Remissvar

Försvarsdepartementet
fo.remissvar@regeringskansliet.se

Finansinspektionen
Box 7821
103 97 Stockholm
Tel +46 8 408 980 00
finansinspektionen@fi.se
www.fi.se

2026-02-02

FI dnr 25-36088
(Anges alltid vid svar)

Hemställan om att skapa rättsliga förutsättningar för behandling av personuppgifter rörande lagöverträdelser

Ert dnr: Fö2025/01534

Sammanfattning

Finansinspektionen (FI) tillstyrker förslaget om att införa en bestämmelse i cybersäkerhetsförordningen (2025:1507) om behandling av personuppgifter rörande lagöverträdelser för att uppfylla kraven i artikel 29 i NIS 2-direktivet[1]. FI anser att det även måste säkerställas att de företag som omfattas av Dora-förordningen[2] har samma förutsättningar som verksamhetsutövare enligt cybersäkerhetslagen (2025:1506) att behandla personuppgifter om lagöverträdelser när de utbyter information om cyberhot. För att upprätthålla informationsutbyte med finanssektorn inom ramen för NIS 2-regelverket bör det också förtydligas vad som gäller för deltagande i informationsutbyte enligt artikel 29 i NIS 2-direktivet, för de finansiella företag som även omfattas av cybersäkerhetslagen. FI lämnar därtill vissa synpunkter på den föreslagna författningstexten.

[1] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).
[2] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.

FI har granskat förslaget mot bakgrund av den verksamhet som myndigheten bedriver och har utifrån denna utgångspunkt följande synpunkter på förslaget.

Informationsutbyte enligt Dora-förordningen

Som Myndigheten för civilt försvar (MCF) uppmärksammar i hemställan (s. 4) finns det i artikel 45 i Dora-förordningen bestämmelser om arrangemang för informationsutbyte liknande de i artikel 29 i NIS 2-direktivet. Typen av information som får utbytas skiljer sig dock något mellan Dora-förordningen och NIS 2-direktivet.

Enligt artikel 45.1 i Dora-förordningen får finansiella entiteter sinsemellan utbyta:

> …information och underrättelser om cyberhot, inbegripet indikatorer på äventyrad säkerhet, taktiker, tekniker och förfaranden, cybersäkerhetsvarningar och konfigurationsverktyg, […].

I artikel 29.1 i NIS 2-direktivet avses:

> …information om cybersäkerhet […], inbegripet information om cyberhot, tillbud, sårbarheter, tekniker och förfaranden, angreppsindikatorer, fientlig taktik, specifik information om fientliga aktörer, cybersäkerhetsvarningar och rekommendationer avseende konfigurationsverktyg för cybersäkerhet för att upptäcka cyberattacker, […].

Dora-förordningens bestämmelse är alltså inte specifikt inriktad på enskilda aktörer eller händelser i samma utsträckning som bestämmelsen i NIS 2-direktivet. Trots detta är det möjligt att den information som anges i artikel 45.1 i Dora-förordningen kan innefatta personuppgifter i samband med till exempel cyberhot i form av dataintrång eller försök till dataintrång, det vill säga lagöverträdelser enligt Integritetsskyddsmyndighetens (IMY) tolkning[3]. Till exempel kan sådana uppgifter förekomma bland så kallade angreppsindikatorer som avses i artikel 29 i NIS 2-direktivet och som också används i Dora-förordningen[4]. I en genomförandeförordning[5] till Dora-förordningen beskrivs en angreppsindikator som information om en incident som kan bidra till att identifiera skadlig aktivitet inom ett nätverks-

[3] IMY:s rättsliga ställningstagande IMYRS 2021:1, s. 7 och 8.
[4] *Angreppsindikatorer* i artikel 29.1 i NIS 2-direktivet är en översättning av den engelska termen *indicators of compromise*. Samma term används i den engelska språkversionen av artikel 45.1 i Dora-förordningen, men har på svenska översatts till *indikatorer på äventyrad säkerhet*.
[5] Kommissionens genomförandeförordning (EU) 2025/302 av den 23 oktober 2024 om fastställande av tekniska genomförandestandarder för tillämpningen av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller standardformulär, mallar och förfaranden för att finansiella entiteter ska kunna rapportera allvarliga IKT-relaterade incidenter och anmäla betydande cyberhot (genomförandeförordningen).

