

Er referens: Fö2024/01550

Försvarsdepartementet

Vår referens: 24-12569

Post- och telestyrelsens (PTS) remissvar avseende slutbetänkandet Motståndskraft i samhällsviktiga tjänster (SOU 2024:64)

Sammanfattning

PTS välkomnar utredningens förslag om att en ny bestämmelse om sekretess ska införas i offentlighet- och sekretesslagen (2009:400) för incidentrapporter och instämmer med utredningens slutsats att en ny bestämmelse om sekretess behövs. Incidentrapporter är ett viktigt underlag i PTS arbete med att bedöma tillsynsinsatser och tillsynsbehov. Det är därför angeläget att verksamhetsutövarna har hög tilltro till att deras känsliga uppgifter ges ett fullgott skydd mot bl.a. antagonister som försöker kartlägga sårbarheter i verksamhetsutövarnas system.

PTS instämmer med utredningens konstaterande att innebörden av begreppen samhällsviktig tjänst och samhällsviktig verksamhet är likartad och språkligt närliggande varandra men inte identisk. Därför är det enligt PTS positivt att det i förslaget till lag om motståndskraft hos samhällsviktiga tjänster (LOM) särskiljs mellan begreppen samhällsviktig *tjänst* och samhällsviktig *verksamhet* så att samhällsviktig tjänst används för att beskriva tjänster som kan träffas av kraven i CER-direktivet¹ för att särskilja dessa från begreppet samhällsviktig

¹ Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

verksamhet som används i förordningen (2022:524) om statliga myndigheters beredskap. Det svenska beredskapssystemet bör inte kopplas till CER-direktivet som avser att reglera den inre marknaden och därmed inte reglerar frågor som rör beredskapssystemen i medlemsstaterna. Beredskapsfrågor ligger istället många gånger nära begreppet nationell säkerhet, vilket tillhör medlemsstaternas nationella regleringskompetens enligt artikel 4.2 FEU.²

Utformningen av LOM innebär att kritiska verksamhetsutövare i den digitala sektorn (som inte omfattas av 3–6 kap. LOM) inte får samma rättighet att begära utdrag ur belastningsregistret som de kritiska verksamhetsutövare som omfattas av samtliga kapitel i LOM. PTS menar att detta innebär att CER-direktivet och NIS2-direktivets³ skyldigheter inte är likvärdiga. Myndigheten anser därför att motsvarande regler om bakgrundskontroller som finns i 6 kap. LOM även bör införas i förslaget till lag om cybersäkerhet (CSL) för kritiska verksamhetsutövare i den digitala sektorn.

Vidare föreslår PTS några förtydliganden i förslaget till lagtext bland annat beträffande begreppet "alla relevanta risker" i 1 kap. 11 § LOM och i 2 kap. 3 § LOM rörande att verksamhetsutövaren ska ange till tillsynsmyndigheten om denne har någon samhällsviktig tjänst som är säkerhetskänslig. PTS anser även att det i 2 kap. 3 § LOM behövs förtydligande av vad som ska framgå av tillsynsmyndighetens beslut när tillsynsmyndigheten utser en kritisk verksamhetsutövare som är verksam i sektorn digital infrastruktur och i ytterligare en sektor som omfattas av LOM. PTS önskar vidare att det i förarbetena förtydligas bland annat vad som ska gälla vid identifieringen av kritiska verksamhetsutövare i några specifika situationer.

Slutligen anser PTS att det föreslagna anslaget för arbetet med sektorn rymden är tillräckligt utifrån de arbetsinsatser myndigheten kan bedöma i nuläget.

² Fördraget om Europeiska Unionen

³ 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.

1. Introduktion

PTS har enligt 1 § förordningen (2007:951) med instruktion för Post- och telestyrelsen ett samlat ansvar inom postområdet och området för elektronisk kommunikation. Utifrån PTS ansvarsområde lämnar myndigheten i detta yttrande synpunkter på slutbetänkandet Motståndskraft i samhällsviktiga tjänster, SOU 2024:64.

2. Synpunkter

2.1 Nationell riskbedömning

PTS anser att det bör förtydligas i 1 kap. 11 § LOM hur "alla relevanta risker" ska tolkas.

Relevant avsnitt i slutbetänkandet 6.1 Nationell riskbedömning

I 1 kap. 11 § LOM ställs krav på att regeringen eller en utpekad myndighet ska göra en nationell riskbedömning och att vid framtagandet av denna ska alla relevanta risker beaktas. PTS menar att det inte är helt klart hur begreppet "alla relevanta risker" ska tolkas och att någon form av ledning i bedömningen är önskvärd.

