

Konsekvensutredning av Post- och telestyrelsens förslag till föreskrifter om skyddsåtgärder vid behandling av uppgifter och vid lagring av uppgifter för brottsbekämpande ändamål

Post och telestyrelsen (PTS) föreslår föreskrifter och allmänna råd om skydd av uppgifter vid tillhandahållandet av allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster samt gällande säkerhet i sådana nät och tjänster i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål. Syftet är att förhindra integritetsincidenter och händelser som leder till oavsiktlig eller otillåten förstöring, oavsiktlig förlust eller ändring, eller otillåten behandling av, lagring av, avslöjande av eller tillgång till uppgifter som lagras för brottsbekämpande ändamål (brottsdatalagringsincidenter).

Föreskrifterna omfattar de delar av PTS föreskrifter och allmänna råd (PTSFS (2022:11) om säkerhet i nät och tjänster) (säkerhetsföreskrifterna) för vilka PTS har föreskriftsbemyndiganden genom 8 kap. 5, 6 och 9 §§ i lagen (2022:482) om elektronisk kommunikation (LEK) respektive 8 kap. 4 och 6 §§ samt 9 kap. 5 § förordningen (2022:511) om elektronisk kommunikation (FEK). PTS förbereder för att upphäva säkerhetsföreskrifterna den 15 januari 2026. Detta eftersom de föreskriftsbemyndiganden som återfinns i 8 kap. 1, 3 och 4 §§ LEK avseende riskhantering i nät och tjänster och säkerhetsincidenter upphävs i och med den kommande cybersäkerhetslagen (se prop. 2025/26:28).

Enligt förslaget till ändrad LEK kommer 8 kap. 5, 6 och 9 §§ LEK att omnumreras till 8 kap. 1, 2 och 5 §§ från och med den 15 januari 2026. I konsekvensutredningen som följer används de paragrafer som gäller för närvarande. I förslag till nya föreskrifter, se bilaga 1, används emellertid den föreslagna nya numreringen vid hänvisningar till LEK.

1. Bakgrund

1.1 Syftet med nya föreskrifter

I samband med att PTS upphäver myndighetens säkerhetsföreskrifter med anledning av ny lagstiftning och ändrade bemyndiganden¹, har PTS identifierat ett behov av att se över och tydliggöra de bestämmelser i säkerhetsföreskrifterna som rör skyddsåtgärder vid behandling av uppgifter och vid lagring av uppgifter för brottsbekämpande ändamål. Regleringen avseende dessa områden i LEK och FEK berörs inte av föreslagna ändringar i prop. 2025/26:28 och nu gällande skyddsåtgärder bedöms därmed kunna beslutas i nya föreskrifter med endast ett fåtal ändringar och förtydliganden gjorda i förhållande till vad som gäller redan i dag enligt säkerhetsföreskrifterna.

PTS syfte med förslaget till nya föreskrifter är att de delar av säkerhetsföreskrifterna (som kommer upphävas den 15 januari 2026) som inte påverkas av ny reglering i cybersäkerhetslagen, ska fortsätta att gälla. Med hänsyn till att begreppet "säkerhetsincident" upphävs i LEK har vissa justeringar gjorts i de föreslagna föreskrifterna men generellt sett har inte några nya krav införts.

1.2 Konsekvenser om ingen åtgärd vidtas

Om de föreslagna föreskrifterna inte beslutas kommer de krav på skyddsåtgärder som gäller idag enligt säkerhetsföreskrifterna inte att finnas kvar efter den 15 januari 2026. Tillhandahållarna kommer då inte längre ha de detaljerade krav som gäller för skyddsåtgärder enligt nuvarande föreskrifter utan behöver förhålla sig till de mer generella krav som gäller enligt LEK. Det kan leda till att fler integritetsincidenter och incidenter avseende uppgifter som lagras för brottsbekämpande ändamål, inträffar. PTS tillsyn över att lämpliga skyddsåtgärder har vidtagits enligt LEK kan antas försvåras när detaljerade regler avseende skyddsåtgärder saknas.

