Datainspektionen informerar

Nr 2/2017

Allmänna råd

Information till landskapsmyndigheter och kommunala myndigheter om EU:s dataskyddsreform.

Datainspektionen

den 3 mars 2017

Datainspektionen • Elverksgatan 10, AX-22100 Mariehamn, Åland • Besöksadress: Kvarteret iTiden
+358 (0)18 25 550 • +358 (0)457 34 320 81 • inspektion@di.ax • www.di.ax

Bakgrund

Den **25 maj 2018** träder EU:s dataskyddsförordning (EU 2016/679) i kraft. Förordningen innehåller omfattande krav och åligganden, med syftet att skapa ett så gott skydd som möjligt för enskilda personers integritet och rättssäkerhet.

EU:s dataskyddsförordning handlar om behandling av personuppgifter. Med **personuppgifter** menas varje upplysning som avser en identifierad eller identifierbar fysisk person. Med **behandling** avses en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, 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.

Alla myndigheter ägnar sig åt behandling av personuppgifter. Myndigheternas behandling av personuppgifter sker på ett stort antal olika sätt. Det är viktigt för myndigheterna att förskaffa sig ingående kunskaper beträffande hur personuppgifter ska behandlas.

För att myndigheterna ska kunna tillämpa EU:s dataskyddsförordning direkt när den träder i kraft behövs det att de redan nu:

1) gör en bedömning av vilka **tekniska och organisatoriska åtgärder** som behövs för deras dataskydd och
2) överväger vilka **materiella och personella resurser** som krävs för att dataskyddsförordningen ska kunna efterlevas.

Dataskyddsförordningen kommer att kompletteras med **landskapslagstiftning**. Landskapsregeringens lagberedning har den 21 december 2016 (beslut vid enskild föredragning, Regeringskansliets allmänna byrå, rättserviceenheten, protokoll nr 72) fått i uppdrag att utforma ett förslag till ny lagstiftning om dataskydd. Det är eftersträvansvärt att lagförslaget färdigställs i god tid före dataskyddsförordningens ikraftträdande.

Vidare kommer en grupp bestående av EU-ländernas nationella dataskyddsmyndigheter (utsedd i enlighet med artikel 29 i EU:s dataskyddsdirektiv från den 24 oktober 1995) att utarbeta **vägledningar** som preciserar kraven som ställs i dataskyddsförordningen. Den 13 december 2016 har gruppen antagit vägledningar angående dataportabilitet (Guidelines on the right to data portability), dataskyddsombud (Guidelines on Data Protection Officers) och ansvariga tillsynsmyndigheter (Guidelines for identifying a controller or processor's lead supervisory authority).

Till **Datainspektionens uppgifter** enligt 1 § 2 mom. landskapslagen om Datainspektionen (2007:89) hör bland annat att följa den allmänna utvecklingen inom sitt verksamhetsområde och ta nödvändiga initiativ samt att ge anvisningar och råd om behandlingen av personuppgifter. Datainspektionen utfärdade den 1 september 2016 en checklista för att stöda myndigheter och andra organisationer i deras förberedandearbete inför EU-dataskyddsförordningens ikraftträdande i maj 2018 (Dnr 14-2016). Den följande informationen, som är avsedd att komplettera den tidigare utfärdade checklistan, syftar främst till att påkalla uppmärksamhet vid behovet av att myndigheterna vidtar stora

ansträngningar för att efterleva de nya kraven. Mer information, med fler detaljer kring hur dataskyddsförordningen ska tillämpas, kommer att lämnas senare.

Det är önskvärt att tjänstemän, som är ansvariga för behandlingen av personuppgifter vid de olika myndigheterna, sätter sig in i det bifogade utdraget ur dataskyddsförordningen.

Den följande informationen är allmänt hållen. Särregler kan gälla för viss verksamhet.

Utseende av dataskyddsombud

Det följer av artikel 37.1 a) i EU:s dataskyddsförordning att landskapsmyndigheter och kommunala myndigheter måste ha dataskyddsombud. Dataskyddsombudet ska, enligt artikel 37.5, utses på grundval av yrkesmässiga kvalifikationer och sakkunskap om lagstiftning och praxis avseende dataskydd. Det är önskvärt att dataskyddsombudet väljs med stor omsorg. Enligt vägledningen om dataskyddsombud från den 13 december 2016 ska dataskyddsombudet ha:

- expertkunskaper beträffande nationella och europeiska dataskyddsbestämmelser och dataskyddspraxis samt djupa kunskaper beträffande EU:s dataskyddsförordning,
- kännedom om myndighetens organisation,
- tillräckliga kunskaper om databehandlingen som myndigheten utför samt IT-systemet, datasäkerheten och dataskyddet som myndigheten behöver,
- gedigna kunskaper om regelverket som tillämpas i myndighetens verksamhet samt
- integritet och högtstående yrkesetik.

