| Datum | Vår referens | Aktbilaga |
|---|---|---|
| 2015-06-25 | Dnr: 15-4419 | 2 |

Nätsäkerhetsavdelningen
[redacted]

Telenor Sverige AB

# Årlig tillsyn rörande incidentrapportering och inträffade incidenter

## Saken

Årlig tillsyn rörande incidentrapportering och inträffade incidenter.

## Post- och telestyrelsens avgörande

Post- och telestyrelsen (PTS) avskriver ärendet från vidare handläggning.

## Bakgrund

PTS genomför årligen planlagda tillsyner över ett urval operatörer bland annat i syfte att dessa ska redogöra för inträffade incidenter under föregående år. Tillsynerna omfattar såväl driftstörningar som integritetsincidenter, vilka operatörerna är skyldiga att rapportera in till PTS.

Ett av huvudsyftena med inrapporteringsskyldigheten är att PTS ska kunna göra en bedömning av om det finns skäl att misstänka att bestämmelser i lagen (2003:389) om elektronisk kommunikation (LEK), t.ex. bestämmelsen om driftsäkerhet i 5 kap. 6 b § LEK, inte efterlevs. Även i de fall en incidentrapport till PTS inte ger upphov till direkta tillsynsåtgärder, kan incidentrapporten innehålla uppgifter som bidrar till myndighetens kunskap om vanliga orsaker till störningar och avbrott eller integritetsincidenter. Detta kan i sin tur utgöra underlag för PTS planlagda tillsynsinsatser och även bidra till myndighetens arbete med risk- och sårbarhetsanalyser för sektorn och till myndighetens arbete med robusthetshöjande åtgärder. Det är PTS avsikt att årligen genomföra planlagda tillsyner över utvalda operatörer rörande incidentrapportering och inträffade incidenter.

PTS inledde den 21 april 2015 den planlagda årliga tillsynen rörande incidentrapportering och inträffade incidenter över Telenor Sverige AB (Telenor).

Den 5 maj 2015 höll PTS ett tillsynsmöte med Telenor gällande rutiner för upptäckt och rapportering av integritetsincidenter, samt gällande föregående års inrapporterade integritetsincidenter.

Vid mötet redogjorde Telenor för sina rutiner för upptäckt av integritetsincidenter., och uppgav att man har ett övervakningssystem för att upptäcka incidenter, samt ett rapporteringssystem för incidenter. Integritetsincidenter kan även upptäckas direkt av personal eller rapporteras in av kunder, enligt Telenor.

Vid mötet redogjorde Telenor även för de tre integritetsincidenter som rapporterats in till PTS under föregående år. De två första incidenterna rörde att kunder kunnat se andra kunders uppgifter på ”Mina sidor”. Telenor uppgav vid mötet att man initialt inte hade kunnat säkerställa orsaken till incidenterna och man heller inte hade kunnat fastställa antalet drabbade kunder. Den tredje incidenten inträffade vid migrering av kunder från en annan operatör, vid vilken kunderna tillfördes epostadresser hos Telenor. På grund av fel i programvaran som producerade epostadresserna så kunde två personer som hade samma namn få del av epost från en annan person med samma namn. Det var, enligt Telenor tre kunder som drabbades av incidenten.

Telenor redogjorde vidare för sina underrättelser till berörda abonnenter och användare och för sina rutiner för inrapportering till PTS.

Inför mötet hade PTS efterfrågat en redogörelse för Telenors arbete med att genomföra riskanalyser för identifierade informationsbehandlingstillgångar i enlighet med PTS föreskrifter och allmänna råd om skydd av behandlade uppgifter (PTSFS 2014:1). Vid mötet presenterade Telenor hur operatören arbetar med riskanalyser på integritetsområdet.