1.3 Alternativ för att uppnå förändringen och den lämpligaste lösningen

Ett alternativ till att meddela föreslagna föreskrifter är att krav på att vidta skyddsåtgärder endast framgår av lag och förordning. Ett sådant alternativ skulle innebära att tillhandahållarna inte får klarhet i vilka åtgärder som förväntas av dem och att PTS tillsyn kan antas försvåras. Den lämpligaste lösningen är att besluta föreskrifter som till största del motsvarar de krav som gäller redan idag, krav som av regleringstekniska skäl behöver upphävas eftersom säkerhetsföreskrifterna

¹ Se Konsekvensutredning avseende upphävande av Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTSFS 2022:11).

innehåller regler som härrör från ett antal bemyndiganden, varav några upphävs i januari 2026.

1.4 Berörda av förslaget

De aktörer som berörs av regleringen är tillhandahållare av allmänna elektroniska kommunikationsnät och -tjänster enligt de definitioner som framgår av LEK. I dagsläget uppgår antalet till ca 750 tillhandahållare. Majoriteten av dessa är anmälningsskyldiga till PTS. De anmälningsskyldiga tillhandahållarna omfattas av samtliga krav i de föreslagna föreskrifterna. En grupp som inte är anmälningsskyldiga enligt LEK men som omfattas av kraven på att vidta skyddsåtgärder för behandlade uppgifter är tillhandahållarna av nummeroberoende interpersonella kommunikationstjänster s.k. Noik. Denna grupp omfattas inte av de krav som ställs på skyddsåtgärder för uppgifter som lagras för brottsbekämpande ändamål eftersom de inte är skyldiga att lagra sådana uppgifter i enlighet med vad som framgår av 9 kap. 19 § LEK.

En utförlig beskrivning av de berörda finns i konsekvensutredningen som skrevs till säkerhetsföreskrifterna 2022.²

1.5 Begrepp

I denna konsekvensutredning används begreppen

- ”kommunikationsnät” och ”nät” synonymt med begreppet ”elektroniskt kommunikationsnät” så som det definieras i LEK,
- ”kommunikationstjänst” och ”tjänst” synonymt med begreppet ”elektronisk kommunikationstjänst” så som det definieras i LEK,
- ”tillhandahållare”, ”aktör” eller ”företag” för verksamhetsutövare som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst, samt
- ”behandlade uppgifter” för de uppgifter som behandlas i samband med tillhandahållande av kommunikationsnät eller kommunikationstjänster och som ska skyddas enligt 8 kap. 5 och 6 §§ LEK (ändras enligt lagrådsremiss om ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag till 8 kap. 1 och 2 §§ LEK)
- ”Noik” avser s.k. nummeroberoende interpersonella kommunikationstjänster

Vidare kommer följande benämningar användas avseende

² Konsekvensutredning avseende föreskrifter och allmänna råd om säkerhet i nät och tjänster, Dnr 20-3324

Svensk reglering

LEK	Lagen (2022:482) om elektronisk kommunikation
FEK	Förordning (2022:511) om elektronisk kommunikation
NIS-lagen	Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
NIS-förordningen	förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster
Cybersäkerhetslagen	Lagen (se prop. 2025/26:28) om cybersäkerhet
Cybersäkerhetsförordningen	Förordning (se SOU 2024:18) om cybersäkerhet

EU-reglering

Kodex	Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation
NIS-direktivet	Direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen
NIS2-direktivet	Direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148
E-dataskyddsdirektivet	Europaparlamentets och rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation

1.6 Ändringar i den nya EU-regleringen och nya nationella lagstiftningen

Genom artikel 41 i NIS2-direktivet upphävs artiklarna 40 och 41 i Kodex och ersätts med de bestämmelserna som återfinns i artikel 21 i NIS2-direktivet. Detta medför att de bestämmelser i LEK som genomför artiklarna 40 och 41 i Kodex upphävs och ersätts med bestämmelser i cybersäkerhetslagen som motsvarar de krav som ställs i artikel 21 i NIS2-direktivet (prop. 2025/26:28). Detta medför i sin tur att 8 kap. 1-4 §§ (säkerhet i nät och tjänster) LEK kommer upphöra att gälla samtidigt som 5-9 §§ LEK (säkerhet i nät och tjänster avseende lagrade uppgifter och skydd av uppgifter vid tillhandahållandet av tjänster) kvarstår oförändrade i LEK. 8 kap. 5-9 §§ föreslås omnumreras till 8 kap. 1-5 §§ LEK. Vidare upphör definitionen av begreppet

”säkerhetsincident” enligt prop. 2025/26:28 i LEK då regler om säkerhet i nät och tjänster generellt överförs till cybersäkerhetslagen.

