Fö2026/00576
Försvarsdepartementet
fo.remissvar@regeringskansliet.se
2026-05-18

SweFinTechs remissvar till Remittering av Europeiska 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

Om SweFinTech
The Swedish Financial Technology Association ("**SweFinTech**") är en branschförening för svenska fintechbolag som samlar över 100 bolag inom fintechbranschen med syfte att stärka det svenska finansiella ekosystemet och skapa en välfungerande marknad för svenska fintechbolag. Våra medlemmar utgörs av företag inom betalningar, krediter, crowdfunding, investeringar med mer.

Övergripande ansats:

SweFinTech tackar för möjligheten att få inkomma med synpunkter till Europeiska kommissionens förslag till ett nytt cybersäkerhetspaket, bestående av ett förslag till ny cybersäkerhetsakt (COM(2026) 11) samt riktade ändringar i NIS 2-direktivet (COM(2026) 13).

För det första, finns det oklarheter kring hur cybersäkerhetscertifieringarna ska samspela med DORA och i vilken utsträckning de faktiskt kan minska efterlevnadsbördan för DORA-reglerade finansiella företag.

För det andra, riskerar förslaget att leda till otydliga mandat, överlappande tillsynsinsatser och parallella informationskrav mellan Enisa, nationella tillsynsmyndigheter och DORA:s tillsynsramverk.

För det tredje, innebär tidslinjen för övergången till postkvantkryptografi betydande praktiska och tekniska utmaningar för finansiella aktörer, särskilt med hänsyn till beroenden i leveranskedjor och behovet av gemensamma standarder.

För det fjärde, finns det en risk att fullharmoniseringen och nya genomförandeakter under NIS 2 leder till motstridiga krav, ökade omställningskostnader och bristande samordning med DORA:s tekniska standarder.

Behov av tydligare koppling mellan cybersäkerhetscertifieringen och DORA

SweFinTech delar kommissionens bedömning att hotbilden inom cybersäkerhetsområdet har förvärrats och att det finns ett behov av ett mer samordnat, ändamålsenligt och framtidssäkrat

regelverk på EU-nivå. Särskilt välkomnas ambitionen att minska fragmenteringen inom unionen och att stärka den gemensamma motståndskraften mot både tekniska och icke-tekniska cyberrisker.

Samtidigt anser SweFinTech att flera delar av förslaget präglas av oklarheter som riskerar att leda till rättsosäkerhet och ökade efterlevnadskostnader, särskilt för finansiella aktörer och teknikdrivna företag som redan omfattas av ett omfattande och detaljerat regelverk genom DORA.

I förslaget anges att innehav av ett giltigt europeiskt cybersäkerhetscertifikat ska kunna ge presumtion om regelefterlevnad i tillämpliga delar av EU:s cyber och digitalreglering (artiklarna 74–75 i cybersäkerhetsakten 2 samt artiklarna 24.4–24.6 i NIS 2-direktivet). Det är dock oklart i vilken utsträckning denna presumtion är relevant för finansiella företag som omfattas av DORA, som är lex specialis i förhållande till NIS 2 och innehåller egna, detaljerade krav på IKT riskhantering, incidentrapportering och säkerhet i leveranskedjor. Presumtionen är enligt förslaget begränsad till de delar där certifieringsordningens krav faktiskt sammanfaller med det aktuella regelverket. Det framgår inte i vilken utsträckning framtida certifieringsordningar kommer att utformas med DORA kraven i åtanke. Därmed är det oklart om certifiering i praktiken kan bidra till att minska efterlevnadsbördan för DORA reglerade finansiella företag.

Tydligare regler för ansvarsfördelning och tillsyn

SweFinTech vill även framhålla att certifiering inte förhindrar nationella tillsynsmyndigheter, såsom Finansinspektionen, från att inleda tillsyn eller konstatera bristande efterlevnad. Certifieringens värde som verktyg för att skapa förutsebarhet och minska administrativa bördor framstår därmed som begränsat.

Förslaget ger Enisa en stärkt roll i tillsynssamordningen av gränsöverskridande entiteter (artikel 5.1(g) i cybersäkerhetsakten 2 samt artikel 37a i NIS 2-direktivet). För finansiella entiteter som är undantagna från NIS 2:s tillsynsregim till förmån för DORA är det emellertid oklart hur detta samspel är tänkt att fungera i praktiken. Förslaget innehåller visserligen ett allmänt krav på samarbete och informationsutbyte mellan Enisa och de europeiska tillsynsmyndigheterna, men detta reglerar inte hur Enisas samordningsfunktion ska förhålla sig till ESA:ernas tillsynsansvar enligt DORA. Det finns därmed en risk för otydliga mandat, överlappande tillsynsinsatser och parallella informationskrav för finansiella aktörer som bedriver gränsöverskridande verksamhet.

