

Nätsäkerhetsavdelningen  
Staffan Lindmark  
08-678 57 36  
staffan.lindmark@pts.se

## **Konsekvensutredning avseende föreskrifter om upphävande av Post- och telestyrelsens föreskrifter (PTSFS 2012:1) och allmänna råd om underrättelse om integritetsincidenter samt innehållet i förteckning över integritetsincidenter**

Post- och telestyrelsen (PTS) avser att med stöd av 34 b § förordningen (2003:396) om elektronisk kommunikation utfärda föreskrifter om upphävande av PTS föreskrifter (PTSFS 2012:1) och allmänna råd om underrättelse om integritetsincidenter samt innehållet i förteckning över integritetsincidenter.

PTS redovisar härmed sin utredning enligt förordning (2007:1244) om konsekvensutredning vid regelgivning.

Förslag till föreskrifter bifogas, se bilaga 1.

# 1 Beskrivning av problemet och vad som ska uppnås

## Beskrivning av marknaden för elektronisk kommunikation

Den svenska marknaden för elektronisk kommunikation är avreglerad sedan drygt 20 år. Avregleringen har skapat en mångfacetterad marknad som karaktäriseras av en ökad konkurrens och snabb teknikutveckling, vilket i sin tur inneburit att vi i Sverige idag har ett brett och diversifierat utbud av nät och tjänster.

Inom sektorn finns i dag drygt 400 tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster (nedan kallade tjänstetillhandahållare), allt från stora multinationella företag med stort tjänsteutbud till mindre operatörer, som erbjuder en begränsad mängd tjänster inom ett begränsat geografiskt område.

## Den nationella regleringen om rapportering av integritetsincidenter

Sedan den 1 juli 2011 är tjänstetillhandahållare skyldiga att utan onödigt dröjsmål underrätta tillsynsmyndigheten om integritetsincidenter samt föra förteckning över dessa. Bestämmelserna i 6 kap. 4 a och 4 b §§ lagen (2003:389) om elektronisk kommunikation (LEK) genomför artikel 4.3 – 4.4 i Europaparlamentets och rådets direktiv 2002/58/EG om integritet och elektronisk kommunikation i svensk rätt.<sup>1</sup>

Den 21 februari 2012 beslutade PTS föreskrifter och allmänna råd om underrättelse om integritetsincidenter samt innehållet i förteckning över integritetsincidenter (PTSFS 2012:1). Föreskrifterna, som trädde i kraft den 1 april 2012, reglerar vilka uppgifter underrättelsen till PTS respektive berörda abonnenter eller användare ska innehålla samt fastställer vad som ska beaktas vid bedömningen av vid vilken tidpunkt underrättelsen ska lämnas. Vidare föreskrivs vissa undantag från skyldigheten att lämna underrättelser om integritetsincidenter. Föreskrifterna anger även vilka uppgifter som ska ingå i tjänstetillhandahållarnas förteckning över integritetsincidenter.

PTS gjorde vid tiden för beslutet bedömningen att vissa av föreskrifterna behövdes för att direktivet skulle anses helt implementerat i svensk rätt. Vidare ansåg PTS att det fanns stora fördelar med en tydligare beskrivning av vad skyldigheterna i lagen innebär.

---

<sup>1</sup> Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation, som ändrats genom Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009

### **Kommissionens förordning om rapportering av personuppgiftsbrott**

Den 24 juni 2013 beslutade EU-kommissionen förordning (EU) nr 611/2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation. Förordningen, som trädde i kraft den 25 augusti 2013, beslutades med stöd av artikel 4.5 i direktiv 2002/58/EG, enligt vilken kommissionen får anta tekniska genomförandeåtgärder avseende omständigheter, format och förfaranden som kan tillämpas för de informations- och anmälningskrav som avses i artikel 4.

Kommissionens förordning reglerar när anmälan av så kallade personuppgiftsbrott ska ske till den behöriga nationella myndigheten respektive berörda abonnenter eller enskilda personer. Vidare reglerar förordningen vilka uppgifter sådana anmälningar ska innehålla. Förordningen föreskriver även vissa undantag från skyldigheten att lämna anmälan till abonnenter eller enskilda personer.

