Nätsäkerhetsavdelningen

Vägledning om skyldigheten att rapportera integritetsincidenter

Rapportering av integritetsincidenter

Sedan den 1 juli 2011 är operatörer skyldiga att rapportera inträffade integritetsincidenter till PTS och till berörda abonnenter eller användare, det framgår av 6 kap. 4 a § lagen (2003:389) om elektronisk kommunikation. När och hur rapportering ska ske samt vad rapporterna ska innehålla framgår fr.o.m. den 25 augusti 2013 av Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott. Den här vägledningen beskriver reglerna närmare.

Vägledningen innehåller förklaringar och exempel som avser att illustrera hur reglerna kan tillämpas. Dessa ska däremot inte betraktas som förhandsbesked om vilka bedömningar PTS kan komma att göra i ett enskilt ärende.

Varför ska integritetsincidenter rapporteras?

Ett tillförlitligt och säkert utbyte av information via elektroniska kommunikationsnät och elektroniska kommunikationstjänster blir alltmer centralt i samhället. PTS har till uppgift att främja tillgången till säkra och effektiva elektroniska kommunikationer och utövar tillsyn över regler om bl.a. integritetsskydd i lagen (2003:389) om elektronisk kommunikation (LEK).

Integritetsincidenter utgör potentiellt ett allvarligt hot mot tilltron till elektroniska kommunikationstjänster. Om information, t.ex. personuppgifter, som behandlats inom ramen för en elektronisk kommunikationstjänst sprids till utomstående eller går förlorad kan det få allvarliga konsekvenser. Om sådana

händelser inte hanteras på ett lämpligt sätt kan det leda till att individer råkar ut för såväl ekonomisk skada som personlig kränkning.

Skyldigheten för operatörer att rapportera integritetsincidenter är tänkt att ge PTS ett underlag för att kunna bedöma om det finns anledning att misstänka att bestämmelserna om integritetsskydd inte efterlevs och i sådana fall möjliggöra för PTS att vidta lämpliga tillsynsåtgärder. Även i de fall en rapport inte ger upphov till direkta tillsynsåtgärder kan den innehålla uppgifter som bidrar till myndighetens kunskap om vanliga orsaker till incidenter m.m. Den kan därmed komma att utgöra en viktig grund för myndighetens långsiktiga arbete för att främja integritetsskyddet i de elektroniska kommunikationerna.

Vem är skyldig att rapportera integritetsincidenter?

Reglerna gäller för alla som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster. En elektronisk kommunikationstjänst är en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät. För mer information om innebörden av dessa begrepp, se anmälningsplikt för operatörer.

Vad är en integritetsincident?

En integritetsincident är enligt definitionen i LEK en händelse som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring, eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster.

Som framgår omfattar begreppet, enligt sin ordalydelse, många olika slags händelser av varierande dignitet. Det finns dock några faktorer som operatörer bör beakta i sin bedömning av om en inträffad händelse utgör en integritetsincident som ska rapporteras.

För att en integritetsincident ska anses ha inträffat krävs att händelsen har samband med behandling av uppgifter. Med behandling avses t.ex. insamling, registrering, lagring och bearbetning. Behandlingen ska ha skett i samband med tillhandahållandet av en allmänt tillgänglig elektronisk kommunikationstjänst, vilket innebär att det inte nödvändigtvis är alla uppgifter som en operatör behandlar som berörs. Uppgifter som enbart hanteras inom eller för att stödja företagets interna processer eller tjänster som är fristående från tillhandahållandet av kommunikationstjänsten omfattas alltså inte.

De typer av uppgifter som framförallt omfattas är dels det innehåll som överförs i kommunikationstjänsten, dels de abonnentuppgifter, trafikuppgifter och lokaliseringsuppgifter som kan kopplas till den överförda informationen,

till abonnemangsinnehavare eller till de användare som kommunicerar. Uppgifterna ska normalt röra eller kunna hänföras till en abonnent eller användare för att omfattas.

I nedanstående tabell framgår (med röd markering) vilka förfaranden med uppgifterna som omfattas av begreppet integritetsincident.

