NÄRINGSLIVETS REGELNÄMND

Försvarsdepartementet
Michael Cherinet
Via e-post: fo.remissvar@regeringskansliet.se

Stockholm	Ert dnr	Vårt dnr
2022-01-10	Fö2021/00796	2021/143

Remissvar angående utredningen Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)

Näringslivets Regelnämnd NNR har beretts tillfälle att avge yttrande över ovan nämnd remiss och anför följande;

Bakgrund
Europeiska unionen (EU) har antagit ett antal strategier, policys och förordningar för att stärka cybersäkerheten i unionen och medlemsstaterna. Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik trädde i kraft den 27 juni 2019. Det huvudsakliga syftet med förordningen är att uppnå en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen och säkerställa en väl fungerande inre marknad. Det europeiska ramverket för cybersäkerhetscertifiering, dvs. EU:s cybersäkerhetsakt och de genomförande-akter som utfärdas med stöd av cybersäkerhetsakten, kommer att reglera den cybersäkerhetscertifiering som följer av en europeisk certifieringsordning för cybersäkerhetscertifiering som fastställts av kommissionen.

Utredningens uppdrag innefattar bl.a. att bedöma om det finns anledning att införa nationella särskilda krav på att IKT-produkter, -tjänster och -processer, som ingår i ett nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet, ska vara certifierade enligt en nationell särskilt anpassad certifieringsordning utformad för säkerhetskänslig verksamhet. Regeringen framhåller i direktiven till utredningen att det måste kunna ställas särskilda krav på säkerhet på nätverks- och informationssystem för att skydda nationell säkerhet och att det finns anledning att överväga om ytterligare nationella krav bör införas för att säkerställa att nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet uppfyller de krav som behövs för att upprätthålla skyddet av sådana verksamheter.

Postadress:	Besöksadress:	Telefon:	E-post:	Internet:
Box 55695	Storgatan 19	08-762 70 90	info@nnr.se	www.nnr.se
102 15 STOCKHOLM				

I uppdraget ingår även att överväga om det finns anledning att införa krav på godkännande från en myndighet för att sådana IKT-produkter, -tjänster och -processer ska få tas i drift i viss eller all säkerhetskänslig verksamhet.

Bakgrund överimplementering
För att undvika och tydliggör de negativa effekter som överimplementering och kompletterande reglering (gällande EU-förordningar) innebär för svenska företag anser NNR att det är EU-lagstiftningens miniminivå som ska gälla vid genomförande och tillämpning. Konsekvensutredningen ska innehålla en beskrivning av miniminivån och en bedömning av om den kommer att överskridas. Det behöver redogöras för om:
- Nationella regelkrav läggs till utöver det som krävs i direktivet/förordningen.
- Området för reglernas tillämpning utvidgas.
- Möjligheter till undantag inte utnyttjas eller utnyttjas bara delvis när detta kan leda till hinder på den inre marknaden.
- Nationella regelkrav som är mer omfattande än vad som krävs av det aktuella direktivet/förordningen behålls.
- Kraven i ett direktiv genomförs tidigare än det datum direktivet kräver.
- Strängare sanktioner eller andra efterlevnadsmekanismer används än vad som är nödvändigt för att genomföra lagstiftningen på ett korrekt sätt.

I det fall miniminivån överskrids bör konsekvensutredningen innehålla en motivering till varför, en beskrivning av vilka genomförandeåtgärder som föreslås och en bedömning av vilka effekter detta får för företag. För att undvika att svenska företag får konkurrensnackdelar och högre kostnader i förhållande till sina konkurrenter behöver jämförelser också göras med hur övriga nordiska länder och andra EU medlemsstater planerar, respektive har genomfört eller tolkat EU-lagstiftning. Syftet med jämförelserna är att undersöka om mer effektiva alternativ finns, som kan användas i Sverige.

De centrala näringslivsorganisationerna i Danmark, Finland och Norge har tillsammans med NNR gjort följande ställningstagande i frågan: Utgångspunkten bör vara en princip om att genomförandet och tillämpningen/tolkningen av EU-rätten inte ska försämra företagens konkurrenskraft. Även den europeiska näringslivsorganisationen Business Europe har gjort motsvarande ställningstagande. (NNR hänvisar också till riksdagens tillkännagivande till regeringen ”EU-direktiv bör inte försämra företagens konkurrenskraft (NU 7)”), https://www.riksdagen.se/sv/dokument-lagar/arende/betankande/naringspolitik_h601nu7)

NNR anser att även tolkning och tillämpning av EU-förordningar bör göras på ett sätt som inte försämrar svenska företags konkurrenskraft och bör därför också omfattas av denna princip. (sidan 28 - https://nnr.se/wp-content/uploads/Starkt-konkurrenskraft-genom-ett-effektivare-genomforande-och-tillampning-av-EU-lagstiftning.pdf)

Konsekvenser
Det är tydligt att utredningen föreslår en relativt omfattande komplettering av den aktuella EU-förordningen om cybersäkerhet. På samma vis som NNR m.fl. ställer särskilda krav på konsekvensutredning vid överimplementering av EU-direktiv krävs särskilt tydlig motivering och konsekvensredovisning vid förslag om nationell lagstiftning som ska komplettera en EU-förordning. De aktuella förslagen om kompletterande lagstiftning riskerar att skapa administrativa bördor för företagen utan att i realiteten bidra till ökad cybersäkerhet och riskerar att försvaga de svenska företagens konkurrenskraft. Bl.a. risken för att en nationell

certifiering blir kostnadsdrivande och leder till att företag väljer att helt avstå från certifiering måste tas upp i konsekvensutredningen. Konsekvensutredningen behöver kompletteras.

NNR noterar att utredningen i kapitel 17 (Konsekvensbeskrivning) tar upp vissa administrativa effekter för företagen. Något som dock helt saknas är effekterna och riskerna för företagen av att aktuella myndigheter i sitt arbete kommer att få tillgång till säkerhetskänslig företagsinformation. NNR konstaterar att den tänkta tillsynsmyndighetens tillsyn kommer att medföra en icke obetydlig tillgång till företagens information. NNR uppfattar också att det kan antas vara sannolikt att tillsynsmyndigheten genom sina befogenheter får tillgång till information som för företagen i fråga är mycket skyddsvärd. Sådan information omfattas ofta av strikt företagssekretess och kan även omfattas av s.k. insiderlagstiftning och/eller sekretessavtal med utländsk stat och/eller med svenska eller utländska företag. NNR frågar sig vilka överväganden som utredningen har gjort när det gäller att skydda företagens information från otillbörliga aktörer, såväl inom som utom staten (inklusive den myndighet som utövar tillsynen).

Slutsats
NNR anser att överimplementering och/eller kompletterande reglering som huvudregel bör undvikas då det leder till ökade olikheter och minskad transparens om vilka regler som gäller på den inre marknaden. Vid övervägande att gå utöver EU-förordningens krav måste konsekvensutredningen innehålla en motivering till varför, en beskrivning av vilka genomförandeåtgärder som föreslås och en bedömning av vilka effekter detta får för företag. Utredningen saknar en genomgång av hur säkerheten för företagens känsliga information säkerställs och NNR finner därför att underlaget behöver kompletteras med avseende på de förslag till kompletterande reglering som föreslås samt med avseende på sekretessen för företagens information.

Näringslivets Regelnämnd NNR

August Liljeqvist