ARTIKEL 29-ARBETSGRUPPEN FÖR UPPGIFTSSKYDD

18/SV

WP250rev.01

Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679

Antagna den 3 oktober 2017

Senast granskade och antagna den 6 februari 2018

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 sekretariatet finns hos direktorat C (Grundläggande rättigheter och unionsmedborgarskap) på Europeiska kommissionens generaldirektorat för rättsliga frågor och konsumentfrågor, B-1049 Bryssel, Belgien, kontor MO-59 02/013.

Webbplats: http://ec.europa.eu/justice/data-protection/index_en.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,

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

med beaktande av dess arbetsordning.

INNEHÅLLSFÖRTECKNING

INLEDNING

I den allmänna dataskyddsförordningen införs ett krav på att en personuppgiftsincident (nedan kallad *incident*) ska anmälas till den behöriga nationella tillsynsmyndigheten[1] (eller om det rör sig om en gränsöverskridande incident, till den ansvariga tillsynsmyndigheten) och i vissa fall att de personer vars personuppgifter har påverkats av incidenten ska informeras om detta.

Vissa organisationer är redan skyldiga att anmäla incidenter, t.ex. företag som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster (i enlighet med direktiv 2009/136/EG och förordning (EU) nr 611/2013)[2]. Vissa medlemsstater har även själva infört en nationell skyldighet att anmäla incidenter. Det kan röra sig om skyldigheten att anmäla incidenter som utöver företag som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster inbegriper olika kategorier av personuppgiftsansvariga (t.ex. i Tyskland och Italien), eller en skyldighet att rapportera alla incidenter (som i Nederländerna) Andra medlemsstater har relevanta uppförandekoder på området (t.ex. Irland[3]). Även om många dataskyddsmyndigheter i EU för närvarande uppmuntrar personuppgiftsansvariga att anmäla incidenter innehåller dataskyddsdirektivet 95/46/EG[4], som dataskyddsförordningen ersätter, inte någon specifik skyldighet att anmäla incidenter och ett sådant krav blir därför en nyhet för många organisationer. Genom dataskyddsförordningen blir det nu obligatoriskt för alla personuppgiftsansvariga att anmäla incidenter, såvida det inte är osannolikt att en incident medför en risk för enskilda personers rättigheter och friheter[5]. Personuppgiftsbiträden har också en viktig roll att spela och de måsta anmäla alla incidenter till sin personuppgiftsansvarige[6].

Artikel 29-arbetsgruppen anser att det nya anmälningskravet har flera fördelar. När personuppgiftsansvariga anmäler en incident till tillsynsmyndigheten kan de få råd om huruvida de individer som påverkas måste informeras. Tillsynsmyndigheten får till och med förelägga den personuppgiftsansvarige att meddela den registrerade att en incident har ägt rum.[7] Genom att meddela enskilda att en incident har inträffat kan den personuppgiftsansvarige informera dessa om vilka risker incidenten medför och vilka åtgärder de kan vidta för att skydda sig mot potentiella konsekvenser. Incidenthanteringsplanerna bör vara inriktade på att skydda enskilda och deras personuppgifter. Anmälan av incidenter bör därför ses som ett verktyg för att öka skyddet för personuppgifter. Det bör påpekas att underlåtelse att rapportera en incident till en enskild eller en tillsynsmyndighet kan medföra att den personuppgiftsansvarige påförs en sanktionsavgift enligt artikel 83 a.

---

[1] Se artikel 4.21 i dataskyddsförordningen.

[2] Se http://eur-lex.europa.eu/legal-content/SV/TXT/?uri=celex:32009L0136 och http://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX%3A32013R0611

[3] Se https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[4] Se http://eur-lex.europa.eu/legal-content/SV/TXT/?uri=celex:31995L0046

[5] De rättigheter som fastställts i Europeiska unionens stadga om de grundläggande rättigheterna, tillgänglig påhttp://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:12012P/TXT

[6] Se artikel 33.2. Detta påminner om artikel 5 i förordning (EU) nr 611/2013, enligt vilken en leverantör som har kontrakterats för att leverera en del av de elektroniska kommunikationstjänsterna (utan att ha ett direkt kontraktsförhållande med abonnenter) omedelbart ska informera den leverantör som har tillhandahållit kontraktet i händelse av en incident.

[7] Se artiklarna 34.4 och 58.2 e.

Personuppgiftsansvariga och personuppgiftsbiträden uppmuntras därför att planera i förväg och införa processer för att upptäcka och snabbt begränsa en incident, bedöma riskerna för enskilda[8], och sedan avgöra om det är nödvändigt att anmäla incidenten till tillsynsmyndigheten, och vid behov informera berörd person. Anmälan till tillsynsmyndigheten bör utgöra en del av incidenthanteringsplanen.

Dataskyddsförordningen innehåller bestämmelser om när en incident behöver anmälas, och till vem, samt vilken information som bör tillhandahållas inom ramen för anmälan. Den information som krävs för anmälan kan lämnas i omgångar, men personuppgiftsansvariga bör i alla händelser agera snabbt vid incidenter.

I sitt yttrande 3/2014 om anmälan av personuppgiftsbrott[9] gav artikel 29-arbetsgruppen vägledning till personuppgiftsansvariga för att hjälpa dem att avgöra om de ska underrätta registrerade vid en incident. I yttrandet diskuterades skyldigheterna för företag som tillhandahåller elektroniska kommunikationstjänster enligt direktiv 2002/58/EG och gavs exempel från flera olika sektorer, inom ramen för det dåvarande förslaget till dataskyddsförordning, samt exempel på god praxis för alla personuppgiftsansvariga.

I dessa riktlinjer förklaras den obligatoriska anmälan av incidenter och det krav på information till registrerade som finns i dataskyddsförordningen, och vissa åtgärder som personuppgiftsansvariga och personuppgiftsbiträden kan vidta för att fullgöra dessa nya skyldigheter. I riktlinjerna ges även exempel på olika typer av incidenter och vem som ska underrättas i olika situationer.

I. Anmälan av personuppgiftsincidenter enligt dataskyddsförordningen

A. Grundläggande säkerhetsöverväganden

Ett av kraven i dataskyddsförordningen är att personuppgifter, med användning av lämpliga tekniska och organisatoriska åtgärder, ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller olaglig behandling och mot förlust, förstöring eller skada genom olyckshändelse[10].

Enligt dataskyddsförordningen måste därför både personuppgiftsansvariga och personuppgiftsbiträden vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken för de personuppgifter som behandlas. Åtgärderna bör beakta den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter[11]. Enligt dataskyddsförordningen måste dessutom alla lämpliga tekniska skyddsåtgärder och alla lämpliga organisatoriska åtgärder ha vidtagits för att omedelbart fastställa om en incident har ägt rum, vilket i sin tur är avgörande för om anmälningsskyldigheten ska fullgöras[12].

---

[8] Detta kan säkerställas genom övervaknings- och granskningskravet i en konsekvensbedömning avseende dataskydd, som krävs för behandlingar som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter (artikel 35.1 och 35.11).

[9] Se yttrande 3/2014 om anmälan om personuppgiftsbrott: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[10] Se artiklarna 5.1 f och 32.

[11] Artikel 32, se även skäl 83.

[12] Se skäl 87.

Ett viktigt inslag i all dataskyddspolitik är därför möjligheten att om det går förhindra en incident, och om en incident ändå äger rum reagera snabbt på den.

B. Vad är en personuppgiftsincident?

1. Definition

För att hantera en incident måste den personuppgiftsansvarige först kunna fastställa en incident. I dataskyddsförordningen definieras ”personuppgiftsincident” på följande sätt i artikel 4.12:

> ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

Vad som avses med ”förstöring” av personuppgifter borde vara ganska tydligt. I detta fall existerar uppgifterna inte längre eller så existerar de i ett format som gör att den personuppgiftsansvarige inte längre kan använda dem. Vad som avses med ”skada” borde också vara ganska tydligt. Det är när personuppgifter har ändrats, blivit korrupta eller inte längre är fullständiga. När det gäller ”förlust” av personuppgifter bör detta tolkas som att uppgifterna fortfarande existerar, men att den personuppgiftsansvarige har förlorat kontrollen över eller åtkomsten till dem, eller inte längre innehar uppgifterna. Slutligen kan obehörig eller olaglig behandling innefatta utlämnandet av personuppgifter (eller åtkomst till dessa) till mottagare som inte är behöriga att motta (eller få åtkomst till) uppgifterna, eller någon annan form av behandling som strider mot dataskyddsförordningen.

Exempel

Ett exempel på förlust av personuppgifter är om en enhet med en kopia av den personuppgiftsansvariges kunddatabas har förlorats eller stulits. Ett annat exempel på förlust är när en enda kopia av en uppsättning personuppgifter har krypterats av s.k. ransomware, eller har krypterats av den personuppgiftsansvarige med hjälp av en krypteringsnyckel som denne inte längre har kvar.

I vilket fall som helst borde det vara tydligt att en personuppgiftsincident är en allvarlig säkerhetsincident. I artikel 4.12 i dataskyddsförordningen anges dock att dataskyddsförordningen endast ska tillämpas vid *personuppgiftsincidenter*. En sådan incident medför att den personuppgiftsansvarige inte kan säkerställa att de principer beträffande behandling av personuppgifter som anges i artikel 5 i dataskyddsförordningen verkligen iakttas. Detta visar på skillnaden mellan en säkerhetsincident och en personuppgiftsincident. Även om alla personuppgiftsincidenter är säkerhetsincidenter är nämligen inte alla säkerhetsincidenter nödvändigtvis personuppgiftsincidenter[13].

En incidents potentiella negativa effekter för enskilda diskuteras nedan.

2. Typer av personuppgiftsincidenter

I sitt yttrande 3/2014 om personuppgiftsbrott förklarade artikel 29-arbetsgruppen att incidenter kan kategoriseras utifrån följande tre välkända informationssäkerhetsprinciper[14]:

[13] Notera att en säkerhetsincident inte begränsas till hotmodeller där en organisation utsätts för ett angrepp från en extern källa, utan även omfattar incidenter till följd av intern behandling som bryter mot säkerhetsprinciper.

[14] Se yttrande 3/2014.

- ”Konfidentialitetsbrott” – vid obehörigt eller oavsiktligt röjande av eller åtkomst till personuppgifter.
- ”Integritetsbrott” – vid obehörig eller oavsiktlig ändring av personuppgifter.
- ”Tillgänglighetsbrott” – vid obehörig eller oavsiktlig förlust av åtkomst[15] till, eller förstöring av, personuppgifter.

Notera även att en incident, beroende på omständigheterna, på en och samma gång kan röra personuppgifters konfidentialitet, integritet och tillgänglighet, eller varje tänkbar kombination av dessa.

Samtidigt som det är relativt lätt att avgöra om det har skett ett konfidentialitets- eller integritetsbrott är det mindre uppenbart huruvida det har skett ett tillgänglighetsbrott. En personuppgiftsincident betraktas alltid som ett tillgänglighetsbrott, även vid permanent förlust eller förstöring av personuppgifter.

Exempel

Exempel på förlust av tillgänglighet är bland annat om uppgifter har raderats, antingen oavsiktligt eller av en obehörig person, eller, när det gäller krypterade uppgifter, om dekrypteringsnyckeln har försvunnit. Om den personuppgiftsansvarige inte kan återställa åtkomsten till uppgifterna med hjälp av t.ex. en säkerhetskopia betraktas detta som en permanent förlust av tillgänglighet.

En förlust av tillgänglighet kan även äga rum om det har funnits stora störningar i en organisations normala tjänst, exempelvis om det inte har gått att få tillgång till personuppgifter på grund av ett strömavbrott eller ett överbelastningsangrepp.

Frågan är huruvida en tillfällig förlust av åtkomst till personuppgifter ska betraktas som en incident, och om så är fallet en incident som måste anmälas. I artikel 32 i dataskyddsförordningen (som har rubriken ”Säkerhet i samband med behandlingen”) förklaras att när man vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken bör man bland annat beakta ”förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna” och ”förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident”.

En säkerhetsincident som resulterar i att personuppgifter under en tid inte är tillgängliga är därför också en typ av personuppgiftsincident, eftersom bristande åtkomst till uppgifterna kan få stora konsekvenser för fysiska personers rättigheter och friheter. Om personuppgifter inte är tillgängliga på grund av ett planerat underhåll är detta dock inte en ”säkerhetsincident” i den mening som avses i artikel 4.12.