Den 11 maj 2015 höll PTS ett tillsynsmöte med Telenor gällande inträffade driftsäkerhetsincidenter, totalt sju driftstörningar, vilka har rapporterats in till PTS under 2014 samt fram till och med februari 2015. Vid genomgången av incidenterna framkom bl.a. att 2014 inledningsvis varit ett lugnt år men att ett flertal ovanliga incidenter inträffat under slutat av året och dessa har även indirekt påverkat Telenors nätsamarbetspartner. Det omvända har även inträffat i ett fall varpå Telenor drabbades av en större störning som inträffade hos sin nätsamarbetspartner som indirekt berörde Telenors nät och tjänster. Telenor beskrev samarbetet som väl fungerande genom vilket man har bytt erfarenheter och delat processer vilket har varit till fördel för båda parter.

Telenor redogjorde även ingående för sitt riskanalysarbete på driftsäkerhetsområdet. Telenor beskrev vidare att det under 2014 har gjorts många förändringar, ett år som innehållit många projekt, bl.a. uppköp av verksamhet och migrering samt stabilisering. Trots en dubblering av antalet nattarbeten har verksamheten kunnat konstatera det lägsta antalet fel per månad. Det har varit ett lärorikt år som inneburit förändrade arbetssätt, nya processer och rutiner.

## Skäl

### Tillämpliga bestämmelser

PTS är enligt 2 § förordningen (2003:396) om elektronisk kommunikation tillsynsmyndighet enligt LEK. PTS ska enligt 7 kap. 1 § LEK utöva tillsyn över efterlevnaden av lagen och de beslut om skyldigheter eller villkor samt de föreskrifter som meddelats med stöd av lagen.

Enligt 6 kap. 3 § LEK ska den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas. Åtgärderna 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.

Av 6 kap. 4 a § första stycket LEK framgår att den som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster utan onödigt dröjsmål ska underrätta tillsynsmyndigheten om inträffade integritetsincidenter. Om incidenten kan antas inverka negativt på de abonnenter eller användare som de behandlade uppgifterna berör, eller om tillsynsmyndigheten begär det, ska även dessa underrättas utan onödigt dröjsmål. En integritetsincident definieras i 6 kap. 1 § LEK som 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

Av PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1) framgår bland annat följande:

Tjänstetillhandahållarens säkerhetsarbete avseende behandlade uppgifter ska enligt 3 § bedrivas långsiktigt, kontinuerligt och systematiskt och det ska finnas en tydlig rollfördelning med särskilt utpekade ansvariga. Rutiner, processer och rollfördelning ska dokumenteras.

Tjänstetillhandahållaren ska enligt 4 § bland annat identifiera informationsbehandlingstillgångar och föra en förteckning över dessa samt analysera riskerna för att integritetsincidenter inträffar för de identifierade informationsbehandlingstillgångarna. Vidtagna skyddsåtgärder samt tjänstetillhandahållarens bedömningar av lämplig nivå ska dokumenteras och följas upp årligen och vid behov.

Tjänstetillhandahållaren ska enligt 10 § ha dokumenterade rutiner för identifiering, intern rapportering, hantering och uppföljning av integritetsincidenter. Rutinerna ska säkerställa
1. att samtliga uppgifter i 11 § förs in i den förteckning som tjänstetillhandahållaren ska föra enligt 6 kap. 4 b § lagen (2003:389) om elektronisk kommunikation,
2. att inträffade integritetsincidenter och dess orsaker beaktas vid genomgång av riskanalyser i enlighet med 4 §, och
3. att skyddsåtgärder vidtas för att undvika liknande integritetsincidenter.

Av 5 kap. 6 b § LEK framgår bl.a. att den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikations-tjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet.

Av 5 kap. 6 c § första stycket LEK framgår att den som tillhandahåller ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst utan onödigt dröjsmål ska rapportera störningar eller avbrott av betydande omfattning till tillsynsmyndigheten.

Av PTS allmänna råd om god funktion och teknisk säkerhet (PTSFS 2007:2) framgår bl.a. vad en riskanalys bör innehålla och hur tillhandahållaren bör hantera risker för störningar och avbrott.