Flera myndigheter kan i enlighet med artikel 37.3 ha ett dataskyddsombud tillsammans, om det är lämpligt med hänsyn till deras organisationsstruktur och storlek. Det förefaller rationellt att flera åländska kommuner skulle ha ett gemensamt dataskyddsombud och att flera av landskapets fristående myndigheter skulle dela på ett dataskyddsombud eller använda sig av landskapsregeringens dataskyddsombud. Vid bedömningen, av hur stort arbetsområde ett och samma dataskyddsombud kan ha, gäller det dock att beakta att arbetsbördan inte får bli oskäligt stor och att det inte får bli orealistiskt svårt för dataskyddsombudet att förvärva tillräcklig kännedom om alla de berörda myndigheternas databehandling av personuppgifter och om alla författningar som inverkar på den aktuella hanteringen av personuppgifter.

Det är möjligt att antingen ha ett anställt dataskyddsombud eller att anlita ett dataskyddsombud genom ett uppdragsavtal (artikel 37.6).

Till uppgifterna för en myndighets dataskyddsombud hör bland annat att ge råd och information inom myndigheten angående de gällande dataskyddsbestämmelserna, att övervaka efterlevnaden av dataskyddsförordningen, andra dataskyddsbestämmelser samt myndighetens strategi för skydd av personuppgifter och att samarbeta med Datainspektionen (artikel 39). Enligt artikel 35:2 ska myndigheten rådfråga sitt dataskyddsombud vid genomförande av konsekvensbedömningar för databehandling som sannolikt leder till hög risk för människors rättigheter och friheter.

Personer, vars personuppgifter registrerats, har enligt artikel 38.4 rätt att kontakta dataskyddsombudet angående alla frågor som rör behandlingen av deras personuppgifter och utövandet av deras rättigheter enligt dataskyddsförordningen.

I enlighet med artikel 38.1-3 ska myndigheten

- säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter,
- stödja dataskyddsombudet i hans eller hennes uppgifter genom att tillhandahålla resurserna som krävs för att fullgöra uppgifterna, genom att ge tillgång till personuppgifter och behandlingsförfaranden samt genom att upprätthålla dataskyddsombudets sakkunskap,
- säkerställa att dataskyddsombudet inte tar emot instruktioner från utomstående personer beträffande utförandet av sina uppgifter,
- avhålla sig från att säga upp eller avskeda dataskyddsombudet eller att på annat sätt bestraffa dataskyddsombudet för att han eller hon har utfört sina uppgifter
- samt låta dataskyddsombudet rapportera direkt till myndighetens högsta förvaltningsnivå.

Dataskyddsombudet får fullgöra även andra uppgifter och uppdrag, utöver sin uppgift som dataskyddsombud, men de andra uppgifterna och uppdragen får inte medföra att dataskydds-ombudet hamnar i en intressekonflikt (artikel 38.6).

Dataskyddsombuden har en mycket viktig funktion. Det är nödvändigt att se till att de har tillräcklig tid avsatt för att utföra sina uppdrag på ett bra sätt.

Tekniska och organisatoriska åtgärder för data-skydd

I enlighet med artikel 21.1 i EU:s dataskyddsförordning ska myndigheterna genomföra lämpliga tekniska och organisatoriska åtgärder för att uppfylla kraven i förordningen och för att skydda de registrerade personernas rättigheter. Därvid ska myndigheterna beakta:

- den senaste utvecklingen (state of the art),
- kostnaderna för genomförandet,
- behandlingens art, omfattning, sammanhang och ändamål samt
- riskerna av varierande sannolikhetsgrad och allvar för människors rättigheter och friheter.

