Kommerskollegium
National Board of Trade Sweden

Enheten för EU:s handelspolitik
Heidi Lund

Välj ett objekt.
2026-04-16 Dnr 2026/00224-2

Finansdepartementet

Kommerskollegiums synpunkter på betänkandet Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115)

Er ref: Fi2026/00065

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 betänkandet Kompletterande bestämmelser till EU:s cyberresiliensförordning. Kommerskollegium kan styrka betänkandets huvudförslag dvs. förslaget en svensk lag och förordning samt en efterföljande institutionell organisation med marknadskontrollmyndigheter och anmälande myndighet som ska bidra till en enhetlig tillämpning av cyberresiliensförordningen i Sverige. Nedan våra synpunkter på specifika sakfrågor.

Risker för fragmentering i tillämpningen av cyberresiliensförordningen

Kommerskollegium ser att betänkandet fokuserar mycket på nationell organisation**,** men mindre på konsekvenser för den inre marknaden och internationell handel. Mot bakgrund av cyberresiliensförordningens betydelse för produkter som omsätts på den inre marknaden är det viktigt att tillsyn och tillämpning sker på ett enhetligt sätt inom EU. Kommerskollegium vill därför understryka vikten av ett nära samarbete mellan medlemsstaternas marknadskontrollmyndigheter för att motverka risker för fragmentering i tillämpningen.

Det bör också observeras att cybersäkerhetsområdet inte nödvändigtvis präglas av samma transparens och öppenhet kring incidenter, rapportering och icke-överensstämmelse i gränsöverskridande internationellt myndighetssamarbete i jämförelse med ordinarie tillsynsområden för icke-digitala varor vilket skulle kunna beaktas i sammanhanget. Cyberincidenter och sårbarheter är dels svåra att upptäcka och följa. Vidare kan cyberincidenter och sårbarheter vara av sådan natur eller beröra samhällsviktig verksamhet och nationell säkerhet så att information inte delas eller kan delas obehindrat av aktörer så som regelverket förutser. Detta kan riskera bidra till brist på transparens och en helhetsbild av bristfälliga IT-produkter vad beträffar cybersäkerhet. Detta gäller såväl inom EU som internationellt. Utan transparens är det

svårt att bedöma och kraven i regelverket är i paritet med risker och brister på marknaden.

Marknadskontroll och bedömning av överensstämmelse

När det gäller marknadskontroll och tillsyn vill Kommerskollegium lyfta utmaningen med att utöva tillsyn över digitala produktegenskaper.

Kommerskollegium vill i detta sammanhang framhålla att marknadskontroll av mjukvarubaserade produkter kan förväntas skilja sig betydligt från marknadskontrollen av traditionella industrivaror. Digitala produkter förändras kontinuerligt genom uppdateringar, vilket innebär att produkters egenskaper kan förändras efter att de släppts på marknaden. Detta innebär att tillsynen i högre grad behöver ta sin utgångspunkt i ett livscykelperspektiv snarare än i en statisk produktbedömning vid tidpunkten för utsläppande på marknaden. Vidare påverkas digitala produkter inte endast av den avsedda användningen och förutsägbara risker. De påverkas också av faktorer som är svårare att förutse och därmed svårare att reglera, övervaka och utöva tillsyn över: frågor om exempelvis personlig integritet, cybersäkerhet och motståndskraft.[1]

Från betänkandet går det att avläsa att produktlivscykelperspektiv för cybersäkerhet har beaktats genom relevanta krav[2] vilket Kommerskollegium ser som positivt.

På samma sätt är bedömning av överensstämmelse kopplat till cybersäkerhet mer komplext än certifiering av icke-digitala industrivaror. Cybersäkerhet är ett dynamiskt tillstånd snarare än en statisk egenskap och kan påverkas av nya sårbarheter, uppdateringar eller förändringar i hotbilden. Det kan därför finnas skäl att ytterligare analysera hur bedömning av överensstämmelse och tillsyn kan hantera denna dynamik *på ett verifierbart sätt*. Information om till vilken grad IT-produkter på den europeiska marknaden faktiskt överensstämmer med gällande rättsliga cybersäkerhetskrav är fortfarande knapphändig. Mer information skulle kunna vara behjälplig för att utvärdera effekten av regleringen och efterföljande tillsynen.