På samma sätt som när det gäller permanent förlust eller förstöring av personuppgifter (eller någon annan typ av incident) bör en incident som innebär att uppgifterna tillfälligt inte går att komma åt dokumenteras i enlighet med artikel 33.5. Detta hjälper den personuppgiftsansvarige att visa för tillsynsmyndigheten att artikeln efterlevs. Tillsynsmyndigheten kan begära att få ta del av

[15] Det är allmänt vedertaget att ”åtkomst” är en grundläggande del av ”tillgänglighet”. Se exempelvis NIST SP800-53rev4, som definierar ”tillgänglighet” på följande sätt: ”Säkerställande av snabb och tillförlitlig åtkomst till och användning av uppgifter”, tillgänglig på http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. I CNSSI-4009 hänvisas dessutom till: ”Snabb, tillförlitlig åtkomst till data och informationstjänster för behöriga användare.” Se https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. I ISO/IEC 27000:2016 definieras också ”tillgänglighet” som ”Egenskapen att finnas tillgänglig och vara användbar för en behörig enhet”: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

dokumentationen[16]. Omständigheterna i det enskilda fallet avgör om det är, eller inte är, nödvändigt att anmäla incidenten till tillsynsmyndigheten och underrätta de personer som påverkas. Den personuppgiftsansvarige måste bedöma sannolikheten för och i vilken grad bristande tillgänglighet till personuppgifter påverkar fysiska personers rättigheter och friheter. I enlighet med artikel 33 måste den personuppgiftsansvarige anmäla en personuppgiftsincident såvida det inte är osannolikt att incidenten medför en risk för fysiska personers rättigheter och friheter. Detta måste naturligtvis bedömas från fall till fall.

Exempel

Om viktiga medicinska uppgifter om patienter inte är tillgängliga på ett sjukhus, om än tillfälligt, kan detta medföra en risk för enskildas rättigheter och friheter. Det kan t.ex. bli nödvändigt att ställa in operationer och liv kan vara i fara.

Om ett mediebolags system ligger nere under flera timmar (t.ex. på grund av ett strömavbrott), och det bolaget därför inte kan skicka ut nyhetsbrev till sina abonnenter, är det däremot osannolikt att detta medför en risk för enskildas rättigheter och friheter.

Notera även att om en personuppgiftsansvarigs system endast ligger nere tillfälligt och inte påverkar enskilda är det viktigt att den personuppgiftsansvarige överväger alla tänkbara konsekvenser som en incident kan leda till, eftersom det fortfarande kan vara nödvändigt att anmäla incidenten av andra skäl.

Exempel

Om en dataenhet blir infekterad av ransomware (skadlig programvara som krypterar den personuppgiftsansvariges enhet tills en lösensumma betalas) kan detta leda till en tillfällig förlust av tillgänglighet om uppgifterna kan återställas från en säkerhetskopia. Det har dock skett ett nätverksintrång och det kan vara nödvändigt att anmäla incidenten om den kan klassificeras som ett konfidentialitetsbrott (dvs. angriparen har fått åtkomst till personuppgifter) och detta medför en risk för enskildas rättigheter och friheter.

3. Tänkbara konsekvenser av en personuppgiftsincident

En incident kan potentiellt få många olika allvarliga negativa effekter för enskilda, som kan leda till fysisk, materiell eller immateriell skada. I dataskyddsförordningen förklaras att detta kan inbegripa förlust av kontrollen över enskildas personuppgifter eller till begränsning av deras rättigheter, diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, obehörigt hävande av pseudonymisering, skadat anseende och förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt. Dessa personer kan även drabbas av andra betydande ekonomiska eller sociala nackdelar[17].

Enligt dataskyddsförordningen är en personuppgiftsansvarig därför skyldig att anmäla en incident till den behöriga tillsynsmyndigheten, såvida det inte är osannolikt att incidenten medför en risk för sådana negativa effekter. Om det sannolikt finns en hög risk för sådana negativa effekter är den personuppgiftsansvarige enligt dataskyddsförordningen skyldig att underrätta de personer som påverkas så snart detta rimligtvis är möjligt[18].

[16] Se artikel 33.5.

[17] Se även skälen 85 och 75.

[18] Se även skäl 86.

Vikten av att kunna fastställa en incident, bedöma risken för enskilda och sedan anmäla incidenten om så krävs, framhålls i skäl 87 i dataskyddsförordningen.

> ”Det bör undersökas huruvida alla lämpliga tekniska skyddsåtgärder och alla lämpliga organisatoriska åtgärder har vidtagits för att omedelbart fastställa om en personuppgiftsincident har ägt rum och skyndsamt informera tillsynsmyndigheten och den registrerade. Att en anmälan gjordes utan onödigt dröjsmål bör fastställas med hänsyn tagen bl.a. till personuppgiftsincidentens art och svårighetsgrad och dess följder och negativa effekter för den registrerade. En sådan anmälan kan leda till ett ingripande från tillsynsmyndighetens sida i enlighet med dess uppgifter och befogenheter enligt denna förordning.”

Ytterligare vägledning om bedömningen av risken för negativa effekter för enskilda ges i avsnitt IV.

Om personuppgiftsansvariga inte anmäler en incident till tillsynsmyndigheten och/eller de registrerade, även om villkoren i artiklarna 33 och/eller 34 är uppfyllda måste tillsynsmyndigheten överväga alla sina möjligheter till korrigerande åtgärder, inbegripet påförandet av en lämplig administrativ sanktionsavgift[19], antingen tillsammans med en korrigerande åtgärd enligt artikel 58.2 eller separat. Om valet faller på en administrativ sanktionsavgift kan denna uppgå till upp till 10 000 000 euro eller 2 procent av ett företags totala globala årsomsättning enligt artikel 83.4 a i dataskyddsförordningen. Det är även viktigt att ha i åtanke att i vissa fall kan en underlåtelse att anmäla en incident antingen vara ett tecken på att befintliga säkerhetsåtgärder saknas eller att det finns brister i de befintliga säkerhetsåtgärderna. I artikel 29-arbetsgruppens riktlinjer om administrativa sanktionsavgifter anges följande: ”Om flera olika överträdelser har ägt rum tillsammans i ett enskilt fall kan tillsynsmyndigheten tillämpa administrativa sanktionsavgifter på en nivå som är effektiv, proportionell och avskräckande inom gränsen för överträdelsen med högst svårighetsgrad.” I så fall har tillsynsmyndigheten även möjlighet att ålägga sanktioner för dels underlåtelse att anmäla eller meddela incidenten (artiklarna 33 och 34), dels avsaknaden av (lämpliga) säkerhetsåtgärder (artikel 32), eftersom det rör sig om två olika överträdelser.

II. Artikel 33 – Anmälan till tillsynsmyndigheten

A. När ska en incident anmälas?

1. Kraven i artikel 33

I artikel 33.1 föreskrivs följande:

> ”Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig i enlighet med artikel 55, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.”

I skäl 87 anges följande[20]:

[19] För mer detaljer se artikel 29-arbetsgruppens riktlinjer för tillämpning och fastställande av administrativa sanktionsavgifter, tillgängliga här: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

[20] Skäl 85 är också viktigt här.

”Det bör undersökas huruvida alla lämpliga tekniska skyddsåtgärder och alla lämpliga organisatoriska åtgärder har vidtagits för att omedelbart fastställa om en personuppgiftsincident har ägt rum och skyndsamt informera tillsynsmyndigheten och den registrerade. Att en anmälan gjordes utan onödigt dröjsmål bör fastställas med hänsyn tagen bl.a. till personuppgiftsincidentens art och svårighetsgrad och dess följder och negativa effekter för den registrerade. En sådan anmälan kan leda till ett ingripande från tillsynsmyndighetens sida i enlighet med dess uppgifter och befogenheter enligt denna förordning.”

2. När har en personuppgiftsansvarig fått ”vetskap” om en incident?

Som påpekats ovan föreskriver dataskyddsförordningen att den personuppgiftsansvarige vid en personuppgiftsincident ska anmäla denna utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den. Frågan som uppkommer är när en personuppgiftsansvarig kan anses ha fått ”vetskap” om en incident. Artikel 29-arbetsgruppen anser att en personuppgiftsansvarig ska anses ha fått ”vetskap” när den personuppgiftsansvarige är rimligt säker på att en säkerhetsincident har ägt rum som har medfört att personuppgifter äventyrats.

Som påpekats ovan krävs i dataskyddsförordningen emellertid att den personuppgiftsansvarige ska vidta alla lämpliga tekniska skyddsåtgärder och alla lämpliga organisatoriska åtgärder för att omedelbart fastställa om en personuppgiftsincident har ägt rum och skyndsamt informera tillsynsmyndigheten och de registrerade. Vidare anges att huruvida en anmälan gjordes utan onödigt dröjsmål bör fastställas med hänsyn tagen bl.a. till incidentens art och svårighetsgrad och dess följder och negativa effekter för den registrerade[21]. Detta innebär att den personuppgiftsansvarige snabbt måste skaffa sig ”vetskap” om eventuella incidenter så att denne kan vidta lämpliga åtgärder.

Exakt när en personuppgiftsansvarig kan anses ha fått ”vetskap” om en viss incident beror på omständigheterna i det enskilda fallet. I vissa fall är det redan från början ganska tydligt att en incident har ägt rum. I andra fall kan det dock ta lite tid att fastställa om personuppgifter har äventyrats. Fokus bör dock ligga på snabba insatser för att undersöka en incident så att man kan fastställa huruvida det verkligen har ägt rum en incident, och i så fall vid behov vidta korrigerande åtgärder och anmäla incidenten.

Exempel

1. Om ett USB-minne med okrypterade personuppgifter förloras är det ofta omöjligt att avgöra om obehöriga personer har fått åtkomst till dessa uppgifter. Även om den personuppgiftsansvarige inte kan fastställa om ett konfidentialitetsbrott har ägt rum måste ett sådant fall ändå anmälas eftersom det är rimligt säkert att ett tillgänglighetsbrott har ägt rum. Den personuppgiftsansvarige har fått ”vetskap” när denne insåg att USB-minnet var borta.

2. En tredje part informerar den personuppgiftsansvarige om att han oavsiktligen har mottagit personuppgifter om en av sina kunder och överlämnar bevis för det obehöriga röjandet av uppgifter. Eftersom den personuppgiftsansvarige har fått tydliga bevis för ett konfidentialitetsbrott kan det inte råda någon tvekan om att denne har fått ”vetskap” om incidenten.

3. En personuppgiftsansvarig upptäcker att det har skett ett tänkbart intrång i dennes nätverk. Den personuppgiftsansvarige kontrollerar sina system för att fastställa huruvida personuppgifter i systemet har äventyrats och bekräftar att så är fallet. Eftersom den personuppgiftsansvarige har tydliga bevis för att en incident har ägt rum råder det inte heller i detta fall någon tvekan om att denne har fått ”vetskap” om incidenten.

[21] Se skäl 87.

4. En it-brottsling kontaktar den personuppgiftsansvarige efter att ha hackat dennes system för att begära en lösensumma. Efter att ha kontrollerat systemet för att bekräfta att det har hackats har den personuppgiftsansvarige i så fall tydliga bevis för att en incident har ägt rum och det råder inte någon tvekan om att den personuppgiftsansvarige har fått ”vetskap” om incidenten.

Efter att den personuppgiftsansvarige har informerats om en potentiell incident av en enskild, en medieorganisation eller en annan källa, eller när denne själv har fastställt en säkerhetsincident, får den personuppgiftsansvarige genomföra en kort undersökning för att fastställa huruvida en incident verkligen har ägt rum. Under denna undersökningsperiod kan den personuppgiftsansvarige inte anses ha fått ”vetskap” om incidenten. Man kan dock förvänta sig att den inledande undersökningen ska inledas så snart som möjligt och med en rimlig grad av säkerhet fastställa huruvida en incident har ägt rum. Detta kan sedan följas av en mer ingående undersökning.

