Försvarsdepartementet
Referens: Fö2026/00576

Vår referens: 26-3776

Remissvar över Europeiska kommissionens cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS 2-direktivet (EU 2022/2555) KOM (2026)11,13

Post- och telestyrelsen (PTS) yttrar sig härmed över remissen av Europeiska kommissionens cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) (CSA2) samt riktade ändringar i NIS2-direktivet (EU 2022/2555) KOM (2026)11,13.

Sammanfattning

PTS välkomnar i huvudsak kommissionens ambition att förenkla, förtydliga och harmonisera EU:s cybersäkerhetsregelverk samt minska den administrativa bördan för berörda aktörer. PTS ser positivt på att ENISA:s roll uppdateras, att cybersäkerhetscertifiering utvecklas som verktyg för att visa efterlevnad och att hanterade säkerhetstjänster, cyberhygien, digitala plånböcker och undervattenskablar tydligare omfattas av regelverket.

PTS anser att förhållandet mellan CSA2, NIS2 och DNA behöver förtydligas, särskilt när det gäller kontroll och upprätthållande av kraven på IKT-leveranskedjor. PTS anser även att detaljerade tekniska krav inte bör fastställas generellt på EU-nivå, utan även fortsättningsvis bör anpassas av tillhandahållarna utifrån respektive nät, arkitektur och riskbild.

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

PTS anser vidare att regleringen av högriskleverantörer riskerar att skapa dubbelreglering i förhållande till befintliga svenska tillståndsvillkor. Uteslutning av specifika högriskleverantörer bör därför framöver hanteras genom CSA2, medan nationella säkerhetskrav som inte täcks av CSA2 fortsatt kan behöva regleras genom tillståndsvillkor som har stöd i lagen (2022:482) om elektronisk kommunikation (LEK).

När det gäller NIS2-tillägget ser PTS positivt på flera föreslagna ändringar, men anser att definitionen av tillhandahållare av undervattenskablar behöver förtydligas. PTS ser även en risk att det nya storleksbegreppet för midcapföretag kan minska antalet väsentliga tillsynsobjekt och därmed begränsa möjligheterna till planerad tillsyn.

Synpunkter

Title I ”General Provisions”

PTS noterar att vissa av definitionerna 42–50 är bristfälliga. PTS har redan lämnat specifika synpunkter till Regeringskansliet vilka därför inte utvecklas ytterligare i detta yttrande.

Title III EUROPEAN CYBERSECURITY CERTIFICATION FRAMEWORK

Denna del handlar om EU:s gemensamma ramverk för cybersäkerhetscertifiering. Syftet är att göra certifiering mer användbart, enhetligt och effektivt för produkter, tjänster, processer, hanterade säkerhetstjänster och organisationers cyberhygien. Certifiering ska kunna användas som ett verktyg för att visa efterlevnad av EU:s cybersäkerhetskrav, bland annat enligt NIS2-direktivet, och samtidigt minska fragmentering och administrativa bördor på den inre marknaden. PTS ser positivt på förenklingarna i EU-certifieringen och välkomnar de nya förslagen på hanterade säkerhetstjänster och cyberhygiencertifiering.

Title IV SECURITY OF ICT SUPPLY CHAINS

Genom dessa förslag införs ett nytt EU-ramverk för att hantera cybersäkerhetsrisker i kritiska IKT-leveranskedjor. Förslaget ger kommissionen möjlighet att identifiera viktiga IKT-tillgångar, bedöma risker kopplade till tredjeländer och högriskleverantörer samt besluta om riskreducerande åtgärder för berörda aktörer. Reglerna är särskilt relevanta för kritiska sektorer och elektroniska kommunikationsnät.

PTS synpunkter på art 98–109 i CSA2

Bakgrund och koppling till DNA/NIS2

För att anmäla sig enligt DNA krävs att tillhandahållaren uppfyller kraven i artikel 9.4. (d) i DNA vilken föreskriver att kraven avseende IKT leveranskedjan i artiklarna 98 – 109 i CSA2 ska vara uppfyllda.

