Datum	Vår referens	Aktbilaga
2019-06-24	Dnr: 19-1559	44

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 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

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

annan tidigare, pågående, planerad eller händelsestyrd tillsyn. För Telia Company AB (Telia) har följande ärenden granskats:

Typ av incident	PTS diarienummer	Telias referensnummer
Integritet (integritetsincident-rapporterna)	18-3691	18-04-00047
	18-4421	2018-04-00173
	18-4982	18-04-00235
	18-6712	18-05-00165
	18-7199	2018-05-00259
	18-8128	2018-06-00197
	18-8593	Telia-2018-06-00301
	18-9155	18-07-00248
	18-11809	18-10-00172
Driftstörningar och avbrott (driftsincident-rapporterna)	18-1805	SDI 6844
	18-2452	TO 160603
	18-6555	SDI 7168
	18-8160	SDI 7370
	18-9314	SDI 7525
	18-11146	SDI 7761
	18-16714	SDI 7967

I tillsynen har PTS begärt in skriftlig redogörelse från Telia avseende 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 Telias svar beskrivs företagets processer, rutiner och organisation för hantering av driftstörningar och avbrott samt integritets-incidenter. Telia beskriver även hur företaget arbetar för att säkerställa att tillämplig reglering efterlevs.

Vidare genomfördes den 25 mars 2019 ett tillsynsmöte med representanter från Telia. Vid mötet behandlades driftsincidentrapporterna.

Telia har i samtliga rapporter beskrivit vad som inträffat vid störningarna och avbrotten, vilka åtgärder som vidtagits för att omedelbart åtgärda störningen eller avbrottet och vilka åtgärder som vidtagits för att förhindra att liknande incidenter inträffar. På mötet lämnade Telia fördjupade förklaringar och beskrivningar i dessa delar.

Avsikten var att även integritetsincidentrapporterna skulle behandlas vid mötet den 25 mars 2019. De personer från Telia som närvarade på mötet saknade dock djupare kunskap om integritetsincidenterna än det som framgår av integritetsincidentrapporterna.

På mötet framkom även att Telia fann gränsdragningen mellan vad som är rapporteringspliktigt enligt LEK och vad som är rapporteringspliktigt enligt den allmänna dataskyddsförordningen (GDPR)[2] svår. Telia berättade att Telia efter GDPR:s ikraftträdande rapporterat vissa incidenter till Datainspektionen, istället för, så som innan GDPR:s ikraftträdande, till PTS.

PTS meddelade Telia den 26 mars 2019 att företaget inte på ett tillfredställande sätt kunnat redogöra för integritetsincidentrapporterna vid mötet den 25 mars. PTS kallade därför den 16 april 2019 Telia till ett uppföljande möte den 25 april 2019.

Efter mötet den 25 mars 2019 förde PTS och Telia en dialog rörande de incidenter som företaget rapporterat till Datainspektionen. Dialogen resulterade i att Telia inkom med ytterligare sju rapporter rörande incidenter upptäckta mellan 9 juli 2018 och 19 februari 2019. PTS meddelade Telia att även dessa rapporter skulle behandlas på det uppföljande mötet. Utöver integritetsincident-rapporterna nämnda ovan behandlades därmed på det uppföljande mötet även följande rapporter:

Typ av incident	**PTS diarienummer**	**Telias referensnummer**
Integritet (de kompletterande integritetsincident-rapporterna)	19-4500	OP-523044
	19-4501	OP-684390
	19-4502	OP-718459
	19-4590	07-00133
	19-4591	GSOC2018-10-0047
	19-4592	OP-712911
	19-4593	OP-611645

Telia har vid ifyllande av den mall som bolaget använt för att lämna in integritetsincidentrapporterna till PTS i fältet ”Date and time of incident (if kown; where necessary an estimate can be made), and of detection of incident” angivit flera olika tidpunkter med beskrivningar som ”First noticed”, ”Confirmed as personal data breach”, och ”was the incident confirmed”. I rapporterna har Telia uppgivit orsaken till incidenten, och i de fall där orsaken inte kunna identifieras vid tiden för rapportering, kompletterat rapporterna med sådan information på mötet. I enstaka fall har Telia uppgett att bolaget inte kunnat fastställa orsaken till incidenten.

[2] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

I rapporterna har Telia beskrivit vilka omedelbara åtgärder som vidtagits för att mildra effekterna av incidenterna samt vilka åtgärder som vidtagits för att förhindra att liknande incidenter ska inträffa igen. På mötet ställde PTS uppföljande frågor avseende dessa åtgärder, vilka besvarades med kompletterande och fördjupande redogörelser från Telia.

Skäl

Tillämpliga bestämmelser

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.

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 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 Telia har rapporterat in såväl drifts- som integritets-incidenter under det gångna året. Det underlag som Telia inkommit med och den information som framkommit vid mötena 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.

