Integritetsskyddsmyndigheten

Regeringskansliet, Försvarsdepartementet

Diarienummer:
IMY-2024-3404

Ert diarienummer:
Fö2024/00496

Datum:
2024-05-27

Yttrande över delbetänkandet nya regler om cybersäkerhet (SOU 2024:18)

Integritetsskyddsmyndigheten (IMY) har granskat förslaget huvudsakligen utifrån myndighetens uppgift att arbeta för att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter.

IMY lämnar följande tre synpunkter av mer väsentlig betydelse (avsnitt 1) och fem synpunkter av mindre betydelse (avsnitt 2).

1. Synpunkter av mer väsentlig betydelse

1.1 Föreskrifter om kraven på riskhanteringsåtgärder, systematiskt och riskbaserat arbete samt utbildning (avsnitt 7.1, 7.2, 8.4.5)

Utredningen bedömer att NIS2-direktivets krav om riskhanteringsåtgärder (artikel 21) bör regleras övergripande i den föreslagna cybersäkerhetslagen (3 kap. 1 §) och fyllas ut av föreskrifter. Denna föreskriftsrätt, som även omfattar kraven på systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning (3 kap. 2 och 3 §§), ska enligt den föreslagna cybersäkerhetsförordningen fördelas på elva tillsynsmyndigheter (8–13 §§) samt Myndigheten för samhällsskydd och beredskap (MSB) för en sektor (35 §).

Experter i utredningen från flera myndigheter[1] har fört fram att det istället borde ankomma på MSB att meddela en gemensam föreskrift med grundkrav på säkerhet och riskhanteringsåtgärder och att de olika tillsynsmyndigheterna, vid behov, kompletterar dessa genom att meddela föreskrifter med särskilda krav på utökad säkerhet för sina sektorer (s. 190 och s. 228). Utredningen bedömer dock att det inte vore lämpligt.[2] Istället föreslår utredningen att regeringen ger MSB i uppdrag att skyndsamt utarbeta en vägledning om riskhanteringsåtgärder till stöd för tillsynsmyndigheternas föreskriftsarbete (s. 189) och att det i cybersäkerhetsförordningen föreskrivs att MSB ska ges tillfälle att yttra sig innan sådana föreskrifter meddelas (35 § första stycket andra meningen).

IMY anser, även med beaktande av de skäl som utredningen för fram, att en gemensam föreskrift med grundkrav bör tas fram. Problemet med eventuella konflikter

[1] IMY, MSB, Säkerhetspolisen och Transportstyrelsen.
[2] De skäl som utredningen anför är i huvudsak att tillsynsmyndigheterna har kunskap om eventuella beaktandesvärda specifika förutsättningar inom sina sektorer, att normgivning och tillsyn bör hållas samman samt att skillnader kan uppstå när kommissionen utnyttjar sin befogenhet att anta genomförandeakter inom vissa sektorer (s. 227–230).

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

med kommissionens kommande genomförandeakter skulle eventuellt kunna lösas genom att dessa sektorer undantas.[3]

IMY bedömer att de åtgärder som utredningen föreslår inte framstår som tillräckliga för att motverka fragmentering. IMY undrar därvid även vad kravet på att MSB ska ges tillfälle att yttra sig innan tillsynsmyndigheterna meddelar föreskrifter (35 § första stycket andra meningen i den föreslagna cybersäkerhetsförordningen) materiellt tillför jämfört med 12 § förordningen (2024:183) om konsekvensutredningar. Vidare föreskrivs i 8 § andra stycket NIS-förordningen en skyldighet för MSB att lämna råd och stöd till tillsynsmyndigheterna och Socialstyrelsen när de tar fram föreskrifter om säkerhetsåtgärder. IMY noterar att motsvarande krav inte finns med i den föreslagna cybersäkerhetsförordningen och att anledningen till det inte berörs i utredningen.

