Regeringen

Dir. 2019:73

# Kommittédirektiv

## Cybersäkerhet – genomförandet av cybersäkerhetsakten och vissa åtgärder till skydd för säkerhetskänslig verksamhet

Beslut vid regeringssammanträde den 31 oktober 2019

### Sammanfattning

En särskild utredare ska föreslå de anpassningar och kompletterande författningsbestämmelser som cybersäkerhetsakten ger anledning till. Syftet är att säkerställa att den kompletterande nationella reglering som behövs finns på plats när hela förordningen börjar tillämpas den 28 juni 2021. Utredaren ska också överväga om det finns anledning att införa ytterligare krav för att skydda verksamheter som är av betydelse för Sveriges säkerhet.

Utredaren ska bl.a.

- undersöka vilka kompletterande nationella föreskrifter, exempelvis processuella bestämmelser och bestämmelser om sanktioner, som förordningen kräver eller Sverige bör införa,
- föreslå vilken befintlig myndighet som ska få i uppdrag att vara tillsynsmyndighet,
- analysera om, och i så fall föreslå vilka kompletterande bestämmelser som bör införas dels om självbedömning av överensstämmelse med de krav som ställs i certifieringsordningar och dels om organ för bedömning av överensstämmelse i den svenska regleringen,
- bedöma 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 och föreslå hur ett sådant system skulle kunna utformas, och

- lämna sådana författningsförslag som i övrigt behövs och är lämpliga.

Uppdraget ska i den del som avser anpassningar med anledning av EU-förordningen redovisas senast den 1 juni 2020. I den del som avser regler för verksamheter som är av betydelse för Sveriges säkerhet ska uppdraget redovisas senast den 1 mars 2021.

### Den nya regleringen – cybersäkerhetsakten

Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) trädde i kraft den 27 juni 2019. Förordningen började tillämpas direkt med undantag för vissa artiklar som kräver kompletterande bestämmelser på nationell nivå och som därför ska börja tillämpas först den 28 juni 2021. Det huvudsakliga syftet med förordningen är att säkerställa en väl fungerande inre marknad och samtidigt sträva efter att uppnå en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen.

Förordningen är uppdelad i två delar. Den första delen gäller fastställandet av mål, uppgifter och organisatoriska frågor som rör Enisa. Denna del kräver enligt regeringens bedömning ingen särskild kompletterande nationell reglering från medlemsstaternas sida. Den andra delen reglerar fastställandet av ett europeiskt ramverk för cybersäkerhetscertifiering. Syftet är att säkerställa en tillfredsställande nivå i fråga om cybersäkerhet för informations- och kommunikationsteknik (IKT) i unionen samt att undvika en fragmentering av den inre marknaden när det gäller certifieringsordningar i unionen. Skapandet av europeiska ordningar för cybersäkerhetscertifiering kommer att medföra att certifikat som utfärdas enligt dessa certifieringsordningar blir giltiga och erkända i alla medlemsstater. Förutom att beskriva de säkerhetsmålsättningar som ska beaktas i utformningen av de europeiska ordningarna för cybersäkerhetscertifieringar, anger förordningen vad minimiinnehållet i sådana ordningar bör vara. Förordningen anger också väsentliga funktioner och uppgifter för Enisa inom cybersäkerhetscertifiering. Kommissionen kommer att utarbeta löpande arbetsprogram för europeisk cybersäkerhetscertifiering där det fastställs strategiska prioriteringar för framtida europeiska ordningar för cybersäkerhetscertifiering. De europeiska certifieringsordningarna kommer sedan att utarbetas av Enisa, med hjälp av expertråd och i nära samarbete med den europeiska gruppen för cybersäkerhetscertifiering (ECCG), som också har inrättats genom förordningen. Gruppens uppgifter regleras i

förordningen och består bl.a. i att ge råd till och bistå kommissionen vad gäller cybersäkerhetscertifiering och utarbetande av de europeiska ordningarna för cybersäkerhetscertifiering. En annan uppgift för gruppen är att underlätta anpassningen av de europeiska ordningarna till internationellt erkända standarder och att, där så är lämpligt, lämna rekommendationer till Enisa om att samarbeta med relevanta internationella standardiseringsorganisationer för att åtgärda brister eller luckor i de befintliga internationellt erkända standarderna. Kommissionen ska, med stöd från Enisa, vara ordförande i gruppen. Kommissionen antar sedan de europeiska ordningarna för cybercertifiering genom genomförandeakter.

