Post- och telestyrelsen arbetar för att alla i Sverige ska ha tillgång till bra telefoni, bredband och post.

Integritetsforum

Fredagen den 27 april 2018

Välkomna!

Agenda

- Förhandlingarna om förslaget till ny eprivacy-förordning
- EU:s dataskyddsförordning (GDPR) och LEK
- PTS rapport *Operatörernas hantering av användarnas uppgifter*
- PTS tillsynsarbete (avslutad, pågående och kommande tillsyn)
- Ev. föreskrift om lagring av trafikuppgifter (NAT)
- Övriga frågor?

Förhandlingarna om förslaget till eprivacy-förordning

- Information från Näringsdepartementet

EU:s dataskyddsförordning och LEK

Vad gäller from 25 maj 2018?

Allmänt om dataskyddsregleringen

- Översyn inom EU av de allmänna och sektorspecifika dataskyddsbestämmelserna
- Parallella förhandlingar med olika tidplaner
- GDPR är antaget och träder i kraft 25 maj 2018
- Förslaget till ny förordning om integritet och elektronisk kommunikation (eprivacy-förordning) förhandlas fortfarande

Vad gäller from 25 maj 2018?

- De allmänna bestämmelserna

- **GDPR träder i kraft**
- **Dataskyddsdirektivet samt PuL med tillhörande förordning och föreskrifter upphör att gälla**
- **Nya lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning träder i kraft**
- **DI ansvarig myndighet**

- De sektorspecifika bestämmelserna

- **Eprivacy-direktivet (2002/58/EG), LEK och EU-förordning 611/2013 fortsätter att gälla**
- **Förhandlingarna om eprivacy-förordningen fortsätter**
- **PTS ansvarig myndighet**

Förhållandet mellan regelverken

- Art 94 GDPR = hänvisningar till dataskyddsdirektivet ska anses vara hänvisningar till GDPR.
  (Eprivacy-direktivet kommer således att precisera och komplettera GDPR)

- Art 95 (och ingresspunkt 173) reglerar GDPRs förhållande till eprivacy-direktivet
  (GDPR ska inte innebära några ytterligare förpliktelser för fysiska eller juridiska personer som behandlar personuppgifter inom ramen för tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät i unionen, när det gäller områden inom vilka de redan omfattas av särskilda skyldigheter för samma ändamål i enlighet med eprivacy-direktivet)

- Eprivacy/LEK fortsatt tillämpligt när det gäller uppgifter som behandlas i samband med tillhandahållandet av elektroniska kommunikationstjänster

Ändringar i LEK

- 6 kap. 1 § = Begreppen behandling, personuppgiftsansvarig och samtycke har i kapitlet samma innebörd som i GDPR
- 6 kap. 2 § = Upplysning om var de allmänna dataskyddsbestämmelserna finns och att GDPRs bestämmelser om rättelse, radering, begränsning och skadestånd även gäller vid behandling av personuppgifter enligt denna lag.

Definitionen av begreppet samtycke

- Begreppet samtycke i LEK kommer att ha samma innebörd som i GDPR
- Artikel 4 (11) GDPR

  varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne
- Se även artikel 7 samt ingresspunkterna 32, 33, 42 och 43 GDPR

Samtycke – frivilligt

- Vid bedömning av huruvida samtycke är frivilligt ska största hänsyn bl.a. tas till huruvida ett avtal eller en tjänst har gjorts beroende av samtycke till sådan behandling av personuppgifter som inte är nödvändig för genomförandet av det avtalet (art 7.4)
- Samtycke är ej frivilligt om den registrerade inte har någon genuin eller fri valmöjlighet eller inte utan problem kan vägra eller ta tillbaka sitt samtycke (ingresspunkt 42)
- Samtycke är ej frivilligt om det inte medger att separata samtycken lämnas för olika behandlingar av personuppgifter eller om ett avtal/en tjänst är avhängigt av samtycket, trots att samtycket inte är nödvändigt för ett sådant genomförande (ingresspunkt 43)

Samtycke – specifikt

- Ändamålet med behandlingen måste specificeras

Samtycke – informerat

- Om den registrerades samtycke lämnas i en skriftlig förklaring som också rör andra frågor, ska begäran om samtycke läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Om en del av förklaringen innebär en överträdelse av denna förordning, ska denna del inte vara bindande (art 7.2)

