

Regelrådets uppgift 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 förslag till föreskrifter om anmälan och identifiering av väsentliga och viktiga verksamhetsutövare

Regelrådets ställningstagande

Regelrådet bedömer att konsekvensutredningen inte uppfyller kraven i förordningen (2024:183) om konsekvensutredningar.

Motivering till Regelrådets ställningstagande

Flertalet relevanta aspekter i konsekvensutredningsförordningen är godtagbart redovisade. Vissa centrala aspekter, såsom redovisningen av konkurrenspåverkan, hänsyn till små och medelstora företag och beskrivning av hur och när konsekvenserna av förslaget kan utvärderas är emellertid bristfälligt redovisade. Förutom bättre beskrivningar av dessa aspekter hade Regelrådet dessutom velat se något mer detaljerade redovisningar i överväganden kring alternativa lösningar vad avser den utvidgade kretsen av berörda företag och sektorer. Det hade också höjt kvaliteten om det hade förekommit en uppskattning av hur de olika aktörerna antalsmässigt var fördelade i olika berörda branscher, särskilt vad avser de branscher och företag som inte uppfyller storlekskravet, men som ändå föreslås omfattas av reglerna. Förslagsställaren borde också ha redovisat exempelberäkningar för att underbygga de slutsatser om marginella kostnader för de befintliga förslagen som dras i innevarande remiss.

Innehållet i förslaget

Myndigheten för samhällsskydd och beredskap (MSB) föreslår föreskrifter som ska komplettera vissa bestämmelser i den kommande cybersäkerhetslagen. Det rör anmälningsskyldighet enligt 2 kap 2 §, kriterier för en organisations bedömning om den utgör en verksamhetsutövare i cybersäkerhetslagens mening avseende undantag från storlekskravet för partnerföretag och anknutna företag enligt 1 kap 4 §, identifiering av huvudsakligt etableringsställe enligt 1 kap 7 § och undantag från kravet på att storleksmässigt motsvara eller vara större än ett medelstort företag enligt 1 kap 5 § p 1 - 3. Förslaget omfattar vidare vilka ytterligare verksamhetsutövare som ska omfattas av regelverket och vilka som ska definieras som väsentliga enligt 1 kap 8 § p 6.

Som väsentliga verksamhetsutövare enligt lagen föreslås bland annat beredskapsflygplatser, flygtrafikledning, karantänshamnar, vissa producenter och distributörer av dricksvatten och akutsjukhus vara. Viktiga verksamhetsutövare föreslås bland annat vara vissa storskaliga verksamheter inom produktion och distribution av kemikalier inom områden såsom dricksvattenrening, avloppsrening, industriell tillverkning av livsmedel, brandsläckningsmedel och rengöringsmedel för hälso- och sjukvård.

Undantagna från tillämpningsområdet föreslås bland annat vara verksamhetsutövare som endast uppfyller storlekskravet genom sin anknytning till andra företag, där drift och förvaltning av den egna produktionsmiljön i hög grad bedrivs oberoende av produktionsmiljön hos verksamhetsutövarens partner eller anknutna företag, eller där denne i övrigt åtnjuter en sådan hög grad av oberoende i förhållande till partnerföretag eller anknutna företag att det skulle vara oproportionerligt att verksamhetsutövaren skulle omfattas.

En anmälan ska bland annat innehålla uppgifter om namn på verksamhetsutövaren, organisationsnummer, adress och telefonnummer till verksamhetsutövaren, identifierare mot externa nätverk såsom ip-adress eller ip-adressintervall, samtliga anmälningspliktiga verksamheter, inom vilka sektorer och viktiga samhällsfunktioner verksamhetsutövaren bedriver verksamhet, om verksamhetsutövaren är väsentlig eller viktig, och i vilka medlemsstater i EU verksamhetsutövaren bedriver verksamhet i enlighet med bilaga 1 eller bilaga 2 till EU:s cybersäkerhetsdirektiv (NIS2-direktivet).