Så snart den personuppgiftsansvarige har fått vetskap måste denne anmäla en incident utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar. Under denna period bör den personuppgiftsansvarige bedöma den sannolika risken för enskilda för att fastställa huruvida kravet för anmälan är uppfyllt, samt den eller de åtgärder som behöver vidtas för att hantera incidenten. Den personuppgiftsansvarige kan emellertid redan ha gjort en inledande bedömning av den potentiella risk som en incident kan medföra, som en del av en konsekvensbedömning avseende dataskydd[22] som gjorts före den berörda behandlingen. Konsekvensbedömningen avseende dataskydd kan emellertid vara mer allmän jämfört med de särskilda omständigheterna i samband med en faktisk incident. I vilket fall som helst måste därför ytterligare en bedömning göras som tar hänsyn till de omständigheterna. För närmare information om riskbedömning, se avsnitt IV.

I de flesta fall bör dessa preliminära åtgärder slutföras så snart som möjligt efter den inledande varningen (dvs. när den personuppgiftsansvarige eller personuppgiftsbiträdet misstänker att en säkerhetsincident har ägt rum som kan inbegripa personuppgifter). Endast i undantagsfall bör detta ta längre tid.

Exempel

En person informerar den personuppgiftsansvarige om att han eller hon har fått ett e-postmeddelande från någon som utger sig för att vara den personuppgiftsansvarige och som innehåller personuppgifter om personens (faktiska) användning av den personuppgiftsansvariges tjänst, vilket tyder på att den personuppgiftsansvarige har utsatts för ett angrepp. Den personuppgiftsansvarige genomför en kort undersökning och fastställer ett intrång i sitt nätverk och bevis på obehörig åtkomst till personuppgifter. Den personuppgiftsansvarige anses nu ha fått ”vetskap” och incidenten måste anmälas till tillsynsmyndigheten, såvida det inte är osannolikt att incidenten medför en risk för enskilda personers rättigheter och friheter. Den personuppgiftsansvarige måste vidta lämpliga korrigerande åtgärder för att åtgärda incidenten.

Den personuppgiftsansvarige bör därför ha interna rutiner för att upptäcka och åtgärda en incident. För att hitta oriktigheter i databehandlingen kan den personuppgiftsansvarige eller personuppgiftsbiträdet använda vissa tekniska åtgärder som dataflödes- och logganalysinstrument. Med hjälp av dessa kan man definiera händelser och varningar genom att korrelera loggdata[23]. När en incident upptäcks är det viktigt att denna rapporteras uppåt till lämplig nivå i ledningsstrukturen så att

[22] Se artikel 29-arbetsgruppens riktlinjer om konsekvensbedömning avseende dataskydd här: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[23] Notera att loggdata som underlättar granskning av t.ex. lagring, ändring eller radering av uppgifter också kan klassificeras som personuppgifter avseende den person som inledde respektive behandling.

den kan åtgärdas, och om det krävs anmälas i enlighet med artikel 33 och, vid behov, artikel 34. Sådana åtgärder och rapporteringsmekanismer kan i detalj beskrivas i den personuppgiftsansvariges incidenthanteringsplaner och/eller ledningsstrukturer. På så sätt blir det lättare för den personuppgiftsansvarige att planera effektivt och fastställa vem som inom organisationen har det operativa ansvaret för att åtgärda en incident och hur eller huruvida det är lämpligt att trappa upp en incident.

Den personuppgiftsansvarige bör även ha rutiner för kontakterna med alla personuppgiftsbiträden som denne använder sig av, och som själva är skyldiga att underrätta den personuppgiftsansvarige i händelse av en incident (se nedan).

Samtidigt som det är upp till personuppgiftsansvariga och personuppgiftsbiträden att vidta lämpliga åtgärder för att förhindra, reagera på och åtgärda en incident finns det vissa praktiska åtgärder som alltid kan vidtas.

- Information om alla säkerhetsrelaterade händelser bör riktas direkt till den eller de personer som ansvarar för att åtgärda incidenter, fastställa förekomsten av en incident och göra en riskbedömning.
- Risk för enskilda till följd av en incident (sannolikhet för ingen risk, risk och hög risk), där relevanta avdelningar inom organisationen informeras.
- Incidenten bör anmälas till tillsynsmyndigheten, och vid behov bör de personer som påverkas underrättas om incidenten.
- Samtidigt bör den personuppgiftsansvarige försöka begränsa och återställa incidenten.
- Dokumenteringen av incidenten bör ske fortlöpande.

Den personuppgiftsansvarige har följaktligen en tydlig skyldighet att agera vid en tidig varning och fastställa huruvida en incident verkligen har ägt rum. Denna korta period räcker för att göra en viss undersökning och gör det möjligt för den personuppgiftsansvarige att samla in bevis och andra relevanta upplysningar. Så snart den personuppgiftsansvarige med en rimlig grad av säkerhet har fastställt att en incident har ägt rum måste denne emellertid, om villkoren i artikel 33.1 är uppfyllda, utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om incidenten anmäla den till tillsynsmyndigheten[24]. Om en personuppgiftsansvarig inte agerar snabbt och det blir uppenbart att en incident har ägt rum kan detta betraktas som en underlåtelse att agera i enlighet med artikel 33.

I artikel 32 klargörs att den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå när det gäller personuppgifter. Förmågan att snabbt upptäcka, åtgärda och rapportera en incident bör ses som viktiga inslag i dessa åtgärder

3. Gemensamt personuppgiftsansvariga

Artikel 26 handlar om gemensamt personuppgiftsansvariga och fastställer deras respektive ansvar när det gäller efterlevnaden av dataskyddsförordningen[25]. I detta ingår att fastställa vilken part som är ansvarig för fullgörandet av skyldigheterna enligt artiklarna 33 och 34. Artikel 29-arbetsgruppen rekommenderar att de gemensamt personuppgiftsansvariga ingår avtal om vilken personuppgiftsansvarig som i första hand ska påta sig ansvaret för att fullgöra anmälningsskyldigheten i dataskyddsförordningen.

[24] Se förordning (EEG, Euratom) nr 1182/71 om regler för bestämning av perioder, datum och frister, tillgänglig på: http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:31971R1182&from=SV

[25] Se även skäl 79.

4. Personuppgiftsbiträdenas skyldigheter

Den personuppgiftsansvarige har det övergripande ansvaret för skyddet av personuppgifter, men personuppgiftsbiträdet har en viktig roll för att göra det möjligt för den personuppgiftsansvarige att fullgöra sina skyldigheter. Detta gäller även vid anmälan av incidenter. I artikel 28.3 anges att när uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal eller en annan rättsakt. I artikel 28.3 f anges att det i avtalet eller rättsakten ska föreskrivas att personuppgiftsbiträdet ska ”bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå”.

I artikel 33.2 klargörs att om en personuppgiftsansvarig använder sig av ett personuppgiftsbiträde och personuppgiftsbiträdet får vetskap om en incident ska personuppgiftsbiträdet underrätta den personuppgiftsansvarige ”utan onödigt dröjsmål”. Lägg märke till att personuppgiftsbiträdet inte först måste bedöma sannolikheten för risk till följd av en incident innan personuppgiftsbiträdet underrättar den personuppgiftsansvarige. Det är den personuppgiftsansvarige som måste göra denna bedömning när denne fått vetskap om incidenten. Personuppgiftsbiträdet behöver bara fastställa huruvida en incident har ägt rum och sedan underrätta den personuppgiftsansvarige. Den personuppgiftsansvarige använder personuppgiftsbiträdet för att uppnå detta mål. I princip bör den personuppgiftsansvarige därför anses ha fått ”vetskap” så snart personuppgiftsbiträdet har informerat om incidenten. Personuppgiftsbiträdets skyldighet att underrätta den personuppgiftsansvarige gör det möjligt för den personuppgiftsansvarige att åtgärda incidenten och fastställa huruvida det är nödvändigt att anmäla incidenten till tillsynsmyndigheten i enlighet med artikel 33.1 och informera de personer som påverkas i enlighet med artikel 34.1. Den personuppgiftsansvarige kan också vilja undersöka incidenten, eftersom personuppgiftsbiträdet kanske inte känner till alla relevanta fakta på området, t.ex. om den personuppgiftsansvarige fortfarande har kvar en kopia eller en säkerhetskopia av personuppgifter som personuppgiftsbiträdet har förstört eller förlorat. Detta kan påverka huruvida den personuppgiftsansvarige behöver anmäla incidenten.

I dataskyddsförordningen anges ingen uttrycklig tidsfrist för när personuppgiftsbiträdet måste varna den personuppgiftsansvarige. Det enda som sägs är att detta måste ske ”utan onödigt dröjsmål”. Artikel 29-arbetsgruppen rekommenderar därför att personuppgiftsbiträdet snabbt underrättar den personuppgiftsansvarige, och sedan fortlöpande lämnar fler upplysningar i takt med att mer detaljer blir kända. Detta är viktigt för att den personuppgiftsansvarige ska kunna uppfylla kravet att anmäla incidenten till tillsynsmyndigheten inom 72 timmar.

Som förklarats ovan bör det i avtalet mellan den personuppgiftsansvarige och personuppgiftsbiträdet anges hur kraven i artikel 33.2 och andra bestämmelser i dataskyddsförordningen ska uppfyllas. I detta kan ingå ett krav på tidig anmälan från personuppgiftsbiträdet, vilket i sin tur underlättar för den personuppgiftsansvarige att uppfylla sin skyldighet att rapportera incidenten till tillsynsmyndigheten inom 72 timmar.

Om personuppgiftsbiträdet utför tjänster för flera personuppgiftsansvariga som alla påverkas av samma incident måste personuppgiftsbiträdet underrätta varje personuppgiftsansvarig om detaljerna kring incidenten.

Ett personuppgiftsbiträde kan göra en anmälan på den personuppgiftsansvariges vägnar om den personuppgiftsansvarige har bemyndigat personuppgiftsbiträdet att göra detta och detta ingår i de avtalade rutinerna mellan den personuppgiftsansvarige och personuppgiftsbiträdet. En sådan anmälan ska göras i enlighet med artiklarna 33 och 34. Det är dock viktigt att notera att den personuppgiftsansvarige fortfarande har det rättsliga ansvaret för anmälan.

B. Information till tillsynsmyndigheten

1. Information som ska lämnas

När en personuppgiftsansvarig anmäler en incident till tillsynsmyndigheten anges i artikel 33.3 att anmälan åtminstone ska

”a) beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,

b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,

c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och

d) beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.”

I dataskyddsförordningen definieras inte kategorier av registrerade eller personuppgiftsposter. Artikel 29-arbetsgruppen föreslår emellertid att kategorier av registrerade ska förstås som de olika typer av enskilda vars personuppgifter har påverkats av en incident. Beroende på vilka deskriptorer som används kan detta bland annat omfatta barn och andra sårbara grupper, personer med funktionsnedsättning, anställda eller kunder. På samma sätt kan kategorier av personuppgiftsposter avse olika typer av poster som den personuppgiftsansvarige kan behandla, t.ex. hälsouppgifter, betyg och andra uppgifter på utbildningsområdet, socialvårdsinformation, finansiella uppgifter, bankkontonummer, passnummer etc.

I skäl 85 klargörs att ett av syftena med att anmäla incidenter är att begränsa potentiella skador för de enskilda. Om typerna av registrerade eller typerna av personuppgifter tyder på en risk för en viss skada till följd av en incident (t.ex. identitetsstöld, bedrägeri, ekonomisk förlust, hot mot tystnadsplikten) är det därför viktigt att dessa kategorier framgår av anmälan. På så sätt kopplas detta till kravet på att beskriva de sannolika effekterna av incidenten.

Om exakt information inte är tillgänglig (t.ex. det exakta antalet registrerade som påverkas) bör detta inte hindra en snabb anmälan av incidenten. Enligt dataskyddsförordningen är det tillåtet att uppskatta hur många personer som påverkas och hur många personuppgiftsposter som berörs. Fokus bör ligga på att åtgärda de negativa effekterna av en incident snarare än att ange exakta sifferuppgifter. När det har fastställts att en incident har ägt rum, men det ännu inte är känt hur omfattande denna är, är en anmälan i flera omgångar (se nedan) ett säkert sätt att fullgöra anmälningsskyldigheten.

I artikel 33.3 anges att den personuppgiftsansvarige ”åtminstone [ska]” tillhandahålla denna information i samband med en anmälan. En personuppgiftsansvarig kan således, vid behov, ange fler detaljer. Olika typer av incidenter (konfidentialitetsbrott, integritetsbrott, tillgänglighetsbrott) kan kräva ytterligare information för att man till fullo ska kunna förklara omständigheterna i det enskilda fallet.