- I synnerhet vid skriftliga förklaringar som rör andra frågor bör det finnas skyddsåtgärder som säkerställer att de registrerade är medvetna om att samtycke ges och om hur långt samtycket sträcker sig. En förklaring om samtycke som den personuppgiftsansvarige i förväg formulerat ska tillhandahållas i en begriplig och lätt tillgänglig form, med användning av ett klart och tydligt språk och utan oskäliga villkor. För att samtycket ska vara informerat bör den registrerade känna till åtminstone den personuppgiftsansvariges identitet och syftet med den behandling för vilken personuppgifterna är avsedda (ingresspunkt 42)

Samtycke – otvetydig viljeyttring

- Nyhet = genom ett uttalande eller genom en entydig bekräftande handling (art 4.11)
- Samtycke kan lämnas genom en skriftlig, inklusive elektronisk, eller muntlig förklaring. Detta kan inbegripa att en ruta kryssas i vid besök på en internetsida, genom val av inställningsalternativ för tjänster på informationssamhällets område eller genom någon annan förklaring eller något annat beteende som i sammanhanget tydligt visar att den registrerade godtar den avsedda behandlingen av sina personuppgifter. Tystnad, på förhand ikryssade rutor eller inaktivitet utgör inte samtycke. Samtycket bör gälla all behandling som utförs för samma ändamål. Om behandlingen tjänar flera olika syften, ska samtycke ges för samtliga syften. Om den registrerade ska lämna sitt samtycke efter en elektronisk begäran, måste denna vara tydlig och koncis och får inte onödigtvis störa användningen av den tjänst som den avser (ingresspunkt 32)

Samtycke – ytterligare villkor

- Bevisbördan på den registeransvarige (art 7.1 och ingresspunkt 42)
- Ett samtycke ska kunna återkallas. Det ska vara lika lätt att återkalla som att ge sitt samtycke (art 7.3)

Läs mer

- Artikel 29-gruppens vägledning
  Guidelines on consent under Regulation 2016/679
  WP259 rev.01
- Datainspektionens hemsida
  https://www.datainspektionen.se/

Incidentrapportering – till vilken myndighet?

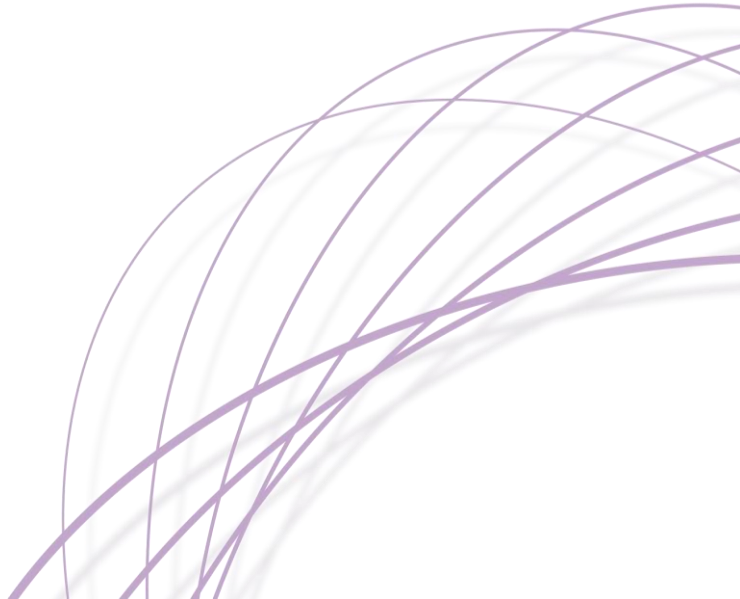
- Krav att rapportera incidenter både i den allmänna och sektorspecifika regleringen
- Olika ansvariga myndigheter, DI respektive PTS
- Artikel 95 GDPR
- LEK och EU-förordning 611/2013 fortsätter att gälla
  - Incidentrapportering till PTS som vanligt, dvs. gällande incidenter som rör uppgifter som behandlas i samband med tillhandahållandet av elektroniska kommunikationstjänster

