Regelrådet

Yttrande	Vårt Dnr	Ert Dnr
2018-09-05	RR 2018-209	2017-11001 2017-10972 2018-05920 2018-05921 2018-05893

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.

Myndigheten för samhällsskydd och beredskap

Yttrande över Myndigheten för samhällsskydd och beredskaps förslag till föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, med flera på sakområdet angränsande förslag

Regelrådets ställningstagande

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

Remissen innehåller även förslag till allmänna råd, vilka inte omfattas av Regelrådets granskning.

Innehållet i förslaget

Till följd av ny lag (2018:1174) respektive förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster föreslår Myndigheten för samhällsskydd och beredskap (MSB) fem nya föreskrifter.

Lagen och förordningen genomför Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverk och informationssystem i hela unionen (NIS-direktivet). NIS-direktivet avser bindande miniminivåer. Det står medlemsstaterna fritt att skärpa kraven i direktivet.

Direktivet, lagen, förordningen och de nu föreslagna föreskrifterna berör flera samhällsviktiga sektorer; energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur.

Av lagen framgår vilka kriterier som ska uppfyllas för att vara leverantör av samhällsviktiga tjänster. De aktörer som är aktiva inom en eller flera av de berörda sektorerna behöver identifiera om de omfattas av regleringen. Föreskriftsförslaget om anmälan och identifiering av leverantörer[1] specificerar närmare vilka tjänster inom varje sektor som ska anses vara samhällsviktiga och vad som är att anse som en betydande störning vid tillhandahållande av tjänsten. Förteckningen över vad som ska anses vara samhällsviktiga tjänster utgår från NIS-direktivets bilaga II, med mindre justeringar för att passa den svenska marknaden. Skyldigheten för leverantörer att bedöma om deras verksamhet kan anses utgöra samhällsviktig tjänst följer av NIS-direktivet och i svensk rätt av lag (2018:1174). Föreskriften syftar till

[1] Förslag till föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, dnr 2018-05893.

att hjälpa leverantörerna i deras bedömning. Föreskrifterna reglerar även hur en identifierad aktör ska anmäla detta till tillsynsmyndigheten.

I förslaget som avser informationssäkerhet[2] ställs krav på att det systematiska och riskbaserade informationssäkerhetsarbetet, som enligt lagen ska bedrivas av leverantörerna, ska ske utifrån de internationellt accepterade och väl kända standarderna SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002. Standarderna bygger på samlade erfarenheter från olika verksamheter och länder och syftar till att uppnå ett effektivt arbete med informationssäkerhet.

Enligt 18 § lagen är leverantörerna skyldiga att rapportera incidenter som har en betydande inverkan på kontinuiteten i en samhällsviktig tjänst. I bedömningen om vad som ska avses med betydande inverkan ska enligt förordning antalet påverkade användare beaktas, hur länge incidenten varar och storleken på det geografiska området som påverkas. Enligt förordningen ska MSB, årligen till EU:s samarbetsgrupp, lämna en sammanfattande rapport om de incidentrapporter som mottagits i enlighet med lagen. Rapporten ska innehålla antalet rapporter, rapporterade incidenters art samt vilka åtgärder som vidtagits. MSB ska också informera berörda länder i EU om en incident som rapporterats av en leverantör har en betydande inverkan på kontinuiteten i samhällsviktiga tjänster i det landet. Föreskriftsförslaget som avser incidentrapportering för leverantörer[3] tydliggör kraven avseende vad, när och hur incidentrapportering till myndigheten ska ske.

Enligt föreskriftsförslaget ska en initial notifiering ske inom sex timmar efter att leverantören har identifierad en incident som rapporteringspliktig och uppföljande rapportering ska ske inom 24 timmar. Tidsfristen räknas från den tidpunkt då leverantören, med stöd av sina interna processer och rutiner, upptäcker incidenten. Bedömningen är att incidentrapporteringen bör ske efter de första kritiska åtgärderna för att avhjälpa incidenten har vidtagits. Den mängd information som ska lämnas inom sex timmar och även anvisade kontaktvägar är anpassade efter skyndsamhetskravet.