En europeisk ordning för cybersäkerhetscertifiering får innehålla en eller flera av följande assuransnivåer för IKT-produkter, IKT-tjänster och IKT-processer, dvs. på vilken nivå produkten, tjänsten eller processen har utvärderats: ”grundläggande”, ”betydande” eller ”hög”. Varje europeiskt cybersäkerhetscertifikat kan avse någon av assuransnivåerna medan EU-försäkran om överensstämmelse endast kan avse assuransnivån ”grundläggande”. De säkerhetskrav som motsvarar varje assuransnivå ska anges i den relevanta europeiska ordningen för cybersäkerhetscertifiering. Certifikatet eller EU-försäkran om överensstämmelse ska hänvisa till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, som syftar till att minska risken för eller förhindra cybersäkerhetsincidenter. Ett europeiskt cybersäkerhetscertifikat eller en EU-försäkran om överensstämmelse med assuransnivån ”grundläggande” ska försäkra att motsvarande säkerhetskrav är uppfyllda, inbegripet säkerhetsfunktioner, och att utvärderingen har skett på en nivå som avser att minimera kända grundläggande risker för incidenter och cyberattacker. Den utvärdering som ska göras ska innefatta åtminstone en granskning av den tekniska dokumentationen. Om en sådan granskning inte är lämplig ska alternativa utvärderingsinsatser med likvärdig effekt utföras. Om en europeisk ordning för cybersäkerhetscertifiering ger möjlighet till självbedömning av överensstämmelse bör det vara tillräckligt att tillverkaren eller leverantören har gjort en självbedömning av IKT-produktens, IKT-tjänstens eller IKT-processens överensstämmelse med certifieringsordningen. För assuransnivån ”betydande” bör utvärderingen, utöver kraven för assuransnivån ”grundläggande”, åtminstone omfatta en kontroll av överensstämmelsen mellan IKT-produktens, IKT-tjänstens eller IKT-processens säkerhetsfunktioner och den tekniska dokumentationen. För assuransnivån ”hög” bör utvärderingen, utöver kraven för assuransnivån ”betydande”, åtminstone omfatta ett effektivitets-

test som bedömer resistensen hos IKT-produktens, IKT-tjänstens eller IKT-processens säkerhetsfunktioner gentemot genomtänkta cyberangrepp som utförs av personer med betydande kompetens och resurser. En europeisk ordning för cybersäkerhetscertifiering kan ha flera olika utvärderingsnivåer beroende på hur stringent och djupgående den aktuella utvärderingsmetoden är.

Enligt förordningen ska övervakning, tillsyn och verkställighetsuppgifter framför allt ligga hos medlemsstaterna. Medlemsstaterna ska utse en eller flera tillsynsmyndigheter, så kallade nationella myndigheter för cybersäkerhetscertifiering. Myndigheten eller myndigheterna kommer bl.a. att få i uppdrag att övervaka och kontrollera organ för bedömning av överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat och utfärdare av en EU-försäkran om överensstämmelse. Ett organ för bedömning av överensstämmelse är ett organ som utför bedömning av överensstämmelse, bl.a. genom kalibrering, provning, certifiering och kontroll.

Förordningens bestämmelser ska inte påverka tillämpningen av särskilda bestämmelser om frivillig eller obligatorisk certifiering i andra unionsrättsakter. Förordningen ska heller inte påverka medlemsstaternas befogenheter i fråga om verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på straffrättens område. Den delen av förordningen som rör cybersäkerhetscertifiering kommer att kräva anpassningar och kompletterande författningsbestämmelser på nationell nivå.