I artikel 5 i CER-direktivet finns en uppräkningslista av vilka relevanta risker medlemsstaternas riskbedömningar ska redogöra för. För en ökad tydlighet vid bedömningen föreslår PTS att skrivningen i 1 kap. 11 § tredje stycket LOM ändras till "relevanta risker kopplade till naturolyckor och risker orsakade av människan, inbegripet risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot eller andra antagonistiska hot, inklusive terroristbrott enligt Europaparlamentets och rådets direktiv (EU) 2017/541" eller att åtminstone en hänvisning till uppräkningslistan i artikel 5 i CER-direktivet finns med i 1 kap. 11 § LOM.

2.2 Identifiering av kritiska verksamhetsutövare

PTS anser att det bör förtydligas i propositionen till LOM att en verksamhetsutövare inom sektorn digital infrastruktur kan pekas ut som kritisk även om den har huvudsakligt etableringsställe i annat EU medlemsland.

Relevant avsnitt i slutbetänkandet 6.3 Krav för identifiering av kritiska verksamhetsutövare

Enligt 2 kap. 2 § LOM krävs att verksamhetsutövaren, för att identifieras som kritisk, tillhandahåller en samhällsviktig tjänst i eller till Sverige, har kritisk infrastruktur belägen i Sverige och att en incident skulle få en betydande störande effekt. En sådan kritisk verksamhetsutövare enligt LOM är enligt 2 kap. 1 § 8 CSL också väsentlig enligt CSL.

För att en gränsöverskridande verksamhetsutövare ska omfattas av CSL krävs enligt 1 kap. 6 § CSL att det huvudsakliga etableringsstället finns i Sverige. Det räcker inte med att ha kritisk infrastruktur belägen i Sverige. Dessa aktörer kommer därmed att omfattas av LOM på grund av att de har infrastruktur i Sverige samtidigt som CSL inte kommer reglera deras riskhanteringsåtgärder och incidentrapportering. Istället kommer dessa verksamhetsutövare att omfattas av den nationella regleringen som genomför NIS2-direktivet i den stat där de har sitt huvudsakliga etableringsställe.

Såsom PTS uppfattar förslaget till 1 kap. 6 § CSL i kombination med 2 kap. 2 § LOM kommer en verksamhetsutövare med sitt huvudsakliga etableringsställe i en annan medlemsstat kunna pekas ut som kritisk enligt LOM. Verksamhetsutövaren blir därmed att anse såsom väsentlig verksamhetsutövare i den stat där det huvudsakliga etableringsstället finns. Beslutet om identifiering behöver enligt 2 kap. 1 § LOM tillställas den utländska verksamhetsutövaren och tillsyn enligt NIS2-regelverket kommer utövas av tillsynsmyndigheten i etableringsstaten. Samma gäller för det omvända, där en verksamhetsutövare har huvudsakligt etableringsställe i Sverige med kritisk infrastruktur i en annan medlemsstat.

PTS önskar förtydliganden avseende hur det gränsöverskridande samarbetet mellan medlemsstaterna bör utformas vid beslutsfattande vid identifiering av kritiska verksamhetsutövare och även vid tillämpning av övriga kapitel i LOM som omfattar digital infrastruktur.

2.3 Tillhandahållande av tjänster inom ramen för unionens rymdprogram ingår inte i sektorn rymden

PTS föreslår att det förtydligas i propositionen att infrastruktur som ägs, förvaltas eller drivs av unionen eller för unionens räkning inom ramen för dess rymdprogram inte omfattas av LOM.

Relevant avsnitt i slutbetänkandet 6.3 Krav för identifiering av kritiska verksamhetsutövare och 6.4 Betydande störande effekt

Enligt 2 kap 2 § LOM är ett av kriterierna för att en verksamhetsutövare ska identifieras som kritisk att man tillhandahåller en tjänst som omfattas av någon av sektorerna som finns i bilagan till CER-direktivet. I skäl 5 till CER-direktivet anges en viktig avgränsning av kriteriet när det gäller sektorn rymden i och med att det förtydligas att infrastruktur som ägs, förvaltas eller drivs av unionen eller för unionens räkning inom ramen för dess rymdprogram, inte omfattas av CER-direktivet.