När det gäller incidentrapportering för leverantörer av digitala tjänster[4] tydliggör även detta föreskriftsförslag kraven avseende vad, när och hur incidentrapportering till MSB ska ske. Vad som ska rapporteras är däremot i högre grad styrt av EU-rätten än i fallet med leverantörer av samhällsviktiga tjänster. Enligt NIS-direktivet ska leverantörer vidta säkerhetsåtgärder i nätverk och informationssystem samt rapportera incidenter. Med digitala nätverk avses internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster. Säkerhetskrav och krav på vilka incidenter som ska rapporteras regleras i Kommissionens genomförandeförordning (EU) 2018/151. I genomförandeförordningen specificeras de aspekter som ska beaktas av leverantörer av digitala tjänster när de hanterar risker som hotar säkerheten i deras nät- och informationssystem samt parametrarna för fastställande av om en incident har avsevärd inverkan och därmed är rapporteringspliktig. EU:s medlemsstater får inte införa ytterligare säkerhets- eller rapporteringskrav för leverantörer av digitala tjänster. Samma tidsfrister föreslås för incidentrapporteringen som för förslaget för leverantörer av samhällsviktiga tjänster.

[2] Förslag till föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster, dnr 2017-11001.
[3] Förslag till föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster, dnr 2017-10972.
[4] Förslag till föreskrifter om rapportering av incidenter för leverantörer av digitala tjänster, dnr 2018-05920.

Föreskriftsförslaget om frivillig incidentrapportering[5] tydliggör kraven på vad, när och hur incidentrapporteringen till MSB ska ske i syfte att MSB på ett enhetligt och strukturerad sätt ska kunna ta emot och använda rapporterna samt hjälpa den rapporterande aktören.

Förslaget om frivillig incidentrapportering bygger på frivillighet och det finns, enligt Regelrådets bedömning, inget i förslaget som tyder på ett indirekt tvång. Regelrådet väljer därför att inte yttra sig över det föreskriftsförslaget.

Skälen för Regelrådets ställningstagande

Bakgrund och syfte med förslaget

I remissernas olika konsekvensutredningar framgår att syftet med NIS-direktivet är att uppnå en hög gemensam nivå av säkerhet i nätverk och informationssystem inom EU, att bli bättre i arbetet med informations- och cybersäkerhet och att skapa tillit till digital hantering av information.

Det framgår vidare att förslagsställarens föreskriftsförslag syftar till att förtydliga de krav som ställs på leverantörer av samhällsviktiga respektive digitala tjänster.

Regelrådet finner att förslagsställarens redovisning av förslagets bakgrund och syfte är godtagbar.

Alternativa lösningar och effekter av om ingen reglering kommer till stånd

I konsekvensutredningen för förslaget om identifiering och anmälan framgår att för att Sverige ska kunna uppfylla sina skyldigheter gentemot EU när det gäller krav på systematiskt och riskbaserat informationssäkerhetsarbete behöver aktörer i utpekade sektorer ett tydligt underlag för att kunna göra bedömningen om de omfattas av NIS-regleringen eller inte. Underlaget behöver även vara förhållandevis konstant för att den bedömning som aktören gör ska vara giltig över tid. MSB anser därför att ett sådant underlag behöver tydliggöras på föreskriftsnivå. Förslagsställaren uppger att föreskrifterna ska utgöra ett stöd för identifieringsarbetet, men att det ankommer på varje aktör att göra en egen bedömning om huruvida den uppfyller kriterierna eller inte.

Förslagsställaren redogör för de bedömningar som gjorts om vilka tjänster inom de olika sektorerna som är samhällsviktiga och anger att bedömningarna utgår från de fem kriterier som följer av lagen. Arbetet med dessa bedömningar uppges ha gjorts i samarbete med berörda tillsynsmyndigheter. Vid formuleringen av förteckningen av samhällsviktiga tjänster har, enligt konsekvensutredningen, NIS-direktivets skrivningar i bilaga II utgjort grunden. MSB uppger att för vissa tjänster är texten i princip översatt från direktivet och för andra har mindre justeringar gjorts för att passa den svenska marknaden. MSB gör därutöver bedömningen att om förteckningen skulle utformas så att färre aktörer skulle omfattas av NIS-regleringen skulle syftet att uppnå en hög säkerhet i nätverk och informationssystem för samhällsviktiga tjänster inte kunna uppnås.

MSB redogör för vilka faktorer som ska beaktas när bedömningen av vad som är en betydande störning görs och redovisar även sektorsvis vilka bedömningar MSB gjort och hur många aktörer som uppskattningsvis kommer att beröras.

[5] Förslag till föreskrifter om frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet, dnr 2018-05921.

