ARTIKEL 29-ARBETSGRUPPEN FÖR SKYDD AV PERSONUPPGIFTER

16/SV
WP 243 rev.01

Riktlinjer om dataskyddsombud

Antagna den 13 december 2016

Senast granskade och antagna den 5 april 2017

Arbetsgruppen inrättades enligt artikel 29 i direktiv 95/46/EG. Den är ett oberoende rådgivande EU-organ i frågor rörande dataskydd och integritet. Dess uppgifter beskrivs i artikel 30 i direktiv 95/46/EG och artikel 15 i direktiv 2002/58/EG.

Gruppens sekretariat finns hos direktorat C (Grundläggande rättigheter och rättsstatsprincipen) på Europeiska kommissionen, Generaldirektoratet för rättsliga frågor och konsumentfrågor, B–1049 Bryssel, Belgien, kontor MO59 05/35.

Webbplats: http://ec.europa.eu/justice/data-protection/index_sv.htm

ARBETSGRUPPEN FÖR SKYDD AV ENSKILDA MED AVSEENDE PÅ BEHANDLING AV PERSONUPPGIFTER HAR ANTAGIT DESSA RIKTLINJER

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995, genom vilket arbetsgruppen inrättades,

med beaktande av artiklarna 29 och 30 i det direktivet, och

med beaktande av sin arbetsordning.

Innehållsförteckning

1 Inledning

Den allmänna dataskyddsförordningen,[1] som träder i kraft den 25 maj 2018, utgör en moderniserad och ansvarsbaserad ram för efterlevnad av bestämmelserna om dataskydd i EU. Dataskyddsombuden kommer att stå i centrum för denna nya rättsliga ram som berör många organisationer, vilket underlättar efterlevnaden av bestämmelserna i den allmänna dataskyddsförordningen.

Enligt förordningen är det obligatoriskt för vissa personuppgiftsansvariga och personuppgiftsbiträden att utnämna ett dataskyddsombud[2]. Så kommer att vara fallet för alla offentliga myndigheter och organ (oavsett vilka uppgifter de behandlar) och för andra organisationer som har som sin kärnverksamhet att systematiskt och i stor omfattning övervaka enskilda personer eller behandla särskilda kategorier av personuppgifter i stor omfattning.

Även om den allmänna dataskyddsförordningen inte innehåller ett specifikt krav på att utnämna ett dataskyddsombud, kan det ibland vara bra för organisationerna att ändå göra det frivilligt. Artikel 29-arbetsgruppen för skydd av personuppgifter (nedan *artikel 29-arbetsgruppen*) uppmuntrar sådana frivilliga ansträngningar.

Dataskyddsombud är ingen ny företeelse. Även om direktiv 95/46/EG[3] inte föreskriver utnämnande av ett dataskyddsombud har flera medlemsstater under årens lopp utvecklat en praxis för att göra detta.

Innan den allmänna dataskyddsförordningen antogs hävdade artikel 29-arbetsgruppen att dataskyddsombud är en hörnsten för ansvarsskyldigheten, och att utnämnande av ett dataskyddsombud underlättar efterlevnaden och dessutom blir en konkurrensfördel för företagen[4]. Förutom att underlätta efterlevnaden genom ansvarsverktyg (t.ex. underlätta konsekvensbedömningar avseende dataskydd eller revisioner) fungerar dataskyddsombud som mellanhänder mellan berörda aktörer (t.ex. tillsynsmyndigheter, de registrerade, samt affärsenheter inom organisationer).

Dataskyddsombudet är inte personligen ansvarigt i händelse av bristande efterlevnad av den allmänna dataskyddsförordningen. Det klargörs i förordningen att det är den personuppgiftsansvarige eller personuppgiftsbiträdet som ska säkerställa och kunna visa att behandlingen utförs i enlighet med

---

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1). Den allmänna dataskyddsförordningen är relevant för Europeiska ekonomiska samarbetsområdet (EES) och kommer att vara tillämplig efter det att den har införlivats i EES-avtalet.

[2] Det är också obligatoriskt för behöriga myndigheter att utnämna ett dataskyddsombud enligt artikel 32 i Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89), och enligt nationell genomförandelagstiftning. Dessa riktlinjer handlar om dataskyddsombud enligt den allmänna dataskyddsförordningen, men den vägledning som ges är även relevant för dataskyddsombud enligt direktiv 2016/680, med hänsyn till likheterna mellan bestämmelserna i fråga.

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

[4] Se http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

förordningens bestämmelser (artikel 24.1). Det är alltså den personuppgiftsansvarige eller personuppgiftsbiträdet som har ansvaret för att uppgiftsskyddet efterlevs.

Den personuppgiftsansvarige eller personuppgiftsombudet spelar även en central roll genom att göra det möjligt för dataskyddsombudet att effektivt utföra sina uppgifter. Utnämnandet av ett dataskyddsombud är det första steget, men dataskyddsombuden måste även ges tillräcklig självständighet för att effektivt kunna utföra sina uppgifter.

Den allmänna dataskyddsförordningen erkänner dataskyddsombuden som viktiga aktörer i det nya dataförvaltningssystemet och fastställer villkor för dataskyddsombudets utnämnande, ställning och uppgifter. Syftet med dessa riktlinjer är att klargöra de relevanta bestämmelserna i dataskyddsförordningen för att hjälpa personuppgiftsansvariga och personuppgiftsbiträden att följa lagen, samtidigt som de hjälper dataskyddsombuden i deras roll. Riktlinjerna innehåller även rekommendationer om bästa praxis som bygger på den erfarenhet som vunnits i några av EU-medlemsstaterna. Artikel 29-arbetsgruppen kommer att övervaka genomförandet av dessa riktlinjer och kan vid behov komplettera dem med närmare uppgifter.

2 Utnämnande av ett dataskyddsombud

2.1 Obligatoriskt utnämnande

Enligt artikel 37.1 i den allmänna dataskyddsförordningen ska ett dataskyddsombud utnämnas i tre specifika fall[5], nämligen om

a) behandlingen genomförs av en myndighet eller ett offentligt organ[6],
b) den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling som 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[7] och[8] personuppgifter som rör fällande domar i brottmål och överträdelser[9].

I följande underavsnitt ger artikel 29-arbetsgruppen riktlinjer om de kriterier och den terminologi som används i artikel 37.1.

Om det inte är uppenbart att en organisation inte är skyldig att utnämna ett dataskyddsombud, rekommenderar artikel 29-arbetsgruppen att personuppgiftsansvariga och personuppgiftsbiträden dokumenterar den interna analys som utförts för att fastställa huruvida ett dataskyddsombud bör

[5] Tänk på att enligt artikel 37.4 kan Europeiska unionens eller medlemsstaternas lagstiftning kräva att dataskyddsombud utnämns även i andra situationer.

[6] Undantaget är när detta sker som en del av domstolarnas dömande verksamhet. Se artikel 32 i direktiv (EU) 2016/680.

[7] Enligt artikel 9 omfattar detta 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.

[8] I artikel 37.1 c används ordet *och*. En förklaring av användningen av *eller* i stället för *och* ges i avsnitt 2.1.5.

[9] Artikel 10.

utnämnas, så att de kan visa att relevanta faktorer har beaktats[10]. Analysen ingår i dokumentationen enligt ansvarsprincipen. Tillsynsmyndigheten kan kräva en sådan analys och den bör uppdateras vid behov, till exempel om personuppgiftsansvariga och personuppgiftsbiträden börjar med nya verksamheter eller tillhandahåller nya tjänster som kan omfattas av dem som anges i artikel 37.1.

Om en organisation utser ett dataskyddsombud på frivillig basis gäller kraven i artiklarna 37–39 för dataskyddsombudets utnämnande, ställning och uppgifter på samma sätt som om utnämningen hade varit obligatorisk.

Inget hindrar en organisation som inte är juridiskt skyldig att utse ett dataskyddsombud och inte vill göra detta frivilligt att ändå anställa personal eller externa konsulter för att utföra dataskyddsuppgifter. I ett sådant fall är det viktigt att se till att det inte råder förvirring kring sådana personers titel, status, ställning och uppgifter. Därför bör det i all kommunikation inom företaget och med dataskyddsmyndigheter, de registrerade och allmänheten i stort, klargöras att den berörda personen eller konsulten inte är dataskyddsombud. [11]

Dataskyddsombudet, vare sig han/hon har utnämnts obligatoriskt eller frivilligt, utnämns för all behandling som utförs av den personuppgiftsansvarige eller personuppgiftsbiträdet.

[10] Se artikel 24.1.