Vid bedömningen av vilken medlemsstat inom EU som ska utgöra huvudsakligt etableringsställe föreslås följande omständigheter beaktas i angiven rangordning: 1) där beslut om ledning och styrning av arbetet med cybersäkerhet i huvudsak fattas, 2) där det huvudsakliga driftcentret för cybersäkerhetsverksamhet är placerat, eller 3) där verksamhetsutövaren har flest anställda.

Uppgifterna ska lämnas på det sätt MSB anvisar.

Bedömning av delaspekter

Problembeskrivning och syftet med förslaget

MSB har givits i uppdrag att föreslå genomförande av vissa bestämmelser i NIS2-direktivet i svensk rätt. Syftet med NIS2-direktivet är förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam nivå på cybersäkerhet. NIS2 omfattar bland annat betydligt fler aktörer och ställer skärpta och tydligare krav på riskanalyser, vilka säkerhetsåtgärder aktörer ska vidta och hur incidentrapportering ska genomföras jämfört med det nuvarande NIS-direktivet. MSB beskriver översiktligt befintlig lagstiftning och det nya direktivet. Genomförandet kommer att ske dels genom en ny lag och förordning (den förra är nu på lagrådsremiss), dels genom föreskrifter. MSB och Post- och telestyrelsen (PTS) kommer att ges bemyndigande att utfärda föreskrifter för att genomföra vissa bestämmelser. Den innevarande remissen syftar till att komplettera förslaget till cybersäkerhetslag.

Regelrådet bedömer redovisningen godtagbar.

Konsekvenser om ingen åtgärd vidtas

Det anges bland annat att Sverige är skyldig att implementera NIS2-direktivet i svensk rätt.

Regelrådet bedömer redovisningen godtagbar.

Alternativa lösningar

Det anges att vägledningar i stället för föreskrifter kunde vara alternativa lösningar.

Därutöver anges att det i 1 kap 4 § p 3 cybersäkerhetslagen framgår att lagen gäller verksamhetsutövare som storleksmässigt motsvarar eller är större än ett medelstort företag.

Enligt 1 kap 5 § i cybersäkerhetslagen kan verksamhetsutövare som inte uppfyller storlekskravet 1 kap 4 § cybersäkerhetslagen ändå omfattas om 1) verksamhetsutövaren är den enda leverantören av en tjänst i Sverige som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, 2) en störning av den tjänst som verksamhetsutövaren tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa eller kan medföra betydande systemrisk, eller 3) verksamhetsutövaren har särskild betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av verksamhetsutövaren. Detta för att säkerställa att även en mindre aktör som kan bedriva en verksamhet, där en störning kan få en stor påverkan på den inre marknaden, fångas upp. Om dessa aktörer inte omfattas kan det innebära att den inre marknads funktion inte kan upprätthållas och det blir svårare att uppfylla cybersäkerhetslagens syfte att uppnå en hög nivå av cybersäkerhet i samhället. Det anges i detta sammanhang att MSB, i samverkan med föreslagna tillsynsmyndigheter, har gjort en bedömning av vilka typer av verksamhetsutövare som borde omfattas av regleringen trots att de inte uppfyller storlekskravet. Alternativet att inte identifiera sådana verksamhetsutövare anges innebära att nyckelaktörer inte skulle omfattas av kraven och därmed inte åläggas att vidta lämpliga och proportionella säkerhetsåtgärder samt att störningar i deras nätverks- och informationssystem som skulle kunna innebära samhällsstörningar inte på samma sätt fångas upp i den nationella lägesbilden.

Därutöver anges att det av skäl 16 i NIS 2-direktivet framgår att medlemsstater kan meddela undantag från tillämpningsområdet för vissa partnerföretag och anknutna företag. Det anges att förslaget till utformning av kriterierna för sådana undantag motsvarar detta skäl. Även om skälen i sig inte är bindande bedöms det motverka en harmoniserad implementering av direktivet i EU att inte beakta skälen. Brist på harmonisering kan bidra till ökade administrativa kostnader för exempelvis företagskoncerner med partnerföretag i flera olika medlemsstater.

