Datum 2017-04-20

Vår referens Dnr: 17-1231

Nätsäkerhetsavdelningen

[redacted]

Com Hem AB

Årlig tillsyn av incidentrapportering och inträffade integritetsincidenter – Com Hem AB

Saken

Årlig tillsyn av incidentrapportering och inträffade integritetsincidenter.

Post- och telestyrelsens avgörande

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

Bakgrund

PTS genomför årligen en planlagd tillsyn mot ett antal operatörer för att granska och följa upp föregående års inträffade integritetsincidenter, vilka operatörerna är skyldiga att rapportera till PTS. I tillsynen granskas operatörernas arbete med att identifiera, hantera, åtgärda och dra lärdomar av inträffade incidenter mot bakgrund av reglerna om skydd av behandlade uppgifter i lagen (2003:389) om elektronisk kommunikation (LEK). Dessutom granskas hur operatörerna följer reglerna om rapportering av de inträffade incidenterna.

Ett av huvudsyftena med inrapporteringsskyldigheten är att PTS ska kunna göra en bedömning av om det finns skäl att misstänka att bestämmelser i LEK, t.ex. bestämmelsen om skydd av behandlade uppgifter i 6 kap. 3 § 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 integritetsincidenter. Detta kan i sin tur utgöra underlag för PTS planlagda tillsynsinsatser.

Post- och telestyrelsen

Postadress: Box 5398 102 49 Stockholm

Besöksadress: Valhallavägen 117 A www.pts.se

Telefon: 08-678 55 00 Telefax: 08-678 55 05 pts@pts.se

Com Hem AB (Com Hem) är en av de operatörer som omfattas av den aktuella tillsynen. PTS inledde tillsyn mot Com Hem den 14 februari 2017 och höll ett tillsynsmöte med bolaget den 22 mars 2017. Com Hem har även inkommit med skriftliga upplysningar.

Vid tillsynsmötet beskrev Com Hem sina rutiner för rapportering av integritetsincidenter samt hur bolaget identifierar och hanterar dessa. Com Hem informerade även att bolaget fortlöpande utbildar personalen i hur uppgifter får hanteras samt hur incidenter identifieras och ska hanteras. Vidare presenterade Com Hem sin förteckning över integritetsincidenter samt redogjorde för de fyra incidenter[1] som rapporterats in till PTS under föregående år och vilka åtgärder som vidtagits med anledning av dessa.

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. 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 6 kap. 4 a § LEK ska den som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster utan onödigt dröjsmål underrätta tillsynsmyndigheten om 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 ska ske framgår av Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott.

Av PTS föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter (PTSFS 2014:1) framgår bl.a. följande.

[1] Com Hem har rapporterat en femte incident till PTS men då den inte ansågs utgöra en sådan incident som ska omfattas av den årliga tillsynen är den undantagen.

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 för hantering av riskerna 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.

Enligt 6 kap. 4 b § LEK ska tjänstetillhandahållaren löpande föra en förteckning över integritetsincidenter. Vad förteckningen närmare ska innehålla framgår av 11 § PTSFS 2014:1.

PTS bedömning

Com Hems redogörelser har gett en god bild av de inträffade incidenterna och de åtgärder som vidtagits med anledning av dessa.

PTS kan konstatera att Com Hems incidentrapporter och förteckningen över integritetsincidenter innehåller de uppgifter som krävs enligt gällande bestämmelser.

När det gäller föregående års inträffade integritetsincidenter har Com Hem rapporterat fyra stycken. Året dessförinnan rapporterade bolaget en integritetsincident och året före det rapporterades ingen incident. PTS ser visserligen positivt på Com Hems kontinuerliga arbete med att utbilda personal i att identifiera och hantera integritetsincidenter men bedömer ändå fortfarande att antalet rapporterade incidenter är lågt. PTS har för avsikt att inom kort inleda en särskild tillsyn rörande upptäckt och intern rapportering av integritetsincidenter. Com Hem kan komma att omfattas av den tillsynen.

Vidare noterar PTS att några incidenter rör brister hos Com Hems underleverantörer. PTS ser positivt på de åtgärder Com Hem vidtagit med anledning av incidenterna men vill understryka vikten av att kontinuerligt arbeta med tydlig kravställning gentemot underleverantörerna. Även detta är sådant som kan komma att omfattas av den ovan nämnda planerade tillsynen.

Skäl att fortsätta den årliga tillsynen av incidentrapportering och inträffade integritetsincidenter föreligger inte, varför ärendet avskrivs från vidare handläggning.

Beslutet har fattats av enhetschefen Staffan Lindmark. I ärendets slutliga handläggning har även juristerna Anders Lindell, Anna Montelius och Camilla Östlund (föredragande) deltagit.