eller informationssystem, omfattande bland annat uppgifter om ip-adresser och avsändare av e-postmeddelanden.[6]

När lagen (2024:1278) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn infördes ansåg lagstiftaren inte att kraven i artikel 45 i Dora-förordningen om att finansiella entiteter ska få utbyta information med varandra krävde någon lagstiftningsåtgärd. I propositionen angavs dock att information inte får delas på ett sätt som strider mot bestämmelser som begränsar möjligheterna att dela information, till exempel bestämmelser om personuppgiftsskydd (prop. 2024/25:44 s. 132–134).

Mot bakgrund av vad MCF anför i hemställan (s. 2 och 3), och IMY:s rättsliga ställningstagande IMYRS 2021:1[7], bör det alltså kunna förekomma personuppgifter om lagöverträdelser också inom ramen för arrangemang om informationsutbyte enligt artikel 45 i Dora-förordningen. Enligt FI är det angeläget att möjligheterna att dela information för de företag som omfattas av Dora-förordningen inte är mer begränsade än vad som gäller för verksamhetsutövare enligt cybersäkerhetslagen. FI anser att det därför bör säkerställas att det finns rättsliga förutsättningar för att behandla personuppgifter om lagöverträdelser också inom ramen för utbyte av information med stöd av artikel 45 i Dora-förordningen.

Finansiella företags deltagande i arrangemang för informationsutbyte enligt NIS 2-direktivet

Av skäl 28 i NIS 2-direktivet framgår att för företag som omfattas av Dora-förordningen bör bestämmelserna om arrangemang för informationsutbyte i förordningen (alltså artikel 45) tillämpas i stället för dem som fastställs i NIS 2-direktivet (artikel 29). Det konstateras också i skäl 28 att det är viktigt att upprätthålla starka förbindelser och informationsutbyte med finanssektorn inom ramen för NIS 2-direktivet.

FI anser att det bör förtydligas på lämpligt sätt hur möjligheterna ser ut för finansiella företag, som också är verksamhetsutövare enligt cybersäkerhetslagen, att delta i arrangemang för informationsutbyte enligt artikel 29 i NIS 2-direktivet, och där utbyta information (inklusive

[6] Se genomförandeförordningen Bilaga II, datafält 3.35 Angreppsindikator a och g.
[7] FI noterar att IMY avser att se över det rättsliga ställningstagandet (https://www.imy.se/nyheter/mojlighet-att-lamna-synpunkter-pa-imys-rattsliga-stallningstagande-om-brottsuppgifter/).

personuppgifter om lagöverträdelser) med andra aktörer. Ett sådant förtydligande blir också viktigt för de finansiella företagen med hänsyn till behovet av lagstöd för att dela personuppgifter rörande lagöverträdelser i samband med informationsutbyte.

Behandling av personuppgifter utan samband med artikel 29 i NIS 2-direktivet

Den föreslagna bestämmelsen i cybersäkerhetsförordningen avser endast situationer när personuppgifter som rör lagöverträdelser behandlas i samband med informationsutbyte enligt artikel 29 i NIS 2-direktivet. Bestämmelsen tar alltså inte sikte på alla situationer när det kan vara nödvändigt för enskilda verksamhetsutövare att behandla sådana personuppgifter för att uppfylla sina skyldigheter enligt NIS 2-regelverket. Propositionen[8] till cybersäkerhetslagen tar inte heller upp behandlingen av dessa personuppgifter.

Till den del de enskilda verksamhetsutövarnas behandling av personuppgifter rörande lagöverträdelser syftar till att ett rättsligt anspråk ska kunna fastställas, göras gällande eller försvaras, eller att en rättslig förpliktelse enligt lag eller förordning (till exempel incidentrapportering) ska kunna fullgöras, bör behandlingen omfattas av 5 § förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.

