Försvarsdepartementet

Vår referens/dnr:
2025-300

Er referens/dnr:
Fö2025/01534

2026-02-05

Remissvar

Angående hemställan från Myndigheten för samhällsskydd och beredskap om att skapa rättsliga förutsättningar för behandling av personuppgifter rörande lagöverträdelser

Svenskt Näringsliv tackar för möjligheten att lämna kommentarer på hemställan.

Svenskt Näringsliv anser att hemställan bör bifallas och delar Myndigheten för civilt försvars övergripande ambition att stärka Sveriges cyberresiliens.

Svenskt Näringsliv noterar att MCF villkorar den rättsliga förutsättningen för att släppa in deltagande från privata aktörer i MISP-SE. I ljuset av det allvarligt försämrade säkerhetspolitiska läget är ett fungerande samarbete mellan offentliga och privata aktörer avgörande för att stärka Sveriges samlade motståndskraft. Ökad möjlighet till ett effektivt cyberförsvar är en förutsättning, men också en effektiv hantering av hybridhot, bakgrundskontroller och proaktiv hotidentifiering.

Vår omedelbara och högsta prioritet är att snabbt och på ett rättssäkert sätt möjliggöra för näringslivet att delta i nationella plattformar för informationsdelning, såsom MISP-SE. Ökad möjlighet till ett effektivt cyberförsvar, hantering av hybridhot, bakgrundskontroller och proaktiv hotidentifiering är områden som skyndsamt behöver åtgärdas.

Vår bedömning är dock generellt att MISP-SE inte kommer att avse informationsdelning av personuppgifter och sannolikt inte personuppgifter som rör fällande domar i brottmål eller lagöverträdelser som innefattar brott enligt artikel 10 GDPR. För att hindra spridning av skadlig kod, upptäcka intrång och bryta angripares möjligheter krävs snabb informationsdelning av indikatorer (IoC) och tekniska signaler om cyberangrepp (TTP). MISP-SE.

I mål C-582/14 Breyer slog EU-domstolen fast att till exempel dynamiska IP-adresser kan vara personuppgift för den aktör som har realistisk möjlighet att komplettera med identifierande information, men inte nödvändigtvis för en annan mottagare som saknar

sådana medel. De företag som kommer vara anslutna till MISP-SE saknar medel att koppla en IoC till en viss individ. Därav följer att de flesta IoC/TTP-poster (hashar, domäner, filnamn, malware-signaturer med mera) som kommer delas i MISP-SE inte är personuppgifter för de företag som behandlar uppgifterna. Uppgifterna är ofta förfalskade eller pseudonymiserade i flera led, vilket gör eventuella personuppgifter oidentifierbara (se skäl 26 GDPR, mål C-582/14, Breyer, och mål C-413/23 P, EDPS vs SRB, samt EU Digital Omnibus förslag om ändring av artikel 4 GDPR). Därmed faller stora delar av threat-intel som delas i MISP-SE utanför GDPR:s tillämpningsområde. I de undantagsfall där personuppgifter ändå kan förekomma (till exempel en kapad e-post eller IP-adress) grundas behandlingen av brottsoffrets uppgifter på artikel 6.1 f i kombination med skäl 49 som erkänner nät- och informationssäkerhet som ett berättigat intresse (se även EDPB:s riktlinjer 1/2024).

Avslutningsvis vill Svenskt Näringsliv understryka att bifallet av MCF:s hemställan inte på något sätt påverkar vår bedömning att IMY:s rättsliga ställningstagande bör ses över, bland annat eftersom ”misstanke om brott” anses omfattas av tillämpningsområdet för artikel 10.

SVENSKT NÄRINGSLIV

Carolina Brånby Frida Pamliden