Avseende förslaget om informationssäkerhet uppger förslagsställaren att ett alternativ till kravet på att det systematiska och riskbaserade informationssäkerhetsarbetet ska bedrivas utifrån de internationellt accepterade standarderna är att istället kräva att leverantörerna certifierar sitt informationssäkerhetsarbete. Ytterligare ett alternativ som anges är att införa en mer detaljerad kravställning för ett systematiskt och riskbaserat arbetssätt utan stöd av standarder. Förslagsställaren bedömer dock att båda alternativen skulle bli mer kostsamma för leverantörerna, men även utgöra ett sämre skydd mot risker, hot och sårbarheter.

När det gäller förslagen om incidentrapportering uppges att förordningen ställer krav på MSB att sammanfatta rapporter till en samarbetsgrupp på EU-nivå med ett visst innehåll. Av förordningen följer även krav på viss internationell rapportering till andra berörda EU-medlemsländer. Kraven medför därför att MSB måste föreskriva om vad, när och hur incidentrapporteringen till MSB ska ske. Avsaknaden av föreskrifter bedöms, förutom att skyldigheten gentemot EU och andra medlemsländer inte kan uppfyllas, även resultera i allt för stor otydlighet om hur en leverantör ska uppfylla rapporteringsplikten, vilket kan leda till en ojämn och sporadisk rapportering, där information inte kan användas för utformning av bland annat stöd och analyser. Därutöver anges att otydligheten skulle försvåra tillsynen.

Avseende incidentrapporter från leverantörer av digitala tjänster framgår dessutom att Kommissionens genomförandeförordning (EU) 2018/151 reglerar vilka åtgärder leverantörerna ska vidta för att hantera risker som hotar säkerheten i nätverk och informationssystem samt reglerar vilka incidenter som ska rapporteras. Medlemsländerna får därför inte införa ytterligare säkerhets- och rapporteringskrav för dessa leverantörer.

I konsekvensutredningen för förslaget som rör incidentrapportering för leverantörer av samhällsviktiga tjänster redovisas de överväganden som förslagsställaren gjort vid valet av kriterier för rapporteringspliktiga incidenter i respektive sektor.

När det gäller kravet på att initial notifiering ska ske inom sex timmar efter att leverantören har identifierat en rapporteringspliktig incident anges att tidsfristen är framtagen med anledning av möjligheten för Sveriges Computer Emergency Response Team (CERT-SE) att hjälpa leverantören med incidenten. Tidsfristen på sex timmar samt kravet på uppföljande rapportering inom 24 timmar möjliggör för CERT-SE och MSB att skapa en gemensam lägesbild och hjälpa leverantören samt informera allmänheten och andra aktörer både nationellt och internationellt.

Regelrådet kan konstatera att förslagsställaren på ett tillfredsställande sätt har redovisat alternativa lösningar i de fall sådana är möjliga, hänsyn tagen till överordnad rätt, liksom konsekvenserna av om en reglering uteblir. Regelrådet anser emellertid att det hade varit önskvärt om förslagsställaren i redovisningen hade inkluderat ett resonemang om huruvida det funnits avvägningar i utformningen av förteckningen som skulle kunna ifrågasättas av berörda företag och i så fall hur.

Regelrådet finner trots detta att förslagsställarens redovisning av alternativa lösningar och effekter av om ingen reglering kommer till stånd är godtagbar.

Förslagets överensstämmelse med EU-rätten

I konsekvensutredningarna för de olika förslagen anges att lag (2018:1174) respektive förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster i svensk rätt genomför Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

Föreskriftsförslagen uppges förtydliga sådant som följer av lagen, förordningen samt av EU-direktivet.

När det gäller förslaget om incidentrapporter från leverantörer av digitala tjänster anges att Kommissionens genomförandeförordning (EU) 2018/151[6] reglerar säkerhetskrav och krav på vilka incidenter som ska rapporteras. Medlemsländerna får inte införa ytterligare säkerhets- och rapporteringskrav för dessa leverantörer.

Förslaget i sin helhet överensstämmer, enligt förslagsställaren, med de skyldigheter som följer av Sveriges medlemskap i EU.

Regelrådet finner att förslagsställarens redovisning av förslagets överensstämmelse med EU-rätten är godtagbar.