1.7 Bestämmelser om skyddsåtgärder som ska vidtas vid brottsdatalagring

Förslaget till föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter motsvarar i sak de delar i säkerhetsföreskrifterna som kompletterar skyldigheter i 8 kap. 5 § LEK. Bestämmelserna om skyddsåtgärder vid lagring och annan behandling av uppgifter som lagras för brottsbekämpande ändamål föreslås överföras till de nya föreskrifterna i princip oförändrade, med vissa språkliga eller redaktionella ändringar.

I en bestämmelse i föreskrifterna, 9 kap. 1 § avseende loggning, införs en mindre materiell förändring i syfte att upprätthålla och förtydliga den säkerhetsnivå som föreskrivs i 9 kap. 4 § FEK. Bedömningen är att den materiella förändringen inte kommer att medföra några nya kostnader eller administrativa bördor då PTS bedömer att kravet som förtydligas redan idag uppfylls av de lagringsskyldiga tillhandahållarna.

Bestämmelserna innebär i princip inte några nya kostnader eller administrativa bördor för de lagringsskyldiga tillhandahållarna. Konsekvenserna av föreskrifterna har i stort bedömts inför när säkerhetsföreskrifterna togs fram³. Endast vissa förtydliganden och klargöranden kommer att göras.

I och med att de delar som avser säkerhet i nät och tjänster behöver upphävas då 8 kap. 1-4 §§ LEK upphör att gälla och att definitionen av ”säkerhetsincident” utgår behöver vissa bestämmelser tas bort eller omformuleras. Omformuleringarna innebär framförallt införandet av ett nytt begrepp – brottsdatalagringsincident.

Vidare behöver kraven i 9 kap. 4 §§ FEK tydliggöras. Kraven innebär att den som är skyldig att lagra uppgifter ska vidta de åtgärder som krävs för att säkerställa att de lagrade uppgifterna är av samma kvalitet och föremål samt bibehåller samma säkerhet och skydd som vid den behandling som skett före lagringen.

1.8 Skydd av behandlade uppgifter

Förslaget till nya föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter motsvarar i sak de delar i säkerhetsföreskrifterna som kompletterar skyldigheter i 8 kap. 6 och 9 §§ LEK. Bestämmelserna om skyddsåtgärder för behandlade uppgifter och innehållet i förteckningen över integritetsincidenter i

³ PTS ärende med dnr 20-3324.

säkerhetsföreskrifterna föreslås överföras till de nya föreskrifterna oförändrade eller med enbart språkliga eller redaktionella ändringar.

Eftersom bestämmelserna överförs oförändrade i sak från nuvarande gällande föreskrifter till de nya medför bestämmelserna inte några nya kostnader eller administrativa bördor. Konsekvenserna av dessa bestämmelser har bedömts inför att säkerhetsföreskrifterna beslutades.

2. Föreslagna krav och effekter för berörda aktörer

De föreslagna föreskrifterna syftar till att säkerställa att nuvarande krav i säkerhetsföreskrifterna rörande aktuella skyddsåtgärder fortsatt ska gälla och motsvara en säkerhetsnivå som är lämplig i förhållande till riskerna för incidenter och samhällets behov av uppgifter som lagras för brottsbekämpande ändamål. Några konsekvenser för tillhandahållarna avseende de regler som redan gäller enligt säkerhetsföreskrifterna bedöms inte uppkomma. För närmare beskrivning av dessa bestämmelser och dess konsekvenser, se konsekvensutredningen till säkerhetsföreskrifterna.⁴ Nedan anges de få justeringar eller förtydliganden som föreslås i förhållande till de skrivningar som finns i säkerhetsföreskrifterna.