Regelförenkling

Cyberresiliensförordningen innebär omfattande och detaljerade rapporteringsskyldigheter för ekonomiska aktörer, inklusive krav på rapportering av sårbarheter och incidenter till både nationella CSIRT-enheter och ENISA inom korta tidsfrister (SOU 2025:115, avsnitt 8.2). Det positivt att utredningen uppmärksammar att systemet innefattar flera rapporteringskanaler och att det finns en uttalad ambition att förenkla regelverket, bland annat genom inrättandet av en gemensam

[1] Se Kommerskollegium (2023*) Innovation, AI, Technical Regulation and Trade* samt SOU 2025:101 om anpassningen till AI-förordningen med referens till Kommerskollegiums analys.

[2] Bl.a. genom att regelverket innebär att bl.a. att tillverkare måste hantera sårbarheter under produktens livstid, tillhandahålla säkerhetsuppdateringar och övervaka cybersäkerhetsrisker även efter att produkten släppts på marknaden.

rapporteringsplattform. Mot denna bakgrund kan det dock konstateras att systemet, trots planer på förenklingsåtgärder, alltjämt fortfarande framstår som fragmenterat.

Standarder och innovation

Kommerskollegium vill framhålla att reglering av cybersäkerhet behöver utformas på ett sätt som är förenligt med snabb teknisk utveckling. Cybersäkerhetskrav riskerar annars att snabbt bli föråldrade eller skapa onödiga hinder för innovation och handel. Det kan därför vara viktigt att säkerställa att regelverket i största möjliga utsträckning är teknikneutralt, och bygger på riskbaserade principer samt internationella standarder.

Vad beträffar standarder har Kommerskollegium tidigare lämnat kommentarer på cyberresiliensutredningens 8 kapitel med syfte att bedöma behovet och konsekvenserna av ett nationellt deltagande i standardiseringsorganisationernas arbete inom ramen för EU:s cyberresiliensförordning[3]. Här har vi bl.a. lyft vikten av att beakta det senaste avgörandet i EU-domstolen, den s.k. Malamuddomen[4] och eventuellt befarade konsekvenser för det europeiska och nationella standardiseringsarbetet samt utmaningar med gemensamma specifikationer ifall harmoniserade standarder inte finns tillgängliga[5]. Därutöver är det av vikt att upplägget med horisontella och vertikala standarder blir lätt att tillämpa och inte skapar osäkerhet på marknaden. Vi har lärt oss av de svenska standardiseringsorganisationerna att det tas fram, såväl standarder som ger presumtion av överensstämmelse och sådana som inte ger det. Detta kan skapa förvirring för företagen om vad kraven innebär och hur kraven ska följas. Vi förstår även att standardiseringsarbetet under cyberresiliensförordningen i Sverige sker i samarbete mellan de nationella standardiseringsorganisationerna (SIS, SEK och ITS). Här vill vi lyfta vikten av ett välkoordinerat samarbete för att, ur ett handelsperspektiv, skapa tydlighet, undvika överlappningar eller eventuella konflikter mellan standarder, samt enhetliga tidsramar för genomförande.

Slutligen ser Kommerskollegium positivt på betänkandets förslag på stödåtgärder och stödfunktioner för att bistå företag, särskilt SME och förslag på regulatoriska sandlådor för att adressera innovation.

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

Agnès Courades Allebeck
Enhetschef

Heidi Lund
Ämnesråd

[3] Dnr 2025/ 01411-3.

[4] ECJ C-588/21 P (Public.Resource.Org et al. ./. European Commission)

[5] Se Digitalisation and alignment of common specifications - Internal Market, Industry, Entrepreneurship and SMEs