Exempel

Som ett led i anmälan till tillsynsmyndigheten kan den personuppgiftsansvarige anse att det är en god idé att namnge sitt personuppgiftsbiträde om denne är inblandad i grundorsaken till incidenten, särskilt vid en incident som påverkar dataposterna hos många andra personuppgiftsansvariga som använder samma personuppgiftsbiträde.

I alla händelser kan tillsynsmyndigheten begära ytterligare detaljer som ett led i sin undersökning av en incident.

2. Anmälan i omgångar

Beroende på incidentens art kan den personuppgiftsansvarige behöva göra ytterligare undersökningar för att fastställa alla relevanta fakta i samband med incidenten. I artikel 33.4 föreskrivs därför följande:

”Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.”

Detta innebär att dataskyddsförordningen medger att personuppgiftsansvariga inte alltid har all nödvändig information för att anmäla en incident inom 72 timmar efter att de har fått vetskap om den, eftersom alla detaljer om incidenten kanske inte finns att tillgå under denna inledande period. Därför är det tillåtet att göra en anmälan i omgångar. Det är troligare att så är fallet vid mer komplicerade incidenter som vissa typer av it-säkerhetsincidenter, där t.ex. en ingående kriminalteknisk undersökning kan behövas för att fullt ut fastställa incidentens art och i vilken omfattning personuppgifter har äventyrats. I många fall behöver den personuppgiftsansvarige följaktligen göra flera undersökningar och följa upp undersökningarna med mer information i ett senare skede. Detta är tillåtet enligt artikel 33.1, förutsatt att den personuppgiftsansvarige anger skälen till förseningen. Artikel 29-arbetsgruppen rekommenderar att den personuppgiftsansvarige vid en inledande anmälan av en incident till tillsynsmyndigheten även informerar tillsynsmyndigheten om att den personuppgiftsansvarige ännu inte har all den information som krävs och kommer att lämna fler detaljer senare. Tillsynsmyndigheten bör ange hur och när den ytterligare informationen ska tillhandahållas. Detta hindrar inte att den personuppgiftsansvarige när som helst kan tillhandahålla ytterligare information, om denne får vetskap om ytterligare relevanta detaljer om incidenten som måste lämnas till tillsynsmyndigheten.

Anmälningskravet är inriktat på att uppmuntra personuppgiftsansvariga att agera snabbt vid en incident, begränsa den och, om möjligt, återställa de personuppgifter som äventyrats, samt att försöka få relevanta råd från tillsynsmyndigheten. Genom att anmäla en incident till tillsynsmyndigheten inom 72 timmar kan den personuppgiftsansvarige förvissa sig om att dess beslut om att informera eller inte informera enskilda personer är korrekta.

Syftet med att anmäla en incident till tillsynsmyndigheten är emellertid inte enbart att få råd om huruvida de personer som påverkas ska underrättas. I vissa fall är det uppenbart att den personuppgiftsansvarige, på grund av incidentens art och riskens svårighetsgrad, utan dröjsmål måste underrätta de personer som påverkas. Vid ett omedelbart hot om identitetsstöld, eller om en särskild kategori[26] personuppgifter röjs online, bör den personuppgiftsansvarige agera utan onödigt dröjsmål för att begränsa incidenten och underrätta de berörda personerna (se avsnitt III). I undantagsfall kan detta till och med ske innan tillsynsmyndigheten underrättas. Mer allmänt får en anmälan till tillsynsmyndigheten inte användas för att rättfärdiga en underlåtelse att informera den registrerade om incidenten när så krävs.

Det framgår även tydligt att en personuppgiftsansvarig efter att ha gjort en inledande anmälan kan uppdatera tillsynsmyndigheten om en uppföljningsundersökning hittar bevis för att säkerhetsincidenten var begränsad och ingen incident egentligen ägde rum. Denna information kan sedan läggas till den information som redan lämnats till tillsynsmyndigheten och incidenten kan därför registreras som en icke-incident. Att anmäla en incident som i slutändan inte visar sig vara en incident får inga påföljder.

Exempel

[26] Se artikel 9.

En personuppgiftsansvarig underrättar tillsynsmyndigheten inom 72 timmar efter att ha upptäckt en incident i form av ett förlorat USB-minne med en kopia på några av sina kunders personuppgifter. USB-minnet hittas senare efter att ha lagts på fel ställe i den personuppgiftsansvariges lokaler och läggs tillbaka på rätt plats. Den personuppgiftsansvarige uppdaterar tillsynsmyndigheten och begär att anmälan ska ändras.

Lägg märke till att en anmälan i omgångar redan tillämpas i fråga om de befintliga skyldigheterna i direktiv 2002/58/EG, förordning (EU) nr 611/2013 och andra självinrapporterade incidenter.

3. Försenade anmälningar

I artikel 33.1 klargörs att om en anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen. Tillsammans med begreppet anmälan i omgångar medges därför att en personuppgiftsansvarig inte alltid kan anmäla en incident inom den tidsfristen, och att en försenad anmälan kan vara tillåten.

Ett sådant scenario är t.ex. tänkbart om en personuppgiftsansvarig drabbas av flera liknande konfidentialitetsbrott under en kort tidsperiod, och dessa påverkar många registrerade på samma sätt. En personuppgiftsansvarig kan få vetskap om en incident och, samtidigt som denne påbörjar sin undersökning och före anmälan, upptäcka ytterligare liknande incidenter som har andra orsaker. Beroende på omständigheterna kan det ta lite tid för den personuppgiftsansvarige att fastställa omfattningen av incidenterna och i stället för att anmäla varje incident var för sig kan den personuppgiftsansvarige göra en anmälan av flera liknande incidenter, med eventuellt olika orsaker. Detta kan medföra att anmälan till tillsynsmyndigheten försenas och görs mer än 72 timmar efter det att den personuppgiftsansvarige först fick vetskap om dessa incidenter.

I strikt mening är varje enskild incident en incident som kan rapporteras. För att arbetsbördan inte ska bli alltför stor kan den personuppgiftsansvarige emellertid göra en ”samlad” anmälan av alla dessa incidenter, förutsatt att incidenterna rör samma typ av personuppgifter och har ägt rum på samma sätt under en relativt kort tidsperiod. Om en rad incidenter som rör olika typer av personuppgifter har ägt rum på olika sätt bör anmälan ske på vanligt sätt, och varje anmälan rapporteras i enlighet med artikel 33.

Även om dataskyddsförordningen tillåter en viss försening i samband med en anmälan bör detta inte betraktas som något som regelbundet äger rum. Det är värt att påpeka att samlade anmälningar även kan göras för flera liknande incidenter som rapporteras inom 72 timmar.

C. Gränsöverskridande incidenter och incidenter vid verksamhetsställen utanför EU

1. Gränsöverskridande incidenter

Vid gränsöverskridande behandling[27] av personuppgifter kan en incident påverka registrerade i fler än en medlemsstat. I artikel 33.1 klargörs att när en incident har ägt rum bör den personuppgiftsansvarige anmäla incidenten till den tillsynsmyndighet som är behörig i enlighet med dataskyddsförordningen[28]. I artikel 55.1 föreskrivs följande:

”Varje tillsynsmyndighet ska vara behörig att utföra de uppgifter och utöva de befogenheter som tilldelas den enligt denna förordning inom sin egen medlemsstats territorium.”

[27] Se artikel 4.23.

[28] Se även skäl 122.

I artikel 56.1 föreskrivs dock följande:

> ”Utan att det påverkar tillämpningen av artikel 55 ska tillsynsmyndigheten för den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga verksamhetsställe eller enda verksamhetsställe vara behörig att agera som ansvarig tillsynsmyndighet för den personuppgiftsansvariges eller personuppgiftsbiträdets gränsöverskridande behandling i enlighet med det förfarande som föreskrivs i artikel 60.”

I artikel 56.6 föreskrivs dessutom följande:

> ”Den ansvariga tillsynsmyndigheten ska vara den personuppgiftsansvariges eller personuppgiftsbiträdets enda motpart när det gäller den registreringsansvariges eller den personuppgiftsbiträdets gränsöverskridande behandling.”

Detta innebär att när en incident äger rum inom ramen för gränsöverskridande behandling och anmälan krävs måste den personuppgiftsansvarige anmäla incidenten till den ansvariga tillsynsmyndigheten[29]. När den personuppgiftsansvarige utarbetar sin incidenthanteringsplan måste denne därför göra en bedömning av vilken tillsynsmyndighet som är den ansvariga tillsynsmyndighet som anmälan ska riktas till[30]. Detta gör det möjligt för den personuppgiftsansvarige att snabbt reagera på en incident och fullgöra skyldigheterna enligt artikel 33. Det borde stå klart att i händelse av en gränsöverskridande incident måste anmälan göras till den ansvariga tillsynsmyndigheten, som inte nödvändigtvis är belägen på den plats där de registrerade befinner sig, eller ens där incidenten ägde rum. När den personuppgiftsansvarige anmäler en incident till den ansvariga tillsynsmyndigheten bör den personuppgiftsansvarige, i förekommande fall, ange huruvida incidenten berör verksamhetsställen i andra medlemsstater, och i vilka medlemsstater de registrerade sannolikt påverkats av incidenten. Om den personuppgiftsansvarige hyser tvivel beträffande vilken tillsynsmyndighet som är ansvarig bör denne åtminstone underrätta den lokala tillsynsmyndigheten på den plats där incidenten ägde rum.

2. Incidenter på verksamhetsställen utanför EU

Artikel 3 rör dataskyddsförordningens territoriella tillämpningsområde, inbegripet när förordningen ska tillämpas på behandling av personuppgifter som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen. I artikel 3.2 anges framför allt följande[31]:

> ”Denna förordning ska tillämpas på behandling av personuppgifter som avser registrerade som befinner sig i unionen och som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen, om behandlingen har anknytning till:
>
> a) utbjudande av varor eller tjänster till sådana registrerade i unionen, oavsett om dessa varor eller tjänster erbjuds kostnadsfritt eller inte, eller
>
> b) övervakning av deras beteende så länge beteendet sker inom unionen.”

[29] Se artikel 29-arbetsgruppens riktlinjer om fastställande av ansvarig tillsynsmyndighet för personuppgiftsansvariga eller personuppgiftsbiträden, tillgängliga på http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[30] En förteckning över alla europeiska nationella dataskyddsmyndigheter finns att tillgå på http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[31] Se även skälen 23 och 24.

Artikel 3.3 är också relevant och i denna anges följande[32]:

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

Om en personuppgiftsansvarig som inte är etablerad i EU omfattas av artikel 3.2 eller artikel 3.3 och drabbas av en incident är denne därför fortfarande bunden av anmälningsskyldigheten enligt artiklarna 33 och 34. Enligt artikel 27 är en personuppgiftsansvarig (och ett personuppgiftsbiträde) skyldig att utse en företrädare i EU om artikel 3.2 tillämpas. I sådana fall rekommenderar artikel 29-arbetsgruppen att anmälan görs till tillsynsmyndigheten i den medlemsstat där den personuppgiftsansvariges företrädare i EU är etablerad[33]. Om ett personuppgiftsbiträde omfattas av artikel 3.2 är denne på samma sätt bunden av personuppgiftsbiträdenas skyldigheter, särskilt skyldigheten att anmäla incidenten till den personuppgiftsansvarige enligt artikel 33.2.

D. Villkor för när en anmälan inte krävs

I artikel 33.1 klargörs att om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” behöver incidenterna inte anmälas till tillsynsmyndigheten. Ett exempel kan vara när personuppgifter redan finns allmänt tillgängliga och utlämnandet av sådana uppgifter inte utgör en sannolik risk för den enskilde. Detta skiljer sig från de befintliga krav på anmälan av incidenter som gäller för allmänt tillgängliga elektroniska kommunikationstjänster enligt direktiv 2009/136/EG, enligt vilka alla relevanta incidenter ska anmälas till behörig myndighet.

