Vår referens: 25-19788

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

Post- och telestyrelsen (PTS) avser att med stöd av 1 kap. 8 § och 8 kap. 4-6 §§ förordningen (2022:511) om elektronisk kommunikation (FEK) utfärda föreskrifter om upphävande av Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTSFS 2022:11), nedan kallade säkerhetsföreskrifterna. PTS redovisar här sin utredning enligt förordning (2024:183) om konsekvensutredningar.

Förslag till föreskrifter bifogas, se bilaga 1.

Sammanfattning

NIS2-direktivet[1] föreslås genomföras i svensk rätt genom cybersäkerhetslagen (CSL). Lagen föreslås enligt propositionen träda ikraft den 15 januari 2026[2].

Enligt propositionen kommer 8 kap. 1-4 §§ lagen (2022:482) om elektronisk kommunikation (LEK) upphävas i samband med att CSL träder ikraft. Det innebär att PTS föreskriftsrätt enligt dessa bestämmelser också upphävs.

PTS bedömer därför att säkerhetsföreskrifterna ska upphävas i sin helhet. Föreskrifterna föreslås upphävas i samband med att CSL och förordningen om cybersäkerhet träder i kraft.

[1] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 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.

[2] prop. 2025/26:28, https://www.regeringen.se/contentassets/9ce81c9da34345b6ad95f10ce104da45/ett-starkt-skydd-for-natverks--och-informationssystem--en-ny-cybersakerhetslag-prop.-20252628.pdf

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

Bakgrund

Nuvarande reglering

Säkerhetsföreskrifterna innehåller bestämmelser om

- fredstida planering enligt 1 kap. 11 § LEK för totalförsvarets behov av elektroniska kommunikationer
- tekniska och organisatoriska åtgärder som enligt 8 kap. 1 § LEK, ska vidtas för att hantera risker som hotar säkerheten i nät och tjänster,
- rapportering enligt 8 kap. 3 § LEK av säkerhetsincidenter som har haft en betydande påverkan på kommunikationsnät och kommunikationstjänster,
- skyldighet enligt 8 kap. 4 § LEK för tillhandahållare att informera användare vid ett konkret och betydande hot om en säkerhetsincident,
- särskilda tekniska och organisatoriska åtgärder som enligt 8 kap. 5 LEK ska vidtas i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål,
- tekniska och organisatoriska åtgärder som enligt 8 kap. 6 § LEK ska vidtas för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av kommunikationstjänsten skyddas,
- innehållet i förteckningen över integritetsincidenter enligt 8 kap. 9 § LEK.

Bemyndigandena att föreskriva om ovanstående återfinns i 1 kap. 8 § och 8 kap. 4–6 §§ FEK.

8 kap. 1-4 §§ LEK genomför artikel 40 och 41 i Kodexen [3].

Kommande reglering

Efter en översyn av NIS-direktivet har ett nytt direktiv arbetats fram, Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 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, det s.k. NIS2- direktivet. NIS2-direktivet är tänkt att kompletteras med ett antal genomförandeakter. Genomförandeförordningen (EU) 2024/2690 som fastställer tekniska och metodologiska krav för

[3] , Europaparlamentets och rådets direktiv 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation.

riskhanteringsåtgärder för vissa verksamhetsutövare[4] trädde ikraft den 7 november 2024 och gäller direkt i medlemsstaterna.

Enligt regeringens proposition föreslås NIS2-direktivet genomföras med en ny cybersäkerhetslag och cybersäkerhetsförordning. Dessutom föreslås bland annat att 8 kap. 1-4 §§ LEK ska upphävas. PTS har i ett regeringsuppdrag fått i uppdrag att förbereda för uppgiften att kunna meddela föreskrifter om säkerhetsåtgärder, skyldigheten att föra register över domännamn, vad som utgör en betydande incident samt skyldighet att informera vid betydande incidenter och betydande cyberhot för att förbereda genomförandet av NIS2-direktivet. Uppdraget omfattar bl.a. sektorn digital infrastruktur i vilken verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster i Sverige ingår.

Bestämmelser som rör

- fredstida planering enligt 1 kap. 11 § LEK,
- särskilda tekniska och organisatoriska åtgärder som enligt 8 kap. 5 LEK ska vidtas i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål,
- tekniska och organisatoriska åtgärder som enligt 8 kap. 6 § LEK ska vidtas för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av kommunikationstjänsten skyddas och
- innehållet i förteckningen över integritetsincidenter enligt 8 kap. 9 § LEK, kommer även fortsatt att regleras i LEK. Enligt propositionen kommer dessa lagrum emellertid att få nya paragrafnummer.

Enligt propositionen kommer upphävandet av 8 kap. 1-4 §§ LEK omfattas av övergångsbestämmelser som innebär att äldre bestämmelser fortfarande gäller för överträdelser som skett före ikraftträdandet.

Varför upphävs föreskrifterna?

Genom NIS2-direktivet upphävs artikel 40 och 41 i kodexen (säkerhet i nät och tjänster) från och med den 18 oktober 2024 och ersätts då med bestämmelserna

[4] Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade säkerhetstjänster, leverantörer av marknadsplatser online, sökmotorer och för plattformar för sociala nätverkstjänster samt kvalificerade tillhandahållare av betrodda tjänster.

som följer av NIS2-direktivet (bl.a. avseende riskhanteringsåtgärder och incidentrapportering). Artikel 40 och 41 i kodexen ligger till grund för bestämmelserna i 8 kap. 1–4 §§ LEK.