Skillnader gällande incidentrapportering och underrättelser – några exempel

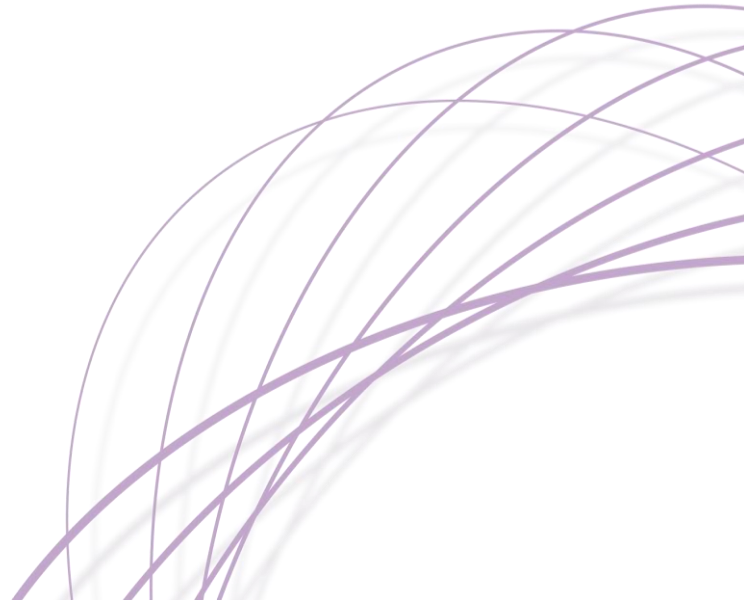
	Eprivacy	GDPR
När ska rapportering göras?	Inledande rapport senast efter 24h, kompletterande inom 3 dagar från inledande rapport	Inte senare än 72h
Undantag från rapportering?	Nej	Om osannolikt att incidenten medför risk för fri- och rättigheter
Vilka uppgifter ska ingå i rapport och underrättelse?	Fler uppgifter (t.ex. orsak och underrättelsers innehåll)	Färre uppgifter (mer fokus konsekvens)
När ska underrättelse göras?	Om incidenten kan antas inverka menligt på personuppgifter eller integritet	Om incidenten leder till en hög risk för fri- och rättigheter
Undantag från underrättelse?	Färre undantag	Fler undantag

Operatörernas hantering av användarnas uppgifter

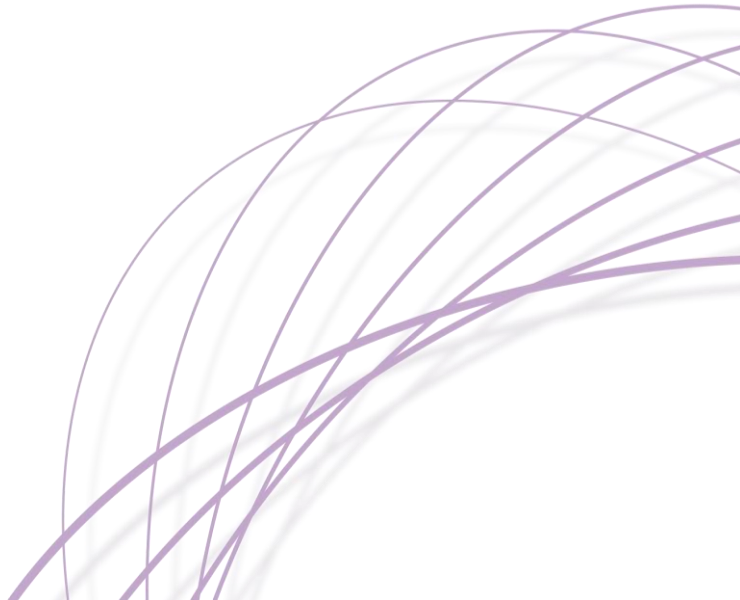
PTS rapport



PTS tillsynsarbete



Avslutad tillsyn



Slutsatser från Årlig tillsyn om

incidentrapportering samt vidtagna åtgärder sett till inträffade integritetsincidenter

