ARTIKEL 29-ARBETSGRUPPEN FÖR SKYDD AV PERSONUPPGIFTER

16/SV
WP 244 rev. 01

Riktlinjer om fastställande av ansvarig tillsynsmyndighet för personuppgiftsansvariga eller personuppgiftsbiträden

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

Innehållsförteckning

1. Att fastställa ansvarig tillsynsmyndighet: viktiga begrepp.

1.1 ”Gränsöverskridande behandling av personuppgifter”

Det är relevant att fastställa en ansvarig tillsynsmyndighet endast i sådana fall där den personuppgiftsansvarige eller personuppgiftsbiträdet genomför gränsöverskridande behandling av personuppgifter. Enligt definitionen i artikel 4.23 i den allmänna dataskyddsförordningen utgör ”gränsöverskridande behandling” antingen

- *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*

- *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*.

Detta innebär att om en organisation till exempel har verksamhetsställen i Frankrike och Rumänien och behandlar personuppgifter inom ramen för sin verksamhet, utgör detta gränsöverskridande behandling.

Alternativt kanske organisationen endast behandlar personuppgifter inom sitt verksamhetsställe i Frankrike. Om verksamheten i väsentlig grad påverkar – eller sannolikt i väsentlig grad kommer att påverka – de registrerade i både Frankrike och Rumänien, utgör dock även detta gränsöverskridande behandling.

1.1.1 ”Påverka i väsentlig grad”

”Påverka” eller ”i väsentlig grad” definieras inte i förordningen. Syftet med ordalydelsen var att säkerställa att definitionen av gränsöverskridande behandling inte ska omfatta all behandling om den bara har *någon som helst* påverkan och om den bara sker inom ett enda verksamhetsställe.

De mest relevanta och vanligaste betydelserna av det engelska ordet *substantial* (väsentlig) är bland annat (i översättning) ”stor mängd eller avsevärd storlek”, ”ansenlig”, ”av betydande storlek”, ”av gediget värde”, ”av verklig vikt”, ”stabil”, ”betydelsefull”, ”viktig” *(Oxford English Dictionary)*.

De mest relevanta betydelserna av det engelska verbet *affect* (påverka) är (i översättning) ”att ha inflytande över” eller ”göra ett stort intryck på”. Det engelska substantivet *effect* (påverkan) betyder i sin tur bland annat (i översättning) ”ett resultat” eller ”en konsekvens” *(Oxford English Dictionary)*. Av detta kan man dra slutsatsen att för att behandling av personuppgifter ska *påverka* någon måste den ha någon form av påverkan på dem. Behandling som inte i väsentlig grad påverkar enskilda personer omfattas inte av den andra delen av definitionen av gränsöverskridande behandling. Sådan behandling skulle dock omfattas av den första delen av definitionen om behandlingen av personuppgifter sker vid personuppgiftsansvarigas eller personuppgiftsbiträdenas verksamhetsställen i mer än en

medlemsstat, i det fall där den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerade i mer än en medlemsstat.

Behandling kan omfattas av den andra delen av definitionen om det är sannolikt att den kan ha en väsentlig påverkan, inte bara en faktisk väsentlig påverkan. Notera att ”sannolikt” inte innebär att det finns en avlägsen möjlighet till väsentlig påverkan. Det måste vara mer sannolikt än inte sannolikt att behandlingen har en väsentlig påverkan. Detta innebär å andra sidan att enskilda personer inte behöver påverkas rent konkret: det är tillräckligt att det är sannolikt att påverkan i väsentlig grad uppstår för att behandlingen ska omfattas av definitionen av gränsöverskridande behandling.

Det faktum att verksamheten i fråga kan omfatta behandling av ett antal, även ett stort antal, enskilda personers personuppgifter i flera medlemsstater, innebär inte nödvändigtvis att behandlingen har, eller sannolikt kan ha, en väsentlig påverkan. Behandling som inte har väsentlig påverkan utgör inte gränsöverskridande behandling enligt den andra delen av definitionen, oavsett hur många enskilda personer som påverkas.