Detta innebär att den behöriga myndigheten för CSA2 eventuellt kommer att skicka en begäran till den behöriga myndigheten för DNA för att upphäva anmälan eller spektrumtillståndet för det fall tillhandahållaren inte uppfyller kraven i CSA2 art 98–102.

Om tillhandahållaren är anmäld under DNA i samma medlemsstat som beslutet angående CSA2-kraven fattas kan samarbetet bli effektivt. En förutsättning för en god tillämpning är att det ska vara samma myndighet som är behörig för både digital infrastruktur enligt NIS2-direktivet, DNA och CSA2:s artiklar 98–109. I de fall myndigheter från olika EU-stater och potentiellt även EU-kommissionen är inblandade i denna process är ansvarsfrågan otydlig, och det är svårt att se hur samarbetet ska fungera effektivt och ändamålsenligt. Erfarenheten från 5G verktygslåderekommendationen har visat att medlemsstaterna gör olika bedömningar vad gäller användningen av högriskleverantörer. PTS anser att det behövs ett tydliggörande (i DNA och/eller CSA2) som innebär att kraven i CSA2 kan kontrolleras och upprätthållas på nationell nivå i varje medlemsstat oavsett i vilken stat som anmälan enligt DNA gjorts.

Artikel 100.4. (a)

Det går att ifrågasätta effekten av denna restriktion när EU-standardiseringen ändå är en öppen och transparent process. De bidrag som kommer från tredje länder kan ändå vara värdefulla.

Artikel 103.2. (b) till (g)

PTS anser att tekniska åtgärder av dessa slag blir svåra att peka ut i en genomförandeordning som ska gälla alla nätverkstyper, tillhandahållare och arkitekturer. Specifika tekniska åtgärder och konfigurationer bör förbli under tillhandahållarens ansvar att genomföra i enlighet med NIS2-direktivet, baserat på de specifika förhållanden som är unika för varje tillhandahållare. Det skapar otydlighet då CSA2 sätter krav som blir samma för alla, vilket gör att verksamhetsutövare inte kan anpassa de tekniska åtgärderna till sina unika och specifika förhållanden (vilket de ska göra enligt kraven i NIS2-direktivet). Ett sätt att kunna bibehålla tydliga gränser mellan NIS2-direktivet och CSA2:s IKT-leveranskedjeramverk skulle kunna vara att enbart använda strategiska kriterier (icke tekniska), dvs att en viss leverantör är tillåten eller inte. En potentiell kompromiss skulle kunna vara en procentuell begränsning på användningen i vissa domäner (icke nyckeltillgångar/ non key-assets).

PTS konstaterar att den föreslagna regleringen för att hantera säkerhetsrisker och utfasning i CSA2 av så kallade högriskleverantörer i telekominfrastruktur i hög grad överensstämmer med den inriktning som Sverige redan tillämpar. De krav som föreslås återspeglar den logik som PTS har implementerat i gällande tillståndsvillkor i flera frekvensband. Tillståndsvillkoren har stöd i LEK, där hänsyn till Sveriges säkerhet utgör en grund för tillståndsgivningen.

CSA2 gör regleringen av högriskleverantörer till en direkt tillämplig förordning på EU-nivå. Enligt förslaget ska användning av specificerade högriskleverantörer uttryckligen förbjudas i listor upprättade av EU-kommissionen. Det kan ifrågasättas om sådana beslut, som Sverige tidigare hävdat ska fattas med hänsyn till nationell säkerhet, ska överföras till EU-kommissionen. Även om möjligheten finns kvar i CSA2 att tillämpa krav utöver det som finns i regelverket måste dessa förmodligen motiveras för EU. Vidare framgår det att bristande regelefterlevnad kan leda till att operatörens spektrumrättigheter återkallas.

PTS anser att fortsatt reglering av leverantörsberoenden som villkor i enskilda frekvenstillstånd, samtidigt som samma säkerhetsrisker från högriskleverantörer nu avses omhändertas av CSA2, skapar en oacceptabel dubbelreglering och komplexitet avseende sanktionsmekanismer och tvingande tidslinjer.