### **Förhållandet mellan nationell reglering och EU-rätten**

Begreppet integritetsincident i svensk rätt är snarlikt begreppet personuppgiftsbrott i direktivet och kommissionens förordning.<sup>2</sup> Det innebär att PTS föreskrifter och Kommissionens förordning till stora delar reglerar samma frågor. Bestämmelserna i respektive författning är dock inte helt samstämmiga.

Av EU-domstolens praxis framgår att nationella regler inte får strida mot EU:s regler. Allmänt gäller alltså att en myndighet inte får införa eller behålla föreskrifter som strider mot de grundläggande fördragen eller institutionernas rättsakter. En annan begränsning, som gäller enligt EU-domstolens praxis, är att EU-förordningar inte får införlivas genom nationell normgivning i medlemsstaterna eftersom det kan skapa tvivel om deras ursprung och rättsliga effekt.<sup>3</sup>

Detta innebär att såväl de av PTS föreskrifter och allmänna råd som inte överensstämmer med reglerna i kommissionens förordning som de föreskrifter och allmänna råd som helt överensstämmer med (och därmed kan anses införliva) förordningen, numera står i strid med EU-rätten. Endast de av PTS föreskrifter och allmänna råd som reglerar frågor utanför det område som omfattas av kommissionens förordning, får behållas.

---

<sup>2</sup> För en närmare beskrivning av skillnaden mellan begreppet integritetsincident och personuppgiftsbrott och den praktiska innebörden av skillnaden, se bilaga 2.

<sup>3</sup> Se DS 1998:43, *Myndigheternas föreskrifter – Handbok i författningsskrivning*, s 56.

**Vad PTS vill uppnå med att upphäva föreskrifterna och allmänna råden**

Som beskrivs ovan står flertalet av föreskrifterna och de allmänna råden i PTSFS 2012:1 i strid med EU-rätten. Detta innebär att PTS måste ändra eller upphäva föreskrifterna så att denna konflikt undanröjs.

Enligt PTS bedömning är det endast bestämmelsen i 10 §, som anger vilka uppgifter tjänstetillhandahållarens löpande förteckning över integritetsincidenter enligt 6 kap. 4 b § LEK ska innehålla, som skulle kunna behållas i oförändrat skick, eftersom kommissionens förordning inte reglerar innehållet i dessa förteckningar.

Den 18 februari 2014 beslutade PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1), vilka träder i kraft den 1 september 2014. I 11 § anges vilka uppgifter tjänstetillhandahållarens förteckning över integritetsincidenter ska innehålla. Denna bestämmelse har i materiellt hänseende samma innehåll som 10 § PTSFS 2012:1, vilket gör att det inte finns något behov av att behålla den senare bestämmelsen.

Mot bakgrund av dels att regleringen om rapportering av integritetsincidenter till stora delar har ersatts av regleringen i kommissionens förordning och dels att bestämmelsen om innehållet i förteckningen över integritetsincidenter i oförändrat skick har överförts till PTSFS 2014:1, anser PTS att det är befogat att upphäva samtliga bestämmelser i PTSFS 2012:1.

## **2 Alternativa lösningar och vilka effekterna blir om ett upphävande inte kommer till stånd**

### **Oförändrade föreskrifter**

Som har beskrivits ovan gör PTS bedömningen att PTS föreskrifter och allmänna råd om underrättelse om integritetsincidenter samt innehållet i förteckning över integritetsincidenter (PTSFS 2012:1), i de delar som reglerar rapporteringen av integritetsincidenter, står i strid med de åtaganden som följer av Sveriges anslutning till EU. Vidare har PTS beslutat att överföra bestämmelsen om innehållet i tjänstetillhandahållarnas förteckning över integritetsincidenter till en annan författning. Att behålla reglerna i oförändrat skick är således inte ett möjligt alternativ.

### **Alternativ till att upphäva föreskrifterna i sin helhet**

Ett alternativ till att helt upphäva föreskrifterna och de allmänna råden är att endast upphäva bestämmelsen om innehållet i förteckningen över integritetsincidenter, och i övrigt ändra reglerna så att de enbart omfattar sådant som ligger utanför det område som regleras av kommissionens förordning.