Tillsynsmyndigheterna tolkar begreppet ”påverka i väsentlig grad” från fall till fall. De faktorer som övervägs inom ramen för behandlingen är typen av uppgifter, ändamålet med behandlingen och om behandlingen

- orsakar eller sannolikt kan orsaka skada, förlust eller känslomässigt lidande för enskilda personer,
- har, eller sannolikt kan ha, en faktisk påverkan genom att den enskilda personens rättigheter begränsas eller han/hon förlorar en möjlighet,
- påverkar, eller sannolikt kan påverka, den enskilda personens hälsa, välbefinnande eller trygghet,
- påverkar, eller sannolikt kan påverka, den enskilda personens finansiella eller ekonomiska ställning eller situation,
- utsätter den enskilda personen för diskriminering eller orättvis behandling,
- omfattar analys av särskilda kategorier av personuppgifter eller andra inkräktande uppgifter, särskilt barns personuppgifter,
- leder till, eller sannolikt kan leda till att den enskilda personen ändrar sitt beteende på ett väsentligt sätt,
- leder till osannolika, oväntade eller oönskade konsekvenser för den enskilda personen,
- ger upphov till pinsamma situationer eller andra negativa resultat, även skadat anseende, eller
- innebär behandling av en stor mängd personuppgifter.

Syftet med testet av ”väsentlig påverkan” är sammanfattningsvis att se till att tillsynsmyndigheterna endast behöver samarbeta formellt med varandra via den allmänna dataskyddsförordningens mekanism för enhetlighet *när en tillsynsmyndighet avser att anta en åtgärd som är avsedd att ha rättsverkan gällande behandlingar som i väsentlig grad påverkar ett betydande antal registrerade i flera medlemsstater (skäl 135).*

1.2 Ansvarig tillsynsmyndighet

Enkelt uttryckt är en ansvarig tillsynsmyndighet den myndighet som har det främsta ansvaret för att handlägga ärenden som rör gränsöverskridande behandling, till exempel om en registrerad inger ett klagomål om behandlingen av sina personuppgifter.

Den ansvariga tillsynsmyndigheten samordnar eventuella utredningar som omfattar andra ”berörda” tillsynsmyndigheter.

För att kunna fastställa ansvarig tillsynsmyndighet måste man avgöra var den personuppgiftsansvariges ”huvudsakliga” eller ”enda” verksamhetsställe i EU finns. Följande anges i artikel 56 i den allmänna dataskyddsförordningen:

- *[T]illsynsmyndigheten för den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga verksamhetsställe eller enda verksamhetsställe [ska] vara behörig att agera som ansvarig tillsynsmyndighet för den personuppgiftsansvariges eller personuppgiftsbiträdets gränsöverskridande behandling i enlighet med* det förfarande [för samarbete] *som föreskrivs i artikel 60.*

1.3 Huvudsakligt verksamhetsställe

”Huvudsakligt verksamhetsställe” definieras på följande sätt i artikel 4.16 i den allmänna dataskyddsförordningen:

- *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,*

- *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.*

2. Steg i fastställandet av ansvarig tillsynsmyndighet

2.1 Att fastställa ”huvudsakligt verksamhetsställe” för personuppgiftsansvariga

För att fastställa var det huvudsakliga verksamhetsstället är beläget måste man först identifiera var den personuppgiftsansvariges centrala förvaltning i EU finns (i förekommande fall)[1]. Tillvägagångssättet enligt den allmänna dataskyddsförordningen är att den centrala förvaltningen i EU är den plats där besluten om ändamålen och medlen för behandlingen av personuppgifter fattas, och att detta verksamhetsställe har befogenhet att genomföra sådana beslut.

[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. Den allmänna dataskyddsförordningen granskas för närvarande i syfte att införlivas, se http://www.efta.int/eea-lex/32016R0679.

