SOFF
Säkerhets- och försvarsföretagen

YTTRANDE
Fö2025/01534

Till
fo.remissvar@regeringskansliet.se
Med kopia till:
fo.rs.remissvar@regeringskansliet.se

Yttrande avseende beredskap om att skapa rättsliga förutsättningar för behandling av personuppgifter rörande lagöverträdelser

Säkerhets- och försvarsföretagen (SOFF) tackar för möjligheten att lämna synpunkter.

SOFF är en branschförening för företag inom säkerhets- och försvarsområdet med verksamhet i Sverige. SOFF har idag 400 medlemsföretag som har verksamhet inom bland annat försvar, samhällssäkerhet, cybersäkerhet.

Inledning och övergripande ställningstagande

SOFF är mycket positivt inställd till att regeringen ser över de rättsliga förutsättningarna för privata aktörer att behandla och dela information, inbegripet *eventuella* personuppgifter, om cyberhot samt cybersäkerhet. Rättsliga förutsättningar att behandla sådan information är avgörande för att kunna snabbt upptäcka och bemöta cyberhot och är därmed avgörande för Sveriges säkerhet och försvarsförmåga.

SOFF noterar att det i andra europeiska länder finns framgångsrika plattformar för att dela information om cybersäkerhet och cyberhot – inbegripet IP-adresser m.m. - där även privata aktörer deltar i informationsdelningen. Detta bör kunna ses som en indikation på att det finns utrymme i EU:s dataskyddsförordning[1] för privata aktörer att behandla information om cyberhot, inbegripet personuppgifter. SOFF konstaterar vidare att det numera är en skyldighet enligt artikel 29.1 i direktiv (EU) 2022/2555 (NIS-2-direktivet) att möjliggöra för privata aktörer att dela information om cyberhot.[2]

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[2] 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).

SOFF tillstyrker därför att regeringen säkerställer att:

- det finns rättslig möjlighet för privata entiteter som omfattas av NIS 2-direktivet att utbyta relevant information om cybersäkerhet, inbegripet eventuella personuppgifter, och att
- inte enbart privata entiteter som omfattas av direktivets tillämpningsområde, utan också *andra relevanta privata entiteter*, ges sådana rättsliga förutsättningar.

I tillägg till ovan föreslår SOFF att lagstiftaren överväger att göra bestämmelsen mer generellt tillämplig och inte begränsad till när en viss form av informationsutbyte sker enligt NIS2-direktivet.

Rättsliga förutsättningar att dela hotinformation om cyberangrepp idag

Föreningens uppfattning är att det idag råder otydliga, och möjligen obefintliga, rättsliga förutsättningar för att dela hotinformation om cyberangrepp mellan företag samt mellan företag och myndigheter. Detta försvårar möjligheten att snabbt upptäcka och bemöta cyberhot, vilket utgör en allvarlig risk för Sveriges säkerhet.

Artikel 10 i dataskyddsförordningen (EU) 2016/679 rör behandling av personuppgifter som rör fällande domar i brottmål samt överträdelser. Integritetsskyddsmyndigheten (IMY) har i sitt rättsliga ställningstagande IMYRS 2021:1 angett att artikel 10 inkluderar ”misstanke om brott”. Denna tolkning av artikel 10 begränsar möjligheten att dela information om cyberhot, exempelvis IP-adresser vid pågående cyberangrepp, i de fall dessa kan betraktas som personuppgifter och därmed omfattas av dataskyddsreglering vid misstänkt dataintrång.

SOFF noterar att IMY:s tolkning av artikel 10 GDPR är mer extensiv än IMY:s motsvarighet i andra EU-länder. Till exempel finns flera exempel på andra länder i Europa där staten tillsammans med privata aktörer driver en så kallad ”Malware Information Sharing Platform” (MISP), vilket är en teknisk plattform för att dela hotinformation. Föreningen respekterar att det kan finnas fall då det finns skäl att införa särskilt skydd för personuppgifter som rör misstanke om brott, men anser att tolkningen i detta fall får långtgående olämpliga konsekvenser med uppenbar fara för Sveriges säkerhet.