## Uppdraget att genomföra EU:s cybersäkerhetsakt

### Allmänna riktlinjer för uppdraget

Cybersäkerhetsakten kommer att reglera den cybersäkerhetscertifiering som följer av en europeisk certifieringsordning för cybersäkerhetscertifiering som fastställts av kommissionen. I dag bestämmer en producent själv om en produkt, tjänst eller process ska certifieras och i så fall vilket certifieringsorgan som ska utföra certifieringen. Utgångspunkten kommer att vara att certifieringen även i framtiden ska vara frivillig, oavsett om en europeisk ordning för cybersäkerhetscertifiering finns på plats eller inte. Detta är dock upp till varje medlemsstat att bestämma. Den största skillnaden är att när en sådan europeisk ordning för cybersäkerhetscertifiering finns på plats, får inte längre nationella cybersäkerhetscertifieringar utföras inom det område som täcks av den europeiska ordningen för cybersäkerhetscertifiering. Förordningen inne-

bär också att när en europeisk ordning för cybersäkerhetscertifiering ska användas reglerar förordningen vilka krav som ställs på certifieringen, certifieringsorganen och de leverantörer och producenter som innehar ett sådant certifikat. Det finns därför ett behov av att ta fram en nationell reglering som kompletterar förordningen.

Utredaren ska därför

- lämna förslag till författningsbestämmelser som kompletterar cybersäkerhetsakten.

### Vilken myndighet ska vara nationell myndighet för cybersäkerhetscertifiering?

Cybersäkerhetsakten föreskriver att varje medlemsstat ska utse en eller flera nationella myndigheter för cybersäkerhetscertifiering på sitt territorium som ansvariga för tillsynsuppgifterna. Alternativt kan medlemsstaten, efter överenskommelse med en annan medlemsstat, utse en eller flera nationella myndigheter för cybersäkerhetscertifiering som är etablerade i denna andra medlemsstat (artikel 58).

Flertalet av cybersäkerhetsaktens bestämmelser om nationella myndigheter för cybersäkerhetscertifiering gäller direkt och medför inga krav på eller behov av kompletterande nationella bestämmelser. Medlemsstaterna ska dock underrätta kommissionen om vilka myndigheter som utsetts och, om fler än en myndighet utsetts, vilka uppgifter de olika myndigheterna ska ha. Myndigheterna kommer bl.a. även att ha en roll när det gäller utfärdandet av europeiska cybersäkerhetscertifikat (på nivån ”hög”), och då måste medlemsstaterna säkerställa att denna verksamhet är avskild från uppgifterna som myndigheten ska utföra som tillsynsmyndighet och att den utförs av oberoende enheter.

Vissa andra frågor är i och för sig reglerade i förordningen men tillåter ytterligare nationell reglering. Detta gäller exempelvis regleringen om tillsynsmyndighetens befogenheter i artikel 58.8. Det är vidare upp till medlemsstaterna att inom vissa angivna ramar reglera bl.a. tillsynsmyndighetens organisation och se till att myndigheten har tillräckliga resurser.

Vid tillsynsmyndigheten kommer det att samlas känslig information om cybersäkerheten i vissa produkter, tjänster och processer eftersom myndig-

heten kommer att ha ett särskilt ansvar för utfärdande av certifikat enligt den högsta assuransnivån. Det är därför viktigt att myndigheten har personal med erfarenhet av och förmåga att bedöma och hantera uppgifter enligt de krav som ställs i offentlighets- och sekretesslagen (2009:400) och säkerhetsskyddslagen (2018:585). Sveriges certifieringsorgan för IT-säkerhet som är lokaliserat vid Försvarets materielverk, CSEC, ska enligt sin instruktion i sin verksamhet beakta nationella säkerhetsintressen. Ett sådant krav bör därför införas även i den reglering som föreslås av utredaren.

