Post- och telestyrelsens författningssamling

ISSN 1400-187X

Post- och telestyrelsens föreskrifter och allmänna råd om skyddsåtgärder vid behandling av uppgifter och vid lagring av uppgifter för brottsbekämpande ändamål;

PTSFS 2026:1

Utkom från trycket
den 26 februari 2026

beslutade den 18 februari 2026.

Post- och telestyrelsen föreskriver följande med stöd av 8 kap. 3 och 4 §§ samt 9 kap. 5 § förordningen (2022:511) om elektronisk kommunikation och beslutar följande allmänna råd.

1 kap. Tillämpningsområde

1 § Dessa föreskrifter innehåller bestämmelser om

– särskilda tekniska och organisatoriska åtgärder som enligt 8 kap. 1 § lagen (2022:482) om elektronisk kommunikation ska vidtas i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål,

– lämpliga tekniska och organisatoriska åtgärder som enligt 8 kap. 2 § lagen om elektronisk kommunikation ska vidtas för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av en allmänt tillgänglig elektronisk kommunikationstjänst skyddas och att den som tillhandahåller ett allmänt elektroniskt kommunikationsnät vidtar de åtgärder som är nödvändiga för att upprätthålla motsvarande skydd i nätet, och

– innehållet i förteckningen över integritetsincidenter enligt 8 kap. 5 § lagen om elektronisk kommunikation.

2 kap. Ord och uttryck

1 § Ord och uttryck i dessa föreskrifter har samma betydelse som i lagen (2022:482) om elektronisk kommunikation och förordningen (2022:511) om elektronisk kommunikation.

2 § I dessa föreskrifter avses med

behandlade uppgifter: uppgifter som behandlas i samband med tillhandahållande av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster,

brottsdatalagringsincident: en händelse som leder till oavsiktlig eller otillåten förstöring av, oavsiktlig förlust eller ändring av, otillåten behandling av, otillåten lagring av, otillåtet avslöjande av eller otillåten tillgång till uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2022:482) om elektronisk

kommunikation så att de lagrade uppgifterna inte är av samma kvalitet och föremål för samma säkerhet och skydd som vid den behandling som skett före lagringen,

förbindelse: del av ett allmänt elektroniskt kommunikationsnät mellan två tillgångar eller mellan en tillgång och en anslutning till ett sådant kommunikationsnät,

informationsbehandlingstillgångar: system, databaser och fysiska resurser som används för informationsbehandling,

tillhandahållare: verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster som avses i 1 kap. 7 § lagen om elektronisk kommunikation,

uppdragstagare: den som anlitats av tillhandahållaren för att utföra installation, underhåll, felavhjälpning, drift eller liknande hantering av tillhandahållarens informationsbehandlingstillgångar och förbindelser.

3 kap. Övergripande säkerhetsarbete

1 § Tillhandahållarens säkerhetsarbete avseende behandlade uppgifter ska bedrivas långsiktigt, kontinuerligt och systematiskt. Arbetet ska omfatta såväl normala förhållanden som extraordinära händelser.

Allmänt råd till 1 §

Till stöd för det långsiktiga, kontinuerliga och systematiska säkerhetsarbetet bör tillhandahållaren utgå från etablerad standard på området.

2 § Tillhandahållaren ska i säkerhetsarbetet ha en tydlig rollfördelning med särskilt utpekade ansvariga för arbetet. Rollfördelningen ska dokumenteras.

3 § Tillhandahållaren ska upprätta, dokumentera och vid behov revidera de processer, rutiner och planer som anges i dessa föreskrifter. Tillhandahållaren ska dokumentera de tester som utförs i enlighet med dessa föreskrifter.

4 § Tillhandahållaren ska säkerställa att anställda och uppdragstagare har kunskap om och tillämpar de processer, rutiner och planer som de är berörda av.

5 § Tillhandahållaren ska dokumentera de åtgärder som vidtas enligt 6 kap. 2–4 §§ och 7–10 kap. samt följa upp dessa åtgärder årligen och vid behov.

Allmänt råd till 5 §

Vid uppföljning av vidtagna åtgärder bör tillhandahållaren använda sig av erfarenheter och resultat från till exempel genomförda tester. Penetrationstester bör användas som en del av säkerhetsarbetet för att följa upp de åtgärder som har vidtagits.