Myndigheterna ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att behandling enbart sker av sådana personuppgifter som är nödvändiga för det specifika ändamålet med behandlingen (artikel 25:2). Denna skyldighet gäller:

- mängden insamlade personuppgifter,
- behandlingens omfattning,
- tiden för personuppgifternas lagring samt
- personuppgifternas tillgänglighet (framför allt så att personuppgifterna inte utan den berörda personens medverkan görs tillgängliga för ett obegränsat antal andra personer).

Myndigheterna behöver göra en genomgång av vilka personuppgifter som behandlas för att försäkra sig om att den ovannämnda begränsningen faktiskt efterlevs. Vidare behöver myndigheten se till att all personal, som arbetar med databehandling av personuppgifter, känner till hur begränsningen ska göras.

För behandlingen av personuppgifterna ska myndigheterna, enligt artikel 32:1, vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en **säkerhetsnivå** som är lämplig i förhållande till riskerna. Även vid bedömningen av vad som är en lämplig säkerhetsnivå ska myndigheterna beakta:

- den senaste utvecklingen (state of the art),
- kostnaderna för genomförandet,
- behandlingens art, omfattning, sammanhang och ändamål samt
- riskerna av varierande sannolikhetsgrad och allvar för människors rättigheter och friheter.

Säkerhetsnivån ska, enligt artikel 32:1, i lämpliga fall inkludera:

a) **pseudonymisering** (behandling av personuppgifter på ett sådant sätt att personuppgifterna inte längre kan tillskrivas en specifik person utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och inte kan kopplas samman med någon specifik person) och kryptering av personuppgifter,
b) möjlighet att fortlöpande säkerställande av **konfidentialitet, integritet, tillgänglighet** och **motståndskraft** hos behandlingssystemen och behandlingstjänsterna,
c) möjlighet 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 åtgärderna som ska säkerställa behandlingens säkerhet.

Vid bedömningen av vad som är lämplig säkerhetsnivå ska särskild hänsyn tas till risken för oavsiktlig eller olaglig förstöring, förlust eller ändring och obehörigt röjande av eller obehörig åtkomst till personuppgifter som överförts, lagrats eller behandlats på annat sätt (artikel 32:2). Ju viktigare personuppgifterna är för den enskilde, desto högre säkerhetsnivå kan krävas. Om förstörande eller ändring av personuppgifterna har stora ekonomiska eller personliga konsekvenser för de berörda personerna, kan det förstås förväntas av myndigheten att det ska finnas en mycket hög säkerhetsnivå.

Den ovannämnda bedömningen behöver göras ytterst omsorgsfullt. Det är olyckligt om det införskaffas dyr utrustning eller dyra program, som behöver bytas ut på grund av att de inte håller en tillräckligt hög säkerhetsstandard.

När datautrustning eller dataprogram upphandlas är det mycket viktigt att säkerställa att de uppfyller dataskyddsförordningens krav. I anbudsförfrågans kravspecifikation behöver det framgå att det upphandlade måste tillgodose myndighetens behov av att efterleva förordningen.

Information till dem vars personuppgifter har insamlats

Efter att en person har lämnat sina personuppgifter till en myndighet, ska myndigheten enligt artikel 13 i EU:s dataskyddsförordning lämna följande information till henne eller honom:

1 a) Kontaktuppgifter för myndigheten.
1 b) Kontaktuppgifter för myndighetens dataskyddsombud.
1 c) Ändamålen med behandlingen av personuppgifterna samt den rättsliga grunden för behandlingen (exempelvis samtycke från den berörda personen eller att behandlingen är nödvändig för att myndigheten ska kunna fullgöra en rättslig förpliktelse, skydda intressen som är av grundläggande betydelse för någon person, utföra någon uppgift av allmänt intresse eller bedriva myndighetsutövning).
1 d) Uppgift om eventuella berättigade intressen hos myndigheten eller någon annan, vilka gör behandlingen av personuppgifterna nödvändig, om detta är den rättsliga grunden för behandlingen.
1 e) Personuppgifternas mottagare.
1 f) Eventuell uppgift om att myndigheten har för avsikt att överföra personuppgifterna till något annat land.
2 a) Uppgift om under vilken tidsperiod som personuppgifterna kommer att lagras eller om kriterierna som ska användas för att bestämma tidsperioden.
2 b) Information om att det föreligger en rätt att begära tillgång till sina personuppgifter, att rätta eller radera sina personuppgifter, att begränsa behandlingen av ens personuppgifter, att invända mot behandling av personuppgifter samt en rätt till dataportabilitet (d.v.s. rätt att få ut personuppgifter och att överföra dessa uppgifter till en annan myndighet eller organisation i ett strukturerat, allmänt använt och maskinläsbart format).
2 c) I sådana fall då behandlingen baseras på samtycke, uppgift om att det går att återkalla sitt samtycke när som helst.
2 d) Information om att det föreligger en rätt att inge klagomål till Datainspektionen.
2 e) En uppgift beträffande huruvida det finns någon lag eller något avtal som kräver att personuppgifter lämnas.
2 f) Uppgift om eventuellt automatiserat beslutsfattande samt om dess betydelse och om dess förutsedda följder för den registrerade personen.