[11] Samma sak gäller dataskyddsansvariga eller andra personer som arbetar med dataskydd som i dag redan finns i en del företag, och som inte alltid uppfyller kriterierna i den allmänna dataskyddsförordningen när det gäller tillgängliga resurser eller garantier för oberoende. Om de inte uppfyller dessa kriterier kan de nämligen inte anses vara eller benämnas dataskyddsombud.

2.1.1 ”EN OFFENTLIG MYNDIGHET ELLER ETT OFFENTLIGT ORGAN”

En offentlig myndighet eller ett offentligt organ definieras inte i den allmänna dataskyddsförordningen. Artikel 29-arbetsgruppen anser att detta begrepp bör definieras i nationell lagstiftning. Offentliga myndigheter och organ omfattar därför nationella, regionala och lokala myndigheter, men enligt tillämpliga nationella lagar omfattar begreppet vanligen även ett antal andra offentligrättsliga organ[12]. I sådana fall är utnämnandet av ett dataskyddsombud obligatoriskt.

Det är inte bara offentliga myndigheter eller offentliga organ som kan bedriva offentlig verksamhet och myndighetsutövning[13], utan även andra offentligrättsliga eller privaträttsliga fysiska eller juridiska personer inom olika sektorer enligt varje medlemsstats nationella lagstiftning, såsom kollektivtrafik, vatten- och energiförsörjning, väginfrastruktur, radio och tv i allmänhetens tjänst, allmännyttiga bostäder eller disciplinorgan för reglerade yrken.

I sådana fall kan de registrerade befinna sig i en mycket liknande situation när deras personuppgifter behandlas av en offentlig myndighet eller ett offentligt organ. Personuppgifter kan behandlas för liknande ändamål och enskilda personer har ofta mycket små eller inga möjligheter att välja om och i så fall hur deras personuppgifter ska behandlas, och behandlingen kan därför kräva det ytterligare skydd som utnämnandet av ett dataskyddsombud kan ge.

Även om det inte föreligger någon skyldighet i sådana fall rekommenderar artikel 29-arbetsgruppen, som god praxis, att privata organisationer som bedriver offentlig verksamhet och myndighetsutövning utnämner ett dataskyddsombud. Sådana dataskyddsombuds verksamhet omfattar all behandling som utförs, även behandling som inte har samband med utövandet av offentlig verksamhet eller ett offentligt uppdrag (t.ex. hantering av en personaldatabas).

[12] Se t.ex. definitionen av *offentliga myndigheter* och *organ som lyder under offentlig rätt* i artikel 2.1 och 2.2 i Europaparlamentets och rådets direktiv 2003/98/EG av den 17 november 2003 om vidareutnyttjande av information från den offentliga sektorn (EUT L 345, 31.12.2003, s. 90).
[13] Artikel 6.1 e.

2.1.2 ”KÄRNVERKSAMHET”

I artikel 37.1 b och 37.1 c hänvisas till *den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet* . I skäl 97 anges att personuppgiftsansvarigas kärnverksamhet avser deras *primära verksamhet och inte behandling av personuppgifter som kompletterande verksamhet*. ”Kärnverksamhet” kan sägas motsvara personuppgiftsansvarigas eller personuppgiftsbiträdenas nödvändiga centrala verksamhet för att uppfylla sina mål.

”Kärnverksamhet” bör dock inte tolkas som att den utesluter verksamhet där behandling av uppgifter utgör en oskiljaktig del av den personuppgiftsansvariges eller personuppgiftsbiträdets verksamhet. Ett sjukhus kärnverksamhet är till exempel att tillhandahålla hälsovård. Sjukhus kan dock inte tillhandahålla hälsovård på ett säkert och ändamålsenligt sätt utan att behandla hälsouppgifter, såsom patientjournaler. Behandling av sådana uppgifter bör därför anses utgöra ett sjukhus kärnverksamhet och sjukhus måste därför utnämna ett dataskyddsombud.

Ett annat exempel är ett privat säkerhetsföretag som övervakar ett antal privata shoppingcenter och allmänna platser. Övervakning är företagets kärnverksamhet, vilken i sin tur är oskiljaktigt kopplad till behandling av personuppgifter. Därför måste även detta företag utnämna ett dataskyddsombud.

Det ska dock sägas att alla organisationer har vissa verksamheter, till exempel för att betala sina anställda eller standardverksamheter i samband med it-stöd. Detta är några exempel på nödvändiga stödfunktioner för organisationens kärnverksamhet eller huvudsakliga verksamhet. Även om sådana verksamheter är nödvändiga eller centrala, betraktas de vanligen som kompletterande funktioner, inte som en kärnverksamhet.

2.1.3 ”BEHANDLING I STOR OMFATTNING”

Enligt artikel 37.1 b och 37.1 c ska behandling av personuppgifter ske i stor omfattning för att ett dataskyddsombud ska utnämnas. Behandling i stor omfattning definieras inte i den allmänna dataskyddsförordningen, men viss vägledning ges i skäl 91[14].

Det är nämligen inte möjligt att ange ett exakt antal som gäller i alla situationer, varken för mängden behandlade uppgifter eller antalet enskilda personer som berörs. Detta utesluter dock inte möjligheten att standardpraxis kan utvecklas med tiden för att på ett mer specifikt sätt och/eller i kvantitativa termer definiera vad som utgör *storskalig* behandling för vissa vanliga typer av behandling. Artikel 29-arbetsgruppen planerar också att bidra till att utveckla sådan standardpraxis genom att utbyta och publicera exempel på relevanta gränser för utnämnandet av ett dataskyddsombud.

[14] Enligt skäl 91 omfattar detta särskilt *storskalig uppgiftsbehandling med syftet att behandla betydande mängder personuppgifter på regional, nationell eller övernationell nivå, vilket skulle kunna påverka ett stort antal registrerade och sannolikt kommer att innebära en hög risk*. Samtidigt anges att *behandling av personuppgifter inte [bör] anses vara storskalig, om det är fråga om personuppgifter från patienter eller klienter som behandlas av enskilda läkare, andra yrkesverksamma på hälsoområdet eller juridiska ombud*. Det är viktigt att tänka på att det i skäl 91 ges exempel på ytterligheter (en enskild läkares behandling jämfört med ett helt lands behandling eller behandling i hela Europa), och det finns en stor gråzon mellan dessa ytterligheter. Dessutom är det viktigt att tänka på att skälet avser konsekvensbedömningar avseende dataskydd. Detta innebär att vissa faktorer kan vara specifika för det berörda sammanhanget och därför inte nödvändigtvis gäller för utnämning av dataskyddsombud på exakt samma sätt.

I alla händelser rekommenderar artikel 29-arbetsgruppen att särskilt följande faktorer övervägs vid fastställandet av huruvida behandling utförs i stor omfattning:

- Antalet berörda registrerade, antingen som ett exakt antal eller som en andel av den berörda befolkningsgruppen.
- Mängden uppgifter och/eller de olika typer av uppgifter som behandlas.
- Uppgiftsbehandlingens längd eller varaktighet.
- Behandlingens geografiska räckvidd.

Behandling i stor omfattning kan t.ex. vara

- behandling av patientuppgifter inom ramen för ett sjukhus normala verksamhet,
- behandling av reseuppgifter avseende enskilda personer som använder kollektivtrafiksystem i en stad (t.ex. spårning via resekort),
- behandling av kunders geolokaliseringsuppgifter i realtid för statistiska ändamål i en internationell snabbmatskedja, varvid behandlingen utförs av ett personuppgiftsbiträde som är specialiserat på att tillhandahålla sådana tjänster,
- behandling av kunduppgifter inom ramen för ett försäkringsbolags eller en banks normala verksamhet,
- behandling av personuppgifter som ska användas för beteendestyrd annonsering av en sökmotor,
- behandling av uppgifter (innehåll, trafik, position) av telefon- eller internettjänstleverantörer.

Behandling som inte sker i stor omfattning kan gälla t.ex. sådana fall där

- en enskild läkare behandlar patientuppgifter,
- en enskild advokat behandlar personuppgifter som rör fällande domar i brottmål samt överträdelser.

2.1.4 ”REGELBUNDEN OCH SYSTEMATISK ÖVERVAKNING”

Begreppet regelbunden och systematisk övervakning av de registrerade definieras inte i den allmänna dataskyddsförordningen, men begreppet *övervakningen av de registrerade personernas beteende* nämns i skäl 24[15], och det står klart att detta omfattar alla former av spårning och profilering på internet, även beteendestyrd annonsering.