4 kap. Identifiering och dokumentation av informations-behandlingstillgångar, förbindelser och uppdragstagare

1 § Tillhandahållaren ska identifiera och dokumentera sina uppdragstagare, samtliga sina informationsbehandlingstillgångar och förbindelser där uppgifter behandlas.

Tillhandahållaren ska för respektive uppdragstagare åtminstone dokumentera

1. uppdragstagarens namn, organisationsnummer och kontaktuppgifter, och

2. en beskrivning av uppdraget.

Tillhandahållaren ska för respektive informationsbehandlingstillgång och förbindelse enligt första stycket åtminstone dokumentera

1. en unik beteckning,
2. dess funktion,
3. geografisk placering, om sådan finns,
4. en hänvisning till aktuell riskanalys enligt 5 kap., och
5. tillverkare.

Dokumentationen ska hållas uppdaterad och bevaras i fem år från att den upprättats. Varje gång uppgifter som ska dokumenteras enligt andra och tredje stycket ändras ska ändringen kunna spåras i fem år.

5 kap. Riskanalys

1 § Tillhandahållaren ska genomföra riskanalyser.

I en riskanalys ska tillhandahållaren analysera risken för att informationsbehandlingstillgångar eller förbindelser orsakar eller drabbas av integritets- eller brottsdatalagringsincidenter. Riskanalyser ska göras för varje informationsbehandlingstillgång och förbindelse.

Allmänt råd till 1 §

För likvärdiga informationsbehandlingstillgångar och förbindelser kan en gemensam riskanalys göras.

2 § Riskanalyser ska genomföras minst en gång per år, samt

1. inför anskaffning av informationsbehandlingstillgångar och förbindelser där behandlade uppgifter förekommer och vid anlitande av uppdragstagare,
2. efter att tidigare okända hot som är relevanta för riskanalysen identifierats, och
3. inför planerade förändringar.

Information om sådana hot som avses i första stycket kan förmedlas av Post- och telestyrelsen.

3 § Riskanalyserna ska innefatta åtminstone

1. identifiering av relevanta hot mot den aktuella informationsbehandlingstillgången eller förbindelsen som kan leda till att en integritets- eller brottsdatalagringsincident inträffar,
2. en bedömning av vilka konsekvenser som kan uppstå i händelse av att identifierade hot realiseras,
3. en bedömning av sannolikheten för att identifierade hot realiseras, och
4. en sammanvägd bedömning av sannolikheten för att identifierade hot inträffar och de konsekvenser det kan medföra om de realiseras (riskbedömning).

4 § I riskanalyser inför planerade förändringar ska tillhandahållare som är lagringsskyldiga enligt 9 kap. 19 lagen (2022:482) om elektronisk kommunikation analysera risken för att förändringarna orsakar en brottsdatalagringsincident.

Riskanalyserna ska innefatta åtminstone

1. identifiering av relevanta hot mot säkerheten för uppgifter som lagras för brottsbekämpande ändamål med anledning av den planerade förändringen,
2. en bedömning av vilka konsekvenser som kan uppstå i händelse av att identifierade hot realiseras,

3. en bedömning av sannolikheten för att identifierade hot realiseras, och
4. en sammanvägd bedömning av sannolikheten för att identifierade hot inträffar och de konsekvenser det kan medföra om de realiseras (riskbedömning).

Allmänt råd till 3 och 4 §§

Vid genomförandet av riskanalyser bör tillhandahållaren åtminstone analysera organisatoriska, logiska och fysiska hot.

En analys av organisatoriska hot bör åtminstone omfatta kritiska personberoenden, otillräcklig kompetensförsörjning, bristfällig incidenthantering, bristfällig behörighets- och åtkomsthantering samt bristfälliga processer för säkerhetsarbetet i övrigt.

En analys av logiska hot bör åtminstone omfatta kända sårbarheter i mjukvara, logiska överbelastningsattacker, logiska intrång, konfigurationsfel, fel och brister i hårdvara eller mjukvara (såväl egenutvecklad som utvecklad av annan) samt bristfällig segmentering av nätverk.

En analys av fysiska hot bör åtminstone omfatta hot relaterade till väder, klimatförändringar och den omgivande miljön, till exempel nederbörd, brand, vind, blixtnedslag, fukt, skadliga temperaturer, översvämningar, vattenläckor samt ras, skred och erosion. Analysen av fysiska hot bör även omfatta intrång, sabotage och annan yttre påverkan, till exempel stöld.