FI anser att det är viktigt att det säkerställs att det finns rättsliga förutsättningar att behandla personuppgifter som rör lagöverträdelser och som behövs för att enskilda verksamhetsutövare ska kunna uppfylla sina skyldigheter enligt cybersäkerhetslagen. Detta måste gälla även i de fall behandlingen inte har samband med ett rättsligt anspråk, till exempel i arbetet med att förebygga cyberhot (jfr strukturen i 5 kap. 6 § lagen [2017:630] om åtgärder mot penningtvätt och finansiering av terrorism [penningtvättslagen]).

Synpunkter på författningstexten

I den föreslagna bestämmelsen i cybersäkerhetsförordningen används begreppet cyber*angrepp*. I NIS 2-direktivet, bland annat i artikel 29.1,

[8] Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag (prop. 2025/26:28).

används begreppen cyber*hot* (som definieras i artikel 6.10) och cyber*attack*. I 1 kap. 2 § 4 och 2 kap. 10 § cybersäkerhetslagen används begreppet cyber*hot*. FI anser att begreppsanvändningen i cybersäkerhetsförordningen bör vara i linje med NIS 2-regelverket i övrigt och noterar i sammanhanget 3 § cybersäkerhetsförordningen som anger att uttryck som används i förordningen har samma innebörd som i cybersäkerhetslagen.

För att tydliggöra vad den föreslagna bestämmelsen reglerar skulle en annan rubrik kunna övervägas, till exempel *Behandling av personuppgifter om lagöverträdelser*[9] eller *Personuppgiftsbehandling*[10]. Om inget av dessa förslag används bör det ändå övervägas om rubriken bör vara *Informationsutbyte* i stället för den föreslagna *Informationsdelning*. Detta för att bättre stämma överens med rubrikerna till kapitel VI och artikel 29 i NIS 2-direktivet där begreppet informations*utbyte* används.

I stället för formuleringen ”andra än myndigheter” i förslaget till bestämmelse kan det övervägas om cybersäkerhetslagens uttryck *enskild verksamhetsutövare* (1 kap. 2 § 9) bör användas för att förtydliga vilka aktörer som träffas av bestämmelsen och för att de ska benämnas på samma sätt som i cybersäkerhetslagen. För att bestämmelsen ska omfatta även sådana ”andra relevanta entiteter som inte omfattas av [NIS 2-direktivets] tillämpningsområde” som nämns i artikel 29.1 i NIS 2-direktivet, bör också enskilda verksamhetsutövares leverantörer och tjänsteleverantörer inkluderas (jfr artikel 29.2).

Förslaget till bestämmelse tar sikte på situationer när ”behandlingen är nödvändig för att *förhindra cyberangrepp* eller *begränsa dess effekter* [våra kursiveringar]”. FI noterar att även om begreppen förhindra och begränsa kan rymma många olika åtgärder, så tar artikel 29.1 a och b i NIS 2-direktivet sikte på fler ändamål med informationsutbytet. Ordvalet *förhindra cyberangrepp* avviker också från språket i artikel 29.1 som avser *incidenter* (som definieras i artikel 6.6). För att undvika oklarhet vid tillämpningen vore det bra om det klargörs om personuppgifter om lagöverträdelser får behandlas för alla de syften och ändamål som framgår av artikel 29.1 a och b, till exempel genom att ange dessa i författningstexten. Om syftet med den föreslagna formuleringen däremot är att begränsa behandlingen av sådana personuppgifter så att den endast får

[9] Jfr rubriken före 5 kap. 6 § penningtvättslagen.
[10] Jfr rubriken före 23 § lagen (2021:34) om tillträdesförbud till butiker, badanläggningar och bibliotek.

ske för vissa ändamål, bör detta framgå av bestämmelsen. Det kan också övervägas om bestämmelser som närmare preciserar förutsättningarna för informationsutbytet behövs (jfr till exempel 4 a kap. 1 och 2 §§ penningtvättslagen).

– – –

FINANSINSPEKTIONEN

Johan Almenberg
Generaldirektör

Sebastian Fichtel
Senior jurist

I detta ärende har generaldirektören Johan Almenberg beslutat. Seniora juristen Sebastian Fichtel har varit föredragande.

Kopia till fo.rs.remissvar@regeringskansliet.se och finansdepartementet.registrator@regeringskansliet.se