Datum	Vår referens	Aktbilaga
2020-04-29	Dnr: 20-990	16

Avdelningen för säker kommunikation

Telenor Sverige AB

Beslut – årlig tillsyn

Saken

Tillsyn enligt 7 kap. 1 § första stycket lagen om elektronisk kommunikation (2003:389), LEK, över inrapporterade incidenter och rutiner för incidentrapportering.

Post- och telestyrelsens avgörande

Ärendet avskrivs.

Bakgrund

Post- och telestyrelsen (PTS) genomför årligen en planlagd tillsyn mot ett antal tillhandahållare av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster (tillhandahållare) för att granska och följa upp föregående års inträffade integritetsincidenter och störningar och avbrott av betydande omfattning, vilka tillhandahållarna är skyldiga att rapportera till PTS. I tillsynen granskas tillhandahållarnas arbete med att hantera, åtgärda och dra lärdomar av inträffade incidenter samt hur tillhandahållarnas rapportering av incidenter ser ut, mot bakgrund av reglerna i LEK med tillhörande föreskrifter och EU-förordning 611/2013[1]. Fokus i tillsynen ligger på uppföljning av tillhandahållarnas säkerhetsarbete mot bakgrund av de inträffade incidenterna.

De incidenter som behandlas i årlig tillsyn är de incidenter som inrapporterats till PTS sedan föregående års årliga tillsyn och som inte omfattas av någon an-

[1] Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott.

nan tidigare, pågående, planerad eller händelsestyrd tillsyn. För Telenor Sverige AB (Telenor) har följande ärenden granskats:

Typ	Telenors referensnr	PTS dnr
Drift	11761903	19-6361
	11904347	19-8037
	12509447	19-9810
Integritet	20190115 Ref: 55	19-456
	20190130 Ref: 60	19-1075
	20190219 Ref: 61	19-1713
	20190411 Ref: 69	19-4067
	20190411 Ref: 70	19-4364
	20190425 Ref: 71	19-4827
	20190514 Ref: 77	19-5821
	20190520 Ref: 79	19-6019
	20190605 Ref: 82	19-8647
	20190704 Ref: 89	19-8874
	20190709 Ref: 92	19-9064
	20190709 Ref: 93	19-9065
	20190605 Ref: 80	19-9146
	20190905 Ref: 99	19-10450
	20190919 Ref: 106	19-10939
	20190924 Ref: 108	19-11077
	20190918 Ref: 105	19-11233
	20191001 Ref: 112	19-11441
	20191202 Ref: 125	19-13283
	20191227 Ref: 130	19-13847

I incidentrapporterna har Telenor bl.a. beskrivit tidpunkterna för när incidenterna inträffade, upptäcktes och åtgärdades samt vilka omedelbara åtgärder som vidtagits för att mildra effekterna av incidenterna och för att förhindra att liknande incidenter ska inträffa igen.

När det gäller integritetsincidenterna har Telenor i flera fall gjort en åtskillnad mellan tidpunkten då händelsen uppdagades för bolaget – t.ex. då den rapporterades av en kund till kundtjänst – och tidpunkten då den blev ”klassad som en incident” av Telenor. I dessa fall har Telenor räknat med att incidenten ska rapporteras till PTS inom 24 timmar från det att händelsen klassades som en incident.

Inom ramen för den aktuella tillsynen har PTS begärt in en skriftlig redogörelse från Telenor avseende rapporterade incidenter, hur företaget säkerställer att incidenter rapporteras i enlighet med regelverket samt hur det säkerställs att relevanta åtgärder vidtas med anledning av de incidenter som inträffat. I Telenors svar beskrivs företagets processer, rutiner och organisation för hantering av driftstörningar och avbrott samt integritetsincidenter. Telenor beskriver även hur företaget arbetar för att säkerställa att tillämplig reglering efterlevs.

Skäl

Tillämpliga bestämmelser

Driftsäkerhet

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

Bestämmelsen förtydligas genom PTS föreskrifter om krav på driftsäkerhet, PTSFS 2015:2.

Enligt 3 § PTSFS 2015:2 ska tillhandahållarens driftsäkerhetsarbete bl.a. bedrivas långsiktigt, kontinuerligt och systematiskt. Arbetet ska omfatta såväl normala driftsförhållanden som extraordinära händelser. Tillhandahållaren ska i driftsäkerhetsarbetet ha en tydlig rollfördelning med särskilt utpekade ansvariga för arbetet.

Enligt 7 § PTSFS 2015:2 ska tillhandahållaren bl.a. säkerställa att 1. inträffade incidenter rapporteras internt, 2. åtgärder vidtas skyndsamt för att hantera en uppkommen incident, 3. åtgärder vidtas för att undvika liknande incidenter, och

4. att erfarenheter från inträffade incidenter beaktas vid genomförande av riskanalyser enligt 5 §.

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 föreskrifter och allmänna råd om rapportering av störningar eller avbrott av betydande omfattning (PTSFS 2012:2), som gällde vid tidpunkten då granskade incidenter rapporterades, framgår bl.a. vilka störningar och avbrott som ska rapporteras samt hur rapporteringen ska gå till. Regler om detta finns numera i PTSFS 2018:4.

