Försvarsdepartementet

103 33 Stockholm

Nya regler om cybersäkerhet (SOU 2024:18)

(Fö2024/00496)

Försäkringskassan har följande synpunkter på förslagen.

7.1 Övergripande lagreglering om riskhanteringsåtgärder

Den föreslagna lagstiftningen innehåller krav som är generellt utformade och som förväntas fyllas ut genom de föreskrifter som tillsynsmyndigheterna ska utfärda. Det är viktigt att de kommande föreskrifterna är tydliga om vad som förväntas av verksamheterna för att leva upp till kraven i lagstiftningen. En risk som Försäkringskassan ser för egen del är att de kommande föreskrifterna inte harmoniserar med Myndigheten för samhällsskydd och beredskaps nuvarande föreskrifter inom informationssäkerhet, vilket kan skapa otydlighet kring vad som gäller.

8.4.2 Tillsynsmyndigheter i Sverige

Det finns oklarheter gällande gränsdragningen mellan tillsynen över den offentliga förvaltningen och övriga tillsynsområden. Risken är att tillsynsområdena överlappar när en myndighet bedriver verksamhet inom en sektor som omfattas av det föreslagna regelverket. Till exempel erbjuder Försäkringskassan IT-drift, E-identitetskort (EFOS) och andra IT-tjänster till ett stort antal myndigheter. En del av den verksamheten skulle eventuellt kunna bedömas ingå i sektorn digital infrastruktur. Någon fullständig rättslig analys i dessa delar har dock inte funnits möjlighet att göra inom ramen för remissvaret.

Eftersom tillsynsmyndigheterna ska meddela föreskrifter inom sitt tillsynsområde kan överlappande tillsynsområden även innebära oklarheter kring vilka föreskrifter som gäller för verksamheten, eller att det finns flera olika föreskrifter som måste följas.

I avsnitt 8.4.7 i delbetänkandet finns resonemang kring samordning av tillsynen. I det avsnittet anges att det i möjligaste mån bör undvikas att en verksamhetsutövare står under tillsyn av flera myndigheter. Det är dock oklart hur denna målsättning tar sig uttryck i det föreslagna regelverket. Det föreslagna regelverket förefaller snarast innebära just att tillsynsansvaret kan överlappa.

En bestämmelse om vad som gäller när tillsynsområdena överlappar föreslås i 13 § i cybersäkerhetsförordningen. Så som den bestämmelsen är utformad är det dock tveksamt om den reglerar frågan om överlappning mellan offentlig förvaltning och andra sektorer. Offentlig förvaltning torde inbegripa hela den verksamhet som myndigheten bedriver, även sådan verksamhet som ingår i en särskilt utpekad sektor.

Försäkringskassan har redan Säkerhetspolisen som tillsynsmyndighet när det gäller den säkerhetskänsliga verksamheten och föreslås få länsstyrelsen som tillsynsmyndighet enligt nu aktuellt regelverk. Försäkringskassan anser inte att tillsynen bör fragmenteras ytterligare än så. Tillsynen över den offentliga förvaltningen borde endast ankomma på länsstyrelserna, oavsett om myndigheten skulle kunna anses bedriva verksamhet som

ingår i en särskilt utpekad sektor. Oavsett bör tillsynsmyndigheternas ansvarsområden klargöras.

12.7 Ekonomiska konsekvenser för offentliga verksamhetsutövare

Förslagen innebär att myndigheterna åläggs nya och obligatoriska uppgifter inom cybersäkerheten. Enligt utredningen bedöms förslagen leda till kostnader, men övergripande för den offentliga sektorn även besparingar. Försäkringskassan anser dock att det är tveksamt att det blir fråga om några större besparingar för den enskilda myndigheten. Myndighetens uppfattning är att förslagen måste finansieras fullt ut.

13 Ikraftträdande med mera

Cybersäkerhetslagen och cybersäkerhetsförordningen föreslås träda i kraft den 1 januari 2025. Bestämmelserna innebär att ett stort antal nya verksamhetsutövare omfattas av krav på riskhanteringsåtgärder och andra krav i lagstiftningen. De närmare kraven framgår dock inte av lag eller förordning, utan förväntas framgå i de föreskrifter som tillsynsmyndigheterna ska utfärda. Innan sådana föreskrifter har utfärdats är det svårt för verksamhetsutövarna att veta hur kraven i lagstiftningen ska uppfyllas.

Det valda sättet att lagstifta innebär att det i nuläget inte går att bedöma konsekvenserna av de föreslagna reglerna eftersom de exakta kraven kommer att tas fram i efterhand genom föreskrifter. Det är först när kraven är kända som det går att bedöma hur stora kostnader som förslagen kommer att innebära för Försäkringskassan. För att Försäkringskassan ska ha möjlighet att anpassa verksamheten till de framtida kraven måste myndigheten tillföras resurser som motsvarar de kostnadsökningar som uppstår.

Efter att kraven har klargjorts behöver verksamhetsutövarna också tid för att anpassa sin verksamhet till kraven. Något förslag på övergångsbestämmelser som medger tid för detta finns dock inte i delbetänkandet.

Enligt Försäkringskassans bedömning krävs det minst ett år av införandetid för att säkerställa att samtliga krav i lagstiftningen uppfylls. Detta gäller från det att myndigheten får kännedom om kraven, det vill säga från att föreskrifter i frågan har meddelats. Övergångsbestämmelserna behöver ses över för att medge en skälig införandetid. Åtminstone bör inte sanktionsbestämmelserna tillämpas förrän verksamhetsutövarna har getts skälig tid att implementera åtgärderna. Det är fråga om kraftfulla sanktioner som kan drabba verksamhetsutövarna, och även personliga konsekvenser för ledningspersoner, om kraven i lagen inte följs. Rättssäkerheten kräver att kraven måste vara kända och att verksamhetsutövarna ges tid att anpassa sig.

Försäkringskassan har inte några synpunkter på förslagen i övrigt.

Beslut i detta ärende har fattats av generaldirektör Nils Öberg i närvaro av överdirektör Maria Rydbeck, rättschef Marie Axelsson och rättslig expert Axel Jönsson, den senare som föredragande.

Nils Öberg

Axel Jönsson