IMY noterar att utredningen föreslår att det inom hälso- och sjukvårdssektorn bör vara Inspektionen för vård och omsorg (IVO) som får meddela föreskrifter och inte som idag Socialstyrelsen (s. 230). Det bör därvid noteras för den fortsatta beredningen att Riksrevisionen utifrån nuvarande ansvarsfördelning har rekommenderat regeringen att förtydliga Socialstyrelsens ansvar för att ta fram verksamhetsanpassat stöd till vårdens och omsorgens informationssäkerhetsarbete.[4]

1.2 Ansvar för tidigare led för säkerhet i leveranskedjan (avsnitt 7.1.2)

Utredningen föreslår att NIS2-direktivets krav på att rikshanteringsåtgärder bland annat åtminstone ska omfatta så kallad säkerhet i leveranskedjan (artikel 21.2 d) ska regleras övergripande i den föreslagna cybersäkerhetslagen (3 kap. 1 § första stycket 3) och fyllas ut genom föreskrifter. Utredningen diskuterar därvid frågan hur många led i kedjan som verksamhetsutövarens ansvar sträcker sig. Utredningen bedömer att en verksamhetsutövare endast behöver vidta riskhanteringsåtgärder i förhållande till sin leverantör, alltså att ansvaret endast sträcker sig ett led, vilket förefaller baseras på ordet ”*direkta*” i sista ledet i artikel 21.2 d (s. 194 f.).

IMY delar inte utredningens bedömning.

Ordalydelsen av artikel 21.2 d tyder snarare på att EU-lagstiftaren inte har haft för avsikt att utesluta att ansvar kan sträcka sig i flera led än ett. Detta eftersom det där förekommer två ord som ger uttryck för att det är en icke uttömmande lista. I artikeln 21.2 anges således att ”de åtgärder som avses […] *ska minst inbegripa*” och i led d att detta avser ”säkerhet i leveranskedjan, *inbegripet* säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess direkta leverantörer eller tjänsteleverantörer”.

Enligt IMY lär det finnas fall där ansvar bör kunna bli aktuellt för åtgärder i fler led. Det bör i sammanhanget påminnas om att kravet handlar om riskhanteringsåtgärder och huruvida verksamhetsutövaren kan hållas ansvarig eller inte för att inte ha vidtagit proportionerliga sådana i förhållande till någon i ett tidigare led. Det är i sig ett brett spektrum av åtgärder som skulle kunna vara proportionerliga beroende på omständigheterna i det enskilda fallet. Det kan visserligen handla om åtgärder i ett led, bland annat att genom i avtal med direkta leverantörer reglera om och i så fall hur

[3] Jämför MSB:s remissvar, dnr MSB 2024-03843-4, s. 9.
[4] Rapporten Informationssäkerhet i vård och omsorg – statens stöd och tillsyn (RiR 2024:6), https://www.riksrevisionen.se/rapporter/granskningsrapporter/2024/informationssakerhet-i-vard-och-omsorg---statens-stod-och-tillsyn.html.

underleverantörer får anlitas. Det kan dock även handla om åtgärder i förhållande till tidigare led, exempelvis att upprätthålla förmåga att under den tid som avtalet löper effektivt hämta in och reagera på information från andra källor än direkta leverantörer om kända brister i säkerhetsnivån hos leverantörens underleverantörer.

En jämförelse kan göras med vad som gäller enligt dataskyddsförordningen. Personuppgiftsansvariga får bara anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga säkerhetsåtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas (artikel 28.1). De ska bland i avtal reglera om, när, och hur underbiträden får anlitas (artikel 28.3 d). Enligt Europeiska dataskyddsstyrelsen (EDPB) innebär kravet på att bara anlita personuppgiftsbiträden som ger tillräckliga garantier en fortgående skyldighet för den personuppgiftsansvariga som regelbundet bör verifiera dessa garantier med ledning av en riskbedömning avseende den anförtrodda personuppgiftsbehandlingen.[5] Det kan inom ramen för det bli aktuellt att utkräva ansvar på motsvarande sätt enligt dataskyddsförordningen mot en personuppgiftsansvarig som inte har vidtagit tillräckliga åtgärder avseende underbiträden, alltså i flera led än ett.

Om lagstiftaren anser att utredningens bedömning är korrekt bör detta motiveras i det fortsatta beredningsarbetet. Vidare bör det av förutsebarhetsskäl övervägas att detta preciseras i lag eller förordning och inte överlåtas till att följa av föreskrifter, särskilt inte eftersom föreskriftsrätten enligt förslaget kommer att vara fördelad på tolv olika myndigheter.

