Datum 2017-02-01

Vår referens Dnr: 16-7626

Nätsäkerhetsavdelningen

[redacted]

Telia Company AB

Tillsyn över dokumentation av informationsbehandlingstillgångar

Saken

Tillsyn över dokumentation av informationsbehandlingstillgångar.

Post- och telestyrelsens avgörande

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

Bakgrund

Tillhandahållare av elektroniska kommunikationstjänster är skyldiga att skydda abonnenters och användares integritet i samband med tillhandahållande av tjänsterna. PTS har tagit fram föreskrifter och allmänna råd (PTSFS 2014:1) som närmare anger vilka krav på skyddsåtgärder som gäller för operatörer när dessa behandlar uppgifter.

De skyddsåtgärder som föreskrivs förutsätter att operatören först har identifierat och dokumenterat de system, databaser och fysiska tillgångar som används för informationsbehandling (s.k. informationsbehandlingstillgångar). Att ha en aktuell och samlad bild över samtliga informationsbehandlings-tillgångar underlättar för operatören att vidta de skyddsåtgärder som krävs, samt andra relevanta åtgärder för att upprätthålla en hög skyddsnivå och följa upp säkerheten för de behandlade uppgifterna över tid.

Krav på identifiering och dokumentation av informationsbehandlingstillgångar har gällt sedan den 1 september 2014. Mot bakgrund av uppgifter som har lämnats till PTS i olika tillsynsärenden har PTS dock misstänkt att flera operatörer ännu inte efterlevt kraven.

Mot bakgrund av detta inledde PTS tillsyn över bl.a. Telia Company AB (Telia) i syfte att granska operatörens efterlevnad av reglerna.

Den 7 september 2016 hölls ett möte med Telia vid vilket de tillämpliga reglerna diskuterades och Telia bl.a. presenterade sin förteckning över informationsbehandlingstillgångar, samt hur operatören arbetar med att hålla förteckningen löpande uppdaterad. Telia skickade även in ett utdrag ur förteckningen till PTS.

Vid mötet framförde Telia bl.a. att man hade tolkat begreppet ”uppgifter som behandlas i samband med tillhandahållandet av tjänsten” såsom innefattandes endast trafikuppgifter och lokaliseringsuppgifter, och inte uppgiftskategorierna *abonnentuppgifter* och *uppgifter i ett elektroniskt meddelande* (innehåll).
Efter påpekande från PTS om detta åtog sig Telia att komplettera sin förteckning med dessa kategorier.

Efter att myndigheten genomfört tillsynsmöte med samtliga tillsynsobjekt som omfattats av tillsynen kunde PTS konstatera att det återkommande hade förelegat vissa generella brister hos tillsynsobjekten. Dessa brister var främst relaterade till tolkningen av vissa för tillsynen relevanta begrepp, såsom just begreppet ”informationsbehandlingstillgång”.

I januari 2017 inkom Telia med ett nytt utdrag ur sin förteckning. Telia har även skriftligen bekräftat att operatören delar PTS syn på de aktuella begreppen, samt att man nu i övrigt efterlever reglerna för dokumentation av informationsbehandlingstillgångar.

Skäl

Tillämpliga bestämmelser

Enligt 6 kap. 3 § lagen (2003:389) om elektronisk kommunikation (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. Enligt 2 § PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1) definieras ”behandlade uppgifter” som uppgifter som behandlas i samband med tillhandahållande av tjänsten enligt 6 kap. 3 § LEK.

Enligt föreskrifternas 3 § ska tjänstetillhandahållarens säkerhetsarbete avseende behandlade uppgifter bedrivas långsiktigt, kontinuerligt och systematiskt. I säkerhetsarbetet ska det finnas en tydlig rollfördelning med särskilt utpekade ansvariga. Rutiner, processer och rollfördelning för säkerhetsarbetet ska dokumenteras.

Enligt 4 § ska tjänstetillhandahållaren identifiera informationsbehandlings-tillgångar där behandlade uppgifter förekommer och föra en förteckning över dessa. Tjänstetillhandahållaren ska i sitt säkerhetsarbete årligen och vid behov följa upp att förteckningen är aktuell.

PTS är enligt 2 § förordningen (2003:396) om elektronisk kommunikation tillsynsmyndighet enligt LEK. Tillsynsmyndigheten ska enligt 7 kap. 1 § LEK utöva tillsyn över bland annat efterlevnaden av lagen.

PTS bedömning

Telia har skriftligen och vid möte med PTS redogjort för operatörens arbete med dokumentation av informationsbehandlingstillgångar. Vid tillsynsmötet redogjorde även PTS för hur myndigheten ser på vissa för tillsynen relevanta begrepp, i syfte att säkerställa att PTS och Telia hade samsyn gällande innebörden av begreppen. Efter att PTS genomfört tillsynsmöten med alla operatörer som omfattats av tillsynen kunde myndigheten konstatera att det förelåg fyra generella brister, främst avseende hur operatörer tolkade vissa för tillsynen relevanta begrepp. PTS gör gällande dessa brister följande bedömningar.

Begreppet ”informationsbehandlingstillgång”

PTS kan konstatera att definitionen i föreskrifterna av ”informationsbehandlingstillgång” är mycket vid i och med att den innefattar samtliga system, databaser och fysiska tillgångar som används för informationsbehandling.

PTS kan vidare konstatera att de flesta operatörer har inkluderat system och databaser i sin förteckning, men att man saknat dokumentation av fysiska tillgångar, alternativt att man endast dokumenterat kundplacerad utrustning.

