmyndighet och till ett effektivt rättsmedel i enlighet med artikel 47 i stadgan, om den registrerade anser att hans eller hennes rättigheter enligt de bestämmelser som antas i enlighet med detta direktiv har kränkts eller om tillsynsmyndigheten inte reagerar på ett klagomål, helt eller delvis avslår eller avvisar ett klagomål eller inte agerar när så är nödvändigt för att skydda den registrerades rättigheter. Utredningen av ett klagomål bör, med förbehåll för eventuell domstolsprövning, ske i den utsträckning som är lämplig i det enskilda fallet. Den behöriga tillsynsmyndigheten bör i rimlig tid informera den registrerade om hur arbetet med klagomålet fortskrider och vad resultatet blir. Om ärendet kräver ytterligare utredning eller samordning med en annan tillsynsmyndighet bör den registrerade underrättas även om detta. För att förenkla inlämnandet av klagomål bör varje tillsynsmyndighet vidta åtgärder, såsom att tillhandahålla ett formulär för inlämnande av klagomål som även kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.
- (86) Varje fysisk eller juridisk person bör ha rätt till ett effektivt rättsmedel vid behörig nationell domstol mot en tillsynsmyndighets beslut som har rättsliga följder för denna person. Ett sådant beslut avser särskilt tillsynsmyndighetens utövande av utrednings-, korrigerings- och godkännandebefogenheter eller avvisande av eller avslag på klagomål. Denna rätt inbegriper dock inte tillsynsmyndigheters övriga åtgärder som inte är rättsligt bindande, såsom yttranden som avgetts eller rådgivning som tillhandahållits av tillsynsmyndigheten. Talan mot en tillsynsmyndighet bör väckas vid domstol i den medlemsstat där tillsynsmyndigheten är etablerad och bör prövas i enlighet med den nationella rätten i den medlemsstaten. Dessa domstolar bör ha fullständig behörighet, vilket bör omfatta behörighet att rättsligt eller faktiskt pröva alla frågor som rör de tvister som anhängiggjorts vid dem.
- (87) Om en registrerad anser att hans eller hennes rättigheter enligt detta direktiv har kränkts bör han eller hon ha rätt att ge ett organ som syftar till att skydda registrerades rättigheter och intressen vad gäller skyddet av deras

personuppgifter, och som inrättats i enlighet med den nationella rätten i en medlemsstat, i uppdrag att på hans eller hennes vägnar lämna in ett klagomål till en tillsynsmyndighet och utöva rätten till rättsmedel. De registrerades rätt att bli företrädare bör inte påverka medlemsstatens nationella processrätt enligt vilken det kan vara obligatoriskt att registrerade företrädare inför nationell domstol av en advokat enligt definitionen i rådets direktiv 77/249/EEG ⁽¹⁾.

- (88) Personer som lider skada till följd av behandling som står i strid med de bestämmelser som antas i enlighet med detta direktiv bör få ersättning av den personuppgiftsansvarige eller av någon annan myndighet som är behörig enligt medlemsstaternas nationella rätt. Begreppet *skada* bör tolkas brett mot bakgrund av domstolens rättspraxis och på ett sätt som fullt ut återspeglar detta direktivs mål. Detta påverkar inte skadeståndsanspråk till följd av överträdelser av andra bestämmelser i unionsrätten eller i medlemsstaternas nationella rätt. Vid hänvisning till behandling som är olaglig eller står i strid med de bestämmelser som antas i enlighet med detta direktiv omfattas även behandling som inte är i överensstämmelse med de genomförandeakter som antagits i enlighet med detta direktiv. Registrerade bör få full och effektiv ersättning för den skada de lidit.
- (89) Om någon fysisk eller juridisk person överträder detta direktiv bör detta leda till sanktioner, oavsett om personen i fråga omfattas av privaträtt eller offentlig rätt. Medlemsstaterna bör säkerställa att sanktioner är effektiva, proportionella och avskräckande och bör vidta alla åtgärder som krävs för att sanktionerna ska verkställas.
- (90) För att säkerställa enhetliga villkor för genomförandet av detta direktiv bör kommissionen tilldelas genomförande-befogenheter vad gäller adekvata skyddsnivåer i ett tredjeland, ett territorium eller en specificerad sektor inom ett tredjeland eller en internationell organisation och för format och förfaranden för ömsesidigt bistånd samt tillvägagångssätten för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ⁽²⁾.
- (91) Mot bakgrund av att dessa rättsakter har allmän räckvidd bör granskningsförfarandet användas vid antagandet av genomförandeakter om adekvata skyddsnivåer i ett tredjeland, ett territorium eller en specificerad sektor inom detta tredjeland eller en internationell organisation och om format och förfaranden för ömsesidigt bistånd samt tillvägagångssätten för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen.
- (92) Kommissionen bör när tvingande skäl till skyndsamhet föreligger i vederbörligen motiverade fall anta omedelbart tillämpliga genomförandeakter avseende ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation där en adekvat skyddsnivå inte längre kan säkerställas.
- (93) Eftersom målen för detta direktiv, nämligen att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, och för att säkerställa ett fritt utbyte av personuppgifter mellan behöriga myndigheter inom unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare på grund av åtgärdens omfattning eller verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i EU-fördraget. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.
- (94) Särskilda bestämmelser i unionsakter på området för straffrättsligt samarbete och polissamarbete som antagits före dagen för antagandet av detta direktiv, och som reglerar behandlingen av personuppgifter mellan medlemsstaterna eller tillträdet för utsedda myndigheter i medlemsstaterna till informationssystem som inrättats i

⁽¹⁾ Rådets direktiv 77/249/EEG av den 22 mars 1977 om underlättande för advokater att effektivt begagna sig av friheten att tillhandahålla tjänster (EGT L 78, 26.3.1977, s. 17).

⁽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).

enlighet med fördragen, bör kvarstå oförändrade, till exempel de särskilda bestämmelser om skydd av personuppgifter som tillämpas i enlighet med rådets beslut 2008/615/RIF ⁽¹⁾, eller artikel 23 i konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater ⁽²⁾. Eftersom artikel 8 i stadgan och artikel 16 i EUF-fördraget kräver att den grundläggande rätten till skydd av personuppgifter bör säkerställas på ett enhetligt sätt i hela unionen bör kommissionen utvärdera situationen vad gäller förhållandet mellan detta direktiv och rättsakter, antagna före dagen för antagandet av detta direktiv, som reglerar behandling av personuppgifter mellan medlemsstaterna eller tillträde för utsedda myndigheter i medlemsstater till informationssystem som inrättats i enlighet med fördragen, i syfte att bedöma om dessa särskilda bestämmelser behöver anpassas till detta direktiv. Vid behov bör kommissionen lägga fram förslag i syfte att säkerställa enhetliga rättsregler angående behandlingen av personuppgifter.

- (95) För att säkerställa ett övergripande och enhetligt skydd av personuppgifter i unionen bör internationella avtal som medlemsstaterna ingått före dagen för detta direktivs ikraftträdande, och som överensstämmer med relevant unionsrätt som var tillämplig före den dagen, fortsätta att gälla till dess att de ändras, ersätts eller upphävs.
- (96) Medlemsstaterna bör medges en period på högst två år från dagen för ikraftträdandet av detta direktiv för att införliva det. Behandling som redan pågår den dagen bör bringas i överensstämmelse med detta direktiv inom en period av två år från det att detta direktiv träder i kraft. I fall där sådan behandling överensstämmer med unionsrätt som var tillämplig före dagen för ikraftträdandet av detta direktiv bör dock inte kraven i detta direktiv rörande förhandssamråd med tillsynsmyndigheten gälla för behandling som redan pågick vid den tidpunkten, eftersom dessa krav, p.g.a. sin natur, är sådana att de ska uppfyllas före själva behandlingen. Om medlemsstaterna tillämpar den längre genomförandeperioden som löper ut sju år efter detta direktivs ikraftträdande för fullgörandet av loggningskyldigheterna för automatiserade behandlingssystem som inrättats före den dagen bör den personuppgiftsansvarige eller personuppgiftsbiträdet ha infört effektiva metoder, t.ex. loggar eller andra typer av register, för att visa att behandlingen av uppgifterna är laglig, möjliggöra egenkontroll samt säkerställa dataintegritet och datasäkerhet.
- (97) Detta direktiv påverkar inte bestämmelserna om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi i Europaparlamentets och rådets direktiv 2011/93/EU ⁽³⁾.
- (98) Rambeslut 2008/977/RIF bör därför upphävas.
- (99) I enlighet med artikel 6a i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till EU-fördraget och EUF-fördraget, är Förenade kungariket och Irland inte bundna av de bestämmelser i detta direktiv som avser medlemsstaternas behandling av personuppgifter när de bedriver verksamhet som omfattas av avdelning V kapitel 4 eller 5 i tredje delen av EUF-fördraget i det fall då Förenade kungariket och Irland inte är bundna av bestämmelserna om formerna för straffrättsligt samarbete eller polissamarbete inom ramen för vilka de bestämmelser måste iakttas som fastställs på grundval av artikel 16 i EUF-fördraget.
- (100) I enlighet med artiklarna 2 och 2a i protokoll nr 22 om Danmarks ställning, fogat till EU-fördraget och EUF-fördraget, är Danmark inte bundet av reglerna i detta direktiv och omfattas inte av den tillämpning av regler som avser medlemsstaternas behandling av personuppgifter när dessa utövar verksamhet som omfattas av tillämpningsområdet för kapitlen 4 och 5 i avdelning V i tredje delen i EUF-fördraget. Eftersom detta direktiv bygger på av Schengenregelverket, som omfattas av avdelning V i tredje delen av EUF-fördraget, ska Danmark i enlighet med artikel 4 i protokollet inom en tid av sex månader efter antagandet av detta direktiv besluta huruvida landet ska genomföra det i sin nationella lagstiftning.
- (101) När det gäller Island och Norge utgör detta direktiv en vidareutveckling av bestämmelserna i Schengenregelverket i enlighet med avtalet mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ⁽⁴⁾.

⁽¹⁾ Rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet (EUT L 210, 6.8.2008, s. 1).

⁽²⁾ Rådets akt av den 29 maj 2000 om att i enlighet med artikel 34 i Fördraget om Europeiska unionen upprätta konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (EGT C 197, 12.7.2000, s. 1).

⁽³⁾ Europaparlamentets och rådets direktiv 2011/93/EU av den 13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om ersättande av rådets rambeslut 2004/68/RIF (EUT L 335, 17.12.2011, s. 1).

⁽⁴⁾ EGT L 176, 10.7.1999, s. 36.

- (102) När det gäller Schweiz utgör detta direktiv, i enlighet med avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket, en utveckling av bestämmelserna i Schengenregelverket ⁽¹⁾.
- (103) När det gäller Liechtenstein utgör detta direktiv en vidareutveckling av bestämmelserna i Schengenregelverket i enlighet med protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Liechtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket ⁽²⁾.
- (104) Detta direktiv respekterar de grundläggande rättigheterna och iakttar de principer som erkänns i stadgan som erkänns i EUF-fördraget, särskilt rätten till respekt för privatlivet och familjelivet, rätten till skydd av personuppgifter, rätt till ett effektivt rättsmedel och till en opartisk domstol. De inskränkningar som gjorts av dessa rättigheter överensstämmer med artikel 52.1 i stadgan eftersom de är nödvändiga för att uppnå av unionen erkända mål av allmänt intresse eller för att skydda andras rättigheter och friheter.
- (105) I enlighet med den gemensamma politiska förklaringen av den 28 september 2011 från medlemsstaterna och kommissionen om förklarande dokument, har medlemsstaterna åtagit sig att, i de fall detta är berättigat, låta anmälan av införlivandeåtgärder åtföljas av ett eller flera dokument som förklarar förhållandet mellan de olika delarna i direktivet och motsvarande delar i de nationella införlivandeåtgärderna. Med avseende på detta direktiv anser lagstiftaren att översändandet av sådana dokument är berättigat.
- (106) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001 och avgav ett yttrande den 7 mars 2012 ⁽³⁾.
- (107) Detta direktiv bör inte hindra medlemsstaterna från att i nationell straffprocesslagstiftning genomföra bestämmelser om registrerades utövande av sina rättigheter vad gäller information, tillgång till och rättelse eller radering av personuppgifter och begränsning av behandling i samband med straffrättsliga förfaranden samt eventuella begränsningar av dessa rättigheter.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Syfte och mål

1. I detta direktiv fastställs bestämmelser om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.
2. Enligt detta direktiv ska medlemsstaterna
 - a) skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, och
 - b) säkerställa att behöriga myndigheters utbyte av personuppgifter inom unionen, när sådant utbyte krävs enligt unionsrätten eller medlemsstaternas nationella rätt, varken begränsas eller förbjuds av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter.

⁽¹⁾ EUT L 53, 27.2.2008, s. 52.

⁽²⁾ EUT L 160, 18.6.2011, s. 21.

⁽³⁾ EGT C 192, 30.6.2012, s. 7.

3. Detta direktiv ska inte hindra medlemsstaterna från att föreskriva starkare skyddsåtgärder än de som fastställs i detta direktiv för skyddet av den registrerades rättigheter och friheter med avseende på behöriga myndigheters behandling av personuppgifter.

Artikel 2

Tillämpningsområde

1. Detta direktiv ska tillämpas på behandling av personuppgifter som utförs av behöriga myndigheter för de ändamål som anges i artikel 1.1.
2. Detta direktiv ska tillämpas på behandling av personuppgifter som helt eller delvis företas på automatiserad väg samt på annan behandling än automatiserad behandling av personuppgifter som ingår i eller kommer att ingå i ett register.
3. Detta direktiv tillämpas inte på behandling av personuppgifter
 - a) som utgör ett led i en verksamhet som inte omfattas av unionsrätten,
 - b) som utförs av unionens institutioner, organ och byråer.

Artikel 3

Definitioner

I detta direktiv avses med

1. *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar enskild person (nedan kallad *en registrerad*), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras, särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller onlineidentifikatorer, eller till en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,
2. *behandling*: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,
3. *begränsning av behandling*: markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden,
4. *profilerings*: varje form av automatiserad behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga aspekter rörande denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar,
5. *pseudonymisering*: behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person,
6. *register*: en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,
7. *behörig myndighet*:
 - a) en offentlig myndighet som har behörighet att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga hot mot den allmänna säkerheten, eller
 - b) annat organ eller annan enhet som genom medlemsstaternas nationella rätt har anförtratts myndighetsutövning för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga och förhindra hot mot den allmänna säkerheten,

8. *personuppgiftsansvarig*: en behörig myndighet som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivs i unionsrätten eller medlemsstaternas nationella rätt,
9. *personuppgiftsbiträde*: en fysisk eller juridisk person, myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,
10. *mottagare*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte; offentliga myndigheter som kan komma att motta personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare; offentliga myndigheters behandling av dessa uppgifter ska vara förenlig med tillämpliga bestämmelser för dataskydd beroende på behandlingens syfte,
11. *personuppgiftsincident*: en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,
12. *genetiska uppgifter*: alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om denna fysiska persons fysiologi eller hälsa och vilka framför allt härrör från en analys av ett biologiskt prov från den fysiska personen i fråga,
13. *biometrisk uppgift*: personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar unik identifiering av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter,
14. *uppgifter om hälsa*: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus,
15. *tillsynsmyndighet*: en oberoende offentlig myndighet som är utsedd av en medlemsstat i enlighet med artikel 41,
16. *internationell organisation*: en organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera länder,

KAPITEL II

Principer

Artikel 4

Principer för behandling av personuppgifter

1. Medlemsstaterna ska föreskriva att personuppgifter ska
 - a) behandlas på ett lagligt och korrekt sätt,
 - b) samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte behandlas på ett sätt som står i strid med dessa ändamål,
 - c) vara adekvata, relevanta och inte för omfattande i förhållande till de syften för vilka de behandlas,
 - d) vara korrekta och, om nödvändigt, uppdaterade; alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål,
 - e) inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas,
 - f) behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

2. Behandling som utförs av samma eller en annan personuppgiftsansvarig för något annat ändamål som anges i artikel 1.1 än det för vilket personuppgifterna samlas in ska tillåtas om
 - a) den personuppgiftsansvarige i enlighet med unionsrätten eller medlemsstaternas nationella rätt är bemyndigad att behandla sådana personuppgifter för ett sådant ändamål, och
 - b) behandlingen är nödvändig och står i proportion till detta andra ändamål i enlighet med unionsrätten eller medlemsstaternas nationella rätt.
3. Behandling som utförs av samma eller en annan personuppgiftsansvarig kan inbegripa arkivändamål av allmänt intresse och vetenskaplig, statistisk eller historisk användning för de ändamål som anges i artikel 1.1 under förutsättning att det finns lämpliga skyddsåtgärder för de registrerades rättigheter och friheter.
4. Den personuppgiftsansvarige ska ansvara för, och kunna visa efterlevnad av, punkterna 1, 2 och 3.

Artikel 5

Tidsgränser för lagring och översyn

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

Artikel 6

Åtskillnad mellan olika kategorier av registrerade

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, i tillämpliga fall och så långt det är möjligt, ska göra en klar åtskillnad mellan personuppgifter som rör olika kategorier av registrerade, såsom

- a) personer avseende vilka det finns tungt vägande skäl att anta att de har begått eller är på väg att begå ett brott,
- b) personer som dömts för brott,
- c) brottsoffer eller personer avseende vilka det finns vissa omständigheter som ger anledning att anta att de kan vara brottsoffer, och
- d) andra som berörs av ett brott, såsom personer som kan komma att kallas att vittna i samband med brottsutredningar eller senare straffrättsliga förfaranden, personer som kan ge information om brott eller personer med kontakter med eller band till någon av de personer som avses i a och b.

