Post- och telestyrelsens författningssamling

Utgivare: Karolina Asp, Post- och telestyrelsen, Box 5398, 102 49 Stockholm
ISSN 1400-187X

Post- och telestyrelsens föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter;

PTSFS 2014:1

Utkom från trycket
den 28 februari 2014

beslutade den 18 februari 2014.

Med stöd av 34 a § och 34 b § andra stycket förordningen (2003:396) om elektronisk kommunikation föreskriver Post- och telestyrelsen följande och utfärdar följande allmänna råd.

Tillämpningsområde och definitioner

1 § Dessa föreskrifter och allmänna råd innehåller bestämmelser om lämpliga tekniska och organisatoriska skyddsåtgärder som den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta enligt 6 kap. 3 § lagen (2003:389) om elektronisk kommunikation. Föreskrifterna innehåller även bestämmelser om innehållet i en förteckning över integritetsincidenter enligt 6 kap. 4 b § samma lag.

2 § I dessa föreskrifter och allmänna råd avses med

Behandlade uppgifter: uppgifter som behandlas i samband med tillhandahållande av tjänsten enligt 6 kap. 3 § lagen (2003:389) om elektronisk kommunikation.

Informationsbehandlingstillgångar: system, databaser och fysiska tillgångar som används för informationsbehandling.

Tjänstetillhandahållare: aktör som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster.

Övergripande säkerhetsarbete

3 § Tjänstetillhandahållarens säkerhetsarbete avseende behandlade uppgifter ska 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.

4 § Tjänstetillhandahållaren ska 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.

Tjänstetillhandahållaren ska analysera riskerna för att integritetsincidenter inträffar för de identifierade informationsbehandlingstillgångarna. Riskanalyserna ska dokumenteras och följas upp årligen och vid behov.

Tjänstetillhandahållaren ska vidta de skyddsåtgärder som föreskrivs i 6-9 §§ samt andra nödvändiga skyddsåtgärder, på den nivå som är lämplig för att hantera de identifierade riskerna. Vidtagna skyddsåtgärder samt tjänstetillhandahållarens bedömningar av lämplig nivå ska dokumenteras och följas upp årligen och vid behov.

Allmänt råd

Tjänstetillhandahållarens vidtagna skyddsåtgärder bör följa etablerade standarder, normer och praxis.

Åtkomst- och behörighetshantering

5 § Tjänstetillhandahållaren ska 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.

Allmänt råd

En relevant utbildning bör 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,
- hur uppföljning av integritetsincidenter sker i organisationen.

6 § Tjänstetillhandahållaren ska 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

7 § Tjänstetillhandahållaren ska 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.

Allmänt råd

Kontroll av loggar bör ske med den periodicitet som är lämplig med hänsyn till verksamhetens omfattning, antalet personer med behörighet, hur behörigheterna tilldelas och hur omfattande kontrollen är.

Skydd mot utplåning och förlust

8 § Tjänstetillhandahållaren ska vidta åtgärder för att säkerställa att behandlade uppgifter som varaktigt lagras skyddas mot oavsiktlig eller otillåten utplåning eller förlust.

Informationsbehandlingstillgångar där behandlade uppgifter varaktigt lagras ska placeras i utrymmen som har skydd mot intrång.

Tjänstetillhandahållaren ska ha dokumenterade rutiner för placering av dessa informationsbehandlingstillgångar.

Allmänt råd

Säkerställande av skydd mot oavsiktlig eller otillåten utplåning eller förlust bör ske genom säkerhetskopiering. Återläsning av säkerhetskopior bör verifieras årligen.

Kryptering

9 § Behandlade uppgifter som överförs via internet ska 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.

Integritetsincidenter

10 § Tjänstetillhandahållaren ska 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.

11 § En förteckning över integritetsincidenter enligt 6 kap. 4 b § lagen (2003:389) om elektronisk kommunikation ska innehålla

1. datum då integritetsincidenten inträffade,
2. en beskrivning av integritetsincidenten,
3. uppskattat antal berörda abonnenter eller användare,
4. bedömda konsekvenser av integritetsincidenten,
5. orsak till att integritetsincidenten inträffade,
6. de åtgärder som vidtagits,
7. referensnummer.

Förteckningen ska hållas uppdaterad.

Denna författning träder i kraft den 1 september 2014.

På Post- och telestyrelsens vägnar

GÖRAN MARBY

Karolina Asp