Begreppet övervakning begränsas dock inte till nätmiljön, och spårning på internet bör endast betraktas som ett exempel på övervakning av de registrerade personernas beteende[16]-

Enligt artikel 29-arbetsgruppens tolkning innebär ”regelbunden” ett eller flera av följande alternativ:

[15] *”För att avgöra huruvida en viss behandling kan anses övervaka beteendet hos registrerade, bör det fastställas om fysiska personer spåras på internet, och om personuppgifterna därefter behandlas med hjälp av teknik som profilerar fysiska personer, i synnerhet för att fatta beslut rörande honom eller henne eller för att analysera eller förutsäga hans eller hennes personliga preferenser, beteende och attityder.”*

[16] Observera att skäl 24 inriktas på den extraterritoriella tillämpningen av den allmänna dataskyddsförordningen. Dessutom finns det även en skillnad mellan ordalydelsen *övervakning av deras beteende* (artikel 3.2 b) och *regelbunden och systematisk övervakning av de registrerade* (artikel 37.1 b), som därför kan anses utgöra ett separat begrepp.

- Pågående övervakning eller övervakning som sker i vissa intervall eller under en viss period.
- Återkommande eller upprepad övervakning vid fasta tidpunkter.
- Ständig eller periodisk övervakning.

Enligt artikel 29-arbetsgruppens tolkning innebär ”systematisk” ett eller flera av följande alternativ:

- Övervakning som sker enligt ett system.
- På förhand arrangerad, organiserad eller metodisk övervakning.
- Övervakning som sker enligt en allmän plan för uppgiftsinsamling.
- Övervakning som utförs som ett led i en strategi.

Följande verksamheter är exempel på vad som kan utgöra regelbunden och systematisk övervakning av de registrerade: drift av ett telekommunikationsnät, tillhandahållande av telekommunikationstjänster, omdirigering av e-post, hantering av datadriven marknadsföring, profilering eller poängsättning för riskbedömningar (t.ex. för bedömning av kreditvärdighet, fastställande av försäkringspremier, förebyggande av bedrägeri, upptäckt av penningtvätt), positionsspårning, t.ex. genom mobilappar, lojalitetsprogram, beteendestyrd annonsering, övervakning av uppgifter om välbefinnande, träning och hälsa via bärbara anordningar, övervakningskameror, anslutna anordningar, t.ex. smarta mätare, smarta bilar, hemautomatisering osv.

2.1.5 SÄRSKILDA UPPGIFTSKATEGORIER OCH PERSONUPPGIFTER SOM RÖR FÄLLANDE DOMAR I BROTTMÅL SAMT ÖVERTRÄDELSER.

Artikel 37.1 c handlar om behandling 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. Även om ordet ”och” används i bestämmelsen, finns det inga politiska skäl till att de två kriterierna måste tillämpas samtidigt. Texten bör därför lyda ”eller”.

2.2 Den personuppgiftsansvariges dataskyddsombud

Artikel 37 är tillämplig på både personuppgiftsansvariga[17] och personuppgiftsbiträden [18] med avseende på utnämnandet av ett dataskyddsombud. Beroende på vem som uppfyller kriterierna för obligatoriskt utnämnande, ibland endast den personuppgiftsansvarige eller endast personuppgiftsbiträdet, är både personuppgiftsansvariga och personuppgiftsbiträden skyldiga att utnämna ett dataskyddsombud (och de bör samarbeta med varandra).

Det är viktigt att betona att även om den personuppgiftsansvarige uppfyller kriterierna för obligatoriskt utnämnande är hans eller hennes personuppgiftsbiträde inte nödvändigtvis skyldigt att göra detta. Detta kan dock vara god praxis.

Exempel:

[17] Den personuppgiftsansvarige definieras i artikel 4.7 som den person eller det organ som bestämmer ändamålen och medlen för behandlingen av personuppgifter.

[18] Personuppgiftsbiträdet definieras i artikel 4.8 som den person eller det organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

- Ett litet familjeföretag som distribuerar hushållsapparater i en enda stad anlitar ett personuppgiftsbiträde vars kärnverksamhet är att tillhandahålla tjänster i form av webbsideanalyser och hjälp med riktad reklam och marknadsföring. Familjeföretagets verksamhet och dess kunder ger inte upphov till ”storskalig” behandling av personuppgifter, med tanke på att kunderna är få och verksamheten är relativt begränsad. Personuppgiftsbiträdet har dock många kunder i likhet med detta lilla företag, och dessa kunder sammantaget innebär att han eller hon bedriver storskalig behandling. Personuppgiftsbiträdet måste därför utnämna ett dataskyddsombud enligt artikel 37.1 b. Samtidigt är inte familjeföretaget i sig skyldigt att utse ett dataskyddsombud.

- Ett medelstort företag som tillverkar kakel lägger ut sina arbetsmiljötjänster på entreprenad till ett externt personuppgiftsbiträde, som har många liknande kunder. Personuppgiftsbiträdet ska utnämna ett dataskyddsombud enligt artikel 37.1 c, under förutsättning att behandlingen sker i stor omfattning. Tillverkaren är dock inte nödvändigtvis skyldig att utnämna ett personuppgiftsombud.

Det dataskyddsombud som personuppgiftsbiträdet har utnämnt övervakar även verksamhet som bedrivs av personuppgiftsbiträdets organisation när detta agerar som personuppgiftsansvarig i sig (t.ex. personal, it, logistik).

2.3 Utnämnande av ett enda dataskyddsombud för flera organisationer

Enligt artikel 37.2 får en koncern utnämna ett enda dataskyddsombud om det *på varje etableringsort är lätt att nå ett dataskyddsombud*. Med lättillgängligheten ovan avses dataskyddsombudets uppgifter som kontaktpunkt för de registrerade[19], tillsynsmyndigheten[20] och även internt inom organisationen, med tanke på att en av dataskyddsombudets uppgifter är att *informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar om deras skyldigheter enligt denna förordning*[21].

För att se till att dataskyddsombudet är lättillgängligt, både internt och externt, är det viktigt att säkerställa att deras kontaktuppgifter finns tillgängliga enligt den allmänna dataskyddsförordningens krav[22].

Han eller hon måste, vid behov med hjälp av en grupp, effektivt kunna kommunicera med de registrerade[23] och samarbeta[24] med de berörda tillsynsmyndigheterna. Detta innebär även att kommunikationen ska ske på det eller de språk som de berörda tillsynsmyndigheterna och registrerade

[19] Artikel 38.4: *Den registrerade får kontakta dataskyddsombudet med avseende på alla frågor som rör behandlingen av dennes personuppgifter och utövandet av dennes rättigheter enligt denna förordning*.

[20] Artikel 39.1 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*.

[21] Artikel 39.1 a.

[22] Se även avsnitt 2.6 nedan.

[23] Artikel 12.1: *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.*

[24] Artikel 39.1 d *: ”Att samarbeta med tillsynsmyndigheten”.*

använder. Det är mycket viktigt att dataskyddsombudet finns tillgängligt (antingen fysiskt i samma lokaler som de anställda, eller via en jourtelefon, alternativt via andra säkra kommunikationssätt) för att säkerställa att de registrerade kan nå dataskyddsombudet.

Enligt artikel 37.3 får ett enda dataskyddsombud utnämnas för flera offentliga myndigheter eller organ, med hänsyn till deras organisationsstruktur och storlek. Samma överväganden gäller för resurser och kommunikation. Med tanke på att dataskyddsombud har ansvar för ett antal olika uppgifter, måste personuppgiftsansvariga eller personuppgiftsbiträden säkerställa att ett enda dataskyddsombud, vid behov med hjälp av en grupp, kan fullgöra dessa uppgifter på ett effektivt sätt trots att de har utnämnts för flera offentliga myndigheter och organ.

2.4 Dataskyddsombudets tillgänglighet och etableringsort

Enligt avsnitt 4 i den allmänna dataskyddsförordningen ska dataskyddsombudet vara lätt att nå.

För att säkerställa att dataskyddsombuden är lätta att nå rekommenderar artikel 29-arbetsgruppen att de bör vara etablerade inom EU, vare sig de personuppgiftsansvariga eller personuppgiftsbiträdena är etablerade i EU eller ej.

I vissa situationer där de personuppgiftsansvariga eller personuppgiftsbiträdena inte är etablerade inom EU[25] kan det dock inte uteslutas att dataskyddsombuden eventuellt kan utöva sin verksamhet mer effektivt om de är etablerade utanför EU.

2.5 Dataskyddsombudets sakkunskap och kompetens

I artikel 37.5 anges att *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.* I skäl 97 anges att den nödvändiga nivån på sakkunskapen bör fastställas särskilt i enlighet med den uppgiftsbehandling som utförs och det skydd som krävs för de personuppgifter som behandlas.

- **Sakkunskapsnivå**

Den sakkunskapsnivå som krävs definieras inte strikt, men måste ändå stå i proportion till mängden behandlade uppgifter samt till hur känsliga och komplexa de uppgifter är som en organisation behandlar. Om behandlingen av personuppgifter är särskilt komplex eller omfattar en stor mängd känsliga uppgifter kan dataskyddsombudet till exempel behöva ha mer sakkunskap och mer stöd. Det finns även en skillnad beroende på om organisationen systematiskt överför personuppgifter utanför EU eller om överföringarna bara sker då och då. Dataskyddsombudet bör därför väljas noggrant, med vederbörlig hänsyn till de dataskyddsproblem som kan uppstå inom organisationen.