Artikel 7

Åtskillnad mellan personuppgifter och kontroll av kvaliteten på personuppgifterna

1. Medlemsstaterna ska föreskriva att personuppgifter som grundar sig på fakta så långt det är möjligt ska åtskiljas från personuppgifter som grundar sig på personliga bedömningar.
2. Medlemsstaterna ska föreskriva att de behöriga myndigheterna ska vidta alla rimliga åtgärder för att se till att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. Varje behörig myndighet ska därför i den mån det är praktiskt möjligt kontrollera kvaliteten på personuppgifterna innan dessa överförs eller görs tillgängliga. Vid all överföring av personuppgifter ska, så långt det är möjligt, sådan nödvändig information läggas till som gör det möjligt för den mottagande behöriga myndigheten att bedöma i vilken grad personuppgifterna är korrekta, fullständiga och tillförlitliga samt i vilken utsträckning de är aktuella.
3. Om det visar sig att felaktiga personuppgifter har överförts eller att personuppgifter olagligen har överförts ska mottagaren omedelbart underrättas om detta. I sådana fall ska personuppgifterna rättas eller raderas eller behandlingen begränsas i enlighet med artikel 16.

*Artikel 8***Laglig behandling av personuppgifter**

1. Medlemsstaterna ska föreskriva att behandling ska vara laglig endast om och i den mån behandlingen är nödvändig för att utföra en uppgift som utförs av en behörig myndighet för de ändamål som anges i artikel 1.1 och som sker på grundval av unionsrätt eller medlemsstaternas nationella rätt.
2. Medlemsstaternas nationella rätt som reglerar behandling inom tillämpningsområdet för detta direktiv ska åtminstone specificera syftet med behandlingen, vilka personuppgifter som ska behandlas och behandlingens ändamål.

*Artikel 9***Särskilda villkor för uppgiftsbehandling**

1. Personuppgifter som samlas in av behöriga myndigheter för de ändamål som anges i artikel 1.1. ska inte behandlas för andra ändamål än de som anges i artikel 1.1 såvida inte sådan behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt. När personuppgifter behandlas för andra ändamål ska förordning (EU) 2016/679 tillämpas, såvida inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten.
2. Om de behöriga myndigheterna enligt medlemsstaternas nationella rätt anförtros utförandet av andra uppgifter än de som utförs för de ändamål som anges i artikel 1.1, ska förordning (EU) 2016/679 vara tillämplig på behandlingen för dessa ändamål, inklusive för arkivändamål av allmänt intresse, för historiska eller vetenskapliga forskningsändamål eller för statistiska ändamål, såvida inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten.
3. Om den unionsrätt eller nationella rätt som är tillämplig på den överförande behöriga myndigheten fastställer särskilda villkor för behandling, ska medlemsstaten föreskriva att den överförande behöriga myndigheten ska informera mottagaren om dessa särskilda villkor och om kravet att respektera dem.
4. Medlemsstaterna ska föreskriva att den överförande behöriga myndigheten inte ska tillämpa villkor enligt punkt 3 på mottagare i andra medlemsstater eller på byråer och organ som inrättats i enlighet med avdelning V kapitlen 4 och 5 i EUF-fördraget, med undantag för de villkor som är tillämpliga på motsvarande överföringar av uppgifter inom den överförande behöriga myndighetens medlemsstat.

*Artikel 10***Behandling av särskilda kategorier av personuppgifter**

Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, samt behandling av genetiska uppgifter, biometriska uppgifter för att unikt identifiera en fysisk person eller uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara tillåten endast om det är absolut nödvändigt och under förutsättning att det finns lämpliga skyddsåtgärder för den registrerades rättigheter och friheter och endast

- a) om behandlingen är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt,
- b) för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan fysisk person, eller
- c) om behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

*Artikel 11***Automatiserat individuellt beslutsfattande**

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

2. Beslut som avses i punkt 1 i den här artikeln får inte grundas på de särskilda kategorier av personuppgifter som avses i artikel 10, såvida inte lämpliga åtgärder för att skydda den registrerades rättigheter och friheter samt berättigade intressen har vidtagits.

3. Profilerings som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter enligt artikel 10 ska förbjudas i enlighet med unionsrätten.

KAPITEL III

Den registrerades rättigheter

Artikel 12

Information om och villkor för utövandet av den registrerades rättigheter

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska vidta rimliga åtgärder för att tillhandahålla den registrerade all information som avses i artikel 13 och alla meddelanden enligt artiklarna 11, 14–18 och 31 som avser behandling i en koncis, begriplig och lättillgänglig form och på ett klart och tydligt språk. Informationen ska tillhandahållas på lämpligt sätt, t.ex. elektroniskt. Som en allmän regel ska den personuppgiftsansvarige tillhandahålla informationen i samma format som begäran.

2. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underlätta utövandet av den registrerades rättigheter enligt artiklarna 11 och 14–18.

3. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige utan onödigt dröjsmål skriftligen ska informera den registrerade om uppföljningen av hans eller hennes begäran.

4. Medlemsstaterna ska föreskriva att den information som tillhandahålls enligt artikel 13 och alla meddelanden eller åtgärder som vidtas enligt artiklarna 11, 14–18 och 31 ska tillhandahållas kostnadsfritt. Om en registrerads begäran är uppenbart ogrundad eller orimlig, särskilt på grund av att den är repetitiv, får den personuppgiftsansvarige antingen

a) ta ut en rimlig avgift med beaktande av de administrativa kostnaderna för tillhandahållandet av informationen eller meddelandet eller vidtagandet av den åtgärd som begärs, eller

b) vägra att tillmötesgå begäran.

Den personuppgiftsansvarige ska visa att begäran är uppenbart ogrundad eller orimlig.

5. Om den personuppgiftsansvarige har rimliga skäl att betvivla identiteten hos den fysiska person som lämnar in en begäran enligt artiklarna 14 eller 16, får den personuppgiftsansvarige begära att ytterligare information som är nödvändig för att bekräfta den registrerades identitet ska tillhandahållas.

Artikel 13

Information som ska göras tillgänglig för eller lämnas till den registrerade

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska göra åtminstone följande information tillgänglig för den registrerade:

a) Den personuppgiftsansvariges identitet och kontaktuppgifter.

b) Dataskyddsombudets kontaktuppgifter, i tillämpliga fall.

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

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

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

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

a) Behandlingens rättsliga grund.

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

- c) I tillämpliga fall, kategorierna av mottagare av personuppgifterna, inbegripet i tredjeländer eller internationella organisationer.
 - d) Vid behov ytterligare information, i synnerhet om personuppgifterna samlas in utan den registrerades vetskap.
3. Medlemsstaterna får anta lagstiftningsåtgärder som gör att informationen till den registrerade enligt punkt 2 senareläggs, begränsas eller utelämnas, i den utsträckning och så länge som en sådan åtgärd är nödvändig och proportionell i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att
- a) undvika att hindra officiella eller rättsliga utredningar, undersökningar eller förfaranden,
 - b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,
 - c) skydda den allmänna säkerheten,
 - d) skydda den nationella säkerheten,
 - e) skydda andra personers rättigheter och friheter.
4. Medlemsstaterna får anta lagstiftningsåtgärder för att fastställa kategorier av behandling som helt eller delvis kan omfattas av något av leden i punkt 3.

Artikel 14

Den registrerades rätt till tillgång till personuppgifter

Med förbehåll för artikel 15 ska medlemsstaterna föreskriva att den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse av huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna och följande information:

- a) Ändamålen med behandlingen och dess rättsliga grund.
- b) De kategorier av personuppgifter som behandlingen gäller.
- c) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats ut, särskilt mottagare i tredjeländer eller internationella organisationer.
- d) Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om det inte är möjligt, de kriterier som används för att fastställa denna period.
- e) Rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifter eller begränsning av behandling av personuppgifter som rör den registrerade.
- f) Rätten att lämna in klagomål till tillsynsmyndigheten samt tillsynsmyndighetens kontaktuppgifter.
- g) Information om vilka personuppgifter som håller på att behandlas och all tillgänglig information om varifrån dessa uppgifter härstammar.

Artikel 15

Begränsningar av rätten till tillgång

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

- a) undvika att hindra officiella eller rättsliga utredningar, förundersökningar eller förfaranden,
- b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,
- c) skydda den allmänna säkerheten,

- d) skydda den nationella säkerheten,
 - e) skydda andra personers rättigheter och friheter.
2. Medlemsstaterna får anta lagstiftningsåtgärder för att fastställa kategorier av behandling som helt eller delvis kan omfattas av undantagen i punkt 1 a–e.
3. I de fall som avses i punkterna 1 och 2 ska medlemsstaterna föreskriva att den personuppgiftsansvarige utan onödigt dröjsmål ska informera den registrerade skriftligen om varje vägran eller begränsning av tillgång och om skälen för vägran eller begränsningen. Denna information kan utelämnas om tillhandahållandet skulle undergräva ett ändamål enligt punkt 1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underrätta den registrerade om möjligheten att lämna in ett klagomål till en tillsynsmyndighet eller begära rättslig prövning.
4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska dokumentera de sakliga och rättsliga grunderna för beslutet. Denna information ska göras tillgänglig för tillsynsmyndigheterna.

Artikel 16

Rätt till rättelse eller radering av personuppgifter och begränsning av behandling

1. Medlemsstaterna ska föreskriva att den registrerade ska ha rätt att utan onödigt dröjsmål av den personuppgiftsansvarige få felaktiga personuppgifter som rör honom eller henne rättade. Med beaktande av ändamålet med behandlingen ska medlemsstaterna föreskriva att den registrerade ska ha rätt att få ofullständiga personuppgifter kompletterade, inbegripet genom att tillhandahålla en kompletterande inlägga.
2. Medlemsstaterna ska kräva att den personuppgiftsansvarige utan onödigt dröjsmål ska radera personuppgifter och ge den registrerade rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få till stånd radering av personuppgifter som rör honom eller henne om behandlingen står i strid med de bestämmelser som antas enligt artiklarna 4, 8 och 10 eller om personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
3. I stället för radering ska den personuppgiftsansvarige begränsa behandling om
- a) den registrerade bestrider personuppgifternas korrekthet och korrektheten inte kan fastställas, eller
 - b) personuppgifterna måste sparas som bevisning.

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

4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige underrättar den registrerade skriftligen om eventuell vägran att rätta, radera eller begränsa behandlingen och om skälen till vägran. Medlemsstaterna får anta lagstiftningsåtgärder som helt eller delvis begränsar skyldigheten att tillhandahålla sådan information i den utsträckning som en sådan begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att
- a) undvika att hindra offentliga eller rättsliga utredningar, undersökningar eller förfaranden,
 - b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,
 - c) skydda den allmänna säkerheten,
 - d) skydda den nationella säkerheten,
 - e) skydda andra personers rättigheter och friheter.

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underrätta den registrerade om möjligheterna att lämna in ett klagomål till en tillsynsmyndighet eller begära rättslig prövning.

5. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska meddela varje rättelse av oriktiga personuppgifter till den behöriga myndighet från vilken de oriktiga personuppgifterna kommer.
6. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, när personuppgifter har rättats, raderats eller begränsats i enlighet med punkterna 1, 2 och 3, ska underrätta mottagarna och att mottagarna ska rätta eller radera personuppgifterna eller begränsa den behandling som utförs under deras ansvar.

Artikel 17

Den registrerades utövande av rättigheter och kontroll genom tillsynsmyndigheten

1. I de fall som avses i artiklarna 13.3, 15.3 och 16.4 ska medlemsstaterna anta bestämmelser om att den registrerades rättigheter även kan utövas genom den behöriga tillsynsmyndigheten.
2. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska underrätta den registrerade om hans eller hennes möjlighet att utöva sina rättigheter genom tillsynsmyndigheten enligt punkt 1.
3. När den rättighet som avses i punkt 1 utövas ska tillsynsmyndigheten åtminstone underrätta den registrerade om att alla nödvändiga kontroller eller en översyn genom tillsynsmyndigheten har ägt rum. Tillsynsmyndigheten ska också informera den registrerade om hans eller hennes rätt att begära rättslig prövning.

Artikel 18

Den registrerades rättigheter i brottsutredningar och straffrättsliga förfaranden

Medlemsstaterna får föreskriva att de rättigheter som avses i artiklarna 13, 14 och 16 ska utövas i enlighet med medlemsstaternas nationella rätt om personuppgifterna ingår i ett domstolsbeslut eller ett rättsligt protokoll eller ärende som behandlas i samband med brottsutredningar och straffrättsliga förfaranden.

KAPITEL IV

Personuppgiftsansvarig och personuppgiftsbiträde

Avsnitt 1

Allmänna skyldigheter

Artikel 19

Den personuppgiftsansvariges skyldigheter

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, med beaktande av behandlingens art, omfattning, sammanhang och ändamål, samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa, och kunna visa, att behandlingen utförs i enlighet med detta direktiv. Dessa åtgärder ska ses över och uppdateras vid behov.
2. Om det står i proportion till behandlingen, ska de åtgärder som avses i punkt 1 omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.

Artikel 20

Inbyggt dataskydd och dataskydd som standard

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

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

Artikel 21

Gemensamt personuppgiftsansvariga

1. Medlemsstaterna ska föreskriva att två eller flera personuppgiftsansvariga har gemensamt ansvar för registret, om de gemensamt fastställer behandlingens ändamål och medel. De ska under öppna former fastställa sitt respektive ansvar för efterlevnaden av detta direktiv, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artikel 13, genom ett inbördes arrangemang, såvida inte och i den mån som de personuppgiftsansvarigas respektive skyldigheter fastställs i unionsrätt eller medlemsstaternas nationella rätt som de personuppgiftsansvariga omfattas av. Inom ramen för arrangemanget ska en kontaktpunkt för de registrerade utses. Medlemsstaterna får fastslå vem av de gemensamt personuppgiftsansvariga som kan fungera som enda kontaktpunkt för de registrerade i fråga om utövandet av deras rättigheter.

2. Oavsett formerna för det arrangemang som avses i punkt 1 får medlemsstaterna föreskriva att den registrerade får utöva sina rättigheter enligt de bestämmelser som antas i enlighet med detta direktiv med avseende på var och en av de personuppgiftsansvariga.

Artikel 22

Personuppgiftsbiträde

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

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

3. Medlemsstaterna ska föreskriva att ett personuppgiftsbiträdes behandling ska regleras genom ett avtal eller annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige och i vilken föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade samt den personuppgiftsansvariges skyldigheter och rättigheter anges. Avtalet eller den andra rättsakten ska särskilt föreskriva att personuppgiftsbiträdet

- a) endast handlar enligt instruktioner från den personuppgiftsansvarige,
- b) säkerställer att personer som har tillstånd att behandla personuppgifterna har förbundit sig att iakttäta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt,
- c) på lämpligt sätt ska bistå den personuppgiftsansvarige att säkerställa efterlevnad av bestämmelserna om den registrerades rättigheter,
- d) beroende på vad den personuppgiftsansvarige väljer, ska radera eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av uppgiftsbehandlingstjänster har avslutats och raderar befintliga kopior, såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt,

- e) ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att denna artikel efterlevs,
 - f) respekterar de villkor som avses i punkterna 2 och 3 för anlitande av ett annat personuppgiftsbiträde.
4. Det avtal eller den andra rättsakt som avses i punkt 3 ska vara skriftligt, inbegripet i elektronisk form.
5. Om ett personuppgiftsbiträde i strid med detta direktiv fastställer ändamålen och medlen för behandlingen ska personuppgiftsbiträdet anses vara personuppgiftsansvarig med avseende på den behandlingen.

Artikel 23

Behandling under den personuppgiftsansvariges eller personuppgiftsbitrådets överinseende

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

Artikel 24

Register över behandling

1. Medlemsstaterna ska föreskriva att alla personuppgiftsansvariga ska föra ett register över alla kategorier av verksamheter i samband med behandling som de ansvarar för. Detta register ska innehålla samtliga följande uppgifter:
- a) Namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga och dataskyddsombudet.
 - b) Ändamålen med behandlingen.
 - c) De kategorier av mottagare som personuppgifterna har lämnats ut till eller ska lämnas ut till, inbegripet mottagare i tredjeländer eller internationella organisationer.
 - d) En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.
 - e) Användning av profilering, i tillämpliga fall.
 - f) I tillämpliga fall, kategorier av personuppgiftsöverföringar till ett tredjeland eller en internationell organisation.
 - g) En uppgift om den rättsliga grunden för den behandling, inbegripet överföringar, för vilken personuppgifterna är avsedda.
 - h) Om möjligt, de planerade tidsfristerna för radering av de olika personuppgiftskategorierna.
 - i) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 29.1.
2. Medlemsstaterna ska föreskriva att alla personuppgiftsbiträden ska upprätthålla ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning, vilket ska omfatta följande:
- a) Namn och kontaktuppgifter för personuppgiftsbiträdet eller registerförarna, för varje personuppgiftsansvarig för vars räkning personuppgiftsbiträdet agerar samt, i tillämpliga fall, för dataskyddsombudet.
 - b) De kategorier av behandling som har utförts för varje personuppgiftsansvarigs räkning.
 - c) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen, om den personuppgiftsansvarige uttryckligen begär detta.
 - d) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 29.1.

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

Den personuppgiftsansvarige och personuppgiftsbiträdet ska på begäran göra registren tillgängliga för tillsynsmyndigheten.

Artikel 25

Loggning

1. Medlemsstaterna ska säkerställa att loggar förs över åtminstone följande typer av behandlingar i automatiserade behandlingssystem: insamling, ändring, läsning, utlämning inbegripet överföringar, sammanförande och radering. Loggarna över läsning och utlämning ska göra det möjligt att fastställa motivering, datum och tidpunkt för sådan behandling och i möjligaste mån vem som har läst eller lämnat ut personuppgifter, samt vilka som har fått tillgång till personuppgifterna.
2. Loggarna bör endast användas för att kontrollera om behandlingen är tillåten, för egenkontroll, för att säkerställa personuppgifternas integritet och säkerhet, samt inom ramen för straffrättsliga förfaranden.
3. Den personuppgiftsansvarige och personuppgiftsbiträdet ska på begäran göra loggarna tillgängliga för tillsynsmyndigheten.