Integritetsforum den 27 april 2018

Årlig tillsyn om incidentrapportering och vidtagna åtgärder

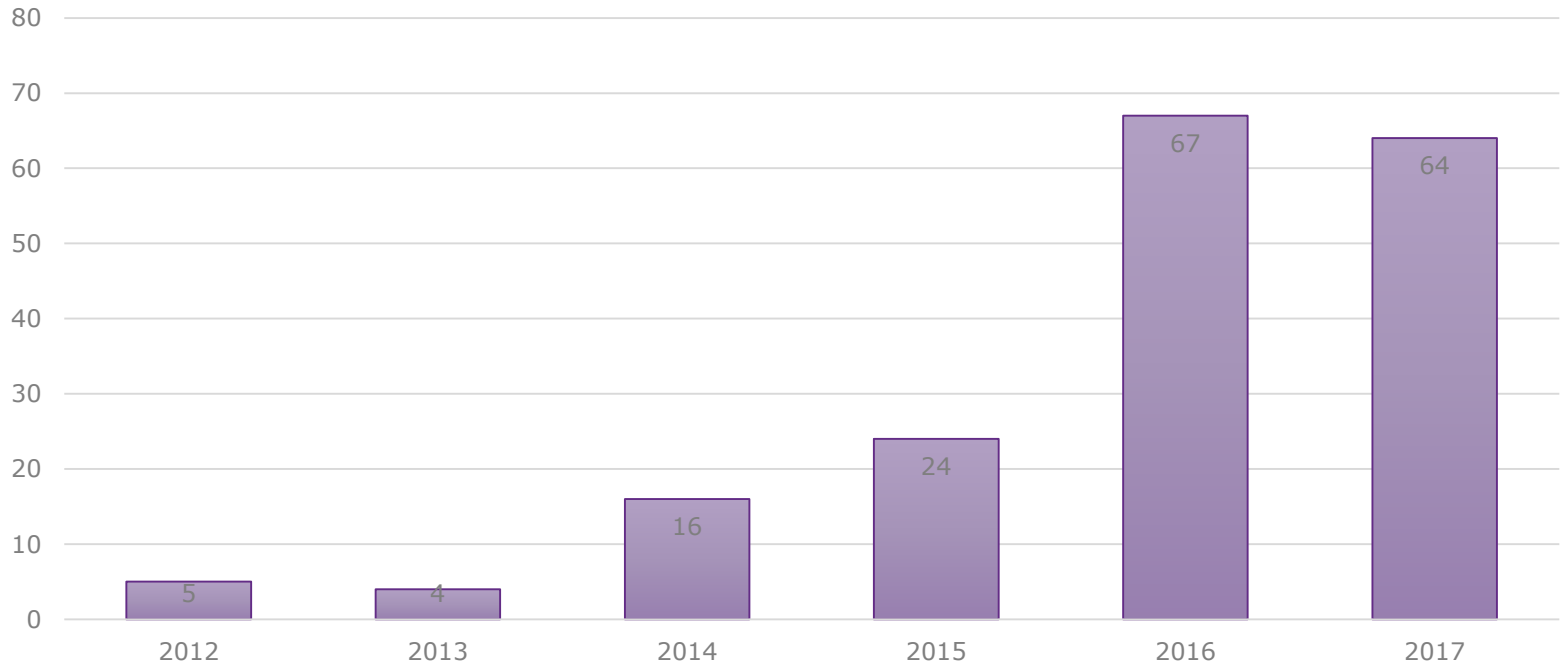
- Sjätte året som tillsynen genomförs
  - ➢ De fem största tillhandahållarnas incidentrapportering och vidtagna säkerhetsarbete med anledning av de inträffade integritetsincidenter.

  - Reglerna är inte nya -> hög förväntansbild på kännedom om och efterlevnad av gällande bestämmelser om incidentrapportering och vidtagande av skyddsåtgärder och bedrivande av säkerhetsarbete.

