Regelrådet

Yttrande
2024-05-02

Vårt diarienummer
RR 2024-57

Ert diarienummer
Fö2024/00496

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 Nya regler om cybersäkerhet (SOU 2024:18)

Regelrådets ställningstagande

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

Innehållet i förslaget

Förslaget rör införlivning av NIS2-direktivet[1] i svenska lag. NIS2-direktivet ställer krav på säkerhet i nätverks- och informationssystem och ersätter det tidigare NIS-direktivet.

Utredningen föreslår en ny lag om cybersäkerhet samt en ny förordning om cybersäkerhet. Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster upphör därmed att gälla. Förslaget innebär också ändringar i följande lagar och förordningar:

- lagen (2006:24) om nationella toppdomäner för Sverige på internet
- lagen (2022:482) om elektronisk kommunikation
- förordningen (2007:951) med instruktion för Post- och telestyrelsen
- offentlighets- och sekretessförordningen (2009:641)
- förordningen (2022:511) om elektronisk kommunikation.

Förslagen föreslås träda i kraft den 1 januari 2025.

Skälen för Regelrådets ställningstagande

Bakgrund och syfte med förslaget

Europaparlamentet och rådet antog den 14 december 2022 två nya EU-direktiv, NIS2-direktivet och CER-direktivet[2]. Det nu aktuella förslaget rör införlivning av NIS2-direktivet. Utredningen kommer i sitt slutbetänkande i september 2024 att lämna förslag om införlivning

[1] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148.
[2] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

av CER-direktivet. NIS2-direktivet ställer krav på säkerhet i nätverks- och informationssystem. Det ersätter det tidigare NIS-direktivet från 2016, som genomfördes i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Utredningen föreslår att NIS2-direktivet i huvudsak införlivas genom en ny lag, cybersäkerhetslagen och att den tidigare lagen upphävs. Det har visat sig att det finns stora skillnader mellan olika medlemsstater när det gäller vilka krav som ställs på verksamhetsutövare. Krav som ställs av en medlemsstat och som skiljer sig från, eller till och med står i strid med, krav som ställs av en annan medlemsstat kan väsentligt påverka sådan gränsöverskridande verksamhet. Det är dessutom sannolikt att otillräckligt utformade eller genomförda cybersäkerhetskrav i en medlemsstat kommer att påverka cybersäkerhetsnivån i andra medlemsstater. Översynen av NIS-direktivet har också visat på stora skillnader i medlemsstaternas genomförande när det gäller dess tillämpningsområde. NIS2-direktivet skärper kraven jämfört med det tidigare direktivet för verksamhetsutövare och innehåller bestämmelser om ett mer långtgående samarbete inom unionen. Direktivets mål är att undanröja de stora skillnader som finna mellan medlemsstaterna, särskilt genom att föreskriva minimiregler för ett fungerande samordnat regelverk, genom att fastställa mekanismer för effektivt samarbete mellan de ansvariga myndigheterna i varje medlemsstat, genom att uppdatera vilka sektorer och verksamheter som omfattas av skyldigheter och genom att föreskriva effektiva rättsmedel och efterlevnadskontrollåtgärder.

Regelrådet gör följande bedömning. Det framgår vilket syftet med förslaget är och mot vilken bakgrund det lämnas. Beskrivningen är tillräckligt tydlig.

Regelrådet finner att redovisningen av bakgrund och syfte med förslaget är godtagbar.

Alternativa lösningar och effekter av om ingen reglering kommer till stånd

Förslaget följer av ett EU-direktiv, vilket innebär att Sverige är skyldiga att införliva bestämmelserna i svensk rätt. Direktivet ger dock medlemsstaterna ett visst utrymme för anpassning till den nationella rätten. I det här fallet innebär det att utredningen skulle kunna lämna förslag om att exempelvis fler sektorer än vad som följer av direktivet skulle kunna omfattas av en reglering. Förslagsställaren uppger dock att utredningens tidsram omöjliggör att tillämpningsområdet utökas och att utredningen i stället bör fokusera på analyser och förslag med syfte att införliva direktivet. Utredningens uppdrag är också att införliva direktivet, inte att utarbeta ett nytt system från grunden. Skälet är att om avvägningen som kommissionen och EU:s lagstiftare förhandlat fram i åsidosätts, behöver konsekvenserna för tillkommande områden övervägas ingående eftersom det arbetet inte utförts tidigare.