I sitt yttrande 3/2014 om anmälan av personuppgiftsbrott[34] förklarade artikel 29-arbetsgruppen att ett konfidentialitetsbrott som rör personuppgifter som krypterats med hjälp av en algoritm enligt den senaste tekniken ändå är ett personuppgiftsbrott och ska anmälas till myndigheten. Om krypteringsnyckelns konfidentialitet är intakt – dvs. om nyckeln inte äventyrades i någon säkerhetsincident och genererades på ett sätt som inte kan fastställas med tillgängliga tekniska hjälpmedel – är uppgifterna dock i princip oläsbara för obehöriga, och det är därmed inte sannolikt att överträdelsen kommer att inverka menligt på de registrerade. De registrerade behöver därför inte underrättas om incidenten[35]. Även om uppgifterna är krypterade kan en förlust eller ändring emellertid få negativa konsekvenser för registrerade om den personuppgiftsansvarige inte har tillräckliga säkerhetskopior. I så fall måste de registrerade underrättas, även om själva uppgifterna omgärdades av tillräckliga krypteringsåtgärder.

Artikel 29-arbetsgruppen förklarade också att så även skulle vara fallet om personuppgifter, t.ex. lösenord, har hashats och saltats på ett säkert sätt, hashvärdena har beräknats med en kryptografisk hashfunktion enligt den senaste tekniken med nyckel, den nyckel som använts för kondensat av data har inte äventyrats genom någon säkerhetsöverträdelse och den nyckel som använts för kondenseringen har genererats så att den inte kan utrönas med tillgängliga tekniska metoder av en person som är obehörig att använda nyckeln.

---

[32] Se även skäl 25.

[33] Se skäl 80 och artikel 27.

[34] Artikel 29-arbetsgruppens yttrande 3/2014 om anmälan av personuppgiftsbrott, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[35] Se även artikel 4.1 och 4.2 i förordning (EU) nr 611/2013.

Om personuppgifter i stort sett har gjorts oläsbara för obehöriga personer och om uppgifterna är en kopia eller om det finns en säkerhetskopia är det därför inte säkert att ett konfidentialitetsbrott som rör korrekt krypterade personuppgifter behöver anmälas till tillsynsmyndigheten. Det är nämligen osannolikt att en sådan incident medför en risk för enskilda personers rättigheter och friheter. Detta innebär naturligtvis att den enskilda personen inte heller behöver underrättas, eftersom det sannolikt inte rör sig om någon hög risk. Man bör dock ha i åtanke att även om det inledningsvis inte krävs någon anmälan om det inte föreligger någon sannolik risk för enskilda personers rättigheter och friheter kan detta ändras över tid. I så fall måste det göras en ny bedömning av risken. Om det senare visar sig att krypteringsnyckelns säkerhet har äventyrats, eller en sårbarhet i krypteringsprogrammet upptäcks, kan det t.ex. fortfarande vara nödvändigt att göra en anmälan.

Dessutom bör det noteras att om en incident äger rum och det inte finns några säkerhetskopior av de krypterade personuppgifterna har ett tillgänglighetsbrott ägt rum som medför risker för enskilda och därför kan behöva anmälas. Om en incident äger rum som rör förlust av krypterade uppgifter kan detta på samma sätt vara en incident som ska rapporteras, även om det finns en säkerhetskopia av personuppgifterna. Om en anmälan ska göras beror på hur lång tid det tar att återställa uppgifterna från säkerhetskopian och hur bristen på tillgänglighet påverkar enskilda personer. I artikel 32.1 c anges att en viktig säkerhetsfaktor är ”förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident”.

Exempel

Ett exempel på en incident som inte kräver anmälan till tillsynsmyndigheten är förlusten av en säkert krypterad mobilenhet som används av den personuppgiftsansvarige och dennes personal. Förutsatt att krypteringsnyckeln är i den personuppgiftsansvariges säkra ägo och detta inte är den enda kopian av personuppgifter är personuppgifterna inte tillgängliga för angriparen. Det innebär att det är osannolikt att en incident medför en risk för de berörda registrerades rättigheter och friheter. Om det senare blir uppenbart att krypteringsnyckelns säkerhet har äventyrats eller att krypteringsprogrammet eller algoritmen är sårbara förändras risken för fysiska personers rättigheter och friheter, och det kan således bli nödvändigt att göra en anmälan.

Artikel 33 efterlevs dock inte om en personuppgiftsansvarig inte anmäler en incident till tillsynsmyndigheten i en situation där uppgifterna faktiskt inte har krypterats på ett säkert sätt. När personuppgiftsansvariga väljer ut krypteringsprogram bör de därför noggrant väga in kvaliteten på och ett korrekt genomförande av den kryptering som erbjuds, förstå vilken grad av skydd krypteringen faktiskt ger och huruvida detta är tillräckligt för de risker som föreligger. Personuppgiftsansvariga bör även närmare känna till hur deras krypteringsprodukter fungerar. En enhet kan t.ex. krypteras när den är avstängd, men inte i standby-läge. Vissa produkter som använder sig av kryptering har ”standardnycklar” som måste ändras av varje kund för att fungera. Säkerhetsexperter kan också anse att krypteringen för närvarande är tillräcklig, men att den kan vara för gammal om några år. I så fall är det tveksamt om den produkten krypterar uppgifterna på ett tillräckligt säkert sätt och ger en tillräcklig skyddsnivå.

III. **Artikel 34 – Information till den registrerade**

A. Information till enskilda

I vissa fall är den personuppgiftsansvarige skyldig att, utöver att anmäla en incident till tillsynsmyndigheten, informera de personer som påverkas av incidenten.

I artikel 34.1 föreskrivs följande:

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

Personuppgiftsansvariga bör komma ihåg att anmälan till tillsynsmyndigheten är obligatorisk, såvida det inte är osannolikt att incidenten leder till en hög risk för fysiska personers rättigheter och friheter. Om incidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter måste de berörda personerna däremot informeras. Tröskeln för att informera de berörda personerna är därför högre än för att anmäla incidenten till tillsynsmyndigheterna och inte alla incidenter behöver därför meddelas enskilda personer. På så sätt slipper dessa tröttas ut av onödig information.

I dataskyddsförordningen anges att enskilda personer ska informeras om en incident ”utan onödigt dröjsmål”, vilket betyder så snabbt som möjligt. Huvudsyftet med informationen till enskilda är att ge dem specifik information om de åtgärder de bör vidta för att skydda sig själva[36]. Som påpekats ovan gör snabb information, beroende på incidentens art och den risk den medför, det lättare för enskilda personer att vidta åtgärder för att skydda sig själva mot negativa konsekvenser av incidenten.

I bilaga B i dessa riktlinjer finns en icke-uttömmande förteckning över när en incident sannolikt leder till en hög risk för enskilda och den personuppgiftsansvarige därför måste informera de berörda om incidenten.

B. Information som ska lämnas

Gällande information till enskilda personer anges följande i artikel 34.2:

”Den information till den registrerade som avses i punkt 1 i denna artikel ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone de upplysningar och åtgärder som avses i artikel 33.3 b, c och d.”

Enligt förordningen ska den personuppgiftsansvarige lämna åtminstone följande information:

- En beskrivning av incidentens art.
- Namnet på och kontaktuppgifterna till dataskyddsombudet eller annan kontaktpunkt.
- En beskrivning av de sannolika konsekvenserna av incidenten.
- Åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda incidenten, inbegripet i förekommande fall åtgärder för att mildra dess potentiella negativa effekter.

För att åtgärda en incident och mildra dess potentiella negativa effekter kan den personuppgiftsansvarige exempelvis förklara att denne efter att ha anmält incidenten till relevant tillsynsmyndighet har fått råd om hur incidenten ska hanteras och effekterna mildras. I förekommande fall bör den personuppgiftsansvarige dessutom tillhandahålla specifik information till enskilda så att de kan skydda sig mot potentiella negativa effekter av en incident, t.ex. att behöva ändra lösenord om deras åtkomstuppgifter har äventyrats. Återigen kan en personuppgiftsansvarig välja att tillhandahålla mer information än vad som krävs.

C. Kontakta enskilda

I princip bör den relevanta incidenten meddelas direkt till de registrerade som påverkas, om inte detta skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en

[36] Se även skäl 86.

liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt (artikel 34.3 c).

Särskilda meddelanden bör användas för att informera de registrerade om en incident och de bör inte skickas ut tillsammans med annan information, t.ex. regelbundna uppdateringar, nyhetsbrev eller standardmeddelanden. Detta bidrar till att göra informationen om incidenten klar och tydlig.

Exempel på tydliga informationsmetoder inbegriper direktmeddelanden (t.ex. e-post, sms, direktmeddelande), framträdande banderoller eller informationsrutor på webbplatser, meddelanden per post och framträdande annonser i tryckta medier. Information som endast anges i ett pressmeddelande eller en företagsblogg är inte en effektiv metod för att informera en enskild person om en incident. Artikel 29-arbetsgruppen rekommenderar att personuppgiftsansvariga ska välja en metod som maximerar chansen för att alla enskilda som påverkas informeras på rätt sätt. Beroende på omständigheterna i det enskilda fallet kan detta innebära att den personuppgiftsansvarige använder sig av flera kommunikationsmetoder, i stället för en enda kontaktkanal.

Personuppgiftsansvariga kan även själva behöva se till att informationen är tillgänglig i lämpliga alternativa format och på relevanta språk för att säkerställa att enskilda kan förstå den information som tillhandahålls. När en enskild informeras om en incident är t.ex. lämpligt språk i regel det språk som tidigare använts vid företagets reguljära korrespondens med mottagaren. Om en incident påverkar registrerade som den personuppgiftsansvarige tidigare inte har varit i kontakt med, och särskilt personer som bor i en annan medlemsstat eller annat land utanför EU än det land där den personuppgiftsansvarige är etablerad, kan information på det lokala språket accepteras, med hänsyn till de resurser som annars skulle krävas. Nyckeln är att hjälpa registrerade att förstå incidentens art och vilka åtgärder de kan vidta för att skydda sig.

Personuppgiftsansvariga är bäst lämpade att fastställa den lämpligaste kontaktkanalen för att meddela enskilda att en incident har ägt rum, särskilt om de ofta har kontakt med sina kunder. Naturligtvis bör en personuppgiftsansvarig vara försiktig med att använda sig av en kontaktkanal som äventyrats av incidenten, eftersom denna kanal även kan användas av angripare som utger sig för att vara den personuppgiftsansvarige.

I skäl 86 förklaras samtidigt följande:

> ”De registrerade bör underrättas så snart detta rimligtvis är möjligt, i nära samarbete med tillsynsmyndigheten och i enlighet med den vägledning som lämnats av den eller andra relevanta myndigheter, exempelvis brottsbekämpande myndigheter. Till exempel kräver behovet av att mildra en omedelbar skaderisk att de registrerade underrättas omedelbart, medan behovet av att vidta lämpliga åtgärder vid fortlöpande eller likartade personuppgiftsincidenter däremot kan motivera längre tid för underrättelsen.”

Personuppgiftsansvariga kan därför vilja kontakta och konsultera tillsynsmyndigheten inte bara för att få råd om hur den bör informera registrerade om en incident i enlighet med artikel 34, utan även om de lämpliga meddelanden som bör skickas ut och det lämpligaste sättet att kontakta enskilda.

Kopplat till detta är det råd som ges i skäl 88 om att man vid en anmälan av en incident bör ”beakta brottsbekämpande myndigheters berättigade intressen, där en för tidig redovisning kan riskera att i onödan hämma utredning av omständigheterna kring en personuppgiftsincident”. Detta kan i vissa situationer innebära att den personuppgiftsansvarige, om det är motiverat och på de brottsbekämpande myndigheternas inrådan, kan vänta med att underrätta de personer som påverkas tills detta inte skadar sådana utredningar. Efter detta måste dock registrerade fortfarande informeras så snabbt som möjligt.

När det inte är möjligt för en personuppgiftsansvarig att informera en enskild person om en incident på grund av otillräckliga kontaktuppgifter till den enskilde bör den personuppgiftsansvarige i så fall informera den enskilde så snart detta är rimligtvis möjligt (t.ex. när en person utövar sin rätt enligt

artikel 15 att få tillgång till personuppgifterna och lämnar kompletterande upplysningar till den personuppgiftsansvarige som behövs för att kontakta personen).