	Utplåning	**Förlust**	**Ändring**	**Avslöjande**	**Åtkomst**
Oavsiktlig					
Otillåten					

En avgränsande faktor är också att skyldigheten att rapportera integritetsincidenter bör ses i ljuset av kraven på att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att behandlade uppgifter skyddas, reglerna om tystnadsplikt för vissa uppgifter samt övriga regler om hur uppgifter får behandlas i LEK. Det innebär att de händelser som faller inom begreppet integritetsincident bör ha en koppling till en sådan teknisk eller organisatorisk åtgärd som operatören är skyldig att vidta eller till någon av de övriga reglerna om integritetsskydd. T.ex. bör inte enbart det faktum att uppgifter behandlats i strid med en intern föreskrift hos operatören, som inte kan kopplas till den lagstadgade skyldigheten att skydda uppgifterna, innebära att behandlingen utgör en integritetsincident. Det bör beaktas särskilt när interna riktlinjer om incidentrapporteringen utformas eftersom det kan vara så att händelser som internt inom företaget anses utgöra incidenter inte omfattas av begreppet i LEK och därför inte behöver rapporteras.

Slutligen bör frågan om när en integritetsincident kan sägas ha inträffat beaktas. Enligt definitionen utgör en incident ”en händelse som leder till…” ett visst förfarande med de berörda uppgifterna. Detta torde innebära att begreppet integritetsincident endast innefattar situationer där dessa förfaranden faktiskt har inträffat. En händelse som t.ex. inneburit en risk för att vissa uppgifter hamnar i otillåtna händer men där operatören löst den underliggande bristen i tid, innan någon obehörig hunnit få åtkomst till informationen, torde alltså normalt inte betraktas som en sådan integritetsincident som avses i denna vägledning. En integritetsincident ska betraktas som upptäckt av operatören, när denne är medveten om att en incident har inträffat och att incidenten berör sådana uppgifter som omfattas av bestämmelsen enligt ovan. Det är inte nödvändigt att alla omständigheter om incidenten är klarlagda för att den ska anses vara upptäckt.

Observera att i Kommissionens förordning nr 611/2013 används begreppet ”personuppgiftsbrott” med samma innebörd som begreppet ”integritetsincident” har i LEK.

Vilka integritetsincidenter ska rapporteras och till vem?

Som utgångspunkt ska samtliga integritetsincidenter rapporteras till både PTS och till berörda abonnenter eller användare. Dessutom ska samtliga integritetsincidenter föras in i en förteckning hos operatören.

När det gäller rapportering till berörda abonnenter eller användare så finns undantag från skyldigheten. Rapport till dessa behöver inte lämnas

- om integritetsincidenten inte kan antas inverka negativt på abonnenterna eller användarna
  eller
- om tjänstetillhandahållaren har vidtagit tekniska skyddsåtgärder som medför att de uppgifter som berörs av incidenten är oläsbara för obehöriga, t.ex. genom kryptering eller hashning av uppgifterna.

Vid bedömningen av om en integritetsincident kan antas inverka negativt på abonnenterna eller användarna ska operatören särskilt ta hänsyn till:

1. Uppgifternas art och innehåll; i synnerhet om de avser finansiell information, känsliga personuppgifter (uppgift om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, eller medlemskap i fackförening), lokaliseringsuppgifter, internetloggar, webbläsarhistorik, uppgifter om e-post eller specificerade samtalslistor.
2. Integritetsincidentens troliga konsekvenser för abonnenterna eller användarna; i synnerhet om incidenten skulle kunna leda till identitetsstöld eller bedrägeri, fysisk skada, psykiska men, förödmjukelse eller skadat rykte.
3. Omständigheterna kring integritetsincidenten; i synnerhet om uppgifterna har stulits eller om operatören vet att uppgifterna finns hos en obehörig tredje part.

När det gäller kryptering av uppgifter sker det en ständig utveckling inom området och den allmänna uppfattningen om säkerhetsnivån i en viss krypteringsmetod kan snabbt förändras om metoder för att kringgå krypteringen uppdagas. Det innebär att det inte är möjligt att närmare specificera vilken slags kryptering det ska röra sig om. Det finns dock rekommendationer på området som kan vara lämpliga att utgå från, t.ex. från ETSI:s Security Algorithms Group of Experts (SAGE).

