Innovationsföretagen

Datum
2026-05-18

Vår ref:
Anders Persson

Er ref:
Fö2026/00576

Försvarsdepartementet

fo.remissvar@regeringskansliet.se

Kopia till
fo.ech.remissvar@regeringskansliet.se

Innovationsföretagens remissvar ”Europeiska kommissionens cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS 2-direktivet (EU 2022/2555)”, KOM (2026) 11 och 13

Innovationsföretagen tackar för möjligheten att lämna remissyttrande på ovan nämnda remiss.

Innovationsföretagen samlar drygt 880 företag med över 45 000 medarbetare inom den kunskapsintensiva tjänstesektorn, med fokus på ingenjörs- och arkitektkunnande.

Innovationsföretagen välkomnar ambitionen att stärka Europas cybersäkerhet, minska fragmenteringen inom den inre marknaden och förenkla regelefterlevnaden. Ett mer sammanhållet, förutsebart och praktiskt användbart regelverk kan bidra till såväl ökad säkerhet som stärkt konkurrenskraft.

Samtidigt är det avgörande att nya regler utformas så att de blir genomförbara och proportionerliga för kunskapsintensiva tjänsteföretag. För Innovationsföretagens medlemsföretag är det särskilt viktigt att regelverket fungerar i projektbaserade verksamheter, att administrativa bördor inte byggs på i flera led och att krav på certifiering, leverantörsstyrning och upphandling inte utvecklas till oproportionerliga marknadstillträdeshinder. Samtidigt finns situationer där oberoende tredjepartskontroll är motiverad, särskilt vid hög risk eller där likvärdiga konkurrensvillkor behöver säkerställas.

Mot denna bakgrund är Innovationsföretagen i huvudsak positiv till paketets inriktning, men vill särskilt framhålla följande.

Innovationsföretagens synpunkter i korthet

- Förenklingsambitionen är välkommen, men måste leda till faktisk förenkling i företagens vardag och inte resultera i nya parallella dokumentations- och rapporteringskrav.
- Krav måste utformas tydligt riskbaserat och proportionerligt, särskilt för små och medelstora företag samt för projekt- och konsultverksamheter som inte själva driver eller förvaltar samhällskritisk digital infrastruktur.
- Certifiering kan vara ett användbart verktyg för att visa regelefterlevnad och skapa tydlighet på den inre marknaden, men bör inte i praktiken utvecklas till ett generellt marknadstillträdeskrav i upphandling eller i leverantörsled. Oberoende tredjepartscertifiering bör användas där risknivån eller behovet av likvärdiga marknadsvillkor motiverar det.

- Det är positivt att kommissionen vill motverka att NIS 2-krav förs vidare oskäligt till leverantörer utanför direktivets kärna. Denna avgränsning behöver bli tydlig, rättssäker och användbar i praktiken.
- Åtgärder kopplade till ICT supply chains, key ICT assets och high-risk suppliers måste bygga på transparens, rättssäkerhet, konsekvensanalys, tillgång till alternativ och rimliga övergångsperioder.
- Cybersäkerhetskrav i offentlig upphandling måste utformas så att de stärker säkerheten utan att i onödan minska konkurrensen eller stänga ute kvalificerade leverantörer.

Inledning

Cybersäkerhet har blivit en allt viktigare del av Europas motståndskraft, konkurrenskraft och ekonomiska säkerhet. Det finns därför goda skäl att stärka det gemensamma regelverket och att förbättra samordningen mellan medlemsstaterna. Samtidigt måste nya regler utformas med stor precision. Ett regelverk som syftar till att minska fragmentering och förenkla efterlevnad får inte i praktiken leda till motsatsen för företag som verkar i komplexa uppdrags- och leverantörsrelationer.

För Innovationsföretagens medlemsföretag är denna fråga viktig av flera skäl. Många verkar som specialiserade leverantörer i längre värdekedjor, ofta i projekt där flera aktörer samverkar och där uppdragens art, risknivå och ansvarsfördelning varierar betydligt. Medlemsföretagen säljer i stor utsträckning kunskap, analys, projektering, systemlösningar och rådgivning snarare än standardiserade produkter eller egen drift av kritisk digital infrastruktur. Därför måste även kontrollformer, certifieringskrav och leverantörsvillkor utformas med hänsyn till faktisk risk och till hur verksamheten fungerar i praktiken.

Innovationsföretagen stödjer därför huvudinriktningen i paketet, men vill understryka vikten av proportionalitet, rättssäkerhet, praktisk användbarhet och konkurrensneutralitet.

Förenkling och harmonisering måste ge verklig effekt

Innovationsföretagen välkomnar att kommissionen lyfter fram behovet av att minska komplexitet, förbättra samordning och göra regelefterlevnaden mer hanterbar för företag. I förslagen anges uttryckligen att dagens ordning präglas av splittrade krav, begränsad överblick och onödig administrativ belastning, och att certifiering och samordning ska kunna användas för att minska dessa problem.