D. Villkor för när information inte krävs

I artikel 34.3 anges tre villkor, som om de är uppfyllda, gör att information till enskilda inte krävs vid en incident. Dessa är följande:

- Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder som tillämpats på de personuppgifter som påverkades av incidenten, i synnerhet sådana som ska göra personuppgifterna oläsbara för obehöriga. Detta kan t.ex. inbegripa skydd av personuppgifter med hjälp av den senaste krypteringstekniken, eller med hjälp av tokenisering.
- Den personuppgiftsansvarige har omedelbart efter en incident vidtagit åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter sannolikt inte längre kommer att uppstå. Beroende på omständigheterna i det enskilda fallet kan den personuppgiftsansvarige t.ex. omedelbart ha fastställt och vidtagit åtgärder mot den person som fick tillgång till personuppgifterna innan denne hann göra något med uppgifterna. Vederbörlig hänsyn bör fortfarande tas till de potentiella konsekvenserna av ett konfidentialitetsbrott, men återigen beror detta på de berörda uppgifternas art.
- Det skulle inbegripa en oproportionell ansträngning[37] att kontakta enskilda om deras kontaktuppgifter kanske har gått förlorade till följd av incidenten eller inte är kända till att börja med. Ett exempel är om ett statistikkontors lagerbyggnad har översvämmats och de handlingar som innehöll personuppgifter endast hade sparats i pappersform. I så fall måste den personuppgiftsansvarige publicera en offentlig kungörelse eller vidta liknande åtgärder, som gör att enskilda informeras på ett lika effektivt sätt. Vid oproportionell ansträngning kan man även ta hjälp av tekniska system för att göra information om incidenten tillgänglig på begäran, vilket kan vara användbart för de personer som kan påverkas av incidenten men som den personuppgiftsansvarige annars inte kan kontakta.

I enlighet med principen om ansvarsskyldighet ska personuppgiftsansvariga kunna visa för tillsynsmyndigheten att de uppfyller ett eller flera av dessa villkor [38]. Det är viktigt att komma ihåg att även om en anmälan inledningsvis inte krävs för att det inte finns någon risk för fysiska personers rättigheter och friheter kan detta ändras över tid och en ny bedömning av risken kan behöva göras.

Om en personuppgiftsansvarig bestämmer sig för att inte underrätta en enskild om en incident förklaras i artikel 34.4 att tillsynsmyndigheten kan kräva att den personuppgiftsansvarige gör detta, om tillsynsmyndigheten anser att incidenten medför en hög risk för enskilda. Alternativt kan tillsynsmyndigheten anse att villkoren i artikel 34.3 är uppfyllda, och att information till enskilda därför inte krävs. Om tillsynsmyndigheten slår fast att beslutet att inte informera registrerade inte är välgrundat får den överväga att tillgripa de befogenheter och sanktioner som den förfogar över.

IV. **Bedömning av risk och hög risk**

A. Risk som utlösande faktor för en anmälan

[37] Se artikel 29-arbetsgruppens riktlinjer om öppenhet, där frågan om oproportionell ansträngning tas upp, tillgängliga på http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] Se artikel 5.2.

Även om dataskyddsförordningen har infört en skyldighet att anmäla en incident gäller inte detta krav i alla situationer.

- Anmälan till behörig tillsynsmyndighet krävs såvida det inte är osannolikt att en incident medför en risk för enskilda personers rättigheter och friheter.
- Den enskilda personen informeras endast såvida det är sannolikt att incidenten medför en risk för dennes rättigheter och friheter.

Detta innebär att det är oerhört viktigt att den personuppgiftsansvarige så fort denne får vetskap om en incident inte enbart försöker begränsa incidenten utan även bedömer den risk som incidenten kan medföra. Det finns två viktiga skäl till detta. För det första blir det lättare för den personuppgiftsansvarige att vidta effektiva åtgärder för att begränsa och åtgärda incidenten om vederbörande känner till hur allvarliga effekter incidenten kan få för den enskilde och hur sannolika de är. För det andra blir det lättare för den personuppgiftsansvarige att fastställa huruvida incidenten måste anmälas till tillsynsmyndigheten och, vid behov, till de berörda personerna.

Som förklarats ovan krävs en anmälan av en incident såvida det inte är osannolikt att den medför en risk för enskilda personers rättigheter och friheter. Den viktigaste utlösande faktorn för när de registrerade måste informeras om en incident är när det är sannolikt att incidenten leder till en *hög* risk för enskildas rättigheter och friheter. En sådan risk finns när incidenten kan medföra fysiska, materiella eller immateriella skador för de enskilda vars uppgifter har drabbats av incidenten. Exempel på sådana skador är diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust och skadat anseende. När incidenten rör personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i en fackförening, eller som innehåller genetiska uppgifter, uppgifter om hälsa eller sexualliv eller fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder, ska risken för en sådan skada anses sannolik[39].

B. Faktorer att tänka på vid riskbedömning

Skälen 75 och 76 i dataskyddsförordningen tyder på att man vid riskbedömning ska ta hänsyn till både sannolikheten och svårighetsgraden när det gäller risken för registrerades rättigheter och friheter. Det anges dessutom att risken bör utvärderas grundat på en objektiv bedömning.

Notera att bedömningen av de risker för personers rättigheter och friheter som en incident kan leda till är inriktad på andra aspekter än den risk som bedöms i en konsekvensbedömning avseende dataskydd[40]. Vid en konsekvensbedömning avseende dataskydd bedömer man både risken för den planerade behandlingen av uppgifterna och risken vid en incident. Vid bedömning av en potentiell incident görs en allmän bedömning av sannolikheten för att en incident ska äga rum, och den skada som den registrerade kan lida till följd av incidenten. Man gör med andra ord en bedömning av en hypotetisk händelse. Vid en faktisk incident har händelsen redan ägt rum och fokus flyttas helt till vilka effekter incidenten riskerar att få för enskilda.

Exempel

En konsekvensbedömning avseende dataskydd tyder på att användningen av en viss programvara för att skydda personuppgifter är en passande åtgärd för att säkerställa en säkerhetsnivå som står i proportion till den risk som behandlingen annars skulle utsätta enskilda för. Om en sårbarhet senare upptäcks ändrar detta programvarans lämplighet att begränsa risken för de skyddade

[39] Se skälen 75 och 85.

[40] Se arbetsgruppens riktlinjer om konsekvensbedömning avseende dataskydd: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

personuppgifterna och det måste därför göras en ny bedömning av denna risk inom ramen för en pågående konsekvensbedömning avseende dataskydd.

En sårbarhet i produkten utnyttjas senare, vilket leder till en incident. Den personuppgiftsansvarige bör bedöma de särskilda omständigheterna i samband med incidenten, de uppgifter som påverkas och den potentiella effekten för enskilda, samt hur sannolikt det är att risken kommer att uppstå.

Vid bedömningen av den risk för enskilda som en incident leder till bör den personuppgiftsansvarige därför ta hänsyn till de specifika omständigheterna i samband med incidenten, inbegripet de potentiella effekternas svårighetsgrad och hur sannolika dessa effekter är. Artikel 29-arbetsgruppen rekommenderar därför att bedömningen bör ta hänsyn till följande kriterier[41]:

- Typen av incident

Typen av incident som har ägt rum kan påverka den risknivå som enskilda utsätts för. Ett konfidentialitetsbrott som medförde att medicinska uppgifter lämnades ut till obehöriga parter kan exempelvis få andra konsekvenser för en enskild än en incident där en persons medicinska uppgifter har gått förlorade och inte längre är tillgängliga.

- Personuppgifternas natur, känslighet och volym

Vid riskbedömning är naturligtvis de av incidenten äventyrade personuppgifternas art och känslighet en viktig faktor. Ju känsligare uppgifterna är desto högre är vanligtvis risken att de personer som påverkas lider skada, men hänsyn bör även tas till andra personuppgifter om den registrerade som kanske redan är tillgängliga. Om en persons namn och adress exempelvis lämnas ut är det vanligtvis osannolikt att detta orsakar någon betydande skada. Om en adoptivförälders namn och adress lämnas ut till den biologiska föräldern kan konsekvenserna emellertid bli mycket allvarliga för både adoptivföräldrarna och barnet.

Incidenter som rör hälsouppgifter, identitetshandlingar eller finansiella uppgifter såsom kreditkortsuppgifter kan alla var för sig orsaka skada, men om de används tillsammans kan de användas för identitetsstöld. En kombination av personuppgifter är vanligtvis känsligare än en enda typ av personuppgifter.

Vissa typer av personuppgifter kan vid första anblicken te sig ganska ofarliga. Man bör dock ta stor hänsyn till vad uppgifterna kan avslöja om den enskilde. En förteckning över kunder som godtar regelbundna leveranser är kanske inte i sig särskilt känslig, men samma uppgifter om kunder som har begärt att deras leveranser ska upphöra under semestern kan vara värdefull information för kriminella.

På samma sätt kan en liten del mycket känsliga personuppgifter få stora effekter för en enskild. Och en stor mängd detaljer kan avslöja ännu mer information om just den personen. En incident som påverkar stora volymer personuppgifter om många registrerade kan få effekter för ett motsvarande stort antal enskilda personer.

- Hur lätt det är att identifiera enskilda personer

[41] I artikel 3.2 i förordning (EU) nr 611/2013 ges vägledning om de faktorer som det ska tas hänsyn till vid anmälan av incidenter inom sektorn för elektroniska kommunikationstjänster. Denna vägledning kan även vara användbar vid anmälan enligt dataskyddsförordningen. Se http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:sv:PDF

En viktig faktor att ta hänsyn till är hur lätt det är för en person som har tillgång till personuppgifter som äventyrats att identifiera specifika personer, eller para ihop uppgifterna med annan information för att identifiera enskilda personer. Beroende på omständigheterna är det möjligt att identifiera en person direkt från de vid incidenten äventyrade personuppgifterna, utan att någon särskild undersökning behöver göras för att avslöja personens identitet, eller så kan det vara extremt svårt att para ihop personuppgifter med en viss person, även om det fortfarande är möjligt under vissa omständigheter. Identifieringen kan göras direkt eller indirekt från de vid incidenten äventyrade uppgifterna, men kan också bero på det specifika sammanhang inom vilket incidenten ägde rum, och huruvida relaterade personuppgifter är tillgängliga för allmänheten. Detta kan vara mer relevant för konfidentialitets- och tillgänglighetsbrott.

Som påpekats ovan är personuppgifter som skyddas av en lämplig krypteringsnivå oläsbara för obehöriga personer utan krypteringsnyckeln. Dessutom kan lämpligt genomförd pseudonymisering (som i artikel 4.5 definieras som ”behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person”) också minska sannolikheten för att enskilda identifieras i händelse av en incident. Pseudonymiseringstekniker kan dock inte i sig anses göra uppgifterna oläsbara.

- Konsekvensernas svårighetsgrad för enskilda personer

Beroende på arten av de personuppgifter som berörs av en incident, t.ex. de särskilda kategorierna av uppgifter, kan de potentiella skador för enskilda som incidenten leder till vara särskilt svåra, särskilt om incidenten kan leda till identitetsstöld, bedrägeri, fysisk skada, psykisk oro, förödmjukelse eller skadat anseende. Om incidenten rör personuppgifter om sårbara personer kan dessa utsättas för en större risk för skada.

Huruvida den personuppgiftsansvarige har fått vetskap om att personuppgifter är i händerna på personer vars avsikter är okända eller skadliga kan ha betydelse för hur stor den potentiella risken är. Det kan röra sig om ett konfidentialitetsbrott, genom vilket uppgifter felaktigt lämnas ut till tredje part, i den mening som avses i artikel 4.10, eller till en annan part. Detta kan t.ex. vara fallet om personuppgifterna av misstag skickas till fel avdelning inom en organisation, eller till en ofta använd leverantör. Den personuppgiftsansvarige kan begära att mottagaren antingen skickar tillbaka de uppgifter som mottagits eller på ett säkert sätt förstör dem. Förutsatt att den personuppgiftsansvarige har ett pågående förhållande med mottagarna och känner till deras rutiner, historik och andra relevanta detaljer, kan mottagarna i båda fallen anses vara ”betrodda”. Den personuppgiftsansvarige kan med andra ord i viss grad vara säker på att mottagaren inte kommer att läsa eller försöka få åtkomst till de uppgifter som felaktigt skickats till dem, utan följa instruktionerna och skicka tillbaka uppgifterna. Även om mottagaren har fått åtkomst till uppgifterna kan den personuppgiftsansvarige eventuellt ändå förlita sig på att mottagaren inte kommer att vidta ytterligare åtgärder med uppgifterna, utan snabbt skicka tillbaka dem till den personuppgiftsansvarige och samarbeta för att återställa dem. I sådana fall kan detta beaktas vid den riskbedömning som den personuppgiftsansvarige utför efter incidenten. Den omständigheten att mottagaren är betrodd kan göra incidenten mindre allvarlig, men innebär inte att en incident inte har ägt rum. Att mottagaren är betrodd kan dock undanröja sannolikheten för en risk för enskilda, och det är därför inte längre nödvändigt att anmäla incidenten till tillsynsmyndigheten, eller informera de personer som påverkas. Återigen avgörs detta från fall till fall. Trots det måste den personuppgiftsansvarige spara information om incidenten som ett led i dennes allmänna skyldighet att föra register över incidenter (se avsnitt V nedan).

