Regelrådet är ett särskilt beslutsorgan inom Tillväxtverket vars ledamöter utses av regeringen. Regelrådet ansvarar för sina egna beslut. Regelrådets uppgifter är att granska och yttra sig över kvaliteten på konsekvensutredningar till författningsförslag som kan få effekter av betydelse för företag.

Försvarsdepartementet

Yttrande över EU:s cyberhetssäkerhetsakt - kompletterande nationella bestämmelser om cybersäkerhetscertifiering (SOU 2020:58)

Regelrådets ställningstagande

Regelrådet finner att konsekvensutredningen inte uppfyller kraven i 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Innehållet i förslaget

Cybersäkerhetsutredningen föreslår kompletterande nationella bestämmelser till förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten) i en ny lag och förordning. Försvarets materielverk (FMV) föreslås utses till nationell myndighet och tillsynsmyndighet för cybersäkerhetscertifiering och det nationella certifieringsorganet vid myndigheten, CSEC, föreslås som ackrediterat organ för bedömning av överensstämmelse. FMV ska fullgöra de uppgifter som följer av EU-förordningen, däribland tillsyn. Myndigheten ska behandla klagomål som rör utfärdade EU-försäkran om överensstämmelse eller europeiska cybersäkerhetscertifikat. Myndigheten ska också kontrollera att tillverkare eller leverantörer som genomför självbedömning av överensstämmelse av IKT-produkter, IKT-tjänster och IKT-processer fullgör sina skyldigheter och att ett europeiskt cybersäkerhetscertifikat som utfärdas överensstämmer med kraven i den europeiska ordningen för cybersäkerhetscertifiering. Myndigheten ska även bistå det nationella ackrediteringsorganet (Styrelsen för ackreditering och teknisk kontroll, Swedac) med övervakning och kontroll av verksamhet som bedrivs av organen för bedömning av överensstämmelse. Utredningen föreslår att sanktionsavgifter, lägst 10 000 kronor och högst 15 miljoner, får påföras den som utfärdar en EU-försäkran om överensstämmelse utan att fastställda krav på cybersäkerhet är uppfyllda, lämnar oriktiga eller ofullständiga uppgifter vid ansökan om certifiering, underlåter att informera om sårbarheter och oriktigheter eller att lämna kompletterande säkerhetsinformation. FMV får vidare meddela de föreskrifter som behövs. Det föreslås även en ändring i offentlighets- och sekretessförordningen (2009:641). Den nya lagen och övriga författningsändringar föreslås träda i kraft den 28 juni 2021.

Skälen för Regelrådets ställningstagande

Bakgrund och syfte med förslaget

Utredningen beskriver digitaliseringen som vår tids starkaste förändringsfaktor och innebär att en allt större andel av aktiviteterna i samhället är beroende av nätverk och informationssystem som används av myndigheter, organisationer, företag och privatpersoner. Den digitala utvecklingen ger stora

möjligheter att förbättra och effektivisera människors vardag och olika verksamheter. Digitaliseringen har skapat nya former av kommunikation, datahantering och datalagring och idag bygger många system för att hantera information huvudsakligen på digital informations- och kommunikationsteknologi (IKT). Med den tilltagande digitaliseringen och globaliseringen, som ökar beroenden över nations-, sektors- och ansvarsgränser, har följt en ökad betoning på cyberfrågor i samhället. Samtidigt som allt fler länder utvecklar strategier, doktriner och förmågor inom cyberområdet ökar förekomsten av cyberattacker som kan vara politiskt, ekonomiskt och brottsligt motiverade, men även oavsiktliga incidenter som påverkar cybersäkerheten ökar. Den kraftiga tillväxten av sakernas internet, molnet och stordata medför större utsatthet för säkerhetsbrister. Cyberincidenterna kan t. ex. störa tillhandahållandet av nödvändiga tjänster, exempelvis vatten, hälso- och sjukvård, elektricitet och mobila tjänster. Möjligheterna till påverkan i informationssystem i demokratiska valprocesser och desinformationskampanjer är också en utmaning. Genom att samhället och människorna blir alltmer beroende av digital infrastruktur och tjänster genom anslutna enheter och utbredd uppkoppling till internet ökar sårbarheten mot cyberattacker till alltmer oroande nivåer. Därutöver syns en ökad hotbild avseende antagonistiska aktörer med hög förmåga till cyberattacker. Vikten av fullgod informations- och cybersäkerhet ökar i motsvarande grad.