Kärnan i den allmänna dataskyddsförordningens princip om ansvarig tillsynsmyndighet är att tillsynen av gränsöverskridande behandling bör ledas av endast en tillsynsmyndighet i EU. I sådana fall där beslut om olika verksamheter som rör gränsöverskridande behandling fattas inom den centrala förvaltningen i EU, utses endast en ansvarig tillsynsmyndighet för de olika typerna av verksamhet som rör sådan behandling av personuppgifter som genomförs av det multinationella företaget. Det kan dock hända att ett annat verksamhetsställe än den centrala förvaltningen fattar självständiga beslut om ändamålen och medlen för en viss typ av behandling. Detta innebär att det kan uppstå situationer där fler än en ansvarig tillsynsmyndighet kan identifieras, dvs. i sådana fall där ett multinationellt företag beslutar att ha verksamhetsställen med beslutsbefogenhet i flera olika länder för olika typer av behandlingsverksamhet.

Det är värt att påminna om att när ett multinationellt företag centraliserar alla beslut om ändamålen och medlen för behandling till ett av sina verksamhetsställen i EU (och detta verksamhetsställe har befogenheten att genomföra sådana beslut) fastställs endast en ansvarig tillsynsmyndighet för det multinationella företaget.

I sådana situationer är det viktigt att företagen exakt fastställer var besluten om ändamålen och medlen för behandlingen fattas. Det ligger i de personuppgiftsansvarigas och personuppgiftsbiträdenas intresse att rätt ansvarig tillsynsmyndighet fastställs, eftersom de då vet vilken tillsynsmyndighet de ska vända sig till med avseende på deras olika efterlevnadsskyldigheter enligt den allmänna dataskyddsförordningen. Dessa skyldigheter omfattar i förekommande fall att utnämna ett dataskyddsombud eller samråda om behandling som medför sådana risker som den personuppgiftsansvarige inte kan begränsa med rimliga medel. Syftet med de relevanta bestämmelserna i den allmänna dataskyddsförordningen är att dessa efterlevnadsuppgifter ska vara hanterliga.

Exemplen nedan åskådliggör detta:

Exempel 1: Ett livsmedelsföretag har sitt huvudkontor (dvs. centrala förvaltning) i Rotterdam i Nederländerna. Det har verksamhetsställen i flera andra EU-länder, som står i kontakt med enskilda personer där. Alla verksamhetsställen använder samma programvara för att behandla konsumenters personuppgifter för marknadsföringsändamål. Alla beslut om ändamålen och medlen för behandlingen av konsumenternas personuppgifter för marknadsföringsändamål fattas vid huvudkontoret i Rotterdam. Detta innebär att företagets ansvariga tillsynsmyndighet för denna gränsöverskridande behandling är Nederländernas tillsynsmyndighet.

Exempel 2: En bank har sitt huvudkontor i Frankfurt och all[2]behandling i samband med bankverksamheten organiseras därifrån, men försäkringsavdelningen är förlagd till Wien. Om verksamhetsstället i Wien har befogenhet att besluta om all behandling som rör försäkringsuppgifter och genomföra dessa beslut i hela EU är det enligt artikel 4.16 i den allmänna dataskyddsförordningen den österrikiska tillsynsmyndigheten som är ansvarig tillsynsmyndighet för den gränsöverskridande behandlingen av personuppgifter för

[2] I samband med behandling av personuppgifter för bankändamål står det klart att detta omfattar många olika behandlingsverksamheter. För enkelhetens skull behandlas all behandling därför som ett enda ändamål. Detsamma gäller behandlingen för försäkringsändamål.

försäkringsändamål, och de tyska myndigheterna (tillsynsmyndigheten i Hessen) skulle övervaka behandlingen av personuppgifter för bankändamål, var kunderna än finns någonstans[3].

2.1.1 Kriterier för att avgöra en personuppgiftsansvarigs huvudsakliga verksamhetsställe när denna plats inte är den plats där den personuppgiftsansvarige har sin centrala förvaltning i EU

Skäl 36 i den allmänna dataskyddsförordningen är användbart för att klargöra vilken den viktigaste faktorn ska vara vid fastställandet av den personuppgiftsansvariges huvudsakliga verksamhetsställe, om inte kriteriet för central förvaltning är tillämpligt. Det handlar bland annat om att fastställa var den faktiska och reella ledningen finns, dvs. den ledning som fattar de huvudsakliga besluten vad avser ändamål och medel för behandlingen med hjälp av en stabil struktur. I skäl 36 klargörs också följande: ”Att tekniska medel och teknik för behandling av personuppgifter eller behandlingsverksamhet finns och används visar i sig inte att det rör sig om ett huvudsakligt verksamhetsställe och utgör därför inte avgörande kriterier för ett huvudsakligt verksamhetsställe”.