Om myndigheten i något senare skede vill behandla de insamlade personuppgifterna för något annat syfte än syftet som myndigheten redan har informerat om, måste myndigheten i enlighet med artikel 13.3 lämna ut information till de berörda personerna om det nya syftet samt om omständigheterna som nämns i 2 a) - 2 f).

Efter att personuppgifter har lämnats till en myndighet av någon annan än den berörda personen, ska myndigheten enligt artikel 14 i dataskyddsförordningen lämna följande information till den berörda personen:

1 a) Kontaktuppgifter för myndigheten.
1 b) Kontaktuppgifter för myndighetens dataskyddsombud.
1 c) Ändamålen med behandlingen av personuppgifterna samt den rättsliga grunden för behandlingen (exempelvis samtycke från den berörda personen eller att behandlingen är nödvändig för att myndigheten ska kunna fullgöra en rättslig

förpliktelse, skydda intressen som är av grundläggande betydelse för någon person, utföra någon uppgift av allmänt intresse eller bedriva myndighetsutövning).
1 d) Uppgift om vilka kategorier av uppgifter som behandlingen gäller.
1 e) Personuppgifternas mottagare.
1 f) Eventuell uppgift om att myndigheten har för avsikt att överföra personuppgifterna till något annat land.
2 a) Uppgift om under vilken tidsperiod som personuppgifterna kommer att lagras eller om kriterierna som ska användas för att bestämma tidsperioden.
2 b) Uppgift om eventuella berättigade intressen hos myndigheten eller någon annan, vilka gör behandlingen av personuppgifterna nödvändig enligt artikel 6:1 f.
2 c) Information om att det föreligger en rätt att begära tillgång till sina personuppgifter, att rätta eller radera sina personuppgifter, att begränsa behandlingen av ens personuppgifter, att invända mot behandling av personuppgifter samt en rätt till dataportabilitet.
2 d) I sådana fall då behandlingen baseras på samtycke, uppgift om att det går att återkalla sitt samtycke när som helst.
2 e) Information om att det föreligger en rätt att inge klagomål till Datainspektionen.
2 f) Uppgift om varifrån personuppgifterna kommer, varvid det ska anges om informationen kommer från allmänt tillgängliga källor.
2 g) Uppgift om eventuellt automatiserat beslutsfattande samt om dess betydelse och om dess förutsedda följder för den registrerade personen.

Om myndigheten i något senare skede vill behandla de insamlade personuppgifterna för något annat syfte än syftet som myndigheten redan har informerat om, måste myndigheten i enlighet med artikel 14.4 lämna ut information till de berörda personerna om det nya syftet samt om omständigheterna som nämns i 2 a) - 2 g).

Den ovannämnda informationen behöver, enligt artikel 13.4 och artikel 14.5 a, inte lämnas till personer som redan har tillgång till informationen.

Till personer som inte har lämnat sina personuppgifter själva behöver information inte ges:

- om det är omöjligt att ge informationen eller om det skulle medföra en oproportionell ansträngning att göra det,
- om erhållande eller utlämnande av uppgifter uttryckligen föreskrivs i EU-rätten eller i den nationella rätten, som den registrerade personen omfattas av och som fastställer lämpliga åtgärder för att skydda den registrerade personens berättigade intressen
- eller om personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt, som föreskrivs i EU-rätten eller i tillämplig lagstiftning (artikel 14.5 b-d).

Enligt artikel 12.1 ska informationen vara koncis, begriplig, klar och tydlig. Ett klart och tydligt språk ska användas, särskilt när informationen är riktad till barn. Informationen ska tillhandahållas skriftligt eller på något annat sätt. Om det är lämpligt kan informationen tillhandahållas elektroniskt. Muntlig information kan tillhandahållas när den berörda personen begär det.