1.3 Uppgiftsskyldighet för domännamnsregistreringsuppgifter (avsnitt 6.3)

Utredningen föreslår att lagen (2006:24) om nationella toppdomäner för Sverige på internet byter namn till lagen om toppdomäner på internet (toppdomänlagen) och ändras bland annat på så att det uttryckligen av toppdomänlagen ska följa att det är möjligt för myndigheter och andra med offentligrättsliga uppgifter inom EES att begära ut uppgifter på annat sätt av registreringsenheten för toppdomäner än genom internet och att de närmare bestämmelserna om detta bör följa av föreskrifter (avsnitt 6.3).

IMY ser positivt på att uppgiftsskyldigheten tydliggörs i lag eftersom, som utredningen påpekar, dataskyddsregleringen gäller vid hanteringen. Det bör dock övervägas att närmare beskriva den behandling som kan bli aktuell och konsekvenserna av den för de registrerade. Det bör exempelvis i förarbetena övervägas att lämnas anvisningar till stöd för den närmare regleringen i föreskrifter om uppgiftsskyldigheten. I dessa bör det tydliggöras att för prövningen av sådana utlämnanden har EU-domstolen betonat att när ett utlämnande av personuppgifter inte direkt grundar sig på den rättsliga bestämmelse som utgör stöd för utlämnandet, utan följer av en begäran från den behöriga myndigheten, måste det särskilda ändamålet med insamlingen av personuppgifterna – mot bakgrund av den aktuella uppgiften av allmänt intresse eller den aktuella myndighetsutövningen – framgå av begäran, så att den som begäran riktar sig till ska kunna försäkra sig om att överföringen av uppgifterna är laglig och för att lagenligheten ska kunna kontrolleras av domstolarna.[6]

[5] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1 Adopted on 07 July 2021, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en, punkterna 96 och 99.
[6] EU-domstolens dom Valsts ieņēmumu dienests, C-175/20, EU:C:2022:124, punkterna 66–71.

2. Synpunkter av mindre betydelse

2.1 Rättelse av direktivet (avsnitt 4.6, 5.3.2, 6.2.1, 8.4.2)

IMY vill uppmärksamma att den svenska språkversionen av NIS2-direktivet har rättats.[7] Således ska bland annat alla förekomster i direktivet av "leverantörer av hanterade tjänster" ersättas med "leverantörer av utlokaliserade driftstjänster" och "leverantör/leverantörer av hanterade säkerhetstjänster" ersättas med "leverantör/leverantörer av utlokaliserade säkerhetstjänster", med nödvändiga grammatiska anpassningar (punkt 6 och 7). Rättelsen förefaller inte ha beaktats av utredningen (jämför exempelvis därvid 1 kap. 2 § 16 och 1 kap. 6 § första stycket 8 i den föreslagna cybersäkerhetslagen).

2.2 Syfte och vad som ligger i en hög cybersäkerhetsnivå (avsnitt 5.1.2)

IMY instämmer i utredningens slutsats att det övergripande syftet i (rätteligen) den föreslagna cybersäkerhetslagen bör följa NIS2-direktivet semantiskt (avsnitt 5.1.2).

När det gäller utredningens fundering om vad som ligger i en hög nivå av cybersäkerhet och därvid all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, särskilt användare av dessa system och andra berörda personer mot cyberhot (s. 121 f.), kan konstateras att en hög cybersäkerhetsnivå som huvudregel lär medföra ett stärkt skydd av människors grundläggande fri- och rättigheter i samband med behandling av personuppgifter. Som EU-domstolen uttalat inrättas genom dataskyddsförordningen ett riskhanteringssystem avseende säkerheten vid behandling av personuppgifter genom kraven i artiklarna 5.1 f, 5.2, 24 och 32 på personuppgiftsansvariga att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa och påvisa en lämplig säkerhetsnivå.[8]

2.3 Offentlig förvaltning, Sveriges organisation och utredningens analys (avsnitt 5.2.4–5.2.6)

IMY invänder inte mot slutsatsen att regeringen inte lär omfattas av NIS2-direktivets definition av offentlig förvaltning, men ställer sig tveksam till utredningens motivering (avsnitt 5.2.6). Utredningen anför därvid att eftersom ordet "hos" används i direktivets bilaga 1 punkt 10 ("offentliga förvaltningsentiteter *hos* nationella regeringar såsom de definieras av en medlemsstat i enlighet med nationell rätt") bör rimligen regeringen falla utanför, trots att även regeringen är en myndighet enligt svenskt statsskick. I den engelska språkversionen används dock ett uttrycksätt som på svenska snarare motsvarar "offentliga förvaltningsentiteter *på* statlig nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt" ("public administration entities *of* central governments as defined by a Member State in accordance with national law"). Motsvarande även i artikel 2.2 f (i) i singular, där den svenska språkversionen också är "på statlig nivå".

