Vår referens: 25-19765

Sammanställning och analys av inkomna remissvar avseende PTS förslag till nya föreskrifter om skyddsåtgärder vid behandling av uppgifter och vid lagring av uppgifter för brottsbekämpande ändamål

1. Inledning

Post- och telestyrelsen (PTS) har den 31 oktober 2025 skickat ut ett förslag till nya föreskrifter om skyddsåtgärder vid behandling av uppgifter och vid lagring av uppgifter för brottsbekämpande ändamål och en tillhörande konsekvensutredning. Remisstiden gick ut den 21 november 2025. Nedan sammanställs de huvudsakliga synpunkter som har framförts i inkomna remissvar, tillsammans med PTS inställning till remissinstansernas synpunkter.

2. Inkomna svar

Följande företag, branschorganisationer och myndigheter har lämnat synpunkter på PTS förslag till nya föreskrifter om skyddsåtgärder vid behandling av uppgifter och vid lagring av uppgifter för brottsbekämpande ändamål

Post- och telestyrelsen
Postadress: Box 6101, 102 32 Stockholm
Besöksadress: Hälsingegatan 38
Telefon: 08-678 55 00
E-post: pts@pts.se
www.pts.se

Kommerskollegium, Konsumentverket, Myndigheten för samhällsskydd och beredskap, Sveriges Kommuner och Regioner, Svenska Stadsnätsföreningen, Svensk Handel, Säkerhetspolisen, Telenor Sverige AB och Telia Sverige AB

Följande remissinstanser har inga synpunkter på, inget att invända mot eller inget ytterligare att tillägga på PTS förslag till nya föreskrifter:

Energimyndigheten, Försvarsmakten, Integritetsskyddsmyndigheten, Konkurrensverket, Myndigheten för delaktighet, Regelrådet, Tech Sverige, Tele2 Sverige AB

Framförda synpunkter redovisas i avsnitt 3 (Övergripande synpunkter), avsnitt 4 (Närmare synpunkter på förslaget), avsnitt 5 (Synpunkter på bestämmelser i tillgänglighetsdirektivet som inte har tagits in i föreskrifterna), avsnitt 6 (Regelrådets bedömning) och avsnitt 7 (Kommerskollegiums bedömning)

3. Övergripande synpunkter

3.1 Föreskrifternas förhållande till cybersäkerhetslagen och kommande föreskrifter

SKR skriver att det är olyckligt att denna föreskrift kommer före föreskrifterna för cybersäkerhetslagen, vilket riskerar överlapp och dubbla krav. De framför vidare att PTS bör beskriva hur regelverkens krav förhåller sig till varandra.

Telenor framför att de föreslagna skyldigheterna och råden i stor utsträckning motsvarar de som redan gäller generellt för säkerhetsarbetet och incidenthanteringen. Men då det ännu inte har publicerats några föreskrifter angående krav på säkerhetsarbete och incidenthantering baserat på Cybersäkerhetslagen är det inte möjligt för Telenor att bilda sig en uppfattning om de föreslagna bestämmelserna är synkroniserade med cybersäkerhetsföreskrifterna. Det är bekymmersamt att det kommer finnas två parallella säkerhetsregelverk för samma verksamhet och om de inte är helt synkroniserade uppstår otydlighet och ineffektivitet. Incidenter hos operatörerna kan ofta utgöra både säkerhetsincident och integritetsincident och att då behöva rapportera till olika myndigheter, i olika formulär och med olika tidskrav är naturligtvis olyckligt. Sättet på vilket säkerhetsarbetet ska bedrivas, risker analyseras och säkerhetsåtgärder prioriteras bör vara detsamma för att hantera både risken för integritetsincidenter som för

säkerhetsincidenter. Ett sätt att hantera detta är att det i stället hänvisas i materiellt hänseende till cybersäkerhetsföreskrifterna i den utsträckning avsikten är att samma krav och principer ska gälla.