Enligt PTS bedömning är emellertid de reglerade områdena till största delen överlappande. Den skillnad som finns mellan PTS föreskrifter och allmänna råd, och kommissionens förordning är att de sistnämnda omfattar så kallade personuppgiftsbrott medan de förstnämnda omfattar det något vidare begreppet integritetsincidenter.

Det skulle således vara möjligt att ändra PTS föreskrifter och allmänna råd så att de enbart gäller sådana integritetsincidenter som inte samtidigt utgör personuppgiftsbrott. Av skäl som närmare anges nedan förordar emellertid PTS inte denna alternativa lösning.

### **3 Vilka som berörs av regleringen**

Av 6 kap. 4 a § LEK framgår att den som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster bland annat ska underrätta tillsynsmyndigheten om integritetsincidenter. Enligt 6 kap. 4 b § LEK ska den som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster löpande föra en förteckning över integritetsincidenter. Samtliga tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster berörs således av skyldigheterna i de föreskrifter och allmänna råd som PTS föreslår ska upphävas.

Marknaden för elektronisk kommunikation tillgodoser i stort sett samtliga företag, hushåll och enskilda individer i Sverige med olika typer av kommunikationstjänster. Drygt 500 företag har anmält till PTS att de tillhandahåller verksamhet som är anmälningspliktig enligt 2 kap. 1 § LEK. Av dessa uppskattar PTS att drygt 400 tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster. Dessa företag berörs direkt av föreskrifterna och de allmänna råden.

Det finns även aktörer som berörs indirekt av regleringen. Det är bland annat slutanvändare, samhällsviktiga aktörer, leverantörer, andra myndigheter etc. Av dessa bör slutanvändarna särskilt nämnas eftersom 6 kap. 4 a § LEK och PTS föreskrifter uppställer krav på att abonnenter och användare som berörs av en integritetsincident ska underrättas om denna.

## 4 Vilka kostnadsmässiga och andra konsekvenser föreskriften medför och en jämförelse av konsekvenser för övervägda alternativ

PTS förslag innebär att det inte längre kommer att finnas någon detaljerad reglering av hur rapporteringen av integritetsincidenter, som inte samtidigt utgör personuppgiftsbrott, ska gå till.

PTS gör bedömningen att det stora flertalet integritetsincidenter samtidigt utgör personuppgiftsbrott.<sup>4</sup> Avsaknaden av detaljreglering torde därmed endast sällan komma att få någon praktisk betydelse. Att det fåtal incidenter som enligt definitionerna utgör integritetsincidenter men inte personuppgiftsbrott ska rapporteras till PTS, framgår direkt av bestämmelsen i 6 kap. 4 a § LEK. Det är endast de närmare formerna för rapporteringen som inte längre kommer att vara reglerad. Vid tolkningen av hur bestämmelsen i 6 kap. 4 a § LEK ska tillämpas i dessa fall, torde regleringen avseende formerna för rapportering av personuppgiftsbrott kunna vara vägledande.

Den alternativa lösning som har övervägts innebär att föreskrifterna och de allmänna råden istället ändras så att de endast gäller sådana integritetsincidenter som inte samtidigt utgör personuppgiftsbrott. Eftersom övriga incidenter redan idag regleras av Kommissionens förordning (EU) nr 611/2013 skulle en sådan förändring inte medföra några konsekvenser alls.

### Administrativa kostnader som följer av förslaget

Ett upphävande av den detaljerade regleringen av hur rapportering av integritetsincidenter, som inte samtidigt utgör personuppgiftsbrott, ska ske medför enligt PTS bedömning en liten minskning av den administrativa kostnaden för att upprätta och inlämna sådana rapporter. Eftersom den grundläggande skyldigheten att upprätta sådana rapporter ändå kvarstår enligt LEK, och med beaktande av det fåtal rapporter som berörs av förändringen, gör PTS emellertid bedömningen att besparingen är ytterst marginell.