Styrelsen för ackreditering och teknisk kontroll (Swedac) har i dag vissa av de uppgifter som den nationella myndigheten för cybersäkerhetscertifiering ska ha. Enligt sin instruktion ska Swedac bl.a. ansvara för frågor om teknisk kontroll, vilket inkluderar ackreditering och frågor i övrigt om bedömning av överensstämmelse. Swedac ska särskilt ansvara för ordningar för bedömning av överensstämmelse/teknisk provning och kontroll. Detta inbegriper att i EU, internationellt och nationellt verka för öppna och harmoniserade tekniska kontrollordningar, ackrediteringssystem och normer för ömsesidigt godtagande av resultat från provningar, certifieringar och andra bevis om överensstämmelse som undanröjer tekniska handelshinder samt upprätthålla och vidareutveckla öppna, kostnadseffektiva och behovsanpassade ordningar för teknisk kontroll och bedömning av överensstämmelse. Swedac är även nationellt ackrediteringsorgan i enlighet med Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 och anmäler och utövar tillsyn över organ som enligt lagen (2011:791) om ackreditering och teknisk kontroll ska anmälas för uppgifter i samband med bedömning av överensstämmelse enligt bestämmelser som gäller inom EU.

För att undvika att den nationella myndigheten för cybersäkerhetscertifiering tilldelas uppgifter som redan utförs av Swedac bör utredaren kartlägga hur förhållandet mellan den nationella myndigheten för cybersäkerhetscertifiering och Swedac ska se ut, i vilka fall de två myndigheterna ska samarbeta och vilket behov av kompletterande nationella bestämmelser som behövs. Det är viktigt att utredaren i detta arbete beaktar de kostnader, den tid och andra aspekter som en dubbel granskning av såväl Swedac som den nationella tillsynsmyndigheten kommer att innebära för den som blir granskad.

Utredaren ska därför

- föreslå vilken befintlig myndighet som ska få i uppdrag att vara nationell tillsynsmyndighet för cybersäkerhetscertifiering,
- ta ställning till hur myndighetens organisation påverkas,
- kartlägga vilket förhållande den nationella myndigheten för cybersäkerhetscertifiering ska ha till Swedac och hur uppgifterna ska fördelas dem emellan för att undvika såväl överlappande granskningar som luckor i tillsynen, samt
- utarbeta nödvändiga kompletterande författningsförslag, inklusive om de befogenheter som den nationella myndigheten för cybersäkerhetscertifiering ska tilldelas, i syfte att myndigheten ska kunna utföra de uppgifter som följer av förordningen.

### Ska det införas kompletterande bestämmelser om sanktioner?

Cybersäkerhetsakten innehåller i artikel 65 bestämmelser om att medlemsstaterna ska fastställa regler om sanktioner vid överträdelser av den delen av förordningen som reglerar ett ramverk för cybersäkerhetscertifiering och för överträdelser av europeiska ordningar för cybersäkerhetscertifiering. Medlemsstaterna ska också vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. I artikel 58.8 finns en lista över de befogenheter som de nationella myndigheterna för cybersäkerhetscertifiering måste ha. I punkt f anges att myndigheterna ska utdöma sanktioner i enlighet med nationell rätt och kräva att överträdelser av skyldigheterna i förordningen omedelbart upphör. Medlemsstaterna ska vidare enligt artikel 65 anmäla dessa regler och åtgärder samt eventuella ändringar som berör dem till kommissionen utan dröjsmål. I förordningen saknas dock närmare bestämmelser om hur detta ska gå till och vilka som ska kunna drabbas av sanktioner. Till detta kommer också att det föreslagna systemet är frivilligt. Om sanktionerna för att bryta mot ett system som inte är obligatoriskt är för långtgående finns det risk för att aktörer inte kommer att använda sig av den europeiska cybersäkerhetscertifieringen eller att de vänder sig till länder med mildare sanktionssystem. Samtidigt får det europeiska systemet inte bli tandlöst för dem som trots allt väljer att använda sig av det. Det finns därför behov av att analysera och ta ställning till i vilken utsträckning överträdelser av förordningen bör bli föremål för sanktioner i Sverige.

Utredaren ska därför

- analysera vilka kompletterande bestämmelser om sanktioner som Sverige behöver eller bör införa,
- lämna sådana författningsförslag som behövs och är lämpliga.