Artikel 26

Samarbete med tillsynsmyndigheten

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige och personuppgiftsbiträdet på begäran ska samarbeta med tillsynsmyndigheten vid utförandet av dess uppgifter.

Artikel 27

Konsekvensbedömning avseende dataskydd

1. Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter, ska medlemsstaterna säkerställa att den personuppgiftsansvarige före behandlingen utför en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.
2. Den bedömning som avses i punkt 1 ska åtminstone innehålla en allmän beskrivning av den planerade behandlingen, en bedömning av riskerna för de registrerades rättigheter och friheter, de åtgärder som planeras för att hantera dessa risker, skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifter och för att visa att detta direktiv efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

Artikel 28

Förhandssamråd med tillsynsmyndigheten

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige eller personuppgiftsbiträdet ska samråda med tillsynsmyndigheten före behandling av personuppgifter som kommer att ingå i ett nytt register som ska inrättas, om
 - a) en konsekvensbedömning avseende dataskydd enligt artikel 27 visar att behandlingen skulle leda till en hög risk om inte den registeransvarige vidtar åtgärder för att minska risken, eller om
 - b) typen av behandling, särskilt vid användning av ny teknik eller nya rutiner eller förfaranden, medför en hög risk för de registrerades rättigheter och friheter.
2. Medlemsstaterna ska föreskriva att tillsynsmyndigheten ska rådfrågas under utarbetandet av ett förslag till lagstiftningsåtgärd som ska antas av ett nationellt parlament eller av en regleringsåtgärd som grundar sig på en sådan lagstiftningsåtgärd som rör behandling.
3. Medlemsstaterna ska föreskriva att tillsynsmyndigheten får upprätta en förteckning över de olika typer av uppgiftsbehandling som omfattas av förhandssamråd enligt punkt 1.

4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige till tillsynsmyndigheten lämnar in den konsekvensbedömning avseende dataskydd som avses i artikel 27 och, på begäran, eventuell övrig information som gör att tillsynsmyndigheten kan göra en bedömning av behandlingens överensstämmelse och särskilt av riskerna för skyddet av den registrerades personuppgifter och av därmed sammanhängande skyddsåtgärder.

5. Medlemsstaterna ska, om tillsynsmyndigheten anser att den planerade behandling som avses i punkt 1 i denna artikel inte skulle vara förenlig med de bestämmelser som antas i enlighet med detta direktiv, särskilt om den personuppgiftsansvarige inte i tillräcklig mån har fastställt eller reducerat risken, föreskriva att tillsynsmyndigheten inom en period på högst sex veckor från det att begäran om samråd mottagits ska ge den personuppgiftsansvarige och, i tillämpliga fall, personuppgiftsbiträdet skriftliga råd och får utnyttja alla de befogenheter som den har enligt artikel 47. Denna period får förlängas med en månad beroende på hur komplicerad den planerade behandlingen är. Tillsynsmyndigheten ska informera den personuppgiftsansvarige och, i tillämpliga fall, personuppgiftsbiträdet om en sådan förlängning inom en månad från det att begäran om samråd mottagits, tillsammans med orsakerna till förseningen.

Avsnitt 2

Säkerhet för personuppgifter

Artikel 29

Säkerhet i samband med behandling

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige och personuppgiftsbiträdet, med beaktande av den senaste utvecklingen och genomförandekostnader och med hänsyn till behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, i synnerhet när det gäller de särskilda kategorier av personuppgifter som avses i artikel 10.

2. När det gäller automatiserad behandling ska varje medlemsstat föreskriva att den personuppgiftsansvarige eller personuppgiftsbiträdet, efter en bedömning av riskerna, ska vidta åtgärder i syfte att

- a) vägra varje obehörig person åtkomst till utrustning för behandling som används för behandling (*åtkomstskydd för utrustning*),
- b) förhindra obehörig läsning, kopiering, ändring eller radering av datamedier (*kontroll av datamedier*),
- c) förhindra obehörig registrering av personuppgifter och obehörig kännedom om, ändring eller radering av lagrade personuppgifter (*lagringskontroll*),
- d) förhindra att obehöriga kan använda automatiserade behandlingssystem med hjälp av utrustning för dataöverföring (*användarkontroll*),
- e) säkerställa att personer som är behöriga att använda ett automatiserat behandlingssystem endast har tillgång till personuppgifter som omfattas av deras behörighet (*åtkomstkontroll*),
- f) säkerställa att det kan kontrolleras och fastställas till vilka organ personuppgifter har överförts eller kan överföras och för vilka organ uppgifterna har gjorts tillgängliga eller kan göras tillgängliga med hjälp av utrustning för dataöverföring (*kommunikationskontroll*),
- g) säkerställa att det är möjligt att i efterhand kontrollera och fastställa vilka personuppgifter som förts in i ett automatiserat behandlingssystem, samt när och av vem personuppgifterna infördes (*indatakontroll*),
- h) förhindra obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med överföring av sådana uppgifter eller under transport av databärare (*transportkontroll*),
- i) säkerställa att de system som används kan återställas vid störningar (*återställande*),
- j) säkerställa att systemet fungerar, att funktionsfel rapporteras (*driftsäkerhet*) och att de lagrade personuppgifterna inte kan förvanskas genom funktionsfel i systemet (*dataintegritet*).

Artikel 30

Anmälan av en personuppgiftsincident till tillsynsmyndigheten

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige vid en personuppgiftsincident utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om incidenten, anmäler den till tillsynsmyndigheten, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar, ska den åtföljas av en motivering till förseningen.
2. Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident.
3. Den anmälan som avses i punkt 1 ska åtminstone
 - a) beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antal registrerade som berörs samt de kategorier av och det ungefärliga antal personuppgiftsposter som berörs,
 - b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller annan kontaktpunkt där mer information kan erhållas,
 - c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten,
 - d) beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, i tillämpliga fall, åtgärder för att mildra dess potentiella negativa effekter.
4. Om, och i den utsträckning, det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.
5. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter som avses i punkt 1, inbegripet omständigheterna rörande personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentation ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av denna artikel.
6. Medlemsstaterna ska föreskriva att den information som avses i punkt 3, om personuppgiftsincidenten rör personuppgifter som har överförts av eller till den personuppgiftsansvarige i en annan medlemsstat, utan onödigt dröjsmål ska meddelas den personuppgiftsansvarige i den medlemsstaten.

Artikel 31

Information till den registrerade om en personuppgiftsincident

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige, om personuppgiftsincidenten sannolikt kommer att leda till en hög risk för fysiska personers rättigheter och friheter, utan onödigt dröjsmål ska informera den registrerade om personuppgiftsincidenten.
2. Den information till den registrerade som avses i punkt 1 i den här artikeln ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone de upplysningar och åtgärder som avses i artikel 30.3 b, c och d.
3. Information till den registrerade i enlighet med punkt 1 ska inte krävas om något av följande villkor är uppfyllda:
 - a) Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder har tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som gör personuppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till dem, såsom kryptering.
 - b) Om den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter som avses i punkt 1 sannolikt inte längre kommer att uppstå.
 - c) Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.

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

5. Den information till den registrerade som avses i punkt 1 i den här artikeln kan senareläggas, begränsas eller utelämnas på de villkor och av de skäl som avses i artikel 13.3.

Avsnitt 3

Dataskyddsombud

Artikel 32

Utnämning av dataskyddsombudet

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska utnämna ett dataskyddsombud. Medlemsstaterna får undanta domstolars och andra oberoende rättsliga myndigheters dömande verksamhet från denna skyldighet.
2. Dataskyddsombudet ska utnämnas på grundval av sina yrkesmässiga kvalifikationer och, i synnerhet, sin sakkunskap om lagstiftning och praxis i fråga om dataskydd samt förmåga att fullgöra de uppgifter som avses i artikel 34.
3. Ett enda dataskyddsombud får utnämnas för flera behöriga myndigheter med hänsyn tagen till organisationsstruktur och storlek.
4. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.

Artikel 33

Dataskyddsombudets ställning

1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.
2. Den personuppgiftsansvarige ska stödja dataskyddsombudet i utförandet av de uppgifter som avses i artikel 34 genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap.

Artikel 34

Dataskyddsombudets uppgifter

Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska anförtro dataskyddsombudet åtminstone följande uppgifter:

- a) Att informera och ge råd till den personuppgiftsansvarige och de anställda som utför behandling om deras skyldigheter enligt detta direktiv och annan unionsrätt eller medlemsstaters bestämmelser om dataskydd.
- b) Att övervaka efterlevnaden av detta direktiv, annan unionsrätt eller medlemsstaternas bestämmelser om dataskydd och av den personuppgiftsansvariges strategier för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandlingen och tillhörande granskning.
- c) Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den enligt artikel 27.
- d) Att samarbeta med tillsynsmyndigheten.
- e) Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, inbegripet det förhandssamråd som avses i artikel 28, och, om så är lämpligt, samråda i andra frågor.

KAPITEL V

Överföringar av personuppgifter till tredjeländer eller internationella organisationer

Artikel 35

Allmänna principer för överföringar av personuppgifter

1. Medlemsstaterna ska föreskriva att de behöriga myndigheterna endast ska överföra personuppgifter som håller på att behandlas eller är avsedda att behandlas efter det att de överförs till ett tredjeland eller en internationell organisation, inklusive för vidare överföring till ett annat tredjeland eller en annan internationell organisation, under förutsättning att de nationella bestämmelser som antas i enlighet med andra bestämmelser i detta direktiv respekteras och endast om de villkor som fastställs i detta kapitel uppfylls, nämligen:

- a) Överföringen är nödvändig för de ändamål som anges i artikel 1.1.
- b) Personuppgifterna överförs till en personuppgiftsansvarig i ett tredjeland eller en internationell organisation som är en behörig myndighet för de ändamål som avses i artikel 1.1.
- c) Den aktuella medlemsstaten, om personuppgifter överförs eller görs tillgängliga från en annan medlemsstat, har gett förhandstillstånd till överföringen i enlighet med medlemsstaternas nationella rätt.
- d) Kommissionen har antagit ett beslut om adekvat skyddsnivå i enlighet med artikel 36 eller, om inget sådant beslut föreligger, när lämpliga skyddsåtgärder har vidtagits eller föreligger enligt artikel 37 eller, om inget beslut om adekvat skyddsnivå enligt artikel 36 föreligger och inga lämpliga skyddsåtgärder enligt artikel 37 har vidtagits, när undantag för särskilda situationer gäller i enlighet med artikel 38.
- e) Att den behöriga myndighet som gjorde den ursprungliga överföringen eller en annan behörig myndighet i samma medlemsstat vid vidare överföring till ett annat tredjeland eller en internationell organisation godkänner vidareöverföringen efter vederbörligt beaktande av alla relevanta faktorer, inbegripet brottets allvar, det ändamål för vilket personuppgifterna ursprungligen överfördes och nivån på skyddet av personuppgifter i tredjelandet till vilket eller den internationella organisationen till vilken personuppgifterna förts vidare.

2. Medlemsstaterna ska föreskriva att överföringar utan förhandstillstånd av en annan medlemsstat i enlighet med punkt 1 c tillåts endast om överföringen av personuppgifter är nödvändig för att avvärja ett omedelbart och allvarligt hot mot den allmänna säkerheten i en medlemsstat eller ett tredjeland eller mot en medlemsstats väsentliga intressen och förhandstillstånd inte kan erhållas i tid. Den myndighet som har ansvar för att ge förhandstillstånd ska underrättas utan dröjsmål.

3. Alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den skyddsnivå för fysiska personer som säkerställs genom detta direktiv inte undergrävs.

Artikel 36

Överföring på grundval av ett beslut om adekvat skyddsnivå

1. Medlemsstaterna ska föreskriva att personuppgifter får överföras till ett tredjeland eller en internationell organisation om kommissionen har beslutat att tredjelandet, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå. En sådan överföring ska inte kräva ett särskilt tillstånd.

2. När kommissionen bedömer om en adekvat skyddsnivå föreligger ska den särskilt beakta

- a) rättsstatsprincipen, respekten för de mänskliga rättigheterna och grundläggande friheterna, relevant lagstiftning, både allmän lagstiftning och sektorslagstiftning, inklusive avseende allmän säkerhet, försvar, nationell säkerhet och straffrätt samt offentliga myndigheters tillgång till personuppgifter liksom tillämpningen av denna lagstiftning, dataskyddsregler, yrkesregler och säkerhetsbestämmelser och regler för vidare överföring av personuppgifter till ett annat tredjeland eller en annan internationell organisation, som ska följas i det tredjeland eller inom den internationella organisation som berörs, rättspraxis, och effektiva och verkställbara rättigheter för registrerade och effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs,
- b) huruvida det finns en eller flera effektivt fungerande oberoende tillsynsmyndigheter i tredjelandet, eller som utövar tillsyn över den internationella organisationen, med ansvar för att säkerställa och kontrollera att dataskyddsbestämmelserna följs, inklusive lämpliga verkställighetsbefogenheter, ge registrerade råd och assistans när det gäller utövandet av deras rättigheter och samarbeta med medlemsstaternas tillsynsmyndigheter, och

c) vilka internationella åtaganden det berörda tredjelandet eller den berörda internationella organisationen har gjort, eller andra skyldigheter som följer av rättsligt bindande konventioner eller instrument samt av dess deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter.

3. Kommissionen får, efter att ha bedömt om skyddsnivån är adekvat, genom en genomförandeakt, besluta att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland, eller en internationell organisation, säkerställer en adekvat skyddsnivå i den mening som avses i punkt 2 i den här artikeln. Genomförandeakten ska inrätta en mekanism för regelbunden översyn, minst vart fjärde år, som ska beakta all relevant utveckling i det tredjelandet eller den internationella organisationen. Den territoriella och sektoriella tillämpningen ska regleras i genomförandeakten, där det också i förekommande fall ska anges vilken eller vilka myndigheter som är tillsynsmyndighet(er) enligt punkt 2 b i den här artikeln. Genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 58.2.

4. Kommissionen ska fortlöpande övervaka utveckling i tredjeländer och internationella organisationer vilken kan påverka hur beslut som antagits enligt punkt 3 fungerar.

5. Kommissionen ska, när tillgänglig information visar, i synnerhet efter den översyn som avses i punkt 3 i den här artikeln, att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom tredjelandet i fråga eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå i den mening som avses i punkt 2 i den här artikeln och, i den mån det behövs, genom genomförandeakter dra tillbaka, ändra eller upphäva det beslut som avses i punkt 3 i den här artikeln utan retroaktiv verkan. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 58.2.

När det föreligger vederbörligen motiverade och tvingande skäl till skyndsamhet, ska kommissionen anta omedelbart tillämpliga genomförandeakter i enlighet med det förfarande som avses i artikel 58.3.

6. Kommissionen ska samråda med tredjelandet eller den internationella organisationen i fråga för att lösa den situation som lett till beslutet enligt punkt 5.

7. Medlemsstaterna ska föreskriva att ett beslut enligt punkt 5 inte ska påverka överföringar av personuppgifter till tredjelandet, territoriet eller en eller flera specificerade sektorer inom tredjelandet, eller den internationella organisationen i fråga, enligt artiklarna 37–38.

8. Kommissionen ska i *Europeiska unionens officiella tidning* och på sin webbplats offentliggöra en förteckning över de tredjeländer och de territorier och specificerade sektorer i ett tredjeland samt de internationella organisationer för vilka den har fastställt att en adekvat skyddsnivå inte eller inte längre säkerställs.

Artikel 37

Överföring som omfattas av lämpliga skyddsåtgärder

1. Om det inte föreligger något beslut enligt artikel 36.3 ska medlemsstaterna föreskriva att en överföring av personuppgifter till ett tredjeland eller en internationell organisation får ske om

a) lämpliga skyddsåtgärder för personuppgifter har fastställts i ett rättsligt bindande instrument, eller

b) den personuppgiftsansvarige har bedömt alla omständigheter kring en överföring av personuppgifter och dragit slutsatsen att lämpliga skyddsåtgärder för personuppgifterna föreligger.

2. Den personuppgiftsansvarige ska informera tillsynsmyndigheten om kategorier av överföringar enligt punkt 1 b.

3. När en överföring grundas på punkt 1 b, ska denna överföring dokumenteras, och dokumentationen ska på begäran göras tillgänglig för tillsynsmyndigheten, inbegripet datum och tidpunkt för överföringen, information om den mottagande behöriga myndigheten, skälet till överföringen och de personuppgifter som har överförts.

Artikel 38

Undantag i särskilda situationer

1. Om det inte föreligger något beslut om adekvat skyddsnivå enligt artikel 36 eller lämpliga skyddsåtgärder enligt artikel 37, ska medlemsstaterna föreskriva att en överföring eller en kategori av överföringar av personuppgifter till ett tredjeland eller en internationell organisation får ske endast om överföringen är nödvändig
 - a) för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan person,
 - b) för att skydda den registrerades berättigade intressen, om lagstiftningen i den medlemsstat som överför personuppgifterna föreskriver detta,
 - c) för att avvärja en omedelbar och allvarlig fara för den allmänna säkerheten i en medlemsstat eller ett tredjeland,
 - d) i enskilda fall för de ändamål som anges i artikel 1.1. eller
 - e) i ett enskilt fall för att fastslå, göra gällande eller försvara rättsliga anspråk som hänför sig till de ändamål som anges i artikel 1.1.
2. Personuppgifter får inte överföras om den överförande behöriga myndigheten fastställer att den berörda registrerades grundläggande rättigheter och friheter väger tyngre än det allmänna intresset av en sådan överföring som avses i punkt 1 d och e.
3. När en överföring grundas på punkt 1, ska denna överföring dokumenteras, och dokumentationen ska på begäran göras tillgänglig för tillsynsmyndigheten, inbegripet datum och tidpunkt för överföringen, information om den mottagande behöriga myndigheten, skälet till överföringen och de personuppgifter som har överförts.