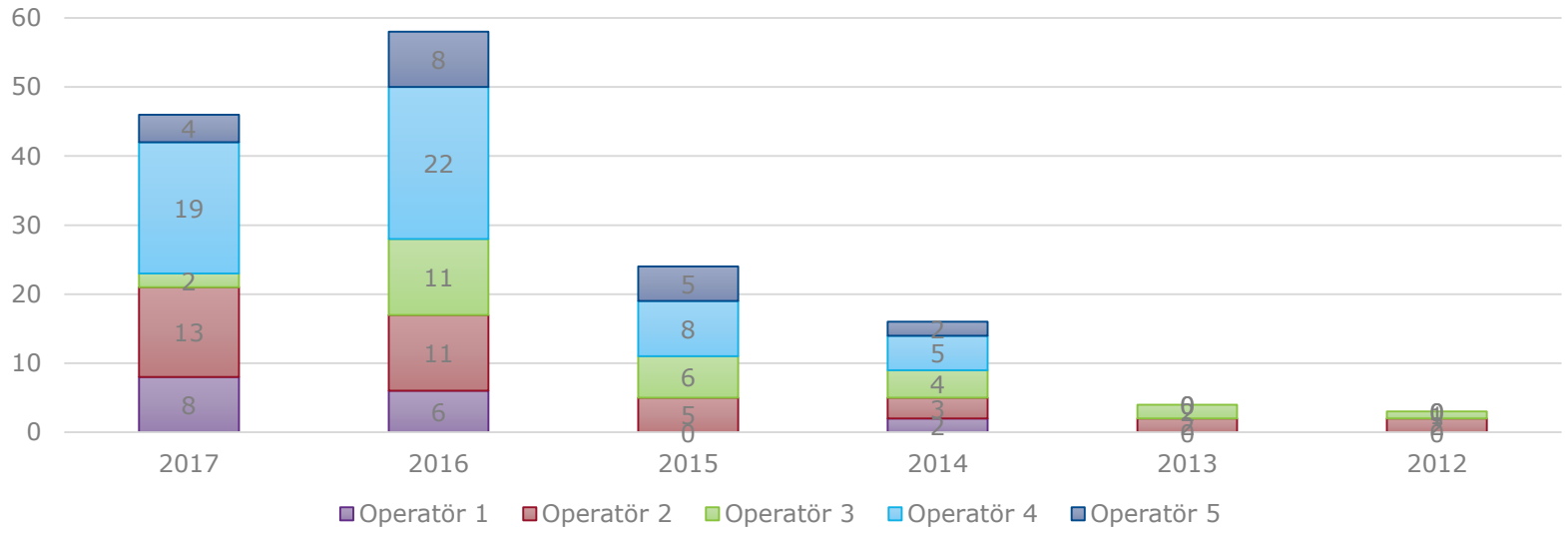
Slutsatser avseende regelefterlevnad av incidentrapporteringen

- Bättre på att rapportera integritetsincidenter –> bättre förmåga att internt upptäcka och rapportera integritetsincidenter
  - Rapporterar i tid (inledande och kompletterande rapport)
  - Förståeliga och tillräckliga beskrivningar om orsak, vidtagna kortsiktiga samt långsiktiga åtgärder överlag
  - Underrättar berörda abonnenter av drabbade integritetsincidenter i enlighet med gällande bestämmelser (per brev eller telefon)
  - Fler incidentrapporter inkommer till oss
- För löpande förteckning över inträffade integritetsincidenter

Utvecklingen av antalet rapporterade integritetsincidentrapporter till PTS



Utveckling antalet integritetsincidentrapporter per operatör



Exempel på vanligt inträffade integritetsincidenter

- Orderbekräftelse, fakturaspecifikation eller liknande skickas elektroniskt eller fysiskt till fel abonnent
- Avslöjande av abonnentuppgifter över telefon eller i butik till fel abonnent
- Uppgifter finns tillgängliga på internet

Vanliga orsaker bakom integritetsincidenter

- Webbtjänster ”Mina sidor”
  - T.ex. bristande säkerhet i sessionshantering
  - Sökmotorindexering
- Mänsklig faktor i kundtjänst, mellan kundtjänst och abonnent
  - Slarv (t.ex. hantering av handlingar – både manuellt, elektroniskt, felaktiga e-postadresser och telefonnummer)
  - Okunskap
  - Avsteg från fastställda rutiner
  - Bristande säkerställande av lämnande av korrekta uppgifter
  - Bristande it-stöd
- Tidigare vanlig orsak – hantering av uppgifter i butiksmiljö
  - Avsteg från fastställda rutiner (utlämnande av en annan abonnents uppgifter)

Exempel på vidtagna åtgärder och lärdomar

1. Genomförande av utbildningar till kundtjänstpersonal
    1. Introduktionsutbildningar för nyanställda
    2. E-learningutbildning tillgänglig på intranätet
    3. Återföring av erfarenheter till berörda efter inträffad incident
2. Översyn av riskanalysmodeller, mallar och rutiner (rutiner tillgängliga på skärmen)
3. Förtydligat samt utökat testning av egenframtagna webbtjänster
4. Utökad kravställning mot tredjepartsleverantörer av testning
5. Översyn av systemberoenden
6. Säkerställande av abonnentens identitet vid kontakt med kundtjänst
7. Utveckling av system och tekniska begränsningar för att motverka att personal kan frångå rutiner

Slutligen - operatörernas vidtagande av skyddsåtgärder

- Samtliga operatörer inom ramen för tillsynen har vidtagit lämpliga åtgärder mot bakgrund av de inträffade incidenterna.
- Inga uppenbara brister i tjänstetillhandahållarnas säkerhetsarbete har påträffats.
- Viktigt att ständigt dra lärdomar och beakta erfarenheter för att bedriva ett långsiktigt, kontinuerligt och systematiskt säkerhetsarbete.

