Sveriges advokatsamfund

Stockholm den 6 februari 2026

R-2025/3001

Till Försvarsdepartementet
Fö2025/01534

Sveriges advokatsamfund har genom remiss den 5 december 2025 beretts tillfälle att yttra sig över hemställan från Myndigheten för samhällsskydd och beredskap (numera Myndigheten för civilt försvar) om att skapa rättsliga förutsättningar för behandling av personuppgifter rörande lagöverträdelser.

Sammanfattning

Advokatsamfundet avstyrker att den föreslagna bestämmelsen införs i den kommande cybersäkerhetsförordningen, i vart fall i sin nuvarande utformning. Skälen till Advokatsamfundets inställning är följande.

Synpunkter

Det rättsliga ställningstagande från Integritetsskyddsmyndigheten (IMY) som MCF stödjer sig på, dvs. IMY:s rättsliga ställningstagande IMYRS 2021:1, är för närvarande föremål för omprövning av IMY. Anledningen är bland annat att ställningstagandet blivit föremål för kritik då detta inte ansetts förenligt med artikel 10 i dataskyddsförordningen[1]. Ett införande av en specialregel i

[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).

cybersäkerhetsförordningen bör därför inte ske innan det uppdaterade rättsliga ställningstagandet har antagits.

Oaktat det rättsliga ställningstagandet är det enligt Advokatsamfundets uppfattning inte säkert att de IP-adresser som kommer att samlas in och delas inom MISP-SE överhuvudtaget utgör personuppgifter, och än mindre personuppgifter om lagöverträdelser enligt artikel 10 i dataskyddsförordningen. En stor andel av de IP-adresser som kommer att samlas in och delas via MISP-SE kommer sannolikt att vara s.k. dynamiska IP-adresser (som tilldelas olika entiteter vid olika tillfällen) eller NAT-adresser, dvs. publika IP-adresser som med hjälp av s.k. *Network Address Translation* delas av flera olika bakomliggande entiteter/individer. Sådana uppgifter kan vara personuppgifter, men som framgår av EU-domstolens praxis för äldre rätt är det inte fallet om ”identifieringen av den registrerade var förbjuden enligt lag eller praktiskt taget omöjlig på grund av att den kräver en oproportionerlig insats i form av tid, kostnader och personal, så att risken för identifiering i själva verket förefaller vara obetydlig”.[2] I fallet med MISP-SE ter det sig inte sannolikt att någon av deltagarna skulle ha möjlighet att genomföra en identifiering av bakomliggande användare. Sådana IP-adresser kommer i detta sammanhang alltså inte kunna härledas till en fysisk individ, och är således inte personuppgifter (och därmed heller inte personuppgifter om lagöverträdelser enligt artikel 10 i dataskyddsförordningen). Därför är förslaget på tillägg till cybersäkerhetsförordningen onödigt.

Om en särskild reglering trots allt bedöms vara nödvändig, anser Advokatsamfundet dock att det tilltänkta informationsutbytet som avses ske med stöd i artikel 29 i NIS 2[3] enligt den föreslagna bestämmelsen är alltför brett. Detta innebär att den tänkta begränsningen i den föreslagna bestämmelsen – att behandlingen ska vara nödvändig för att ”förhindra cyberangrepp eller förhindra dess effekter” inom ramen för informationsutbytesarrangemang enligt artikel 29 – inte blir särskilt begränsande.

Det är tydligt av innehållet i MCF:s hemställan att myndigheten främst tycks se framför sig att det kommer att vara fråga om behandling av IP-adresser i vissa begränsade fall. Enligt Advokatsamfundets bedömning finns det, med den föreslagna lydelsen av

[2] Se punkt 46 i EU-domstolens avgörande i mål C-582/14 (Breyer) av den 19 oktober 2016.
[3] 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).

bestämmelsen, dock ingenting som hindrar att MSB skapar ett register som innehåller såväl IP-adresser, misstänkta personer och/eller fällda brottslingar som utfört, eller misstänkt ha utfört, handlingar som utgör cyberhot/cyberattacker. Sådan information kan ju i högsta grad vara relevant för att ”förhindra cyberangrepp eller förhindra dess effekter”.

Enligt Advokatsamfundet måste regleringen vara mer precis utifrån det ändamål lagstiftaren vill uppnå. Advokatsamfundet förordar därför att den tilltänkta regleringen modifieras och kompletteras med ett krav på gallring av uppgifter inom en viss tid. Ett exempel på en mer balanserad och precis reglering av behandling av personuppgifter som innefattar lagöverträdelser finns t.ex. i 6 kap. 1–9 §§ lagen (2010:751) om betaltjänster. Ett annat exempel på reglering finns i 5 kap. 6 § lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism, se särskilt 5 kap. 6 § sistnämnda lag.

SVERIGES ADVOKATSAMFUND

Mia Edwall Insulander