Förslagsställaren uppger vidare att utredningen övervägt alternativet att finansiera förslaget med avgifter, men att man slutligen landat i att anslagsfinansiering är mer lämpligt. Frågan utreddes redan i samband med utredningen om genomförande av NIS-direktivet och utredningen bedömde då att det var svårt att bestämma avgifterna eftersom såväl antalet leverantörer som skulle omfattas och komplexiteten i verksamheten var oklar. Detta gäller i ännu högre grad för NIS2-direktivet. Det är delvis oklart vilka enskilda verksamhetsutövare som kommer att omfattas. I samband med NIS-utredningen menade Statskontoret att det huvudsakliga skälet mot avgiftsfinansiering var risken för konkurrenssnedvridande effekter och höga administrationskostnader. Därutöver fanns det svårigheter att utforma tillsynen över sektorerna på ett enhetligt sätt och en svårighet att påvisa en tydlig motprestation för

avgiften.[3] Förslagsställaren uppger att den här utredningen sammantaget ansluter sig till dessa tidigare bedömningar och menar att argumenten är aktuella även för NIS2-tillsynen. Effekten av att inte reglera skulle vara att Sverige inte följer skyldigheterna enligt EU-rätten.

Regelrådet gör följande bedömning. Förslagsställaren redogör för de möjligheter som finns att föreslå alternativa lösningar och motiverar varför utredningen inte haft möjlighet att utreda detta närmare. Enligt Regelrådets mening hade konsekvensutredningens kvalitet förbättrats om förslagsställaren resonerat mer kring möjliga alternativ till den föreslagna regleringen. Det finns dock ett resonemang kring alternativa sätt att finansiera förslaget, vilket Regelrådet uppskattar.

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

Förslagets överensstämmelse med EU-rätten

Sveriges medlemskap i EU innebär en skyldighet att, inom en bestämd tid, införliva bestämmelser i direktiven med bindande regler i den svenska rättsordningen. Förslagsställaren uppger att NIS2-direktivet är ett minimidirektiv med innebörd att den svenska lagstiftningen skulle kunna innehålla längre gående skyldigheter. Förslagen innehåller med undantag av skyldigheten om systematiskt informationssäkerhetsarbete inga krav som syftar till att uppnå en högre nivå av säkerhet än de som följer av direktivet. Det betyder att den föreslagna regleringen i princip uteslutande är en konsekvens av Sveriges medlemskap i EU och går inte utöver dessa skyldigheter.

Regelrådet gör följande bedömning. Förslagsställaren redogör för vilken koppling förslaget har till EU-rätten, vilka bestämmelser som är tillämpliga och på vilket sätt förslaget uppfyller de skyldigheter som Sverige har till följd av EU-lagstiftning. Det finns även en motivering till varför man i vissa fall valt att gå längre än vad direktivet föreskriver. Beskrivningen är tillräckligt tydlig.

Regelrådet finner att redovisningen av förslagets överensstämmelser med EU-rätten är godtagbar.

Särskild hänsyn till tidpunkt för ikraftträdande och behov av speciella informationsinsatser

Utredningen föreslår att förslagen ska träda i kraft den 1 januari 2025. Av artikel 41 följer att medlemsländerna senast den 17 oktober 2024 ska anta och offentliggöra de bestämmelser som är nödvändiga för att följa direktivet. Bestämmelserna ska tillämpas från den 18 oktober 2024. Utredningen föreslår med hänsyn till det och svensk lagstiftningstradition att den lag och förordning som ska innehålla direktivets krav träder i kraft den 1 januari 2025. Genom lagen upphävs också den tidigare NIS-lagen och genom den nya förordningen den tidigare NIS-förordningen.

Det framgår av utredningen att varje verksamhetsutövare även enligt nuvarande reglering själv bär ansvaret för att identifiera att verksamheten omfattas av lagen och har en skyldighet

[3] https://www.statskontoret.se/publicerat/publikationer/publikationer-2018/tillsyn-enligtnis-direktivet--kostnader-och-finansiering/?publication=true#_Toc508707866, inhämtat januari 2024.

att anmäla sig till myndigheten samt lämna uppgifter om verksamheten. Utredningens uppfattning är att detta ska vara fallet även avseende den nu föreslagna regleringen, men att det ska bli lättare för verksamhetsutövare att göra denna bedömning. Det framgår att det ligger på varje tillsynsmyndighet att med stöd av Myndigheten för samhällsskydd och beredskap (MSB) utforma en vägledning om de oklarheter som kan föreligga i sektorsbeskrivningarna till stöd för den enskilde verksamhetsutövaren. I konsekvensutredningen nämns inget om behov av speciella informationsinsatser. Det framgår dock av rapporten från Sweco (bilaga 4 i utredningen) att tillsynsmyndigheterna bedömer att det kommer att finnas ett ökat behov av informationsinsatser, både bland de som redan i dag är tillsynsmyndigheter och de som tillkommer genom den föreslagna regleringen.