Särskild hänsyn till tidpunkt för ikraftträdande och behov av speciella informationsinsatser

I konsekvensutredningarna för de olika förslagen anges att föreskrifterna bör träda ikraft så snart det är möjligt, eftersom NIS-direktivet började gälla den 10 maj i år och lag och förordning den 1 augusti. Förslagsställaren bedömer att ikraftträdandet av föreskrifterna skulle kunna ske under sista kvartalet år 2018.

Förslagsställaren gör bedömningen att berörda leverantörer kommer att behöva informeras genom speciella informationsinsatser som koordineras med respektive tillsynsmyndighet.

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

Berörda företag utifrån antal, storlek och bransch

I de olika konsekvensutredningarna anges att NIS-direktivet reglerar leverantörer av samhällsviktiga tjänster inom sju olika sektorer; energi, transport, bank, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten och digital infrastruktur. Direktivet anger att det är leverantörerna som bedriver verksamhet inom en eller flera av de angivna sektorerna och tillhandahåller en samhällsviktig tjänst som är ansvariga för att avgöra om de omfattas av direktivet eller inte. Både statliga myndigheter, kommuner, landsting och enskilda företag berörs.

[6] Kommissionens genomförandeförordning (EU) 2018/151[6] om tillämpningsföreskrifter för Europaparlamentets och rådet direktiv (EU) 2016/1148 om åtgärder för en högre gemensam nivå på säkerhet i nätverk och informationssystem i hela unionen.

I konsekvensutredningen för förslaget om anmälan och identifiering framgår att för energislaget el ingår stamnätsföretag, regionnätsföretag som utgör länken mellan stamnät och distribution respektive anslutning för större produktion. Vidare ingår elnätsföretag som tillhandahåller el till användare inom de högsta prioritetsklasserna enligt Styrel[7]. Eftersom även små företag levererar el till användare inom dessa högsta prioriteringsklasser kan de vara berörda. Kraftverk som är anslutna till stam- och regionnät berörs med undantag för industrimottryck eller annan elproduktion till direkt ansluten industri. Därutöver ingår ett trettiotal elhandelsbolag som har tecknat avtal med Svenska kraftnät och balanserar felprognostiseringar. Totalt bedöms att cirka 200 aktörer inom elsektorn kan komma att identifiera sig som leverantörer av samhällsviktiga tjänster.

För energislaget olja förtydligar förslagsställaren att endast hanteringen med flytande bränslen och drivmedel ska avses vara av samhällsviktig, vilket är ett avsteg från NIS-direktivet där även tunga produkter som bitumen, smörjoljor och industrioljor, diverse bränslen samt nafta och gasol ingår. Bedömningen är att 10 till 20 aktörer inom sektorn berörs och att dessa avser aktörer inom import, export, produktion, raffinering eller bearbetning, aktörer som verkar inom områden för de största och viktigaste depåerna av drivmedelslager i landet, inklusive aktörer som handhar lastning och lossningsutrustning inom området. Därutöver berörs aktörer som arbetar med överföring av olja i ledningar och distributionsnät i den mån de finns sådana som hanterar överföring i större omfattning.

Inom energislaget gas anges att endast cirka 10 aktörer bedöms uppfylla kriterierna för att leverera samhällsviktiga tjänster. I NIS-direktivet avses naturgas, det vill säga metangas med fossilt ursprung. Naturgas ingår, enligt förslagsställaren, ibland i stadsgas som är en blandning av metangas och luft. Biogas omfattas inte av direktivet. Tjänster som hanterar systemansvar för transmissionssystem, liksom distributionssystem samt handel och leverans av naturgas omfattas.

När det gäller transportsektorn delas den in i trafiktjänster som tillhandahålls av transportföretag, förvaltning av viktig infrastruktur och trafikledningstjänster. I bedömningen av vad som ska anses vara en samhällsviktig leverantör av trafiktjänster har hänsyn tagits till mängden passagerare eller gods som tjänsten hanterar, liksom hur stora de samhälleliga och ekonomiska konsekvenserna skulle bli vid en störning exempelvis för handeln och tillgången på varor. Här ingår lufttrafikföretag, rederier och järnvägsoperatörer.

