Post- och telestyrelsens författningssamling

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

Post- och telestyrelsens föreskrifter och allmänna råd om skyddsåtgärder i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål;

PTSFS 2012:4

Utkom från trycket
den 6 november 2012

beslutade den 24 oktober 2012.

Med stöd av 37 § förordningen (2003:396) om elektronisk kommunikation föreskriver Post- och telestyrelsen följande och utfärdar följande allmänna råd.

Tillämpningsområde och definitioner

1 § Dessa föreskrifter innehåller bestämmelser om de särskilda tekniska och organisatoriska skyddsåtgärder som den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation ska vidta enligt 6 kap. 3 a § samma lag.

2 § I dessa föreskrifter avses med

Lagrade uppgifter: uppgifter som lagras för brottsbekämpande ändamål.

Lagringsskyldig: den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation.

Personal med särskild behörighet: person som genom säkerhetsprövning har bedömts vara lämplig att hantera lagrade uppgifter.

Tekniska och organisatoriska skyddsåtgärder

3 § Den lagringsskyldige ska bedriva ett kontinuerligt och systematiskt säkerhetsarbete med beaktande av de särskilda risker som lagringsskyldigheten medför. Säkerhetsarbetet ska följas upp regelbundet och innehålla åtminstone de åtgärder som framgår av 4-7 §§. Den lagringsskyldige ska ha rutiner och processer för att uppfylla kraven på skyddsåtgärder. Dessa rutiner och processer ska dokumenteras. Upprättade rutiner ska uppdateras vid förändringar som påverkar skyddet för de lagrade uppgifterna.

Allmänt råd

Den lagringsskyldige bör göra en riskanalys där de särskilda riskerna för den egna verksamheten identifieras.

De åtgärder som vidtas med anledning av skyldigheten i 3 § bör dokumenteras. Denna dokumentation bör behandlas konfidentiellt.

Personal som hanterar eller kommer i kontakt med lagrade uppgifter bör regelbundet få utbildning och information om vikten av att skyddsnivån upprätthålls.

Allt säkerhetsarbete som utförs bör kontrolleras, godkännas och följas upp av för detta ändamål särskilt utsedd personal inom organisationen.

Behörighet och åtkomst

4 § Den lagringsskyldige ska ha rutiner som säkerställer att endast personal med särskild behörighet har tillgång till lagrade uppgifter och de system som hanterar dessa uppgifter.

Allmänt råd

Den lagringsskyldige bör i en ansvarsbeskrivning fastställa personalens roller och ansvar i fråga om säkerhet för lagrade uppgifter. I ansvarsbeskrivningen bör det tydligt framgå att berörd personal har ansvar för att upprätthålla skyddet för de lagrade uppgifterna.

Den lagringsskyldige bör ha rutiner för säkerhetsprövning av personal som ska ges särskild behörighet. Säkerhetsprövningen bör grundas på den personliga kännedom som finns om den som ska prövas, uppgifter som framgår av betyg, intyg, referenser och liknande och sådana uppgifter som har framkommit vid en eventuell registerkontroll eller särskild personutredning.

Alla som hanterar lagrade uppgifter bör skriva under ett sekretessavtal. När någon annan än den lagringsskyldiges egen personal med behörighet utför reparation och service av till exempel it-utrustning bör ett avtal om säkerhet och sekretess ingås. Ett sådant avtal bör bland annat innehålla bestämmelser om vilka säkerhetsrutiner som ska tillämpas i dessa fall.

Den lagringsskyldige bör ha en behörighetshantering och behörighetskontroll för åtkomst till alla delar av system, utrustning och utrymmen som används för lagring av uppgifter. Utdelade behörigheter bör revideras kontinuerligt så att endast de som behöver ha tillgång till de lagrade uppgifterna har sådan behörighet.

Fysiskt skydd

5 § Utrustning som används för att lagra uppgifter ska placeras i ett utrymme som har skydd mot elavbrott, brand, översvämning och obehörigt tillträde för att förhindra förlust och otillåten tillgång till lagrade uppgifter.

Behandlingshistorik (logg)

6 § All behandling av lagrade uppgifter ska dokumenteras (så kallad loggning). Loggning ska ske på ett sådant sätt att det går att se vem som har haft tillgång till vilka uppgifter och vid vilken tidpunkt. Den lagringsskyldige ska säkerställa att personal som har haft tillgång till lagrade uppgifter inte ges tillgång till behandlingshistoriken.

Behandlingshistoriken ska användas för att genomföra regelbunden och systematisk uppföljning och kontroll. Detta ska ske innan uppgifterna utplånas enligt 6 kap. 16 d § lagen (2003:389) om elektronisk kommunikation. Därefter ska behandlingshistoriken utplånas.

Behandlingshistoriken ska skyddas genom kryptering under lagring och överföring. Kryptering ska ske med en allmänt erkänd krypteringsmetod med tillräcklig nyckellängd.

Krypteringsnycklar ska hanteras på ett säkert sätt.

Säkerhetskopiering

7 § Lagrade uppgifter och behandlingshistorik enligt 6 § ska säkerhetskopieras tillräckligt ofta för att säkerställa att uppgifterna skyddas mot oavsiktlig eller otillåten förstöring och oavsiktlig förlust eller ändring.

Säkerhetskopiorna ska förvaras fysiskt åtskilda från och omfattas av samma skydd som de lagrade uppgifterna.

Säkerhetskopiorna ska utplånas samtidigt som de lagrade uppgifterna.

Allmänt råd

För att uppfylla kraven på skydd för de lagrade uppgifterna bör separata säkerhetskopior sparas vid flera olika tidpunkter. Den lagringsskyldige bör regelbundet kontrollera att det går att återskapa uppgifter från säkerhetskopiorna och skapa rutiner för att säkerställa att inga fel har uppstått i samband med kopiering.

Denna författning träder i kraft den 1 december 2012.

På Post- och telestyrelsens vägnar

GÖRAN MARBY

Eva Hallén