Det är den personuppgiftsansvarige som själv fastställer var det huvudsakliga verksamhetsstället finns och följaktligen vilken tillsynsmyndighet som är ansvarig tillsynsmyndighet. Detta kan dock bestridas av respektive berörda tillsynsmyndigheter i efterhand.

Nedanstående faktorer är till hjälp för att avgöra platsen för en personuppgiftsansvarigs huvudsakliga verksamhetsställe enligt villkoren i den allmänna dataskyddsförordningen när denna plats inte är platsen för den personuppgiftsansvariges centrala förvaltning i EU.

- Var ges det slutliga godkännandet av beslut om ändamål och medel för behandlingen?
- Var fattas beslut om affärsverksamhet som omfattar behandling av personuppgifter?
- Var finns den faktiska befogenheten att genomföra beslut?
- Var finns direktören (eller direktörerna) som har det huvudsakliga ansvaret för den gränsöverskridande behandlingen?
- Var är den personuppgiftsansvarige eller personuppgiftsbiträdet registrerad som ett företag, om behandlingen sker inom ett enda territorium?

Observera att denna lista inte är uttömmande. Andra faktorer kan vara relevanta beroende på den personuppgiftsansvarige eller behandlingen i fråga. Om en tillsynsmyndighet har skäl att tvivla på att det verksamhetsställe som fastställts av den personuppgiftsansvarige verkligen är det huvudsakliga verksamhetsstället enligt den allmänna dataskyddsförordningen, kan den naturligtvis begära att den personuppgiftsansvarige lämnar nödvändiga kompletterande uppgifter för att visa var det huvudsakliga verksamhetsstället är beläget.

[3] Det är också viktigt att tänka på att den allmänna dataskyddsförordningen föreskriver möjligheten till lokal tillsyn i speciella fall. Se skäl 127: *”Varje tillsynsmyndighet* ***som inte agerar som ansvarig tillsynsmyndighet bör vara behörig att behandla lokala fall****, om den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat men ärendet för den specifika behandlingen* ***endast avser behandling som utförs i en enda medlemsstat och endast omfattar registrerade i denna enda medlemsstat****, till exempel om ärendet avser behandling av anställdas personuppgifter inom ramen för en medlemsstats specifika anställningsförhållanden.”* Denna princip innebär att tillsynen av personuppgifter om anställda kan ligga på flera tillsynsmyndigheters ansvar, då behandlingen av personuppgifter har samband med lokala anställningsförhållanden.

2.1.2 Företagskoncerner

När behandling genomförs av en företagskoncern som har sitt huvudkontor i EU förutsätts verksamhetsstället för det företag som har den övergripande kontrollen vara den plats där besluten om behandling av personuppgifter fattas. Detta verksamhetsställe anses därför vara koncernens huvudsakliga verksamhetsställe, utom om besluten om ändamålen och medlen för behandlingen fattas av ett annat verksamhetsställe. Moderföretaget eller koncernens operativa huvudkontor i EU är sannolikt det huvudsakliga verksamhetsstället, eftersom det är den plats där den centrala förvaltningen finns.

Definitionen innehåller en hänvisning till platsen för en personuppgiftsansvarigs centrala förvaltning, och den fungerar väl för organisationer som har ett centraliserat huvudkontor för beslutsfattande och en filialstruktur. I sådana fall står det klart att det är företagets huvudkontor som har befogenheten att fatta beslut om gränsöverskridande behandling av personuppgifter och att genomföra dessa beslut. Här kan det avgöras direkt vilken plats som är det huvudsakliga verksamhetsstället, och därmed vilken tillsynsmyndighet som är ansvarig tillsynsmyndighet. En koncerns beslutssystem kan dock vara mer invecklat, där olika verksamhetsställen ges oberoende beslutsbefogenheter för gränsöverskridande behandling. De kriterier som anges ovan bör vara till hjälp för koncerner för att fastställa deras huvudsakliga verksamhetsställe.