Av PTS föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning (PTSFS 2012:2) framgår bl.a. vilka störningar och avbrott som ska rapporteras samt hur rapporteringen ska gå till.

**PTS bedömning**

Inledningsvis kan PTS konstatera att Telenor under det föregående året har rapporterat in tre integritetsincidenter till PTS, vilket är en mer än året innan. Mot bakgrund av att definitionen av vad som utgör en integritetsincident är så vid bedömer PTS att det inte kan uteslutas att det inträffar integritetsincidenter i Telenors verksamhet som inte upptäcks och rapporteras till PTS. Telenor har dock ett system för upptäckt och ett system för intern rapportering av integritetsincidenter, vilket PTS ser positivt på. Arbetet med att säkerställa att processerna för upptäckt och intern rapportering också följs och uppdateras över

tid är ett kontinuerligt arbete som Telenor uppmanas att utveckla och förbättra, i syfte att bland annat öka möjligheten att upptäcka och rapportera integritetsincidenter till PTS. Med detta påpekande lämnar PTS denna del av tillsynen utan åtgärd.

När det gäller den första integritetsincidenten där kunder kunnat se andra kunders uppgifter på ”Mina sidor” kan PTS konstatera att det faktum att Telenor initialt inte lyckades utreda felorsaken till incidenten innebar att felet kunde inträffa igen vid ett senare tillfälle och därmed orsaka den andra integritetsincidenten. PTS bedömer att incidenterna kan tyda på brister i Telenors felsökningsrutiner och rutiner för incidenthantering. Hade felorsaken och incidenthanteringen fungerar fullt ut vid den första incidenten bedömer PTS att den andra incidenten inte hade behövt inträffa. PTS uppmanar därför Telenor att följa upp sina rutiner för felsökning och incidenthantering för att säkerställa att felsökning och felavhjälpning i framtiden sker snabbare, i syfte att undvika att en incident blir långvarig eller riskerar att upprepas. Med denna uppmaning lämnar PTS denna del av tillsynen utan ytterligare åtgärd.

När det gäller den tredje incidenten gör PTS bedömningen att hanteringen av incidenten varit godtagbar men att underrättelsen till berörda abonnenter och användare inte fullt ut följt kraven enligt förordningen (se lista på vad underrättelserna ska innehålla i förordningens Bilaga 2). Telenor har i underrättelserna t.ex. inte tillräckligt utförligt beskrivit de berörda uppgifternas art och omfattning, vilka åtgärder som bolaget har vidtagit med anledning av incidenterna och har inte heller angett vilka, om några, åtgärder som de berörda abonnenterna och användarna kan vidta för att minska den negativa effekten av incidenterna. Utan utförligare information om vilka uppgifter som omfattas, vilka åtgärder som har vidtagits av Telenor eller kan vidtas av berörda abonnenter och användare kan de som drabbats inte fullt ut bedöma potentiella konsekvenser av incidenterna och vilka eventuella åtgärder som den enskilde kan vidta för att begränsa sin negativa påverkan. PTS förutsätter att Telenor vid kommande underrättelse ser till att samtlig information som måste inkluderas i underrättelserna skickas till berörda abonnenter och användare. Med detta lämnar PTS även denna del av tillsynen utan åtgärd.

När det gäller de störningar och avbrott som inträffat kan PTS konstatera att det varit fråga om ett flertal störningar, totalt sju stycken, dock ej av samma typ eller orsak och det föreligger heller inget samband mellan incidenterna. PTS finner det dock anmärkningsvärt att så många incidenter inträffat inom så kort tid och att merparten av incidenterna även indirekt drabbat Telenors nätsamarbetspartner. Även det omvända har i ett fall inträffat och i ett sådant fall, när orsakerna till incidenterna är hänförliga till en annan part, åligger det Telenor att se till att t.ex. erforderliga avtal och samarbeten finns på plats som säkerställer driftsäkerheten för Telenors nät och tjänster. En brist hos en underleverantör eller nätsamarbetspartner kan mycket väl utgöra en brist i det