Artikel 39

Överföringar av personuppgifter till mottagare som är etablerade i tredjeländer

1. Genom undantag från artikel 35.1 b och utan att det påverkar tillämpningen av internationella avtal som avses i punkt 2 i den här artikeln, får det i unionsrätten eller medlemsstaternas nationella rätt föreskrivas att de behöriga myndigheter som avses i artikel 3.7 a, i enskilda och särskilda fall, får överföra personuppgifter direkt till mottagare som är etablerade i tredjeländer endast om de övriga bestämmelserna i detta direktiv efterlevs och samtliga följande villkor är uppfyllda:
 - a) Överföringen är absolut nödvändig för att utföra en uppgift som en överförande behörig myndighet ansvarar för i enlighet med unionsrätten eller medlemsstaternas nationella rätt för de ändamål som anges i artikel 1.1.
 - b) Den överförande behöriga myndigheten har fastställt att ingen av den berörda registrerades grundläggande rättigheter och friheter väger tyngre än det allmänna intresse som nödvändiggör överföringen i det aktuella fallet.
 - c) Den överförande behöriga myndigheten anser att överföring till en myndighet som är behörig för de ändamål som avses i artikel 1.1 i tredjelandet är ineffektivt eller olämpligt, i synnerhet eftersom överföringen inte kan göras inom rimlig tid.
 - d) Den myndighet i tredjelandet som är behörig för de ändamål som avses i artikel 1.1 har utan dröjsmål informerats, såvida detta inte är ineffektivt eller olämpligt.
 - e) Den överförande behöriga myndigheten har informerat mottagaren om det eller de specifika ändamål för vilka och personuppgifterna ska behandlas av den senare förutsatt att den behandlingen är nödvändig.
2. Med ett internationellt avtal som avses i punkt 1 avses varje gällande bilateralt eller multilateralt internationellt avtal mellan medlemsstater och tredjeländer inom området för straffrättsligt samarbete och polissamarbete.
3. Den överförande behöriga myndigheten ska informera tillsynsmyndigheten om överföringar enligt denna artikel.
4. Överföringar som grundar sig på punkt 1 ska dokumenteras.

Artikel 40

Internationellt samarbete för skydd av personuppgifter

När det gäller tredjeländer och internationella organisationer ska kommissionen och medlemsstaterna vidta lämpliga åtgärder för att

- a) utveckla rutiner för det internationella samarbetet för att underlätta en effektiv tillämpning av lagstiftningen om skydd av personuppgifter,
- b) på internationell nivå erbjuda ömsesidigt bistånd för en effektiv tillämpning av lagstiftningen om skydd av personuppgifter, bland annat genom underrättelse, hänskjutande av klagomål, bistånd vid utredningar samt informationsutbyte, med iakttagande av lämpliga skyddsåtgärder för personuppgifter samt skyddet av andra grundläggande rättigheter och friheter,
- c) involvera berörda aktörer i diskussioner och åtgärder som syftar till att öka det internationella samarbetet när det gäller tillämpningen av lagstiftningen om skydd av personuppgifter,
- d) främja utbyte och dokumentation om lagstiftning och praxis för skydd av personuppgifter, inklusive avseende behörighetskonflikter med tredjeländer.

KAPITEL VI

Oberoende tillsynsmyndigheter

Avsnitt 1

Oberoende ställning

Artikel 41

Tillsynsmyndighet

1. Varje medlemsstat ska föreskriva att en eller flera offentliga myndigheter ska vara ansvariga för att övervaka tillämpningen av detta direktiv, i syfte att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandlingen samt att underlätta det fria flödet av sådana uppgifter inom unionen (*tillsynsmyndighet*).
2. Varje tillsynsmyndighet ska bidra till en enhetlig tillämpning av detta direktiv i hela unionen. För det ändamålet ska tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen i enlighet med kapitel VII.
3. Medlemsstaterna får föreskriva att en tillsynsmyndighet som har inrättats enligt förordning (EU) 2016/679 ska vara den tillsynsmyndighet som avses i detta direktiv och ta på sig ansvaret för de uppgifter som ska utföras av den tillsynsmyndighet som inrättats enligt punkt 1 i denna artikel.
4. Om det finns fler än en tillsynsmyndighet i en medlemsstat ska medlemsstaten utse den tillsynsmyndighet som ska företräda myndigheterna i fråga i den styrelse som avses i artikel 51.

Artikel 42

Oberoende

1. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet ska vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med detta direktiv.
2. Medlemsstaterna ska föreskriva att dess tillsynsmyndigheters ledamot eller ledamöter i utförandet av sina uppgifter och i utövandet av sina befogenheter enligt detta direktiv ska stå fria från utomstående påverkan, direkt såväl som indirekt, och varken begära eller ta emot instruktioner av någon.
3. Medlemsstaternas tillsynsmyndigheters ledamot eller ledamöter ska avhålla sig från alla handlingar som står i strid med deras tjänsteutövning och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet som står i strid med deras tjänsteutövning.
4. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet förfogar över de personella, tekniska och finansiella resurser samt de lokaler och den infrastruktur som behövs för att myndigheten ska kunna utföra sina uppgifter och utöva sina befogenheter, inklusive inom ramen för det ömsesidiga biståndet, samarbetet och deltagandet i styrelsens verksamhet.

5. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet väljer och förfogar över egen personal, som ska ta instruktioner uteslutande från den berörda tillsynsmyndighetens ledamot eller ledamöter.

6. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet är föremål för finansiell kontroll, utan att detta påverkar tillsynsmyndighetens oberoende och att de förfogar över en separat, offentlig årsbudget som kan ingå i den övergripande statsbudgeten eller nationella budgeten.

Artikel 43

Allmänna villkor för tillsynsmyndighetens ledamöter

1. Medlemsstaterna ska föreskriva att varje ledamot av deras tillsynsmyndigheter ska utses genom ett öppet förfarande av
 - deras parlament
 - deras regering
 - deras statschef, eller
 - ett oberoende organ som enligt medlemsstaternas nationella rätt anförtrotts utnämningen.
2. Varje ledamot ska ha de kvalifikationer, den erfarenhet och den kompetens, särskilt på området skydd av personuppgifter, som krävs för att de ska kunna utföra sitt uppdrag och utöva sina befogenheter.
3. En ledamots uppdrag ska upphöra då mandattiden löper ut eller om ledamoten avgår eller avsätts från sin tjänst i enlighet med den nationella rätten i den berörda medlemsstaten.
4. En ledamot ska avsättas endast på grund av allvarlig försummelse eller när ledamoten inte längre uppfyller de krav som ställs för att kunna utföra sina uppgifter.

Artikel 44

Regler för inrättandet av en tillsynsmyndighet

1. Varje medlemsstat ska i lag fastställa samtliga följande:
 - a) Varje tillsynsmyndighets inrättande.
 - b) De kvalifikationer och de villkor för lämplighet som krävs för att någon ska kunna utnämnas till ledamot av en tillsynsmyndighet.
 - c) Regler och förfaranden för att utse varje tillsynsmyndighets ledamot eller ledamöter.
 - d) Mandattiden för varje tillsynsmyndighets ledamot eller ledamöter, vilken inte får understiga fyra år, utom vid tillsättandet av de första ledamöterna efter den 6 maj 2016, då ett stegvis tillsättningsförfarande med kortare perioder för några av ledamöterna får tillämpas om detta är nödvändigt för att säkerställa myndighetens oberoende.
 - e) Huruvida varje tillsynsmyndighets ledamot eller ledamöter får ges förnyat mandat, och om så är fallet, för hur många perioder,
 - f) Vilka villkor som gäller för de skyldigheter som varje tillsynsmyndighets ledamot eller ledamöter och personal har, förbud mot handlingar, yrkesverksamhet och förmåner som står i strid därmed under och efter mandattiden och vilka bestämmelser som gäller för anställningens upphörande.
2. Varje tillsynsmyndighets ledamot eller ledamöter och personal ska i enlighet med unionsrätten eller medlemsstaternas nationella rätt omfattas av tystnadsplikt både under och efter sin mandattid vad avser konfidentiell information som de fått kunskap om under utförandet av deras uppgifter eller utövandet av deras befogenheter. Under mandatperioden ska denna tystnadsplikt i synnerhet gälla rapporter från fysiska personer om överträdelser av detta direktiv.

Avsnitt 2

Behörighet, uppgifter och befogenheter*Artikel 45***Behörighet**

1. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet ska vara behörig att utföra de uppgifter och utöva de befogenheter som tilldelas den i enlighet med detta direktiv inom sin egen medlemsstats territorium.
2. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet inte ska vara behörig att utöva tillsyn över domstolar som behandlar personuppgifter inom ramen för sin dömande verksamhet. Medlemsstaterna får föreskriva att deras tillsynsmyndighet inte ska vara behörig att utöva tillsyn över andra oberoende rättsliga myndigheter som behandlar personuppgifter inom ramen för sin rättsliga verksamhet.

*Artikel 46***Uppgifter**

1. Varje medlemsstat ska föreskriva att varje tillsynsmyndighet inom sitt territorium ska
 - a) övervaka och verkställa tillämpningen av de bestämmelser som antas i enlighet med detta direktiv och dess genomförandeåtgärder,
 - b) öka allmänhetens medvetenhet och kunskaper om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen,
 - c) i enlighet med medlemsstaternas nationella rätt ge rådgivning åt det nationella parlamentet, regeringen och andra institutioner och organ om lagstiftningsmässiga och administrativa åtgärder rörande skyddet av fysiska personers rättigheter och friheter när det gäller behandling,
 - d) öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter enligt detta direktiv,
 - e) på begäran tillhandahålla information till registrerade om hur de ska utöva sina rättigheter enligt detta direktiv, och om så krävs samarbeta med tillsynsmyndigheter i andra medlemsstater för detta ändamål,
 - f) behandla klagomål från en registrerad eller från ett organ, en organisation eller en sammanslutning enligt artikel 55, och där så är lämpligt undersöka den sakfråga som klagomålet gäller och inom rimlig tid underrätta den enskilde om hur undersökningen fortskrider och om resultatet, i synnerhet om det krävs ytterligare undersökningar eller samordning med en annan tillsynsmyndighet,
 - g) kontrollera att behandling enligt artikel 17 är laglig och inom en rimlig period informera den registrerade om resultatet av kontrollen enligt artikel 17.3 eller om skälen till att kontrollen inte har genomförts,
 - h) samarbeta, inbegripet genom att utbyta information, med och ge ömsesidigt bistånd till andra tillsynsmyndigheter för att se till att detta direktiv tillämpas och verkställs på ett enhetligt sätt,
 - i) utföra undersökningar om tillämpningen av detta direktiv, inbegripet på grundval av information som erhålls från en annan tillsynsmyndighet eller annan offentlig myndighet,
 - j) följa sådan utveckling som påverkar skyddet av personuppgifter, bland annat inom informations- och kommunikationsteknik,
 - k) ge råd om sådan behandling av personuppgifter som avses i artikel 28, och
 - l) bidra till styrelsens verksamhet.
2. Varje tillsynsmyndighet ska underlätta inlämningen av klagomål enligt punkt 1 f genom åtgärder, såsom att tillhandahålla ett särskilt formulär för ändamålet, vilket också kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.

3. Utförandet av alla tillsynsmyndigheters uppgifter ska vara avgiftsfritt för den registrerade och för dataskyddsombudet.

4. Om en begäran är uppenbart ogrundad eller orimlig, särskilt på grund av att den är repetitiv, får tillsynsmyndigheten ta ut en rimlig avgift grundad på de administrativa kostnaderna eller vägra att tillmötesgå begäran. Det åligger tillsynsmyndigheten att visa att begäran är uppenbart ogrundad eller orimlig.

Artikel 47

Befogenheter

1. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har effektiva undersökningsbefogenheter. Dessa befogenheter ska minst inbegripa rätten att från den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter som behandlas och all information som tillsynsmyndigheten behöver för att kunna fullgöra sina uppgifter.

2. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har effektiva korrigerande befogenheter, till exempel för att:

- a) Utfärda varningar till den personuppgiftsansvarige eller personuppgiftsbiträdet om att planerade behandlingar sannolikt kommer att stå i strid med de bestämmelser som antas i enlighet med detta direktiv.
- b) Beordra den personuppgiftsansvarige eller personuppgiftsbiträdet att se till att uppgiftsbehandlingen är förenlig med de bestämmelser som antas enligt detta direktiv, om lämpligt på ett visst sätt och inom en viss tid, bland annat genom att beordra rättelse, eller radering av personuppgifter eller begränsning av behandling enligt artikel 16.
- c) Införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, uppgiftsbehandlingen.

3. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har effektiva befogenheter att ge den personuppgiftsansvarige råd i enlighet med det förfarande för förhandssamråd som avses i artikel 28 och att på eget initiativ eller på begäran avge yttranden till det nationella parlamentet, medlemsstatens regering eller, i enlighet med dess nationella rätt, till andra institutioner och organ samt till allmänheten, i frågor som rör skydd av personuppgifter.

4. Utövandet av de befogenheter som tillsynsmyndigheten tilldelas enligt denna artikel ska omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel och rättssäkerhet, som fastställts i unionsrätten och medlemsstaternas nationella rätt i enlighet med stadgan.

5. Varje medlemsstat ska i lag säkerställa att varje tillsynsmyndighet har befogenhet att göra rättsliga myndigheter uppmärksamma på överträdelser av de bestämmelser som antas i enlighet med detta direktiv och att, när så är lämpligt, inleda eller på annat sätt delta i rättsliga förfaranden, i syfte att säkerställa efterlevnaden av bestämmelser som antas i enlighet med detta direktiv.

Artikel 48

Rapportering av överträdelser

Medlemsstaterna ska föreskriva att de behöriga myndigheterna ska inrätta effektiva mekanismer för att uppmuntra till konfidentiell rapportering av överträdelser av detta direktiv.

Artikel 49

Verksamhetsrapport

Varje tillsynsmyndighet ska upprätta en årlig rapport om sin verksamhet, vilken kan omfatta en förteckning över typer av anmälda överträdelser och typer av ålagda sanktioner. Rapporterna ska översändas till det nationella parlamentet, regeringen och andra myndigheter som utsetts genom medlemsstaternas nationella rätt. Den ska göras tillgänglig för allmänheten, kommissionen och styrelsen.

KAPITEL VII

Samarbete

Artikel 50

Ömsesidigt bistånd

1. Medlemsstaterna ska föreskriva att tillsynsmyndigheterna ska utbyta relevant information och ge ömsesidigt bistånd i arbetet för att genomföra och tillämpa detta direktiv på ett enhetligt sätt, och ska införa åtgärder som bidrar till ett verkningsfullt samarbete. Det ömsesidiga biståndet ska särskilt omfatta begäranden om information och tillsynsåtgärder, till exempel begäranden om att genomföra samråd, inspektioner och utredningar.
2. Medlemsstaterna ska föreskriva att varje tillsynsmyndighet ska vidta alla lämpliga åtgärder för att kunna besvara en begäran från en annan tillsynsmyndighet utan onödigt dröjsmål och inte senare än en månad efter det att den tagit emot begäran. Till sådana åtgärder hör bland annat att översända relevant information om genomförandet av en pågående utredning.
3. En begäran om bistånd ska innehålla all nödvändig information, inklusive syftet med och skälen till denna. Information som utbyts får endast användas för det syfte för vilket den har begärts.
4. En tillsynsmyndighet som tar emot begäran får bara vägra att tillmötesgå begäran om
 - a) den inte är behörig att behandla den sakfråga som begäran avser eller de åtgärder som det begärs att den ska utföra, eller
 - b) det skulle stå i strid med detta direktiv eller med den unionsrätt eller medlemsstatens nationella rätt som den tillsynsmyndighet som mottar begäran omfattas av att tillmötesgå begäran.
5. Den tillsynsmyndighet som tagit emot begäran ska meddela den myndighet som begäran kommer ifrån om resultatet eller, allt efter omständigheterna, om hur de åtgärder som vidtagits för att tillmötesgå begäran fortskrider. Den tillsynsmyndighet som tagit emot begäran ska redogöra för sina skäl för att vägra tillmötesgå begäran i enlighet med punkt 4.
6. Varje tillsynsmyndighet som tar emot begäran ska som regel tillhandahålla den information som begärts av andra tillsynsmyndigheter på elektronisk väg med användning av ett standardiserat format.
7. Tillsynsmyndigheter som tar emot begäran får inte ta ut någon avgift för åtgärder som de vidtagit efter en begäran om ömsesidigt bistånd. Tillsynsmyndigheter får i undantagsfall komma överens med andra tillsynsmyndigheter om regler för ersättning från varandra för vissa utgifter i samband med tillhandahållande av ömsesidigt bistånd.
8. Kommissionen får genom genomförandeakter närmare ange format och förfaranden för sådant ömsesidigt bistånd som avses i denna artikel samt formerna för elektronisk överföring av information tillsynsmyndigheter emellan, samt mellan tillsynsmyndigheter och styrelsen. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 58.2.

Artikel 51

Styrelsens uppgifter

1. Styrelsen som inrättats genom förordning (EU) 2016/679 ska i samband med uppgiftsbehandling som omfattas av detta direktivs tillämpningsområde ha följande uppgifter:
 - a) Ge kommissionen råd i alla frågor som gäller skydd av personuppgifter inom unionen, till exempel om eventuella förslag till ändring av detta direktiv.
 - b) På eget initiativ, på begäran av en av sina ledamöter eller av kommissionen behandla frågor om tillämpningen av detta direktiv och utfärda riktlinjer, rekommendationer och bästa praxis i syfte att främja en enhetlig tillämpning av detta direktiv.
 - c) Utforma riktlinjer för tillsynsmyndigheterna i fråga om tillämpningen av de åtgärder som avses i artikel 47.1 och 47.3.
 - d) Utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led b i detta stycke för att konstatera personuppgiftsincidenter och fastställa det otillbörliga dröjsmål som avses i artikel 30.1 och 30.2 och för de särskilda omständigheter under vilka ett personuppgiftsbiträde eller en personuppgiftsansvarig är skyldig att anmäla personuppgiftsincidenten.