- **Yrkesmässiga kvalifikationer**

[25] Mer information om det territoriella tillämpningsområdet finns i artikel 3 i den allmänna dataskyddsförordningen.

Även om artikel 37.5 inte anger vilka yrkesmässiga kvalifikationer som bör övervägas vid utnämnandet av ett dataskyddsombud, är det relevant att de har sakkunskap om dataskyddslagstiftning och praxis på nationell nivå och EU-nivå och en djupgående förståelse av den allmänna dataskyddsförordningen. Det är också till hjälp om tillsynsmyndigheterna främjar lämplig och regelbunden fortbildning av dataskyddsombud.

Kunskap om affärssektorn och den personuppgiftsansvariges organisation är användbar. Dataskyddsombudet bör även ha en god förståelse av den behandling som genomförs och vara insatt i den personuppgiftsansvariges informationssystem samt datasäkerhets- och dataskyddsbehov.

Om det rör sig om en offentlig myndighet eller ett offentligt organ bör dataskyddsombudet även ha god kännedom om organisationens administrativa regler och förfaranden.

- **Förmåga att fullgöra uppgifter**

Dataskyddsombudens förmåga att fullgöra sina uppgifter bör tolkas som att det både rör deras personliga kvaliteter och kunskap och deras ställning inom organisationen. Personliga kvaliteter är till exempel integritet och hög yrkesetik: dataskyddsombudets främsta prioritering bör vara ett möjliggöra efterlevnad av den allmänna dataskyddsförordningen. Dataskyddsombudet spelar en central roll för att främja en dataskyddskultur inom organisationen och bidrar till att genomföra viktiga delar i den allmänna dataskyddsförordningen, såsom principerna om behandling av personuppgifter[26], de registrerades rättigheter[27], inbyggt dataskydd och dataskydd som standard[28], register över behandling av personuppgifter[29], säkerhet i samband med behandlingen[30] samt anmälan och meddelande av personuppgiftsincidenter[31].

- **Dataskyddsombud på grundval av tjänsteavtal**

Dataskyddsombudet får även utföra uppgifterna på grundval av ett tjänsteavtal som ingås med en enskild person eller organisation utanför den personuppgiftsansvariges/personuppgiftsbiträdets organisation. I det senare fallet är det viktigt att alla personer i organisationen som arbetar som dataskyddsombud uppfyller alla tillämpliga krav i avsnitt 4 i den allmänna dataskyddsförordningen (det är t.ex. viktigt att de inte har några intressekonflikter). Lika viktigt är att sådana personer skyddas av förordningens bestämmelser (t.ex. rättsstridigt upphävande av tjänsteavtal som dataskyddsombud får inte förekomma, och inte heller rättsstridig uppsägning av en enskild person i organisationen om han eller hon fullgör sådana uppgifter som ingår i dataskyddsombudets arbete). Samtidigt kan individuella kompetenser och starka sidor kombineras så att flera personer, som arbetar i en grupp, mer effektivt kan betjäna sina kunder.

För att skapa rättslig klarhet, underlätta en god organisation och förebygga intressekonflikter bland gruppmedlemmarna rekommenderas att uppgifterna fördelas tydligt inom det externa dataskyddsombudets grupp, och att en enda person utses till huvudkontakt och ”ansvarig person” för varje kund. Generellt är det också bra om dessa punkter anges specifikt i tjänsteavtalet.

[26] Kapitel II.
[27] Kapitel III.
[28] Artikel 25.
[29] Artikel 30.
[30] Artikel 32.
[31] Artiklarna 33 och 34.

2.6 Offentliggörande och meddelande av dataskyddsombudets kontaktuppgifter

Enligt artikel 37.7 i den allmänna dataskyddsförordningen ska den personuppgiftsansvarige eller personuppgiftsbiträdet

- offentliggöra dataskyddsombudets kontaktuppgifter och
- meddela dessa till de berörda tillsynsmyndigheterna.

Syftet med dessa krav är att se till att de registrerade (både inom och utanför organisationen) och tillsynsmyndigheterna enkelt och direkt kan kontakta dataskyddsombudet utan att behöva kontakta någon annan del av organisationen. Konfidentialitet är lika viktigt: anställda kan till exempel vara ovilliga att lämna in klagomål till dataskyddsombudet om inte kommunikationens konfidentialitet garanteras.
Dataskyddsombudet ska, när det gäller dennes genomförande av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt (artikel 38.5).

Dataskyddsombudets kontaktuppgifter bör inbegripa information som gör det möjligt för de registrerade och tillsynsmyndigheter att enkelt nå dataskyddsombudet (t.ex. postadress, ett särskilt telefonnummer och/eller en särskild e-postadress). Vid behov, och för kommunikation med allmänheten, kan det även vara lämpligt att tillhandahålla andra kommunikationssätt, t.ex. en särskild jourtelefon eller ett särskilt kontaktformulär som riktas till dataskyddsombudet och som finns på organisationens webbplats.

I artikel 37.7 i förordningen föreskrivs inte att dataskyddsombudets namn behöver anges i de offentliggjorda kontaktuppgifterna. Det kan visserligen vara bra praxis att göra detta, men det är den personuppgiftsansvarige eller personuppgiftsbiträdet som beslutar om det är nödvändigt eller användbart under de rådande omständigheterna[32].

Det är emellertid viktigt att dataskyddsombudets namn förmedlas till tillsynsmyndigheten för att dataskyddsombudet ska kunna fungera som en kontaktpunkt mellan organisationen och tillsynsmyndigheten (artikel 39.1 e).

Som god praxis rekommenderar även artikel 29-arbetsgruppen att organisationerna informerar sina anställda om dataskyddsombudets namn och kontaktuppgifter. Dataskyddsombudets namn och kontaktuppgifter kan till exempel publiceras internt på organisationens intranet, interna telefonlista och organisationsscheman.

[32] Det är värt att notera att artikel 33.3, som anger vilken information som ska lämnas till tillsynsmyndigheten och till de registrerade i händelse av personuppgiftsincidenter, till skillnad från artikel 37.7 innehåller ett specifikt krav på att dataskyddsombudets namn (och inte bara kontaktuppgifter) ska förmedlas.

3 Dataskyddsombudets ställning

3.1 Dataskyddsombudets deltagande i alla frågor som rör skyddet av personuppgifter

Enligt artikel 38 i den allmänna dataskyddsförordningen ska den personuppgiftsansvarige och personuppgiftsbiträdet säkerställa att dataskyddsombudet *på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.*

Det är viktigt att dataskyddsombuden och/eller deras grupper så tidigt som möjligt görs delaktiga i alla frågor som rör dataskydd. När det gäller konsekvensbedömningar avseende dataskydd föreskriver den allmänna dataskyddsförordningen uttryckligen att dataskyddsombudet ska göras delaktigt redan i ett tidigt skede och att den personuppgiftsansvarige ska rådfråga dataskyddsombudet vid genomförande av en konsekvensbedömning avseende dataskydd[33]. Att säkerställa att dataskyddsombudet informeras och rådfrågas redan från början underlättar efterlevnaden av förordningen och främjar en strategi för inbyggt dataskydd och bör därför vara en standardrutin i organisationens styrning. Dessutom är det viktigt att dataskyddsombudet ses som en diskussionspartner inom organisationen och att han eller hon ingår i de relevanta arbetsgrupper som har ansvar för behandling av personuppgifter inom organisationen.

Organisationen bör bland annat säkerställa följande:

- Dataskyddsombudet ska regelbundet inbjudas att delta i möten på högsta och mellanliggande förvaltningsnivå,
- Dataskyddsombudet rekommenderas delta när beslut med följder för dataskyddet fattas. All relevant information ska i god tid förmedlas till dataskyddsombudet så att han eller hon kan ge lämpliga råd.
- Dataskyddsombudets åsikt måste alltid ges tillbörlig vikt. I händelse av oenighet rekommenderar artikel 29-arbetsgruppen att organisationen som god praxis dokumenterar skälen till att dataskyddsombudets råd inte har följts.
- Dataskyddsombudet ska rådfrågas omedelbart när en personuppgiftsincident eller annan incident har inträffat.

Vid behov kan den personuppgiftsansvarige eller personuppgiftsbiträdet ta fram riktlinjer eller program för dataskydd, där det anges när dataskyddsombudet ska rådfrågas.