2.1.3 Gemensamt personuppgiftsansvariga

Frågan om vilken tillsynsmyndighet som ska vara ansvarig när två eller flera personuppgiftsansvariga som är etablerade i EU gemensamt avgör ändamålen och medlen för behandlingen, dvs. när det finns gemensamma personuppgiftsansvariga, behandlas inte uttryckligen i den allmänna dataskyddsförordningen. I artikel 26.1 och skäl 79 klargörs att i situationer där personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen tillsammans med andra personuppgiftsansvariga ska de under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt förordningen. För att kunna utnyttja principen om en enda kontaktpunkt bör gemensamt personuppgiftsansvariga därför utse (bland de verksamhetsställen där beslut fattas) vilka av de gemensamt personuppgiftsansvarigas verksamhetsställen som har befogenhet att genomföra beslut om behandling med avseende på alla gemensamt personuppgiftsansvariga. Detta verksamhetsställe anses därefter vara det huvudsakliga verksamhetsstället för sådan behandling som utförs av de gemensamt personuppgiftsansvariga. Arrangemanget med gemensamt personuppgiftsansvariga påverkar inte ansvarsbestämmelserna i den allmänna dataskyddsförordningen, särskilt artikel 82.4.

2.2 Gränsfall

Det kommer att uppstå gränsfall och komplexa situationer, där det är svårt att fastställa det huvudsakliga verksamhetsstället eller avgöra var besluten om behandling fattas. Så kan vara fallet när behandlingen är gränsöverskridande och den personuppgiftsansvarige är etablerad i flera medlemsstater men inte har sin centrala förvaltning i EU, och när inget av verksamhetsställena i EU fattar beslut om behandling (dvs. besluten fattas endast utanför EU).

I ovanstående fall kan ett företag som genomför gränsöverskridande behandling helst vilja regleras av en ansvarig tillsynsmyndighet för att kunna utnyttja principen om en enda kontaktpunkt. Den allmänna dataskyddsförordningen ger dock ingen lösning för sådana situationer. Det verksamhetsställe som har befogenhet att genomföra beslut om behandlingen och tar ansvaret för denna samt har tillräckliga tillgångar bör under dessa omständigheter utses till huvudsakligt verksamhetsställe av företaget. Om företaget inte utser ett huvudsakligt verksamhetsställe på detta sätt är det inte heller möjligt att utse en ansvarig tillsynsmyndighet. Tillsynsmyndigheterna kan alltid utreda ärenden närmare om det behövs.

”Forum shopping” är inte tillåtet enligt den allmänna dataskyddsförordningen. Om ett företag hävdar att det har sitt huvudsakliga verksamhetsställe i en medlemsstat, men den faktiska och reella ledningen eller beslutsfattandet om behandling av personuppgifter inte sker där, beslutar de relevanta tillsynsmyndigheterna (eller i sista hand Europeiska dataskyddsstyrelsen) vilken tillsynsmyndighet som är ansvarig, med hjälp av objektiva kriterier och med hänsyn till tillgängliga belägg. Processen för att avgöra var det huvudsakliga verksamhetsstället finns kan kräva aktiva efterforskningar och aktivt samarbete av och mellan tillsynsmyndigheterna. Slutsatserna kan inte bara grundas på den granskade organisationens redogörelser. Bevisbördan ligger i sista hand hos de personuppgiftsansvariga och personuppgiftsbiträdena, eftersom det är deras ansvar att visa de relevanta tillsynsmyndigheterna var de berörda besluten om behandling fattas och vilken plats som har befogenhet att genomföra sådana beslut. Noggrann registrering av behandlingen hjälper både organisationerna och tillsynsmyndigheterna att fastställa den ansvariga tillsynsmyndigheten. Den ansvariga tillsynsmyndigheten eller de berörda myndigheterna kan avvisa den personuppgiftsansvariges analys baserat på en objektiv granskning av relevanta fakta, och kan begära ytterligare uppgifter om så behövs.