PTS ser detta som en viktig avgränsning av vilka verksamhetsutövare som kan identifieras som kritiska och anser att det borde framgå tydligt i förarbetena till LOM att dessa verksamhetsutövare inte omfattas av tillämpningsområdet för sektorn rymden.

2.4 Upplýsningsskyldighet för kritiska verksamhetsutövare

PTS föreslår att 2 kap. 3 § LOM kompletteras med en upplýsningsskyldighet för tillsynsmyndigheten rörande att verksamhet som omfattas av säkerhetsskyddslagen är undantagen från LOM och att verksamhetsutövaren ska ange till tillsynsmyndigheten om sådan samhällsviktig tjänst finns.

Relevant avsnitt i slutbetänkandet 6.5 Beslut om identifiering och underrättelse om skyldigheter

Det finns inte någon uttalad skyldighet i LOM för verksamhetsutövare att invända att del av tjänsten är säkerhetskänslig. Det framgår dock indirekt av 2 kap. 4 § LOM att om en verksamhetsutövare anger att tjänsten till någon del träffas av bestämmelserna i säkerhetsskyddslagen ska ansvarig tillsynsmyndighet enligt LOM skicka en underrättelse om det till ansvarig tillsynsmyndighet enligt säkerhetsskyddslagen. PTS anser att det i LOM tydligare bör framgå att en sådan invändning ska göras om säkerhetskänslig verksamhet finns. En möjlig placering av en sådan bestämmelse kan vara i den paragraf som reglerar vad tillsynsmyndigheten i sitt beslut om identifiering ska upplysa verksamhetsutövaren om. PTS föreslår därför att en tredje punkt i första stycket till 2 kap. 3 § LOM läggs till med följande lydelse:

”att 3–6 kap. inte gäller för den del av den samhällsviktiga tjänsten som är säkerhetskänslig och att den kritiska verksamhetsutövaren i en sådan situation ska invända till tillsynsmyndigheten att sådan tjänst finns.”

2.5 Förtydligande angående undantag för vissa sektorer

PTS anser att det behövs förtydligande av vad som ska framgå av beslutet när tillsynsmyndigheten utser en kritisk verksamhetsutövare som är verksam både i sektorn digital infrastruktur och även i ytterligare minst en sektor som omfattas av samtliga kapitler i LOM.

Relevant avsnitt i slutbetänkandet 6.5 Beslut om identifiering och underrättelse om skyldigheter

En verksamhetsutövare som är identifierad som kritisk verksamhetsutövare och som är verksam inom sektorn digital infrastruktur ska enligt 2 kap 3 § sista stycket LOM inte omfattas av kap 3 – 6 samma lag. Om en sådan kritisk verksamhetsutövare även är verksam inom en annan sektor, till exempel energisektorn, och blir utpekad som kritisk verksamhetsutövare enligt LOM även här, uppstår en otydlighet huruvida verksamhetsutövaren inte överhuvudtaget ska omfattas av kap 3-6 LOM även om denne är utpekad inom sektorn energi.

CSL ställer inte upp säkerhetskrav på de fysiska delarna för sektorer som inte är digital infrastruktur på samma sätt som CER-direktivet varför detta vore en oönskad konsekvens.

PTS föreslår att följande text läggs till 2 kap 3 § sista stycket LOM för att undanröja denna otydlighet:

”Om den kritiska verksamhetsutövaren är verksam inom sektorerna bankverksamhet, finansmarknadsinfrastruktur eller digital infrastruktur ska det framgå av beslutet att verksamhetsutövaren inte är skyldig att vidta sådana åtgärder som följer av 3–6 kap **för den verksamheten.**”

2.6 Bakgrundskontroller

PTS föreslår att regler om bakgrundskontroller även bör införas i CSL för kritiska verksamhetsutövare i den digitala sektorn.

Relevant avsnitt i slutbetänkandet 9.3.3 Befattningsanalys utgör grunden för vilka som ska bakgrundskontrolleras, 9.3.4 När ska en bakgrundskontroll genomföras?, 9.3.5 Bakgrundskontrollens innehåll och omfattning.

PTS ser positivt på utredningens förslag i 6 kap. LOM om regler kring bakgrundskontroll. Enligt PTS är det emellertid problematiskt att verksamhetsutövare i sektorn digital infrastruktur inte omfattas av dessa krav eftersom kapitel 3–6 LOM inte gäller för dem.

