Regeringen

Bilaga 1 till III:6 vid regeringssammanträde den 28 november 2024.

Dir. 2024:119

Kommittédirektiv

Kompletterande bestämmelser till EU:s cyberresiliensförordning

Beslut vid regeringssammanträde den 28 november 2024.

Sammanfattning

En särskild utredare ska analysera behovet av och föreslå åtgärder och kompletterande författningsbestämmelser som behövs i syfte att anpassa svensk rätt till EU:s cyberresiliensförordning.

Utredaren ska bl.a.

- analysera om befintliga bestämmelser i nationell rätt behöver upphävas eller ändras eller om nya bestämmelser behövs med anledning av förordningen,
- föreslå vilken befintlig myndighet eller vilka befintliga myndigheter som ska utses till nationell marknadskontrollmyndighet,
- föreslå vilken befintlig myndighet som ska utses till anmälande myndighet med ansvar för att bl.a. inrätta och genomföra de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse, och
- lämna de förslag, inklusive författningsförslag, i övrigt som är nödvändiga eller annars bedöms lämpliga för att komplettera förordningen.

Uppdraget ska redovisas senast den 15 december 2025.

EU-förordningen

Europaparlamentet och rådet har antagit förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen), i fortsättningen benämnd EU:s cyberresiliensförordning. Förordningen träder i kraft den 10 december 2024 och ska tillämpas fr.o.m. 11 december 2027. Artikel 14 ska dock tillämpas fr.o.m. den 11 september 2026 och kapitel IV (artiklarna 35–51) ska tillämpas fr.o.m. den 11 juni 2026.

Syftet med förordningen är att skapa förutsättningar för utveckling av säkra produkter med digitala element genom att säkerställa att hård- och mjukvara släpps ut på marknaden med färre sårbarheter och att tillverkare ska ta större ansvar för produkters cybersäkerhet genom deras livscykel. Förordningen syftar vidare till att konsumenter ska få tillräcklig information om cybersäkerheten för de produkter med digitala element som de köper och använder. Ekonomiska operatörer, vilka i huvudsak är tillverkare, importörer och distributörer, ska följa de cybersäkerhetskrav förordningen anger för alla produkter med digitala element, för att de ska kunna tillhandahållas på den inre marknaden.

Kraven innebär att tillverkare ska ta cybersäkerhet i beaktande i designen och utvecklingen av produkter med digitala element. Därtill ska tillverkare granska säkerhetsaspekter under utvecklingsprocessen, ha transparens gentemot konsumenter gällande cybersäkerhetsaspekter samt försäkra säkerhetssupport och uppdateringar på ett proportionerligt sätt under produktens livscykel. Regelefterlevnad uppvisas genom en konformitetsbedömning och i vissa fall certifiering.

Uppdraget att identifiera berörda svenska regelverk

Det finns ett behov av att identifiera vilka bestämmelser i svenska författningar som berörs av EU:s cyberresiliensförordning samt att analysera om de behöver upphävas eller ändras eller om nya bestämmelser behövs med anledning av förordningen.

Produktsäkerhetslagen (2004:451) syftar till att säkerställa att produkter som tillhandahålls på marknaden är säkra för konsumenter. EU:s cyberresiliensförordning ställer krav på säkerhet i digitala produkter, vilket kan medföra ett behov av att ändra produktsäkerhetslagen för att inkludera krav i fråga om

cybersäkerhet och sårbarhet i digitala produkter. Även Europaparlamentets och rådets förordning (EU) 2023/988 av den 10 maj 2023 om allmän produktsäkerhet, ändring av Europaparlamentets och rådets förordning (EU) nr 1025/2012 och Europaparlamentets och rådets direktiv (EU) 2020/1828 och om upphävande av Europaparlamentets och rådets direktiv 2001/95/EG och rådets direktiv 87/357/EEG, i fortsättningen benämnd EU-förordningen om allmän produktsäkerhet, som börjar tillämpas den 13 december 2024, kan behöva beaktas vid denna bedömning.