Dessutom kan den nuvarande ordningen stå i strid med EU-rätten, då artikel 29.1 i NIS-2-direktivet föreskriver att sådan information ska kunna delas inte bara mellan myndigheter, utan även med, från och mellan privata aktörer.

Oaktat IMY:s rättsliga ställningstagande om hur ”misstanke om brott” förhåller sig till artikel 10, så saknas det i vart fall rättsliga förutsättningar för privata entiteter att hantera information som faller inom tillämpningsområdet för artikel 10. Sådan behandling är enligt artikel 10 endast tillåten ”…då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt…”, och någon sådan möjlighet finns inte i svensk rätt idag.

Risken för att personuppgifter behandlas vid hotdelning om cyberangrepp

Enligt SOFF finns skäl att i detta sammanhang också resonera lite kring risken för att personuppgifter överhuvudtaget behandlas vid informationsutbyte om cyberangrepp.

Informationsdelning avseende cyberhot kan till exempel ske i en MISP. I en MISP hanteras bland annat IP-adresser och e-postadresser kopplade till misstänkta cyberhot eller andra skadliga incidenter. Dessa uppgifter kan i vissa fall, beroende på innehåll och karaktär, utgöra personuppgifter. Vidare kan ytterligare uppgifter om typen av hot och aktivitet registreras; sådana uppgifter kan endast utgöra personuppgifter om de kopplas till annan identifierande information.

I en MISP är det emellertid mycket osannolikt att informationen om delas utgör personuppgifter. IP-adresser är till exempel ofta är dynamiska och ”maskade”, vilket gör det svårt att spåra dem till en specifik användare på ett sådant sätt som krävs för att IP-adressen ska betraktas som en personuppgift. E-postadresser kan utgöra personuppgifter om de innehåller en persons namn eller annan identifierande information, vilket sannolikt endast kommer att förekomma i ytterst få fall i samband med rapportering i en MISP eller annan informationsdelning avseende cyberhot. Det måste antas att en stor majoritet av de som avsiktligen förbereder eller genomför ett cyberangrepp gör sitt yttersta för att dölja sin identitet, exempelvis genom att obehörigen nyttja en annan IP-adress och använda en för ändamålet särskilt framtagen e-postadress som inte går att härleda till en fysiskt identifierbar person.

Även om uppgifterna i en MISP nästan uteslutande därför kan väntas bestå av uppgifter där det föreligger en obefintlig eller försumbar risk för identifiering, går det sammantaget inte att utesluta all förekomst av personuppgifter i en MISP.

SOFF:s inställning till MSB:s hemställan

SOFF instämmer i och understryker vikten av att regeringen säkerställer att det finns effektiva möjligheter för både privata och offentliga aktörer att behandla och dela uppgifter om cyberhot, även om och när dessa uppgifter kan omfatta personuppgifter såsom IP-adresser och e-postadresser.

SOFF tillstyrker förslaget att inte enbart privata entiteter som omfattas av direktivets tillämpningsområde, utan också *andra relevanta privata entiteter*, ges rättsliga förutsättningar att behandla personuppgifter inom ramen för informationsdelning avseende cyberhot.

SOFF föreslår dock att lagstiftaren överväger att göra bestämmelsen mer generellt tillämplig och inte begränsad till när en viss form av informationsutbyte sker enligt NIS2-direktivet. Den nu föreslagna skrivningen skulle kunna tolkas motsatsvis som att den innebär att exempelvis IP-adresser som använts vid lagöverträdelser och som kan hänföras till enskilda personer inte får behandlas i de fall informationen inte ska delas genom detta särskilda förfarande. Det kan finnas andra situationer där det är legitimt för privata aktörer

att behandla denna typ av information och det vore olyckligt om den föreslagna skrivningen resulterar i att detta blir otillåtet.

Yttrandet har beretts av föreningens medlemsgrupp för Cyberförsvar.

Stockholm den 5 februari 2026.

För föreningen

Robert Limmergård
Generalsekreterare
SOFF