I förvaltning av trafikinfrastruktur ingår flygplatser, hamnar, järnvägar och vägnät. För flyg, hamnar och järnväg har hänsyn tagits till mängden passagerare eller gods samt konsekvenserna av störning för passagerare, utrikeshandel och tillgång på varor. För hamnar ingår isbrytningsverksamhet.
För vägnätet utgör staten den största aktören samt kommuner. Det handlar om drift, underhåll byggande, liksom nätverks- och informationssystem kopplat till funktionaliteten. Längre tunnlar ingår också. Vidare ingår tjänster inom transportsektorn, till exempel larmcentraler som SOS Alarm och deras tjänst e-Call (automatisk larmtjänst i bilen) och NVDB (Nationell VägDataBas) som förvaltas av Trafikverket.

Inom trafikledningstjänster ingår, enligt konsekvensutredningen flygkontrolltjänster, sjötrafikinformationstjänst och trafikledning inom järnväg. MSB bedömer att i hela transportsektorn berörs några hundratal aktörer.

[7] Energimyndighetens projekt som prioriterar elberoende för samhällsviktiga elanvändare.

För banksektorn utgår MSB från den EU-gemensamma regleringen på området och det regelverk som tillämpas av tillsynsmyndigheterna. De samhällsviktiga tjänsterna inom sektorn bedöms i Sverige utgöras av betaltjänster enligt 1 kap. 2 § 1-6 lag (2010:751) om betaltjänster. Betalningsinitieringstjänster och kontoinformationstjänster ingår däremot inte. För att betraktas som samhällsviktig ska en aktör utöver att den tillhandahåller en rad betaltjänster som anges i lagen, även vara ett kreditinstitut enligt 1 kap. 5 § 10 lag (2004:297) om bank- och finansieringsrörelse som enligt Finansinspektionens årliga tillsynskategorisering tillhör kategori 1 eller 2, eller utgöra ett utländskt kreditinstitut som driver finansieringsrörelse i Sverige genom en filial med en balansomslutning om minst 500 miljarder kronor. Bedömningen är att cirka 10 aktörer uppfyller kriterierna.

Liksom för banksektorn utgår MSB från den EU-gemensamma regleringen som gäller för finansmarknadsinfrastrukturen. I syfte att säkerställa att NIS-regleringen endast omfattar de samhällsviktiga handelsplatserna, där en incident skulle kunna orsaka en betydande störning, har en avgränsning satts till handelsomsättningen om minst 1 miljard kronor per dag. MSB bedömer att ett fåtal aktörer uppfyller kriterierna.

Inom hälso- och sjukvård berörs både de största vårdgivarna som akutsjukhusen och mindre aktörer på regional och lokal nivå. Vårdgivare där antal årsanställd legitimerad vårdpersonal överstiger 50 personer berörs enligt konsekvensutredningen.

När det gäller leverans och distribution av dricksvatten berörs huvudman enligt 2 § lag (2006:412) om allmänna vattentjänster som producerar och/eller distribuerar dricksvatten till fler än 20 000 personer. Om en beräkning av hur många personer som tillhandahålls dricksvatten behöver göras bör 200 liter per person och dygn användas. De huvudmän som levererar dricksvatten till akutsjukhus berörs också, oavsett hur många personer aktören levererar vatten till. Aktörer inom förpackat dricksvatten berörs inte i Sverige. MSB bedömer att det finns cirka 200 aktörer som berörs inom sektorn för dricksvatten.

Inom digital infrastruktur berörs domännamnssystemet DNS-tjänster och administration av toppdomäner samhällsviktiga tjänster. Det uppges att avseende registreringsenheter för toppdomäner berörs två domäner nämligen *.se* (1,8 miljoner registrerade domännamn) och *.nu* (295 000 registrerade domännamn). Gällande DNS-tjänster berörs stora kommersiella aktörer som allmänt tillhandahåller tjänsterna. DNS-tjänster i form av en rekursiv namnservertjänst som används av fler än 100 000 användare, eller en auktoritativ namnservertjänst som har fler än 25 000 aktiva domännamn anslutna. MSB bedömer att cirka 30 aktörer uppfyller kriterierna för att anses vara leverantörer av samhällsviktiga tjänster.

När det gäller förslaget om rapportering av incidenter för leverantörer av digitala tjänster uppges att juridiska personer berörs om de tillhandahåller en digital tjänst och har sitt huvudsakliga etableringsställe i Sverige eller har utsett en företrädare som är etablerad här. Totalt rör det sig, enligt MSB, om cirka 90 leverantörer fördelat på internetbaserade marknadsplatser, internetbaserade sökmotorer samt molntjänster. Det uppges vidare att NIS-direktivets indelning och beskrivning av digitala tjänster inte motsvarar någon etablerad indelning på den svenska digitala marknaden idag. Det är, enligt MSB, sannolikt att det finns digitala tjänster på den svenska marknaden som berörs av regleringen, men som inte kunde identifieras i den initiala kartläggningen. Marknaden förändras dessutom snabbt, liksom de branscher som verkar inom den och sammantaget kan detta, enligt MSB, medföra att en undersökning kan behöva genomföras igen.