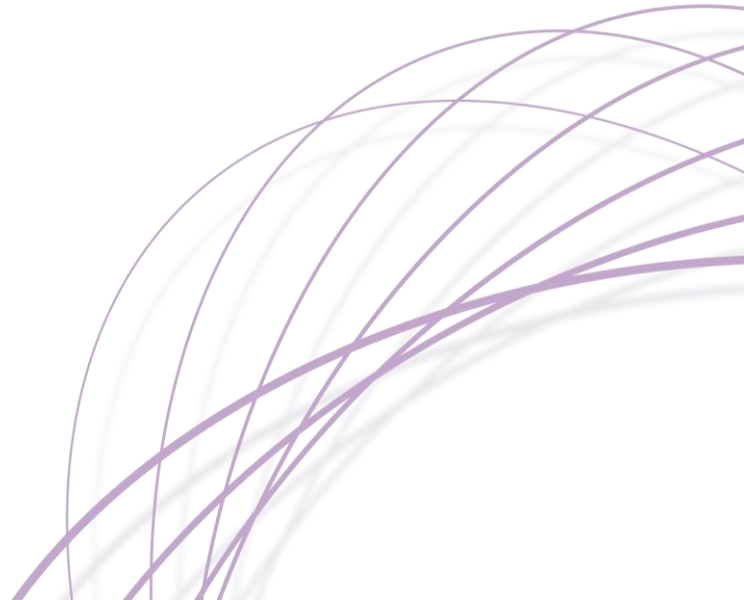
Tillsyn avseende behandling av trafikuppgifter

- särskilt gallring och lagring av sådana uppgifter

Tillsyn över skyddsåtgärder för behandlade uppgifter i kundtjänst

- Aktivering av SIM-kort i kundtjänst av obehörig person
- Åtgärder
  - Begränsning av behörighet
  - Införande av bank-ID
- Aktuella regelverk
  - 6 kap. 3 § LEK
  - PTS föreskrifter om skyddsåtgärder för behandlade uppgifter (2014:1)
- Lämplig teknisk och organisatorisk åtgärd att införa bank-ID
- Aktuell incident kan medföra allvarliga konsekvenser
- Kommande tillsyn kommer granska tillhandahållares rutiner och andra skyddsåtgärder i samband med kundtjänstkontakter

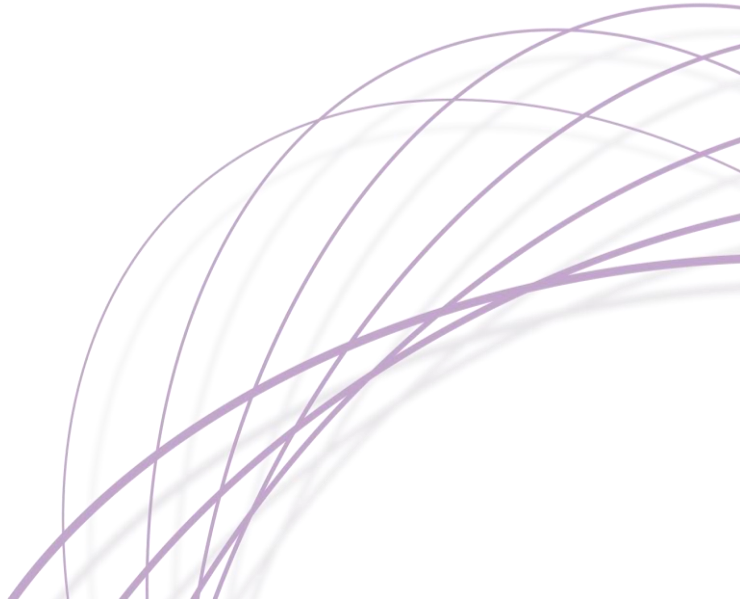
Pågående tillsyn



Pågående tillsynsaktiviteter

- Skyddsåtgärder gentemot underleverantörer
- Genomförande av riskanalyser för informationsbehandlingstillgångar
- Musikstreamingtjänst
- Förmågan att verkställa beslut om HAK/HÖK dygnet runt
- Förmågan att identifiera och internt rapportera integritetsincidenter
- Förmågan att upptäcka och hantera sårbarheter i SS7