I vissa fall ber de relevanta tillsynsmyndigheterna den personuppgiftsansvarige att lämna tydliga belägg enligt riktlinjerna från Europeiska dataskyddsstyrelsen om var det huvudsakliga verksamhetsstället finns eller var besluten om en viss typ av behandling fattas. Dessa belägg beaktas vederbörligen och de berörda tillsynsmyndigheterna samarbetar för att besluta vilken av dem som tar ansvaret för utredningen. Sådana ärenden hänskjuts till Europeiska dataskyddsstyrelsen för beslut enligt artikel 65.1 b endast om tillsynsmyndigheterna har motstridiga åsikter om fastställandet av ansvarig tillsynsmyndighet. Oftast bör de relevanta tillsynsmyndigheterna dock kunna enas om ett ömsesidigt tillfredsställande handlingssätt.

2.3 Personuppgiftsbiträden

Enligt den allmänna dataskyddsförordningen får även personuppgiftsbiträden som omfattas av förordningen och har verksamhetsställen i mer än en medlemsstat utnyttja systemet med en enda kontaktpunkt.

Enligt artikel 4.16 b i förordningen ska personuppgiftsbiträdets verksamhetsställe vara den plats i EU där personuppgiftsbiträdet har sin centrala förvaltning eller, om personuppgiftsbiträdet inte har någon central förvaltning i EU, det av personuppgiftsbiträdets verksamhetsställen i EU där den huvudsakliga behandlingen sker.

Enligt skäl 36 bör dock den personuppgiftsansvariges tillsynsmyndighet vara ansvarig tillsynsmyndighet i sådana fall som omfattar både en personuppgiftsansvarig och ett

personuppgiftsbiträde. I denna situation blir personuppgiftsbiträdets tillsynsmyndighet en ”berörd tillsynsmyndighet”, och bör delta i samarbetsförfarandet. Denna regel gäller endast om den personuppgiftsansvarige är etablerad i EU. I sådana fall där personuppgiftsansvariga omfattas av den allmänna dataskyddsförordningen enligt artikel 3.2 kan de inte utnyttja mekanismen för en enda kontaktpunkt. Ett personuppgiftsbiträde kan tillhandahålla tjänster till flera personuppgiftsansvariga som är etablerade i olika medlemsstater, till exempel en stor molntjänstleverantör. I ett sådant fall är den ansvariga tillsynsmyndigheten den tillsynsmyndighet som är behörig att agera som ansvarig tillsynsmyndighet för den personuppgiftsansvarige. I praktiken innebär detta att personuppgiftsbiträden kan behöva ha kontakt med flera tillsynsmyndigheter.

3. Andra relevanta frågor

3.1 Den ”berörda tillsynsmyndighetens” roll

Följande anges i artikel 4.22 i den allmänna dataskyddsförordningen:

> *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.*

Syftet med begreppet ”berörd tillsynsmyndighet” är att säkerställa att modellen med en ansvarig tillsynsmyndighet inte hindrar andra tillsynsmyndigheter som berörs att vara med och besluta hur ett ärende behandlas när till exempel enskilda personer som är bosatta utanför den ansvariga tillsynsmyndighetens behörighetsområde i väsentlig grad påverkas av en behandling. När det gäller led a) ovan gäller samma överväganden som vid fastställandet av ansvarig tillsynsmyndighet. Observera att i fråga om led b) måste de registrerade endast vara bosatta i den berörda medlemsstaten, dvs. han eller hon behöver inte vara medborgare i den staten. När det gäller led c) är det vanligen enkelt att i sak fastställa huruvida en viss tillsynsmyndighet har mottagit ett klagomål.

