Försvarsdepartementet Stockholm, 2024-05-27

YTTRANDE
Fö2024/00496
Till Försvarsdepartementet:
fo.remissvar@regeringskansliet.se
Kopia till:
visnja.raguz@regeringskansliet.se

Remiss av delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Med avseende på ovan remiss får Swedsoft härmed inkomma med yttrande.

Swedsoft ställer sig generellt bakom det yttrande som ***Teknikföretagen*** har skickat in till Försvarsdepartementet, och som följer nedan, samt bakom ***SOFFs*** yttrande specifikt (av den 240522) vad avser säkerhets- och försvarsföretag.

Teknikföretagen företräder svensk teknikindustri. Tillsammans står våra ca 4 500 medlemsföretag för en tredjedel av Sveriges export. Gemensamt för våra medlemsföretag är att de utvecklar varor och tjänster i världsklass och att nästan all försäljning sker i global konkurrens. Samtidigt som medlemsföretagen löser många av vår tids utmaningar skapar de tillväxt och välstånd i Sverige.

Teknikföretagen tackar för möjligheten att inkomma med synpunkter på ovan förslag och har sammanfattningsvis kommentarer inom följande områden.

- ***Samverkan*** *– vi önskar ett ökat fokus på tillitsfull samverkan mellan myndigheter och de sektorer och företag som de ansvarar för*
- ***Tillsyn*** *- strukturen med många (nya) tillsynsmyndigheter riskerar att leda till olika bedömningar och också att företag kan komma att stå under tillsyn av flera myndigheter och stärkt samordning behövs därför*
- ***Konsekvensanalys*** *- den gjorda analysen är bristfällig och uppfyller inte kraven men konsekvenserna för företagen behöver utredas*
- ***Tidplan*** *- det kommer att vara utmanande för såväl myndigheter som verksamheter att kunna förbereda sig och uppfylla de krav som ställs inom den tid som ges och en så kallad Grace period skulle kunna övervägas för att förenkla*
- *Det* ***svenska genomförandet*** *– förslaget går i delar utöver vad direktivet stadgar utan att det närmare analyseras vad effekterna av detta blir, trots att detta särskilt angavs i direktiven till utredningen*

Tillitsfull samverkan

Inledningsvis vill Teknikföretagen framhålla att vi självfallet instämmer i behovet av, och nyttan med, att alla delar av samhället ökar sin kunskap kring cybersäkerhet, genomför riskanalyser av den egna verksamheten och genomför de åtgärder som analysen visar behövs för att skydda sina digitala tillgångar och system. Vi kan alla göra mer och vi behöver lära av varandra och samarbeta för att öka vår gemensamma cybersäkerhet.

Som Teknikföretagen flera gånger också påpekat är en effektiv privat-offentlig samverkan fundamental för att stärka vår förmåga mot cyberhot. Vi välkomnar de initiativ och projekt som i andra fora har initierats inom området och vi ser fram emot fler samverkansformer. I linje med detta kan vi bara beklaga att den nu aktuella utredningen i stora delar saknar närmare skrivningar om vikten av sådan samverkan. Inte minst i skenet av att det föreslås utpekas en lång rad nya tillsynsmyndigheter anser vi att det hade varit såväl välkommet som behövligt om utredningen hade kunnat understryka vikten av konkret samverkan och samarbete mellan tillsynsmyndigheterna och företagen/verksamheterna inom de sektorer som de föreslås få ansvar för.

Det bör noteras att flertalet av de verksamheter som kommer omfattas av reglerna inte tidigare varit föremål för denna typ av regler och att det därför kan finnas ett särskilt stort behov av såväl informationsinsatser som rådgivning och vägledning. Detta gäller inte minst för alla de relativt sett små företag som omfattas av EU:s definition av att vara ett medelstort företag och därmed också av kraven. Vi vill vidare påpeka det beklagliga faktum att utredningens arbete i hög grad präglas av en brist på näringslivsdeltagande. Det har i den expertgrupp som tillsattes för att stödja utredningen inte funnits någon representant för näringslivet, vilket vi anser har försvårat och försvagat arbetet inte minst vad gäller att beskriva effekterna på företag som omfattas men också vad gäller att beskriva de utmaningar som finns och hur effektiv offentlig-privat samverkan kan bedrivas för att uppnå de målsättningar som direktivet, och därmed den svenska lagstiftningen, syftar till att uppnå.