3.2 Resurser som krävs

Enligt artikel 38.2 i den allmänna dataskyddsförordningen ska organisationen stödja sitt dataskyddsombud genom att *tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap*. Följande faktorer bör särskilt övervägas:

- Högsta ledningen bör aktivt stödja dataskyddsombudets arbete (t.ex. på styrelsenivå).
- Dataskyddsombudet bör ha tillräckligt med tid på sig för att fullgöra sina uppgifter. Detta är särskilt viktigt när ett internt dataskyddsombud utnämns på deltid eller om ett externt

[33] Artikel 35.2.

dataskyddsombud arbetar med dataskydd vid sidan om andra uppgifter. Annars kan motstridiga prioriteringar leda till att dataskyddsombudet försummar sitt uppdrag. Det är mycket viktigt att dataskyddsombudet har tillräckligt med tid för att ägna sig åt sina dataskyddsuppgifter. Det är god praxis att fastställa en procentandel för den tid som behövs för dataskyddsombudsfunktionen om det inte är en heltidstjänst. Det är även god praxis att bestämma hur mycket tid som behövs för att utföra dataskyddsuppgifterna, att fastställa en lämplig prioritetsnivå för dataskyddsombudets uppgifter och att dataskyddsombudet (eller organisationen) tar fram en arbetsplan.

- Lämpligt stöd i form av ekonomiska resurser, infrastruktur (lokaler, hjälpmedel, utrustning) och personal i förekommande fall.
- Utnämningen av dataskyddsombudet bör officiellt meddelas till all personal för att säkerställa att personalen vet att det finns ett dataskyddsombud inom organisationen och vilka uppgifter dataskyddsombudet utför.
- Nödvändig tillgång till andra avdelningar, t.ex. personalavdelningen, den juridiska avdelningen, it-avdelningen, säkerhetsavdelningen och så vidare, så att dataskyddsombudet får viktig hjälp och information från dessa andra avdelningar.
- Fortbildning. Dataskyddsombud måste ges möjlighet att hålla sig uppdaterade om utveckling på dataskyddsområdet. Målet bör vara att ständigt öka dataskyddsombudens sakkunskap, och de bör uppmuntras att delta i fortbildningskurser om dataskydd och andra yrkesutvecklingskurser, t.ex. genom att delta i forum och seminarier om integritetsfrågor.
- Alltefter organisationens storlek och struktur kan det vara nödvändigt att upprätta en dataskyddsgrupp (ett dataskyddsombud och hans/hennes personal). I sådana fall bör gruppens interna struktur och varje medlems uppgifter och ansvar tydligt fastställas. När dataskyddsombudet är en extern tjänsteleverantör kan en grupp av enskilda personer som arbetar för denna enhet även utföra dataskyddsombudets uppgifter som en grupp, under ansvar av en utsedd huvudkontakt för kunden.

Generellt sett gäller att ju mer komplex och/eller känslig behandlingen är desto mer resurser bör anslås till dataskyddsombudet. Dataskyddsfunktionen måste vara effektiv och ha tillräckligt med resurser i förhållande till den uppgiftsbehandling som utförs.

3.3 Instruktioner och bestämmelser om att dataskyddsombudet ska *utföra sina uppgifter på ett oberoende sätt*

I artikel 38.3 fastställs vissa grundläggande garantier för att bidra till att säkerställa att dataskyddsombuden kan fullgöra sitt uppdrag och utföra sina uppgifter på ett tillräckligt självständigt sätt inom organisationen. Personuppgiftsansvariga/personuppgiftsbiträden ska i synnerhet säkerställa att dataskyddsombudet *inte tar emot instruktioner som gäller utförandet av [sina] uppgifter.* I skäl 97 tilläggs att *denna typ av dataskyddsombud bör, oavsett om de är anställda av den personuppgiftsansvarige eller ej, kunna fullgöra sitt uppdrag och utföra sina uppgifter på ett oberoende sätt*.

Detta innebär att dataskyddsombud, när de utför sina uppgifter enligt artikel 39, inte får instrueras om hur de ska hantera en fråga, till exempel vilka resultat som bör uppnås, hur ett klagomål ska utredas eller huruvida tillsynsmyndigheten ska rådfrågas eller ej. Dataskyddsombuden får inte heller instrueras att inta en viss ståndpunkt i frågor som rör dataskyddslagstiftningen, till exempel en viss tolkning av lagen.

Dataskyddsombudets självständighet innebär dock inte att de har beslutsbefogenheter utöver sina uppgifter enligt artikel 39.

Den personuppgiftsansvarige eller personuppgiftsbiträdet behåller ansvaret för efterlevnaden av dataskyddslagstiftningen och måste kunna visa att bestämmelserna efterlevs[34]. Om den personuppgiftsansvarige eller personuppgiftsbiträdet fattar beslut som är oförenliga med den allmänna dataskyddsförordningen och dataskyddsombudets råd, bör dataskyddsombudet ges möjlighet att klargöra sin avvikande ståndpunkt genom ett yttrande riktat till högsta förvaltningsnivå och till dem som fattar besluten. I detta avseende anges i artikel 38.3 att dataskyddsombudet *ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå*. Sådan direkt rapportering säkerställer att högsta ledningen (t.ex. styrelsen) är medveten om dataskyddsombudets råd och rekommendationer, som en del av dataskyddsombudets uppdrag att informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet. Ett annat exempel på direkt rapportering är att dataskyddsombudet utarbetar en årsrapport om sin verksamhet, varefter årsrapporten lämnas till högsta ledningen.

3.4 Avsättande eller sanktioner för att ha utfört dataskyddsombudets uppgifter

Enligt artikel 38.3 får dataskyddsombudet *inte avsättas eller bli föremål för sanktioner av den personuppgiftsansvarige eller personuppgiftsbiträdet för att ha utfört sina uppgifter*.

Detta krav stärker dataskyddsombudens självständighet och bidrar till att se till att de agerar oberoende och ges tillräckligt skydd när de utför sina dataskyddsuppgifter.

Sanktioner är förbjudna enligt den allmänna dataskyddsförordningen om de införs endast till följd av att dataskyddsombudet fullgör sitt uppdrag som sådant. Ett dataskyddsombud kan till exempel anse att en viss behandling sannolikt kan leda till en hög risk och råda den personuppgiftsansvarige eller personuppgiftsbiträdet att göra en konsekvensbedömning avseende dataskydd, men den personuppgiftsansvarige eller personuppgiftsbiträdet håller inte med om dataskyddsombudets bedömning. I en sådan situation kan dataskyddsombudet inte avsättas för att ha gett detta råd.

Sanktioner kan ha olika former och vara direkta eller indirekta. De kan till exempel bestå i att den berörda personen inte blir befordrad eller att befordran dröjer, att personen förhindras att gå vidare i karriären, eller inte får förmåner som andra anställda får. Sanktionerna behöver inte förverkligas – bara ett hot är tillräckligt om de används för att bestraffa dataskyddsombudet av skäl som har samband med verksamheten som dataskyddsombud.

Som en normal förvaltningsregel, och som för alla andra anställda eller leverantörer som omfattas av tillämplig nationell avtals-, arbets- eller straffrätt, kan dataskyddsombud lagligen avsättas av andra skäl än för att ha utfört sina uppgifter som dataskyddsombud (t.ex. stöld, alternativt fysiska, psykologiska eller sexuella trakasserier eller liknande grova tjänstefel).

I detta sammanhang är det viktigt att notera att den allmänna dataskyddsförordningen inte uttryckligen föreskriver hur och när ett dataskyddsombud kan avsättas eller ersättas av en annan person. Ju mer

[34] Artikel 5.2.

stabila dataskyddsombudens tjänsteavtal är, och ju fler garantier som finns mot rättsstridig uppsägning, desto mer sannolikt är det att de kan agera på ett oberoende sätt. Artikel 29-arbetsgruppen välkomnar därför ansträngningar från organisationerna i detta avseende.

3.5 Intressekonflikter

Enligt artikel 38.6 får dataskyddsombud *fullgöra andra uppgifter och uppdrag*. Det krävs dock att organisationen ska se till att *sådana uppgifter och uppdrag inte leder till en intressekonflikt*.

Kravet att det inte får föreligga intressekonflikter är nära kopplat till kravet att dataskyddsombuden ska kunna agera på ett oberoende sätt. Även om dataskyddsombud får ha andra funktioner, kan de anförtros andra uppgifter och uppdrag endast på villkor att de inte ger upphov till intressekonflikter. Detta innebär särskilt att dataskyddsombudet inte kan inneha en sådan tjänst inom organisationen som innebär att han/hon fastställer ändamålen med och medlen för behandlingen av personuppgifter. Detta måste avgöras från fall till fall beroende på hur organisationen är strukturerad.

