

**BESLUT**

|              |                     |             |
|--------------|---------------------|-------------|
| <b>Datum</b> | <b>Vår referens</b> | <b>Sida</b> |
| 2017-10-06   | Dnr: 16-11006       | 1(6)        |

Nätsäkerhetsavdelningen  
Telia Company AB  


Endast via e-post

## Tillsyn av åtgärder för skydd av behandlade uppgifter i butiks- och återförsäljarledet

### Saken

Tillsyn av åtgärder enligt 5 – 7 och 9 §§ PTSFS 2014:1 för skydd av behandlade uppgifter i butiks- och återförsäljarledet.

---

### Post- och Telestyrelsens beslut

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

### Bakgrund

Den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst (tjänstetillhandahållare) ska vidta lämpliga åtgärder för att säkerställa att de uppgifter som överförs, lagras eller på annat sätt behandlas i samband med tillhandahållandet av tjänsten skyddas. 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.<sup>1</sup>

Tjänstetillhandahållare är således skyldiga att analysera riskerna för att integritetsincidenter inträffar och utifrån dessa vidta nödvändiga åtgärder för att skydda behandlade uppgifter. För att säkerställa ett visst minimiskydd har PTS föreskrivit om ett antal grundläggande åtgärder som tjänstetillhandahållare åtminstone ska vidta.<sup>2</sup>

---

<sup>1</sup> 6 kap. 3 § lagen (2003:389) om elektronisk kommunikation (LEK).

<sup>2</sup> Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter.

---

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

Under 2015 och 2016 inträffade ett antal integritetsincidenter i butiks- och återförsäljarledet hos flera tillhandahållare av mobiltelefonitjänster. Till följd av detta beslutade PTS att inleda tillsyn mot de fyra största aktörerna som tillhandahåller dessa tjänster i egna butiker, hos återförsäljare eller bådadera för att granska deras åtgärder för skydd av behandlade uppgifter och om dessa åtgärder uppfyller föreskrivna krav.<sup>3</sup>

PTS beslutade att avgränsa tillsynen till en granskning av de grundläggande åtgärder som krävs enligt 5 – 7 och 9 §§ PTS föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter. De åtgärder som ska vidtas enligt dessa paragrafer avser åtkomsthantering, behörighetshantering, loggning och kryptering. Tjänstetillhandahållarnas eventuella ytterligare skyddsåtgärder – som krävs enligt 4 § PTSFS 2014:1 – faller således utanför tillsynen. PTS beslutade vidare att avgränsa tillsynen till att avse skyddsåtgärder för uppgifter som behandlas i tjänstetillhandahållarnas IT-system som används vid försäljning av mobiltelefonabonnemang i butiksmiljö (nedan kallat säljstödsystem). För varje tjänstetillhandahållare som ingick i tillsynen har PTS hållit möten och besökt en butik som antingen tillhört tjänstetillhandahållaren eller en återförsäljare.

Telia Company AB (Telia) är en av de tjänstetillhandahållare som omfattas av den aktuella tillsynen. PTS inledde tillsynen mot bolaget den 16 november 2016. PTS besökte Telia den 9 december 2016 i Stockholm och, tillsammans med representanter från Telia, en av återförsäljaren Mediamarkts butiker i Stockholm.

Telia har vid dessa besök redogjort för bolagets skyddsåtgärder och förevisat säljstödsystemet. PTS granskning av Telia åtgärder för skydd av uppgifter som behandlas i bolagets säljstödsystem baseras på de iakttagelser och de muntliga uppgifter som framkommit i samband med tillsynsbesöken.

#### *Iakttagelser och inhämtade uppgifter*

I Telias säljstödsystem behandlas vissa uppgifter, såsom kostnader och förbrukad datamängd, samt uppgift om abonnemang.

Telia ger säljare i egna butiker och hos återförsäljare behörighet till säljstödsystemet. Administrationen är delegerad, så att utpekade ansvariga hos återförsäljaren kan lägga till individuella säljare själv.

Personal i Telias egna butiker utbildas och upplyses om tystnadsplikten i samband med att behörigheten till säljstödsystemet tilldelas. Utöver det utbildas de löpande genom veckomöten och webbaserad utbildning. För återförsäljare

---

<sup>3</sup> 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.

framgår av avtalet med Telia att säljare ska utbildas och upplysas om tystnadsplikt för att få behörighet till säljstödsystemet.