Genom att kontrollera och certifiera produkter, tjänster och processer kan man göra dem säkrare och därigenom även öka förtroendet för dessa. Det finns certifieringsordningar inom ett stort antal områden, bl.a. inom informationssäkerhetsområdet men även på områden som lednings-, miljö- och trafikledningssystem samt inom hälso- och sjukvård. Motsvarande gäller för provning och kontroll inom dessa områden, som utförs av olika ackrediterade organ för bedömning av överensstämmelse med fastställda krav och standarder. Certifieringar, prov och kontroller som utförs av ackrediterade organ för bedömning grundas i stor utsträckning på internationella standarder. Avtal om ömsesidigt erkännande av certifikat inom EU har ingåtts mellan några av medlemsstaterna, men eftersom avtalen inte omfattar alla medlemsstater begränsas dess tillämplighet och genomslag samt effektiviteten på den inre marknaden. Ett certifikat utfärdat av en nationell myndighet för cybersäkerhetscertifiering erkänns dessutom i begränsad omfattning av andra medlemsstater, vilket medför att inom EU är cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer begränsad och fragmenterad. Företag kan därför behöva certifiera sina IKT-produkter, IKT-tjänster och IKT-processer i flera medlemsstater där de bedriver verksamhet, vilket är kostsamt. I syfte att uppnå en hög nivå av cybersäkerhet, cyberresiliens och förtroende inom EU och sträva efter att säkerställa en väl fungerande inre marknad antogs därför en ny EU-förordning, den s.k. cybersäkerhetsakten. Förordningen är uppdelad i två delar, där den första delen reglerar Enisa:s mandat och uppgifter för att stärka informations- och cybersäkerheten i unionen. Genom den andra delen införs ett europeiskt ramverk för cybersäkerhetscertifiering som bl.a. ålägger medlemsstaterna att utse nationella myndigheter med ansvar för certifierings- och tillsynsverksamheten samt i de nationella rättsordningarna införa sanktionssystem och effektiva rättsmedel i syfte att säkerställa en ändamålsenlig och effektiv tillämpning av cybersäkerhetsakten i medlemsstaterna, vilket är sådana förslag som utredningen lägger fram.

Cybersäkerhetsakten innebär vidare ett ramverk för upprättande av europeiska ordningar för cybersäkerhetscertifiering, som ska antas genom genomförandeakter. Innehållet i sådana ordningar är i dagsläget inte känt och det är inte heller klart i vilken utsträckning olika certifieringar kommer att bli frivilliga eller tvingande. Utredningen anger att man i slutbetänkandet, som ska redovisas senast den 1 mars 2021, ska överväga om det bör införas krav på certifiering och godkännande av vissa produkter, tjänster och processer som ska användas i verksamheter som är av betydelse för Sveriges säkerhet. Denna del av uppdraget ska redovisas senast den 1 mars 2021.

Regelrådet finner redovisningen av bakgrund och syfte godtagbar.

Alternativa lösningar och effekter av om ingen reglering kommer till stånd

Utredningen anger att cybersäkerhetsakten är en EU-förordning vars bestämmelser har direkt effekt och tillämpning i medlemsstaten, men även förutsätter kompletterande nationell lagstiftning. Det gäller bland annat artiklarna 58, 64 och 65. Av artikel 58 följer att medlemsstaterna ska utse en eller flera nationella myndigheter för cybersäkerhetscertifiering och som ansvariga för tillsynsuppgifterna i medlemsstaten. Av artikel 64 följer att fysiska och juridiska personer ska ha rätt till effektiva rättsmedel i de fall som anges i bestämmelsen. Av artikel 65 framgår att medlemsstaterna ska fastställa regler om sanktioner vid överträdelse av artiklarna 49–65 och ska vidta alla nödvändiga åtgärder för att se till att de tillämpas. Utredningen redovisar sina överväganden i dessa delar.

Regelrådet finner redovisningen av alternativa lösningar och effekter av om ingen reglering kommer till stånd godtagbar.

Förslagets överensstämmelse med EU-rätten

Utredningen redovisar utförligt för det EU-rättsliga ramverket liksom olika strategier, policybeslut och internationella samarbeten på området. Såvitt Regelrådet kan bedöma har utredningen tillräckligt väl visat hur förslagen på kompletterande bestämmelser förhåller sig till aktuella rättsakter.

Regelrådet finner redovisningen av förslagets överensstämmelse med EU-rätten godtagbar.

Särskild hänsyn till tidpunkt för ikraftträdande och behov av speciella informationsinsatser

Utredningen anger att EU-förordningen trädde i kraft den 27 juni 2019 och började tillämpas direkt med undantag för de artiklar som kräver kompletterande bestämmelser på nationell nivå. Dessa bestämmelser ska börja tillämpas den 28 juni 2021. Den nya lagen och förordningen med kompletterande bestämmelser föreslås träda ikraft detta datum. Det saknas uppgifter om eventuella behov av speciella informationsinsatser.