Informationen, som ska lämnas ut, är tämligen utförlig. Det är önskvärt att myndigheterna så snart som möjligt gör klart för sig alla olika fall då det behöver lämnas ut information samt förbereder mallar för informationen som ska lämnas ut.

Särskilda krav vid behandling som medför stora integritetsrisker

All behandling av personuppgifter är inte lika känslig för människorna vars personuppgifter behandlas. Viss behandling av personuppgifter är självklar och skadar uppenbart inte de registrerade personerna. Det är dock viktigt att myndigheterna noga begrundar sådana åtgärder som kan utgöra en stor risk för enskilda personers integritet.

I artikel 35:1 i EU:s dataskyddsförordning föreskrivs att myndigheter ska göra **konsekvens-bedömningar** 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 människors rättigheter och friheter. Enligt artikel 35:3 krävs konsekvensbedömningar avseende dataskydd särskilt vid:

A. systematisk och omfattande bedömning, på grundval av automatisk behandling, av människors personliga omständigheter, när bedömningen kan leda till rättsliga följder eller påverka personerna på liknande sätt,
B. behandling i stor omfattning av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en person, uppgifter om hälsa eller uppgifter om en persons sexualliv eller sexuella läggning.
C. systematisk övervakning av en allmän plats i stor omfattning (kameraövervakning).

Vid bedömningen av vilka förfaranden som utgör en hög risk för människors rättigheter och friheter är det lämpligt att tänka på att 10 § Finlands grundlag föreskriver att vars och ens **privatliv** och **heder** är tryggade. Om ett förfarande sannolikt innebär ett intrång i människors privatliv och hotar deras heder, utgör det rimligen en hög risk för deras rättigheter och friheter.

Beträffande artikel 35:1 b) kan det framhållas att även om myndigheterna naturligtvis inte för förteckningar som enbart tar upp sådana omständigheter som etniskt ursprung, åsikter, övertygelse, fackföreningstillhörighet, hälsa, sexualliv eller sexuell läggning, så kan den typen av uppgifter eventuellt ändå finnas registrerade på sådant sätt att de lätt skulle kunna tas fram. Exempel på sådana känsliga uppgifter som registreras är uppgifter om avdrag för fackföreningsavgifter, vilka registreras vid myndigheternas lönekontor och uppgifter om medlemsskap i den evangelisk-lutherska kyrkan eller annat trossamfund, vilka registreras av de kommunala grundskolorna vid inskrivningen av elever.

Datainspektionen kommer, i enlighet med artikel 35:4, att upprätta och offentliggöra en förteckning över behandlingsverksamheter som omfattas av kravet på konsekvensbedömning avseende dataskydd.

Enligt artikel 35:7 ska en konsekvensbedömning innehålla:

A. en systematisk beskrivning av den planerade personuppgiftsbehandlingen och behandlingens syften,
B. en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,
C. en bedömning av vilka risker som det finns för de registrerades rättigheter och friheter samt

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 dataskyddsförordningen efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

Enligt artikel 35.9 ska myndigheten, när det är lämpligt, inhämta synpunkter om den planerade behandlingen från de berörda personerna. Det kan troligen vara lämpligt att inhämta synpunkter beträffande planerad kameraövervakning från dem som kan komma att beröras av övervakningen.

Det finns ett krav i artikel 36:1 på att **myndigheten samråder med Datainspektionen** innan den aktuella databehandlingen påbörjas, om konsekvensbedömningen visar att databehandlingen utan riskminskande åtgärder leder till en hög risk. Det kan vara lämpligt att kontakta Datainspektionen för att diskutera huruvida förhandssamråd behövs.

I anslutning till förhandssamrådet kan Datainspektionen i enlighet med artikel 36:2 ge skriftliga råd till myndigheten som den samråder med samt har enligt artikel 58 möjlighet till att bland annat:

- utfärda en varning till myndigheten om att den planerade behandlingen av personuppgifter sannolikt kommer att bryta mot bestämmelserna i dataskyddsförordningen,
- förelägga myndigheten att se till att behandlingen sker i enlighet med bestämmelserna i dataskyddsförordningen,
- införa en tillfällig eller permanent begränsning av eller ett förbud mot behandling och
- påföra administrativa sanktionsavgifter som ska vara effektiva, proportionella och avskräckande.