Som en tumregel kan motstridiga befattningar inom organisationen vara befattningar i högsta ledningen (t.ex. verkställande direktör, högste verkställande beslutsfattare, finansdirektör, chefsläkare, marknadsföringschef, personalchef eller it-chef), men även andra funktioner lägre i organisationsstrukturen, om sådana befattningar eller funktioner innebär att dataskyddsombudet fastställer ändamålen med och medlen för behandlingen av personuppgifter. En intressekonflikt kan även uppstå om ett externt dataskyddsombud till exempel ombes att företräda den personuppgiftsansvarige eller personuppgiftsbiträdet vid en domstol i dataskyddsärenden.

Beroende på organisationens verksamhet, storlek och struktur kan det vara god praxis för personuppgiftsansvariga eller personuppgiftsbiträden att

- identifiera befattningar som är oförenliga med dataskyddsombudets uppgifter,
- utarbeta interna regler för detta ändamål i syfte att undvika intressekonflikter,
- inbegripa en mer allmän förklaring av intressekonflikter,
- utfärda en förklaring om att deras dataskyddsombud inte har intressekonflikter i förhållande till sin roll som dataskyddsombud, som ett sätt att öka medvetenheten om detta krav,
- inbegripa garantier i organisationens interna regler och säkerställa att meddelandet om ledig tjänst som dataskyddsombud eller tjänsteavtalet är tillräckligt exakt och detaljerat för att undvika intressekonflikter. I detta sammanhang är det även viktigt att tänka på att intressekonflikter kan ha olika former beroende på om dataskyddsombudet rekryteras internt eller externt.

4 Dataskyddsombudets uppgifter

4.1 Att övervaka efterlevnaden av den allmänna dataskyddsförordningen

Enligt artikel 39.1 b anförtros dataskyddsombuden bland annat uppdraget att övervaka efterlevnaden av den allmänna dataskyddsförordningen. I skäl 97 anges dessutom att dataskyddsombudet bör *bistå den personuppgiftsansvarige eller personuppgiftsbiträdet för att övervaka den interna efterlevnaden av denna förordning*.

Som ett led i skyldigheten att övervaka efterlevnaden kan dataskyddsombuden

- samla in information för att identifiera hur behandling av personuppgifter sker,
- analysera och kontrollera huruvida bestämmelser om behandlingen efterlevs, och
- informera samt ge råd och utfärda rekommendationer till den personuppgiftsansvarige eller personuppgiftsbiträdet.

Övervakning av efterlevnaden innebär inte att dataskyddsombudet är personligen ansvarigt i händelse av bristande efterlevnad. Det klargörs i förordningen att det är den personuppgiftsansvarige, inte dataskyddsombudet, som ska *genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning* (artikel 24.1). Det är alltså den personuppgiftsansvariges organisation som har ansvaret för att uppgiftsskyddet efterlevs, inte dataskyddsombudet.

4.2 Dataskyddsombudets roll i samband med konsekvensbedömningar avseende dataskydd

Enligt artikel 35.1 är det den personuppgiftsansvariges, inte dataskyddsombudets, uppgift att vid behov utföra en konsekvensbedömning avseende dataskydd. Dataskyddsombudet kan emellertid spela en mycket viktig och användbar roll genom att bistå den personuppgiftsansvarige. Enligt principen om inbyggt dataskydd krävs i artikel 35.2 uttryckligen att den personuppgiftsansvarige *ska rådfråga* dataskyddsombudet när en konsekvensbedömning avseende dataskydd utförs. Enligt artikel 39.1 c ges dataskyddsombudet i sin tur uppgiften att *på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den enligt artikel 35*.

Artikel 29-arbetsgruppen rekommenderar att personuppgiftsansvariga rådfrågar dataskyddsombuden om bland annat följande frågor:[35]

- Huruvida en konsekvensbedömning avseende dataskydd bör göras.
- Vilken metod som ska användas för konsekvensbedömningen avseende dataskydd.
- Huruvida konsekvensbedömningen avseende dataskydd bör göras internt eller läggas ut på en extern part.
- Vilka skyddsåtgärder (inbegripet tekniska och organisatoriska åtgärder) som bör vidtas för att begränsa eventuella risker för de registrerades rättigheter och intressen.

[35] I artikel 39.1 anges dataskyddsombudets uppgifter och att dataskyddsombudet ska ha *minst* de uppgifter som fastställs i de efterföljande leden. Det finns därför ingenting som förhindrar den personuppgiftsansvarige från att tilldela dataskyddsombudet andra uppgifter än de uppgifter som anges uttryckligen i artikel 39.1, eller att ange dessa uppgifter mer detaljerat.

- Huruvida konsekvensbedömningen avseende dataskydd har utförts korrekt och om dess slutsatser (om behandlingen ska fortsätta eller ej och vilka skyddsåtgärder som ska vidtas) överensstämmer med den allmänna dataskyddsförordningen.

Om den personuppgiftsansvarige inte håller med om de råd so givits av dataskyddsombudet, bör det uttryckligen och skriftligen motiveras i dokumentationen över konsekvensbedömningen avseende dataskydd varför rådet inte har beaktats[36].

Artikel 29-arbetsgruppen rekommenderar dessutom att den personuppgiftsansvarige, till exempel i dataskyddsombudets tjänsteavtal, men även i information som lämnas till de anställda, ledningen (och andra aktörer i förekommande fall), tydligt anger dataskyddsombudets exakta uppgifter och deras omfattning, särskilt när det gäller konsekvensbedömningar avseende dataskydd.

4.3 Att samarbeta med tillsynsmyndigheten och fungera som kontaktpunkt

Enligt artikel 39.1 d och e bör dataskyddsombudet *samarbeta med tillsynsmyndigheten* och *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*.

Dessa uppgifter avser dataskyddsombudets roll som en förmedlare som underlättar efterlevnad, vilket nämns i inledningen till dessa riktlinjer. Dataskyddsombudet fungerar som en kontaktpunkt för att underlätta tillsynsmyndighetens åtkomst till dokument och information för utförandet av de uppgifter som anges i artikel 57 och för att tillsynsmyndigheten ska kunna utöva sina utredande, korrigerande, tillståndsgivande och rådgivande befogenheter enligt artikel 58. Såsom redan nämnts ska dataskyddsombudet, när det gäller dennes genomförande av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt (artikel 38.5). Sekretess-/konfidentialitetskravet innebär dock inte att det är förbjudet för dataskyddsombuden att kontakta och samråda med tillsynsmyndigheten. Artikel 39.1 e föreskriver att dataskyddsombuden vid behov får samråda med tillsynsmyndigheten i alla andra frågor.

[36] Följande anges i artikel 24.1: *Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa **och kunna visa** att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov*.

4.4 Riskbaserad metod

Enligt artikel 39.2 ska dataskyddsombudet *ta vederbörlig hänsyn till de risker som är förknippade med behandling, med beaktande av behandlingens art, omfattning, sammanhang och syften*.

Denna artikel påminner om den allmänt vedertagna principen om sunt förnuft, som kan vara relevant för många aspekter av dataskyddsombudets dagliga arbete. Sammanfattningsvis innebär detta att dataskyddsombuden ska prioritera sin verksamhet och inrikta sitt arbete på eventuella problem som utgör en högre risk för dataskyddet. Detta betyder dock inte att de ska försumma övervakningen av efterlevnad avseende sådan uppgiftsbehandling som medför en jämförelsevis lägre risk, utan att de främst bör inrikta sig på områden med högre risk.

Syftet med detta selektiva och pragmatiska tillvägagångssätt är att hjälpa dataskyddsombuden att tillråda personuppgiftsansvariga om vilken metod de bör använda för konsekvensbedömningar avseende dataskydd, vilka områden som bör genomgå en intern eller extern revision av dataskyddet, vilka interna fortbildningsverksamheter som bör tillhandahållas till anställda eller ledningspersonal som ansvarar för uppgiftsbehandling, och vilken typ av behandling som de bör ägna mer av sin tid och sina resurser åt.

4.5 Dataskyddsombudets roll vid registerföringen

Enligt artikel 30.1 och 30.2 är det den personuppgiftsansvarige eller personuppgiftsbiträdet, inte dataskyddsombudet, som ska *föra ett register över behandling som utförts under dess ansvar* eller *föra ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning.*

I praktiken skapar dataskyddsombud ofta förteckningar och för ett register över behandling, vilket baseras på uppgifter som de får från olika avdelningar inom organisationen som ansvarar för behandling av personuppgifter. Denna praxis har fastställts i många aktuella nationella lagar och i de dataskyddsbestämmelser som är tillämpliga på EU:s institutioner och organ[37].