Regelrådet finner redovisningen av särskild hänsyn till tidpunkt för ikraftträdande godtagbar, men redovisningen av behov av speciella informationsinsatser bristfällig.

Berörda företag utifrån antal, storlek och bransch

Utredningen anger att förslaget framför allt berör de ekonomiska aktörer som utfärdar EU-försäkran om överensstämmelse eller europeiska cybersäkerhetscertifikat eller innehar ett sådana certifikat. Mot bakgrund av att det ännu inte fastställts någon europeisk ordning för cybersäkerhetscertifiering är det svårt att ange vilka och hur många företag som berörs, men det rör sig om såväl företag som tillverkar eller levererar produkter och tjänster som företag som använder sig av dessa. De aktörer som ansöker om europeisk cybersäkerhetscertifiering kan komma att variera beroende på utvecklingen av de europeiska certifieringsordningarna och huruvida certifiering blir frivillig eller obligatorisk. Utredningen anger att dessa kan komma att inkludera bl.a. tillverkare, importörer eller användarorganisationer för olika grupper av IKT-produkter, leverantörer av molntjänster, mjukvaruutvecklare och leverantörer av IKT-infrastruktur. Även andra aktörer som använder informations- och kommunikationsteknik kan förväntas beröras av förslagen. Det anges att de aktörer som berörs finns inom många olika branscher och verksamhetsområden och att aktörerna utgörs av stora, medelstora och små företag. Såväl tillverkare som leverantörer kan vara belägna i Sverige, annan medlemsstat eller tredje land. Utredningen anger att Sveriges certifieringsorgan för IT-säkerhet, CSEC, vid FMV behandlade cirka 30 certifieringar under 2019.

Regelrådet gör följande bedömning. Regelrådet inser svårigheterna med att uppskatta både antal och storlek på de företag som kan komma att beröras av förslaget. Regelrådet anser emellertid att utredningen borde ha redovisat betydligt mer information än vad som är fallet. Exempelvis kunde man ha resonerat kring hur många svenska företag som idag tillverkar och importerar olika typer av IKT-produkter eller tjänster och kring deras storlek. Det hade också varit möjligt att redovisa eventuell förekomst av privata organ för bedömning av överensstämmelse på cybersäkerhetsområdet, liksom i vilken utsträckning det idag finns företag som är cybersäkerhetscertifierade samt eventuell efterfrågan i olika branscher.

Regelrådet finner därför redovisningen av berörda företag utifrån antal, storlek och bransch bristfällig.

Påverkan på berörda företags kostnader, tidsåtgång och verksamhet

Utredningen anger att det är svårt att identifiera några omedelbara konsekvenser för näringsliv och företag bl.a. mot bakgrund av att det ännu inte fastställts någon europeisk ordning för cybersäkerhetscertifiering. Förslaget om att utse en nationell myndighet för cybersäkerhetscertifiering i stället för att ansvaret fördelas på flera myndigheter bedöms både förenkla och begränsa de ekonomiska aktörernas kontakter med myndigheter. Förslaget om att berörda myndigheter så långt det är möjligt ska samverka när det berör frågor om cybersäkerhetscertifiering förväntas ha positiva effekter för de ekonomiska aktörerna. Utredningen anger vidare att de ekonomiska aktörerna gynnas av att myndigheterna i större utsträckning kan lämna information mellan sig och samverka runt kontroller, vilket anges kan antas särskilt positivt för mindre företag som inte har samma resurser att lägga på den administrativa delen av verksamheten som större aktörer.

Regelrådet gör följande bedömning. Regelrådet inser svårigheterna med att redovisa kvantitativa uppgifter, men mer utförlig information hade varit behövlig. Det borde exempelvis varit möjligt att redovisa vilka kostnader som vanligtvis är förknippade med jämförbara certifieringsordningar för produkter, tjänster eller processer, inkl. kostnader och tidsåtgång för ansökningsprocesser och tillsyn.

Regelrådet finner redovisningen av påverkan på berörda företags kostnader, tidsåtgång och verksamhet bristfällig.

Påverkan på konkurrensförhållandena för berörda företag

Utredningen anger att innehållet i de framtida europeiska certifieringsordningarna, och hur väl svenska företagsprodukter m.m. motsvarar kraven i dessa ordningar, kan antas komma att påverka svenska företags konkurrenskraft. Utredningen anger även att en effektiv tillsyn ökar förutsättningarna för att företagare ska kunna konkurrera på lika villkor. Utredningen anger att de föreslagna bestämmelserna på sikt förväntas bidra till ökad cybersäkerhet och en bättre fungerande marknad, vilket i förlängningen är till fördel för både ekonomiska aktörer och unionsmarknadens funktion.