Hänsyn bör också tas till hur långvariga konsekvenserna för enskilda är, där effekten kan anses större om effekterna är långvariga.

- Den enskildes speciella egenskaper

En incident kan påverka personuppgifter som rör barn eller andra sårbara personer, som till följd av detta utsätts för en större risk för fara. Det kan finnas andra faktorer beträffande den enskilde som kan påverka vilken effekt en incident får för dem.

- Den personuppgiftsansvariges speciella egenskaper

Den personuppgiftsansvariges karaktär och roll och dennes verksamhet kan påverka risknivån för enskilda till följd av en incident. En medicinsk organisation behandlar t.ex. särskilda kategorier av personuppgifter, vilket innebär att det finns ett större hot mot enskilda om deras uppgifter äventyras. jämfört med en tidnings sändlista.

- Antalet personer som påverkas

En incident kan påverka endast en eller ett fåtal individer eller flera tusen personer, eller till och med ännu fler. I regel får en incident större effekter ju fler individer som påverkas. En incident kan dock få svåra följder även för en enda individ, beroende på personuppgifternas art och det sammanhang i vilket de har äventyrats. Även här är det viktigt att ta hänsyn till effekternas sannolikhet och hur svårt de drabbar de berörda personerna.

- Allmänna aspekter

Vid bedömningen av den risk som en incident sannolikt leder till bör den personuppgiftsansvarige ta hänsyn till en kombination av hur allvarlig den potentiella effekten är för enskildas rättigheter och friheter och hur sannolikt det är att incidenten inträffar. Ju allvarligare konsekvenserna av en incident är desto större är naturligtvis risken och ju större sannolikheten för att dessa konsekvenser inträffar desto mer ökar också risken. Om den personuppgiftsansvarige inte är säker på hur allvarlig en incident är bör denne ta det säkra före det osäkra och anmäla den. I bilaga B anges några användbara exempel på olika typer av incidenter som innebär en risk eller en hög risk för enskilda.

Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) har tagit fram rekommendationer gällande en metod att bedöma hur allvarlig en incident är. Detta är något som personuppgiftsansvariga och personuppgiftsbiträden kan ha hjälp av när de utarbetar sin incidenthanteringsplan[42].

V. **Ansvarsskyldighet och registerföring**

A. Dokumentering av incidenter

Oavsett om en incident måste anmälas till tillsynsmyndigheten eller inte måste den personuppgiftsansvarige föra ett register över alla incidenter. I artikel 33.5 anges följande:

> ”Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av denna artikel.”

[42] Enisa, *Recommendations for a methodology of the assessment of severity of personal data breaches*, https://www.enisa.europa.eu/publications/dbn-severity

Detta är kopplat till ansvarsskyldighetsprincipen i artikel 5.2 i dataskyddsförordningen. Syftet med att registrera både incidenter som inte behöver anmälas och incidenter som ska anmälas är även kopplat till den personuppgiftsansvariges skyldigheter enligt artikel 24, och tillsynsmyndigheten kan begära att få se dessa register. Personuppgiftsansvariga uppmuntras därför att föra interna register över incidenter, oavsett om de är skyldiga att anmäla dem eller inte[43].

Även om det är upp till den personuppgiftsansvarige att fastställa vilken metod och struktur som ska användas vid dokumenteringen av en incident finns det vissa nyckelkomponenter som alltid bör ingå. Enligt artikel 33.5 ska den personuppgiftsansvarige dokumentera alla detaljer kring incidenten, inbegripet dess orsaker, vad som skedde och de personuppgifter som berördes. Dokumentationen ska även innehålla incidentens konsekvenser och de korrigerande åtgärder som vidtagits av den personuppgiftsansvarige.

I dataskyddsförordningen anges inte hur länge sådan dokumentation ska sparas. Om dokumentationen innehåller personuppgifter ankommer det på den personuppgiftsansvarige att fastställa en passande lagringsperiod i enlighet med principerna om behandling av personuppgifter[44] och uppfylla en laglig grund för behandling[45]. Den personuppgiftsansvarige måste spara dokumentationen i enlighet med artikel 33.5, eftersom den personuppgiftsansvarige kan uppmanas att överlämna bevis till tillsynsmyndigheten för att den artikeln, eller mer allmänt principen om ansvarsskyldighet, efterlevs. Om registren inte själva innehåller några personuppgifter gäller naturligtvis inte principen om lagringsminimering[46] i dataskyddsförordningen.

Utöver dessa detaljer rekommenderar artikel 29-arbetsgruppen att den personuppgiftsansvarige även dokumenterar sina skäl för de beslut som fattas som en reaktion på en incident. Framför allt om en incident inte anmäls bör en motivering till det beslutet dokumenteras. Motiveringen bör innehålla skälen till varför den personuppgiftsansvarige anser att incidenten sannolikt inte kommer att leda till en risk för enskildas rättigheter och friheter[47]. Alternativt, om den personuppgiftsansvarige anser att något av villkoren i artikel 34.3 är uppfyllda, bör denne kunna lägga fram lämpliga bevis för att så är fallet.

Om den personuppgiftsansvarige anmäler en incident till tillsynsmyndigheten, men anmälan är försenad, måste den personuppgiftsansvarige kunna ange skälen till denna försening. Dokumentation om detta kan göra det lättare att visa att förseningen kan motiveras och inte är onödigt lång.

Om den personuppgiftsansvarige informerar de berörda personerna om en incident bör den personuppgiftsansvarige tydligt förklara incidenten och informera de berörda på ett snabbt och effektivt sätt. Det blir dessutom lättare för den personuppgiftsansvarige att visa att denne varit ansvarsfull och efterlevt förordningen om den personuppgiftsansvarige sparar bevis på sådan kommunikation.

För att göra det lättare att följa artiklarna 33 och 34 vore det fördelaktigt för både personuppgiftsansvariga och personuppgiftsbiträden att ha ett dokumenterat anmälningsförfarande,

[43] Den personuppgiftsansvarige kan välja att dokumentera incidenter inom ramen för det register över behandlingar som förs i enlighet med artikel 30. Ett separat register behövs inte, förutsatt att relevant information beträffande incidenten tydligt kan fastställas som sådan och på begäran kan extraheras.

[44] Se artikel 5.

[45] Se artiklarna 6 och 9.

[46] Se artikel 5.1 e.

[47] Se skäl 85.

som anger vilken process som ska följas när en incident har upptäckts, inbegripet hur incidenten ska begränsas, hanteras och återställas, samt hur riskbedömningen ska gå till och hur incidenten ska anmälas. För att visa att dataskyddsförordningen efterlevs kan det även vara lämpligt att visa att anställda har informerats om att sådana förfaranden och mekanismer finns och att de vet hur de ska reagera på incidenter.

Notera att underlåtelse att dokumentera en incident på rätt sätt kan leda till att tillsynsmyndigheten utövar sina befogenheter enligt artikel 58, eller ålägger en administrativ sanktionsavgift i enlighet med artikel 83.

B. Dataskyddsombudets roll

En personuppgiftsansvarig eller ett personuppgiftsbiträde kan ha ett dataskyddsombud[48], antingen i enlighet med kravet i artikel 37 eller frivilligt som ett exempel på god praxis. I artikel 39 i dataskyddsförordningen anges ett antal obligatoriska uppgifter som dataskyddsombudet har. Detta hindrar dock inte att den personuppgiftsansvarige i förekommande fall tilldelar dataskyddsombudet ytterligare uppgifter.

Vad som framför allt är relevant i samband med anmälan av en incident är att dataskyddsombudets obligatoriska uppgifter bland annat inbegriper att ge den personuppgiftsansvarige och personuppgiftsbiträdet råd och information i dataskyddsfrågor, övervaka att dataskyddsförordningen efterlevs, och ge råd i samband med konsekvensbedömningar avseende dataskydd. Dataskyddsombudet ska även samarbeta med tillsynsmyndigheten och fungera som kontaktpunkt för tillsynsmyndigheten och de registrerade. Notera även att när en incident anmäls till tillsynsmyndigheten är den personuppgiftsansvarige enligt artikel 33.3 b skyldig att förmedla namnet på och kontaktuppgifterna till dataskyddsombudet eller andra kontaktpunkter.

När det gäller att dokumentera incidenter kan den personuppgiftsansvarige eller personuppgiftsbiträdet vilja inhämta ett yttrande från sitt dataskyddsombud om hur denna dokumentation ska struktureras, utarbetas och förvaltas. Dataskyddsombudet kan dessutom även ges i uppdrag att spara sådan dokumentation.

Dessa faktorer innebär att dataskyddsombudet bör spela en nyckelroll när det gäller att hjälpa till att förhindra en incident eller förberedelserna inför en incident, genom att ge råd och övervaka efterlevnaden, samt under en incident (dvs. när tillsynsmyndigheten underrättas), och under tillsynsmyndighetens eventuella efterföljande undersökningar. Mot denna bakgrund rekommenderar artikel 29-arbetsgruppen att dataskyddsombudet snabbt informeras om förekomsten av en incident och deltar i hela processen för att hantera och anmäla en incident.

VI. Anmälningsskyldigheter enligt andra rättsinstrument

Utöver, och separat från, anmälan av och information om incidenter enligt dataskyddsförordningen bör personuppgiftsansvariga även känna till eventuella krav på att anmäla säkerhetsincidenter enligt annan närstående lagstiftning som de eventuellt omfattas av, och huruvida detta även gör att de är skyldiga att samtidigt anmäla en personuppgiftsincident till tillsynsmyndigheten. Sådana krav kan skilja sig åt mellan medlemsstaterna. Som exempel på anmälningsskyldigheter i andra rättsinstrument och hur de hänger ihop med dataskyddsförordningen kan dock följande nämnas:

[48] Se artikel 29-arbetsgruppens riktlinjer om dataskyddsombudsmän här: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

- Förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS-förordningen)[49].

Enligt artikel 19.2 i eIDAS-förordningen är tillhandahållare av betrodda tjänster skyldiga att underrätta sitt tillsynsorgan om alla säkerhetsincidenter eller integritetsförluster som i betydande omfattning påverkar den betrodda tjänst som tillhandahålls eller på de personuppgifter som ingår i denna. I tillämpliga fall – dvs. om en sådan incident eller förlust även är en personuppgiftsincident enligt dataskyddsförordningen – bör tillhandahållaren av betrodda tjänster även underrätta tillsynsmyndigheten.

- Direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet)[50].

Enligt artiklarna 14 och 16 i NIS-direktivet är leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster skyldiga att anmäla säkerhetsincidenter till deras behöriga myndighet. Som påpekas i skäl 63 i NIS-direktivet[51] kan säkerhetsincidenter ofta inbegripa att personuppgifter undergrävs. Även om behöriga myndigheter och tillsynsmyndigheter i NIS-direktivet åläggs att samarbeta och utbyta information på detta område är det fortfarande så att när sådana incidenter är, eller blir, personuppgiftsincidenter enligt dataskyddsförordningen är dessa leverantörer skyldiga att göra en separat anmälan om incidenterna till tillsynsmyndigheten, separat från den anmälan av incidenter som krävs enligt NIS-direktivet.

Exempel

En leverantör av molntjänster som anmäler en incident enligt NIS-direktivet kan även behöva underrätta en personuppgiftsansvarig, om incidenten inbegriper en personuppgiftsincident. På samma sätt kan en leverantör av betrodda tjänster enligt eIDAS också vara skyldig att anmäla incidenten till relevant dataskyddsmyndighet.

- Direktiv 2009/136/EG (medborgarrättsdirektivet) och förordning (EU) nr 611/2013 (förordningen om anmälan av incidenter).

Leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster inom ramen för direktiv 2002/58/EG[52] måste anmäla incidenter till behöriga nationella myndigheter.

Personuppgiftsansvariga bör även vara medvetna om andra rättsliga, medicinska eller yrkesmässiga anmälningsplikter enligt andra tillämpliga bestämmelser.

[49] Se http://eur-lex.europa.eu/legal-content/SV/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.SWE

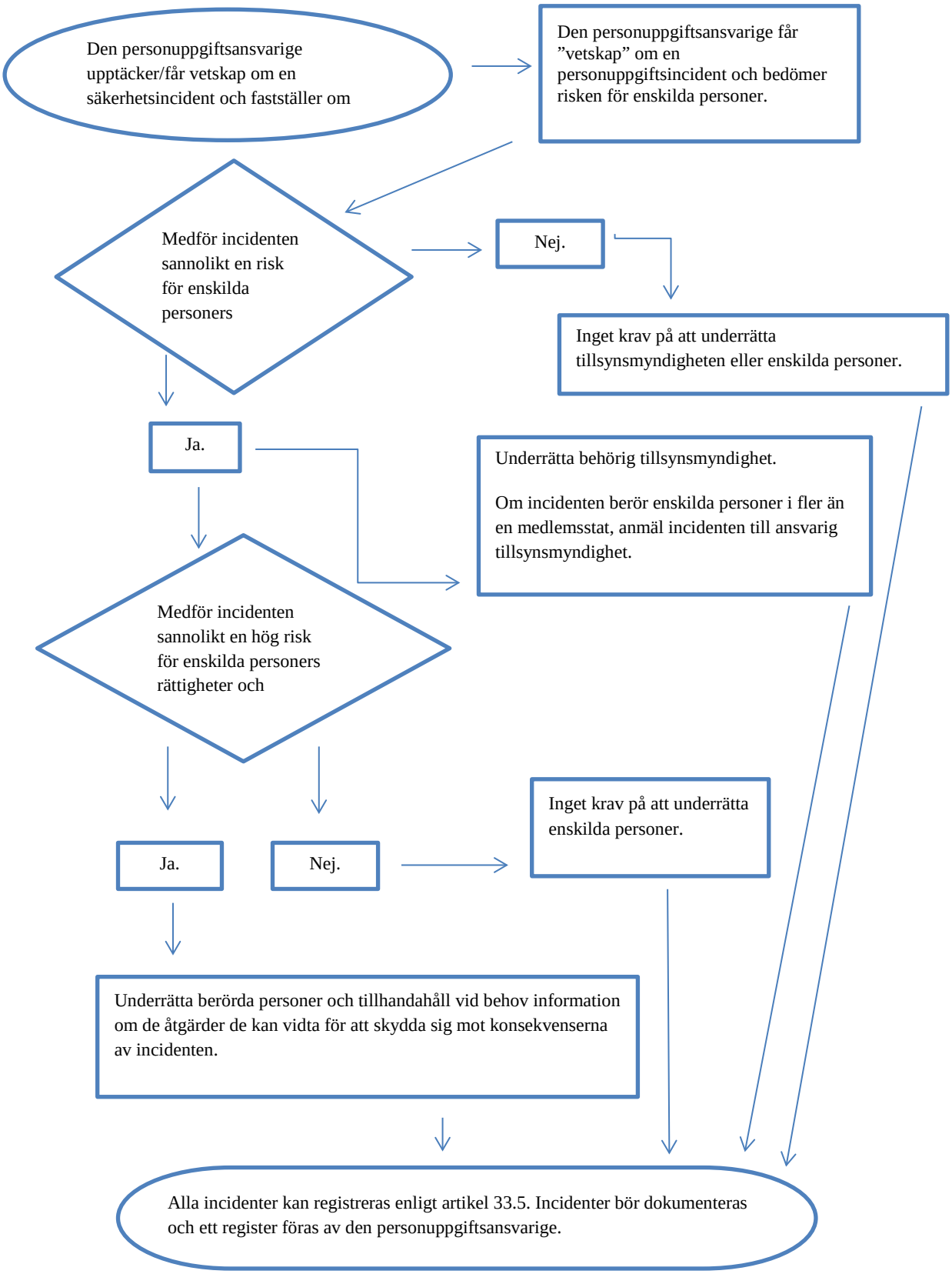
[50] Se http://eur-lex.europa.eu/legal-content/SV/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.SWE

51 Skäl 63: *”Säkerheten för personuppgifter undergrävs ofta till följd av incidenter. I detta sammanhang bör behöriga myndigheter och dataskyddsmyndigheter samarbeta och utbyta information om alla relevanta frågor för att hantera personuppgiftsincidenter till följd av incidenter.”*

[52] Den 10 januari 2017 lade Europeiska kommissionen fram en förordning om integritet och elektronisk kommunikation som kommer att ersätta direktiv 2009/136/EG och slopa kravet på anmälan. Fram tills detta förslag har godkänts av Europaparlamentet gäller fortfarande det nuvarande kravet på anmälan, se https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

VII. **Bilaga**

A. Flödesschema som visar anmälningskrav



B. Exempel på personuppgiftsincidenter och vem som ska underrättas

Följande icke-uttömmande förteckning kommer att hjälpa personuppgiftsansvariga att avgöra huruvida de behöver anmäla en personuppgiftsincident i olika situationer. Exemplen kan även göra det lättare att skilja mellan risk och hög risk för enskilda personers rättigheter och friheter.

Exempel	**Anmäla till tillsynsmyndigheten?**	**Underrätta den registrerade?**	**Anmärkningar/rekommendationer**
i. En personuppgiftsansvarig sparade en säkerhetskopia av ett arkiv över personuppgifter på ett USB-minne. Minnet stals under ett inbrott.	Nej.	Nej.	Så länge uppgifterna är krypterade med den senaste typen av algoritm, det finns säkerhetskopior av uppgifterna, det unika minnet inte har äventyrats och uppgifterna snabbt kan återställas, är det inte säkert att incidenten behöver rapporteras. Om uppgifterna senare äventyras krävs dock en anmälan.
ii. En personuppgiftsansvarig driver en onlinetjänst. Till följd av ett it-angrepp på den tjänsten har enskilda personers personuppgifter exfiltrerats. Den personuppgiftsansvarige har kunder i en enda medlemsstat.	Ja, rapportera till tillsynsmyndigheten om incidenten sannolikt leder till konsekvenser för enskilda personer.	Ja, rapportera till enskilda personer beroende på de berörda personuppgifternas art och om det är sannolikt att de leder till mycket allvarliga konsekvenser för enskilda personer.	
iii. Ett kort strömavbrott under några minuter på en personuppgiftsansvarigs teletjänstcentral innebär att kunder inte kan ringa till den personuppgiftsansvarige och få tillgång till sina uppgifter.	Nej.	Nej.	Detta är inte en incident som behöver anmälas, men som trots det ska registreras enligt artikel 33.5. Den personuppgiftsansvarige bör föra ett lämpligt register.
iv. En personuppgiftsansvarig utsätts för ett angrepp med ransomware vilket leder till att alla uppgifter krypteras. Det	Ja, rapportera till tillsynsmyndigheten om incidenten sannolikt leder till konsekvenser för enskilda personer	Ja, rapportera till enskilda personer, beroende på de berörda personuppgifter	Om det fanns en säkerhetskopia och uppgifterna snabbt kunde återställas behöver incidenten inte rapporteras till tillsynsmyndigheten eller till de enskilda personerna eftersom

finns inga säkerhetskopior och uppgifterna kan inte återställas. Vid en närmare undersökning visar det sig att det enda syftet med angreppet var att kryptera uppgifterna, och att det inte fanns några andra sabotageprogram i systemet.	eftersom detta utgör en förlust av tillgänglighet.	nas art och de potentiella konsekvenserna av förlusten av tillgänglighet, samt andra sannolika konsekvenser.	det inte har varit tal om någon permanent förlust av tillgänglighet eller konfidentialitet. Om tillsynsmyndigheten emellertid fick vetskap om incidenten på annat sätt kan den överväga att göra en undersökning för att bedöma efterlevnaden av de mer allmänna säkerhetskraven i artikel 32.
v. En person ringer en banks teletjänstcentral för att rapportera en personuppgiftsincident. Personen har fått någon annans månatliga kontoutdrag. Den personuppgiftsansvarige genomför en kort undersökning (som slutförs inom 24 timmar) och fastställer med rimlig säkerhet att en personuppgiftsincident har ägt rum och huruvida det finns en brist i systemet som innebär att andra personer har påverkats eller kan påverkas.	Ja.	Endast de personer som påverkades underrättas om det finns en hög risk och det är uppenbart att andra personer inte påverkades.	Om det efter en närmare undersökning visar sig att fler personer påverkas måste en uppdatering göras till tillsynsmyndigheten, och den personuppgiftsansvarige ska vidta de ytterligare åtgärder som krävs genom att underrätta andra personer om det finns en hög risk för dem.
vi. En personuppgiftsansvarig driver en marknadsplats på nätet och har kunder i flera medlemsstater. Marknadsplatsen utsätts för ett it-angrepp och angriparen publicerar användarnamn, lösenord och köphistorik på nätet.	Ja, rapportera till ansvarig tillsynsmyndighet om det rör sig om gränsöverskridande behandling.	Ja, eftersom detta kan leda till en hög risk.	Den personuppgiftsansvarige bör vidta åtgärder, t.ex. att tvinga de berörda kontona att återställa lösenorden och andra åtgärder för att minska risken. Den personuppgiftsansvarige bör även överväga andra anmälningsskyldigheter, t.ex. enligt NIS-direktivet som leverantör av digitala tjänster.

vii. Ett webbhotell som fungerar som personuppgiftsbiträde noterar ett fel i den kod som styr användarauktorisationen. Konsekvensen av bristen innebär att alla användare kan få tillgång till alla andra användares kontouppgifter.	Som personuppgiftsbiträde måste webbhotellet underrätta de berörda kunderna (de personuppgiftsansvariga) utan onödigt dröjsmål. Förutsatt att webbhotellet har gjort en egen undersökning bör de berörda personuppgiftsansvariga vara rimligen säkra på huruvida de har drabbats av en incident, och därför ska anses ha ”fått vetskap”, så snart de har underrättats av webbhotellet (personuppgiftsbiträdet). Den personuppgiftsansvarige ska därefter underrätta tillsynsmyndigheten.	Om det sannolikt inte finns någon hög risk för enskilda personer behöver dessa inte underrättas.	Webbhotellet (personuppgiftsbiträdet) måste överväga andra anmälningsskyldigheter (t.ex. enligt NIS-direktivet som leverantör av digitala tjänster). Om det inte finns något som tyder på att denna sårbarhet har utnyttjats av någon av de personuppgiftsansvariga är det inte säkert att incidenten behöver anmälas men den måste sannolikt registreras som ett exempel på bristande efterlevnad enligt artikel 32.
viii. Patientjournaler på ett sjukhus är inte tillgängliga under 30 dagar på grund av ett it-angrepp.	Ja, sjukhuset är skyldigt att anmäla incidenten eftersom den kan leda till hög risk för patienternas välbefinnande och deras personliga integritet.	Ja, rapportera till de personer som påverkas.	
ix. Personuppgifter från en stor mängd studenter skickas av misstag till fel sändlista med över 1 000 mottagare.	Ja, rapportera till tillsynsmyndigheten.	Ja, rapportera till enskilda personer beroende på de berörda personuppgifternas omfattning och typ och de potentiella konsekvensernas svårighetsgrad.	

x. Ett e-postmeddelande i direktmarknadsföringssyfte skickas till mottagare i fälten ”till:” eller ”cc:”, vilket gör det möjligt för alla mottagare att se andra mottagares e-postadress.	Ja, det kan vara obligatoriskt att anmäla incidenten till tillsynsmyndigheten om en stor mängd personer berörs, om känsliga uppgifter röjs (t.ex. en psykoterapeuts sändlista) eller om andra faktorer innebär en hög risk (t.ex. att e-postmeddelandet innehåller de ursprungliga lösenorden).	Ja, rapportera till enskilda personer beroende på de berörda personuppgifternas omfattning och typ och de potentiella konsekvensernas svårighetsgrad.	En anmälan är eventuellt inte nödvändig om ingen känslig information röjs och endast ett litet antal e-postadresser har avslöjats.