Åtgärder vid personuppgiftsincidenter

Vid behandling av personuppgifter kan det inträffa personuppgiftsincidenter, d.v.s. säkerhetsincidenter 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.

I enlighet med artikel 33.1 i EU:s dataskyddsförordning måste myndigheterna **anmäla personuppgiftsincidenter till Datainspektionen** utan onödigt dröjsmål och om så är möjligt inte senare än **inom 72 timmar** efter att personuppgiftsincidenterna har kommit till myndighetens kännedom.

Det kan hända att en myndighet kl 14 på skärtorsdagen upptäcker att en utomstående person av misstag har fått tillgång till sekretessbelagda personuppgifter i ett register. Myndigheten bör då anmäla personuppgiftsincidenten till Datainspektionen före kl 14 på påskdagen. För att kunna göra anmälningar inom 72 timmar behöver myndigheterna planera sin verksamhet på sådant sätt att det när som helst under året ska finnas någon person som tillräckligt snabbt kan utreda och anmäla en personuppgiftsincident.

Anmälan till datainspektionen ska enligt artikel 33.3 innehålla:

E. personuppgiftsincidentens art, inbegripet om så är möjligt uppgifter om vilka kategorier av registrerade personer som berörs, vilket ungefärligt antal registrerade som berörs, vilka kategorier av personuppgifter som berörs och vilket ungefärligt antal personuppgifter som berörs,
F. dataskyddsombudets namn och kontaktuppgifter eller andra kontaktpunkter där mer information kan erhållas,
G. de sannolika konsekvenserna av personuppgiftsincidenten,
H. en beskrivning av åtgärderna som myndigheten har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet åtgärder som mildrar personuppgiftsincidentens potentiella negativa effekter.

Skulle det vara osannolikt att personuppgiftsincidenten medför en risk för människors rättigheter och skyldigheter, behöver den enligt artikel 33.1 inte anmälas. Om det i en konkret situation föreligger någon osäkerhet kring huruvida en anmälan behöver göras eller inte, är det lämpligt att kontakta Datainspektionen.

Myndigheten ska enligt artikel 33.5 **dokumentera alla personuppgiftsincidenter**, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och vilka korrigerande åtgärder som har vidtagits.

Om personuppgiftsincidenten sannolikt leder till en hög risk för någon persons rättigheter och friheter ska myndigheten utan onödigt dröjsmål informera den berörda personen om personuppgiftsincidenten (artikel 34:1). Informationen till den berörda personen ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art, dataskyddsombudets namn och kontaktuppgifter eller andra kontaktpunkter där mer information kan erhållas, de sannolika konsekvenserna av personuppgiftsincidenten samt en beskrivning av åtgärderna som myndigheten har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet åtgärder som mildrar personuppgiftsincidentens potentiella negativa effekter.(artikel 34:2). Skulle information direkt till den berörda personen innebära en oproportionell ansträngning, ska informationen om personuppgiftsincidenten i stället gå ut till allmänheten (artikel 34:3 c). Ett sådant förfarande kan vara tänkbart när myndigheten saknar kontaktuppgifter till personerna som berörs av personuppgiftsincidenten.

En personuppgiftsincident kan upptäckas av ett personuppgiftsbiträde, d.v.s. en annan myndighet eller organisation, som har åtagit sig att behandla personuppgifter åt den ansvariga myndigheten. Enligt artikel 33.2 måste personuppgiftsbiträdet, efter att ha fått vetskap om en personuppgifts-incident, utan onödigt dröjsmål underrätta myndigheten på vars uppdrag den har behandlat personuppgifterna.

Behandling av personuppgifter i anställnings-förhållanden

I enlighet med artikel 88:1 i EU:s dataskyddsförordning är det möjligt att i **kollektivavtal** fastställa mer specifika regler för att säkerställa skyddet av rättigheter och friheter vid behandling av anställdas personuppgifter i anställningsförhållanden. Sådana regler kan handla om behandling av personuppgifter vid exempelvis rekrytering, ledning, planering och organisering av arbetet, eller hälsa och säkerhet på arbetsplatsen. Enligt artikel 88:2 ska sådana regler innehålla lämpliga och specifika åtgärder för att skydda den registrerades mänskliga värdighet, berättigade intressen och grundläggande rättigheter. I kommande förhandlingar om nya tjänste- och arbetskollektivavtal är det tänkbart att någon av avtalsparterna framställer yrkanden om avtalsbestämmelser beträffande skydd för de anställdas personuppgifter.