I direktiven anges att utredningen ska beakta de konsekvenser som bl.a. införandet av det europeiska ramverket för cybersäkerhetscertifiering kan få när det gäller internationell handel med tredjeland. Utredningen anger att det av tidsskäl inte varit möjligt att genomföra en djupare analys av dessa frågor, men redogör för några slutsatser som återfinns i en rapport från Kommerskollegium (*The Cyber Effect – the implications of IT security regulation on international trade*). I rapporten framhålls att myndigheter ofta inför specifika, nationella regler som kompletterar, eller fungerar som alternativ till, befintliga internationella standarder. Detta motiveras med att det finns särskilda nationella säkerhetsbehov. Dessa nationella standarder eller certifieringskrav leder till att företag måste genomgå certifieringar i flera länder, vilket leder till ökade kostnader. Vidare framhålls att de åtgärder som myndigheter vidtar när det gäller it-säkerhet karakteriseras av specifika nationella behov med säkerhet som prioritet, snarare än

åtgärder som följer internationella standarder och åtaganden som beaktar handel och marknadstillträde. Denna utveckling, där åtgärder för nationell säkerhet prioriteras på bekostnad av handel och varors marknadstillträde, är inte förvånande eftersom det får anses naturligt att vilja dölja hemligstämplad eller skyddsvärd information från utomstående, men konsekvensen av sådana nationella regler, som när det gäller it-säkerhet ofta är icke-transparenta, blir densamma som för reglering inom andra områden, d.v.s. en fragmentering av regleringar som riskerar att skapa handelshinder. I rapporten påpekas att även om EU:s cybersäkerhetsakt har som målsättning att bidra till mer harmoniserade ordningar för bedömning av överensstämmelse har tillfrågade företag betonat att IKT-marknaden är global och att det således krävs internationellt accepterade lösningar för reglering. Utredningen bedömer att det finns skäl att återkomma till dessa frågor även i det fortsatta arbetet med analys av behovet av certifiering eller godkännande av informations- och kommunikationssystem i säkerhetskänslig verksamhet.

Regelrådet gör följande bedömning. Utredningen har redovisat en hel del värdefull information och angivit att förslaget kommer att påverka konkurrensen för berörda företag. Det hade emellertid varit önskvärt med en mer detaljerad redogörelse med utgångspunkt från svenska företag i relation till europeiska och globala motsvarigheter. Då utredningen aviserar att detta delvis kommer att behandlas i slutbetänkandet samt att det är svårt att förutse innehåll – och därmed konsekvenser av – framtida europeiska certifieringsordningar, anser Regelrådet att beskrivningen är tillräcklig i detta ärende.

Regelrådet finner därför redovisningen av förslagets påverkan på konkurrensen godtagbar.

Regleringens påverkan på företagen i andra avseenden

Såvitt Regelrådet kan bedöma förekommer ingen redovisning av regleringens påverkan på företagen i andra avseenden. Mot bakgrund av redan angiven information samt förslagets karaktär finner dock Regelrådet avsaknad av sådan redovisning godtagbar.

Särskilda hänsyn till små företag vid reglernas utformning

Såvitt Regelrådet kan bedöma finns ingen redovisning av särskilda hänsyn till små företag vid reglernas utformning och finner därför denna aspekt bristfällig.

Sammantagen bedömning

Utredningen har gjort en grundlig genomgång av behovet av kompletterande nationella bestämmelser till EU:s cyberhetsakt och tydligt redovisat sina överväganden i dessa aspekter. Bakgrund och problembild är väl beskriven och det finns mycket värdefull information i betänkandet. Det förekommer emellertid vissa brister. Redovisningen av berörda företag och det nya regelverkets konsekvenser för företag är otillräcklig, även om Regelrådet har förståelse för svårigheterna mot bakgrund av att det ännu inte finns några antagna ordningar för cybersäkerhetscertifiering med stöd av förordningen. Regelrådet vill uppmuntra till kompletterande uppgifter i Cybersäkerhetsutredningens slutbetänkande.

Regelrådet finner att konsekvensutredningen inte uppfyller kraven i 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Stöd till regelgivare i konsekvensutredningsarbetet finns i Tillväxtverkets handledning för konsekvensutredning.

Regelrådet behandlade ärendet vid sammanträde den 27 januari 2021.

I beslutet deltog Elisabeth Thand Ringqvist, Hans Peter Larsson, Claes Norberg och Lennart Renbjer.

Ärendet föredrogs av Anna Stattin.

Elisabeth Thand Ringqvist
Ordförande

Anna Stattin
Föredragande