Operatören ska även föra en egen förteckning över samtliga inträffade integritetsincidenter. Förteckningen ska även uppdateras löpande, vilket innebär att operatören ska fortsätta uppdatera den även efter det att rapporter har lämnats till PTS och berörda abonnenter eller användare.

När och hur ska rapportering ske till PTS och vad ska rapporterna innehålla?

Rapporterna om integritetsincidenter ska i första hand utgöra ett underlag för PTS vid bedömningen om operatören bedriver sin verksamhet i enlighet med bestämmelserna om integritetsskydd i LEK och om det finns anledning att vidta tillsynsåtgärder till följd av den inträffade händelsen. För att kunna göra en sådan bedömning behöver PTS information om vad som har skett, omfattningen och konsekvenserna av incidenten samt vilka åtgärder som vidtagits för att förhindra liknande incidenter i framtiden.

Den obligatoriska rapporteringsskyldigheten innebär att operatören självmant ska lämna en rapport till PTS senast 24 timmar efter det att integritetsincidenten upptäcks. I vissa fall, t.ex. vid större incidenter som tar tid att utreda, ska istället operatören lämna flera delrapporter till PTS. En inledande rapport ska alltid lämnas senast 24 timmar efter att incidenten upptäcks och, om operatören vid denna tidpunkt ännu inte har tillgång till alla uppgifter om incidenten, ska resterande uppgifter lämnas i en kompletterande rapport så snart som möjligt, dock senast tre dagar efter den inledande rapporten. Om operatören genom sitt utredningsarbete inte har kunnat ta fram alla uppgifter inom tre dagar ska operatören lämna en välgrundad motivering till detta tillsammans med en rapport som innehåller alla då tillgängliga uppgifter. Operatören ska därefter lämna resterande uppgifter och, om det är nödvändigt, uppdateringar av redan lämnade uppgifter, så snart det är möjligt.

De uppgifter som sammantaget ska rapporteras till PTS är följande:

När integritetsincidenten inträffade och upptäcktes

När en incident rör ett tekniskt system bör en operatör många gånger, med stöd av uppgifter från system för övervakning eller loggning, kunna fastställa relativt exakt när en integritetsincident inträffade. När så inte är fallet får istället en uppskattning göras med utgångspunkt från de fakta om incidenten som operatören kan fastställa i sin utredning. Utöver tidsangivelsen bör operatören i rapporten redogöra för hur uppgifterna har fastställts.

Det är inte ovanligt att händelseförloppet för en incident kan delas in i flera steg. Integritetsincidenter kan många gånger uppkomma genom en kedja av händelser; t.ex. där en underliggande brist eller sårbarhet uppkommer varefter den vid en eller flera senare tidpunkter utnyttjas på

ett sätt som leder till att något av de för inrapporteringsskyldigheten relevanta förfarandena med uppgifter inträffar. Även arbetet med att åtgärda en inträffad incident kan ske i flera steg. I dessa fall bör operatören i rapporten ange tidpunkten för varje sådan relevant händelse i samband med integritetsincidentens uppkomst och avhjälpande.

Tidpunkten när integritetsincidenten upptäcktes ska också anges i rapporten.

Antal berörda abonnenter eller användare

En integritetsincident bör normalt alltid beröra minst en abonnent eller användare. I många fall bör det vara relativt enkelt för operatören att fastställa vilka och hur många dessa är. I dessa fall ska antalet anges i rapporten. Det kan dock förekomma incidenter där det inte är möjligt att fastställa ett exakt antal men i dessa fall bör operatören istället beskriva konsekvenserna i andra termer, som ger en tydlig bild av omfattningen.

Beskrivning av integritetsincidenten, dess orsaker och konsekvenser

Beroende på incidentens komplexitet kan beskrivningen behöva vara allt från mycket kortfattad till mycket omfattande. Berörda elektroniska kommunikationstjänster bör normalt anges. I de fall incidenten involverar vissa tekniska system bör även dessa beskrivas. Likaså vilka kategorier av abonnenter eller användare som berörs av incidenten. Har viss personal varit bidragande till eller inblandad i incidentens förlopp bör även detta anges.