Vidare bortfaller de begränsade undantagen från skyldigheten att underrätta PTS och berörda abonnenter. Enligt 8 § i föreskrifterna behöver en underrättelse inte lämnas till PTS om en integritetsincident endast berör ett fåtal abonnenter eller användare och inte kan antas inverka negativt på dessa abonnenter eller användare. Vidare gäller enligt 9 § i föreskrifterna att en

---

<sup>4</sup> För en närmare beskrivning av skillnaden mellan begreppet integritetsincident och personuppgiftsbrott och den praktiska innebörden av skillnaden, se bilaga 2.

underrättelse inte behöver lämnas till berörd abonnent eller användare om tjänstetillhandahållaren med en allmänt erkänd krypteringsmetod av tillräcklig nyckellängd krypterat de uppgifter som berörs av en integritetsincident och uppgifterna därför var oläsbara för alla obehöriga när incidenten inträffade.

Konsekvensen av PTS förslag blir således att en mindre andel av de redan mycket få integritetsincidenter som inte samtidigt utgör personuppgiftsbrott, nu måste rapporteras. Förändringen torde innebära en liten ökning av de administrativa kostnaderna. Med hänsyn till det mycket begränsade antal integritetsincidenter som berörs av denna förändring gör emellertid PTS bedömningen att ökningen är ytterst marginell.

Sammanfattningsvis kan PTS förslag medföra såväl en marginell ökning som en marginell minskning av de administrativa kostnaderna. Ingendera låter sig med lätthet kvantifieras i nominella belopp. PTS gör dock bedömningen att de administrativa kostnaderna, vid en sammanvägning, är väsentligen oförändrade av förslaget.

#### **Slutsats**

Sammanfattningsvis gör PTS bedömningen att PTS förslag inte medför några väsentliga förändringar vad gäller vare sig administrativa eller övriga kostnader. Det kan dock finnas enstaka tjänstetillhandahållare som, på grund av de tjänster de tillhandahåller eller vilka slags kunder de vänder sig till, kan beröras i något högre grad än vad som angivits ovan.

Den alternativa lösningen medför, som konstaterats ovan, inte några konsekvenser alls och påverkar därför inte heller vare sig de administrativa eller övriga kostnaderna. Det skulle enligt PTS bedömning ändå vara av mycket liten praktisk betydelse att utfärda föreskrifter och allmänna råd som endast omfattar rapportering av de fåtal integritetsincidenter som inte samtidigt utgör personuppgiftsbrott. Föreskrifter och allmänna råd med ett så snävt tillämpningsområde kan, enligt PTS mening, snarare leda till missförstånd om vilka regler som gäller för rapportering av integritetsincidenter. Det är då bättre att låta PTS inom ramen för sin tillsyn precisera hur rapporteringen av de berörda integritetsincidenterna ska gå till.

Mot denna bakgrund gör PTS bedömningen att det bästa regleringsalternativet är att upphäva PTS föreskrifter och allmänna råd om underrättelse om integritetsincidenter samt innehållet i förteckning över integritetsincidenter (PTSFS 2012:1) i sin helhet.



## **5 Bedömning av om regleringen överensstämmer med skyldigheter som följer av Sveriges anslutning till EU**

Som beskrivits ovan gör PTS bedömningen att ikraftträdandet av Kommissionens förordning (EU) nr 611/2013 medfört att PTS föreskrifter (PTSFS 2012:1) och allmänna råd om underrättelse om integritetsincidenter samt innehållet i förteckning över integritetsincidenter, står i strid med EU-rätten.

Förslaget till upphävande av föreskrifterna och de allmänna råden syftar till att genomföra åtgärder som är nödvändiga för att efterleva de skyldigheter som följer av Sveriges anslutning till EU.

## **6 Bedömning av om särskilda hänsyn behöver tas när det gäller tidpunkt för ikraftträdande och om det finns behov av speciella informationsinsatser**

När det gäller tidpunkten för ikraftträdande av PTS föreskrifter, vilka innebär ett upphävande av PTS föreskrifter (PTSFS 2012:1) och allmänna råd om underrättelse om integritetsincidenter samt innehållet i förteckning över integritetsincidenter, gör PTS bedömningen att särskilda hänsyn behöver tas till att åtgärden är nödvändig för att efterleva de skyldigheter som följer av Sveriges anslutning till EU. Vidare gör PTS bedömningen upphävandet endast medför ringa konsekvenser. Föreskrifterna bör därför träda ikraft snarast.