Riskanalysen bör innehålla en beskrivning av hur informationsbehandlings-tillgångarna och förbindelserna kan påverkas i samband med att identifierade hot realiseras och vilken påverkan detta kan få på de behandlade uppgifterna.

5 § Vid genomförande av riskanalyser ska tillhandahållaren beakta erfarenheter från tidigare inträffade integritets- eller brottsdatalagringincidenter, allmänt uppmärksammade integritets- eller brottsdatalagringsincidenter samt aktuella och relevanta omvärldsföreteelser.

Vid genomförande av riskanalyser ska tillhandahållaren tillämpa processer som utgår från etablerad standard på området.

Tillhandahållaren ska ha en plan för vid vilka tidpunkter och i vilka situationer riskanalyser ska genomföras.

Tillhandahållaren ska dokumentera genomförda riskanalyser.

6 kap. Riskhantering och åtgärder efter riskbedömning

Riskhantering

1 § Tillhandahållaren ska utifrån riskbedömningen besluta hur respektive risk ska hanteras genom att avgöra om riskerna ska undvikas, reduceras eller accepteras. Sådana beslut ska dokumenteras. Beslut om att acceptera en risk ska motiveras.

Allmänt råd till 1 §

Tillhandahållaren bör eftersträva att reducera risker framför att acceptera dem.

Åtgärder efter riskbedömning

2 § Tillhandahållaren ska vidta tekniska och organisatoriska åtgärder för att hantera de risker som ska undvikas eller reduceras. Åtgärderna ska vidtas på en nivå som är anpassad till den risk som föreligger, med beaktande av tillgänglig teknik och kostnaderna för åtgärderna.

Första stycket andra meningen gäller inte för sådana uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation. Tillhandahållaren ska för sådana uppgifter vidta åtgärder i enlighet med 9 kap. 4 § förordningen (2022:511) om elektronisk kommunikation.

Allmänt råd till 2 §

Tillhandahållarens åtgärder bör följa etablerade standarder, normer, säkerhetsvägledningar och praxis.

3 § Tillhandahållarens bedömning vid val av åtgärder ska dokumenteras samt följas upp årligen och vid behov.

Särskilda åtgärder vid planerade förändringar

4 § När tillhandahållarens riskanalys enligt 5 kap. visar att det finns risker för att planerade förändringar kan orsaka en brottsdatalagringsincident ska tillhandahållaren tillämpa en process som utgår från etablerad standard på området och utöver vad som följer av 2 § åtminstone

1. utföra tester inför förändringen och efter förändringen verifiera att den inte påverkat säkerheten negativt,
2. säkerhetskonfigurera (härda) berörda informationsbehandlingstillgångar, och
3. ta fram planer för att återställa behandlade uppgifter i händelse av att en brottsdatalagringsincident inträffar.

Tester, härdning, och planer för återställande eller åtgärdande ska vara anpassade till den planerade förändringens art och omfattning.

7 kap. Åtkomst och behörighet

1 § Tillhandahållaren ska medge åtkomst till behandlade uppgifter endast till den som är behörig. Tillhandahållaren ska tilldela sådan behörighet endast till den som behöver det för att kunna utföra sina arbetsuppgifter.

Tillhandahållaren ska tillämpa en process för tilldelning, ändring och uppföljning av tilldelade behörigheter enligt första stycket. Tilldelade behörigheter ska dokumenteras samt följas upp årligen och vid behov.

Tillhandahållaren ska ha system för hantering och kontroll av identiteter och behörigheter.

Allmänt råd till 1 §

Tillhandahållaren bör se till att den som kommer i kontakt med behandlade uppgifter regelbundet får utbildning och information om när och på vilket sätt behandlade uppgifter får hanteras. Den som kommer i kontakt med behandlade uppgifter bör även få utbildning i att upptäcka integritets- eller brottsdatalagringsincidenter och att analysera tänkbara konsekvenser av en inträffad

integritets- eller brottsdatalagringsincident för abonnenter och användare, inklusive brottsbekämpande myndigheter.

Tilldelade behörigheter bör vara begränsade i tid och omfattning, särskilt för tillfälliga uppdragstagare. Tilldelade behörigheter bör tas bort efter utfört uppdrag.

2 § Tillhandahållaren ska säkerställa att åtkomst endast ges till den som har upplysts om tystnadsplikten i de fall 9 kap. 31 och 32 §§ lagen (2022:482) om elektronisk kommunikation är tillämpliga.