I artikel 39.1 anges de uppgifter som dataskyddsombudet minst ska ha. Inget förhindrar därför den personuppgiftsansvarige eller personuppgiftsbiträdet att tilldela dataskyddsombudet uppgiften att föra ett register över behandling under den personuppgiftsansvariges eller personuppgiftsbiträdets ansvar. Registren bör betraktas som ett av de verktyg som gör det möjligt för dataskyddsombudet att fullgöra sina uppgifter att övervaka efterlevnaden samt informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet.

I alla händelser bör det register som ska föras enligt artikel 30 även ses som ett verktyg som hjälper den personuppgiftsansvarige och tillsynsmyndigheten att, på begäran, skaffa sig en översikt av all behandling av personuppgifter som utförs av en organisation. Register är således en nödvändig förutsättning för efterlevnad, och är som sådant en effektiv ansvarsåtgärd.

[37] Artikel 24.1 d i förordning (EG) nr 45/2001.

5 BILAGA – RIKTLINJER OM DATASKYDDSOMBUD BRA ATT VETA

Syftet med denna bilaga är att på ett förenklat sätt och i ett lättläst format förklara några av de viktigaste frågorna som olika organisationer kan ha om de nya kraven i den allmänna dataskyddsförordningen för utnämnande av dataskyddsombud.

Utnämning av dataskyddsombudet

1 Vilka organisationer måste utnämna ett dataskyddsombud?

Utnämnande av ett dataskyddsombud är ett krav om

- behandlingen genomförs av en myndighet eller ett offentligt organ (oavsett vilka uppgifter som behandlas),
- den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning,
- den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter, eller personuppgifter som rör fällande domar i brottmål och överträdelser.

Tänk på att unionens eller medlemsstaternas lagstiftning kan kräva att dataskyddsombud utnämns även i andra situationer. Även om det inte är obligatoriskt att utnämna ett dataskyddsombud kan det ibland vara bra för organisationerna att ändå göra det frivilligt. Artikel 29-arbetsgruppen för skydd av personuppgifter uppmuntrar sådana frivilliga ansträngningar. Om en organisation utser ett dataskyddsombud på frivillig basis gäller samma krav för dataskyddsombudets utnämnande, ställning och uppgifter, dvs. på samma sätt som om utnämningen hade varit obligatorisk.

Källa: Artikel 37.1 i den allmänna dataskyddsförordningen.

2 Vad betyder ”kärnverksamhet”?

”Kärnverksamhet” kan sägas motsvara de centrala verksamheter som personuppgiftsansvariga eller personuppgiftsbiträden bedriver för att uppfylla sina mål. Kärnverksamhet omfattar även all verksamhet där behandling av uppgifter utgör en oskiljaktig del av den personuppgiftsansvariges eller personuppgiftsbiträdets verksamhet. Behandling av hälsouppgifter, såsom patientjournaler, bör till exempel anses utgöra ett sjukhus kärnverksamhet och sjukhus måste därför utnämna ett dataskyddsombud.

Det ska dock sägas att alla organisationer har vissa stödjande verksamheter, till exempel för att betala sina anställda, eller standardverksamheter i samband med it-stöd. Detta är några exempel på nödvändiga stödfunktioner för organisationens kärnverksamhet eller huvudsakliga verksamhet. Även om sådana verksamheter är nödvändiga eller centrala, betraktas de vanligen som kompletterande funktioner, inte som en kärnverksamhet.

Källa: Artikel 37.1 b och c i den allmänna dataskyddsförordningen.

3 Vad betyder behandling ”i stor omfattning”?

Behandling i stor omfattning definieras inte i den allmänna dataskyddsförordningen. Artikel 29-arbetsgruppen rekommenderar att särskilt följande faktorer övervägs vid fastställandet av huruvida behandling utförs i stor omfattning:

- Antalet berörda registrerade, antingen som ett exakt antal eller som en andel av den berörda befolkningsgruppen.
- Mängden uppgifter och/eller de olika typer av uppgifter som behandlas.
- Uppgiftsbehandlingens längd eller varaktighet.
- Behandlingens geografiska räckvidd.

Behandling i stor omfattning kan t.ex. vara

- behandling av patientuppgifter inom ramen för ett sjukhus normala verksamhet,
- behandling av reseuppgifter avseende enskilda personer som använder kollektivtrafiksystem i en stad (t.ex. spårning via resekort),
- behandling av kunders geolokaliseringsuppgifter i realtid för statistiska ändamål i en internationell snabbmatskedja, varvid behandlingen utförs av ett personuppgiftsbiträde som är specialiserat på sådana verksamheter,
- behandling av kunduppgifter inom ramen för ett försäkringsbolags eller en banks normala verksamhet,
- behandling av personuppgifter som ska användas för beteendestyrd annonsering av en sökmotor,
- behandling av uppgifter (innehåll, trafik, position) av telefon- eller internettjänstleverantörer.

Behandling som inte sker i stor omfattning kan gälla t.ex. sådana fall där

- en enskild läkare behandlar patientuppgifter,
- en enskild advokat behandlar personuppgifter som rör fällande domar i brottmål samt överträdelser.

Källa: Artikel 37.1 b och c i den allmänna dataskyddsförordningen.

4 Vad betyder ”regelbunden och systematisk övervakning”?

Begreppet regelbunden och systematisk övervakning av de registrerade definieras inte i den allmänna dataskyddsförordningen, men det står klart att detta omfattar alla former av spårning och profilering på internet, även beteendestyrd annonsering. ”Övervakning” begränsas dock inte bara till nätmiljön.

Följande verksamheter är exempel på vad som kan utgöra regelbunden och systematisk övervakning av de registrerade: drift av ett telekommunikationsnät, tillhandahållande av telekommunikationstjänster, omdirigering av e-post, hantering av datadriven marknadsföring, profilering eller poängsättning för riskbedömningar (t.ex. för bedömning av kreditvärdighet, fastställande av försäkringspremier, förebyggande av bedrägeri, upptäckt av penningtvätt), positionsspårning, t.ex. genom mobilappar, lojalitetsprogram, beteendestyrd annonsering, övervakning av uppgifter om välbefinnande, träning och hälsa via bärbara anordningar, övervakningskameror, anslutna anordningar, t.ex. smarta mätare, smarta bilar, hemautomatisering osv.

Enligt artikel 29-arbetsgruppens tolkning innebär ”regelbunden” ett eller flera av följande alternativ:

- Pågående övervakning eller övervakning som sker i vissa intervall eller under en viss period.
- Återkommande eller upprepad övervakning vid fasta tidpunkter.

- Ständig eller periodisk övervakning.

Enligt artikel 29-arbetsgruppens tolkning innebär ”systematisk” ett eller flera av följande alternativ:
- Övervakning som sker enligt ett system.
- På förhand arrangerad, organiserad eller metodisk övervakning.
- Övervakning som sker enligt en allmän plan för uppgiftsinsamling.
- Övervakning som utförs som ett led i en strategi.

Källa: Artikel 37.1 b i den allmänna dataskyddsförordningen.

5 Kan organisationer gemensamt utnämna ett dataskyddsombud? Om ja, under vilka förhållanden?

Ja. En koncern får utnämna ett enda dataskyddsombud om det *på varje etableringsort är lätt att nå ett dataskyddsombud*. ”Lättillgänglig” avser dataskyddsombudets uppgifter som kontaktpunkt för de registrerade, tillsynsmyndigheten och även internt inom organisationen. För att se till att dataskyddsombudet är lättillgängligt, både internt och externt, är det viktigt att säkerställa att deras kontaktuppgifter finns tillgängliga. Dataskyddsombudet måste, vid behov med hjälp av en grupp, effektivt kunna kommunicera med de registrerade och samarbeta med de berörda tillsynsmyndigheterna. Detta innebär att kommunikationen ska ske på det eller de språk som de berörda tillsynsmyndigheterna och registrerade använder. Det är mycket viktigt att dataskyddsombudet finns tillgängligt (antingen fysiskt i samma lokaler som de anställda, eller via en jourtelefon, alternativt via andra säkra kommunikationssätt) för att säkerställa att de registrerade kan nå dataskyddsombudet.

Ett enda dataskyddsombud får utnämnas för flera offentliga myndigheter eller organ, med hänsyn till deras organisationsstruktur och storlek. Samma överväganden gäller för resurser och kommunikation. Med tanke på att dataskyddsombud har ansvar för ett antal olika uppgifter, måste personuppgiftsansvariga eller personuppgiftsbiträden säkerställa att ett enda dataskyddsombud, vid behov med hjälp av en grupp, kan fullgöra dessa uppgifter på ett effektivt sätt trots att de har utnämnts för flera offentliga myndigheter och organ.

Källa: Artikel 37.2 och 37.3 i den allmänna dataskyddsförordningen.