### Processuella frågor och rätten att klaga

Av artikel 58.8 i förordningen framgår det att utövandet av tillsynsmyndighetens befogenheter ska vara föremål för lämpliga skyddsåtgärder, bl.a. effektiva rättsmedel. Enligt artikel 58.8 d ska tillsynsmyndigheten ha befogenhet att få tillgång till lokaler hos organ för bedömning av överensstämmelse eller hos innehavare av ett europeiskt cybersäkerhetscertifikat i enlighet med unionsrätten eller nationell processrätt. Fysiska och juridiska personer ska, enligt förordningen, ha rätt att lämna in klagomål till utfärdaren av ett europeiskt cybersäkerhetscertifikat eller, när klagomålet rör ett europeiskt cybersäkerhetscertifikat som utfärdats av ett organ för bedömning av överensstämmelse, till den behöriga nationella myndigheten för cybersäkerhetscertifiering (artikel 63.1). Vidare ska fysiska och juridiska personer ha rätt till ett effektivt rättsmedel mot den myndighet eller de organ som nämnts ovan och som fattat ett beslut, och när det gäller underlåtenhet att vidta åtgärder med anledning av ett klagomål som lämnats in till myndigheten eller organet (artikel 64.1). Detta torde för svensk del bäst tillgodoses genom en rätt för enskilda att överklaga tillsynsmyndighetens beslut till allmän förvaltningsdomstol.

Behovet av kompletterande nationella bestämmelser i de ovanstående frågorna behöver bli föremål för närmare analys.

Utredaren ska därför

- analysera i vilken utsträckning det behövs kompletterande bestämmelser om utövandet av tillsynsmyndighetens befogenheter,
- ta ställning till i vilken utsträckning det behövs kompletterande bestämmelser om de rättsmedel för enskilda som regleras i förordningen, och
- lämna sådana författningsförslag som behövs och är lämpliga.

### Hur ska förordningens bestämmelser om organ för bedömning av överensstämmelse och självbedömning av överensstämmelse genomföras?

Förordningen reglerar även organ för bedömning av överensstämmelse, som bl.a. kan utfärda europeiska cybersäkerhetscertifikat. I bilagan till förordningen finns närmare bestämmelser med krav på dessa organ, bl.a. om upp-

rätthållande av konfidentialitet och tystnadsplikt. Organen för bedömning av överensstämmelse ska ackrediteras av det nationella ackrediteringsorganet – i Sveriges fall är det Swedac. I fall där ett europeiskt cybersäkerhetscertifikat utfärdas av en nationell myndighet för cybersäkerhetscertifiering ska certifieringsorganet hos den nationella myndigheten för cybersäkerhetscertifiering ackrediteras som organ för bedömning av överensstämmelse.

En europeisk ordning för cybersäkerhetscertifiering kan också ge tillverkare eller leverantörer möjlighet att göra en självbedömning av överensstämmelse. Detta tillåts endast i förhållande till produkter, tjänster och processer där de uppfyllda säkerhetskraven är ställda på en lägre nivå. I förordningen finns bestämmelser om hur detta ska gå till (artikel 53). Där anges också att detta är frivilligt att utfärda, om inte annat anges i unionsrätten eller i medlemsstaternas nationella rätt.

Utredaren ska därför

- föreslå hur bestämmelserna om kraven på organen för överensstämmelse ska genomföras,
- analysera om nuvarande sekretessbestämmelser för offentliga organ och bestämmelser om tystnadsplikt för privata aktörer behöver anpassas eller ny lagstiftning föreslås, med anledning av förordningens reglering om tystnadsplikt och konfidentialitet hos organen för överensstämmelse, och
- lämna sådana författningsförslag som behövs och är lämpliga.

### Frivillighet

Cybersäkerhetscertifieringen ska enligt förordningen vara frivillig, om inte annat anges i unionsrätten eller i medlemsstaternas nationella rätt (artikel 56.2). Förordningen ger dock kommissionen i uppdrag att regelbundet bedöma effektiviteten hos och användningen av de antagna europeiska ordningarna för cybersäkerhetscertifiering och huruvida en specifik europeisk ordning för cybersäkerhetscertifiering ska göras obligatorisk genom unionsrätten i syfte att säkerställa en adekvat cybersäkerhetsnivå och förbättra den inre marknadens funktion. Den första bedömningen ska göras senast den 31 december 2023, och efterföljande bedömningar ska göras minst en gång vartannat år. Kommissionen ska sedan på grundval av bedömningen fastställa om produkter, tjänster eller processer ska omfattas av en obligatorisk certifieringsordning.