Telenor noterar att Kommissionen i förslag till Digital Omnibus (ändringsförordning (25) 837) anser att artikel 4 i e-dataskyddsdirektivet ska upphöra att gälla. Om detta förslag realiseras borde det få till följd att PTS inte ska reglera särskilt hur säkerhetsarbetet ska bedrivas avseende behandlade uppgifter, utan istället ska tillhandahållarna följa bestämmelserna i Cybersäkerhetslagen och föreskrifter baserade på den lagen i dessa delar. I stället för att reglera säkerhetsarbetet och de olika säkerhetsåtgärderna genom de nu föreslagna kraven och råden bör det därför, såsom Telenor påpekat i svaret, hänvisas till de relevanta bestämmelser som framgår av cybersäkerhetsföreskrifterna.

PTS svar:

Framtagandet av nya föreskrifter om skyddsåtgärder vid behandling av uppgifter och vid lagring av uppgifter för brottsbekämpande ändamål syftar enbart till att upprätthålla de krav för vilka PTS har föreskriftsbemyndiganden efter det att ändringar införs i lag (2022:482) om elektronisk kommunikation (LEK) genom cybersäkerhetslagen[1] som träder i kraft den 15 januari 2026. Ändringarna i LEK innebär att föreskriftsbemyndiganden gällande säkerhet i nät och tjänster upphör och flyttas över och till viss del ändras i cybersäkerhetslagen varför PTS måste upphäva föreskrifter och allmänna råd PTSFS (2022:11) om säkerhet i nät och tjänster (PTS säkerhetsföreskrifter) i samband med ikraftträdandet av cybersäkerhetslagen. Föreskriftsbemyndigandena avseende behandling av uppgifter och vid lagring av uppgifter för brottsbekämpande ändamål kvarstår dock oförändrade i LEK.

PTS nya föreskrifter om skyddsåtgärder vid behandling av uppgifter och vid lagring av uppgifter för brottsbekämpande ändamål avser därför endast att så kontinuerligt som möjligt upprätthålla gällande krav som tydliggör och specificerar kraven avseende dessa uppgifter. I nuläget är det därför inte möjligt att ta hänsyn till kommande föreskrifter och EU-rättsliga regelverk för vilka tidsperspektiven är oklara.

3.2 Föreskrifternas förhållande till säkerhetsskyddslagen

Telenor vill påtala att säkerheten är mycket hög gällande brottsdatalagring, bl.a. för att verksamheten med bistånd till brottsutredande myndigheter normalt omfattas av säkerhetsskydd. Detta aktualiserar frågan om säkerhets- och

[1] Se proposition 2025/26:28, Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag.

incidentrapporteringskraven enligt säkerhetsskyddslagstiftningen bör ha företräde, på samma sätt som kommer att gälla enligt Cybersäkerhetslagen. PTS har inte i konsekvensutredningen berört denna fråga, trots att denna princip genomdrivs i förhållandet mellan Cybersäkerhetslagen och Säkerhetsskyddslagen, dvs att den förra inte är tillämplig för säkerhetsåtgärder och incidentrapportering för verksamhet som omfattas av säkerhetsskydd.

PTS svar:

Tillhandahållare som omfattas av LEK kan i vissa fall även bedriva säkerhetskänslig verksamhet och omfattas i dessa delar av säkerhetsskyddslagen (2018:585). LEK och säkerhetsskyddslagen har olika tillämpningsområden och syften. Båda lagarna kan bli tillämpliga i en verksamhet som helt eller delvis är säkerhetskänslig. Exempelvis kan det krävas att en säkerhetsincident ska rapporteras enligt både LEK och säkerhetsskyddslagen alternativt den ena eller andra. Åtgärder enligt LEK måste vara förenliga med proportionalitetsprincipen vilket inte är fallet avseende verksamhet som avser Sveriges säkerhet enligt säkerhetsskyddslagen.[2] Säkerhetsskyddslagen utgör så kallat *lex specialis* och har företräde framför LEK.