Teknikföretagen uppmanar regeringen att i de uppdrag som kommer att ges till myndigheter att ansvara för tillsyn betonar vikten av att dessa etablerar och/eller fördjupar fora för förtroendefulla samarbeten med verksamheterna inom sina respektive sektorer.

Tillsyn – struktur och effekter

Teknikföretagen konstaterar att det redan i direktiven till utredningen angavs att nuvarande sektorsuppdelning av tillsynsansvaret fortsatt skulle vara strukturen. Det är därför inte förvånande, om än försvårande för ett effektivt genomförande och utmanande för såväl utpekade myndigheter som tillsynsobjekt, att detta innebär förslag på en rad nya tillsynsmyndigheter. Teknikföretagens medlemmar omfattas framför allt genom sektorn tillverkning vilken omfattar ett mycket stort antal

företag/verksamheter. För denna sektor är det främst fyra länsstyrelser som föreslås ska vara tillsynsmyndigheter.

Det bör noteras att dessa länsstyrelser, utöver ansvar för tillverkning, också föreslås ansvara för tillsyn av Sveriges samtliga kommuner, regioner, de flesta statliga myndigheterna liksom även för forskning. Ett oerhört omfattande tillsynsuppdrag med andra ord. Teknikföretagen känner sig tveksam till på vilket sätt dessa länsstyrelser kommer förmå sätta sig in i dessa sektorers förutsättningar, för att kunna meddela lämpliga föreskrifter inklusive om i vilken omfattningen anställda ska erbjudas utbildning (se 7.2).

En följd av en struktur med en lång rad olika tillsynsmyndigheter är att företag och verksamheter riskerar att bedömas olika baserat på vilken sektor de tillhör och alltså vilken tillsynsmyndighet de står inför. Det faktum att fyra länsstyrelser föreslås få ansvar utifrån geografiskt område kan dessutom riskera att leda till att det blir olika bedömning inom en och samma sektor. Teknikföretagen vill här peka på att Näringslivets regelnämnd, NNR, i granskning av länsstyrelsers arbete visat på betydande variationer i hur nationella regelverken tillämpas som inte kunnat förklaras på annat sätt än att reglerna helt enkelt tolkas olika och att det finns skillnader i attityden gentemot myndighetsutövandet. Detta är en källa till oro för Teknikföretagen – att våra medlemmar helt enkelt riskerar att bedömas olika endast på grund av var i landet de är verksamma och alltså vilken länsstyrelse de står under tillsyn av.

En ytterligare aspekt av den föreslagna strukturen är att företag och verksamheter riskerar att ställas under tillsyn av inte bara en utan flera myndigheter givet utredningens formulering att ”hela verksamheten” utgör tillsynsobjekt. Utredningen skriver förvisso på sid. 242 att ”Det får förutsättas att tillsynsmyndigheterna samarbetar vid genomförande av tillsyn rörande verksamhetsutövare som bedriver verksamhet i flera sektorer” och att detta inte behöver regleras här eftersom det följer av förvaltningslagen. Teknikföretagen befarar ändå att detta kan komma att leda till problem, och inte minst administrativ och regelmässig börda, för de företag och verksamheter som berörs och anser att detta är ytterligare ett argument till att överväga hur väl den sektorsuppdelning som föreslås kommer att fungera.

Det finns behov av att säkerställa en stärkt samordning mellan tillsynsmyndigheterna för att säkra enhetliga tolkningar och tillämpning av lagstiftningen och Teknikföretagen uppmanar regeringen vidta åtgärder för att uppnå detta.

Konsekvensanalys

Teknikföretagen instämmer i Regelrådets yttrande att redovisning avseende påverkan på företag är bristfällig. Det saknas helt analys av de ekonomiska effekterna på företag som kommer omfattas av förslaget, vilket inte kan ses som annat än att utredningen inte har uppfyllt sitt uppdrag enligt konsekvensutredningsförordningen (2007:1244). Som Teknikföretagen närmare redogör för under

avsnittet Det svenska genomförandet nedan saknas också analys av vilken påverkan kraven, som går utöver vad direktivet ställer, har på företagens konkurrenskraft.