Regelrådet kan konstatera att utöver redovisningen av antalet berörda per bransch finns även en generell beskrivning av storleken på företagen, och i de fall mindre företag berörs redovisas anledningen till detta samt en motivering.

Regelrådet finner att förslagsställarens redovisning av berörda företag utifrån antal, storlek och bransch är godtagbar.

Påverkan på berörda företags kostnader, tidsåtgång och verksamhet

Administrativa kostnader

I konsekvensutredningen för förslaget om identifiering och anmälan anges att tidsåtgången och tillkommande administrativa kostnader för identifiering och anmälan bedöms vara försumbara.

När det gäller förslaget om informationssäkerhet uppger förslagsställaren att ett systematiskt riskbaserat informationssäkerhetssamarbete ska ske enligt 11 § lag (2018:1174). Det pågår ständigt och behöver även kontinuerligt anpassas till nya förutsättningar. Kostnaden för detta arbete uppges variera utifrån hur väl arbetet sker hos leverantören idag och den samhällsviktiga verksamhet som företaget bedriver. Förslaget i föreskrifterna om att det systematiska och riskbaserade informationssäkerhetsarbetet ska bedrivas utifrån internationellt accepterade standarder medför för de flesta företagen, enligt MSB, ingen kostnad, eftersom arbetet redan idag styrs av reglering som motsvarar eller som har högre krav än i förslaget. MSB anser att de företag som behöver bygga upp ett systematiskt riskbaserat informationssäkerhetssamarbete från grunden till viss del kan omfördela de resurser som redan idag arbetar på annat sätt med att upprätthålla leveranser genom att företagen flyttar fokus till förebyggande arbete. Det kan då uppstå en initial kostnad under ett till två år innan effekten av säkrare leveranser kan hämtas hem. MSB bedömer att leverantörerna kan komma att vältra över initiala kostnader på konsumenter och kunder.

I konsekvensutredningen för förslaget om incidentrapportering för leverantörer av samhällsviktiga tjänster anges att kravet på incidentrapportering framgår av 18 § lag (2018:1174). Föreskriftförslaget anger i sin tur hur rapporteringen ska gå till. MSB bedömer att för flertalet leverantörer kan kravet på incidentrapportering vara en ny uppgift som medför nya kostnader. Kostnaderna bedöms främst uppstå i uppbyggnadsskedet när anpassning av processer och rutiner kan behöva ske. Myndigheten uppger dock att den arbetar med att ta fram ett tekniskt gränssnitt för rapporteringen som syftar till att underlätta för leverantörerna. Vidare uppges att även leverantörer som lägger ut sin informationshantering på underleverantörer kan få kostnader i samband med att processer och rutiner kan behöva anpassas och nya avtal eventuellt behöver skrivas.

MSB uppger att när det gäller kravet på att den initiala notifieringen ska ske inom sex timmar efter att en incident identifierats som rapporteringspliktig har hänsyn tagits till leverantörens behov att hantera de första kritiska åtgärderna för att avhjälpa incidenten. Vidare anges att när det gäller den mängd information som ska lämnas inom dessa sex timmar, liksom anvisade kontaktvägar är kraven anpassade efter skyndsamhetskravet. Tidsfristen på sex timmar är därutöver, enligt MSB, framtagen för att CERT-SE, vid behov och när så är möjligt, ska kunna hjälpa leverantören med incidenten. Kravet på både initial notifiering inom sex timmar och på uppföljande rapportering inom 24 timmar har vidare valts för att CERT-SE och MSB ska kunna skapa en samlad lägesbild och därefter kunna agera på lämpligt

sätt för att avhjälpa incidenten samt i sin tur uppfylla krav på vidare rapportering såväl nationellt som internationellt. MSB understryker vikten av ett fungerande säkerhetsarbete för att förebygga allvarliga incidenter.