Telia följer upp tilldelade behörigheter en gång i månaden och tar bort behörigheter i samband med att säljare avslutar sin anställning.

En säljare som har fått behörighet kan komma åt uppgifterna i säljstödsystemet genom de datorer som finns i butiken. Säljstödsystemets webbsida nås genom det krypterade protokollet HTTPS.

För att komma åt säljstödsystemet måste varje säljare logga in på ett eget konto med ett personligt användarnamn och lösenord. Vissa av återförsäljarnas butiker är utrustade med Telias certifikat, som är unikt för varje återförsäljarnummer och är giltigt i två år. I dessa butiker räcker det att säljare anger det personliga användarnamnet och lösenordet för att komma åt säljstödsystemet. I övriga återförsäljarbutiker, som alltså saknar certifikat, måste säljare använda SMS-inloggning. Systemet kräver att lösenord byts var 90:e dag. Skulle ett konto inte ha använts under 60 dagar stängs det.

För Telias egna butiker finns en dokumenterad policy som innebär att personlig inloggning ska användas. Vid första mötestillfället var den dokumenterade policyn emellertid inte helt genomförd i praktiken. Samma inloggnings-id användes samtidigt av flera säljare för flera terminaler i ett antal Teliabutiker. Telia har efter mötestillfället inkommit med uppgift om att denna policy nu tillämpas i alla Telias egna butiker och att den kommer att följas upp.

I den besökta Mediamarkt-butiken är datorerna som är avsedda för abonnemangsförsäljning placerade i en avgränsad del av butiken. Skärmarna saknar insynsskydd.

Telia, såväl som den besökta Mediamarkt-butiken, har rutiner för att kunder alltid ska legitimera sig innan uppgifter hänförliga till kunden behandlas i säljstödsystemet. Systemet kräver dock inte tekniskt detta utan säljaren anger manuellt kundens mobil- och personnummer i systemet för att komma åt uppgifterna. Om mobil- och personnumret inte stämmer överens går det inte att komma åt uppgifterna.

Telia loggar uppgiftsbehandling som sker i säljstödsystemet. Månadsvisa rapporter utifrån loggarna kontrolleras och loggarna är utrustade med larm.

## **Skäl för beslutet**

### **Föreskrivna krav**

#### *Åtkomsthantering*

Enligt 5 § PTSFS 2014:1 ska tjänsteställhandahållaren säkerställa att åtkomst till behandlade uppgifter endast ges till den som

1. behöver det för att utföra sina arbetsuppgifter,

2. har relevant utbildning med hänsyn till de uppgifter denne hanterar,
3. har upplysts om tystnadsplikten i 6 kap. 20 – 21 §§ lagen (2003:389) om elektronisk kommunikation.

Enligt allmänna råd till 5 § bör en relevant utbildning innehålla information om när och hur behandlade uppgifter får hanteras, tecken på att en integritetsincident har inträffat, tänkbara konsekvenser av en inträffad integritetsincident för abonnenter och användare, hur rapportering av integritetsincidenter ska ske samt hur uppföljning av integritetsincidenter sker i organisationen.

#### *Behörighetshantering*

Enligt 6 § ska tjänstetillhandahållaren tilldela behörighet i enlighet med vad som föreskrivs i 5 §. Tjänstetillhandahållaren ska ha dokumenterade rutiner för tilldelning, ändring och uppföljning av behörigheter. Uppföljning av tilldelade behörigheter ska ske årligen. Tjänstetillhandahållaren ska ha system för identitets- och åtkomsthantering som säkerställer att åtkomst endast medges i enlighet med tilldelade behörigheter.