Teknikföretagen uppmanar regeringen att omgående tillse att det utförs en analys av vilka konsekvenserna blir för företagen av de föreslagna skyldigheterna.

Tidplan

Förslaget till direktiv presenterades av EU-kommissionen i december 2020 och förhandlingarna, som resulterade i det nu antagna direktivet, slutfördes ganska precis två år senare i december 2022. Några månader senare fattade den svenska regeringen beslut om det kommittédirektiv som initierade den nu aktuella utredningen. Utredningen fick därefter lite drygt ett år på sig att slutföra sitt arbete och föreslå hur direktivet ska genomföras i svensk lag. Enligt det nu remitterade förslaget föreslås den nya svenska cybersäkerhetslagen att träda i kraft den 1 januari 2025. Givet att remisstiden löper till den 25 maj 2024 bör en slutligt beslutad ny svensk lag och uppdrag till berörda myndigheter med resurser, rimligen kunna vara på plats först under senhösten 2024. Detta leder i så fall till att såväl tillsynsmyndigheter som verksamheter/företag inom de utpekade sektorerna medges en mycket kort tid för att anpassa sig till de nya bestämmelserna, vara vissa inte heller i detalj kommer att kunna finnas på plats förrän ansvariga myndigheter har meddelat närmare föreskrifter. Det är således en oerhört utmanande tidplan. Enligt Teknikföretagens uppfattning hade regeringen bort vidta åtgärder för att kunna förbereda och senare genomföra direktivet redan under förhandlingarna (se även nedan om implementeringsråd). Hade dessutom representanter från näringslivet fått möjlighet till dialog och bistå med underlag och förslag under förhandlingsarbetet hade förberedelserna kunnat inledas långt tidigare än nu är fallet. Förutsättningarna för ett framgångsrikt genomförande, i termer av att vi gemensamt uppnår målen med att tillsammans öka cybersäkerheten, hade därmed sannolikt ökat väsentligt.

Den korta tidsfristen medför inte bara utmaningar för verksamheterna inom sektorerna utan så klart också för de tillsynsmyndigheter som får uppdrag. Teknikföretagen vill här särskilt peka på vikten av att myndigheterna får verkliga förutsättningar att kunna utföra sitt uppdrag och initiera samverkan med sektorerna. Utmaningarna med kompetensförsörjning inom cybersäkerhetsområdet är något som många aktörer länge pekat på och givet att det nu kommer bli såväl mer omfattande tillsynsuppdrag som fler tillsynsmyndigheter befarar Teknikföretagen att det kan komma att bli svårt att i vart fall inledningsvis säkerställa att det finns rätt kompetens på tillsynsmyndigheterna, något som vi ser riskerar att ytterligare försvåra genomförandet och slutligen uppfyllandet av syftet med lagstiftningen.

Givet den situation vi nu ändå är i vill Teknikföretagen att regeringen överväger att instruera de tillsynsmyndigheter som får uppdragen att tillämpa så kallade Grace periods. Givet den oerhört korta förberedelsetiden är det viktigt att tillsynsmyndigheterna inledningsvis fokuserar på att ge stöd till företag att kunna tillämpa lagstiftningen och inledningsvis är försiktiga i utfärdande av sanktioner. Inte minst då utredningen föreslår strikt tillämpning av dessa.

Det svenska genomförandet

EU:s inre marknad är svenska företags hemmamarknad och ungefär tre fjärdedelar av Sveriges utrikeshandel sker med övriga Europa. Genom den fria rörligheten, gemensamma produktregler och lika konkurrensvillkor har EU:s inre marknad bidragit till en oöverträffad marknadsintegration och liberalisering av handeln som idag är helt avgörande för en internationellt konkurrenskraftig industri i Sverige. Grundbultar för denna är fri rörlighet och harmoniserad lagstiftning, dvs att lagstiftningen ser lika ut och tillämpas lika i alla MS. Därför är överimplementering och nationella särkrav problematisk.