- e) Utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led b i detta stycke angående de omständigheter under vilka en personuppgiftsincident sannolikt kommer att orsaka en hög risk för rättigheterna och friheterna för de fysiska personer som avses i artikel 31.1.
- f) Se över den praktiska tillämpningen av de riktlinjer och rekommendationer samt den bästa praxis som avses i leden b och c.
- g) Avge ett yttrande till kommissionen för bedömningen av huruvida skyddsnivån i ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland, eller en internationell organisation är adekvat, inbegripet för en bedömning av huruvida det tredjelandet, det territoriet, den specificerade sektorn eller den internationella organisationen inte längre säkerställer en adekvat skyddsnivå.
- h) Främja samarbete och effektivt bilateralt och multilateralt utbyte av bästa praxis och information mellan tillsynsmyndigheterna.
- i) Främja gemensamma utbildningsprogram och underlätta personalutbyte mellan tillsynsmyndigheterna, och där så är lämpligt även med tillsynsmyndigheter i tredjeland och internationella organisationer.
- j) Främja utbyte av kunskap och dokumentation om lagstiftning och bästa praxis på området för dataskydd med tillsynsmyndigheter med ansvar för dataskydd i hela världen.

Vad gäller första stycket led g ska kommissionen lämna all nödvändig dokumentation till styrelsen, inklusive korrespondens med regeringen i tredjelandet, med territoriet eller den specificerade sektorn i det tredjelandet eller med den internationella organisationen.

- 2. När kommissionen begär rådgivning från styrelsen får den ange en tidsfrist med hänsyn till hur brådskande ärendet är.
- 3. Styrelsen ska vidarebefordra sina yttranden, riktlinjer, rekommendationer och exempel på bästa praxis till kommissionen och till den kommitté som avses i artikel 58.1, samt offentliggöra dem.
- 4. Kommissionen ska hålla styrelsen underrättad om de åtgärder den vidtagit som en följd av styrelsens yttranden, riktlinjer, rekommendationer och bästa praxis.

KAPITEL VIII

Rättsmedel, ansvar och sanktioner

Artikel 52

Rätt att lämna in ett klagomål till en tillsynsmyndighet

- 1. Utan att det påverkar andra administrativa prövningsförfaranden eller rättsmedel ska medlemsstaterna föreskriva att alla registrerade personer som anser att behandling som avser dem står i strid med de bestämmelser som antas i enlighet med detta direktiv har rätt att lämna in ett klagomål till en enda tillsynsmyndighet.
- 2. Medlemsstaterna ska föreskriva att den tillsynsmyndighet som mottagit klagomålet ska överlämna det till den behöriga tillsynsmyndigheten utan onödigt dröjsmål, om klagomålet inte inlämnats till den myndighet som är behörig enligt artikel 45.1. Den registrerade ska informeras om överlämnandet.
- 3. Medlemsstaterna ska föreskriva att den tillsynsmyndighet som mottagit klagomålet ska tillhandahålla ytterligare hjälp på den registrerades begäran.
- 4. Den registrerade ska underrättas av den behöriga tillsynsmyndigheten om klagomålets handläggning och dess resultat, inbegripet rätten till rättsmedel enligt artikel 53.

Artikel 53

Rätt till ett effektivt rättsmedel mot en tillsynsmyndighets beslut

- 1. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol ska medlemsstater föreskriva att en fysisk eller juridisk person har rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut som avser dem och som meddelats av en tillsynsmyndighet.

2. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol ska varje registrerad person ha rätt till ett effektivt rättsmedel om den enligt artikel 45.1 behöriga tillsynsmyndigheten inte inom tre månader behandlar ett klagomål eller om tillsynsmyndigheten inte informerar den registrerade om handläggningen eller resultatet av det klagomål som inlämnats enligt artikel 52.
3. Medlemsstaterna ska föreskriva att talan mot en tillsynsmyndighet ska väckas vid domstol i den medlemsstat där tillsynsmyndigheten har sitt säte.

Artikel 54

Rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde

Utan att det påverkar tillgängliga administrativa prövningsförfaranden eller prövningsförfaranden utanför domstol, inbegripet rätten att lämna in ett klagomål till en tillsynsmyndighet enligt artikel 52, ska medlemsstaterna föreskriva en rätt till effektiva rättsmedel för registrerade om han eller hon anser att deras rättigheter enligt de bestämmelser som antas enligt detta direktiv har kränkts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med dessa bestämmelser.

Artikel 55

Företrädande av registrerade personer

Medlemsstaterna ska i enlighet med medlemsstaternas nationella processrätt se till att den registrerade har rätt att ge ett organ, en organisation eller en sammanslutning utan vinstsyfte som har inrättats på lämpligt sätt i enlighet med lagen i en medlemsstat, och vars stadgeenliga mål är av allmänt intresse och som är verksam inom området skydd av registrerades rättigheter och friheter vad gäller skyddet av deras personuppgifter, i uppdrag att lämna in klagomålet för hans eller hennes räkning och att utöva de rättigheter som avses i artiklarna 52, 53 och 54 för hans eller hennes räkning.

Artikel 56

Rätt till ersättning

Medlemsstaterna ska föreskriva att var och en som lidit materiell eller immateriell skada till följd av en olaglig behandling av personuppgifter eller av någon annan åtgärd som står i strid med de nationella bestämmelser som antas i enlighet med detta direktiv ska ha rätt till ersättning för denna skada från den personuppgiftsansvarige eller varje annan myndighet som är behörig enligt medlemsstaternas nationella rätt.

Artikel 57

Sanktioner

Medlemsstaterna ska föreskriva sanktioner för överträdelse av bestämmelser som antas enligt detta direktiv och ska vidta de åtgärder som krävs för att säkerställa att dessa sanktioner genomförs. Sanktionerna ska vara effektiva, proportionella och avskräckande.

KAPITEL IX

Genomförandeakter

Artikel 58

Kommittéförfarande

1. Kommissionen ska biträdas av den kommitté som inrättats enligt artikel 93 i förordning (EU) 2016/679. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.
2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.
3. När det hänvisas till denna punkt, ska artikel 8 i förordning (EU) nr 182/2011 jämförd med artikel 5 i den förordningen tillämpas.

KAPITEL X

Slutbestämmelser

Artikel 59

Upphävande av rambeslut 2008/977/RIF

1. Rambeslut 2008/977/RIF ska upphöra att gälla från och med den 6 maj 2018.
2. Hänvisningar till det upphävda beslut som avses i punkt 1 ska anses som hänvisningar till detta direktiv.

Artikel 60

Gällande unionsrättsakter

Detta direktiv ska inte påverka särskilda bestämmelser om skydd av personuppgifter i unionsrättsakter på området för straffrättsligt samarbete och polissamarbete som trädde i kraft den 6 maj 2016 eller tidigare, vilka reglerar behandling medlemsstaterna emellan och medlemsstaternas utsedda myndigheters tillgång till informationssystem som inrättats på grundval av fördragen och som är relevanta för detta direktivs tillämpningsområde.

Artikel 61

Förhållande till tidigare ingångna internationella avtal på området för straffrättsligt samarbete och polissamarbete

Internationella avtal som rör överföring av personuppgifter till tredjeländer eller internationella organisationer som ingicks av medlemsstaterna före den 6 maj 2016 och som är förenliga med unionsrätten så som den tillämpades före den dagen ska fortsätta att gälla tills de ändras, ersätts eller återkallas.

Artikel 62

Kommissionens rapporter

1. Kommissionen ska senast den 6 maj 2022 och därefter vart fjärde år överlämna en rapport om utvärderingen och översynen av detta direktiv till Europaparlamentet och rådet. Rapporten ska offentliggöras.
2. Inom ramen för de utvärderingar och översyner som avses i punkt 1 ska kommissionen i synnerhet granska tillämpningen av kapitel V om överföring av personuppgifter till tredjeländer och internationella organisationer samt hur bestämmelserna fungerar, och därvid särskilt beakta beslut som antagits i enlighet med artiklarna 36.3 och 39.
3. För de ändamål som avses i punkterna 1 och 2 får kommissionen begära information från medlemsstaterna och tillsynsmyndigheterna.
4. Kommissionen ska när den utför de utvärderingar och översyner som avses i punkterna 1 och 2 ta hänsyn till ståndpunkter och slutsatser från Europaparlamentet, rådet och andra relevanta organ och källor.
5. Dessa rapporter får vid behov överlämnas tillsammans med lagstiftningsförslag om ändring, i syfte att ändra detta direktiv med särskild hänsyn till informationsteknikens utveckling och informationssamhällets framsteg.
6. Kommissionen ska senast den 6 maj 2019 se över andra rättsakter som antagits av unionen och som reglerar de behöriga myndigheternas behandling för att uppnå de mål som anges i artikel 1.1, inklusive de som avses i artikel 60, i syfte att bedöma om de behöver anpassas till detta direktiv och att, i förekommande fall, lägga fram förslag till ändring av dessa rättsakter för att säkerställa ett enhetligt tillvägagångssätt för skydd av personuppgifter inom detta direktivs tillämpningsområde.

*Artikel 63***Införlivande**

1. Medlemsstaterna ska senast den 6 maj 2018 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att följa detta direktiv. De ska genast överlämna texten till dessa bestämmelser till kommissionen. De ska tillämpa dessa bestämmelser från och med den 6 maj 2018.

När en medlemsstat antar dessa bestämmelser ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

2. Genom undantag från punkt 1 får medlemsstaterna föreskriva att de automatiserade behandlingssystem som inrättades före den 6 maj 2016 undantagsvis, när det innebär oproportionella ansträngningar, ska bringas i överensstämmelse med artikel 25.1 senast den 6 maj 2023.

3. Genom undantag från punkterna 1 och 2 i denna artikel får en medlemsstat under exceptionella omständigheter bringa ett automatiserat behandlingssystem som avses i punkt 2 i denna artikel i överensstämmelse med artikel 25.1 inom en specifik tidsperiod efter den period som avses i punkt 2 i den här artikeln om det annars skulle uppstå allvarliga problem för driften av detta specifika automatiserade behandlingssystem. Den berörda medlemsstaten ska underrätta kommissionen om skälen till dessa allvarliga problem och skälen till den angivna tidsperioden inom vilken den ska bringa detta specifika automatiserade databehandlingssystem i överensstämmelse med artikel 25.1. Den angivna perioden ska under inga omständigheter inte vara senare än 6 maj 2026.

4. Medlemsstaterna ska till kommissionen överlämna texten till de centrala bestämmelser i medlemsstaternas nationella rätt som de antar inom det område som omfattas av detta direktiv.

*Artikel 64***Ikraftträdande**

Detta direktiv träder i kraft dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

*Artikel 65***Adressater**

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Bryssel den 27 april 2016.

På Europaparlamentets vägnar

M. SCHULZ

Ordförande

På rådets vägnar

J.A. HENNIS-PLASSCHAERT

Ordförande

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2016/681**av den 27 april 2016****om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet**

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 82.1 d och 87.2 a,

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⁾,

efter att ha hört Regionkommittén,

i enlighet med det ordinarie lagstiftningsförfarandet ⁽²⁾, och

av följande skäl:

- (1) Den 6 november 2007 antog kommissionen ett förslag till rådets rambeslut om användning av passageraruppgiftssamlingar (PNR-uppgifter) i brottsbekämpningssyfte. Ikraftträdandet av Lissabonfördraget den 1 december 2009 ledde dock till att kommissionens förslag, som ännu inte hade antagits av rådet, blev inaktuellt.
- (2) I *Stockholmsprogrammet – ett öppet och säkert Europa i medborgarnas tjänst och för deras skydd* ⁽³⁾ uppmanades kommissionen att lägga fram ett förslag om användning av PNR-uppgifter för att förebygga, förhindra, upptäcka, utreda och lagföra terrorism och grov brottslighet.
- (3) I sitt meddelande av den 21 september 2010 om en övergripande strategi när det gäller överföring av passageraruppgiftssamlingar (PNR-uppgifter) till tredjeländer skisserade kommissionen ett antal huvuddrag i en ny unionsstrategi på detta område.
- (4) I rådets direktiv 2004/82/EG ⁽⁴⁾ regleras transportörers översändande av förhandsinformation om passagerare (API-uppgifter) till behöriga nationella myndigheter i syfte att förbättra gränskontrollerna och bekämpa olaglig invandring.
- (5) Målen för detta direktiv är bland annat att trygga säkerheten, skydda personers liv och säkerhet och att inrätta en rättslig ram för skydd av PNR-uppgifter vid behöriga myndigheters behandling av dessa.
- (6) En effektiv användning av PNR-uppgifter, exempelvis genom att jämföra PNR-uppgifter med uppgifter i olika databaser över eftersökta personer och föremål, är nödvändig för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet och därigenom förbättra den inre säkerheten, för att samla in bevisning och i förekommande fall för att hitta medbrottslingar och avslöja kriminella nätverk.
- (7) Bedömningen av PNR-uppgifter gör det möjligt att identifiera personer som tidigare inte har varit misstänkta för delaktighet i terroristbrott eller grov brottslighet innan en sådan bedömning görs och som bör undersökas

⁽¹⁾ EUT C 218, 23.7.2011, s. 107.⁽²⁾ Europaparlamentets ståndpunkt av den 14 april 2016 (ännu ej offentliggjord i EUT) och rådets beslut av den 21 april 2016.⁽³⁾ EUT C 115, 4.5.2010, s. 1.⁽⁴⁾ Rådets direktiv 2004/82/EG av den 29 april 2004 om skyldighet för transportörer att lämna uppgifter om passagerare (EUT L 261, 6.8.2004, s. 24).

närmare av de behöriga myndigheterna. Genom att använda PNR-uppgifter är det möjligt att möta hotet från terroristbrott och grov brottslighet från en annan utgångspunkt än vid behandling av andra kategorier av personuppgifter. För att säkerställa att behandlingen av PNR-uppgifter begränsas till vad som är nödvändigt, bör emellertid utformning och tillämpning av bedömningskriterierna begränsas till att endast omfatta terroristbrott och grov brottslighet för vilka användningen av sådana kriterier är relevant. Bedömningskriterierna bör dessutom fastställas på ett sätt som gör att så få oskyldiga människor som möjligt identifieras felaktigt av systemet.

- (8) Redan nu samlar lufttrafikföretagen in och behandlar PNR-uppgifter om sina passagerare för sina egna kommersiella syften. Detta direktiv bör inte medföra någon skyldighet för lufttrafikföretagen att samla in eller lagra några ytterligare uppgifter om passagerare eller någon skyldighet för passagerare att tillhandahålla några uppgifter utöver dem som redan tillhandahålls lufttrafikföretagen.
- (9) Vissa lufttrafikföretag lagrar insamlade API-uppgifter som en del av PNR-uppgifterna, andra gör det inte. Att använda PNR-uppgifter tillsammans med API-uppgifter tillför ett mervärde, genom att det hjälper medlemsstaterna att kontrollera en individs identitet, vilket ökar PNR-uppgifternas betydelse för brottsbekämpningen och minimerar risken för att man kontrollerar och utreder oskyldiga människor. Därför är det viktigt att säkerställa att lufttrafikföretag, om de samlar in API-uppgifter, överför dessa, oavsett om de lagrar API-uppgifter med hjälp av andra tekniska metoder än andra PNR-uppgifter.
- (10) För att det ska gå att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet är det av största vikt att alla medlemsstater inför bestämmelser om skyldigheter för lufttrafikföretag som tillhandahåller flygförbindelser utanför EU att överföra de PNR-uppgifter, inklusive API-uppgifter, som de samlar in. Medlemsstaterna bör även ha möjlighet att utsträcka denna skyldighet till lufttrafikföretag som tillhandahåller flygförbindelser inom EU. De bestämmelserna bör inte påverka tillämpningen av direktiv 2004/82/EG.
- (11) Behandlingen av personuppgifter bör stå i proportion till de särskilda säkerhetsmål som detta direktiv syftar till att uppfylla.
- (12) Den definition av terroristbrott som tillämpas i detta direktiv bör vara densamma som i rådets rambeslut 2002/475/RIF⁽¹⁾. Definitionen av allvarlig brottslighet bör omfatta de brottskategorier som förtecknas i bilaga II till detta direktiv.
- (13) PNR-uppgifter bör överföras till en särskild enhet för passagerarinformation i den berörda medlemsstaten, för att säkerställa klarhet om vad som gäller och för att minska kostnaderna för lufttrafikföretagen. Enheten för passagerarinformation får ha olika avdelningar i en medlemsstat och medlemsstater får också gemensamt inrätta en enhet för passagerarinformation. Medlemsstaterna bör utbyta information med varandra genom relevanta nät för informationsutbyte för att underlätta informationsutbyte och säkerställa driftskompatibilitet.
- (14) Medlemsstaterna bör betala kostnaderna för användning, lagring och utbyte av PNR-uppgifter.
- (15) En förteckning över PNR-uppgifter som ska vidarebefordras till en enhet för passagerarinformation bör utformas i syfte att återspegla de offentliga myndigheternas legitima krav på att kunna förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet och därigenom förbättra den inre säkerheten i unionen, samtidigt som grundläggande rättigheter skyddas, särskilt rätten till skydd av privatlivet och rätten till skydd av personuppgifter. I detta syfte bör höga standarder tillämpas, i enlighet med Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*), konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter (nedan kallad *konvention nr 108*) och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (nedan kallad *Europakonventionen*). En sådan förteckning bör inte grundas på en persons ras eller etniska ursprung, religion eller övertygelse, politiska eller annan åskådning, medlemskap i fackförening, hälsotillstånd, sexualliv eller sexuella läggning. PNR-uppgifterna bör endast omfatta sådan information om passagerarens bokning och resrutt som gör det möjligt för de behöriga myndigheterna att identifiera flygpassagerare som utgör ett hot mot den inre säkerheten.
- (16) Det finns för närvarande två möjliga metoder för överföring av uppgifter: direktåtkomstmetoden (*pull*-metoden), som innebär att de behöriga myndigheterna i den medlemsstat som begär PNR-uppgifterna kan få direkt åtkomst till lufttrafikföretagets bokningssystem för att hämta en kopia av de PNR-uppgifter som behövs, och sändmetoden (*push*-metoden), som innebär att lufttrafikföretagen överför de begärda PNR-uppgifterna till den myndighet som har begärt dem, vilket således gör det möjligt för lufttrafikföretagen att behålla kontrollen över vilka uppgifter som tillhandahålls. Sändmetoden anses ge en bättre skyddsnivå för uppgifterna och bör vara obligatorisk för alla lufttrafikföretag.