Integritet

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. Den som tillhandahåller ett allmänt kommunikationsnät ska vidta de åtgärder som är nödvändiga för att upprätthålla detta skydd i nätet. 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.

Närmare bestämmelser om vilka tekniska och organisatoriska åtgärder som tjänstetillhandahållare ska vidta finns i PTS föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter.

Enligt 10 § PTSFS 2014:1 ska tjänstetillhandahållaren ha dokumenterade rutiner för identifiering, intern rapportering, hantering och uppföljning av integritetsincidenter. Rutinerna ska bl.a. säkerställa att skyddsåtgärder vidtas för att undvika liknande 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.

När och hur rapportering av integritetsincidenter ska ske och vad rapporterna ska innehålla framgår av Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott. Enligt

artikel 2.2 första stycket denna förordning ska anmälan ha inkommit till PTS senast 24 timmar efter att personuppgiftsbrottet upptäckts (eng. *detection*). Av tredje stycket samma artikel framgår att ett personuppgiftsbrott ska anses ha upptäckts om leverantören har varit tillräckligt medveten om att en säkerhetsincident har inträffat som ledde till att personuppgifter äventyrats, för att göra en anmälan i enlighet med förordningen.

Tillsyn

Enligt 7 kap. 1 § LEK ska tillsynsmyndigheten bl.a. ha tillsyn över efterlevnaden av lagen och de föreskrifter som har meddelats med stöd av lagen. Enligt 2 § förordningen (2003:396) om elektronisk kommunikation är PTS tillsynsmyndighet enligt LEK.

Enligt 7 kap. 4 § LEK ska tillsynsmyndigheten, om den finner skäl att misstänka att den som bedriver verksamhet enligt samma lag inte efterlever lagen eller de beslut om skyldigheter eller villkor eller de föreskrifter som har meddelats med stöd av lagen skar myndigheten underrätta den som bedriver verksamheten om detta förhållande och ge denne möjlighet att yttra sig inom skälig tid.

PTS bedömning

Rutiner för incidentrapportering

PTS konstaterar att Telenor har rapporterat in såväl drifts- som integritetsincidenter under det gångna året. Det underlag som Telenor inkommit med visar enligt PTS bedömning att Telenor har etablerade rutiner, utpekade personer och en organisation för såväl intern hantering som rapportering till PTS av integritetsincidenter samt störningar och avbrott av betydande omfattning.

Vad gäller tidpunkten för rapportering kan PTS konstatera att Telenor har rapporterat incidenter som gäller driftstörningar och avbrott i enlighet med tidsgränserna i PTSFS 2012:2.

I sin rapportering av integritetsincidenter anger Telenor i flera fall tidpunkter för upptäckt av incidenter med begrepp som saknar motsvarighet i aktuella regler. Ett exempel på detta är formuleringen ”klassad som integritetsincident”.

Beträffande tolkningen av begreppet ”upptäckt” i EU-förordningen konstaterar PTS följande. Det är givet att integritetsincidenter kan uppträda på vitt skilda sätt. Huruvida en incident har blivit upptäckt eller ej kan i vissa, mer komplicerade fall vara beroende av att en teknisk utredning av de bakomliggande orsakerna görs, men bör i andra fall inte vara avhängig en sådan.

Vidare kan tillhandahållarnas rapporteringsplikt enligt PTS bedömning inte anses beroende av hur tillhandahållarna organiserar sitt arbete, vare sig detta sker internt eller via underleverantörer. Tillhandahållarnas processer för att utreda och klassa händelser har alltså ingen direkt koppling till frågan om en incident har upptäckts eller inte.

PTS vill framhålla att syftet med regelverket i denna del bl.a. är att personer vars uppgifter otillbörligt röjts ska kunna vidta åtgärder med anledning av de eventuella negativa konsekvenser som detta kan innebära för dem. Med detta påpekande förutsätter PTS att Telenor framöver förtydligar sin rapportering på så sätt att det klart framgår när en incident upptäckts och att rapporterna görs inom föreskriven tid.

Vidtagande av skyddsåtgärder

Annat har inte framkommit genom de aktuella incidentrapporterna och den skriftliga information som lämnats inom ramen för tillsynsärendet än att Telenor har vidtagit skyddsåtgärder som är lämpliga för att hantera identifierade brister i enlighet med 5 kap. 6 § LEK och 7 § PTSFS 2015:2 samt 6 kap. 3 § LEK 10 § PTSFS 2014:1.

Sammanfattningsvis bedömer PTS att Telenor har förutsättning att framöver hantera incidenter och incidentrapporteringen i enlighet med regelverket och det finns därmed inte skäl att fortsätta tillsynen.

Ärendet avskrivs därför från vidare handläggning.

Beslutet har fattats av enhetschefen Anna Montelius. I ärendets slutliga handläggning har även Per Ekare (föredragande) deltagit.

PTS Beslutat av: Anna Montelius