Beskrivningen ska också innehålla information om vilka slags uppgifter om abonnenter eller användare, t.ex. vilka abonnent- eller trafikuppgifter, som har berörts av incidenten.

Normalt bör den grundläggande orsaken till integritetsincidenten anges i beskrivningen. Exempel på sådana grundläggande orsaker kan vara brister i organisation eller processer, tekniska fel i system, mänskliga misstag eller uppsåtligt felaktigt agerande. Utöver den grundläggande orsaken bör även bidragande orsaker anges, så att det av beskrivningen tydligt framgår hur den aktuella integritetsincidenten kunde uppkomma.

Konsekvenserna av incidenten bör dels beskrivas i tekniska termer (i de fall tekniska system är inblandade) och dels i termer av hur abonnenter eller användare har berörts av incidenten. Den tekniska beskrivningen bör vara specifik och t.ex. ange att en viss angiven databas med ett visst angivet innehåll varit åtkomlig för obehöriga under vissa angivna omständigheter. Beskrivningen av hur abonnenter eller användare berörts

bör istället ta sikte på att beskriva konsekvenserna ur deras perspektiv, t.ex. vilken personlig information som berörs och på vilket sätt. I de fall incidenten bedöms ha haft en negativ inverkan på abonnenter eller användare ska beskrivas på vilket sätt dessa kan ha påverkats negativt.

Åtgärder för att avhjälpa brister och för att undvika liknande incidenter

Operatören ska redogöra för vilka åtgärder som har vidtagits för att lindra effekterna av incidenten. Vidare ska operatören redogöra för de tillfälliga och permanenta åtgärder som har vidtagits eller som planeras för att åtgärda grundorsaken och de bidragande orsakerna till integritetsincidenten. Det kan t.ex. röra sig om förändrade rutiner på företaget, uppdatering av felaktig mjukvara eller förstärkning av tekniska säkerhetsåtgärder.

Efter att en integritetsincident har inträffat och avhjälpts är det väsentligt att händelsen analyseras i syfte att finna eventuella förbättringsåtgärder som kan minska risken för att incidenter ska kunna uppkomma på grund av liknande orsaker i framtiden. I vissa fall kan åtgärder vidtas relativt omgående i samband med incidenten medan det i vissa fall krävs en långsiktig åtgärdsplan. I operatörens redogörelse bör det framgå, dels vilka åtgärder som redan vidtagits och när så skedde, dels vilka åtgärder som planeras framöver och när de enligt planen kommer att vidtas.

Medverkan av andra tjänsteleverantörer

I de fall operatören har använt sig av en extern leverantör för att tillhandahålla en del av en tjänst, är operatören skyldig att genom avtal eller annan utfästelse se till att denna andra leverantör omedelbart informerar operatören om inträffade incidenter som berör denna leverantör. Sådana andra leverantörers medverkan vid incidenter ska sedan anges i rapporten från operatören till PTS. Det bör där beskrivas vilken leverantör som berörts och på vilket sätt leverantören har medverkat till eller påverkats av incidenten.

Medverkan eller påverkan på abonnenter eller användare i andra länder

Om en integritetsincident även berör abonnenter eller användare i andra länder ska rapporten innehålla uppgift om vilket eller vilka länder. Dessutom ska rapporten innehålla uppgift om vilka myndigheter i dessa länder som incidenten har anmälts till.

Vid all rapportering som rör en och samma integritetsincident bör operatören ange ett referensnummer för incidenten. Detta nummer bör vara kopplat till operatörens förteckning över integritetsincidenter. Orsaken till detta är bland annat att PTS, vid en eventuell tillsyn, enkelt ska kunna erhålla all information

som operatören har om en viss angiven integritetsincident. I rapporter som lämnas om integritetsincidenter ska operatören dessutom lämna uppgift om en kontaktperson, som kan vara PTS behjälplig med ytterligare information om incidenten.

Utöver den rapport som är ställd till PTS och som beskrivs ovan, ska operatören också lämna kopior till PTS på de rapporter som skickats till berörda abonnenter eller användare. Se mer om detta nedan.