En mer realistisk övergång till postkvantkryptografi

I förslaget anges att medlemsstaterna inom ramen för sina nationella cybersäkerhetsstrategier ska anta policyer för övergången till postkvantkryptografi (artikel 7.2(k) i NIS 2-direktivet), med målsättningen att kritiska användningsfall ska vara migrerade senast 2030. För finansiella aktörer och fintech-företag är denna tidslinje särskilt utmanande, eftersom kryptografi utgör en grundläggande funktion i flertalet kritiska processer, såsom betalningsautentisering, digitala signaturer, nyckelutbyte och API-säkerhet. Med mindre än fyra år till 2030-målet behöver berörda aktörer påbörja kartläggning och planering i närtid. Därutöver måste migreringen genomföras samordnat längs hela leveranskedjan, inklusive motparter, infrastrukturleverantörer och

betalningssystem, för att den samlade säkerhetsnivån ska kunna upprätthållas. Även om förslaget anger att nationella strategier ska stödja framtagandet av migreringsplaner och testning av postkvantkryptografi är det oklart i vilken utsträckning dessa kommer att ge finanssektorn tillräckligt konkret vägledning om prioriteringar, tekniska standarder och praktisk samordning.

Risk för motstridiga krav och ökade omställningskostnader.

SweFinTech välkomnar förslaget att kommissionen, med stöd av artikel 21.2(d) i NIS 2-direktivet, ska ta fram riktlinjer för NIS 2-entiteters krav på leverantörer i fråga om säkerhet i leveranskedjor. Sådana riktlinjer kan i princip bidra till ökad rättslig tydlighet och motverka att skyldigheter på ett otillbörligt sätt överförs till aktörer som inte omfattas av direktivet. Samtidigt noterar SweFinTech att riktlinjerna enligt förslaget inte är rättsligt bindande. Av konsekvensbedömningen framgår att de är av frivillig natur och att tillämpningen kan komma att variera mellan medlemsstater. Det är därmed oklart om riktlinjerna i praktiken kommer att leda till en faktisk minskning av den administrativa bördan för leverantörer, eller om NIS 2-entiteter även fortsättningsvis kommer att ställa egna, mer långtgående eller avvikande informationskrav utöver vad riktlinjerna rekommenderar.

Kraven på fullharmonisering innebär att Sverige inte längre kan ställa upp strängare eller avvikande nationella krav inom de områden som omfattas av kommissionens genomförandeakter (artikel 21.5 i NIS 2-direktivet). I nuläget är det oklart vilka genomförandeakter som kommer att antas och på vilken detaljnivå de kommer att ligga. Fullharmoniseringen innebär risker i två riktningar. Å ena sidan finns en risk att den faktiska ambitionsnivån sänks jämfört med dagens svenska krav. Å andra sidan kan genomförandeakterna medföra nya eller annorlunda krav som innebär betydande omställningskostnader för företag som redan anpassat sina system och processer till befintlig nationell reglering. För finansiella företag som omfattas av DORA finns därutöver en risk att genomförandeakter under NIS 2 inte samordnas tillräckligt med DORA:s tekniska standarder. Detta kan leda till motstridiga krav inom överlappande områden såsom kryptering, åtkomstkontroll och incidenthantering, samt indirekta effekter via gemensamma IKT-leverantörer.

Sammanfattningsvis anser SweFinTech att förslagen i cybersäkerhetspaketet behöver förtydligas och i vissa delar justeras innan de genomförs. För att uppnå ökad cybersäkerhet och minska fragmentering inom unionen utan att skapa osäkerhet eller onödiga merkostnader krävs en tydligare samordning med befintlig sektorsspecifik reglering, i synnerhet DORA. Dessutom krävs det klara besked om tillsynsansvar, certifieringarnas faktiska rättsverkningar, relationen mellan Enisa och de finansiella tillsynsmyndigheterna samt mer realistiska och vägledande tidsramar för tekniskt komplexa omställningar, såsom övergången till postkvantkryptografi, är nödvändiga. Utan sådana förtydliganden riskerar förslagen att leda till överlappande krav, bristande rättssäkerhet och ökade administrativa bördor för finansiella aktörer och fintechbolag, utan att den samlade motståndskraften i praktiken stärks.

Roslana Cederhage
Generalsekreterare
SweFinTech