Lagen (2022:482) om elektronisk kommunikation innehåller bl.a. bestämmelser om säkerhet och integritet inom sektorn för elektronisk kommunikation. Bestämmelserna kan bl.a. ställa krav på säkerheten i nätverksutrustning och programvara som motsvarar kraven i bilaga III i EU:s cyberresiliensförordning. Förordningens bestämmelser kan därför medföra ett behov av ändringar i denna lag för att inkludera nya krav på cybersäkerhet och hantering av sårbarheter i den tekniska infrastrukturen.

I konsumentköplagen (2022:260) och konsumenttjänstlagen (1985:716) regleras konsumenters rättigheter vid köp av varor och tjänster. EU:s cyberresiliensförordning kan medföra att säkerhetsrelaterade garantier och rättigheter för digitala produkter behöver integreras i dessa lagar.

Av artikel 2.7 i EU:s cyberresiliensförordning framgår dock att förordningen inte tillämpas på produkter med digitala element som utvecklats eller ändrats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål eller på produkter som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter.

Utredaren ska därför

- identifiera vilka bestämmelser i svensk rätt som omfattas av tillämpningsområdet för EU:s cyberresiliensförordning,
- analysera om bestämmelserna behöver upphävas eller ändras eller om nya bestämmelser behövs med anledning av förordningen,
- ta ställning till behovet av undantag från befintliga eller föreslagna bestämmelser med hänsyn till nationell säkerhet eller skydd av andra väsentliga statliga funktioner,
- kartlägga potentiellt överlappande krav som följer av andra EU-rättsakter, bl.a. Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäker-

hetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet), 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) och Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), och

- lämna nödvändiga författningsförslag.

Uppdraget att föreslå sanktionsbestämmelser

Medlemsstaterna ska enligt EU:s cyberresiliensförordning fastställa regler om sanktioner för överträdelser av förordningen. Detta avser bristande efterlevnad av de cybersäkerhetskrav som anges i bilaga I i förordningen. Sanktionerna ska vara effektiva, proportionella och avskräckande.

Utredaren ska därför

- analysera vilka sanktioner som behövs för att uppfylla kravet på sanktioner vid överträdelse av förordningen, och
- lämna nödvändiga författningsförslag.

Uppdraget att utse nationell marknadskontrollmyndighet och anmälande myndighet

EU:s cyberresiliensförordning ställer krav på att medlemsstaterna ska utse en eller flera nationella marknadskontrollmyndigheter för att säkerställa ett effektivt genomförande av förordningen. Medlemsstaterna får utse en befintlig eller en ny myndighet till att vara marknadskontrollmyndighet enligt förordningen. Flera myndigheter arbetar med marknads- och produktkontroll utifrån olika regelverk, exempelvis Post- och telestyrelsen, Statens energimyndighet och Elsäkerhetsverket.

Medlemsstaterna ska vidare utse en anmälande myndighet med ansvar för att inrätta och genomföra de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och för övervakning av dessa.

Utredaren ska därför

- föreslå vilken befintlig myndighet eller vilka befintliga myndigheter som ska utses till nationell marknadskontrollmyndighet för Sveriges räkning,
- föreslå vilken befintlig myndighet som ska utses till anmälande myndighet med ansvar för att bl.a. inrätta och genomföra de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse,
- analysera om det finns möjligheter att samordna marknadskontrollen med andra regelverk, och
- föreslå de författningsändringar och andra åtgärder som krävs för att föreslagna myndigheter ska kunna vidta de åtgärder som följer av förordningen.

Uppdraget att lämna förslag om stöd för regelefterlevnad till mikroföretag, små företag och medelstora företag

Mikroföretag, små företag och medelstora företag har ofta särskilda utmaningar gällande regelefterlevnad av förordningar när det gäller resurser och kunskap. EU:s cyberresiliensförordning ställer krav på medlemsstaterna att, när så är lämpligt, vidta vissa stödåtgärder för mikroföretag, små företag och medelstora företag. För att undvika att förordningen ska hämma näringslivet och innovation ska utredningen överväga vilka stödåtgärder och stödfunktioner som skulle kunna vara lämpliga för att bistå dessa företag.