All rapportering av integritetsincidenter till PTS bör ske elektroniskt. För ändamålet har PTS upprättat en särskild e-tjänst för operatörer att skapa och skicka in rapporter men även se tidigare lämnade rapporter. E-tjänsten nås på adressen incident.pts.se. Rapporter kan även skickas in med e-post till incidentrapport@pts.se. Rapporter som skickas till denna adress tas emot direkt av de handläggare på myndigheten som arbetar med tillsyn inom integritetsområdet. PTS har för avsikt att göra det möjligt att även skicka krypterad e-post till denna adress.

När och hur ska rapportering ske till berörda abonnenter eller användare och vad ska rapporterna innehålla

Anledningen till att även de abonnenter eller användare som berörs av en integritetsincident ska underrättas om den är i första hand att ge dem möjligheten att vidta lämpliga åtgärder för att begränsa eller på något sätt hantera den skada som incidenten kan medföra. Observera att rapporter om integritetsincidenter ska lämnas oavsett om operatören anser att det finns några reella möjligheter för abonnenterna eller användarna att begränsa sin egen skada eller inte.

Den obligatoriska rapporteringsskyldigheten innebär att operatören självmant ska lämna en rapport till berörda abonnenter eller användare utan onödigt dröjsmål efter det att integritetsincidenten upptäcks. Rapporten till abonnenter och användare är fristående från den rapport som ska lämnas till PTS.

Operatören får som utgångspunkt göra en egen bedömning av vilket dröjsmål som inte är ”onödigt” i varje enskilt fall. Operatören bör beakta abonnenternas och användarnas intresse av och möjlighet att själva vidta åtgärder för att begränsa sin skada. Det innebär att det i vissa fall kan vara motiverat att lämna sådana rapporter omgående efter det att integritetsincidenten har upptäckts och en preliminär bedömning har gjorts av dess konsekvenser. Det kan alltså vara lämpligt att lämna information till abonnenter eller användare redan baserat på preliminära bedömningar om det kan antas att eventuella åtgärder från deras sida bör vidtas så snart som möjligt för att skadan ska kunna begränsas. Skulle det senare visa sig att de preliminära bedömningarna varit felaktiga, får uppdaterad och korrigerad information lämnas i en förnyad rapport.

De uppgifter som sammantaget ska rapporteras till abonnenter eller användare är följande:

När integritetsincidenten inträffade

Till skillnad från rapporteringen till PTS så bör det i normalfallet inte behövas en lika ingående beskrivning av incidentens förlopp. Den tidpunkt som bör anges i rapporten till abonnenter eller användare bör istället avse den tid då den händelse inträffade som är relevant ur deras perspektiv, t.ex. det datum när en obehörig fick åtkomst till eller tog del av vissa uppgifter.

Beskrivning av integritetsincidenten och dess konsekvenser

För att de berörda abonnenterna eller användarna ska kunna göra egna bedömningar av vilka eventuella åtgärder som är nödvändiga eller lämpliga att vidta till följd av incidenten är det viktigt att operatören på ett så begripligt sätt som möjligt förklarar vad det är som har inträffat och hur det inträffade påverkar abonnenterna eller användarna. Det bör alltså normalt inte vara nödvändigt att beskriva incidenten i tekniska termer men däremot utförligt vad incidenten kan innebära ur abonnenternas eller användarnas perspektiv.

Informationen bör så långt som möjligt anpassas efter varje abonnent eller användare som berörs av integritetsincidenten. Om t.ex. olika kategorier av användare berörs i olika grad eller på olika sätt så bör informationen anpassas för varje sådan kategori eller i vart fall tydligt ange de skillnader som finns.

Rapporten ska beskriva vilka slags uppgifter, t.ex. vilka abonnent- eller trafikuppgifter, som berörs av integritetsincidenten samt innehållet i dessa uppgifter.

Åtgärder som operatören vidtar som påverkar abonnenter eller användare

Rapporten ska vidare beskriva de åtgärder som operatören har vidtagit eller har för avsikt att vidta som kan påverka berörda abonnenter eller användare. Beskrivningen bör ange varför dessa åtgärder vidtas, vad operatören förväntar sig att uppnå med åtgärderna och på vilket sätt abonnenterna eller användarna påverkas av dem.