Alternativa lösningar

Med anledning av att en ny lag om cybersäkerhet kommer att träda i kraft, som genomför NIS2-direktivet i Sverige (samt en ny förordning om cybersäkerhet), bedömer PTS att säkerhetsföreskrifterna behöver upphävas i sin helhet. Anledningen är att så stora delar av säkerhetsföreskrifterna till följd av NIS2-direktivet och CSL måste upphävas att resterande delar skulle komma att bli svåra att läsa, ta till sig och tillämpa. Att behålla delar av föreskrifterna är därmed inte ett möjligt alternativ.

Rättsliga förutsättningar

Bemyndigande

PTS får enligt 1 kap. 8 § och 8 kap. 4-6 §§ FEK meddela föreskrifter om den fredstida planeringen för totalförsvarets behov av elektroniska kommunikationer och om säkerhet i nät och tjänster.

Innan föreskrifter meddelas som avser den fredstida planeringen för totalförsvarets behov av elektroniska kommunikationer ska PTS samråda med Försvarsmakten och Myndigheten för samhällsskydd och beredskap.

Yttrande från Regelrådet

PTS bedömer att Regelrådets granskning av konsekvensutredningen skulle sakna betydelse och avstår därför enligt 13 § tredje stycket förordningen om konsekvensutredningar från att ge Regelrådet tillfälle att yttra sig.

Överensstämmelse med EU-rätt

Upphävandet av föreskrifterna bedöms överensstämma med och inte gå utöver de skyldigheter som följer av Sveriges anslutning till EU.

Aktörer som berörs av regleringen

De aktörer som berörs av upphävandet av säkerhetsföreskrifterna är leverantörer av elektroniska kommunikationsnät och elektroniska kommunikationstjänster med tillhörande faciliteter och tjänster samt annan radioanvändning.

Konsekvenser av regleringen

Föreskrifterna om upphävande föreslås innehålla övergångsbestämmelser. Enligt övergångsbestämmelserna ska föreskrifterna fortsätta att gälla för överträdelser som har skett före upphävandet. Det är i linje med regeringens förslag att aktuella bestämmelser i LEK ska omfattas av liknande övergångsbestämmelser.

De aktörer som anges ovan kommer efter upphävandet inte längre att behöva tillämpa säkerhetsföreskrifterna om inte övergångsbestämmelserna är tillämpliga. Detta skulle i sig ha kunnat innebära framtida kostnadsbesparingar för aktörerna, men som behandlats tidigare kommer aktörerna i stället att omfattas av den kommande cybersäkerhetslagen med tillhörande förordning med nya föreskrifter som PTS har fått i uppdrag[5] att förbereda för med utgångspunkt i cybersäkerhetsregleringen. Aktörerna kommer även fortsättningsvis att omfattas av de bestämmelser som kvarstår i LEK dvs. krav på särskilda tekniska och organisatoriska åtgärder som ska vidtas i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål, tekniska och organisatoriska åtgärder som ska vidtas för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av kommunikationstjänsten skyddas, innehållet i förteckningen över integritetsincidenter, samt fredstida planering för totalförsvarets behov av elektroniska kommunikationer.

PTS bedömning är att åtminstone motsvarande krav som ställs idag enligt säkerhetsföreskrifterna kommer att gälla genom CSL, LEK och föreskrifter som PTS arbetar med. Arbete pågår med dessa föreskrifter och särskilda konsekvensutredningar kommer att utarbetas till respektive föreskrifter i det fall nya krav kommer att ställas på aktörerna. Nya föreskrifter och allmänna råd om skyddsåtgärder för lagrade uppgifter för brottsbekämpande ändamål och för behandlade uppgifter och föreskrifter om den fredstida planeringen för totalförsvarets behov av elektroniska kommunikationer planeras att beslutas inom kort efter upphävandet. Föreskrifter som ska förberedas enligt regeringsuppdraget kommer inte att kunna beslutas i anslutning till att CSL träder ikraft med hänsyn till det omfattande arbetet med att analysera den nya regleringen.

PTS utgår från att de grundläggande kraven i CSL med tillhörande förordning under denna mellanperiod kan ligga till grund för att aktörerna vidtar lämpliga säkerhetsåtgärder och rapporterar incidenter samt informerar användare vid hot om incidenter. De upphävda föreskrifterna gäller fortfarande för överträdelser som har skett före upphävandet.

[5] Uppdrag till Post- och telestyrelsen att förbereda genomförandet av NIS 2-direktivet, Fi2025/01676.

Upphävandet i sig kan med andra ord inte sägas leda till några större konsekvenser för aktörerna, men den nya regleringen leder till att aktörer kommer att behöva anpassa sin verksamhet efter de nya kraven som ställs. Upphävandet bedöms inte heller få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.

Ikraftträdande och informationsinsatser

Föreskrifter om upphävande av säkerhetsföreskrifterna föreslås träda i kraft den 15 januari 2026 när PTS föreskriftsbemyndigande enligt LEK och FEK upphävs och ersätts av ny reglering.

Informationsinsatser genomförs av PTS i samband med den nya regleringens ikraftträdande, och det blir då naturligt att samtidigt informera om att de tidigare meddelade säkerhetsföreskrifterna upphör att gälla. De upphävda föreskrifterna gäller dock som angetts ovan fortfarande för överträdelser som har skett före upphävandet.

Kontaktuppgifter

Kontaktpersoner:

Mats Jönsson, enheten för säkra nät och tjänster, mats.jonsson@pts.se

Sofie Sandell, rättsavdelningen, sofie.sandell@pts.se