Utredaren ska därför

- föreslå hur de åtgärder som avses i artikel 33 i EU:s cyberresiliens-förordning kan genomföras i Sverige,
- föreslå lämpliga samarbetsformer eller forum där expertis och kunskap kan delas mellan såväl företag som offentlig-privata initiativ, och
- föreslå andra lämpliga stödåtgärder för mikroföretag, små företag och medelstora företag.

Uppdraget att lämna anslutande förslag

Om det som en följd av utredarens förslag i övrigt bedöms nödvändigt, får utredaren ta upp och lämna förslag i närliggande frågor.

Allmänna utgångspunkter för uppdragets genomförande

Utredaren ska vid utformningen av sina förslag noga beakta skyddet för grundläggande fri- och rättigheter, däribland yttrande- och informationsfriheten samt äganderätten, behovet av att upprätthålla ett högt skydd för den nationella säkerheten och för produkter som har utvecklats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål. Utredarens förslag ska även utformas utifrån kostnadseffektivitet och så att företagens och myndigheternas totala regelbörda och kostnader inte ökar mer än nödvändigt. Utredaren ska ta medborgarnytta, effektivitet och konkurrenskraft i beaktning.

Konsekvensbeskrivningar

Utredaren ska i enlighet med kommittéförordningen (1998:1474) och förordningen (2024:183) om konsekvensutredningar bedöma och beskriva förslagens ekonomiska och samhällsekonomiska konsekvenser, samt konsekvenser i övrigt för enskilda, företag och det allmänna. Utredaren ska bl.a. beskriva och beräkna eventuella offentligfinansiella konsekvenser, däribland eventuella konsekvenser för berörda myndigheter. Utredaren ska beräkna hur statens inkomster och utgifter påverkas. Om förslag som lämnas medför offentligfinansiella kostnader, ska förslag till finansiering lämnas. Utredaren ska även redovisa förslagens konsekvenser ur ett jämställdhetsperspektiv och för den personliga integriteten.

Processerna för att ta fram standarder kan komma att innebära ett omfattande åtagande både i fråga om resurser och personal för bl.a. deltagande i arbetskommittéer. Utredaren ska bedöma vilka konsekvenser standardiseringsarbetet som följer av förslagen kan antas medföra för berörda myndigheter, företag och andra nationella organisationer.

Mikroföretag, små företag och medelstora företag är särskilt sårbara för risken att omfattande regelverk hämmar affärsverksamheten. Utredaren ska därför särskilt redogöra för vilka ekonomiska konsekvenser de förslag som lämnas kan få för mikroföretag, små företag och medelstora företag.

Kontakter och redovisning av uppdraget

Utredaren ska ha en dialog med och inhämta upplysningar från Post- och telestyrelsen, Försvarets materielverk, Myndigheten för samhällsskydd och beredskap, Statens energimyndighet, Elsäkerhetsverket och Styrelsen för ackreditering och teknisk kontroll (Swedac). Utredaren ska även, i den

utsträckning som bedöms lämplig, ha en dialog med och inhämta upplysningar från övriga berörda myndigheter, näringslivet, Implementeringsrådet och organisationer som berörs av uppdraget.

Utredaren ska hålla sig informerad om och beakta annat relevant arbete som bedrivs inom Regeringskansliet, exempelvis uppdraget åt en sakkunnig att analysera behovet av kompletterande bestämmelser till EU-förordningen om allmän produktsäkerhet, och i internationella forum med anledning av genomförandet av EU:s cyberresiliensförordning. Detta inkluderar t.ex. Europeiska unionens cybersäkerhetsbyrå (Enisa) och högnivåforumet för europeisk standardisering. Utredaren bör, om det bedöms lämpligt och främjar uppdraget, också undersöka hur andra medlemsstater planerar att genomföra förordningen.

Uppdraget ska redovisas senast den 15 december 2025.

(Finansdepartementet)