Bilaga 1: Några av myndigheternas åligganden för att förbättra sitt dataskydd

I EU:s dataskyddsförordning finns det bestämmelser om att:

- Utse ett dataskyddsombud (artikel 37).
- Genomföra tekniska och organisatoriska åtgärder för att kraven i dataskyddsförordningen ska uppfyllas, för att de registrerade personernas rättigheter ska skyddas och för att endast nödvändiga personuppgifter ska behandlas (artikel 25).
- Vidta tekniska och organisatoriska åtgärder för en lämplig säkerhetsnivå (artikel 32).
- Föra register över behandling av personuppgifter (artikel 30).
- Ge information till registrerade personer (artiklarna 12-14 och 34).
- Rätta och komplettera personuppgifter på begäran av registrerade personer (artiklarna 16 och 19).
- Radera personuppgifter på begäran av registrerade personer (artiklarna 17 och 19).
- Begränsa behandling av personuppgifter på begäran av registrerade personer (artikel 18 och 19).
- Utföra konsekvensbedömningar av behandling av personuppgifter, vilken sannolikt medför hög risk för människors rättigheter och friheter (artikel 35).
- Anmäla och dokumentera personuppgiftsincidenter (artikel 33).

Bilaga 2: Konsekvensbeömning vid behandling av personuppgifter

Denna konsekvensbedömning görs, i enlighet med artikel 35 i EU:s dataskyddsförordning (EU 2016/679), på grund av att en planerad behandling av personuppgifter eventuellt kan leda till en hög risk för människors rättigheter och friheter.

- **Vilken är den planerade personuppgiftsbehandlingen? Beskriv den så systematiskt som möjligt!**

- **Vilka syften har behandlingen?**

- **Hur stort är behovet av behandlingen?**

- **Hur befogad anser myndigheten att behandlingen av personuppgifterna är i proportion till dess syften?**

- **Vilken risk finns för att personerna, vars personuppgifter behandlas, får sina rättigheter och friheter inskränkta?**

- **Vilka åtgärder planeras för att minska risken för att behandlingen av personuppgifter ska kränka människors rättigheter och friheter? Ange vilka skyddsåtgärder, säkerhetsåtgärder och rutiner som vidtas för att säkerställa skyddet av personuppgifter!**

- **Har synpunkter inhämtats från berörda personer och vilka har dessa synpunkter varit? Om synpunker från berörda personer inte har inhämtats, varför?**

Bilaga 3: Anmälan av personuppgiftsincident

Till Datainspektionen, Elverksgatan 10, 22100 Mariehamn, inspektion@di.ax

Nedanstående uppgifter anmäls i enlighet med artikel 33.1 och 33.3 i EU:s dataskyddsförordning på grund av att det har inträffat en säkerhetsincident, som lett 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. Om all information beträffande personuppgiftsincidenten ännu inte kan tillhandahållas, kommer resterande information att lämnas vid senare tillfälle, utan onödigt ytterligare dröjsmål.

- **Namn på anmälande myndighet:**

- **Namn, telefonnummer och e-postadress till myndighetens dataskyddsombud samt till andra personer som kan lämna information om personuppgiftsincidenten:**

- **Vilken är personuppgiftsincidentens art?**

- **Vilka kategorier registrerade personer berörs och hur stort är det ungefärliga antalet registrerade personer som berörs?**

- **Vilka kategorier av personuppgifter berörs och hur stort är det ungefärliga antalet personuppgiftsposter som berörs?**

- **När inträffade personuppgiftsincidenten? Om denna anmälan görs senare än inom 72 timmar efter personuppgiftsincidenten, vad är orsaken till förseningen?**

- **Vilka är de sannolika konsekvenserna av personuppgiftsincidenten?**

- **Vilka åtgärder har myndigheten vidtagit eller vilka åtgärder föreslår myndigheten för att åtgärda personuppgiftsincidenten? Ange åtgärder som mildrar personuppgiftsincidentens potentiella negativa effekter!**

Underskrift av företrädare för myndigheten:

Bilaga 4: Utdrag ur dataskyddsförordningen

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679

av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

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 lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,
2. **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 personuppgiftsbiträdets 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 personuppgiftsbiträdets verksamhetsställen i unionen där den huvudsakliga behandlingen inom ramen för verksamheten vid ett av personuppgiftsbiträdets 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 (19),
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.