MSB uppger att Kommissionens genomförandeförordning (EU) 2018/151 specificerar vilka hänsyn som ska tas när leverantörer av digitala tjänster vidtar tekniska eller organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem samt vad som avses när en incident har avsevärd inverkan och därmed är rapporteringspliktig, det vill säga vilka incidenter som ska rapporteras.

MSB bedömer att incidentrapportering är en ny uppgift för flertalet leverantörer, men att de flesta torde bedriva ett informationssäkerhetsarbete på något sätt. Kraven i NIS-direktivet, i nationell lag och i genomförandeförordningen gällande incidentrapportering bedöms därför medföra nya kostnader för berörda företag. Kostnaderna avser främst uppstå i uppbyggnadsarbetet med processer och rutiner, men bedöms inte vara betydande. MSB:s arbete med ett tekniskt gränssnitt för rapporteringen bedöms underlätta för leverantörerna när de ska rapportera. Avseende förskrifternas krav om tidsfristerna för rapporteringen anger förslagsställaren samma uppgifter som i konsekvensutredningen för rapportering av incidenter för leverantörer av samhällsviktiga tjänster.

Regelrådet anser att förslagsställaren borde ha fört ett fördjupat resonemang om den anpassning till den svenska marknaden som gjorts av förteckningen över samhällsviktiga tjänster och kopplat det resonemanget till företagens kostnader. Såvitt Regelrådet förstår blir förteckningen helt avgörande för om ett företag ska identifiera sig som leverantör av en samhällsviktig tjänst och därmed omfattas av den reglering som nu föreslås i de olika föreskrifterna och till följd av det även komma att omfattas av de kostnader som följer av förslagen. Regelrådet efterlyser, liksom redan påtalats, en redovisning av om det funnits avvägningar i utformningen av förteckningen som skulle kunna ifrågasättas och i så fall hur.

Regelrådet anser därutöver att redovisningen är motsägelsefull när det kommer till beskrivningen av förslagens konsekvenser för berörda företag. Förslagsställaren anger tydligt att bedömningen är att förslagen får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt, men samtidigt beskrivs genomgående de kostnadsmässiga effekterna som obetydliga, begränsade eller försumbara. Regelrådet kan konstatera att kraven på att identifiering och anmälan ska göras, liksom på att ett systematiskt och riskbaserat informationssäkerhetsarbete ska bedrivas samt kraven på att incidentrapportering ska ske kommer från överordnad EU- respektive nationell rätt och att MSB nu i sina föreskriftsförslag förtydligar regelverket och anger detaljbestämmelser för hur allt detta ska hanteras. De administrativa kostnaderna som omskrivs synes därför till största delen komma från just överordnad rätt. Regelrådet anser att det likväl hade varit önskvärt med en tydligare redovisning av de administrativa kostnader som följer av de föreslagna detaljbestämmelserna och en motivering till varför effekterna trots sina försumbara kostnader likväl ska betraktas som betydande.

Regelrådet finner därför att förslagsställarens redovisning av förslagets administrativa kostnader är bristfällig.

Andra kostnader och verksamhet

I konsekvensutredningen till förslaget om informationssäkerhet uppges att genom att leverantörerna kommer att arbeta kontinuerligt och effektivt för att uppnå tillräcklig säkerhet i sina leveranser, kommer de över tid även att minska sin risk för störningar i leveranserna till kunderna.

Det uppges även att en kostnad för utbildning i systematiskt och riskbaserat arbete utifrån standarderna SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002 eller motsvarande kan tillkomma för berörda företag.

När det gäller förslaget om incidentrapportering för leverantörer av samhällsviktiga tjänster anges att kraven avseende tidsfristerna för rapporteringen inte ska tolkas som krav på ökad bemanning.

Regelrådet kan konstatera att förslagsställaren i sina respektive konsekvensutredningar bedömer att förslagen kan få betydande effekter bland annat för företagens arbetsförutsättningar och villkor i övrigt. Regelrådet saknar en närmare redovisning av vad som avses med denna bedömning. Regelrådet anser därutöver att det hade varit önskvärt om förslagsställaren hade redovisat en uppskattning av de utbildningskostnader som leverantörerna kan komma att få.

Regelrådet finner därför att förslagsställarens redovisning av andra kostnader och verksamhet är bristfällig.