Även om ett direktiv ger utrymme för nationella kompletterande regler anser Teknikföretagen att EU-direktiv i Sverige bör genomföras i linje med vad som överenskommits i Bryssel och att vi alltså bör avhålla oss från att lägga på krav, inte minst för att inte ge oss själva och våra företag konkurrensnackdelar. Det är därför med oro och beklagande vi noterar att man i utredningen ändå väljer att lägga ett antal förslag som går längre än vad direktivet anger och utan att närmare analysera behovet och nyttan i förhållande till kostnaden av dessa. Detta står också i bjärt kontrast till det uppdrag utredningen fått ”Om förslag lämnas som går utöver EU-direktivens krav, ska utredaren särskilt motivera varför dessa är nödvändiga för att uppnå nationella svenska mål och göra en analys av om förslagen är samhällsekonomiskt effektiva och hur förslagen påverkar svenska företags konkurrenskraft.”[1]

Exempel på sådana extra krav är bl.a. kravet på cybersäkerhetsutbildning där det i direktivet står att all personal ska ”uppmuntras” att genomgå sedan medan utredningen föreslår ett krav att alla ska ”erbjudas”. Vidare föreslår utredningen att det personliga ansvaret för att uppfylla skyldigheterna i lagen ska åläggas enskilda styrelseledamöter. Detta är inte något som följer av direktivet och Teknikföretagen vill gärna framhålla att en styrelse fattar sina beslut kollektivt. Kravet på säkerhetsrevision – på tillsynsobjektets bekostnad - har heller inte sin grund i direktivet. Vad som semantiskt möjligen kan uppfattas som en mindre skillnad men som i praktiken är en reell skillnad är att utredningen föreslår att verksamheterna ska utföra ett systematiskt säkerhetsarbete medan direktivet kräver ett riskbaserat arbete. Samtliga dessa exempel på över-implementering riskerar att ge våra svenska företag högre kostnader för uppfyllandet än företag i andra medlemsstater, vilket naturligtvis påverkar svenska företags konkurrenskraft på den inre marknaden.

Enligt direktivet har EU-kommissionen befogenhet att genom delegerade akter föreskriva att vissa kategorier av entiteter ska vara skyldiga att använda vissa certifierade produkter. Om och när arbete med sådana akter inleds, är det viktigt att Sverige har en dialog med berört svenskt näringsliv.

---

[1] Dir 2023:30 sid 20

Teknikföretagen vill här gärna påpeka på de rekommendationer för en förbättrad beslutsprocess kring delegerade akter och annan följdlagstiftning som NNR publicerade den 7 december 2022.

Avslutningsvis ser Teknikföretagen att arbetet med NIS2 och det svenska genomförandet tjänar som ett tydligt exempel på behovet av att det av regeringen aviserade ***implementeringsrådet****. Som inte minst NNR pekat på är det brådskande att ett sådant inrättas så att Sverige på ett tidigare och tydligare sätt kan förbereda genomförande av EU-lagstiftning i svensk rätt genom att involvera näringslivet i tidigare skeden, identifiera särskilda nationella utmaningar och också planera för hur genomförandet rent faktiskt ska kunna genomföras i syfte att ge transparens och förutsebarhet. Här kan inspiration hämtas bl.a. från våra grannländer Danmark och Finland. Vi behöver säkerställa att genomföranden inte försämrar svenska företags konkurrenskraft jämte europeiska konkurrenters.*

Bästa hälsningar,

SWEDSOFT

Stefan Jakab

Generalsekreterare

Stefan Frank

Ordförande

+46 8 782 09 39

c/o Teknikföretagens Branschgrupper AB

Storgatan 5

Box 5510

114 85 Stockholm

I Swedsoft samlas organisationer från hela Sverige som har intresse för mjukvaruutveckling. Vår styrka ligger i den stora bredd av medlemmar som finns i föreningen. Här samlas några av våra största svenska företag, unga start-ups och andra SME-bolag från olika branscher med akademi, institut, organisationer med mera. Tillsammans i föreningen arbetar vi för att stötta svensk mjukvaruutveckling och säkra Sveriges framtida konkurrenskraft tillsammans.

www.swedsoft.se