3.3 Urval av aktörer i tidigt samråd

Stadsnätsföreningen (SSNF) vill uppmärksamma Post- och telestyrelsen på att det urval av tillhandahållare som myndigheten valt att kontakta i det tidiga samrådet, det vill säga Telia, Telenor, Tele2 och Hi3G, enligt sin bedömning inte speglar den faktiska strukturen på den svenska marknaden.

Att kommunala tillhandahållare inte inkluderats i det initiala samrådsurvalet innebär att en central del av sektorn inte fått möjlighet att lämna synpunkter i ett tidigt skede, trots att de berörs i minst lika hög grad av de föreslagna föreskrifterna. Stadsnätsföreningen vill därför lyfta vikten av att även denna grupp involveras vid framtida samråd och dialoger.

PTS svar:

PTS noterar medskicket från SSNF.

[2] Prop. 2021/22:136 - Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation, avsnitt *Sveriges säkerhet*, s. 118 ff.

3.4 Skyddsåtgärder mot oavsiktlig eller otillåten utplåning eller förlust

Telia vill framhålla följande om de nuvarande och kommande kraven; eftersom leverantörerna ska säkerställa att tekniska och organisatoriska åtgärder vidtas som säkerställer att uppgifter som lagras för brottsförebyggande ändamål skyddas vid behandling, dvs att de uppgifter som lagras bibehåller en hög kvalitet då de behandlas och att det finns ett skydd mot integritetsintrång, krävs det att uppgifter finns tillgängliga för att garantera den lagstadgade lagringstiden. PTS bör av denna anledning möjliggöra att leverantörerna tillåts att lagra data längre i syfte att säkerställa uppgifternas riktighet och tillgänglighet under lagringstiden.

Vidare är de gällande och föreslagna kraven vad avser uppgifter som lagras för brottsbekämpande ändamål mycket kostnadsdrivande. Samtidigt ersätts tillhandahållare endast för utlämnanden, trots att aktörerna lagrar de uppgifter som framgår av lagen. Det kan starkt ifrågasättas att endast utlämnanden ska ge aktörerna rätt till ersättning. I sammanhanget är det värt att notera att kostnaderna för lagring vida överstiger de kostnader aktörerna har för arbete med utlämnande, varför Telia anser att det är angeläget att frågan om ersättning för aktörernas anpassning till lagringskraven lyfts och att frågan utreds grundligt.

PTS svar:

Lagringstiden är reglerad i lagen om elektronisk kommunikation (LEK) 9 kap 22 § och PTS har mandat att meddela närmare föreskrifter om lagringstid enligt LEK 9 kap 23 §. PTS kan däremot inte förlänga de tider som gäller enligt lag. Enligt EU-domstolens praxis efter den s.k. Tele2-domen (förenade målen C-203/15 och C-698/15) behöver lagringstiden differentieras i förhållande till dess nödvändighet och proportionalitet vilket gör att den svenska regleringen behöver förhålla sig till denna praxis (se avsnitt 6.3 i SOU 2023:22 – Datalagring och åtkomst till elektronisk information).

Ersättning ska, enligt LEK 9 kap 29a §, utgå när uppgifter lämnas ut. Närmare bestämmelser om ersättning regleras i *PTS föreskrifter (2022:16) om ersättning för kostnader vid utlämnande av uppgifter som lagras eller bevaras för brottsbekämpande ändamål* och inte i de föreslagna föreskrifterna.

4. Närmare synpunkter på förslaget

4.1 1 kap.

4.2 2 kap. ord och uttryck

SKR framför att begrepp som tex 'brottsdatalagringsincident' bör användas sparsamt och alltid tydligt definieras.