Påverkan på konkurrensförhållandena för berörda företag

I de respektive konsekvensutredningarna anges att ett av syftena med regleringen är att säkerställa att leverantörerna får samma förutsättningar att konkurrera på lika villkor. Detta motverkar, enligt förslagsställaren, att en leverantör erbjuder en tjänst till lägre pris för att därefter ta ut en extra kostnad från sina kunder när leveransen på grund av bristande informationssäkerhet inte fungerar. De leverantörer som idag arbetar systematiskt och riskbaserat bedöms därmed få en mer rättvis konkurrenssituation. Kravet på incidentrapportering är lika för leverantörerna, men den som drabbas av många incidenter måste i högre grad rapportera.

Det uppges även att företag som inte påverkas av regleringen likväl aktivt kan välja att arbeta på ett systematiskt och riskbaserat sätt med informationssäkerhet och då marknadsföra sig som leverantörer som arbetar utifrån föreskriftskraven.

När det gäller förslaget om identifiering och anmälan och närmare bestämt identifiering av leverantörer inom energislaget gas uppger förslagsställaren att det i Sverige sker en stark utveckling av gassegmentet metangas. Det uppges att metangas i form av biogas inte omfattas av NIS-direktivet och därför inte heller av NIS-regleringen i Sverige. Endast metangas i form av naturgas omfattas, vilket, enligt förslagsställaren, kan bidra till en snedvridning av konkurrensen i delsektorn gas.

Regelrådet finner att förslagsställarens redovisning av förslagets påverkan på konkurrensförhållandena för berörda företag är godtagbar.

Regleringens påverkan på företagen i andra avseenden

I konsekvensutredningarna till förslagen om incidentrapportering framgår att den kunskapsbank som MSB kan bygga upp tack vare incidentrapporteringen och analyser som genomförs av informationen ger underlag till utvecklingen av råd och stöd som kan förmedlas till leverantörerna.

Regelrådet finner att förslagsställarens redovisning av regleringens påverkan på företagen i andra avseenden är godtagbar.

Särskilda hänsyn till små företag vid reglernas utformning

I konsekvensutredningen för förslaget om identifiering och anmälan framgår att förslagsställaren vid utformningen av kriterier för identifieringen har volym och därmed indirekt storlek på företagen varit en parameter. Små företag bedöms endast i undantagsfall beröras av regleringen och då på grund av att de tjänster som företagen levererar är samhällsviktiga. Förslagsställaren bedömer att undantag avseende kravställningen därför inte kan göras.

I konsekvensutredningen för förslaget om ett riskbaserat säkerhetsarbete uppger förslagsställaren att det inte har tagits någon särskild hänsyn till små företag. Säkerhetsarbetet ska emellertid anpassas efter leverantörens verksamhet, vilket gör det möjligt för små företag att utgå från sina egna förutsättningar i sitt informationssäkerhetsarbete.

I konsekvensutredningarna för förslagen om incidentrapportering uppges att ingen särskild hänsyn till små företag har tagits, eftersom det bedöms att dessa företag endast i undantagsfall berörs av regleringen.

Regelrådet finner att förslagsställarens redovisning av särskild hänsyn till små företag vid reglernas utformning är godtagbar.

Sammantagen bedömning

Regelrådet kan konstatera att förslagsställaren på ett godtagbart sätt redovisar konsekvenserna av sina förslag på samtliga punkter, förutom när det gäller de kostnads- och verksamhetsmässiga effekterna. Redovisningen av sådana effekter väger vanligtvis tungt i Regelrådets bedömningar av konsekvensutredningars kvalitet. Regelrådet kan likväl konstatera att kraven i allt väsentligt, härrör från överordnad EU- respektive nationell rätt. De kostnads- och verksamhetsmässiga, liksom de konkurrensmässiga effekterna synes därför till största delen komma från just överordnad rätt. Även om Regelrådet anser att det hade varit önskvärt med en tydligare redovisning av de kostnads- och verksamhetsmässiga effekter som följer av de föreslagna detaljbestämmelserna, liksom en motivering till varför effekterna, trots sina försumbara kostnader, likväl ska betraktas som betydande, anser Regelrådet att redovisningen i detta fall kan betraktas som tillräcklig.

Regelrådet finner därför att konsekvensutredningen 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 5 september 2018.

I beslutet deltog Pernilla Lundqvist (ordförande), Annika Bergman, Claes Norberg, Lennart Renbjer och Marie-Louise Strömgren.

Ärendet föredrogs av Annika LeBlanc.

Pernilla Lundqvist
Ordförande

Annika LeBlanc
Föredragande