Under handläggningen av ärendet har det dock framkommit att Telia, efter GDPR:s ikraftträdande den 25 maj 2018 gjort en ny tolkning av skyldigheten att rapportera integritetsincidenter och rapporterat vissa incidenter till Datainspektion istället för till PTS. Då incidenterna rört uppgifter som behandlas i samband med tillhandahållande av en allmänt tillgänglig elektronisk kommunikationstjänst ska sådana incidenter rapporteras till PTS. PTS kan alltså konstatera att Telia vad det gäller dessa incidenter inte rapporterat dem i enlighet med bestämmelserna i 6 kap. 4 a § LEK. Efter uppmaning från PTS har Telia i efterhand inkommit med dessa incidentrapporter. PTS finner det anmärkningsvärt att Telia inte efterfrågat PTS ställningstagande innan företaget upphörde att rapportera sådana incidenter som Telia tidigare inkommit med till myndigheten. PTS gör dock bedömningen att Telia framöver kommer att rapportera till berörd myndighet i enlighet med gällande regler. Det finns därför inte någon anledning att fortsätta granskningen i denna del.

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

Om Telia rapporterar integritetsincidenter inom de tidsfrister som uppställs i gällande reglering är inte helt klart. I sin rapportering anger Telia flera tid-punkter för upptäckt av incidenter, med begrepp som saknar koppling till aktuella regler. För flera av de incidenter som integritetsrapporterna avser är det därför otydligt om rapporterna inkommit till PTS inom föreskriven tidsram.

Enligt artikel 2.2 första stycket kommissionens förordning (EU) 611/2013 ska anmälan ha inkommit till PTS senast 24 timmar efter att personuppgiftsbrottet upptäckts (eng. *detection*). Av tredje stycket samma artikel framgår att ett person-uppgiftsbrott ska anses upptäckts om leverantören har varit tillräckligt med-veten om att en säkerhetsincident har inträffat som ledde till att personupp-gifter äventyrats, för att göra en anmälan i enlighet med denna förordning.

Vad Telia avser med t.ex. ”first noticed” och ”confirmed as personal data breach” och hur begreppen förhåller sig till kommissionens förordning har ej tydliggjorts av Telia. PTS kan därför för vissa av integritetsincidentrapporterna, inte klart fastställa huruvida Telia inkommit med rapporterna i tid. 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 eventuella negativa konsekvenser detta kan innebära för dem. Med detta påpekande förutsätter PTS att Telia framöver förtydligar sin rapportering på så sätt att det klart framgår när en incident upptäckts och att rapporterna görs inom föreskriven tid.

Telias förberedelser inför tillsynmöte

Vid det inledande tillsynsmötet den 25 mars 2019 var Telia påfallande oförberett och kunde varken redogöra för samtliga inträffade incidenter eller på ett tillfredställande sätt besvara PTS frågor. Detta trots att det klart framgått av möteskallelsen vad mötet skulle behandla samt att årlig tillsyn genomförts enligt samma koncept vid ett flertal tillfällen tidigare. Då mötet inte gav det underlag som behövdes för ärendets handläggning fann PTS det nödvändigt att kalla till ett uppföljande möte för att återigen gå igenom samtliga incidenter. Telia står under tillsyn av PTS och ska bl.a. lämna de uppgifter som myndigheten behöver för att granska Telias verksamhet. Att på tillsynsmöte alltid delta med rätt personer med fullständig information och kunskap ser PTS som en förutsättning för att Telias organisation ska anses arbeta långsiktigt, kontinuerligt och systematiskt med säkerhetsarbetet, samt utgör en förutsättning för att tillsynen ska kunna bedrivas effektivt.

Vid det uppföljande mötet närvarade personer med relevant kompetens och Telia hade förberett information om incidenterna som behandlades. PTS förutsätter att Telia framöver kommer att vara väl förberedda vid kommande tillsynsmöten med PTS.

Vidtagande av skyddsåtgärder

Av det som framkommit i de rapporter som Telia lämnat till PTS som omfattas av denna tillsyn samt den information som lämnats av Telia skriftligen och vid tillsynsmöten har det dock inte framkommit annat än att Telia vidtagit åtgärder som framstår som lämpliga skyddsåtgärder i enlighet med 5 kap. 6 § LEK och 7 § PTSFS 2015:2 samt 6 kap. 3 § LEK 10 § PTSFS 2014:1 för att hantera identifierade brister. Telia har vidare uppgett att de har för avsikt att organisationen ska lära och förbättras utifrån de erfarenheter som dragits av inträffade incidenter.

Sammanfattningsvis bedömer PTS att Telia 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 t.f. enhetschefen Anna Montelius. I ärendets slutliga handläggning har även Björn Hesthamar, Caroline Sundholm och Linus Kilander (föredragande) deltagit.