Regelrådet gör följande bedömning. Det framgår varför förslagsställaren valt den aktuella tidpunkten för ikraftträdande. Förslagsställaren resonerar kring företagens ansvar att avgöra om de omfattas av regleringen, men konsekvensutredningen innehåller inte någon egentlig information om behov av speciella informationsinsatser. Det går visserligen att utläsa detta av Swecos rapport, men enligt Regelrådets mening borde förslagsställaren ha varit tydlig med detta även i konsekvensutredningen.

Regelrådet finner ändå att redovisningen av särskild hänsyn till tidpunkt för ikraftträdande och behov av speciella informationsinsatser är godtagbar.

Berörda företag utifrån antal, storlek och bransch

Det finns två viktiga skillnader mellan gällande lagstiftning och förslaget till cybersäkerhetsreglering. Den första är att cybersäkerhetslagen föreslås omfatta betydligt fler aktörer, eftersom antalet sektorer utökas från sju till 18. Den andra viktiga skillnaden är att kraven kommer att gälla för hela verksamheten inte bara för samhällsviktiga och digitala tjänster. De sektorer som kommer att omfattas är:

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvårdssektorn
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Förvaltning av IKT-tjänster (mellan företag)
- Offentlig förvaltning
- Rymden
- Post- och budtjänster

- Avfallshantering
- Tillverkning, produktion och distribution av kemikalier
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning
- Digitala leverantörer
- Forskning

Innebörden är att den som bedriver verksamhet inom någon av sektorerna som utgångspunkt omfattas av kraven i cybersäkerhetsregleringen. Det gäller för såväl offentliga som enskilda verksamhetsutövare. Förslagsställaren menar att för de flesta sektorerna är det tydligt vem som omfattas, men för några krävs en analys. Utredningen har därför föreslagit att regeringen ger tillsynsmyndigheterna i uppdrag att med stöd av MSB skyndsamt utarbeta en vägledning. Här finns det alltså fortfarande en oklarhet. Däremot är det klart att förslaget innebär att betydligt fler enskilda verksamhetsutövare kommer att omfattas av krav än vad som gäller enligt gällande NIS-lag. En vidare förutsättning är dock att huvudregeln är att verksamheten sysselsätter minst 50 personer eller har en omsättning som överstiger 10 miljoner euro per år. Innebörden av det är att utredningens förslag som huvudregel inte omfattar små företag. Definitionen för små företag är alltså att verksamheten sysselsätter mindre än 50 personer och har en omsättning som är lägre än 10 miljoner euro. Därutöver gäller dock att storlekskravet inte behöver vara uppfyllt för vissa utpekade verksamhetsutövare. Det vill säga de som erbjuder allmänna elektroniska kommunikationsnät, allmänt tillgängliga elektroniska kommunikationstjänster, betrodda tjänster, registreringsenhet för toppdomäner eller DNS-tjänster. MSB kommer också att ha möjlighet att peka ut vissa särskilt kritiska mindre verksamheter. Enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet, brottsbekämpning eller erbjuder tjänster till myndigheter som gör det, är undantagna.

Regelrådet gör följande bedömning. Det framgår vilka branscher som omfattas av förslaget och även att förslaget som huvudregel inte omfattar små företag. Det är tydligt att fler verksamheter än tidigare kommer att omfattas av bestämmelserna, men det går inte att få en klar bild av hur många företag det rör sig om, vilket är en brist. Förslagsställaren verkar vara medveten om att det finns en hel del oklarheter och att dessa behöver utredas vidare.

Regelrådet finner att redovisningen av berörda företag utifrån antal är bristfällig.

Regelrådet finner att redovisningen av berörda företag utifrån storlek och bransch är godtagbar.

Påverkan på berörda företags kostnader, tidsåtgång och verksamhet

Förslagsställaren uppger att verksamhetsutövarna har vissa skyldigheter. Till att börja med finns det en anmälningsskyldighet om verksamheten till tillsynsmyndigheten (läs mer i kapitel 6). Därutöver ska verksamhetsutövaren vidta riskhanteringsåtgärder och, i tillämpliga fall genomföra incidentrapportering. I riskhanteringsåtgärder innefattas utbildning om riskhantering och systematiskt och riskbaserat informationsarbete (läs mer i kapitel 7).

