Datum	Vår referens	Aktbilaga
2020-04-29	Dnr: 20-989	12

Avdelningen för säker kommunikation

Telia Company 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.

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 annan tidigare, pågående, planerad eller händelsestyrd tillsyn.

Hur reglerna om rapportering av incidenter efterlevs av Telia Company AB (Telia), mot bakgrund av LEK med tillhörande föreskrifter och EU-förordning

611/2013[1], har under året varit föremål för PTS tillsyn i annat ärende, varför den frågan har fallit utanför ramen för förevarande ärende.

För Telia har följande ärenden granskats särskilt:

Telias referens	PTS referens
SDI 8659	19-3694
SDI 8843	19-5906
SDI 9449	19-10860
SDI 9544	19-11416
PDB SE OP-907259	19-5249
PDB SE OP-1008507	19-6034
PDB SE OP-1008586	19-6406
PDB SE OP-1031429	19-7653
PDB SE OP-1040158	19-7933
PDB SE OP-1045395	19-8257
PDB SE OP-1630224	19-13234
PDB SE OP-1667751	19-13570
PDB SE OP-1675751	19-13728
PDB SE OP-1535427	19-12318
PDB SE OP-1589553	19-12960

Därutöver det har ett antal rapporterade incidenter med liknande grundorsaker granskats övergripande.

PDB SE OP-939592	19-5466
PDB SE OP-1006297	19-7592
PDB SE OP-1038704	19-7652
PDB SE OP-1504281	19-12296
PDB SE OP-1380740	19-11464
PDB SE OP-1222691	19-9011
PDB SE OP-1151026	19-9088
PDB SE OP-1335844	19-10740

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

PDB SE OP-1335831	19-10887
PDB SE OP-1364802	19-10935
PDB SE OP-1357588	19-11133
PDB SE OP-1399766	19-11580
PDB SE OP-1419214	19-11581
PDB SE OP-1456533	19-11833
PDB SE OP-1456538	19-11834
PDB SE OP-1484238	19-11967
PDB SE OP-1573483	19-12984
PDB SE OP-1616820	19-13099

I incidentrapporterna ges en beskrivning av integritetsincidenterna eller driftstörningarna, vid vilka tidpunkter de inträffat och i förekommande fall vad de har fått för konsekvenser för slutanvändare. Vidare anges åtgärder som Telia vidtagit eller har för avsikt att vidta för att mildra effekterna av incidenterna och för att förhindra att liknande incidenter ska inträffa igen.

PTS har begärt in en skriftlig redogörelse för rapporterade incidenter som granskats särskilt. Avsikten har varit att, där så varit nödvändigt, klargöra orsakerna till incidenterna och huruvida vidtagna åtgärder har haft avsedd verkan eller om ytterligare åtgärder varit påkallade.

Telia har inkommit med svar på PTS frågor den 4 mars 2020 och vid tillsynsmöte den 10 mars 2020 redogjorde Telia utförligare för de särskilt behandlade incidenterna och även för sitt löpande arbete i övrigt för att motverka incidenter. De åtgärder som vidtagits hade enligt Telias bedömning antingen haft önskad effekt, kompletterats med ytterligare åtgärder eller inte föranlett några andra åtgärder än de redan vidtagna.

Det fortlöpande arbetet handlar framför allt om att motverka mänskliga fel, vilka kan vara svåra att komma till rätta med. Telia har uppgett att det pågår ett arbete med att byta äldre system mot ett system med bättre kundbild som enligt Telias bedömning motverkar mänskliga fel. Det gäller även sådana fel som kunderna riskerar att orsaka genom att förse Telia med felaktiga uppgifter. Telia arbetar också i forum för att upptäcka förbättringsmöjligheter.

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

Organisation för incidenthantering

PTS konstaterar att Telia har rapporterat in såväl driftstörningar som integritetsincidenter under det gångna året. De underlag som Telia inkommit med och vad som framkommit vid mötet den 10 mars 2020 visar enligt PTS bedömning att Telia 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.

Vidtagande av skyddsåtgärder

När det gäller de incidenter som PTS har granskat särskilt framgår det att Telia har vidtagit åtgärder i syfte att avhjälpa problemen.

I samband med att incidenter upptäcks görs även en genomgång av aktuell rutin för att se om det finns någon brist. Särskilt vid ofta förekommande fel ses systemen över för att se om det är något som behöver förbättras i dem.

Annat har inte framkommit genom de aktuella incidentrapporterna och den ytterligare skriftliga och muntliga information som lämnats inom ramen för tillsynsärendet än att Telia har vidtagit skyddsåtgärder som är lämpliga för att avhjälpa och 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 Telia har förutsättning att framöver hantera incidenter 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 Björn Andersson (föredragande) deltagit.