2026-05-07

fo.remissvar@regeringskansliet.se
fo.ech.remissvar@regeringskansliet.se

Europeiska kommissionens cybersäkerhetspaket

Svenska Bankföreningen välkomnar möjligheten att lämna synpunkter på 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.

Kommissionen publicerade den 20 januari 2026 förslag på uppdateringar av cybersäkerhetsakten (CSA2), som omfattar två specifika förslag: en förordning om revidering av CSA2 samt ett direktiv med riktade ändringar av NIS2-direktivet.

Svenska Bankföreningen stöder målet att förenkla och harmonisera EU:s regelverk på cybersäkerhetsområdet. Särskilt viktigt är arbete med att säkerställa proportionalitet, praktisk tillämpbarhet och samstämmighet mellan horisontella och sektorsspecifika regelverk.

Ramverk för betrodda IKT-leveranskedjor inom EU

Förslaget till CSA2 inför ett nytt, unionsövergripande ramverk för säkerhet i IKT-leveranskedjor som syftar till att minska cybersäkerhetsrisker som är kopplade till icke-tekniska risker och beroenden med leverantörer utanför EU. För banksektorn innebär Kommissionens förslag om CSA2 en förskjutning från den riskbaserade ansats som etablerats genom förordningen om digital operativ motståndskraft (DORA) till ett ramverk som fokuserar på icke-tekniska risker. Medan DORA betonar motståndskraft och ett robust tillsynsramverk, inför CSA2 befogenheter för Europeiska kommissionen att förbjuda specifika IKT-leverantörer baserat på geopolitiska och andra icke-tekniska risker. Den ansats som föreslås inom ramen för CSA2 skapar osäkerhet för finansiella företag om vilka leverantörer som kan komma att omfattas av ett sådant ramverk.

Bankföreningen önskar att Kommissionen tydliggör den metodik och styrning som ska användas för att identifiera och utse högriskleverantörer och länder utanför EU som bedöms utgöra cybersäkerhetsrisker. Mot bakgrund av komplexiteten i globala IKT-leveranskedjor är förutsebarhet och transparens i sådana processer av avgörande betydelse för att finansiella företag ska kunna hantera

Besök (Visit):
Blasieholmsgatan 4B
Stockholm
Sverige (Sweden)

Post:
Box 7603
SE-103 94 Stockholm
Sverige (Sweden)

+46 (0)8 453 44 00
info@financesweden.se

www.financesweden.se

leveranskedjeberoenden på ett ändamålsenligt sätt och planera riskreducerande åtgärder. För banker med global verksamhet är det oklart om användning av högriskleverantörer skulle kunna tillåtas i andra icke-EU länder om inga alternativ står till buds.

Bankföreningen vill också påpeka att utpekandet av högriskleverantörer och restriktioner att nyttja dessa, kan leda till en potentiell koncentration på EU-nivå till ett begränsat antal leverantörer, med därpå följande prisökningar och skapandet av koncentrationsrisker och single points of failures.

Identifiering av centrala IKT-lösningar och system (artikel 102 CSA2)

Om vissa kritiska komponenter förbjuds inom hela EU bör det, som ett minimum, införas tillräckligt långa övergångsperioder för att undvika negativa konsekvenser för bankernas verksamhet och kontinuiteten i IT-verksamheten. Vidare bör undantag eller lättnadsbestämmelser införas i de fall där det saknas tekniska alternativ för bankerna.

Processen att identifiera centrala IKT-lösningar och system kan dessutom medföra ökad komplexitet eller dubbelarbete i situationer där Kommissionens identifiering av centrala IKT-tillgångar inte överensstämmer med den omfattande inrapportering av IKT-leverantörer som redan genomförs enligt DORA-regelverket. Det bör därför klargöras huruvida banker kan komma att bli föremål för ytterligare inrapportering om underlag avseende IKT-beroenden och tillgångar, trots att sådan information redan samlas in av de europeiska tillsynsmyndigheterna inom ramen för DORA.

Riskreducerande åtgärder i IKT-leverantörskedjan (artikel 103 CSA2)

Förslaget ger även Kommissionen befogenhet att införa ett brett spektrum av riskreducerande åtgärder som påverkar företags IKT-leverantörskedjor, inklusive begränsningar av avtalsrelationer med leverantörer, krav på tekniska konfigurationer, inskränkningar av fjärråtkomst samt krav på diversifiering av leverantörer.

För finansiella företag, som redan idag är genomdigitaliserade, kan sådana åtgärder få betydande konsekvenser för outsourcing, molnstrategier och IT-arkitektur. Det riskbaserade angreppssätt för att hantera IKT-tredjepartsrisker som etablerats i DORA samt bankernas strategiska beslut att investera i teknik och hantera dessa risker behöver därför beaktas i CSA2.

Bankföreningen uppmanar Kommissionen att säkerställa att dessa typer av riskreducerande åtgärder vidtas i konsultation med berörda aktörer så att det finns förutsättningar att förutse eventuella förbud eller andra åtgärder och undvika investeringar som i efterhand visar sig vara oanvändbara.

Den finansiella sektorn omfattas redan av ett heltäckande ramverk för hantering av IKT-tredjepartsrisker genom DORA, inklusive tillsyn av kritiska IKT-tredjepartsleverantörer på unionsnivå. En tydlig beskrivning av relationen mellan dessa regelverk skulle bidra till att undvika överlappande eller överlappande regelverk.

Ändringsförlag i relaterade artiklar

Artikel 98

"X. The requirements laid down in this Title shall apply to the entities referred to in Regulation (EU) 2022/2554 only insofar as the specific matters regulated herein are not addressed by the provisions of that Regulation."

Artikel 100

(1) “(new) The verification shall be based on objective, substantiated, and up-to-date evidence. In carrying out the verification, the Commission shall:
(a) consult relevant stakeholders;
(b) ensure the application of a transparent methodology and publicly available; and
(c) balance technical, economic, and security considerations.”

(2)“(new) Before adopting a decision designating a third country pursuant to paragraph 2, the Commission shall carry out a comprehensive impact assessment, by:

(a) consulting relevant stakeholders, including, where appropriate, affected undertakings and industry associations;
(b) evaluating the potential economic, technological, and supply chain impacts of the designation;
(c) analysing the availability and viability of alternative suppliers; and
(d) assessing the projected effects of the designation on the resilience of the EU internal market and the global competitiveness of the Union’s ICT sector.”

En förstärkt operativ roll för ENISA

Den finansiella sektorn utsätts för en snabbt föränderlig och mer sofistikerad cyberhotbild sedan antagandet av CSA 2019. Ransomware, avancerade angrepp och sårbarheter i leverantörskedjor utgör i dag betydande risker för finansiell stabilitet.

Förslagen i CSA2 stärker inte tillräckligt den operativa krisledningsförmågan på unionsnivå. ENISA ges ökade stödjande uppgifter men saknar mandat att leda, samordna eller initiera krishantering vid storskaliga gränsöverskridande

cyberangrepp. Samtidigt riskerar skillnaderna mellan NIS2- och DORA-ramverken att skapa samordningsbrister, särskilt i kriser som samtidigt berör finansiell och annan kritisk digital infrastruktur. För att hantera detta föreslås att ENISA ges en tydligare EU-övergripande krissamordnande roll, i nära samverkan med de europeiska finansiella tillsynsmyndigheterna, centralbankerna och nationella behöriga myndigheter, för att säkerställa både cybersäkerhet och finansiell stabilitet.

SVENSKA BANKFÖRENINGEN

Hans Lindberg

Magnus Jacobson