PTS har redan information på sin webbplats om skyldigheterna att rapportera integritetsincidenter. Bland annat har PTS publicerat en vägledning som beskriver hur reglerna kan tillämpas. Denna information har uppdaterats sedan ikraftträdandet av Kommissionens förordning (EU) nr 611/2013. Eftersom upphävandet av PTS föreskrifter och allmänna råd bedöms medföra endast ringa konsekvenser, gör PTS bedömningen att några ytterligare informationsinsatser inte är nödvändiga.

## **7 Förslagets betydelse för företag**

Som beskrivits ovan gör PTS bedömningen att upphävande av PTS föreskrifter (PTSFS 2012:1) och allmänna råd om underrättelse om integritetsincidenter samt innehållet i förteckning över integritetsincidenter, endast medför ringa konsekvenser. Regleringen bedöms inte heller få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Konsekvensutredningen innehåller därför inte någon närmare beskrivning av sådana effekter.

## **8 Underrättelse för anmälan till Europeiska kommissionen**

Det föreskrivs i 6 § förordningen (1994:2029) om tekniska regler att en myndighet som avser fatta beslut om en teknisk regel i god tid ska underrätta Kommerskollegium om det förslag som den har utarbetat. Bestämmelserna i förordningen ansluter till Sveriges internationella förpliktelser enligt bl.a. Europaparlamentets och rådets direktiv 98/34/EG av den 22 juni 1998, ändrat genom Europaparlamentets och rådets direktiv 98/48/EG, om ett informationsförfarande beträffande tekniska standarder och föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

Enligt PTS bedömning är nu föreslagna föreskrifter inte att se som sådana tekniska regler som ska underrättas enligt nämnda förordning.

## 9 Kontaktpersoner

*Rättsliga frågor:*

Sofie Sandell

[sofie.sandell@pts.se](mailto:sofie.sandell@pts.se)

08-678 56 19

*Sakfrågor:*

Staffan Lindmark

[staffan.lindmark@pts.se](mailto:staffan.lindmark@pts.se)

08-678 57 36

## BILAGA 1 Förslag till föreskrifter

### Post- och telestyrelsens författningssamling

Utgivare: Karolina Asp, Post- och telestyrelsen, Box 5398, 102 49 Stockholm  
ISSN 1400-187X



---

**Föreskrifter om upphävande av Post- och telestyrelsens föreskrifter (PTSFS 2012:1) och allmänna råd om underrättelse om integritetsincidenter samt innehållet i förteckning över integritetsincidenter; beslutade den 10 juni 2014.**

**PTSFS ÅR:NR**

Utkom från trycket  
den XX 2014

Med stöd av 34 b § förordningen (2003:396) om elektronisk kommunikation föreskriver Post- och telestyrelsen att Post- och telestyrelsens föreskrifter (PTSFS 2012:1) och allmänna råd om underrättelse om integritetsincidenter samt innehållet i förteckning över integritetsincidenter ska upphöra att gälla vid utgången av augusti 2014.

---

På Post- och telestyrelsens vägnar

GÖRAN MARBY

Karolina Asp

## **BILAGA 2**

### **Begreppen ”integritetsincident” och ”personuppgiftsbrott”**

I denna bilaga beskrivs närmare hur begreppen ”integritetsincident” och ”personuppgiftsbrott” förhåller sig till varandra. Begreppsskillnaden har betydelse för analys av konsekvenserna vid ett upphävande av PTS föreskrifter och allmänna råd om underrättelse om integritetsincidenter samt innehållet i förteckning över integritetsincidenter (PTSFS 2012:1).

#### **Begreppet personuppgiftsbrott i EU-rätten**

Direktiv 2002/58/EG avser att reglera skyddet av integritet och konfidentialitet inom sektorn elektronisk kommunikation. I artikel 1.2 anges:

*”Bestämmelserna i detta direktiv skall precisera och komplettera direktiv 95/46/EG för de ändamål som avses i punkt 1. Bestämmelserna är vidare avsedda att skydda berättigade intressen för de abonnenter som är juridiska personer.”*

Artikel 4 i direktivet avser säkerhet i samband med behandlingen av uppgifter och i vart fall bestämmelserna i punkterna 1 och 2, som uppställer krav på att vidta säkerhetsåtgärder respektive att upplysa abonnenterna om vissa säkerhetsrisker, torde gälla de elektroniska kommunikationstjänsterna i sin helhet, innefattande samtliga uppgifter som behandlas i samband med tillhandahållande av tjänsterna.