Vad avser väsentliga och viktiga verksamhetsutövare som omfattas av föreskrifterna beskrivs och hänvisas till överordnad rätt.

Regelrådet gör följande bedömning. Förslagsställaren har redogjort för olika typer av alternativa lösningar. Dels sådana som rör alternativ till föreskrifter, dels sådana som rör mer substantiella överväganden. Regelrådet bedömer att beskrivningen av alternativ till föreskrifter är utförlig och väl motiverad. Det samma gäller de mer substantiella förslagen om föreslagna undantag. Vad avser förslagen till inkludering av ytterligare verksamheter som inte möter storlekskravet i direktivet är de översiktligt motiverade. Det hade höjt kvaliteten om de varit lite mer detaljerat beskrivna och att redovisningen även hade beskrivit vilka verksamheter som övervägts, men som valts bort och av vilka skäl.

Regelrådet bedömer dock redovisningen godtagbar.

Berörda företag

Det anges att NIS2-direktivets tillämpningsområde följer av dess artikel 2, som hänvisar till bilaga 1 och 2. I bilaga 1 pekas 11 högkritiska sektorer ut. De rör energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvårdssektorn, dricksvatten, avloppsvatten, digital infrastruktur, förvaltning av IKT-tjänster mellan företag, offentlig förvaltning och rymden. Dessa högkritiska sektorer anges i hög grad motsvara de som i dag omfattas av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

I bilaga 2 finns övriga sektorer som omfattas av NIS2-direktivet. Dessa benämns som kritiska sektorer och avser post- och budtjänster, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion, bearbetning och distribution av livsmedel, digitala leverantörer och forskning. Bland de kritiska sektorerna ingår också tillverkning, som i sin tur omfattar delsektorerna tillverkning av medicintekniska produkter, datorer, elektronikvaror och optik, elapparater, övriga maskiner, motorfordon, släpfordon och påhängsvagnar och andra transportmedel. I jämförelse med det tidigare NIS-direktivet och NIS-lagen är det i sin helhet nya områden. Vissa sektorer och typer av verksamhetsutövare omfattas av NIS2-direktivet oavsett storlek. Det gäller exempelvis verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät, allmänt tillgängliga elektroniska kommunikationstjänster, betrodda tjänster, registreringsenhet för toppdomäner, DNS-tjänster eller domännamnsregistrering.

MSB gör uppskattningen att cirka 600 privata och offentliga aktörer idag omfattas av NIS-direktivet. När det gäller NIS2-direktivet anges regeringen uppskatta att cirka 1 500 företag skulle kunna beröras och att dessa, med några undantag, rör företag som klassas som minst medelstora. MSB anger att en grov uppskattning av hur många företag som tillkommer med stöd av föreskrifterna om anmälan och identifiering sannolikt inte handlar om fler än 50 och att majoriteten av dessa verkar inom avloppsvattenshantering och dricksvattenförsörjning. För tillverkning av kemikalier medför föreskriften att antalet potentiella aktörer som kan omfattas begränsas. Det anges vidare att mer exakta siffror kan ges när cybersäkerhetslagen träder i kraft och verksamhetsutövarna anmäler sig till utpekad myndighet.

Regelrådet gör följande bedömning. Det förekommer en översiktlig redovisning av berörda företag till följd av det nya regelverket, både egna uppskattningar och sådana som regeringen gjort, liksom en genomsnittlig bedömning av storlek. Det är positivt att MSB har försökt uppskatta antal tillkommande företag och inom vilka branscher som följer av det nya regelverket i de föreslagna delarna som nu är aktuella. Det hade höjt kvaliteten om det hade förekommit en uppskattning av hur de olika aktörerna antalsmässigt var fördelade i olika berörda branscher, särskilt vad avser de branscher och företag som inte uppfyller storlekskravet i 1 kap 4 § cybersäkerhetslagen, men som ändå föreslås omfattas av reglerna.

Regelrådet bedömer dock redovisningen godtagbar.