Det är däremot PTS bedömning att CSA2 inte fullt ut kan ersätta nuvarande säkerhetskrav i tillståndsvillkoren som reglerar att funktioner och personal ska placeras nationellt, om nätens centrala funktioner är beroende av dessa. Inte heller kräver CSA2 en redundant nationell källa för tidsreferens. Dylika specifika krav för att trygga Sveriges säkerhet kan därmed även fortsättningsvis behöva regleras genom LEK-stödda tillståndsvillkor. Mot bakgrund av ovanstående anser PTS att bestämmelser som rör uteslutning av specifika högriskleverantörer ur telekominfrastrukturen framöver bör hanteras enbart genom CSA2. Vid en svensk anpassning av regelverket bör således krav på leverantörsberoenden flyttas ut ur LEK och ur de enskilda frekvenstillstånden.

Synpunkter på NIS2-tillägget

Artikel 3

I artikel 3 punkt 1 a införs ett nytt storleksbegrepp för ”midcapföretag”. PTS anser att storlekströskeln är väldigt hög och befarar att flera av de tillsynsobjekt som idag definieras som väsentliga i stället kommer att definieras som viktiga vilket innebär att PTS möjligheter att göra planerad tillsyn begränsas.

PTS ser positivt på att DNS-tjänster tas bort från Punkt 1 b, vilket innebär att DNS-tjänster som är små eller mikroföretag inte längre faller inom tillämpningsområdet.

Artikel 21

PTS ser positivt på att entiteter som regleras av NIS2-direktivet ska kunna erhålla certifikat för cybersäkerhetscertifiering enligt NIS2-direktivet som utvecklats inom det europeiska ramverket.

PTS ser även positivt på att EU-kommissionen ska ta fram riktlinjer för tillämpning av de säkerhetskrav i leveranskedjan som de entiteter som omfattas av NIS2-direktivet överför till sina leverantörer.

Artikel 21 (5) (b)

Kommissionen har föreslagit en ny punkt i artikel 21 (5) (b) som anger att om kommissionen antar genomförandeakter som avses i första och andra styckena i denna punkt, får medlemsstaterna inte införa några ytterligare tekniska, metodologiska eller sektorsspecifika krav för de åtgärder som avses i artikel 21.2 i direktiv (EU) 2022/2555 på de enheter som omfattas av dessa genomförandeakter."

PTS anser att det förslagna tillägget i artikel 21 5 b ska utgå då det är av stor vikt att Sverige fortsatt har möjlighet att införa nationella och sektorspecifika krav för de sektorer som omfattas av direktivet, särskilt för tillhandahållare av allmänna elektroniska kommunikationsnät och tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster eftersom villkoren för dessa entiteter är speciella för ett land som Sverige och det är viktigt att kunna anpassa reglerna efter det.

Artikel 37a

PTS ser positivt på att ENISA får en ny roll som stödjer medlemsstaterna i tillsynen av entiteterna.

Bilaga 1

PTS ser positivt på att tillhandahållare av den Europeiska Digitala Plånboken och tillhandahållare av den Digitala företags Plånboken läggs till i sektorn Digital infrastruktur.

PTS ser vidare positivt på att tillhandahållare av undervattenskablar föreslås omfattas. Detta innebär att även de tillhandahållare som faller utanför definitionen av "tillhandahållare av allmänna elektroniska kommunikationsnät" och "tillhandahållare av allmänt tillgängliga elektroniska kommunikationsnät" nu kommer att omfattas och därmed ska rapportera incidenter och vidta säkerhetsåtgärder. PTS vill dock framhålla att det är viktigt med en tydlig definition av tillhandahållare av undervattenskablar.

Detta yttrande har beslutats av divisionschef Catarina Wretman. I ärendets slutliga handläggning har även handläggaren Sabrine Wennberg (föredragande), cybersäkerhetsstrategen James Christie, enhetschef Isabelle Westerlund, enhetschef Magnus Leijel, verksjurist Per Andersson, verksjurist Sofie Sandell, systemvetare Åsa Gihl, jurist Maria Wiberg och avdelningschef Patrik Bylund deltagit.