Detta är en viktig ansats. För innovationssektorns företag är det dock avgörande att förenklingsambitionen också får genomslag i praktiken. Om nya certifieringsordningar, rapporteringsstrukturer, leverantörskrav och upphandlingskrav läggs ovanpå redan existerande krav, utan verklig samordning, riskerar resultatet att bli ökad komplexitet snarare än minskad.

Sverige bör därför i det fortsatta förhandlingsarbetet verka för att paketets förenklingsambition omsätts i konkret regelförenkling. Nya krav bör samordnas med befintliga skyldigheter, utformas med tydlig ansvarsfördelning och så långt möjligt undvika parallella dokumentations- eller rapporteringsspår för samma risk eller samma verksamhet.

Proportionalitet för små och medelstora företag samt projektbaserade tjänsteverksamheter

Innovationsföretagen vill särskilt understryka att de nya reglerna måste utformas tydligt riskbaserat och proportionerligt. Detta är särskilt viktigt för små och medelstora företag samt för konsult- och projektverksamheter som inte själva driver eller förvaltar samhällskritisk digital infrastruktur, men som ändå kan påverkas indirekt genom avtal, upphandlingar eller krav i leverantörsled.

För innovationssektorns företag är det ofta stor skillnad mellan att leverera kvalificerade tekniska eller digitala tjänster inom ramen för ett projekt och att bära ett direkt operativt ansvar för samhällskritiska system. Regelverket måste därför kunna skilja mellan olika typer av aktörer, olika nivåer av ansvar och olika riskprofiler.

Proportionalitet handlar inte bara om vilka krav som ställs, utan också om hur efterlevnaden ska verifieras. Där riskerna är begränsade bör enklare former av verifiering eller egenförsäkran kunna vara tillräckliga, medan oberoende tredjepartsgranskning bör reserveras för situationer där riskbilden eller marknadsförhållandena motiverar detta.

Certifiering som verktyg för regelefterlevnad

Innovationsföretagen ser positivt på att certifiering kan användas som ett verktyg för att underlätta regelefterlevnad och skapa ökad tydlighet mellan medlemsstaterna. Rätt utformad kan certifiering minska dubbelarbete, stärka förutsebarheten och underlätta gränsöverskridande verksamhet.

Samtidigt vill Innovationsföretagen framhålla att certifiering inte bör utvecklas till ett generellt eller indirekt obligatorium för aktörer där riskbilden inte motiverar detta. För mindre företag och konsultverksamheter är det särskilt viktigt att såväl krav som kontrollformer anpassas till faktisk risk. I annat fall finns en påtaglig risk att kostnader för certifiering, uppföljning och återkommande bedömningar blir betydande utan motsvarande säkerhetsnytta. Det får aldrig uppfattas som ett verktyg som blir konkurrens- eller affärshindrande för små- och mellanstora företag på den inre marknaden. Detta gäller särskilt om stora beställare eller upphandlande myndigheter i praktiken börjar använda certifikat som standardkrav oavsett uppdragets art, vilket kan minska konkurrensen och försvåra för mindre och specialiserade aktörer att delta på marknaden. Krav om cybersäkerhetscertifiering måste utformas proportionerligt och får enbart ställas om det är nödvändigt med hänsyn till föremålet för upphandlingen.

Regeringen bör därför verka för att certifieringsordningar utformas riskbaserat, proportionerligt och praktiskt användbart, samt så att de faktiskt minskar den samlade administrativa bördan. Innovationsföretagen anser samtidigt att oberoende tredjepartscertifiering bör användas där risknivån eller behovet av likvärdiga marknadsvillkor motiverar det, inte minst för att stärka tillit, jämförbarhet och konkurrensneutralitet. Förslagen om ett reformerat europeiskt certifieringsramverk och möjligheten att utveckla certifiering som stöd för efterlevnad gör denna avvägning särskilt viktig.

Krav i leverantörsledet får inte vältras över oskäligt

Innovationsföretagen ser positivt på att kommissionen uppmärksammar risken för att NIS 2-relaterade krav förs vidare oskäligt till leverantörer utanför direktivets kärna. Denna fråga är av stor praktisk betydelse för medlemsföretagen, eftersom många verkar som specialiserade leverantörer i längre avtals- och projektkedjor där större beställare ofta har ett starkt förhandlingsläge.

Det är viktigt att cybersäkerhetskrav i leverantörsledet utformas så att de speglar faktisk risk, relevant ansvar och uppdragets art. Om krav förs vidare slentrianmässigt eller utan tydlig koppling till leverantörens faktiska roll riskerar detta att skapa övervältring av ansvar, ökade kostnader och sämre konkurrensförutsättningar, utan motsvarande säkerhetsnytta.

Sverige bör därför verka för att avgränsningen av vilka krav som får föras vidare i leverantörsledet blir tydlig och praktiskt användbar. Det bör också framgå att större aktörer inte rutinmässigt ska kunna använda regelverket som grund för att överföra allmänna, otydliga eller oproportionerliga cybersäkerhetskrav nedåt i kedjan. I den delen ligger förslagens inriktning nära Innovationsföretagens bredare syn på balanserade och fungerande avtalsvillkor i näringslivet.