Påverkan på företagens kostnader och intäkter

Det anges att givet att nödvändiga vägledningar och systemstöd finns att tillgå bedöms föreskrifterna om anmälan och identifiering i sig endast innebära marginell tidsåtgång och marginellt ökade administrativa kostnader för företagen. Bedömningen är också att de kan bidra till minskade kostnader genom att tillhandahålla tydliga rättsliga ramar och därmed bidra till förutsebarhet vid implementeringen av NIS2-direktivet i Sverige.

Konsekvensutredningen beskriver översiktligt de kostnadsuppskattningar som EU-kommissionen respektive tidigare utredning (SOU 2024:188) gjort och anger att de kostnadsmissiga och andra konsekvenser som följer av det nya regelverket bör bedömas utifrån ett helhetsperspektiv tillsammans med MSB:s övriga föreskrifter som kommer att utfärdas i enlighet med mandatet i cybersäkerhetsförordningen. Det hänvisas specifikt till kommande konsekvensutredningar för MSB:s NIS2-föreskrifter om säkerhetsåtgärder och utbildning respektive incidentrapportering och informationskyldighet för en mer detaljerad genomgång av kostnader för berörda verksamhetsutövare.

Regelrådet gör följande bedömning. Förslagsställaren borde åtminstone ha redovisat exempelberäkningar för att underbygga dragna slutsatser om marginella kostnader för de befintliga förslagen i innevarande remiss. Det förekommer inga resonemang kring påverkan på intäkter.

Regelrådet bedömer redovisningen bristfällig.

Påverkan på konkurrens

MSB bedömer att regleringen inte kommer att påverka konkurrensförhållanden eftersom NIS2-direktivet kommer att gälla samma typer av företag i hela unionen.

Regelrådet gör följande bedömning. Redovisningen är inte tillräcklig. För det första är det inte troligt att företags-, branschstrukturer eller marknadsvillkor ser ut på samma sätt i olika medlemsstater, vilket kan påverka konkurrenssituationen mellan företag inom EU. För det andra finns en risk att medlemsstaterna kommer att genomföra direktivet på olika sätt, något som medges mot bakgrund av att det är fråga om ett minimidirektiv. För det tredje förekommer inget resonemang kring relationen till företag i tredje land, vilket är högst relevant för en analys om konkurrenspåverkan. Förslagsställaren borde ha resonerat kring dessa tre aspekter, åtminstone vad avser förslagen och överväganden kring tillämpningsområdet.

Regelrådet bedömer redovisningen bristfällig.

Särskilda hänsyn till små och medelstora företag

Det anges att föreskrifterna som huvudregel inte gäller små företag och att någon generell hänsyn därför inte bedömts behövas tas till dessa vid reglernas utformning. De små företag som ändå omfattas gör det på grund av deras vikt för samhällets funktionalitet. Extra stödinsatser kan bli aktuella i det fall det behövs.

Regelrådet bedömer redovisningen knapphändig, men godtagbar.

Åtgärder för att begränsa kostnader och andra negativa effekter

Det förekommer vissa omnämmanden om behovet och utarbetande av vägledning, tekniska system och andra stödinsatser.

Regelrådet bedömer redovisningen knapphändig, men godtagbar.

Särskild hänsyn till tidpunkt för ikraftträdande och behov av speciella informationsinsatser

Det anges att lag och förordning om cybersäkerhet som ska genomföra NIS2-direktivet planeras att träda i kraft den 15 januari 2026. Eftersom innevarande förslag till föreskrifter har som syfte att stödja verksamhetsutövarna genom att konkretisera kraven i lag och förordning och därmed göra det enklare att efterleva dessa anges föreskrifterna behöva träda i kraft i så nära anslutning som möjligt till detta datum. Med hänsyn till remissförfarande och beredning bedöms föreskrifterna om anmälan och identifiering tidigast kunna träda i kraft den 15 januari 2026.