Enligt artikel 56.2 och 56.5 i den allmänna dataskyddsförordningen får en berörd tillsynsmyndighet delta i behandlingen av ett ärende utan att vara ansvarig tillsynsmyndighet. Om den ansvariga tillsynsmyndigheten beslutar att inte behandla ett ärende ska den tillsynsmyndighet som underrättade den ansvariga tillsynsmyndigheten behandla ärendet. Detta överensstämmer med förfarandena enligt artikel 61 (Ömsesidigt bistånd) och artikel 62 (Tillsynsmyndigheters gemensamma insatser) i den allmänna dataskyddsförordningen. Så kan till exempel vara fallet om ett marknadsföringsföretag som har sitt huvudsakliga verksamhetsställe i Paris lanserar en produkt som endast påverkar registrerade som är bosatta i Portugal. I detta fall kan de franska och portugisiska tillsynsmyndigheterna enas om att den portugisiska tillsynsmyndigheten bör ansvara för behandlingen av ärendet. Tillsynsmyndigheterna kan begära att de personuppgiftsansvariga lämnar uppgifter som klargör deras företagsarrangemang. Med tanke på att behandlingen endast har en lokal påverkan, dvs. på enskilda personer i Portugal, kan de franska och portugisiska tillsynsmyndigheterna efter eget gottfinnande fatta beslut om vilken tillsynsmyndighet som bör behandla ärendet, enligt skäl 127.

Enligt den allmänna dataskyddsförordningen ska ansvariga tillsynsmyndigheter och berörda tillsynsmyndigheter, med vederbörlig respekt för varandras åsikter, samarbeta för att se till att ärenden utreds och löses på ett sätt som varje myndighet finner tillfredsställande, med effektiva rättsmedel för de registrerade. Tillsynsmyndigheterna bör sträva efter att enas om ett ömsesidigt godtagbart handlingssätt. Den formella mekanismen för enhetlighet bör endast åberopas om samarbetet inte leder till ett ömsesidigt godtagbart resultat.

Ömsesidigt godtagande av beslut kan gälla för väsentliga slutsatser, men även för det beslutade handlingssättet, inklusive tillsyn (t.ex. fullständig utredning eller begränsad utredning). Det kan även gälla för beslut om att inte behandla ett ärende enligt den allmänna dataskyddsförordningen, till exempel på grund av att det finns en formell prioriteringspolicy, eller på grund av att det finns andra berörda tillsynsmyndigheter enligt beskrivningen ovan.

Samförstånd och god vilja i tillsynsmyndigheternas förbindelser med varandra är avgörande för att den allmänna dataskyddsförordningens process för samarbete och enhetlighet ska fungera.

3.2 Lokal behandling

Lokal behandling av personuppgifter omfattas inte av den allmänna dataskyddsförordningens bestämmelser om samarbete och enhetlighet. Tillsynsmyndigheterna ska respektera sina respektive befogenheter för att hantera lokal behandling på lokal nivå. Behandling som genomförs av offentliga myndigheter hanteras alltid också på lokal nivå.

3.3 Företag som inte är etablerade i EU

Den allmänna dataskyddsförordningens mekanism för samarbete och enhetlighet tillämpas endast på personuppgiftsansvariga som har ett eller flera verksamhetsställen inom EU. Om ett företag inte har något verksamhetsställe i EU, men har ett ombud i någon av medlemsstaterna, innebär detta inte att systemet med en enda kontaktpunkt tillämpas. Det innebär i sin tur att personuppgiftsansvariga som inte har ett verksamhetsställe i EU måste ha kontakt med lokala tillsynsmyndigheter i varje medlemsstat där de är aktiva, via sitt lokala ombud.

Riktlinjer antagna i Bryssel den 13 december 2016

På arbetsgruppens vägnar,
ordförande
Isabelle Falque-Pierrotin

Senast granskade och antagna den 5 april 2017

På arbetsgruppens vägnar,
ordförande
Isabelle Falque-Pierrotin

BILAGA – Frågor till hjälp för fastställandet av ansvarig tillsynsmyndighet

1. Genomför den personuppgiftsansvarige eller personuppgiftsbiträdet gränsöverskridande behandling av personuppgifter?

a. Ja, om

- den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat, och
- behandlingen av personuppgifter sker inom ramen för verksamhetsställen i mer än en medlemsstat.