Förslagsställaren uppger vidare att förslagen kommer att medföra kostnader på samma sätt som för offentliga verksamhetsutövare, men samtidigt även stöd och övergripande besparingar.

Regelrådet gör följande bedömning. Det finns en övergripande beskrivning av vilka skyldighet företagen har utifrån direktivet, men det framgår inte vilken påverkan dessa skulle ha på företagens verksamhet, varken i tid eller kostnader. Utredningen innehåller en viss uppskattning av vilka kostnader de olika myndigheterna kommer ha, men det finns ingen motsvarande uppskattning för berörda företag. Förslagsställaren uppger visserligen att effekterna av förslagen behöver utredas vidare, men enligt Regelrådets mening borde utredningen ha resonerat mer kring vilka effekterna skulle kunna bli för berörda företag.

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

Påverkan på konkurrensförhållandena för berörda företag

Förslagsställaren uppger att samma krav kommer att gälla samtliga enskilda verksamhetsutövare inom respektive sektor, inte bara i Sverige utan även inom hela EES. Utredningen bedömer därför att regleringen inte får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.

Regelrådet gör följande bedömning. Det finns ett kortfattat resonemang kring varför konkurrensförhållandena inte påverkas, men Regelrådet menar att det hade förbättrat konsekvensutredningens kvalitet om förslagsställaren hade utvecklat detta resonemang närmare. Enbart det faktum att samma regler gäller för samtliga aktörer innebär inte att konkurrensförhållandena inte påverkas. Exempelvis kan betydelsen av en given kostnad för att följa regelkrav variera stort mellan olika företag.

Regelrådet finner att redovisningen av påverkan på konkurrensförhållandena för berörda företag är bristfällig.

Regleringens påverkan på företagen i andra avseenden

Det finns ingen information om att förslaget förväntas påverka företagen i andra avseenden.

Regelrådet bedömer att det inte finns något som uppenbart talar för att förslaget skulle medföra en påverkan på företagen i andra avseenden.

Regelrådet finner att avsaknaden av information om regleringens påverkan på företagen i andra avseenden är godtagbar.

Särskilda hänsyn till små företag vid reglernas utformning

Som tidigare nämnts under avsnittet *Berörda företag utifrån antal, storlek och bransch* omfattas små företag som huvudregel inte av bestämmelserna. Enligt förslaget är huvudregeln att verksamheten sysselsätter minst 50 personer eller har en omsättning som överstiger 10 miljoner euro per år för att företaget ska omfattas. Enskilda verksamheter kan dock komma att omfattas, men förslagsställaren bedömer att det endast bör röra sig om ett fåtal små företag.

Regelrådet gör följande bedömning. Det finns en tydlighet kring att små företag som regel inte omfattas och även en motivering till varför de i vissa fall omfattas. Regelrådet anser dock

att konsekvensutredningens kvalitet hade förbättrats om den även innehållit en beskrivning av vilka konsekvenserna blir för de små företag som faktiskt omfattas av reglerna.

Regelrådet finner ändå att redovisningen av särskilda hänsyn till små företag vid reglernas utformning är godtagbar.

Sammantagen bedömning

Förslaget innebär ett införlivande av det så kallade NIS2-direktivet som rör nätverks- och informationssystem. Utredningen föreslår att detta huvudsakligen sker genom en ny lag om cybersäkerhet. Regleringen omfattar fler verksamheter än tidigare, men huvudregeln är att mindre företag inte omfattas.

Regelrådet bedömer att det saknas en redovisning av hur många företag som kan komma att påverkas av regleringen. Det finns inte heller någon tydlig beskrivning av påverkan på kostnader, tidsåtgång och verksamhet för berörda företag, vilket är en brist. Beskrivningen av påverkan på konkurrensförhållandena för berörda företag får också anses knapphändig. Resterande delaspekter redovisas på ett godtagbart sätt. Sammantaget bedömer dock Regelrådet att konsekvensutredningen som helhet innehåller alltför lite information om vilka företag som berörs och hur de påverkas av regleringen.

Regelrådet finner därför 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 2 maj 2024.

I beslutet deltog Anna-Lena Bohm, ordförande, Helena Fond, Hans Peter Larsson, Lennart Renbjer och Lars Silver.

Ärendet föredrogs av Katarina Kjellström

Anna-Lena Bohm

Ordförande

Katarina Kjellström

Föredragande