I artikel 4.3 i direktiv 2002/58/EG anges emellertid att tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, utan onödigt dröjsmål, ska anmäla s.k. personuppgiftsbrott till den behöriga nationella myndigheten. Enligt artikel 2 avses med detta begrepp

*”ett brott mot säkerhetsbestämmelserna som leder till oavsiktlig eller olaglig utplåning, förlust, ändring, otillåtet avslöjande eller åtkomst av personuppgifter som överförs, lagras eller på annat sätt behandlas i samband med tillhandahållandet av allmänt tillgänglig elektronisk kommunikationstjänst inom gemenskapen.”*

Med personuppgift avses enligt samma bestämmelse, jämförd med artikel 2 i direktiv 95/46/EG,

*”varje upplysning som avser en identifierad eller identifierbar fysisk person (den registrerade). En identifierbar person är en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet”.*

Kommissionens förordning (EU) nr 611/2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation, är beslutad med stöd av artikel 4 i direktivet. Det innebär således att reglerna i Kommissionens förordning endast avser händelser som berör uppgifter avseende fysiska personer.

### **Begreppet integritetsincident i svensk rätt**

Reglerna i 6 kap. 4 a § LEK, och därmed även PTS föreskrifter och allmänna råd till dessa bestämmelser, omfattar istället s.k. integritetsincidenter, med vilket enligt 6 kap. 1 § LEK avses

*”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”.*

Avsikten med de ovan nämnda reglerna i svensk rätt är att genomföra direktiv 2002/58/EG. Enligt förarbetena bygger definitionen av integritetsincident på definitionen av personuppgiftsbrott. Anledningen till att den svenska lagstiftaren valde ett annat begrepp var främst att undvika intrycket av att en brottslig handling åsyftas samt att det är olämpligt att använda begreppet personuppgifter, eftersom bestämmelserna i 6 kap. LEK genomgående handlar om alla typer av behandlade uppgifter. Vidare anges: ”Definitionen omfattar inte bara avsiktliga säkerhetsintrång utan varje händelse, oavsett orsak, som leder till intrång. I många fall utgör de uppgifter som avses personuppgifter. Så är dock inte alltid fallet. Definitionen omfattar samtliga uppgifter som behandlas.”<sup>5</sup>

Att lagstiftaren valt att således ge begreppet integritetsincident en vidare betydelse än begreppet personuppgiftsbrott torde falla tillbaka på att reglerna i 6 kap. LEK, vilka till stora delar utgör genomförande av reglerna i direktiv 2002/58/EG, med ett fåtal undantag har utformats så att de gäller uppgifter om samtliga abonnenter och användare, oavsett om dessa är fysiska eller juridiska personer.

Lagstiftaren har markerat att det finns en koppling mellan kravet i 6 kap. 3 § LEK på att vidta säkerhetsåtgärder för att skydda behandlade uppgifter och skyldigheten att rapportera incidenter, genom att uttryckligen ange att säkerhetsåtgärderna ”ska vara ägnade att säkerställa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsincidenter”. 6 kap. 3 § LEK genomför artikel

---

<sup>5</sup> Se prop. 2010/11:115 ss 130-131, 181.



4.1 i direktivet, som inte heller den torde vara avgränsad till personuppgifter utan gäller generellt för ”säkerheten i [tjänstetillhandahållarens] tjänster”.

#### **Närmare om de uppgifter som omfattas av begreppen**

Både begreppet integritetsincident och begreppet personuppgiftsbrott är mycket omfattande, sett till de många olika händelser som ryms inom definitionerna. Som framgår ovan torde det dock vara så att begreppet integritetsincident är något vidare än begreppet personuppgiftsbrott, genom att det även inrymmer händelser som berör uppgifter som inte utgör personuppgifter.

Den yttre ramen för vilka slags uppgifter som kan anses omfattas av begreppen utgörs av det gemensamma rekvisitet att det ska röra sig om uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgänglig elektronisk kommunikationstjänst. Det torde främst röra sig om de uppgiftskategorier som på olika sätt omfattas av andra bestämmelser i LEK respektive direktivet, dvs. uppgifter om abonnemang, trafikuppgifter, lokaliseringsuppgifter samt innehåll i elektroniska meddelanden.