2.1 Förändringar i förhållande till vad som redan gäller enligt säkerhetsföreskrifterna för behandlade uppgifter och uppgifter som lagras för brottsbekämpande ändamål

2.1.1 Kapitel 2 – Brottsdatalagringsincident införs som definition

2.1.1.1 Integritetsincident jämfört med säkerhetsincident

En säkerhetsincident omfattar enligt 1 kap. 7 § LEK händelser med faktiskt negativ inverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos nät och tjänster samt hos lagrade, överförda eller behandlade uppgifter samt hos närliggande tjänster som erbjuds eller är tillgängliga via sådana tjänster eller, på förmågan att motstå sådana händelser. En integritetsincident omfattar enligt 1 kap. 7 § LEK händelser som kan leda till att behandlade uppgifter oavsiktligt eller otillåtet utplånas, försvinner, ändras eller otillåtet avslöjas eller kan komma åt i samband med tillhandahållandet av elektroniska kommunikationstjänster.

⁴ Konsekvensutredning avseende föreskrifter och allmänna råd om säkerhet i nät och tjänster, Dnr 20-3324.

De bakomliggande ändamålen med att skydda sig mot säkerhetsincidenter och integritetsincidenter är något olika. Integritetsincidenter tar sikte på det säkerhetsskydd som krävs för att upprätthålla möjligheterna till att ha kontroll över egna (enskildas eller juridiska personers) behandlade uppgifter samt uppgifternas konfidentialitet. Säkerhetsincidenter tar i stället sikte på att uppgifter faktiskt ska kunna behandlas, exempelvis lagras för brottsbekämpande ändamål.

Enligt LEK finns krav om att lagra uppgifter för brottsbekämpande ändamål. Det rör sig här om samhällets behov om att få tillgång till behandlade uppgifter för att bekämpa brott. I dessa fall kan inte sägas att en integritetsincident uppstår om uppgifter exempelvis inte lagras, avidentifieras eller raderas. Denna situation omfattas i stället av det som benämns som "säkerhetsincident". Detta eftersom begreppet "säkerhetsincident" exempelvis omfattar krav på att behandlade uppgifter ska vara tillgängliga, autentiska, riktiga och konfidentiella för att faktiskt kunna lämnas ut till brottsbekämpande myndigheter. Med anledning av att begreppet säkerhetsincident inte längre kommer att definieras i LEK efter den 15 januari 2026 behöver de aktuella föreskrifterna ha en ny definition för att skyddsåtgärder ska vidtas enligt de krav som ställs även fortsättningsvis i LEK och FEK.

2.1.1.2 Begreppet brottsdatalagringsincident

Begreppet "säkerhetsincident" omfattar både incidenter kopplade till säkerhet i nät och tjänster och säkerhet för uppgifter som lagras för brottsbekämpande ändamål. När begreppet "säkerhetsincident" upphävs i LEK är det mer rimligt att ett annat begrepp används för incidenter som kan uppstå i förhållande till uppgifter som lagras för brottsbekämpande ändamål. För att illustrera och tydliggöra vad som omfattas införs genomgående begreppet "brottsdatalagringsincident" i stället för "säkerhetsincident". Denna begreppsändring antas inte medföra några konsekvenser för tillhandahållarna i de föreskrifter där det nya begreppet förekommer.

Begreppet används inte i något annat hänseende i svensk lagstiftning och anknyter enbart till lagring för brottsbekämpande ändamål.

2.1.2 Kapitel 4 – Identifiering och dokumentation av informationsbehandlingstillgångar och uppdragstagare

I 4 kap. 1 § har kravet på dokumentation och kravet avseende att spara versioner tydliggjorts på så sätt att det anges att kravet är begränsat till de uppgifter som explicit anges i bestämmelsen, och inte ytterligare uppgifter som tillhandahållare själva väljer att dokumentera.

Förtydligandet medför inga konsekvenser jämfört med säkerhetsföreskrifterna.

2.1.3 Kapitel 6 – Riskhantering och åtgärder efter riskbedömning

Bestämmelsen i 6 kap. 4 § som gäller särskilda åtgärder som ska vidtas vid planerade förändringar har ändrats till att omfatta brottsdatalagringsincidenter i stället för rapporteringspliktiga säkerhetsincidenter. Rapporteringspliktiga säkerhetsincidenter enligt 17 kap. säkerhetsföreskrifterna ställer krav på att säkerhetsincidenten haft faktisk påverkan enligt vissa tröskelvärden eller att den haft betydande påverkan på funktioner i samhället (17 kap. 5–6 §§ säkerhetsföreskrifterna).

