

WP 243 BILAGA – VANLIGA FRÅGOR OCH SVAR

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 för att utnämna dataskyddsombud enligt den allmänna dataskyddsförordningen.

Utnämning av dataskyddsombudet (artikel 37)

1 Vilka organisationer ska utnämna dataskyddsombud (artikel 37.1)?

Enligt den allmänna dataskyddsförordningen ska ett dataskyddsombud utnämnas i tre specifika fall, nämligen 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, och
- den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter och 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. När 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 uppmuntrar till sådana frivilliga ansträngningar.

Närmare information finns i avsnitt 2.1 i riktlinjerna.

2 Vad står begreppet ”kärnverksamhet” för (artikel 37.1 b och c)?

”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. Sådana stödfunktioner är nödvändiga för organisationens kärnverksamhet eller huvudsakliga verksamhet. Även om sådana verksamheter är nödvändiga eller centrala, betraktas de vanligen som kompletterande funktioner, inte som en kärnverksamhet.

Närmare information finns i avsnitt 2.1.2 i riktlinjerna.

3 Vad står begreppet ”stor omfattning” för (artikel 37.1 b och c)?

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 geolokaliseringssuppgifter 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 internetjänstleverantörer.

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.

Närmare information finns i avsnitt 2.1.3 i riktlinjerna.

4 Vad står begreppet ”regelbunden och systematisk övervakning” för (artikel 37.1 b)?

Begreppet ”regelbunden och systematisk övervakning av 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.

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.

Exempel: drift av ett telekommunikationsnät, tillhandahållande av telekommunikationstjänster, omdirigering av e-post, 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, beteendestyrda annonsering, övervakning av uppgifter om välbefinnande, träning och hälsa via bärbara anordningar, övervakningskameror, anslutna anordningar, t.ex. smarta mätare, smarta bilar, hemautomatisering osv.

Närmare information finns i avsnitt 2.1.4 i riktlinjerna.

5 Kan organisationer gemensamt utnämna ett dataskyddsbud? Om ja, under vilka förhållanden? (artikel 37.2 och 37.3)

Enligt den allmänna dataskyddsförordningen får en koncern utnämna ett enda dataskyddsbud om det *på varje etableringsort är lätt att nå ett dataskyddsbud*. ”Lättillgänglig” avser dataskyddsbudets uppgifter som kontaktpunkt för de registrerade, tillsynsmyndigheten och även internt inom organisationen. För att se till att dataskyddsbudet är lättillgängligt, både internt och externt, är det viktigt att säkerställa att deras kontaktoppgifter finns tillgängliga enligt den allmänna dataskyddsförordningen. Dataskyddsbudet måste kunna kommunicera effektivt 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 dataskyddsbudet finns personligen 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 dataskyddsbudet.

Närmare information finns i avsnitt 2.3 i riktlinjerna.

6 Är det möjligt att utnämna ett externt dataskyddsbud (artikel 37.6)?

Ja. Enligt artikel 37.6 får dataskyddsbudet ingå i den personuppgiftsansvariges eller personuppgiftsbiträdets personal (internt dataskyddsbud), eller ”utföra uppgifterna på grundval av ett tjänsteavtal”. Detta innebär att dataskyddsbudet 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.

Om dataskyddsbudet är externt gäller samtliga krav i artiklarna 37–39 för denna person. I riktlinjerna anges att när dataskyddsbudet är en extern tjänsteleverantör kan en grupp av enskilda personer som arbetar för denna enhet utföra dataskyddsbudets 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 dataskyddsbud uppfyller alla relevanta krav i den allmänna dataskyddsförordningen.

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

Närmare information finns i avsnitt 2.3, 2.4 och 3.5 i riktlinjerna.

7 Vilka yrkesmässiga kvalifikationer bör ett dataskyddsombud ha (artikel 37.5)?

Enligt den allmänna dataskyddsförordningen ska dataskyddsombudet *uteses på grundval av yrkesmässiga kvalifikationer och, särskilt, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i artikel 39.*

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.

Dataskyddsombud bör besitta följande kvalifikationer och sakkunskap:

- 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.

Närmare information finns i avsnitt 2.4 i riktlinjerna.

Dataskyddsombudets ställning (artikel 38)

8 Vilka resurser bör dataskyddsombudet ges för att han/hon ska kunna utföra sina uppgifter?

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.*

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.

Närmare information finns i avsnitt 3.2 i riktlinjerna.

9 Vilka skyddsåtgärder finns för att dataskyddsombudet ska kunna utföra sina uppgifter på ett oberoende sätt (artikel 38.3)?

Det finns flera skyddsåtgärder för att dataskyddsombud ska kunna agera på ett oberoende sätt, vilket anges i skäl 97:

- 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.

Närmare information finns i avsnitt 3.3–3.5 i riktlinjerna.

10 Vilka ”andra uppgifter och uppdrag” som innehas av ett dataskyddsombud kan leda till en intressekonflikt (artikel 38.6)?

Dataskyddsombudet kan inte 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 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.

Närmare information finns i avsnitt 3.5 i riktlinjerna.

Dataskyddsombudets uppgifter (artikel 39)

11 Vad står begreppet ”övervaka efterlevnaden” för enligt den allmänna dataskyddsförordningen (artikel 39.1 b)?

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.

Närmare information finns i avsnitt 4.1 i riktlinjerna.

12 Är dataskyddsombudet personligen ansvarigt för bristande efterlevnad av den allmänna dataskyddsförordningen?

Nej, dataskyddsombudet är inte personligen ansvarigt för 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 denna förordning” (artikel 24.1). 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 (artikel 37.1 c) och register över behandling (artikel 30)?

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 den allmänna dataskyddsförordningen.

Närmare information finns i avsnitt 4.2 i riktlinjerna.

När det gäller register över behandling är det den personuppgiftsansvarige eller personuppgiftsbiträdet, inte dataskyddsombudet, som ska föra ett register över behandling. Inget hindrar dock den personuppgiftsansvarige eller personuppgiftsbiträdet från att tilldela dataskyddsombudet uppgiften att föra ett register över behandling under den personuppgiftsansvariges 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.

Närmare information finns i avsnitt 4.4 i riktlinjerna.