Som tidigare nämnts upphör de nationella ordningarna för cybersäkerhetscertifiering och tillhörande förfaranden att gälla så fort det finns europeiska motsvarigheter. Befintliga certifikat kommer dock att förbli giltiga till dess att de löper ut. Medlemsstaterna förbinder sig också att inte införa nya nationella ordningar, som omfattas av en befintlig europeisk ordning för cybersäkerhetscertifiering, och ska meddela kommissionen och ECCG om alla avsikter att utarbeta nya nationella ordningar för cybersäkerhetscertifiering. Detta regleras i förordningen och kommer att påverka såväl innehavare av befintliga certifikat som de certifieringsorgan som i dag utfärdar certifikat enligt andra ordningar. Verksamheter måste anpassas till det nya systemet, och branschen måste hålla sig uppdaterad om de förslag till europeiska ordningar för cybersäkerhetscertifiering som utarbetas.

Utredaren ska därför

- hålla sig uppdaterad om hur arbetet med att utarbeta europeiska ordningar för cybersäkerhetscertifiering fortgår, och
- lämna sådana författningsförslag som behövs och är lämpliga.

### Certifiering på den högsta assuransnivån

I Sverige finns i dag vid Försvarets materielverk ett nationellt certifieringsorgan för it-säkerhet i produkter och system, CSEC. CSEC ska i sin verksamhet beakta nationella säkerhetsintressen och verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat. Dessutom är CSEC Sveriges signatär och representant inom den internationella överenskommelsen för ömsesidigt erkännande av certifikat, Common Criteria Recognition Arrangement (CCRA), och motsvarande överenskommelse inom Europa, Senior Officials Group Information Systems Security – Mutual Recognition Arrangement (SOG-IS MRA), (5 § förordningen [2007:854] med instruktion för Försvarets materielverk). Detta innebär att CSEC representerar och tar tillvara landets intressen inom organisationerna. Som nationellt certifieringsorgan ansvarar CSEC för att ta fram och utveckla regler för granskning av it-säkerhet i produkter och system enligt Common Criteria, CC. CSEC licensierar företag som utför granskningar enligt dessa regler samt utövar tillsyn över dessa företag. Produkter som certifierats av CSEC används bl.a. av Försvarsmakten. CC erkänns internationellt av världens ledande länder inom it-säkerhet och anses obligatoriskt för it-produkter i kritiska infrastrukturer i flera länder. CSEC har även som uppdrag att samverka internationellt med andra certifieringsorgan och säkerhetsmyndigheter.

CCRA och SOG-IS MRA tillåter endast statliga certifieringsorgan, vilket medför att det i dag bara är CSEC som utfärdar certifikat enligt den standarden i Sverige. Med cybersäkerhetsakten tillåts privata certifieringsorgan endast att utfärda certifikat på nivån ”grundläggande” eller ”betydande”. För nivån ”hög” är det den nationella myndigheten för cybersäkerhetscertifiering som är behörig. Myndigheten kan dock delegera detta till ett organ för bedömning av överensstämmelse genom en allmän delegering på förhand av uppgiften eller efter förhandsgodkännande av varje enskilt europeiskt cybersäkerhetscertifikat.

Utredaren ska därför

- föreslå hur certifiering på assuransnivån ”hög” ska genomföras i Sverige och utreda om detta kan och bör regleras genom författning. Utredaren ska ha som utgångspunkt att CSEC ska ha en roll då det gäller denna typ av certifiering.

### Uppdraget att överväga om det bör införas krav på certifiering och godkännande till skydd för Sveriges säkerhet

Särskilda krav på säkerhet måste kunna ställas på nät- och informationssäkerhet för att skydda nationell säkerhet. Åtgärder för att skydda nationell säkerhet faller utanför EU:s kompetens (art. 4.2 EU-fördraget). Av artikel 1.2 cybersäkerhetsakten framgår även att förordningen inte ska påverka medlemsstaternas befogenheter i fråga om nät- och informationssäkerhet, särskilt inte verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på strafflagstiftningens område.