Det anges vidare att de som kommer att omfattas av regleringen består av både verksamhetsutövare som tidigare omfattats av NIS-direktivets regler och verksamhetsutövare

som inte har någon tidigare erfarenhet av den typen av reglering. MSB bedömer att det finns behov av att, i samverkan med berörda tillsynsmyndigheter, genomföra särskilda informationsinsatser inför och i samband med att regleringen börjar gälla för att säkerställa att verksamhetsutövarna ges möjlighet att få en god bild av både sina skyldigheter och rättigheter. Det anges också vara angeläget att det finns tillgång till relevant stöd i form av vägledningar och tekniska system i samband med att föreskrifterna börjar gälla samt att verksamhetsutövarna ges kunskap om dessa. Vid utformningen av informationsinsatserna anges hänsyn behöva tas till om mottagarna sedan tidigare omfattas av lagen om informationssäkerhet i samhällsviktiga tjänster eller inte. Det anges vidare att MSB har påbörjat arbetet med att ta fram en vägledning som stöd för organisationernas bedömning om de omfattas eller inte.

Regelrådet bedömer redovisningen godtagbar.

Hur och när konsekvenserna kan utvärderas

Det anges att en första uppföljning kommer att ske så snart det är möjligt att utvärdera reglernas effekter och därefter regelbundet. Har de grundläggande förutsättningarna för regleringen ändrats kommer reglerna att omprövas och en ny konsekvensutredning göras.

Regelrådet gör följande bedömning. Beskrivningen av hur och när konsekvenserna av förslaget kan utvärderas är alltför vag. I lagrådsremissen anges att en utvärdering av konsekvenserna för företagen bör ske tre år efter den nya lagens ikraftträdande och att en översyn av författningarna kopplade till genomförandet av NIS 2-direktivet bör ske i samband med detta. Förslagsställaren borde ha förhållit sig till denna tidpunkt i sin redovisning, samt presenterat ett något mer detaljerat förslag på hur utvärderingen kan ske.

Regelrådet bedömer redovisningen bristfällig.

Överensstämmelse med EU-rätten och om förslaget går utöver minimikraven

Förslagsställaren anger att förslaget bedöms överensstämma med de skyldigheter som följer av Sveriges anslutning till Europeiska unionen. Konsekvensutredningen innehåller relativt utförliga beskrivningar av EU-direktivet och det nationella handlingsutrymmet, inklusive motivering till när man går utöver minimikraven, i förslaget till genomförande i de nu aktuella delarna.

Regelrådet bedömer redovisningen godtagbar.

Övrigt som Regelrådet vill framföra

Det nya NIS2-regelverket kan i sin helhet förväntas få betydande konsekvenser för företag. Regelrådet noterar att regeringen i sin lagrådsremiss (Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag) efter remissinstansernas, inklusive Regelrådets, synpunkter på brister i konsekvensutredningen i tidigare nämnda utredning, kompletterat med en del kostnadsuppskattningar, bland annat från utredningar genomförda i Finland och Danmark. Regelrådet ser positivt på detta och vill uppmuntra till mer detaljerade kostnadsuppskattningar och annan påverkan på berörda svenska företag i anslutning till kommande författningsförslag. Kommande analyser bör avse såväl konsekvenser av enskilda författningskrav som på aggregerad nivå vad avser företagspåverkan av det nya regelverket i sin helhet. Regelrådet noterar exempelvis att lagrådsremissen anger att det danska lagförslaget beräknas få negativa ekonomiska konsekvenser för ca 3 255 företag i Danmark

och att de administrativa kostnaderna uppskattas uppgå till 3,3 miljarder DKK i engångskostnader och 0,7–1,2 miljarder DKK årligen i löpande utgifter. Regelrådet noterar även att regeringen i lagrådsremissen bedömer att den största kostnaden för enskilda hänförs till de säkerhetsåtgärder som ska vidtas enligt den nya lagen. Det är därför av stor vikt att dessa kostnader uppskattas samt följs upp i kommande processer.

Regelrådet behandlade ärendet vid sammanträde den 4 november 2025.

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

Ärendet föredrogs av Anna Stattin.



Anna-Lena Bohm
Ordförande



Anna Stattin
Föredragande