⁽¹⁾ Rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism (EGT L 164, 22.6.2002, s. 3).

- (17) Kommissionen stöder Internationella civila luftfartsorganisationens (Icao) riktlinjer om PNR. Dessa riktlinjer bör därför fungera som underlag vid antagandet av understödda dataformat för överföring av PNR-uppgifter från lufttrafikföretag till medlemsstater. För att säkerställa enhetliga villkor för genomförandet av understödda dataformat och av relevanta protokoll som gäller för överföring av uppgifter från lufttrafikföretag bör kommissionen ges genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ⁽¹⁾.
- (18) Medlemsstaterna bör vidta alla nödvändiga åtgärder för att göra det möjligt för lufttrafikföretagen att uppfylla sina skyldigheter enligt detta direktiv. Medlemsstaterna bör fastställa effektiva, proportionella och avskräckande sanktioner, även ekonomiska sanktioner, för de lufttrafikföretag som inte uppfyller sina skyldigheter med avseende på överföring av PNR-uppgifter.
- (19) Varje medlemsstat bör ansvara för att bedöma potentiella hot från terroristbrott och grov brottslighet.
- (20) Med fullt beaktande av rätten till skydd av personuppgifter och rätten till icke-diskriminering, bör inga beslut som har negativa rättsliga verkningar för en person eller som på ett väsentligt sätt påverkar denna person fattas enbart på grund av den automatiska behandlingen av PNR-uppgifter. Med hänsyn till artiklarna 8 och 21 i stadgan bör sådana beslut inte diskriminera på grund av en persons kön, ras, hudfärg, etniska eller sociala ursprung, genetiska särdrag, språk, religion eller övertygelse, politiska eller annan åskådning, tillhörighet till en nationell minoritet, förmögenhet, börd, funktionshinder, ålder eller sexuella läggning. Kommissionen bör även beakta dessa principer när den ser över tillämpningen av detta direktiv.
- (21) Medlemsstaterna bör under inga omständigheter använda resultatet av behandlingen av PNR-uppgifter för att kringgå sina internationella skyldigheter enligt konventionen av den 28 juli 1951 angående flyktingars rättsliga ställning i dess lydelse enligt protokollet av den 31 januari 1967 eller för att förvägra asylsökande säkra, ändamålsenliga och lagliga möjligheter att ta sig till unionens territorium för att utöva sin rätt till internationellt skydd.
- (22) Med fullt beaktande av principerna i aktuell relevant rättspraxis från Europeiska unionens domstol bör tillämpningen av detta direktiv säkerställa full respekt för de grundläggande rättigheterna, rätten till skydd av privatlivet och proportionalitetsprincipen. Den bör även till fullo vara förenlig med vad som är nödvändigt och proportionellt för att de mål av allmänt intresse som erkänts av unionen ska uppnås och med behovet att skydda andras rättigheter och friheter i kampen mot terroristbrott och grov brottslighet. Tillämpningen av detta direktiv bör vara vederbörligen motiverad och nödvändiga skyddsåtgärder bör vidtas för att säkerställa att all lagring, analys, överföring eller användning av PNR-uppgifter sker på laglig grund.
- (23) Medlemsstaterna bör utbyta PNR-uppgifter som de har mottagit med varandra och med Europol, om detta bedöms vara nödvändigt för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Enheterna för passagerarinformation bör om lämpligt och utan dröjsmål översända resultatet av behandlingen av PNR-uppgifter till enheterna för passagerarinformation i andra medlemsstater för ytterligare utredning. Bestämmelserna i detta direktiv bör inte påverka andra unionsinstrument om informationsutbyte mellan polismyndigheter och andra brottsbekämpande myndigheter och rättsliga myndigheter, till exempel rådets beslut 2009/371/RIF ⁽²⁾ och rådets rambeslut 2006/960/RIF ⁽³⁾. Ett sådant utbyte av PNR-uppgifter bör omfattas av bestämmelserna om polissamarbete och rättsligt samarbete och bör inte undergräva den höga skyddsnivå för både privatlivet och personuppgifter som stadgan, konvention nr 108 och Europakonventionen föreskriver.
- (24) Ett säkert informationsutbyte om PNR-uppgifter mellan medlemsstaterna bör säkerställas genom någon av de befintliga kanalerna för samarbete mellan medlemsstaternas behöriga myndigheter och särskilt med Europol genom Europolns nätapplikation för säkert informationsutbyte (Siena).

⁽¹⁾ 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).

⁽²⁾ Rådets beslut 2009/371/RIF av den 6 april 2009 om inrättande av Europeiska polisbyrå (Europol) (EUT L 121, 15.5.2009, s. 37).

⁽³⁾ Rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater (EUT L 386, 29.12.2006, s. 89).

- (25) Lagringstiden för PNR-uppgifter bör vara tillräckligt lång och stå i proportion till ändamålen, nämligen att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Med tanke på PNR-uppgifternas art och användningsområden bör det vara tillåtet att lagra dem tillräckligt länge för att de ska kunna användas i samband med analyser och utredningar. För att undvika oproportionell användning bör PNR-uppgifterna efter den inledande lagringsperioden avidentifieras genom maskering av uppgifter. För att säkerställa högsta möjliga nivå av dataskydd bör åtkomst till fullständiga PNR-uppgifter, vilka gör det möjligt att direkt identifiera den registrerade, endast beviljas under mycket strikta och begränsade villkor efter den inledande perioden.
- (26) Om specifika PNR-uppgifter har överförts till en behörig myndighet för att användas inom ramen för särskilda brottsutredningar eller lagföringsåtgärder, bör den behöriga myndighetens lagring av dessa uppgifter regleras av nationell rätt, oavsett vilken lagringstid för uppgifter som anges i detta direktiv.
- (27) Den behandling av PNR-uppgifter som i medlemsstaterna utförs av enheten för passagerarinformation och de behöriga myndigheterna bör omfattas av en standard för skydd av personuppgifter enligt nationell rätt i linje med rådets rambeslut 2008/977/RIF ⁽¹⁾ och de särskilda krav på dataskydd som fastställs i detta direktiv. Hänvisningar till rambeslut 2008/977/RIF bör ses som hänvisningar till gällande lagstiftning och till lagstiftning som kommer att ersätta denna.
- (28) Med hänsyn till rätten till skydd för personuppgifter är det viktigt att de registrerades rättigheter vid behandling av PNR-uppgifter som rör dem, till exempel rätt till åtkomst, rättelse, radering och begränsning samt rätt till ersättning och tillgång till rättsmedel överensstämmer med både rambeslut 2008/977/RIF och den höga skyddsnivå som stadgan och Europakonventionen föreskriver.
- (29) Med hänsyn till passagerares rätt att bli informerade om behandlingen av personuppgifter bör medlemsstaterna se till att passagerare förses med korrekt, lättåtkomlig och lättbegriplig information om insamlingen av PNR-uppgifter och överföringen av dessa uppgifter till enheten för passagerarinformation samt om sina rättigheter i egenskap av registrerade.
- (30) Detta direktiv påverkar inte tillämpningen av unionsrätt och nationell rätt om principen om allmänhetens tillgång till officiella handlingar.
- (31) Överföring av PNR-uppgifter från medlemsstater till tredjeländer bör endast vara tillåten i enskilda fall och i full överensstämmelse med de bestämmelser som medlemsstaterna fastställt i enlighet med rambeslut 2008/977/RIF. För att säkerställa skyddet av personuppgifter bör sådana överföringar omfattas av kompletterande krav knutna till syftet med överföringen. De bör också omfattas av principerna om nödvändighet och proportionalitet och av den höga skyddsnivå som stadgan och Europakonventionen föreskriver.
- (32) Den nationella tillsynsmyndighet som har inrättats enligt rådets rambeslut 2008/977/RIF bör även ansvara för att meddela riktlinjer för och utöva tillsyn över tillämpningen av de bestämmelser som medlemsstaterna antar i enlighet med detta direktiv.
- (33) Detta direktiv påverkar inte medlemsstaternas möjligheter att i enlighet med nationell rätt tillhandahålla ett system för insamling och behandling av PNR-uppgifter från ekonomiska aktörer som inte är transportörer, t.ex. resebyråer och researrangörer som tillhandahåller reserelaterade tjänster, inklusive bokning av flygningar, för vilka de samlar in och behandlar PNR-uppgifter, eller från andra transportföretag än de som anges i detta direktiv, förutsatt att sådan nationell rätt är förenlig med unionsrätten.
- (34) Detta direktiv påverkar inte gällande unionsbestämmelser om formerna för utförande av gränskontroller eller unionsbestämmelser om in- och utresa från unionens territorium.
- (35) På grund av rättsliga och tekniska skillnader mellan olika nationella bestämmelser om behandling av personuppgifter, däribland PNR-uppgifter, möts lufttrafikföretagen av olika krav på vilken typ av information som ska översändas och vilka villkor som gäller för översändandet av denna information till de behöriga nationella

⁽¹⁾ Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (EUT L 350, 30.12.2008, s. 60).

myndigheterna. Dessa skillnader kan vara till skada för ett effektivt samarbete mellan de behöriga nationella myndigheterna för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Det är därför nödvändigt att på unionsnivå inrätta en gemensam rättslig ram för överföring och behandling av PNR-uppgifter.

- (36) Detta direktiv står i överensstämmelse med de grundläggande rättigheterna och principerna i stadgan, särskilt rätten till skydd av personuppgifter, rätten till respekt för privatlivet och rätten till icke-diskriminering, som skyddas genom artiklarna 8, 7 och 21 i stadgan, och bör därför genomföras i enlighet med dessa. Detta direktiv överensstämmer med principerna om dataskydd och dess bestämmelser är förenliga med rambeslut 2008/977/RIF. För att detta direktiv inte ska inkräkta på proportionalitetsprincipen kommer dess bestämmelser om dataskydd i vissa fall att vara strängare än motsvarande bestämmelser i rambeslut 2008/977/RIF.
- (37) Tillämpningsområdet för detta direktiv är så begränsat som möjligt eftersom det föreskriver att PNR-uppgifter får lagras i enheter för passagerarinformation i högst fem år, varefter de bör raderas, det föreskriver att uppgifterna bör avidentifieras genom maskering av uppgifter efter en inledande period av sex månader, och det förbjuder insamling och användning av känsliga uppgifter. För att säkerställa effektivitet och en hög nivå av dataskydd, bör medlemsstaterna se till att en oberoende nationell tillsynsmyndighet och särskilt ett dataskyddsombud ges ansvaret för att meddela riktlinjer för och övervaka på vilket sätt PNR-uppgifter behandlas. All behandling av PNR-uppgifter bör loggas eller dokumenteras i syfte att kontrollera att den är laglig, att möjliggöra självövervakning och att säkerställa uppgifternas integritet och en säker behandling. Medlemsstaterna bör också se till att passagerarna klart och tydligt informeras om insamlingen av PNR-uppgifter och om sina rättigheter.
- (38) Eftersom målen för detta direktiv, nämligen lufttrafikföretags överföring av PNR-uppgifter och behandling av dessa uppgifter för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.
- (39) I enlighet med artikel 3 i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, har Förenade kungariket och Irland meddelat att de önskar delta i antagandet och tillämpningen av detta direktiv.
- (40) I enlighet med artiklarna 1 och 2 i protokoll nr 22 om Danmarks ställning, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, deltar Danmark inte i antagandet av detta direktiv, som inte är bindande för eller tillämpligt på Danmark.
- (41) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001 ⁽¹⁾ och avgav ett yttrande den 25 mars 2011.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Syfte och tillämpningsområde

1. Detta direktiv innehåller bestämmelser om
 - a) lufttrafikföretags överföring av passageraruppgiftssamlingar (PNR-uppgifter) om passagerare på flygningar utanför EU,
 - b) behandlingen av de uppgifter som avses i led a, inbegripet medlemsstaternas insamling, användning, lagring och inbördes utbyte av dessa uppgifter.

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

2. PNR-uppgifter som samlas in i enlighet med detta direktiv får endast behandlas i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet i enlighet med artikel 6.2 a, b och c.

Artikel 2

Detta direktivs tillämpning på flygningar inom EU

1. Om en medlemsstat beslutar att tillämpa detta direktiv på flygningar inom EU, ska denna medlemsstat skriftligen meddela kommissionen detta. En medlemsstat får när som helst lämna eller återkalla ett sådant meddelande. Kommissionen ska offentliggöra detta meddelande, och en eventuell återkallelse av det, i *Europeiska unionens officiella tidning*.
2. När ett meddelande som avses i punkt 1 lämnas, ska alla bestämmelser i detta direktiv gälla för flygningar inom EU som om de vore flygningar utanför EU och för PNR-uppgifter från flygningar inom EU som om de vore PNR-uppgifter från flygningar utanför EU.
3. En medlemsstat får besluta att endast tillämpa detta direktiv på valda flygningar inom EU. När medlemsstaten fattar ett sådant beslut, ska den välja de flygningar som den anser vara nödvändiga för att efterfölja målen för detta direktiv. Medlemsstaten får när som helst besluta att ändra urvalet av flygningar inom EU.

Artikel 3

Definitioner

I detta direktiv avses med

1. *lufttrafikföretag*: ett lufttrafikföretag med giltig operativ licens eller motsvarande som ger rätt att bedriva passagerarflygtrafik,
2. *flygning utanför EU*: varje reguljär eller icke-reguljär flygning som utförs av ett lufttrafikföretag, med avgång från ett tredjeland och planerad landning på en medlemsstats territorium eller flygning från en medlemsstats territorium med planerad landning i ett tredjeland, i båda fallen inklusive eventuella mellanlandningar på territorier i medlemsstater eller tredjeländer,
3. *flygning inom EU*: varje reguljär eller icke-reguljär flygning som utförs av ett lufttrafikföretag, med avgång från en medlemsstats territorium och planerad landning på en eller flera andra medlemsstaters territorium, utan eventuella mellanlandningar på tredjeländers territorier,
4. *passagerare*: alla personer, inbegripet personer i transfer eller transit förutom besättningsmedlemmar, som transporteras eller ska transporteras med ett flygplan med lufttrafikföretagets godkännande, vilket godkännande framgår av att denna person står med på passagerarförteckningen,
5. *passageraruppgiftssamling* eller *PNR-uppgifter*: en sammanställning av för resan nödvändiga uppgifter om varje enskild passagerare som gör det möjligt för det lufttrafikföretag som sköter bokningen och andra deltagande lufttrafikföretag att behandla och kontrollera reservationen för varje resa som bokas av en person eller för en persons räkning, oavsett om uppgifterna finns i reservationssystemet, det avgångskontrollsystem som används för att checka in passagerare på flygningar eller likvärdiga system med motsvarande uppgift,
6. *reservationssystem*: lufttrafikföretagets interna system, där PNR-uppgifter samlas för hantering av reservationer,
7. *sändmetod*: den metod varigenom lufttrafikföretagen överför de PNR-uppgifter som förtecknas i bilaga I till databasen vid den myndighet som begärt dem,

8. *terroristbrott*: de brott enligt nationell rätt som avses i artiklarna 1–4 i rambeslut 2002/475/RIF,
9. *grov brottslighet*: brott som förtecknas i bilaga II vilka bestraffas med fängelse eller annan frihetsberövande åtgärd i minst tre år enligt en medlemsstats nationella rätt,
10. *avidentifiering genom maskering av uppgifter*: att göra de uppgifter som kan användas för att omedelbart identifiera den registrerade osynliga för en användare.

KAPITEL II

Medlemsstaternas skyldigheter

Artikel 4

Enhet för passagerarinformation

1. Varje medlemsstat ska inrätta eller utse en myndighet med behörighet att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet eller en avdelning inom en sådan myndighet, vilken ska fungera som medlemsstatens enhet för passagerarinformation.
2. Enheten för passagerarinformation ska ansvara för att
 - a) samla in PNR-uppgifter från lufttrafikföretagen, lagra och behandla dessa uppgifter och överföra dessa uppgifter eller resultatet av behandlingen av dem till de behöriga myndigheter som avses i artikel 7,
 - b) utbyta både PNR-uppgifter och resultatet av behandlingen av dessa uppgifter med andra medlemsstaters enheter för passagerarinformation och med Europol i enlighet med artiklarna 9 och 10.
3. Personal vid enheten för passagerarinformation kan utgöras av tjänstemän som avdelats från behöriga myndigheter. Medlemsstaterna ska ge enheterna för passagerarinformation tillräckliga resurser för att de ska kunna utföra sina uppgifter.
4. Två eller flera medlemsstater (nedan kallade *de deltagande medlemsstaterna*) får inrätta eller utse en och samma myndighet till sin gemensamma enhet för passagerarinformation. En sådan enhet för passagerarinformation ska inrättas i en av de deltagande medlemsstaterna och fungera som nationell enhet för passagerarinformation för alla deltagande medlemsstater. De deltagande medlemsstaterna ska tillsammans enas om närmare bestämmelser för driften av enheten för passagerarinformation utan att avvika från kraven i detta direktiv.
5. Varje medlemsstat ska inom en månad från inrättandet eller utseendet av sin enhet för passagerarinformation meddela kommissionen detta och får när som helst ändra detta meddelande. Kommissionen ska offentliggöra meddelandet och eventuella ändringar därav i *Europeiska unionens officiella tidning*.