Säkerhetspolisen (Säpo) framför att det nya begreppet brottsdatalagringsincident riskerar att föra tankarna till brottsdatalagen (2018:1177), inte till lagen (2022:482) om elektronisk kommunikation. Något annat begrepp hade därför varit att föredra även om Säpo inte har något konkret förslag. För att undvika missförstånd föreslår Säpo att PTS benämner aktuella incidenter som ”brottsdatalagringsincident enligt LEK” eller liknande.

PTS svar:

PTS noterar medskicket från SKR och Säpo.

4.3 4 kap. Identifiering och dokumentation av informationsbehandlingstillgångar, förbindelser och uppdragstagare

Telia ifrågasätter behovet av 4 kap. 1 § andra, tredje och fjärde stycket i föreskrifterna och anser att första stycket bör revideras. PTS bör enligt Telias mening inte reglera *hur* verksamhetsutövare ska identifiera och dokumentera sina tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare utan PTS bör reglera *att* tillhandahållare bör ha kontroll över sin verksamhet eftersom det bör ankomma på tillhandahållare själva att bestämma hur kontrollen över verksamheten bör bedrivas för att säkerställa kontroll över verksamheten och för att fastställa vad som omfattas av säkerhetsarbetet.

Telia anser vidare att det medför en stor risk och har och kommer att ha en direkt inverkan på tillhandahållarnas skyddsvärden att dokumentera informationen kring tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare på det sätt som följer av både nuvarande föreskrifter och förslaget till nya föreskrifter när det gäller brottsbekämpande ändamål och i andra fall där tillgångar,

informationsbehandlingstillgångar, förbindelser och uppdragstagare kan vara en del av tillhandahållarens verksamhet som omfattas av säkerhetsskyddslagen. Vidare är syftet med regelverket inte att reglera tillhandahållarnas säkerhetsskyddsarbete och redan av denna anledning bör föreskrifterna inte reglera dessa tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare. Ett alternativ är därmed att överväga om inte en undantagsbestämmelse som avser tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare som omfattas av säkerhetsskyddslagen bör införas.

Indikatorer

PTS svar

Kravet på identifiering, dokumentation samt bevarande av uppgifter är inte nytt och har i tidigare föreskriftsarbeten konsekvensutretts av PTS. Bestämmelsen är inte avsedd att innebära en ändring i sak jämfört med 4 kap 1 § i PTSFS 2022:11.

En aktuell och samlad bild över samtliga tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare är enligt PTS en förutsättning för att ha god kontroll över verksamheten och fastställa vad som omfattas av säkerhetsarbetet. Identifieringen och dokumentationen är utgångspunkten för arbetet med riskanalyser och vidtagandet av säkerhetsåtgärder. Utan detta är det inte möjligt att genomföra en korrekt riskanalys eller avgöra vilka åtgärder som behöver vidtas för att hantera eventuella risker. Dokumentationen är vidare en viktig del för att kunna följa upp och kontrollera säkerhetsarbetet, t.ex. ta reda på vilka säkerhetsåtgärder som har vidtagits för en viss tillgång eller vilka uppdragstagare som har utfört ett visst uppdrag även sedan en viss tid förflutit. Om en tillgång, informationsbehandlingstillgång eller förbindelse inte identifieras och dokumenteras finns det en risk att denna faller utanför det systematiska säkerhetsarbetet och över tid löper risk att bli exponerad för de risker som bristande säkerhetsarbete innebär. Sparade versioner av dokumentation är dessutom ett viktigt redskap i PTS tillsyn.

Vad gäller förhållandet till säkerhetsskyddslagen se avsnitt 3.2 ovan.

4.4 5 kap. Riskanalys

SKR framför att styrningen av riskanalysprocessen är mycket detaljerad och föreskrifterna uttrycker att verksamheten bör reducera risker snarare än acceptera dem. Samtidigt krävs uppskattning av sannolikhet, vilket är svårt och kan skapa osäkerhet.

Tillåt flexibilitet i val av metod och erkänn att kvalitativa bedömningar eller scenariobaserade analyser kan vara lämpliga. Hänvisa till etablerade metoder som ISO/IEC 27005 och MSB:s vägledningar.