#### *Loggning*

Enligt 7 § ska tjänstetillhandahållaren dokumentera (logga) all läsning, kopiering, ändring och utplåning av behandlade uppgifter samt åtkomst till de system som används för behandling av sådana uppgifter. Loggning ska ske på ett sådant sätt att det går att se vem som har vidtagit vilken åtgärd med vilka uppgifter och vid vilken tidpunkt. Tjänstetillhandahållaren ska systematiskt och återkommande kontrollera loggarna. Kontrollerna får avgränsas till att omfatta utvalda behandlingar under begränsade tidsperioder, om kostnaderna för kontrollen motiverar en sådan avgränsning. Tjänstetillhandahållaren ska dokumentera genomförda kontroller av loggar. Vid misstanke om att en integritetsincident har inträffat ska relevanta loggar alltid kontrolleras. Tjänstetillhandahållaren ska ha dokumenterade rutiner för kontroll av loggar.

Enligt allmänna råd till 7 § bör kontroll av loggar ske med den periodicitet som är lämplig med hänsyn till verksamhetens omfattning, antalet personer med behörighet, hur behörigheterna tilldelas och hur omfattande kontrollen är.

#### *Kryptering*

Enligt 9 § ska behandlade uppgifter som överförs via internet skyddas genom kryptering. Detta gäller inte vid överföring till berörd abonnent eller användare om denne vid det enskilda tillfället har samtyckt till att överföringen sker utan kryptering. Kryptering ska ske med en allmänt erkänd krypteringsmetod med tillräcklig nyckellängd. Krypteringsnycklar ska hanteras på ett säkert sätt. Tjänstetillhandahållaren ska ha dokumenterade rutiner för kryptering och hantering av krypteringsnycklar.

### **PTS bedömning**

Telia är skyldigt att säkerställa att åtkomst till behandlade uppgifter endast ges till den som behöver det för att utföra sina arbetsuppgifter samt att kunna se vilken säljare som har vidtagit vilken åtgärd med vilken uppgift och vid vilken tidpunkt. För att säkerställa detta förutsätts det personlig inloggning. Telia uppger att detta nu är infört för säljstödsystemet i egna butiker. PTS lämnar denna del av tillsynen utan åtgärd men kan komma att följa upp att den policy som finns angående personlig inloggning faktiskt tillämpas.

Förbindelsen mellan webbläsaren och säljstödsystemet använder HTTPS vilket innebär att den är krypterad och därmed torde uppfylla kraven enligt 9 § PTSFS 2014:1, under förutsättning att nycklarna är tillräckligt långa och hanteras säkert samt att rutinerna för detta dokumenteras.

PTS vill även framhålla vikten av att fortlöpande arbeta med att säkerställa att endast behöriga får del av uppgifter i säljstödsystemet. Detta har både en intern och en extern dimension, dvs. det innefattar både att säljare endast kommer åt uppgifter om de kunder som de faktiskt betjänar och att obehöriga butiksbesökare inte ges åtkomst till behandlade uppgifter i säljstödsystemet. Det är Telia som är skyldigt att analysera riskerna för att integritetsincidenter inträffar och utifrån dessa vidta de åtgärder som är lämpliga för att hantera de identifierade riskerna. Riskanalyserna ska regelbundet följas upp och vid behov justeras, t.ex. i ljuset av incidenter som inträffar. Om analyserna visar att det finns risk för bedrägerier och att säljare bryter mot tystnadsplikten kan det därför finnas anledning att ytterligare begränsa åtkomsten till uppgifter i säljstödsystemet. T.ex. kan det finnas anledning att överväga om åtkomsten till uppgifter i säljstödsystemet bör begränsas så att det endast är möjligt att få åtkomst till kunduppgifter efter att systemet automatiskt läst av den aktuella kundens id-handling, och därmed ta bort möjligheten att manuellt ange en kunds personnummer och därmed få åtkomst till kunduppgifterna. Det kan även finnas anledning att överväga om ytterligare fysiska hinder, såsom insynsskydd på datorer, lösenordskyddad skärmläckning eller automatisk utloggning vid inaktivitet, skulle kunna vara åtgärder som i ytterligare utsträckning skulle kunna förhindra obehörig – och därmed otillåten – åtkomst till behandlade uppgifter.

Skäl att fortsätta tillsynen av avseende skyddsåtgärder för behandlade uppgifter i butiks- och återförsäljarledet finns inte, varför ärendet avskrivs från vidare handläggning.

---

Beslutet har fattats av enhetschefen Staffan Lindmark. I ärendets slutliga handläggning har även Camilla Östlund och Mikael Ejner (föredragande) deltagit.



Beslutat av: Staffan Lindmark