Med innehåll i elektroniska meddelanden avses den information som överförs mellan avsändare och mottagare, i de elektroniska kommunikationstjänsterna. Det kan till exempel röra sig om ljudet i ett telefonsamtal, brödtexten i ett e-postmeddelande eller innehållet på en webbplats som hämtas. Eftersom en stor del av kommunikationen sker mellan fysiska personer, torde en även stor andel av det innehåll som överförs direkt eller indirekt kunna härledas till fysiska personer och utgör därmed personuppgifter. I de fall kommunikationen sker helt utan mänsklig inblandning och inte alls berör personliga förhållanden, till exempel så kallad maskin-till-maskin-kommunikation, så torde innehållet dock inte utgöra personuppgifter.

Trafikuppgifter avser uppgifter som beskriver kommunikationen, t.ex. uppgifter om avsändare och mottagares adresser eller nummer, samt tidpunkter för när kommunikationen inleddes och avslutades. Adresser och nummer kan många gånger härledas till fysiska personer och utgör därmed personuppgifter. I den utsträckning uppgifterna endast kan härledas till en juridisk person faller de dock utanför personuppgiftsbegreppet.

Lokaliseringsuppgifter avser den geografiska positionen för terminalutrustningen för en användare. Även om det förekommer terminaler som inte används av någon fysisk person så torde den absoluta majoriteten av alla terminaler direkt eller indirekt kunna knytas till en fysisk person. I normalfallet torde därför även lokaliseringsuppgifter utgöra personuppgifter.

Uppgifter om abonnemang avser uppgifter av mer statisk karaktär om de som abonnerar på allmänt tillgängliga elektroniska kommunikationstjänster. Det kan till exempel röra sig om uppgifter som anger vem som innehar ett visst nummer eller en viss adress, samt uppgifter om dennes personnummer, postadress etc. Abonnenten är den som ingått avtal med tjänstetillhandahållaren och kan således vara såväl en fysisk som en juridisk person. I normalfallet torde endast uppgifter om abonnemang som innehas av fysiska personer utgöra personuppgifter.

#### **Den praktiska betydelsen av skillnaden mellan begreppen**

Som konstaterats ovan finns inom alla de aktuella kategorierna av uppgifter en delmängd som inte utgör personuppgifter. Händelser som enbart berör andra uppgifter kan utgöra integritetsincidenter men inte personuppgiftsbrott.

Som regel torde såväl personuppgifter som övriga uppgifter inom samma uppgiftskategori behandlas i samma system och enligt i stort sett samma rutiner. När det gäller mer omfattande händelser, som beror på till exempel bristande rutiner, fel i tekniska system eller antagonistiska angrepp, torde därför varje sådan händelse i normalfallet beröra ett större antal abonnenter och användare, och såväl personuppgifter som andra uppgifter. Därmed blir händelsen att betrakta som såväl en integritetsincident som ett personuppgiftsbrott.

När det gäller händelser som rör enskilda abonnenter, till exempel att en specificerad faktura skickas till fel adress eller att ett så kallat hemligt nummer lämnas ut till ett abonnentupplysningsföretag, torde däremot andelen integritetsincidenter som inte samtidigt utgör personuppgiftsbrott vara något större. Det torde då uteslutande röra sig om händelser som enbart berör uppgifter om abonnenter som är juridiska personer, och där inte några uppgifter om de personer som faktiskt använt den elektroniska kommunikationstjänsten inte förekommer. Ett av få exempel på detta kan vara att samtalsspecifikationen för ett företags växelanknytning lämnas ut till en obehörig mottagare.

Samtliga integritetsincidenter som hittills har rapporterats till PTS, utgör enligt myndighetens bedömning även personuppgiftsbrott. Även om antalet underrättelser ännu är för litet för att kunna dra några säkra slutsatser så tyder detta på att det endast är en mycket liten andel integritetsincidenter som inte också utgör personuppgiftsbrott. Den praktiska betydelsen av skillnaden mellan begreppen torde därför vara begränsad.