Inför krav på återkommande revision av riskanalys samt dokumenterad riskacceptans och ansvarsfördelning.

PTS svar

Reglerna i 5 kap är inte nya och har konsekvensutretts av PTS i tidigare föreskriftsarbeten. Reglerna hindrar inte användning av etablerade standarder eller MSB:s vägledningar.

5 kap innehåller krav på återkommande riskanalyser, se 5 kap 1 §. Riskacceptans och ansvarsfördelning regleras i föreskrifternas 6 kap om riskhantering och åtgärder efter riskbedömning.

4.5 6 kap. Riskhantering och åtgärder efter riskbedömning

SKR framför att PTS borde Inkludera krav på att utvärdera effektiviteten i skyddsåtgärder (t.ex. enligt cybersäkerhetslagens 2 kap. §3 p.6) – revisioner, tester, övningar.

MSB vill framföra att det vore fördelaktigt om det i 6 kap. 4 § andra punkten tillförs ett ”och” alternativt ett ”eller” för att det ska vara tydligt hur de olika punkterna i paragrafen förhåller sig till varandra.

PTS svar:

I föreskrifternas 5 kap 5 § regleras att tillhandahållaren, vid genomförande av riskanalyser, ska beakta erfarenheter från tidigare inträffade säkerhets- och integritetsincidenter, allmänt uppmärksammade säkerhets- och integritetsincidenter samt aktuella och relevanta omvärldsföreteelser. Syftet med detta är att utvärdera effektiviteten av skyddsåtgärder. Det framgår även i föreskrifternas allmänna råd till 3 kap 5 § att penetrationstester bör användas som en del av säkerhetsarbetet för att följa upp de åtgärder som har vidtagits.

PTS lägger till ett ”och” för att förtydliga hur punkterna i paragrafen förhåller sig till varandra.

4.6 7 kap Åtkomst och behörighet

SKR framför att formuleringen *'system för hantering och kontroll av identiteter och behörigheter'* är vag och kan i praktiken innebära en mängd olika saker. Kravet bör antingen förtydligas eller kompletteras med ett råd.

PTS svar:

Kravet på system för hantering och kontroll av identiteter är inte nytt och synpunkter om detta besvarades av PTS i samband med den externa remissen *av PTS föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTSFS 2022:11).*

Det finns inget krav på hur bestämmelsen ska efterlevas. Det är upp till tillhandahållare att avgöra vilket eller vilka system som behövs för att säkerställa att bestämmelsen efterlevs. Systemet ska dock säkerställa att åtkomst endast medges i enlighet med tilldelade behörigheter och omfattar bl.a. att unika identiteter skapas, behörigheter tilldelas administrativt, användare loggar in och enbart kan göra det som behörigheterna tillåter i systemet. En tillhandahållare kan uppfylla regleringen genom ett ensamt system eller med flera olika system som samverkar kring hantering av identiteter, hantering av behörigheter, kontroll av inloggningsuppgifter och kontroll (enforcement) av behörigheterna.

4.7 8 kap Skyddsåtgärder mot oavsiktlig eller otillåten utplåning eller förlust

SKR framför att specifika åtgärder som hårdning (härdning) behöver tydligare definition: inaktivera onödiga tjänster, uppdatera mjukvara, säkra konfigurationer enligt CIS-/ISO-standarder.

PTS svar:

PTS anser att härdning är ett gängse uttryck inom vanlig cyberhygien och inte behöver definieras närmre.

4.8 9 kap Loggning

SKR framför att PTS ska beakta den tekniska paradoxen i 9 kap logghantering: användare med förhöjd behörighet kan behöva åtkomst till loggar; klargör mekanismer eller undantag

PTS svar:

Avsikten med föreskrifterna är inte att detaljstyra hur systemen ska fungera, utan att det ska finnas en genomtänkt process och mekanism för att användare har den behörighet de behöver för de uppgifter man utför.