Enligt skäl 9 i CER-direktivet bör samstämmighet säkerställas med NIS2-direktivet. Orsaken till att sektorn för digital infrastruktur i skäl 20 undantas från skyldigheter i CER-direktivet uppges vara för att undvika dubbelarbete och onödig administrativ börda samt för att skyldigheter att vidta riskhanteringsåtgärder enligt NIS2-direktivet minst är likvärdiga med motsvarande skyldigheter enligt CER-direktivet.

Genom att CSL inte möjliggör samma rättighet att begära utdrag ur belastningsregistret som LOM gör menar PTS att CER-direktivet och NIS2-direktivets skyldigheter inte är likvärdiga. PTS anser därför att regler om bakgrundskontroller i 6 kap LOM bör införas även i CSL för kritiska verksamhetsutövare i den digitala sektorn.

2.7 Tillsynsmyndighetens undersökningsbefogenheter

PTS föreslår att en ny rubrik med lydelsen "Uppgiftsskyldighet" införs ovanför 7 kap. 3 § LOM för att tydliggöra att det finns en uppgiftsskyldighet för kritiska verksamhetsutövare i paragrafen.

Relevant avsnitt i slutbetänkandet 10.5 Tillsynsmyndighetens undersökningsbefogenhet.

PTS föreslår att en ny rubrik med lydelsen "Uppgiftsskyldighet" införs ovanför 7 kap. 3 § LOM för att tydliggöra att det finns en uppgiftsskyldighet för kritiska verksamhetsutövare i paragrafen. Den nuvarande rubriken föreslås flyttas ned till att gälla 7 kap. 4 § och efterföljande paragrafer.

För sektorn digital infrastruktur gäller inte skyldigheterna i 3–6 kapitlet och med en sådan rubrik blir det tydligt att det finns skyldigheter som gäller även för denna sektor när verksamhetsutövarna har identifierats. Detta framgår inte helt tydligt i betänkandet, jfr. författningskommentaren till 2 kap. 3 § 2 st. som nämner att dessa verksamhetsutövare endast ska identifieras, utan att skyldigheter uppstår för dem.

2.8 Ekonomiska konsekvenser

PTS anser att det föreslagna anslaget är tillräckligt utifrån de arbetsinsatser myndigheten kan bedöma i nuläget.

Relevant avsnitt i slutbetänkandet: 15:5.2 Ekonomiska konsekvenser för tillsynsmyndigheterna

Av utredningens förslag framgår att PTS bör ges ett förstärkt anslag för löpande kostnader med en miljon kronor per år eftersom PTS ska utföra samtliga uppgifter enligt CER-direktivet för sektorn rymden.

PTS kommer att behöva identifiera kritiska verksamhetsutövare inom sektorn digital infrastruktur och upprätta en förteckning över dessa samt bidra till Myndigheten för samhällsskydd och beredskaps (MSB) nationella riskbedömning. Tillsyn över den digitala infrastrukturen sker enligt NIS2-direktivet.

När det gäller sektorn rymden ska PTS även för denna sektor identifiera verksamhetsutövare och upprätta en förteckning men även vara tillsynsmyndighet enligt LOM samt bidra till MSB:s nationella riskbedömning.

PTS har i tidigare remissvar till delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18) framfört att finansiering behövs för att utföra de uppgifter som påförs PTS enligt CSL och om det behovet tillgodoses är den finansieringen tillräcklig för de ytterligare arbetsinsatser som PTS påförs enligt LOM när det gäller den digitala sektorn och utifrån de arbetsinsatser som PTS kan bedöma nu utifrån slutbetänkandet.

Vad gäller det förstärkta anslaget för sektorn rymden som föreslås anser PTS att det är tillräckligt utifrån de arbetsinsatser som PTS kan bedöma hittills i sin utredning med att identifiera och tolka sektorn rymden. PTS jobbar fortsatt med utredningsarbete kring sektorn rymden och då bl.a. ENISA tolkar sektorn mer extensivt än vad PTS hittills har gjort⁴ kan sektorns omfattning vara större än vad PTS tidigare uppgett till utredningen.

Detta yttrande har beslutats av divisionschefen Catarina Wretman. I ärendets slutliga handläggning har Åsa Gihl (föredragande), verksjuristen Sofie Sandell, jurist, jur.dr EU-rätt

⁴ [Understanding the new NIS2 Directive cybersecurity requirements and their practical applications for the EU space sector](#), s 9. Och [NIS Investments 2024](#), avsnitt 8 Sectorial Analysis: Space.

Maria Wiberg och avdelningschefen Patrik Bystedt deltagit. Vid föredragningen närvarade kommunikationschefen Anne-Catherine Worth.

