Inspektionen för vård och omsorg

2024-05-08 Dnr 6.1.1-08434/2024

Box 45184, 104 30 Stockholm
Telefon 010-788 50 00 ● registrator@ivo.se
www.ivo.se ● Org.nr 202100-6537

Avdelning syd
Birgitta Åkerson

Försvarsdepartementet
fo.remissvar@regeringskansliet.se

Remissvar över delbetänkandet Nya regler om cybersäkerhet, SOU 2024:18

Ert dnr Fö2024/00496

Inspektionen för vård och omsorg (IVO) bedömer sammantaget att förslagen i betänkandet innebär en tydligare och mer detaljerad reglering inom området.

IVO vill dock framföra följande synpunkter.

6.2 Register över väsentliga och viktiga verksamhetsutövare

”Av artikel 3.3 följer att medlemsstater senast den 17 april 2025 ska upprätta ett register över väsentliga och viktiga verksamhetsutövare samt verksamhetsutövare som erbjuder domännamnsregistreringstjänster.”

Utredningen föreslår att varje tillsmyndighet inom det egna tillsynsområdet, liksom idag, ska upprätta ett register över väsentliga och viktiga verksamhetsutövare. Dessa register ska sedan rapporteras till den gemensamma kontaktpunkten (MSB). IVO anser att ett centralt system för att samla in anmälningar och förändringar av anmälningar från verksamhetsutövarna vore mer ändamålsenligt. IVO anser inte att det är resurseffektivt att tillsynsmyndigheterna ska ta fram egna nya informationssystem för insamling av uppgifterna, för att sedan överföra information till MSB.

7.1.2 Riskhanteringsåtgärder

IVO önskar ett förtydligande vad som avses med en riskanalys. Är avsikten att samtliga risker som berör de nätverk och informationssystem som behövs hos en verksamhetsutövare samlas i *en* enda riskanalys?

IVO vill lyfta fram att i författningskommentarerna samt i direktivet (21.1-21.3) nämns inte "en riskanalys". I direktivet står: "De åtgärder som avses i punkt 1 ska baseras på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö från incidenter." IVO anser att det vore lämpligare att skrivningen i 3 kap 1 § förslag till lag om cybersäkerhet överensstämmer med skrivningen i direktivet.

8.4.5 Föreskrifter

Utredningen föreslår bl.a. att tillsynsmyndigheterna inom sitt tillsynsområde får meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning enligt 3 kap. 1-3 §§ förslag till lag om cybersäkerhet.

I utredningen föreslås också att när det gäller hälso- och sjukvårdssektorn ska det till skillnad mot i dag vara IVO i egenskap av tillsynsmyndighet, och inte Socialstyrelsen, som får utfärda föreskrifter. IVO anser inte att bemyndigandefrågan är tillräckligt utredd och IVO önskar ytterligare resonemang i denna del.

8.4.7 Samordning och informationsutbyte

Det har framförts ett behov av ökade möjligheter för MSB att vägleda tillsynsmyndigheterna och följa upp arbetet med tillsyn.

IVO delar uppfattningen som MSB, Livsmedelsverket och Transportstyrelsen framfört till utredningen, att MSB bör få utökade möjligheter att styra och samordna tillsynen och dess metodik för att uppnå likvärdighet mellan tillsynsmyndigheterna. Tillsynsmyndigheterna bör ha i uppdrag att aktivt bidra till samordningen.

Utredningen bedömer *”Om tillsyn över en verksamhetsutövare utövas av fler än en tillsynsmyndighet ska respektive tillsynsmyndighet inte utöva tillsyn gällande den del av verksamheten som anges som en annan tillsynsmyndighets tillsynsområde”* IVO vill uppmärksamma att skrivningen kan tolkas som att delar av en verksamhets nätverk och informationssystem som inte hör till en NIS-sektor kan hamna under tillsyn av flera tillsynsmyndigheter.

9.3 Vilka överträdelser kan läggas till grund för sanktioner?

I utredningen föreslås att tillsynsmyndigheten ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter enligt denna lag, eller föreskrifter som har meddelats med stöd av bestämmelserna om

1. skyldighet att utse företrädare enligt 1 kap. 6 §,
2. anmälningsskyldighet enligt 2 kap. 2 §,
3. riskhanteringsåtgärder enligt 3 kap. 1 §,
4. utbildning enligt 3 kap. 3 §, eller
5. incidentrapportering enligt 3 kap. 5–7 §§.

Enligt utredningens förslag ska tillsynsmyndigheterna därmed *inte* ha möjlighet att ingripa med sanktionsavgifter, föreläggande eller anmärkning om en verksamhetsutövare inte följer 3 kap 2 § förslag till lag om cybersäkerhet. IVO vill påpeka att ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete är grunden för att en verksamhetsutövare ska kunna välja och utforma riskhanteringsåtgärder (säkerhetsåtgärder). Arbetet med riskanalys och utvärdering är grundläggande beståndsdelar i ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete. Brister när det gäller det systematiska och riskbaserade informations- och cybersäkerhetsarbetet påverkar därför riskhanteringsåtgärderna.

I den nu gällande NIS-regleringen omfattas en verksamhetsutövares arbete med riskanalys som en grund för val av säkerhetsåtgärder av tillsyn och möjlighet att utfärda sanktion och föreläggande.

IVO föreslår att tillsynsmyndigheterna ges möjligheter att ingripa mot verksamhetsutövares brister i sitt systematiska och riskbaserade informations- och cybersäkerhetsarbete, genom *ytterligare en punkt* 4 i 5 kap 1 § i förslag till lag om cybersäkerhet *”Punkt 4 systematiskt och riskbaserat informations- och cybersäkerhetsarbete enligt 3 kap. 2 §.”*

_____

Beslut i detta ärende har fattats av generaldirektören Sofia Wallström. I den slutliga handläggningen har avdelningschefen Patrick Barringer, chefsjuristen Karin Lewin och enhetschefen Helene Klackenberg Ingrao deltagit. Föredragande har varit verksamhetsstrateg Birgitta Åkerson.

Beslutet har godkänts elektroniskt den 240513.