Finansdepartementet

Felisa Krzyzanski

Vår referens/dnr:
2026–16

Er referens/dnr:
Fi2026/00065

2026-04-21

Remissvar

Betänkandet Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115)

Svenskt Näringsliv

- Tillstyrker utredningens skrivningar om standardisering, konsumentskydd, sekretess, tystnadsplikt och regulatoriska sandlådor.
- Efterfrågar samordning med övriga cybersäkerhetsregleringar.
- Efterfrågar gemensam rapportering för samma cyberincident.
- Understryker vikten av regelförenkling i den Digitala Omnibusen och EU:s digitala fitness check.
- Tillstyrker utredningens förslag om stödåtgärder till företag men ser en risk att stödåtgärdernas betydelse överskattas i förhållande till de faktiska utmaningar som små och medelstora företag står inför.

Sekretess och tystnadsplikt

Svenskt Näringsliv tillstyrker införande av sekretess i enlighet med CRA artikel 14 och 15 samt förslaget om tystnadsplikt för att inte röja eller utnyttja information om affärs- eller driftförhållanden.

Regulatoriska sandlådor och testmöjligheter

Svenskt Näringsliv välkomnar möjligheten att använda regulatoriska sandlådor som ett verktyg för att främja innovation och samtidigt säkerställa regelefterlevnad. Sandlådorna bör kompletteras med testmöjligheter under verkliga förhållanden, särskilt vid utveckling och införande av mer komplexa produkter och system. Mot denna bakgrund är det bra att ansvariga myndigheter ges utrymme att vidareutveckla och anpassa sådana verktyg i

nära dialog med näringslivet. En praktisk och flexibel tillämpning är avgörande för att sandlådor och testmiljöer ska utgöra ett reellt stöd och inte medföra onödig administrativ belastning.

Incidentrapportering och tillsyn

Det är av stor vikt för näringslivet att tillsynsprocesser och rapporteringskrav samordnas för att undvika parallella granskningar av samma förhållanden eller incidenter. Detta gäller tillsyn enligt EU:s cyberresiliensförordning (CRA), cybersäkerhetslagen (NIS2), säkerhetsskyddslagstiftningen, GDPR, DORA, eIDAS förordningen och CER direktivet.

Vad gäller rapporteringskrav av intrång och incident finns nu ett viktigt regelförenklingsinitiativ i den pågående förhandlingen om EU-kommissionens Digitala Omnibus. Det cypriotiska ordförandeskapet föreslår en nationell ingång för all incidentrapportering och med ENISA som Single Information Point och nationella CSIRT som informationsgivare mellan berörda medlemsländer.

Förslaget skulle innebära att cyberincidenter rapporteras in på en och samma portal (”en väg in”) nationellt vad gäller NIS 2 direktivet, GDPR, DORA, eIDAS förordningen och CER direktivet. Här saknas dock CRA, som borde inkluderas. Dessa lagar kräver idag att företag rapporterar incidenter på olika sätt med olika tidsramar. I en hypotetisk situation där ett fysiskt intrång eller olycka sker i energisektorn (CER) och leder till cyberintrång hos tjänsten (NIS2), ska incidenten rapporteras enligt dessa två lagar. Och om intrånget var en funktion av en offentligt känd utnyttjad sårbarhet i en produkt integrerad i systemet ska en rapport om detta också göras enligt CRA till tillverkaren. Har dessutom personuppgifter läckt måste enheten rapportera enligt GDPR.

I den digitala omnibusen föreslås också lättnade i rapporteringskraven i GDPR som har varit i kraft längst tid och hunnit utvärderats i omgångar. En gemensam EU-mall föreslås liksom förlängd rapporteringstid från 72 h till 96 med mera, vilket vore mycket välkommet. I CRA är en första rapporteringsskyldighet satt till 24 timmar till behörig myndighet. Företag av alla storlekar är förvirrade över alla rapporteringskrav och deras potentiella överlappningar och kraven att lämna rapporter med liknande information flera gånger till olika myndigheter. Näringslivet efterfrågar förenkling genom en väg in och med en tydlig instruktion om att en rapport om en betydande incident räcker.

Sverige borde kunna ta ett första steg och införa en gemensam incidentrapporteringsportal där samtliga ovan nämnda regeringar ingår på åtminstone det sätt som Danmark och Luxemburg redan genomfört. De överlappande rapporteringsskyldigheter innebär onödiga ekonomiska och administrativa bördor.

I väntan på en väg in för incidentrapportering finns behov av ytterligare förtydliganden kring hur rapporteringskraven enligt cyberresiliensförordningen ska förhålla sig till befintliga incidentrapporteringskrav enligt den svenska cybersäkerhetslagen.

Stöd till företag

Utredningens förslag om stöd till företag i samband med genomförandet av CRA är i grunden positiv. Särskilt välkomnas fokus på vägledning, samordning mellan myndigheter och tidiga stödinsatser till företag. Svenskt Näringsliv vill särskilt understryka behovet av tydlig, lättillgänglig och praktiskt användbar vägledning.
Samtidigt är det viktigt att detta stöd fullt ut följer EU:s kommande vägledning så att den harmoniserade tillämpningen av CRA inte riskeras. EU:s utkast till vägledning fokuserar på fjärrbaserade databehandlingslösningar samt fri och öppen källkod, begreppet stödperioder samt samspelet mellan CRA och annan EU-lagstiftning.

Vi ser en risk att stödåtgärdernas betydelse överskattas i förhållande till de faktiska utmaningar som små och medelstora företag står inför. För dessa företag är det inte i första hand brist på stöd som utgör hindret, utan de ökade kostnader, den administrativa börda och den komplexitet som följer av regelverket. Stödåtgärder kan vara ett viktigt komplement, men kan inte ersätta behovet av förenklade regler, minskad administrativ belastning och krav som är anpassade efter mindre företags förutsättningar.

För att möjliggöra det skulle ett systematiskt SME-test införas i det fortsatta arbetet, där såväl regelverkets som stödåtgärdernas tillgänglighet, kostnader och praktiska användbarhet för små företag prövas. Först då kan de bidra till ökad regelefterlevnad och stärkt konkurrenskraft hos små och medelstora företag.

Konsekvenser och behov av regelförenkling

Cybersäkerhetsområdet har fått ett antal nya regleringar under senare tid. Samtidigt som resiliens och säkerhet är viktigt är det centralt att företagen kan vara konkurrenskraftiga och att oproportionerlig lagstiftning inte tillåts bli ett hinder för företagande. Regelförenkling av cybersäkerhetsregleringarna

bör omhändertas i EU:s digitala fitness check under 2027 i den del som inte omfattas av den Digitala Omnibusen.

SVENSKT NÄRINGSLIV

Göran Grén Carolina Brånby