[7] Se Rättelse, EGT L, 22.12.2023, s. 1 ((EU) 2022/2555) https://eur-lex.europa.eu/eli/dir/2022/2555/corrigendum/2023-12-22/oj.
[8] EU-domstolens dom 2023-12-14 Natsionalna agentsia za prihodite, C-340/21, EU:C:2023:986, punkt 29.

2.4 I vilken mån offentlig sektor omfattas och alternativt förslag (avsnitt 5.2.9–5.2.11)

IMY har inget att invända mot utredningens slutsats att NIS2-direktivet inte lär kräva att regeringen, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen och domstolarna omfattas (avsnitt 5.2.9 och 5.2.10).

Som utredningen påpekar skulle det kunna finnas fördelar i att låta hela den offentliga sektorn omfattas av den föreslagna cybersäkerhetslagens krav, som en så kallad lämplig ”bottenplatta” som i förekommande fall kompletteras av säkerhetsskyddslagen, även om utredningen inte haft möjlighet att lägga fram förslag om det (avsnitt 5.2.11).

Såvitt IMY förstår har EU-lagstiftaren uttryckligen i artikel 6.35 i direktivet undantagit *domstolarna* (som, vid en jämförelse med de franska, tyska och engelska språkversionerna, lär vara vad som avses snarare än ”rättsväsendet” utifrån svenskt språkbruk) och inte gjort några anpassningar i regleringen som syftar till att ta hänsyn till särdragen hos domstolarnas verksamhet, såsom exempelvis gjorts i dataskyddsförordningen gällande tillsynsmyndigheternas behörighet (artikel 55.3).

Om lagstiftaren skulle överväga en utvidgning trots att NIS2-direktivet inte kräver det, behöver vad utredningen anfört, om att det inte är effektivt att införa skyldigheter som det inte är lämpligt att bedriva tillsyn över och som inte skulle vara sanktionerade, bemötas (s. 164). Gällande det kan noteras att EU-domstolen i dom har betonat att även i situationer där tillsynsmyndigheten inte är behörig att utöva tillsyn måste domstolarna följa dataskyddsförordningens materiella bestämmelser.[9] Det kan alltså vara motiverat att införa skyldigheter som det inte är lämpligt att bedriva tillsyn över.

2.5 Jurisdiktion för enskilda verksamhetsutövare (avsnitt 5.3.2)

Gällande begreppet huvudsakligt verksamhetsställe föreslår utredningen omständigheter som bör vara styrande vid bedömningen och att dessa bör framgå av förordningen (3 § cybersäkerhetsförordningen). Dessa är i första hand platsen för beslut om riskhanteringsåtgärder, i andra hand platsen för cybersäkerhetsoperationer och i sista hand det etableringsställe som har flest anställda (s. 149). Det kan därvid noteras att motsvarande begrepp används i dataskyddsförordningen (artikel 4.16) för att avgöra om förordningens mekanism för en enda kontaktpunkt ska tillämpas. Europeiska dataskyddstyrelsen (EDPB) har nyligen tolkat begreppet i ett yttrande och därvid bland annat uttalat att avgörande bör vara om det huvudsakliga verksamhetsstället har befogenhet att fatta beslut om behandlingen.[10]

Detta yttrande har beslutats av enhetschefen Catharina Fernquist efter föredragning av avdelningsjuristen Olle Pettersson.

Catharina Fernquist, 2024-05-27 (Det här är en elektronisk signatur)

---

[9] EU-domstolens dom 2022-03-24 Autoriteit Persoonsgegevens, C-245/20, EU:C:2022:216, punkterna 25, 37 och 38.
[10] EDPB, 2024-02-13, Yttrande 04/2022, Opinion 04/2024 on the notion of main establishment of a controller in the Union under Art. 4.16(a) GDPR, punkt 12–27, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-042024-notion-main-establishment_en.