Kommerskollegium
National Board of Trade Sweden

Enheten för EU:s handelspolitik
Heidi Lund

YTTRANDE
2026-05-12 Dnr 2026/00992-2

Försvarsdepartementet

Kommerskollegiums remissvar avseende Europeiska kommissionens cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS 2-direktivet (EU 2022/2555)

Er ref: Fö2026/00576

Kommerskollegium ansvarar för frågor som rör utrikeshandel, EU:s inre marknad och handelspolitik. Kommerskollegiums uppdrag är att verka för frihandel. Det innebär att vi verkar för fri rörlighet på den inre marknaden och för liberaliseringar av handeln mellan EU och omvärlden samt globalt.

Vi har tagit emot Europeiska kommissionens cybersäkerhetspaket för synpunkter och vill lämna följande kommentarer.

Kommerskollegium instämmer i cybersäkerhetspaketets övergripande förslag, som syftar till att vidareutveckla befintlig lagstiftning för att adressera både ny teknik och en förändrad hotbild för ökad motståndskraft. Att EU:s medlemsstater har en gemensamt hög cybersäkerhet är av stor vikt för en välfungerande inre marknad. I vårt yttrande fokuserar vi på följande; stärkt kapacitet genom ENISA, det nya ramverket för IT-leverantörskedjor, reform av systemet för cybersäkerhetscertifiering samt regelförenklingen genom harmonisering men överlag mer strikta krav.

Stärk kapacitet genom ENISA
Kommerskollegium noterar att ENISA genom förslaget får en tydligare roll att definiera säkerhetsnivåer, ta fram detaljerade krav och utveckla tekniska specifikationer inom cybersäkerhet även om kommissionen formellt ansvarar för framtagandet av regler och godkännande av samma. Detta innebär att ENISA går från en rent rådgivande roll till agendasättare och systemarkitekt. Då cybersäkerhetsregelverket redan från början är oerhört komplext är det rimligt att fråga sig om det finns en process för konsekvensanalys av de regler och certifieringar som tas fram samt insyn i prioriteringar som kommer göras på teknisk nivå och som kan ha omfattande konsekvenser för handeln. När det gäller leveranssäkerhet som utgör en av paketets huvudpunkter ska ENISA och kommissionen ta fram riskbedömningar och identifiera potentiella riskleverantörer. Då sådana bedömningar ofta bygger på säkerhetsklassad information, underrättelser och geopolitisk analys kan

insynen försvåras ytterligare, framför allt för ekonomiska aktörer. Detta anser Kommerskollegium som ett problem från en proportionalitetssynvinkel. Medlemsstater kan dock få insyn via kommittéarbete. Som Kommerskollegium lyft i tidigare yttranden finns det idag väldigt lite information om hur pass bra cybersäkerhetskrav fungerar, t.ex. i form av antalet/andelen IT-produkter på marknaden som överensstämmer med gällande regler och certifieringskrav.[1] Detta är en brist särskilt då kravuppfyllnad t.ex. genom cybercertifiering är en kostnadskrävande process för företagen.

Det nya ramverket för IT-leverantörskedjor

Förslaget till det nya ramverket för IT-leverantörskedjor indikerar att EU rör sig ännu starkare från "klassisk IT-säkerhet" till geopolitik, beroenden, framför allt genom riskstyrning av leverantörer. Fokus är inte längre bara vad som används utan vem som levererar det. Kärnan är att organisationer (och i vissa fall medlemsstater) ska identifiera kritiska leverantörer, bedöma risker kopplade till dessa och vidta åtgärder beroende på risknivå. Riskerna kan handla om tekniska sårbarheter, bristande säkerhetsrutiner, beroenden (”single supplier”) och, vilket är nytt, även geopolitisk exponering, Riskerna ska bedömas centralt på EU-nivå av ENISA. Insynen kring de så kallade högriskleverantörerna bedöms begränsad, vilket Kommerskollegium ser att kan öka risken för diskriminering och handelshinder.

Reform av systemet för cybersäkerhetscertifiering

Reformen för cybersäkerhetscertifiering ska leda till snabbare framtagande av relevanta certifieringsordningar genom en tydligare och mer strömlinjeformad process. Detta ska ske genom en mer aktiv styrning av vilka områden som ska certifieras och tydliga kravnivåer samt en stark koppling till andra regelverk. Detta bör ses som en viktig ansats för att minska nationella certifieringsordningar och fragmentering, inte minst då certifiering får en starkare roll i att visa överensstämmelse, styra marknaden och hantera leverantörsrisker än tidigare. Dock kvarstår problematiken med regelverkets komplexitet som förmodligen inte någonsin helt kan avskaffas samt frågor om begränsad transparens och risk för handelshinder.

Regelförenkling genom harmonisering men i överlag mer strikta krav

Cybersäkerhetsområdet är komplext, därför är det positivt att paketet innehåller åtgärder för regelförenkling genom samordning mellan regelverk (t.ex. NIS2 och andra cybersäkerhetsregler). Det kan minska överlappande krav och göra det lättare för företagen att hantera bl.a. genom färre dubbla rapporteringskrav, riskbedömningar och mindre komplex terminologi. Även användningen av certifiering för att visa kravuppfyllnad samt en bättre samordnad tillsyn bör kunna bidra till regelförenkling och minskad administrativ börda för företagen. Det handlar således främst om harmonisering av regler, inte om att ta bort krav. Detta bör gynna både aktörer inom och utanför EU.

---

[1] Kommerskollegiums synpunkter på betänkandet Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115) Dnr 2026/00224-2.

Samtidigt kan de höga kraven skapa inträdesbarriärer för tredje länder och minska flexibiliteten vilket kan ge indirekta extraterritoriella effekter. Detta bör beaktas mot bakgrund av den digitala handeln och globala handelsmönster. Vi noterar att perspektivet i huvudsak är regulatoriskt och säkerhetsdrivet snarare än handelsdrivet. Frågan om internationell regelharmonisering kan därför behöva få större utrymme.

ENISA ska enligt artikel 18 utarbeta tekniska specifikationer under beaktande av befintliga europeiska och internationella standarder samt, när så är relevant, även delta och leda arbetet med att utveckla standardiseringen på unionsnivå. Här bör det pågående arbetet med revideringen av standardiseringsförordningen tas i beaktande. Frågan om vem som utvecklar standarder i framtiden för att komplettera europeisk lagstiftning är en aktuell fråga. Även om det finns ett behov att särskilt på cybersäkerhetsområdet, snabbt kunna ta fram standarder för att kunna möta den globala marknadens behov, måste det uppnås genom de enligt WTO/TBT-avtalet etablerade principerna om transparens, öppenhet, konsensus och effektivitet. Dessa principer är centrala för att säkerställa teknikneutralitet och rättssäkerhet. Därför är det viktigt att tydligt definiera ENISA:s roll i förhållande till andra relevanta aktörer inom standardiseringen.

Ärendet har avgjorts av enhetschefen Agnès Courades Allebeck i närvaro av ämnesrådet Heidi Lund, föredragande. I den slutliga handläggningen har även chefsjuristen Christian Finnerman, ämnesrådet Anna Sabelström samt utredarna Hannes Berggren och Anna Ryde deltagit.

Agnès Courades Allebeck
Enhetschef

Heidi Lund
Ämnesråd