8 kap. Skyddsåtgärder mot oavsiktlig eller otillåten utplåning eller förlust

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

Allmänt råd till 1 §

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

2 § Uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation ska i stället för vad som framgår av 1 § skyddas mot oavsiktlig eller otillåten utplåning samt oavsiktlig förlust eller ändring genom lagring på minst två fysiskt åtskilda platser.

Första stycket gäller även loggar enligt 9 kap. 1 § avseende åtkomst till uppgifter som ska lagras för brottsbekämpande ändamål.

Säkerhetskopior eller motsvarande ska omfattas av samma skydd och utplånas samtidigt som de uppgifter som lagras för brottsbekämpande ändamål.

Allmänt råd till 2 §

Skydd för uppgifter som lagras för brottsbekämpande ändamål kan uppnås genom redundant lagring, säkerhetskopiering eller liknande.

9 kap. Loggning

1 § Tillhandahållaren ska logga

1. all läsning, kopiering, ändring och utplåning av behandlade uppgifter, och
2. 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. Vid misstanke om att en integritets- eller brottsdatalagringsincident har inträffat ska relevanta loggar alltid kontrolleras.

Tillhandahållaren ska ha rutiner för kontroll av loggar. Kontroller av loggar ska ske systematiskt och återkommande. Genomförda kontroller av loggar ska dokumenteras.

Allmänt råd till 1 §

Tillhandahållaren bör tillämpa automatisk övervakning av loggar, i syfte att snabbt upptäcka onormala användarmönster, händelser eller serier av händelser. Detta gäller dock inte för loggar avseende åtkomst till uppgifter som ska lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2002:482) om elektronisk kommunikation.

2 § Den som är skyldig att lagra uppgifter för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation ska säkerställa att den som har haft tillgång till sådana uppgifter inte ges tillgång till loggar avseende åtkomst till uppgifterna.

3 § Innan uppgifter som lagras för brottsbekämpande ändamål utplånas i enlighet med 9 kap. 22 § lagen (2022:482) om elektronisk kommunikation ska tillhandahållaren utföra en systematisk kontroll av loggar avseende åtkomst till uppgifterna. I samband med att uppgifterna utplånas ska även loggar utplånas.

10 kap. Kryptering

1 § Behandlade uppgifter som överförs via internet ska skyddas genom kryptering.

Uppgifterna behöver dock inte skyddas genom kryptering om det med hänsyn till uppgifternas art och sammanhang är osannolikt att överföring utan kryptering kan leda till en integritets- eller brottsdatalagringsincident.

Allmänt råd till 1 §

Koder, lösenord och sammanställningar av uppgifter som rör en användare eller abonnent bör krypteras vid överföring via internet.

2 § Anslutningar för konfigurering och styrning av informationsbehandlings-tillgångar via internet eller allmänna elektroniska kommunikationsnät som även andra än tillhandahållaren har rådighet över ska skyddas genom kryptering.

3 § Loggar avseende åtkomst till uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation ska skyddas genom kryptering under lagring och överföring.

4 § Kryptering ska ske med en allmänt erkänd krypteringsmetod med tillräcklig nyckellängd. Krypteringsnycklar ska hanteras på ett säkert sätt.

5 § Tillhandahållaren ska ha rutiner för kryptering och hantering av krypteringsnycklar.

11 kap. Intern incidenthantering

1 § Tillhandahållaren ska säkerställa att

1. inträffade integritets- eller brottsdatalagringsincidenter rapporteras internt,
2. åtgärder vidtas skyndsamt för att hantera en uppkommen integritets- eller brottsdatalagringsincident,
3. åtgärder vidtas för att undvika liknande integritets- eller brottsdatalagringsincidenter, och

4. erfarenheter från inträffade integritets- eller brottsdatalagringsincidenter beaktas vid genomförande av riskanalyser enligt 5 kap.

Vid åtgärder enligt första stycket ska tillhandahållaren tillämpa processer som utgår från etablerad standard på området.

Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster ska också ha rutiner för identifiering av integritetsincidenter.

2 § Den som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster ska löpande föra en förteckning över integritetsincidenter i enlighet med 8 kap. 5 § lagen (2022:482) om elektronisk kommunikation.

Förteckningen 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, och
7. referensnummer.

Dessa föreskrifter och allmänna råd träder i kraft den 1 april 2026.

På Post- och telestyrelsens vägnar

DAN SJÖBLOM

Karolina Asp