Artikel 5

Dataskyddsombud vid enheten för passagerarinformation

1. Enheten för passagerarinformation ska utse ett dataskyddsombud, som ska ansvara för övervakningen av behandlingen av PNR-uppgifter och för genomförandet av relevanta skyddsåtgärder.
2. Medlemsstaterna ska förse dataskyddsombuden med de resurser som de behöver för att utföra sina uppgifter i enlighet med denna artikel på ett effektivt och oberoende sätt.
3. Medlemsstaterna ska se till att en registrerad har rätt att kontakta dataskyddsombudet, i egenskap av enda kontaktpunkt, i alla frågor som rör behandlingen av den registrerades PNR-uppgifter.

Artikel 6

Behandling av PNR-uppgifter

1. PNR-uppgifter som överförs av lufttrafikföretag ska samlas in av den berörda medlemsstatens enhet för passagerarinformation i enlighet med artikel 8. Om PNR-uppgifter som överförs av lufttrafikföretag omfattar andra uppgifter än dem som anges i bilaga I, ska enheten för passagerarinformation omedelbart och slutgiltigt radera dessa vid mottagandet.
2. Enheten för passagerarinformation ska enbart behandla PNR-uppgifterna för följande ändamål:
 - a) Göra en bedömning av passagerare före deras beräknade ankomst till eller avresa från den berörda medlemsstaten, för att identifiera personer som de behöriga myndigheterna enligt artikel 7 och i förekommande fall Europol enligt artikel 10 behöver utreda ytterligare, på grund av att dessa personer kan vara inblandade i terroristbrott eller grov brottslighet.
 - b) I enskilda fall, besvara en vederbörligen motiverad förfrågan som bygger på tillräckliga skäl från de behöriga myndigheterna om att tillhandahålla och behandla PNR-uppgifter i specifika fall i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet och tillhandahålla de behöriga myndigheterna eller, när så är lämpligt, Europol resultaten av sådan behandling.
 - c) Analysera PNR-uppgifter för att uppdatera och skapa nya kriterier som ska användas vid de bedömningar som genomförs enligt punkt 3 b, i syfte att identifiera personer som kan vara delaktiga i terroristbrott eller grov brottslighet.
3. När enheten för passagerarinformation utför den bedömning som avses i punkt 2 a får den:
 - a) Jämföra PNR-uppgifter med uppgifter i databaser som är relevanta för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet, inklusive databaser över personer eller föremål som är eftersökta eller finns uppförda på spärlista, i enlighet med unionsbestämmelser eller internationella eller nationella bestämmelser som är tillämpliga på sådana databaser, eller
 - b) behandla PNR-uppgifter i enlighet med på förhand fastställda kriterier.
4. En bedömning av passagerare före planerad ankomst till eller avresa från medlemsstaten som görs enligt punkt 3 b i enlighet med på förhand fastställda kriterier ska utföras på ett icke-diskriminerande sätt. Dessa på förhand fastställda kriterier måste vara riktade, proportionella och specifika. Medlemsstaterna ska se till att kriterierna fastställs och regelbundet ses över av enheterna för passagerarinformation i samarbete med de behöriga myndigheter som avses i artikel 7. Dessa på förhand fastställda kriterier får under inga omständigheter vara baserade på en persons ras, etniska ursprung, politiska åskådning, religiösa eller filosofiska övertygelse, fackföreningstillhörighet, hälsotillstånd, sexualliv eller sexuella läggning.
5. Medlemsstaterna ska se till att eventuella träffar i samband med automatisk behandling av PNR-uppgifter enligt punkt 2 a granskas individuellt med icke-automatiska metoder, för att verifiera huruvida den behöriga myndighet som avses i artikel 7 behöver vidta åtgärder enligt nationell rätt.
6. Enheten för passagerarinformation i en medlemsstat ska översända PNR-uppgifterna beträffande personer som har identifierats i enlighet med punkt 2 a eller resultaten av behandlingen av dessa uppgifter till de behöriga myndigheter som avses i artikel 7 i samma medlemsstat för vidare granskning. Sådana överföringar får endast göras i enskilda fall och, vid automatisk behandling av PNR-uppgifter, efter individuell icke-automatisk granskning.
7. Medlemsstaterna ska se till att dataskyddsombudet har åtkomst till alla uppgifter som enheten för passagerarinformation behandlar. Om dataskyddsombudet anser att behandlingen av vissa uppgifter inte har varit lagenlig, ska dataskyddsombudet hänskjuta ärendet till den nationella tillsynsmyndigheten.
8. Lagring, behandling och analys av PNR-uppgifter vid enheten för passagerarinformation ska uteslutande utföras på en eller flera säkra platser på en medlemsstats territorium.

9. Konsekvenserna av de bedömningar av passagerare som avses i punkt 2 a i denna artikel får inte äventyra rätten för personer som åtnjuter fri rörlighet enligt unionsrätten att resa in på den berörda medlemsstatens territorium i enlighet med Europaparlamentets och rådets direktiv 2004/38/EG ⁽¹⁾. När bedömningarna sker i samband med flygningar inom EU mellan medlemsstater för vilka Europaparlamentets och rådets förordning (EG) nr 562/2006 ⁽²⁾ är tillämplig, ska konsekvenserna av sådana bedömningar vara förenliga med den förordningen.

Artikel 7

Behöriga myndigheter

1. Varje medlemsstat ska fastställa en förteckning över de behöriga myndigheter som har befogenhet att begära eller motta PNR-uppgifter eller resultat av behandlingen av dessa uppgifter från enheten för passagerarinformation för vidare granskning av informationen eller för att vidta lämpliga åtgärder för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet.
2. De myndigheter som avses i punkt 1 ska vara myndigheter som är behöriga att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet.
3. Med avseende på tillämpningen av artikel 9.3 ska varje medlemsstat senast den 25 maj 2017 meddela kommissionen förteckningen över sina behöriga myndigheter och får när som helst ändra sitt meddelande. Kommissionen ska offentliggöra meddelandet och eventuella ändringar därav i *Europeiska unionens officiella tidning*.
4. PNR-uppgifter och resultaten av behandling av dessa uppgifter som mottas av enheten för passagerarinformation får endast vidarebehandlas av de behöriga myndigheterna i medlemsstaterna, om det specifika syftet är att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet.
5. Punkt 4 ska inte påverka de brottsbekämpande eller rättsliga myndigheternas befogenheter på nationell nivå, om andra brott eller indikationer på sådana upptäcks i samband med brottsbekämpande insatser som görs till följd av sådan behandling av PNR-uppgifter.
6. De behöriga myndigheterna får inte fatta några beslut som har negativa rättsliga konsekvenser för en person eller på annat sätt allvarligt påverkar en person endast på grund av den automatiska behandlingen av PNR-uppgifter. Besluten får inte grunda sig på en persons ras eller etniska ursprung, politiska åskådning, religiösa eller filosofiska övertygelse, fackföreningstillhörighet, hälsotillstånd, sexualliv eller sexuella läggning.

Artikel 8

Lufttrafikföretagens skyldigheter vad gäller överföring av uppgifter

1. Medlemsstaterna ska anta de åtgärder som är nödvändiga för att se till att lufttrafikföretag genom sändmetoden överför de PNR-uppgifter som förtecknas i bilaga I, förutsatt att de redan samlar in sådana uppgifter som en del av sin normala affärsverksamhet, till databasen hos enheten för passagerarinformation i den medlemsstat på vars territorium flygningen kommer att ankomma eller från det territorium varifrån flygningen kommer att avgå. Om flygningens linjebeteckning delas med ett eller flera andra lufttrafikföretag, ska det företag som utför flygningen ha skyldighet att överföra PNR-uppgifter om samtliga passagerare ombord. Om en flygning utanför EU omfattar en eller flera mellanlandningar på medlemsstaternas flygplatser, ska lufttrafikföretagen överföra PNR-uppgifterna för alla passagerare till enheterna för passagerarinformation i alla berörda medlemsstater. Detta gäller även om en flygning inom EU innebär en eller flera mellanlandningar på olika medlemsstaters flygplatser, men endast i fråga om medlemsstater som samlar in PNR-uppgifter från flygningar inom EU.

⁽¹⁾ Europaparlamentets och rådets direktiv 2004/38/EG av den 29 april 2004 om unionsmedborgares och deras familjemedlemmars rätt att fritt röra sig och uppehålla sig inom medlemsstaternas territorier och om ändring av förordning (EEG) nr 1612/68 och om upphävande av direktiven 64/221/EEG, 68/360/EEG, 72/194/EEG, 73/148/EEG, 75/34/EEG, 75/35/EEG, 90/364/EEG, 90/365/EEG och 93/96/EEG (EUT L 158, 30.4.2004, s. 77).

⁽²⁾ Europaparlamentets och rådets förordning (EG) nr 562/2006 av den 15 mars 2006 om en gemenskapskodex om gränspassage för personer (kodex om Schengengränserna) (EUT L 105, 13.4.2006, s. 1).

2. Om lufttrafikföretagen har samlat in sådan förhandsinformation om passagerare (API-uppgifter) som förtecknas i punkt 18 i bilaga I men inte lagrar denna information med hjälp av samma tekniska metoder som för andra PNR-uppgifter, ska medlemsstaterna vidta nödvändiga åtgärder för att säkerställa att lufttrafikföretagen genom sändmetoden även överför dessa uppgifter till enheten för passagerarinformation i de medlemsstater som avses i punkt 1. Vid sådan överföring ska alla bestämmelser i detta direktiv vara tillämpliga på dessa API-uppgifter.

3. Lufttrafikföretagen ska överföra PNR-uppgifter elektroniskt med användning av de gemensamma protokoll och understödda dataformat som ska antas i enlighet med det granskningsförfarande som avses i artikel 17.2 eller, vid eventuella tekniska problem, på något annat sätt som säkerställer ett lämpligt dataskydd

a) 24–48 timmar före flygningens planerade avgång, och

b) omedelbart efter det att gatens dörrar stängts, det vill säga när passagerarna har stigit ombord på planet inför avgång och passagerare inte längre tillåts stiga ombord eller stiga av.

4. Medlemsstaterna ska tillåta lufttrafikföretag att begränsa den överföring som avses i punkt 3 b till uppdateringar av sådana överföringar som avses i punkt 3 a.

5. I situationer där åtkomst till PNR-uppgifter är nödvändig för att reagera på ett specifikt och faktiskt hot med anknytning till terroristbrott eller grov brottslighet, ska lufttrafikföretag efter en bedömning i det enskilda fallet på begäran av en enhet för passagerarinformation, i enlighet med nationell rätt, överföra PNR-uppgifter vid andra tidpunkter än de som anges i punkt 3.

Artikel 9

Utbyte av information mellan medlemsstaterna

1. När personer identifieras av en enhet för passagerarinformation i enlighet med artikel 6.2, ska medlemsstaterna se till att enheten översänder alla relevanta och nödvändiga PNR-uppgifter eller resultaten av en eventuell behandling av dessa uppgifter till motsvarande enheter i de andra medlemsstaterna. Enheterna för passagerarinformation i de mottagande medlemsstaterna ska översända den mottagna informationen till sina behöriga myndigheter i enlighet med artikel 6.6.

2. Enheten för passagerarinformation i en medlemsstat ska ha rätt att vid behov begära att en enhet för passagerarinformation i en annan medlemsstat tillhandahåller PNR-uppgifter som lagras i den senares databas och ännu inte har avidentifierats genom maskering av uppgifter i enlighet med artikel 12.2 och vid behov även resultaten av en eventuell behandling av dessa uppgifter, om en sådan redan har utförts i enlighet med artikel 6.2 a. En sådan begäran ska vederbörligen motiveras. Den får avse en viss uppgift eller en kombination av sådana uppgifter, beroende på vilken information den begärande enheten för passagerarinformation anser vara nödvändig i ett särskilt fall för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet. Enheterna för passagerarinformation ska tillhandahålla den begärda informationen så snart som möjligt. Om de begärda uppgifterna har avidentifierats genom maskering av uppgifter i enlighet med artikel 12.2, ska enheten för passagerarinformation endast tillhandahålla fullständiga PNR-uppgifter, om det rimligen kan antas vara nödvändigt för de ändamål som anges i artikel 6.2 b och detta endast efter tillstånd från en behörig myndighet som avses i artikel 12.3 b.

3. Endast i nödfall och enligt de villkor som fastställts i punkt 2 får en medlemsstats behöriga myndigheter vända sig direkt till enheten för passagerarinformation i en annan medlemsstat med en begäran om utlämnande av PNR-uppgifter som finns lagrade i den enhetens databas. Begäran från de behöriga myndigheterna ska motiveras. En kopia av begäran ska alltid skickas till enheten för passagerarinformation i den begärande medlemsstaten. I alla andra fall ska de behöriga myndigheterna översända sina framställningar via enheten för passagerarinformation i den egna medlemsstaten.

4. Om åtkomst till PNR-uppgifter är nödvändig för att reagera på ett specifikt och faktiskt hot med anknytning till terroristbrott eller grov brottslighet, ska enheten för passagerarinformation i en medlemsstat i undantagsfall ha rätt att begära att enheten för passagerarinformation i en annan medlemsstat införskaffar PNR-uppgifter i enlighet med artikel 8.5 och vidarebefordrar dessa till den begärande enheten för passagerarinformation.

5. Informationsutbyte enligt denna artikel får göras via alla befintliga kanaler för samarbete mellan medlemsstaternas behöriga myndigheter. Det språk som används i samband med begäran och informationsutbytet ska vara det som gäller

för den kanal som används. Medlemsstaterna ska i samband med att de lämnar meddelanden i enlighet med artikel 4.5 även meddela kommissionen uppgifter om de kontaktpunkter till vilka framställningar kan sändas i nödfall. Kommissionen ska underrätta medlemsstaterna om dessa uppgifter.

Artikel 10

Villkor för Europols åtkomst till PNR-uppgifter

1. Europol ska inom ramen för sina befogenheter och för fullgörandet av sina arbetsuppgifter ha rätt att begära PNR-uppgifter eller resultatet av behandlingen av dessa uppgifter från enheterna för passagerarinformation i medlemsstaterna.
2. Europol får från fall till fall via Europols nationella enhet lämna in en elektronisk, vederbörligen motiverad begäran till enheten för passagerarinformation i en medlemsstat om översändande av specifika PNR-uppgifter eller resultaten av behandlingen av dessa uppgifter. Europol får lämna in en sådan begäran när detta är absolut nödvändigt för att stödja och stärka medlemsstaternas åtgärder för att förebygga, förhindra, upptäcka eller utreda ett specifikt terroristbrott eller grovt brott i den mån brottet i fråga omfattas av Europols behörighet enligt beslut 2009/371/RIF. I den motiverade begäran ska rimliga skäl anges till varför Europol anser att översändandet av PNR-uppgifterna eller resultaten av behandlingen av PNR-uppgifter väsentligt kommer att bidra till att brottet i fråga förebyggs, upptäcks eller utreds.
3. Europol ska informera det dataskyddsombud som utsetts i enlighet med artikel 28 i beslut 2009/371/RIF om varje informationsutbyte enligt den här artikeln.
4. Informationsutbyte enligt denna artikel ska äga rum via Siena och i enlighet med beslut 2009/371/RIF. Det språk som används för framställningen och informationsutbytet ska vara det som gäller för Siena.

Artikel 11

Överföring av uppgifter till tredjeländer

1. En medlemsstat får överföra PNR-uppgifter och resultaten av behandling av sådana uppgifter som lagras av enheten för passagerarinformation i enlighet med artikel 12 till ett tredjeland efter bedömning i det enskilda fallet, endast under förutsättning att
 - a) de villkor som fastställs i artikel 13 i rambeslut 2008/977/RIF är uppfyllda,
 - b) överföringen är nödvändig för detta direktivs syften enligt artikel 1.2,
 - c) det berörda tredjelandet godtar att överföra uppgifterna till ett annat tredjeland endast om det är strikt nödvändigt för detta direktivs ändamål enligt artikel 1.2 och endast efter uttryckligt samtycke av medlemsstaten, och
 - d) samma villkor som de som fastställs i artikel 9.2 är uppfyllda.
2. Trots vad som sägs i artikel 13.2 i rambeslut 2008/977/RIF ska överföring av PNR-uppgifter utan förhandssamtycke av den medlemsstat från vilken uppgifterna hämtades tillåtas i undantagsfall och endast om
 - a) överföringen är absolut nödvändig för att reagera på ett specifikt och faktiskt hot med anknytning till terroristbrott eller grov brottslighet i en medlemsstat eller ett tredjeland, och
 - b) förhandssamtycke inte kan erhållas i tid.

Den myndighet som ansvarar för att ge samtycke ska informeras utan dröjsmål och överföringen ska vederbörligen registreras samt genomgå efterhandskontroll.

3. Medlemsstaterna ska överföra PNR-uppgifter till behöriga myndigheter i tredjeländer på villkor som är förenliga med detta direktiv endast efter att ha förvässat sig om att mottagarnas planerade användning av uppgifterna är förenlig med dessa villkor och skyddsåtgärder.
4. Dataskyddsombudet vid enheten för passagerarinformation i den medlemsstat som har överfört PNR-uppgifterna ska informeras varje gång medlemsstaten överför PNR-uppgifter enligt denna artikel.