ICT supply chains, key ICT assets och high-risk suppliers

Innovationsföretagen delar uppfattningen att säkerheten i kritiska ICT-leveranskedjor behöver stärkas och att beroenden som skapar verklig sårbarhet måste kunna hanteras. Samtidigt är de föreslagna verktygen långtgående och kan få betydande konsekvenser för marknadstillträde, upphandling, investeringar och leverantörsrelationer.

Förslag som rör key ICT assets, high-risk suppliers och möjliga restriktioner eller exkluderingar måste därför bygga på tydliga kriterier, öppna processer, väl underbyggda konsekvensanalyser och rimliga övergångsperioder. Det måste också finnas ett tydligt fokus på om det faktiskt finns fungerande alternativ på marknaden, så att inte reglerna i praktiken leder till leveransproblem, ökade kostnader eller förseningar i projekt utan tillräckligt tydlig säkerhetsnytta.

Innovationsföretagen vill även framhålla vikten av rättssäkerhet och förutsebarhet i processer som kan få långtgående marknadseffekter. När regler kopplas till exkludering, restriktioner eller särskilda krav i upphandling och leverantörsled måste det vara tydligt på vilka grunder detta sker, hur beslut fattas och vilka övergångsmekanismer som gäller. Förslagen på detta område är centrala i CSA 2 och måste därför hanteras med särskild omsorg i förhandlingarna.

Offentlig upphandling

Krav på cybersäkerhetscertifiering i offentlig upphandling måste utformas så att de stärker säkerheten utan att i onödan minska konkurrensen eller stänga ute kvalificerade eller mindre leverantörer. För Innovationsföretagens medlemsföretag är detta en mycket viktig fråga, eftersom våra medlemsföretag deltar i offentliga upphandlingar som konsulter, teknikleverantörer eller underkonsulter i större projekt.

Det är legitimt att upphandlande myndigheter ställer relevanta cybersäkerhetskrav där riskbilden motiverar det. Samtidigt finns en risk att krav på certifiering, dokumentation eller leverantörsbedömningar standardiseras på ett sätt som inte står i proportion till uppdragets art. Det kan slå särskilt hårt mot mindre och specialiserade aktörer, trots att dessa ofta tillför hög kompetens, innovation och kvalitet.

Sverige bör därför verka för att cybersäkerhetskrav i upphandling utformas med tydlig koppling till faktisk risk, säkerhetsnytta och uppdragets innehåll. Oberoende tredjepartscertifiering kan i vissa upphandlingar vara motiverad för att säkerställa likvärdig prövning och konkurrens på rättvisa villkor, men bör inte användas som ett generellt standardkrav utan närmare riskbedömning.

ENISA:s roll och tillsyn över gränsöverskridande aktörer

Innovationsföretagen ser positivt på att ENISA ges en tydligare roll i att stödja genomförande, samordning och praktisk användbarhet i regelverket. Ett starkare och mer samordnande stöd på EU-nivå kan vara värdefullt, särskilt om det bidrar till mer enhetliga tillämpningar mellan medlemsstaterna och bättre stöd till företag i tolkning och efterlevnad.

Samtidigt är det viktigt att denna förstärkning av ENISA:s roll medför ett ökat samarbete med näringslivet och inte leder till otydlighet i ansvarsfördelningen mellan EU-nivå, nationella myndigheter och sektorsansvariga organ. För företag behöver det vara klart vem som ansvarar för vägledning, tillsyn, uppföljning och praktiska kontakter. Ett förenklat regelverk förutsätter också en tydlig och begriplig myndighetsstruktur.

Avslutning

Innovationsföretagen stödjer ambitionen att stärka cybersäkerheten i EU samt att skapa ett mer sammanhållet, effektivt och mindre fragmenterat regelverk. Förslagen har potential att bidra till såväl ökad säkerhet som stärkt konkurrenskraft, under förutsättning att de utformas proportionerligt, rättssäkert och med beaktande av hur kunskapsintensiva tjänste- och projektverksamheter fungerar i praktiken.

Innovationsföretagen vill samtidigt framhålla att krav på certifiering och verifiering måste utformas riskbaserat, proportionerligt och konkurrensneutralt. Oberoende tredjepartskontroll fyller en viktig funktion där risknivån är hög eller där den behövs för att säkerställa likvärdiga marknadsvillkor, men bör inte utvecklas till ett generellt standardkrav utan tydlig koppling till faktisk risk och säkerhetsnytta.

I det fortsatta förhandlingsarbetet bör Sverige särskilt verka för att förenklingsambitionen får ett reellt genomslag, att krav i leverantörsledet inte vältras över oskäligt på aktörer utanför regelverkets kärna, att certifiering inte utvecklas till oproportionerliga inträdeshinder samt att regler om ICT supply chains och high-risk suppliers präglas av transparens, rättssäkerhet och rimliga övergångsperioder.

Innovationsföretagen står gärna till förfogande för fortsatt dialog.

18 maj 2026

INNOVATIONSFÖRETAGEN

Anders Persson

Director of Strategic Development and International Affairs