Kommande tillsyn



Plan för PTS tillsyn avseende konfidentiell kommunikation 2018-2019

Integritetsforum

Tillsynsplan avseende konfidentiell kommunikation 2018-2019

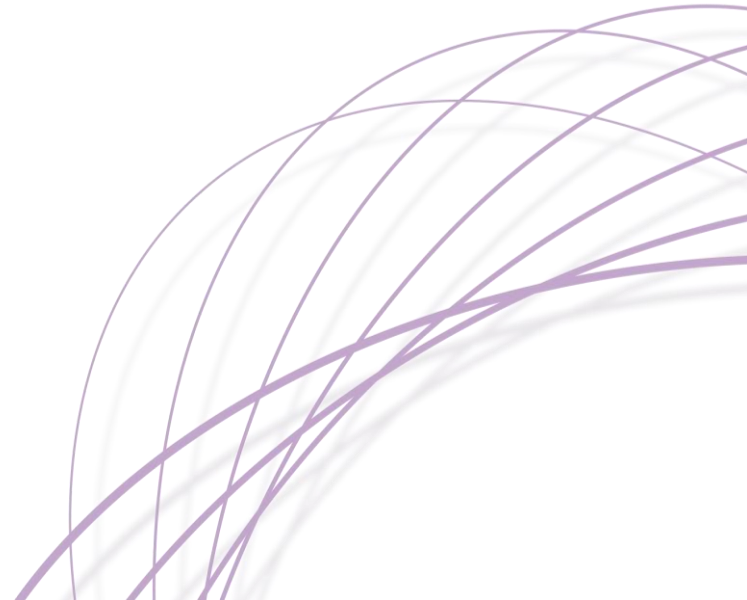
- Vi tar årligen fram en plan för vårt tillsynsarbete avseende konfidentiell kommunikation
- Planen beskriver inriktningen på vår tillsyn de två kommande åren
- Tillsynsplanen hittas här:

https://www.pts.se/sv/bransch/internet/integritet/tillsyn/

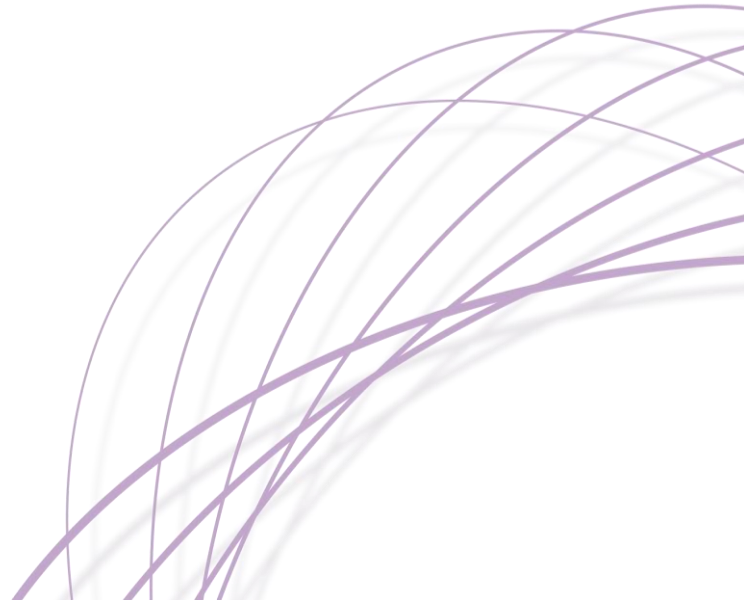
Fokusområden för tillsyn avseende säker och konfidentiell kommunikation 2018-2019

1. Årlig granskning och uppföljning incidentrapportering och vidtagande av åtgärder – de fem största tjänstetillhandahållarna
2. Små och medelstora tjänstetillhandahållares efterlevnad av krav på skyddsåtgärder och incidentrapportering
3. Skydd av information under överföring (fokus fram till nu på säkerhet i informationsbehandlingstillgångar)
4. Tjänstetillhandahållarnas genomförande av riskanalyser för sina informationsbehandlingstillgångar
5. Åtgärder för att säkerställa identitet och behörighet vid kontakt med kundtjänst

Eventuell föreskrift om lagring av trafikuppgifter (NAT)



Något övrigt?



Tack för idag!