En brottsdatalagringsincident anses alltid ha betydande påverkan på funktioner i samhället då det inskränker brottsbekämpande myndigheters möjlighet att bekämpa och motverka brott. Det nya begreppet medför därmed ingen förändring av krav och konsekvenser som redan gäller enligt säkerhetsföreskrifterna.

De föreslagna bestämmelserna om riskhantering och riskbedömning omfattar samtliga tillhandahållare, förutom de delar som rör uppgifter som lagras för brottsbekämpande ändamål, som omfattar samtliga tillhandahållare förutom tillhandahållare av Noik.

2.1.4 Kapitel 7 – Åtkomst och behörighet

2.1.4.1 Inledning

7 kap. 1 § i de föreslagna föreskrifterna innehåller en bestämmelse om åtgärder avseende åtkomst och behörighet. Bestämmelsen handlar om vem som har rätt att få åtkomst till nät, tjänster och uppgifter samt att förhindra att obehöriga får sådan åtkomst.

I 7 kap. 1 § införs ett förtydligande om att behörigheter ska tilldelas den som behöver det för att kunna utföra sina arbetsuppgifter i stället för att ange att det endast gäller anställda och uppdragstagare. Den tidigare skrivningen kan uppfattas för avgränsande och det kan finnas andra än anställda och uppdragstagare som behöver få åtkomst till behandlade uppgifter för att kunna utföra sina arbetsuppgifter, t.ex. återförsäljare, vilket hela tiden har varit avsikten med kravet.

Det förtydligas vidare i det allmänna rådet till 1 §, i förhållande till att – den som kommer i kontakt med behandlade uppgifter bör få utbildning i att upptäcka integritets- eller brottsdatalagringsincidenter och att analysera tänkbara konsekvenser av en inträffad integritets- eller brottsdatalagringsincident för abonnenter och användare, *inklusive för brottsbekämpande myndigheter*. ”Användare” inkluderar brottsbekämpande myndigheter vilket tidigare var underförstått men inte utskrivet varför detta förtydligas.

De föreslagna bestämmelserna om åtkomst och behörighet omfattar samtliga tillhandahållare, förutom de delar som rör uppgifter som lagras för brottsbekämpande ändamål, som omfattar samtliga tillhandahållare förutom tillhandahållare av Noik.

2.1.5 Kapitel 9 – Loggning

9 kap i de föreslagna föreskrifterna innehåller bestämmelser om loggning. Loggning handlar om registrering av genomförda aktiviteter i tillhandahållares elektroniska kommunikationsnät och -tjänster inklusive system och tjänster för behandlade uppgifter i syfte att incidenter ska upptäckas så tidigt som möjligt, och i vissa fall förhindras, samt kunna utredas. Loggar är viktiga för att kunna utreda vad som har inträffat efter en inträffad händelse. Självfallet ska krav enligt EU:s dataskyddsförordning⁵ efterlevas vid upprättande och genomförande av loggning och endast nödvändiga personuppgifter ska loggas. Enligt dataskyddsförordningens grundläggande principer vid personuppgiftsbehandling råder uppgiftsminimering samt lagringsminimering.

Kravet i 9 kap 1 § föreskrifterna om kontroll av loggar har utvidgats till att kontroll av loggar även ska ske vid misstänkt brottsdatalagringsincident och inte endast vid misstänkt integritetsincident. Det nya kravet bedöms inte medföra några ekonomiska konsekvenser för tillhandahållarna.

I 9 kap 2 § säkerhetsföreskrifterna finns krav på att tillhandahållarna ska logga systemhändelser nödvändiga för att kunna utreda säkerhetsincidenter. 1 § i de föreslagna föreskrifterna listar vad som behöver loggas för att utreda integritets- och brottsdatalagringsincidenter. Den del av 9 kap. 2 § säkerhetsföreskrifterna som omfattar brottsdatalagringsincidenter kommer med förslaget att omfattas av 1 §. Att 9 kap. 2 § säkerhetsföreskrifterna upphävs bedöms därmed inte få några konsekvenser i och med skrivningen i 1 §.

