Regelrådet

Beslutsdatum 2026-05-13
Vårt diarienummer RR 2026-83
Ert diarienummer Fö2026/00576

Regelrådets uppgift är att granska och yttra sig över kvaliteten på konsekvensutredningar till författningsförslag som kan få effekter av betydelse för företag.

Försvarsdepartementet

Yttrande över Europeiska kommissionens cybersäkerhetspaket med förslag till ändringar i cybersäkerhetsakten och NIS 2-direktivet

Regelrådet har beretts möjlighet att yttra sig över rubricerade förslag. Regelrådet har i uppgift att bistå regelgivare, om dessa begär det, med att granska konsekvensutredningar till förslag från Europeiska unionen som bedöms få stor påverkan för företag i Sverige och lämna råd om vad en svensk konsekvensutredning bör innehålla. Regelrådet har därför översiktligt granskat EU-kommissionens konsekvensutredning, SWD (2026) 11, liksom själva författningsförslagen, COM (2026) 11 och COM (2026) 13 och Regeringskansliets faktapromemoria 2025/26:FPM78.

EU-kommissionens motivering till och syfte med förslaget

Kommissionen anger att sedan cybersäkerhetsakten antogs 2019 har hotbilden på cybersäkerhetsområdet utvecklats avsevärt i en alltmer komplex geopolitisk verklighet. Antalet cyberattacker har ökat och de har blivit mer sofistikerade och inriktade på kritisk infrastruktur, företag och allmänheten, med utpressningsprogram som ett centralt inslag. Statliga fientliga aktörer utnyttjar ny teknik såsom artificiell intelligens (AI) för att ytterligare skala upp och optimera sina attacker. EU:s cybersäkerhetslandskap står inför betydande utmaningar i en situation med alltmer komplexa hot. Otillräcklig samordning mellan medlemsstaterna och andra aktörer på EU-nivå, rättsliga hinder och komplicerade regelverk står i vägen för en effektiv hantering av cybersäkerheten och leder till ökade kostnader för företag och myndigheter, större risker för cyberincidenter och lägre skyddsnivåer för medborgarna.

De föreslagna ändringarna i cybersäkerhetsakten rör bland annat utökade uppgifter och mandat för EU:s cybersäkerhetsbyrå, ENISA, och ramverket för cybersäkerhetscertifiering. Det föreslås nya regler för säkerhet i leveranskedjor för informations- och kommunikationsteknik (IKT) som syftar till att harmonisera och stärka EU:s arbete med detta.

Ändringar i NIS 2-direktivet anges syfta till att anpassa detta till ändringarna i cybersäkerhetsakten samt att förenkla efterlevnaden och minska regelbördan för framför allt mindre företag. Exempelvis föreslås små företag som är leverantörer av domännamnsystem-(DNS-)tjänster undantas från tillämpningsområdet. Det införs en ny kategori mindre företag (small midcaps) som föreslås omfattas av färre krav än i dag. Det föreslås även harmoniserad uppgiftslämning avseende attacker med utpressningsprogram. Förslaget innebär även att tillämpningsområdet utökas med nya aktörer såsom leverantörer av europeiska företagsplånböcker, operatörer av undervattensinfrastruktur för elektronisk kommunikation, tillhandahållare av elektroniska kommunikationsnät och entiteter som ansvarar för strategisk infrastruktur med både civil och militär användning.

Konsekvenser för företag

Kommissionen anger i sin konsekvensutredning bland annat att utfasningen av specifik högriskutrustning under en övergångsperiod på tre år uppskattas leda till årliga kostnader på 3,4–4,3 miljarder EUR för mobilnätsoperatörer, medan investeringarna i betrodda leverantörer samtidigt kan öka med upp till 2 miljarder EUR per år. Förenklade och minskade efterlevnadskraven uppskattas innebära kostnadsbesparingar för företagen på upp till 14,6 miljarder EUR. Vidare anges företag komma att åtnjuta fördelar i form av en förbättring av EU:s övergripande cybersäkerhetsstatus och tekniska suveränitet och främja innovation och konkurrenskraft.

Regelrådets bedömning

Kommissionen presenterar i sin konsekvensutredning beräkningar och effekter på aggregerad nivå. Regelrådet rekommenderar därför att regeringen upprättar en preliminär kompletterande nationell konsekvensutredning som innehåller en kartläggning och analys av den svenska marknaden, inklusive antal berörda företag och möjliga konsekvenser av förslagen för svenska företag. Regelrådet rekommenderar en granskning och anpassning av kommissionens siffror till en svensk kontext. Analysen bör innehålla exempelberäkningar av kostnader för olika typer av företag, inklusive för små och stora företag och en rimlighetsbedömning av de kostnadsbesparingar som förekommer i kommissionens utredning. Det är vidare relevant att, inför förhandlingarna, i en nationell konsekvensutredning även granska kommissionens redovisningar av effekter för de olika policyalternativen.

Regelrådet noterar att det i faktapromemorian anges att förslagen förhandlas under våren och att åtminstone förhandlingarna om Enisas mandat enligt förslaget till cybersäkerhetsakt även förväntas avslutas under våren. Att deadline för remissvar är den 18 maj reser därför vissa frågor. Regelrådet anser generellt att förhandlingar i rådet bör inledas först när medlemsstaterna har haft tillräckligt med tid för nationella samråd och analyser.

Regelrådet behandlade ärendet vid sammanträde den 13 maj 2026.

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

Postadress
Box 4044, 102 61 Stockholm

Webbplats
www.regelradet.se

E-post
regelradet@regelradet.se