6 Var bör dataskyddsombudet vara etablerat?

För att säkerställa att dataskyddsombuden är lätta att nå rekommenderar artikel 29-arbetsgruppen att de bör vara etablerade inom EU, vare sig de personuppgiftsansvariga eller personuppgiftsbiträdena är etablerade i EU eller ej. I vissa situationer där de personuppgiftsansvariga eller personuppgiftsbiträdena inte är etablerade inom EU kan det dock inte uteslutas att dataskyddsombuden eventuellt kan utöva sin verksamhet mer effektivt om de är etablerade utanför EU.

7 Är det möjligt att utnämna ett externt dataskyddsombud?

Ja. Dataskyddsombudet får ingå i den personuppgiftsansvariges eller personuppgiftsbiträdets personal (internt dataskyddsombud), eller utföra uppgifterna på grundval av ett tjänsteavtal. Detta innebär att dataskyddsombudet kan vara externt, och att han/hon i detta fall kan fullgöra sin funktion på grundval av ett tjänsteavtal som ingåtts med en enskild person eller en organisation.

När dataskyddsombudet är en extern tjänsteleverantör, kan en grupp av enskilda personer som arbetar för denna enhet utföra dataskyddsombudets uppgifter som en grupp, under ansvar av en utsedd huvudkontakt och ”ansvarig person” hos kunden. I sådana fall är det viktigt att alla personer i den externa organisationen som fullgör uppgifter som dataskyddsombud uppfyller alla tillämpliga krav i den allmänna dataskyddsförordningen.

För att skapa rättslig klarhet, underlätta en god organisation och förebygga intressekonflikter bland gruppmedlemmarna innehåller riktlinjerna en rekommendation om att tjänsteavtalet bör föreskriva en tydlig uppgiftsfördelning inom det externa dataskyddsombudets grupp, och att en enda person utses till huvudkontakt och ”ansvarig person” hos kunden.

Källa: Artikel 37.6 i den allmänna dataskyddsförordningen.

8 Vilka yrkesmässiga kvalifikationer bör ett dataskyddsombud ha?

Dataskyddsombudet ska utses på grundval av yrkesmässiga kvalifikationer och, särskilt, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra sina uppgifter.

Den nödvändiga nivån på sakkunskapen bör fastställas i enlighet med den uppgiftsbehandling som utförs och det skydd som krävs för de personuppgifter som behandlas. Om behandlingen av personuppgifter är särskilt komplex eller omfattar en stor mängd känsliga uppgifter kan dataskyddsombudet till exempel behöva ha mer sakkunskap och mer stöd.

Följande kvalifikationer och sakkunskap är relevanta:

- Kunskap om dataskyddslagstiftning och praxis på nationell nivå och EU-nivå, inklusive djupgående kunskap om den allmänna dataskyddsförordningen.
- Förståelse av hur behandlingen av personuppgifter genomförs.
- Kunskap om olika typer av informationsteknik och datasäkerhet.
- Kunskap om affärssektorn och organisationen i fråga.
- Förmåga att främja en dataskyddskultur inom organisationen.

Källa: Artikel 37.5 i den allmänna dataskyddsförordningen.

Dataskyddsombudets ställning

9 Vilka resurser bör den personuppgiftsansvarige eller personuppgiftsbiträdet ställa till dataskyddsombudets förfogande?

Dataskyddsombudet måste ha de resurser som krävs för att kunna fullgöra sina uppgifter.

Beroende på uppgiftsbehandlingens natur och organisationens verksamheter och storlek bör följande resurser tillhandahållas till dataskyddsombudet:

- Aktivt stöd från högsta ledningen för dataskyddsombudets arbete.

- Tillräckligt med tid för att dataskyddsombudet ska kunna fullgöra sina uppgifter.
- Lämpligt stöd i form av ekonomiska resurser, infrastruktur (lokaler, hjälpmedel, utrustning) och personal i förekommande fall.
- Officiellt meddelande till all personal om att dataskyddsombudet utnämnts.
- Tillgång till andra avdelningar inom organisationen som kan ge det stöd, de bidrag och den information som dataskyddsombudet behöver i sitt arbete.
- Fortbildning.

Källa: Artikel 38.2 i den allmänna dataskyddsförordningen.

10 Vilka skyddsåtgärder finns för att dataskyddsombudet ska kunna utföra sina uppgifter på ett oberoende sätt? Vad betyder ”intressekonflikt”?

Det finns flera skyddsåtgärder för att dataskyddsombud ska kunna agera på ett oberoende sätt:

- Personuppgiftsansvariga eller personuppgiftsbiträden får inte ge instruktioner som gäller utförandet av dataskyddsombudets uppgifter.
- Han eller hon får inte avsättas eller bli föremål för sanktioner för att ha utfört sina uppgifter.
- Det får inte förekomma intressekonflikter i samband med eventuella andra uppgifter och uppdrag.

Dataskyddsombudets andra uppgifter och uppdrag får inte leda till en intressekonflikt. Detta innebär för det första att dataskyddsombudet inte kan inneha en sådan tjänst inom organisationen som innebär att han/hon fastställer ändamålen med och medlen för behandlingen av personuppgifter. Detta måste avgöras från fall till fall beroende på hur organisationen är strukturerad.

Som en tumregel kan motstridiga befattningar inom organisationen vara befattningar i högsta ledningen (t.ex. verkställande direktör, högste verkställande beslutsfattare, finansdirektör, chefsläkare, marknadsföringschef, personalchef eller it-chef), men även andra funktioner lägre i organisationsstrukturen, om sådana befattningar eller funktioner innebär att dataskyddsombudet fastställer ändamålen med och medlen för behandlingen av personuppgifter. En intressekonflikt kan även uppstå om ett externt dataskyddsombud till exempel ombes att företräda den personuppgiftsansvarige eller personuppgiftsbiträdet vid domstol i dataskyddsärenden.

Källa: Artikel 38.3 och 38.6 i den allmänna dataskyddsförordningen

Dataskyddsombudets uppgifter

11 Vad betyder ”övervaka efterlevnaden”?

Som ett led i skyldigheten att övervaka efterlevnaden kan dataskyddsombuden

- samla in information för att identifiera hur behandling av personuppgifter sker,
- analysera och kontrollera huruvida bestämmelser om behandlingen efterlevs, och

- informera samt ge råd och utfärda rekommendationer till den personuppgiftsansvarige eller personuppgiftsbiträdet.

Källa: Artikel 39.1 b i den allmänna dataskyddsförordningen

12 Är dataskyddsombudet personligen ansvarigt för bristande efterlevnad av dataskyddskraven?

Nej, dataskyddsombudet är inte personligen ansvarigt för bristande efterlevnad av dataskyddskraven. Det är den personuppgiftsansvarige eller personuppgiftsbiträdet som ska säkerställa och kunna visa att behandlingen utförs i enlighet med den allmänna dataskyddsförordningen. Det är alltså den personuppgiftsansvarige eller personuppgiftsbiträdet som har ansvaret för att uppgiftsskyddet efterlevs.

13 Vilken roll har dataskyddsombudet när det gäller konsekvensbedömningar avseende dataskydd och register över behandling?

När det gäller konsekvensbedömningar avseende dataskydd ska den personuppgiftsansvarige eller personuppgiftsbiträdet rådfråga dataskyddsombudet om bland annat följande:

- Huruvida en konsekvensbedömning avseende dataskydd bör göras.
- Vilken metod som ska användas för konsekvensbedömningen avseende dataskydd.
- Huruvida konsekvensbedömningen avseende dataskydd bör göras internt eller läggas ut på en extern part.
- Vilka skyddsåtgärder (inbegripet tekniska och organisatoriska åtgärder) som bör vidtas för att begränsa eventuella risker för de registrerades rättigheter och intressen.
- Huruvida konsekvensbedömningen har utförts korrekt och om dess slutsatser (om behandlingen ska fortsätta eller ej och vilka skyddsåtgärder som ska vidtas) överensstämmer med dataskyddskraven.

När det gäller register över behandling är det den personuppgiftsansvarige eller personuppgiftsbiträdet, inte dataskyddsombudet, som ska föra ett register över behandling. Inget förhindrar dock den personuppgiftsansvarige eller personuppgiftsbiträdet att tilldela dataskyddsombudet uppgiften att föra ett register över behandling under den personuppgiftsansvariges eller personuppgiftsbiträdets ansvar. Registren bör betraktas som ett av de verktyg som gör det möjligt för dataskyddsombudet att fullgöra sina uppgifter att övervaka efterlevnaden samt informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet.

Källa: Artiklarna 39.1 c och 30 i den allmänna dataskyddsförordningen.

På arbetsgruppens vägnar,
ordförande

Isabelle Falque-Pierrotin

Senast granskade och antagna den 5 april 2017

På arbetsgruppens vägnar,
ordförande

Isabelle Falque-Pierrotin