De föreslagna bestämmelserna om loggning omfattar samtliga tillhandahållare, förutom de delar som rör uppgifter som lagras för brottsbekämpande ändamål, som omfattar samtliga tillhandahållare förutom tillhandahållare av Noik.

3. Övrigt

3.1 Samråd

Av 9 kap. 5 § FEK följer att PTS ska ge Integritetsskyddsmyndigheten, Polismyndigheten och Säkerhetspolisen tillfälle att yttra sig innan närmare föreskrifter

⁵ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG

meddelas om åtgärder som ska vidtas för att skydda uppgifter som lagras bör brottsbekämpande ändamål. PTS har därför genomfört samråd med Polismyndigheten, Säkerhetspolisen, och Integritetsskyddsmyndigheten. Utöver detta har PTS också kontaktat följande urval av tillhandahållare; Telia, Telenor, Tele2 och Hi3G.

Samrådet har skett skriftligen och utgått ifrån de föreslagna ändringarna i föreskrifterna. Syftet var att samla in information och synpunkter i ett tidigt skede av processen för att säkerställa en ändamålsenlig reglering. PTS har i den mån det har varit relevant för detta arbete och utifrån vad som ryms inom myndighetens bemyndigande beaktat de synpunkter som inkommit.

3.2 Bedömning av om förslaget eller beslutet överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen

PTS gör bedömningen att de föreslagna föreskrifterna överensstämmer med de skyldigheter som följer av Sveriges anslutning till EU. Bestämmelser om tillhandahållares integritetsskyddsåtgärder har sitt ursprung i e-dataskyddsdirektivet och återfinns i LEK. De föreslagna föreskrifterna har utformats i enlighet med dessa bestämmelser och gällande EU-rättspraxis genom att de syftar till att uppnå en nivå på säkerheten som är lämplig i förhållande till risken. PTS bedömer således att bestämmelserna om skyddsåtgärder i de föreslagna föreskrifterna står i överensstämmelse med EU-rätten.

3.3 Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

Enligt 8 kap. 4 § FEK får PTS meddela ytterligare föreskrifter om skyddsåtgärder enligt 8 kap. 5 § LEK. I 8 kap. 5 § LEK anges att den som enligt 9 kap. 19 § är skyldig att lagra uppgifter ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling.

Av 8 kap. 6 § FEK framgår att PTS får meddela närmare föreskrifter om förteckningar över integritetsincidenter enligt 8 kap. 9 § LEK där det framgår att den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst löpande ska föra en förteckning över integritetsincidenter.

Vidare framgår av 9 kap. 5 §§ FEK att PTS får, efter att ha gett Integritetsskyddsmyndigheten, Polismyndigheten och Säkerhetspolisen tillfälle att yttra sig, meddela närmare föreskrifter om de åtgärder som ska vidtas enligt 4 § första och andra styckena. Enligt dessa stycken ska den som är skyldig att lagra uppgifter enligt 9 kap. 19 § LEK vidta de åtgärder som krävs för att säkerställa att de

lagrade uppgifterna är av samma kvalitet och föremål för samma säkerhet och skydd som vid den behandling som skett före lagringen. Den lagringsskyldige ska vidta de åtgärder som krävs för att skydda uppgifterna mot oavsiktlig eller otillåten förstöring och oavsiktlig förlust eller ändring. Sådana åtgärder ska även vidtas för att förhindra otillåten lagring av, behandling av eller tillgång till uppgifterna och otillåtet avslöjande av uppgifterna. Uppgifterna får göras tillgängliga endast för personal med särskild behörighet

3.4 Ikraftträdande

Med anledning av att säkerhetsföreskrifterna kommer upphävas den 15 januari 2026 när PTS bemyndigande till vissa av bestämmelserna upphävs i LEK, föreslås dessa föreskrifter träda ikraft i så nära anslutning till upphävandet som är möjligt med hänsyn till remisstider och andra administrativa krav.

3.5 Kontaktpersoner

För sakfrågor:

Maria Wiberg, enheten för cybersäkerhet och samordning, maria.wiberg@pts.se

Fanny Schönenberg, enheten för betrodda tjänster och datalagring,
fanny.schonenberg@pts.se

För rättsliga frågor:

Verksjuristen Sofie Sandell, sofie.sandell@pts.se