grundläggande säkerhetsarbetet hos Telenor. PTS kan dock konstatera att det sedan tillsynsmötet inte inträffat några ytterligare incidenter som orsakats av Telenor eller dess nätsamarbetspartner, vilket skulle kunna tyda på att det inte föreligger några väsentliga brister i samarbetet. PTS kan dock komma att granska nätsamarbetet i kommande tillsyn för det fall att myndigheten skulle få ytterligare indikationer på att samarbetet inte fungerar tillräckligt bra för att Telenors verksamhet ska anses uppfylla rimliga krav på driftsäkerhet enligt 5 kap. 6 b § LEK. Därtill har även framkommit att orsakerna till incidenterna har varit ovanliga och vitt skilda till sin natur samt att Telenor har dragit lärdomar av samtliga inträffade incidenter vilket har lett till förbättrade processer och rutiner något som PTS ser positivt på. PTS lämnar med detta påpekande denna del av tillsynen utan ytterligare åtgärd.

När det gäller rapporteringen som sådan har PTS vid ett flertal tillfällen varit tvungen att begäran kompletterande uppgifter då rapporteringen varit kortfattad eller inte följt den mall för rapportering som PTS tagit fram mot bakgrund av vad som följer av de föreskrifter som finns om hur rapporteringen ska gå till. PTS förutsätter därför att Telenor förbättrar sina rutiner för incidentrapportering. Med denna uppmaning lämnar PTS även denna del av tillsynen utan ytterligare åtgärd.

Både på mötet gällande integritetsincidenter och mötet gällande driftsäkerhet redogjorde Telenor för sitt riskanalysarbete och sin riskhanteringsprocess. Såvitt framgått görs analyserna utifrån en närhetsprincip med fokus på risker, med en genomlysning på flera olika ledder istället för på respektive system, varigenom en risk kan påträffas flera gånger vilket minimerar risken för att en känd risk faller mellan stolarna. Detta arbete bedrivs regelbundet och kontinuerligt och en ny värdering av risker görs varje kvartal. Telenor har en s.k. riskbank och arbetar med generiska risker. Detta riskanalysarbete görs likadant för både driftsäkerhets- och integritetsrisker. Mot bakgrund av det krav som idag finns i 5 kap. 6 b § LEK att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet och vad en riskanalys bör omfatta bedömer PTS att det sätt på vilket Telenor bedriver sitt riskanalysarbete är tillfyllest vad gäller driftsäkerhetsaspekter.

Sedan den 1 september 2014 gäller nya föreskrifter om skyddsåtgärder för behandlade uppgifter enligt vilka riskerna för att integritetsincidenter inträffar ska analyseras för de identifierade informationsbehandlingstillgångarna. Någon sådan särskild analys har inte gjorts av Telenor och de har även uppgett att man har svårt att lyfta ut särskilda analyser avseende integritetsrisker på PTS förfrågan. Vad gäller riskanalysarbetet för integritetsincidenter har PTS därför svårt att ta ställning till om det sätt på vilket Telenor genomför analyserna fullt ut lever upp till kraven i de nya föreskrifterna om skyddsåtgärder för

behandlade uppgifter. PTS förutsätter att Telenor kommer att vidta de åtgärder som är nödvändiga för att efterleva skyldigheterna i föreskrifterna (PTSFS 2014:1). PTS kommer att följa upp att detta sker i en kommande planlagd tillsyn. Med detta påpekande lämnar PTS också denna del av tillsynen utan åtgärd i dagsläget.

Skäl att fortsätta den årliga tillsynen av incidentrapportering och inträffande störningar och avbrott av betydande omfattning föreligger inte, varför ärendet avskrivs från vidare handläggning.

## Underrättelse om överklagande

Beslutet kan inte överklagas.

---

Beslutet har fattats av enhetschefen Patrik Bystedt. I ärendets slutliga handläggning har även Anna Wibom, Karin Lodin, Peder Cristvall och Jeanette Kronwall (föredragande) deltagit.