Alla fysiska tillgångar som används för informationsbehandling, dvs. behandlar uppgifter, ska dokumenteras. Som exempel på fysiska tillgångar som typiskt sett behandlar uppgifter för t.ex. en mobiloperatör kan anges routrar, switchar, DSLAM, BNC, RNC, HLR, servrar, aktiva fysiska förbindelser och media converters.

Till stöd för bedömningen av vilka tillgångar som omfattas bör operatören, enligt PTS bedömning, utreda vilka tillgångar som skulle kunna drabbas av en integritetsincident, genom att t.ex. ställa sig frågan om den fysiska tillgången på något sätt, oavsiktligt eller otillåtet, kan vara föremål för utplåning, förlust, ändring, avslöjande eller åtkomst till behandlade uppgifter.

Begreppet ”uppgifter som behandlas i samband med tillhandahållandet av tjänsten”

Det andra begreppet där flera operatörer inte har haft samma tolkning som PTS är ”uppgifter som behandlas i samband med tillhandahållandet av tjänsten”. Begreppet återfinns både i föreskrifterna och i 6 kap. 3 § LEK.

Det finns, enligt PTS bedömning, ingen begränsning i de tillämpliga reglerna avseende vilka uppgifter som omfattas av begreppet, utan i vart fall samtliga uppgiftskategorier som omnämns i 6 kap. LEK omfattas. Dessa kategorier utgörs åtminstone av

- uppgifter i ett elektroniskt meddelande (innehåll) (t.ex. 6 kap. 17 § LEK),
- uppgifter om abonnemang (6 kap. 20 § LEK),
- lokaliseringsuppgifter (t.ex. 6 kap. 9 § LEK) och
- trafikuppgifter (t.ex. 6 kap. 5 § LEK).

Den kategori som PTS genom tillsynen har kunnat konstatera att operatörer generellt har haft okunskap rörande har varit ”uppgifter i elektroniskt meddelanden”, dvs. meddelandens innehåll. Enligt PTS bedömning utgör denna kategori ofta den mest integritetskänsliga av de kategorier som omfattas av uttrycket ”uppgifter som behandlas vid tillhandahållandet av tjänsten”.

Det PTS inom ramen för tillsynen vidare har konstaterat är att många av operatörerna i sin förteckning endast har angett en kategori av uppgifter och att den ofta har kallats ”personuppgifter”. Även om t.ex. trafikuppgifter mycket väl kan utgöra personuppgifter skyddas i LEK inte bara personuppgifter utan även t.ex. uppgifter om företag och själva konfidentialiteten i kommunikationen, oavsett om den går att härleda till en viss person eller inte.

Även i de fall operatören benämnt uppgifterna för t.ex. ”kunduppgifter” och med det avsett att även t.ex. företag inkluderas, så är en sådan omfattande kategorisering, enligt PTS bedömning, inte tillräckligt specificerad för ändamålet. PTS är av uppfattningen att det är lämpligt att operatören i t.ex. sin förteckning över informationsbehandlingstillgångar tydligt anger vilken typ av uppgifter som varje tillgång behandlar, bl.a. eftersom dessa uppgifter utgör en del av den information som operatören ska beakta vid genomförande av analys

av riskerna och för att kunna vidta ändamålsenliga skyddsåtgärder för tillgången.

Vilken information förteckning ska innehålla

Inom ramen för tillsynen har även omfattats granskning av vilken information som en godtagbar förteckning åtminstone bör innehålla.

PTS gör härvid bedömningen att, även om föreskrifterna inte innehåller några specifika krav på förteckningens innehåll, förteckningen bör vara ändamålsenlig för de efterföljande kraven i föreskrifterna. Förteckningen bör således kunna användas som underlag till de riskanalyser som ska genomföras för samtliga informationsbehandlingstillgångar, samt för de skyddsåtgärder som ska vidtas efter riskanalyserna. Enligt PTS bedömning är det mot bakgrund av detta lämpligt att i sin förteckning inkludera information om

- vilken eller vilka uppgifter som en specifik tillgång behandlar,
- namn på tillgången och dess funktion,
- placering (fysiska tillgångar),
- vem som ansvarar för den, samt
- en hänvisning till den riskanalys, eller de riskanalyser, som genomförts för tillgången.

Att hålla förteckningen löpande uppdaterad

Slutligen har PTS kunnat konstatera att det i flera fall har förelegat vissa tveksamheter gällande hur ofta förteckningen över informationsbehandlingstillgångar uppdateras. Flera operatörer har uppgivit att detta sker årligen inom ramen för en befintlig process. Kravet i föreskrifterna är dock att förteckningen, utöver årlig revision, ska ses över ”vid behov”.

Även om flera operatörer har uppgivit att man även ser över förteckningen vid anskaffning av nya tillgångar eller vid avveckling, har det förekommit att operatörer har saknat en process som säkerställer att förteckningen även uppdateras t.ex. vid förändringar av befintliga tillgångar.

Efterlevnad av Telia

Efter att PTS har delgivit Telia sin syn på tolkningen och tillämpningen av de relevanta begreppen och reglerna, har Telia kompletterat sin förteckning och därefter också skriftligen bekräftat att operatören följer PTS tolkningar avseende de aktuella begreppen, samt att man uppdaterar sin förteckning årligen och vid behov.

Utifrån de övriga uppgifter som inkommit från Telia och det utdrag ur förteckningen av informationsbehandlingstillgångar som insänts till myndigheten bedömer PTS att Telia efterlever reglerna för identifiering och dokumentation över informationsbehandlingstillgångar.

Skäl att fortsätta den aktuella tillsynen föreligger därför inte, varför ärendet avskrivs från vidare handläggning.

Beslutet har fattats av enhetschefen Staffan Lindmark. I ärendets slutliga handläggning har även juristen Karin Lodin (föredragande) deltagit.

.