➢ I detta fall, gå till avsnitt 2.

b. Ja, om

- behandlingen av personuppgifter sker inom ramen för verksamheten vid den personuppgiftsansvariges eller personuppgiftsbiträdets enda verksamhetsställe i unionen, men
- behandlingen i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka de registrerade i mer än en medlemsstat.

➢ I detta fall är den ansvariga tillsynsmyndigheten den myndighet som ansvarar för den personuppgiftsansvariges eller personuppgiftsbiträdets enda verksamhetsställe i en enda medlemsstat. Detta måste logiskt sett vara den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga verksamhetsställe, eftersom det är det enda verksamhetsstället.

2. Hur fastställer man den ansvariga tillsynsmyndigheten?

a. Om endast personuppgiftsansvariga berörs:

i. Fastställ den plats i EU där den personuppgiftsansvarige har sin centrala förvaltning.

ii. Tillsynsmyndigheten i det land där den centrala förvaltningen finns är då den personuppgiftsansvariges ansvariga tillsynsmyndighet.

Följande måste dock beaktas:

iii. Om besluten om ändamålen och medlen för behandlingen fattas vid ett annat verksamhetsställe i EU och det verksamhetsstället har befogenhet att genomföra besluten, är det tillsynsmyndigheten i det land där verksamhetsstället finns som är ansvarig tillsynsmyndighet.

b. Om både personuppgiftsansvariga och personuppgiftsbiträden berörs:

i. Kontrollera om den personuppgiftsansvarige är etablerad i EU och omfattas av systemet med en enda kontaktpunkt. Om så är fallet:

ii. Fastställ den personuppgiftsansvariges ansvariga tillsynsmyndighet. Denna myndighet är också ansvarig tillsynsmyndighet för personuppgiftsbiträdet.

iii. Den tillsynsmyndighet (ej ansvarig) som är behörig för personuppgiftsbiträdet blir då en ”berörd myndighet” – se punkt 3.

c. Om endast personuppgiftsbiträden berörs:

i. Fastställ den plats i EU där personuppgiftsbiträdet har sin centrala förvaltning.

ii. Om personuppgiftsbiträdet inte har sin centrala förvaltning i EU ska det fastställas vid vilket verksamhetsställe i EU personuppgiftsbiträdet huvudsakligen genomför behandlingen.

d. Om gemensamt personuppgiftsansvariga berörs:

i. Kontrollera om de gemensamt personuppgiftsansvariga är etablerade i EU.

ii. Jämför de verksamhetsställen där besluten om ändamålen och medlen för behandlingen fattas, och fastställ vilket verksamhetsställe som har befogenhet att genomföra besluten med avseende på samtliga gemensamt personuppgiftsansvariga. Detta verksamhetsställe anses därefter vara det huvudsakliga verksamhetsstället för den behandling som utförs av de gemensamt personuppgiftsansvariga. Den ansvariga tillsynsmyndigheten är myndigheten i det land där verksamhetsstället finns.

3. Finns det några ”berörda tillsynsmyndigheter”?

En myndighet är en ”berörd myndighet”

- när den personuppgiftsansvarige eller personuppgiftsbiträdet har ett verksamhetsställe på myndighetens territorium, eller
- när de registrerade på myndighetens territorium i väsentlig grad påverkas eller sannolikt i väsentlig grad kommer att påverkas av behandlingen, eller
- när en viss myndighet mottar ett klagomål.

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 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.

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, beteendestyrd 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 dataskyddsombud? Om ja, under vilka förhållanden? (artikel 37.2 och 37.3)

Enligt den allmänna dataskyddsförordningen får en koncern 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 enligt den allmänna dataskyddsförordningen. Dataskyddsombudet 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 dataskyddsombudet 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 dataskyddsombudet.

Närmare information finns i avsnitt 2.3 i riktlinjerna.

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

Ja. Enligt artikel 37.6 får dataskyddsombudet 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.

Om dataskyddsombudet är externt gäller samtliga krav i artiklarna 37–39 för denna person. I riktlinjerna anges att 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 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 dataskyddsombudets 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 *utses 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.