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 oförenlig med de ursprungliga ändamålen (ändamålsbegränsning).
c) De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering).
d) De ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (korrekthet).
e) De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (lagringsminimering).
f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet).

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 eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.
h) Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system, på grundval av unionsrätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet och under förutsättning att de villkor och skyddsåtgärder som avses i punkt 3 är uppfyllda.
i) Behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter, på grundval av unionsrätten eller medlemsstaternas nationella rätt, där lämpliga

och specifika åtgärder för att skydda den registrerades rättigheter och friheter fastställs, särskilt tystnadsplikt.
j) Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

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

4. Medlemsstaterna får behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om hälsa.

Artikel 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.

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.

Artikel 13
Information som ska tillhandahållas om personuppgifterna samlas in från den registrerade

1. Om personuppgifter som rör en registrerad person samlas in från den registrerade, ska den personuppgiftsansvarige, när personuppgifterna erhålls, till den registrerade lämna information om följande:
a) Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.
b) Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall.
c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.
d) Om behandlingen är baserad på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen.
e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.
f) I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artikel 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

2. Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige vid insamlingen av personuppgifterna lämna den registrerade följande ytterligare information, vilken krävs för att säkerställa rättvis och transparent behandling:
a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
b) Att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.
c) Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, att det föreligger en rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.
d) Rätten att inge klagomål till en tillsynsmyndighet.
e) Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav eller ett krav som är nödvändigt för att ingå ett avtal samt huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att sådana uppgifter inte lämnas.
f) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

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

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

Artikel 14

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

1. Om personuppgifterna inte har erhållits från den registrerade, ska den personuppgiftsansvarige förse den registrerade med följande information:
a) Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.
b) Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall.
c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.
d) De kategorier av personuppgifter som behandlingen gäller.
e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.
f) I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till en mottagare i ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artiklarna 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

2. Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige lämna den registrerade följande information, vilken krävs för att säkerställa rättvis och transparent behandling när det gäller den registrerade:
a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
b) Om behandlingen grundar sig på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen.
c) Förekomsten av rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade och att invända mot behandling samt rätten till dataportabilitet.
d) Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, rätten att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.
e) Rätten att inge klagomål till en tillsynsmyndighet.
f) Varifrån personuppgifterna kommer och i förekommande fall huruvida de har sitt ursprung i allmänt tillgängliga källor.
g) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

3. Den personuppgiftsansvarige ska lämna den information som anges i punkterna 1 och 2
a) inom en rimlig period efter det att personuppgifterna har erhållits, dock senast inom en månad, med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas,
b) om personuppgifterna ska användas för kommunikation med den registrerade, senast vid tidpunkten för den första kommunikationen med den registrerade, eller

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

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

5. Punkterna 1–4 ska inte tillämpas i följande fall och i den mån
a) den registrerade redan förfogar över informationen,
b) tillhandahållandet av sådan information visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning, särskilt för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, eller i den mån den skyldighet som avses i punkt 1 i den här artikeln sannolikt kommer att göra det omöjligt eller avsevärt försvårar uppfyllandet av målen med den behandlingen; i sådana fall ska den personuppgiftsansvarige vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen, inbegripet göra uppgifterna tillgängliga för allmänheten,
c) erhållande eller utlämnande av uppgifter uttryckligen föreskrivs genom unionsrätten eller genom en medlemsstats nationella rätt som den registrerade omfattas av och som fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen, eller
d) personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt, inbegripet andra lagstadgade sekretessförpliktelser.

Artikel 15
Den registrerades rätt till tillgång

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna och följande information:
a) Ändamålen med behandlingen.
b) De kategorier av personuppgifter som behandlingen gäller.
c) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer.
d) Om möjligt, den 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.

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.

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 utrycka 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.

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 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 32
Säkerhet i samband med behandlingen

1. Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt
a) pseudonymisering och kryptering av personuppgifter,
b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

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

3. Anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att kraven i punkt 1 i den här artikeln följs.

4. Den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets 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.

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 överträdelser 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.

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 personuppgiftsbiträdets 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 personuppgiftsbiträdets 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 överträdelser, 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 personuppgiftsbiträdets 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 personuppgiftsbiträdets 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 personuppgiftsbiträdets 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.

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 uppgiftsbehandlingens 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 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.