Säkerhetsskyddslagen gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet). För informationssystem som används i eller har betydelse för säkerhetskänslig verksamhet finns särskilda krav i säkerhetsskyddsförordningen (2018:658). Det rör sig dels om förberedande åtgärder inför driftsättning av sådana informationssystem, dels om säkerhetskrav som kontinuerligt ställs på informationssystemen. Bestämmelserna innehåller även krav på samråd med Säkerhetspolisen eller Försvarsmakten i vissa fall. Detta gäller för informationssystem som kan komma att behandla säkerhetsskyddsklassificerade uppgifter av visst slag och informationssystem där obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är

obetydlig. Bestämmelserna innebär att det är verksamhetsutövaren som ansvarar för att se till att informationssystemen upprätthåller kraven på informationssäkerhet.

Det finns anledning att överväga om ytterligare 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. En möjlighet kan vara att införa krav på att produkter, tjänster och processer inom nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet ska vara certifierade enligt särskilda certifieringsordningar som ställer krav anpassade för användning i säkerhetskänslig verksamhet. En kompletterande eller alternativ möjlighet är att införa krav på godkännande från en utpekad myndighet innan en sådan produkt, tjänst eller process tas i drift i säkerhetskänslig verksamhet.

Utredaren ska därför:

- bedöma om det finns anledning att införa särskilda krav på att produkter, tjänster och processer som ingår i ett nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet, ska vara certifierade enligt särskilda certifieringsordningar utformade för säkerhetskänslig verksamhet,
- överväga om det finns anledning att införa krav på godkännande från en myndighet för att sådana produkter, tjänster och processer ska få tas i drift i viss eller all säkerhetskänslig verksamhet,
- göra en internationell jämförelse av lagstiftning som innebär särskilda krav med anledning av nationell säkerhet för produkter, tjänster och processer som ingår i ett nätverks- eller informationssystem i länder som utredaren bedömer vara av intresse,
- lämna förslag, förenliga med EU-rätten, på hur ett sådant regelverk skulle kunna se ut, inklusive vilken eller vilka myndigheter som skulle ansvara för uppgiften och vilka sanktioner en sådan reglering bör förenas med,
- lämna nödvändiga författningsförslag som behövs och är lämpliga.

Utredningen har i denna del att förhålla sig till betänkandet Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82) som för närvarande bereds i Regeringskansliet.

### Övriga frågor

Utredaren är fri att inom de ramar som anges i de allmänna riktlinjerna ta upp och belysa även andra frågeställningar som är relevanta för uppdraget.

Om utredaren kommer fram till att det krävs eller är lämpligt med kompletterande nationella bestämmelser i andra delar ska sådana kunna föreslås.

### Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för enskilda. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. Utredaren ska särskilt ange konsekvenserna för företag i form av kostnader och ökade administrativa bördor samt personella konsekvenser för berörda myndigheter.

Utredaren ska även beakta de konsekvenser som förordningens genomförande kan få när det gäller internationell handel med tredjeland och erkännande och utfärdande av certifikat och andra åtaganden som följer av Sveriges medlemskap i bl.a. CCRA.

### Kontakter och redovisning av uppdraget

Utredaren ska hålla Regeringskansliet (Försvarsdepartementet) informerat om det löpande arbetet.

Vid genomförandet av uppdraget ska utredaren hålla sig informerad om och beakta relevant arbete som bedrivs inom Regeringskansliet (exempelvis arbetet med betänkandet Kompletteringar till den nya säkerhetsskyddslagen, SOU 2018:82), utredningsväsendet och inom EU. Under genomförandet av uppdraget ska utredaren, i den utsträckning som bedöms lämplig, också ha en dialog med och inhämta upplysningar från myndigheter, näringslivet och andra som kan vara berörda av de aktuella frågorna.

Uppdraget ska redovisas i den del som avser anpassningar med anledning av EU-förordningen senast den 1 juni 2020. I den del som avser regler till skydd för Sveriges säkerhet ska uppdraget redovisas senast den 1 mars 2021.

(Försvarsdepartementet)