4.9 10 kap Kryptering

Konsumentverket har noterat att 10 kap. 1 § *Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTSFS 2022:11)* tolkats långtgående av näringsidkare vid konsumenters kontakt med kundtjänst.

Näringsidkare får inte ställa upp formkrav för uppsägning, utövande av ångerrätt eller reklamation från konsument, exempelvis genom att kräva att konsumenten kontaktar näringsidkaren via telefon. Ett sådant krav utgör ett oskäligt avtalsvillkor. En långtgående tolkning av 10 kap. 1 § samt tillhörande allmänt råd kan innebära att e-post endast kan användas för kommunikation innehållandes allmänt hållen information. En sådan tolkning inskränker det konsumentskyddande regelverkets syften och konsumenterna drabbas negativt, särskilt drabbas de konsumenter som inte kan kommunicera via andra tekniker, exempelvis telefon. Konsumentverket bedömer att 10 kap. 1 § andra stycket i förslaget till föreskrifter och det allmänna rådet måste preciseras ytterligare för att bestämmelsen inte ska tolkas som så att alla uppgifter måste krypteras i samtliga fall och att näringsidkaren med anledning av detta tillämpar otillåtna formkrav.

Telia framför att kravet på kryptering enligt nuvarande och de föreslagna föreskrifterna innebär svårigheter i den praktiska hanteringen när kunder efterfrågar information om sina avtal och fakturor per e-post. Telia anser att det vore att föredra att PTS i föreskriften krävde att tillhandahållare erbjuder en lösning där uppgifterna skyddas, t.ex. en filöverföringstjänst med kryptering. Samtidigt önskar Telia att PTS i föreskriften öppnar upp för att skicka information över internet okrypterat när abonnenten samtycker till det eftersom ett flertal kunder kräver att uppgifter om fakturor skickas okrypterat till fakturainläsningscentraler.

SKR framför att PTS bör lyfta fram konkreta krav: kryptering i vila och transit, nyckelhantering, pseudonymisering där det är förenligt med lag och praxis (ISO 27002 kap. 8 och 10).

PTS svar:

10 kap 1 § ger utrymme att tolka föreskriften i enlighet med ett fullgott konsumentskydd, eftersom regeln möjliggör överföring av okrypterade uppgifter om det med hänsyn till uppgifternas art och sammanhang är osannolikt att överföring utan kryptering kan leda till en integritets- eller brottsdatalagringsincident. Paragrafen hindrar inte att uppgifter överförs okrypterat vid uppsägning, utövande av ångerrätt eller reklamation eller när kunden samtyckt till det.

Avsikten med föreskrifterna är inte att detaljstyra hur systemen ska fungera utan att det ska finnas en genomtänkt process och mekanism för att användare har den behörighet de behöver för de uppgifter man utför.

5. Regelrådets bedömning

Regelrådet har inga synpunkter på förslaget.

6. Kommerskollegiums bedömning

Kommerskollegium bedömde initialt att PTS ska anmäla det föreskriftsförslaget till kollegiet enligt förordning (1994:2029) om tekniska regler eftersom det innehåller krav på informationssamhällets tjänster. Kommerskollegium ändrade sin bedömning efter förtydligande från PTS om att föreskrifterna inte innebär några nya krav och att de anmäldes för *Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTSFS 2022:11).* PTS kommer därför inte att anmäla föreskrifterna enligt förordning (1994:2029) om tekniska regler.

Kommerskollegium bedömer att PTS inte behöver anmäla de föreslagna föreskrifterna varken enligt förordning (1994:2029) om tekniska regler, WTO:s TBT-avtal eller enligt förordning (2009:1078) om tjänster på den inre marknaden eftersom föreskrifterna inte innebär några nya krav.

7. Avslutning

PTS till tacka samtliga remissinstanser för inkomna synpunkter.