I första hand bör beskrivningen omfatta åtgärder som har direkt koppling till den inträffade integritetsincidenten och dess konsekvenser men det kan vara lämpligt att även beskriva hur operatören arbetar på länge sikt för att undvika att liknande incidenter inträffar igen.

Rekommenderade åtgärder som abonnenten eller användaren bör vidta

I de fall operatören kan identifiera en eller flera åtgärder som abonnenter eller användare kan vidta för att begränsa sin skada till följd av integritetsincidenten så ska dessa åtgärder beskrivas i rapporten. Beskrivningen ska vara tydlig och lättbegriplig så att den genomsnittlige abonnenten eller användaren förstår syfte och effekter av föreslagna åtgärder och kan följa de angivna instruktionerna.

Har en integritetsincident inträffat där operatören gör bedömningen att abonnenterna eller användarna inte kan vidta några egna åtgärder för att begränsa eller hantera skadan, så bör även detta tydligt anges och förklaras.

Kontaktuppgifter till operatören

En rapport om en integritetsincident kan många gånger antas ge upphov till följdfrågor eller synpunkter från de berörda abonnenterna eller användarnas sida. Därför ska rapporten även innehålla information om hur abonnenter och användare kan komma i kontakt med operatören i frågor som rör incidenten. Det är givetvis lämpligt att operatören också säkerställer att det finns tillräcklig kompetens och kapacitet hos den uppgivna kontakten, för att kunna hantera frågor och synpunkter från de berörda abonnenterna eller användarna.

Slutligen bör även i rapporterna till abonnenter och användare anges det referensnummer för incidenten som beskrivs ovan.

Rapporterna ska lämnas till de berörda abonnenterna eller användarna på ett sätt som säkerställer att informationen snabbt kan tas emot och att den skyddas på lämpligt sätt. Som utgångspunkt bör operatören använda någon av de kommunikationskanaler som operatören brukar använda för att kommunicera med abonnenterna eller användarna. Det är dock viktigt att operatören tar rimliga steg för att säkerställa att informationen verkligen når fram. Detta innebär t.ex. att operatören inte alltid kan förlita sig på att en e-postadress som operatören har tilldelat en abonnent verkligen används av abonnenten. Vilken kommunikationsform som används bör också vara beroende av hur brådskande det är att informationen når fram till abonnenten eller användaren. Finns det t.ex. åtgärder som användaren kan vidta för att begränsa sin skada så bör operatören välja en kommunikationskanal som låter informationen snabbt nå fram till användaren. I vissa fall kan det även vara lämpligt att lämna samma information parallellt via flera olika kanaler.

Rapporterna ska formuleras tydligt och lättbegripligt och får inte lämnas tillsammans med någon annan information, t.ex. tillsammans med marknadsföring av tjänster.

När en rapport avseende en integritetsincident har lämnats till en abonnent eller användare ska en kopia på innehållet i rapporten också lämnas till PTS. I de fall en likalydande rapport har lämnats till samtliga abonnenter eller användare är det tillräckligt att ett exemplar av rapporten lämnas till PTS. Har däremot anpassningar gjorts för olika grupper eller kategorier av abonnenter eller användare bör ett exemplar av varje variant av rapporten lämnas till PTS. Uppgifter som kan identifiera enskilda abonnenter eller användare ska dock inte finnas med i de exemplar som lämnas till PTS.

Kopian eller kopiorna ska lämnas till PTS i samband med att de lämnas till abonnenter och användare eller senast tillsammans med den rapport som ska lämnas till PTS. Eftersom PTS även har ansvar för tillsyn över att operatörer lämnar korrekt och fullständig information till berörda abonnenter eller användare, och att informationen lämnas i rätt tid, är det viktigt att PTS får ta del av denna information så snart som möjligt.

När kopior på rapporter till abonnenter eller användare lämnas till PTS, ska operatören också ange vilka kommunikationskanaler operatören har använt för att förmedla rapporterna till de berörda abonnenterna eller användarna.