Artikel 12

Lagringstid för uppgifter och avidentifiering

1. Medlemsstaterna ska se till att PNR-uppgifter som lämnas av lufttrafikföretag till enheten för passagerarinformation lagras i en databas vid enheten under en period på fem år efter överföringen till enheten för passagerarinformation i den medlemsstat på vars territorium flygningen ankom eller avgick.
2. Vid utgången av en period på sex månader efter överföringen av de PNR-uppgifter som avses i punkt 1 ska alla PNR-uppgifter avidentifieras genom maskering av följande uppgifter, som kan användas för att omedelbart identifiera de passagerare som PNR-uppgifterna avser:
 - a) Namn, inklusive namn på andra passagerare i PNR samt antal passagerare i PNR som reser tillsammans.
 - b) Adress och kontaktuppgifter.
 - c) Alla former av betalningsinformation, inbegripet faktureringsadress, om denna innehåller uppgifter som kan användas för att omedelbart identifiera den passagerare som passageraruppgiftssamlingar avser eller andra personer.
 - d) Uppgifter om bonusprogram.
 - e) Allmänna anmärkningar, om dessa innehåller uppgifter som kan användas för att omedelbart identifiera den passagerare som passageraruppgiftssamlingar avser.
 - f) Alla API-uppgifter som samlats in.
3. Vid utgången av den sexmånadersperiod som avses i punkt 2 ska utlämnande av de fullständiga PNR-uppgifterna tillåtas endast
 - a) om det rimligen kan antas vara nödvändigt för de ändamål som avses i artikel 6.2 b, och
 - b) efter tillstånd från
 - i) en rättslig myndighet, eller
 - ii) en annan nationell myndighet som i enlighet med nationell rätt är behörig att kontrollera om villkoren för tillgång är uppfyllda, under förutsättning att dataskyddsombudet vid enheten för passagerarinformation informeras och att denne genomför en efterhandsutvärdering.
4. Medlemsstaterna ska se till att PNR-uppgifterna slutgiltigt raderas vid utgången av den period som avses i punkt 1. Denna skyldighet gäller dock inte om specifika PNR-uppgifter har överförts till en behörig myndighet och används i specifika fall i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrott eller grov brottslighet, varvid den behöriga myndighetens lagring av uppgifterna i stället ska regleras av nationell rätt.
5. Resultaten av den behandling som avses i artikel 6.2 a ska bevaras endast av enheten för passagerarinformation så länge som krävs för att informera de behöriga myndigheterna och, i enlighet med artikel 9.1, för att informera enheterna för passagerarinformation i andra medlemsstater om en träff. Även om automatisk behandling som utförs efter en sådan individuell icke-automatisk granskning som avses i artikel 6.5 inte ger någon träff, får resultatet bevaras för att undvika framtida "falska" träffar, så länge de bakomliggande uppgifterna inte har raderats enligt punkt 4 i den här artikeln.

Artikel 13

Skydd av personuppgifter

1. Medlemsstaterna ska föreskriva att alla passagerare vid all behandling av personuppgifter i enlighet med detta direktiv har samma rätt till skydd av sina personuppgifter, rätt till åtkomst, rättelse, radering och begränsning samt rätt till ersättning och tillgång till rättsmedel som fastställs i unionsrätten och nationell rätt och för genomförande av artiklarna 17, 18, 19 och 20 i rambeslut 2008/977/RIF. Dessa artiklar ska därför tillämpas.

2. Medlemsstaterna ska föreskriva att de nationella bestämmelser om konfidentiell behandling och datasäkerhet som har antagits för genomförande av artiklarna 21 och 22 i rambeslut 2008/977/RIF även är tillämpliga på all behandling av personuppgifter i enlighet med detta direktiv.

3. Detta direktiv påverkar inte tillämpligheten av Europaparlamentets och rådets direktiv 95/46/EG ⁽¹⁾ på lufttrafikföretags behandling av personuppgifter, i synnerhet deras skyldigheter att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifters säkerhet och konfidentialitet.

4. Medlemsstaterna ska förbjuda behandling av PNR-uppgifter som avslöjar en persons ras eller etniska ursprung, politiska åsikter, religion eller filosofiska övertygelse, fackföreningstillhörighet, hälsotillstånd, sexualliv eller sexuella läggning. Om enheten för passagerarinformation mottar PNR-uppgifter som avslöjar sådana uppgifter, ska dessa uppgifter omedelbart raderas.

5. Medlemsstaterna ska se till att enheten för passagerarinformation bevarar dokumentation om alla system och förfaranden för uppgiftsbehandling inom deras ansvarsområde. Dokumentationen ska minst innehålla

- a) namn och kontaktuppgifter för den organisatoriska enhet och den personal vid enheten för passagerarinformation som anförtrots behandlingen av PNR-uppgifter och de olika nivåerna av åtkomstbehörighet,
- b) begäran från behöriga myndigheter och enheter för passagerarinformation i andra medlemsstater,
- c) begäran om och överföring av PNR-uppgifter till ett tredjeland.

Enheten för passagerarinformation ska på begäran göra all dokumentation tillgänglig för den nationella tillsynsmyndigheten.

6. Medlemsstaterna ska se till att enheten för passagerarinformation för loggar över åtminstone följande typer av behandling: insamling, läsning, utlämning och radering. Loggarna över läsning och utlämning ska särskilt visa ändamål, datum och tidpunkt för sådan behandling och i möjligaste mån identitetsuppgifter för den person som har läst eller lämnat ut PNR-uppgifterna samt identitetsuppgifter för de personer som mottagit uppgifterna. Loggarna ska uteslutande användas för kontroll och självövervakning, för att säkerställa dataintegritet och datasäkerhet och för revision. Enheten för passagerarinformation ska på begäran göra loggarna tillgängliga för den nationella tillsynsmyndigheten.

Loggarna ska bevaras i fem år.

7. Medlemsstaterna ska se till att deras enhet för passagerarinformation genomför lämpliga tekniska och organisatoriska åtgärder och förfaranden för att säkerställa en så hög säkerhetsnivå som är lämplig med tanke på de risker som är förknippade med behandlingen och arten av PNR-uppgifterna.

8. Om ett en personuppgiftsincident kan antas medföra ett avsevärt hot mot skyddet av den registrerades personuppgifter eller negativt påverka dennes integritet, ska medlemsstaterna se till att enheten för passagerarinformation utan onödigt dröjsmål informerar den registrerade och den nationella tillsynsmyndigheten för dataskydd om incidenten.

Artikel 14

Sanktioner

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella bestämmelser som antagits enligt detta direktiv och vidta alla nödvändiga åtgärder för att se till att de genomförs.

Medlemsstaterna ska särskilt fastställa bestämmelser om sanktioner, inklusive ekonomiska sanktioner, mot lufttrafikföretag som inte översänder uppgifter i enlighet med artikel 8 eller som inte översänder uppgifterna i det fastställda formatet.

Sanktionerna ska vara effektiva, proportionella och avskräckande.

⁽¹⁾ Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).

Artikel 15

Nationell tillsynsmyndighet

1. Varje medlemsstat ska föreskriva att den nationella tillsynsmyndighet som avses i artikel 25 i rambeslut 2008/977/RIF ska ansvara för att inom sitt territorium ge riktlinjer för och övervaka tillämpningen av de bestämmelser som medlemsstaterna antar i enlighet med detta direktiv. Artikel 25 i rambeslut 2008/977/RIF ska tillämpas.
2. De nationella tillsynsmyndigheterna ska utföra sina uppgifter enligt punkt 1 i syfte att skydda grundläggande rättigheter i samband med behandling av personuppgifter.
3. Varje nationell tillsynsmyndighet ska
 - a) hantera klagomål från en registrerad, undersöka ärendet och inom rimlig tid informera de registrerade om förloppet för och resultatet av dennes klagomål,
 - b) kontrollera att uppgiftsbehandlingen är laglig, genomföra utredningar, inspektioner och revision i enlighet med nationell rätt, antingen på eget initiativ eller på grundval av ett klagomål som avses i led a.
4. Varje nationell tillsynsmyndighet ska på begäran ge registrerade råd om hur de kan utöva de rättigheter som fastställs i de bestämmelser som antas i enlighet med detta direktiv.

KAPITEL III

Genomförandeåtgärder

Artikel 16

Gemensamma protokoll och understödda dataformat

1. All överföring av PNR-uppgifter från lufttrafikföretag till enheter för passagerarinformation inom ramen för detta direktiv ska göras med elektroniska medel som tillhandahåller tillräckliga garantier med avseende på de tekniska säkerhetsåtgärder och de organisatoriska åtgärder som styr den behandling som ska utföras. I händelse av tekniska problem får PNR-uppgifterna överföras på annat lämpligt sätt under förutsättning att samma säkerhetsnivå upprätthålls och att unionsrätten om dataskydd respekteras fullt ut.
2. Ett år från den dag då kommissionen för första gången antar gemensamma protokoll och understödda dataformat i enlighet med punkt 3, ska all överföring av PNR-uppgifter från lufttrafikföretag till enheter för passagerarinformation inom ramen för detta direktiv göras på elektronisk väg med användning av säkra metoder i överensstämmelse med dessa godkända gemensamma protokoll. Dessa protokoll ska vara gemensamma för alla överföringar, så att PNR-uppgifternas säkerhet under överföringen tryggas. PNR-uppgifterna ska överföras i ett understött dataformat, för att säkerställa att de kan läsas av alla berörda parter. Alla lufttrafikföretag ska bestämma vilket gemensamt protokoll och vilket dataformat de avser att använda för sina överföringar och underrätta enheten för passagerarinformation om detta.
3. En förteckning över gemensamma protokoll och understödda dataformat ska upprättas och vid behov anpassas av kommissionen genom genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 17.2.
4. Punkt 1 ska tillämpas så länge som de gemensamma protokoll och understödda dataformat som avses i punkterna 2 och 3 inte finns tillgängliga.
5. Inom ett år från den dag då de gemensamma protokoll och understödda dataformat som avses i punkt 2 antas, ska medlemsstaterna vidta de tekniska åtgärder som krävs för att dessa gemensamma protokoll och dataformat ska kunna börja användas.

*Artikel 17***Kommittéförfarande**

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i Europaparlamentets och rådets förordning (EU) nr 182/2011.
2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

Om kommittén inte avger något yttrande, ska kommissionen inte anta utkastet till genomförandeakt och artikel 5.4 tredje stycket i förordning (EU) nr 182/2011 ska tillämpas.

*KAPITEL IV***Slutbestämmelser***Artikel 18***Införlivande**

1. Medlemsstaterna ska sätta i kraft de bestämmelser i lagar och andra författningar som är nödvändiga för att följa detta direktiv senast den 25 maj 2018. De ska genast underrätta kommissionen om detta.

När en medlemsstat antar dessa bestämmelser ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

2. Medlemsstaterna ska till kommissionen överlämna texterna till de centrala bestämmelser i nationell rätt som de antar inom det område som omfattas av detta direktiv.

*Artikel 19***Översyn**

1. På grundval av information som medlemsstaterna tillhandahållit, inbegripet de statistiska uppgifter som avses i artikel 20.2, ska kommissionen senast den 25 maj 2020 göra en översyn av samtliga delar av detta direktiv och överlämna till och lägga fram en rapport för Europaparlamentet och rådet.

2. Kommissionen ska, när den utför sin översyn, lägga särskild vikt vid
 - a) efterlevnaden av de tillämpliga standarderna för skydd av personuppgifter,
 - b) nödvändigheten och proportionaliteten i insamlingen och behandlingen av PNR-uppgifter för vart och ett av de syften som fastställs i detta direktiv,
 - c) längden på den period som uppgifterna lagras,
 - d) ändamålsenligheten i informationsutbytet mellan medlemsstaterna, och
 - e) kvaliteten på bedömningarna, även med hänsyn till den statistik som samlats in i enlighet med artikel 20.

3. Den rapport som avses i punkt 1 ska också innefatta en översyn av nödvändigheten, proportionaliteten och ändamålsenligheten i att i detta direktivs tillämpningsområde inbegripa obligatorisk insamling och överföring av PNR-uppgifter avseende samtliga eller utvalda flygningar inom EU. Kommissionen ska beakta medlemsstaternas erfarenheter, särskilt de medlemsstater som tillämpar detta direktiv på flygningar inom EU i enlighet med artikel 2. Rapporten ska också beakta huruvida det är nödvändigt att låta ekonomiska aktörer som inte är trafikföretag, t.ex. resebyråer och researrangörer som tillhandahåller reserelaterade tjänster, inklusive bokning av flygningar, omfattas av detta direktivs tillämpningsområde.

4. Mot bakgrund av den översyn som genomförs i enlighet med denna artikel, ska kommissionen om lämpligt lägga fram ett lagstiftningsförslag för Europaparlamentet och rådet i syfte att ändra detta direktiv.

Artikel 20

Statistik

1. Medlemsstaterna ska årligen tillhandahålla kommissionen statistik om PNR-uppgifter som lämnats till enheterna för passagerarinformation. Sådan statistik får inte innehålla några personuppgifter.
2. Statistiken ska åtminstone omfatta följande:
 - a) Det totala antalet passagerare vars PNR-uppgifter samlats in och utbyts.
 - b) Antalet passagerare som identifierats för ytterligare undersökning.

Artikel 21

Förhållande till andra instrument

1. Medlemsstaterna får fortsätta att sinsemellan tillämpa de bilaterala eller multilaterala avtal eller ordningar som är i kraft den 24 maj 2016 på utbyte av uppgifter mellan behöriga myndigheter, förutsatt att dessa avtal eller ordningar är förenliga med detta direktiv.
2. Detta direktiv påverkar inte tillämpligheten av direktiv 95/46/EG på lufttrafikföretags behandling av personuppgifter.
3. Detta direktiv påverkar inte medlemsstaternas eller unionens eventuella skyldigheter och åtaganden enligt bilaterala eller multilaterala avtal med tredjeländer.

Artikel 22

Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Detta direktiv riktar sig till medlemsstaterna i enlighet med fördragen.

Utfärdat i Bryssel den 27 april 2016.

På Europaparlamentets vägnar
M. SCHULZ
Ordförande

På rådets vägnar
J.A. HENNIS-PLASSCHAERT
Ordförande

BILAGA I

PNR-uppgifter som samlas in av lufttrafikföretag

1. PNR-uppgifternas lokaliseringskod.
2. Datum för bokning/utfärdande av biljett.
3. Planerat/planerade resdatum.
4. Namn.
5. Adress och kontaktuppgifter (telefonnummer och e-postadress).
6. Alla former av betalningsinformation, inbegripet faktureringsadress.
7. Hela resrutten för aktuell passageraruppgiftssamling.
8. Uppgifter om bonusprogram.
9. Resebyrå/resebyråtjänsteman.
10. Passagerarens resestatus, inbegripet resebekräftelser, incheckningsstatus, no show (passagerare som inte infinner sig) eller go show (passagerare utan bokning).
11. Delade PNR-uppgifter.
12. Allmänna anmärkningar (inklusive alla tillgängliga uppgifter om ensamkommande barn under 18 år, såsom namn och kön, ålder, språkkunskaper, namn och kontaktuppgifter för den person som följer barnet till incheckning för avresan och denna persons förhållande till barnet, namn och kontaktuppgifter för den person som hämtar barnet vid ankomsten och denna persons förhållande till barnet, flygplatsanställd som ledsagar barnet vid avresan respektive ankomsten).
13. Biljettinformation, inbegripet biljettnummer, datum för utfärdande av biljetten, enkelbiljetter och automatisk biljettprisuppgift.
14. Platsnummer och annan platsinformation.
15. Information om gemensam linjebeteckning.
16. All bagageinformation.
17. Antal medresenärer i PNR-uppgifterna samt deras namn.
18. Eventuell förhandsinformation (API) som samlats in (inklusive typ av identitetshandling, identitetshandlingens nummer, utfärdandeland och sista giltighetsdag, efternamn, förnamn, kön, födelsedatum, lufttrafikföretag, flygnummer, utresedatum, ankomstdatum, avresehamn, ankomsthavn, avresetid och ankomsttid).
19. Alla ändringar som gjorts av de PNR-uppgifter som anges i punkterna 1–18.

BILAGA II

Förteckning över brott enligt artikel 3.9

1. Deltagande i en kriminell organisation.
 2. Människohandel.
 3. Sexuellt utnyttjande av barn samt barnpornografi.
 4. Olaglig handel med narkotika och psykotropa ämnen.
 5. Olaglig handel med vapen, ammunition och sprängämnen.
 6. Korruption.
 7. Bedrägeri, inbegripet riktat mot unionens finansiella intressen.
 8. Penningtvätt och penningförfalskning, inklusive förfalskning av euron.
 9. It-brottslighet/cyberbrottslighet.
 10. Miljöbrott, inbegripet olaglig handel med hotade djurarter och hotade växtarter och växtsorter.
 11. Hjälptill olovlig inresa och olovlig vistelse.
 12. Mord, grov misshandel.
 13. Olaglig handel med mänskliga organ och vävnader.
 14. Människorov, olaga frihetsberövande och tagande av gisslan.
 15. Organiserad stöld och väpnat rån.
 16. Olaglig handel med kulturföremål, inbegripet antikviteter och konstverk.
 17. Varumärkesförfalskning och piratkopiering.
 18. Förfalskning av administrativa dokument och handel med sådana förfalskningar.
 19. Olaglig handel med hormonsubstanser och andra tillväxsubstanser.
 20. Olaglig handel med nukleära och radioaktiva ämnen.
 21. Våldtäkt.
 22. Brott som omfattas av den internationella brottmålsdomstolens behörighet.
 23. Kapning av flygplan eller fartyg.
 24. Sabotage.
 25. Handel med stulna fordon.
 26. Industrispionage.
-

ISSN 1977-0820 (elektronisk utgåva)
ISSN 1725-2628 (pappersutgåva)



Europeiska unionens publikationsbyrå
2985 Luxemburg
LUXEMBURG

SV