

Datum

2026-10-02

Finansdepartementet

Inskickat till:fi.remissvar@regeringskansliet.se**Kopia till:**fi.ofa.dis.remisser@regeringskansliet.se**Handläggare**

Sofia Donner

sofia.donner@teliacompany.com**Ert diarienummer**

Fi2026/01676

Remissvar över Europeiska kommissionens förslag till förordning om utveckling av moln och AI, COM(2026) 502 final

1. Sammanfattning av Telias huvudsakliga synpunkter

Telia Sverige AB (Telia) har beretts tillfälle att yttra sig över Europeiska kommissionens förslag till Europaparlamentets och rådets förordning om inrättande av en ram med åtgärder för att stärka Europas moln- och AI-ekosystem, den så kallade Cloud and AI Development Act (CADA).

Telia delar förslaget övergripande mål att stärka Europas konkurrenskraft, innovationsförmåga och motståndskraft samt att öka tillgången till säker, hållbar och konkurrenskraftig moln- och AI-infrastruktur.

Telia anser emellertid att flera centrala bestämmelser behöver preciseras och avgränsas för att kraven ska bli förutsebara, proportionerliga och tekniskt genomförbara. Telia utvecklar sin syn i denna del nedan.

Telia anser att Sverige i de fortsatta förhandlingarna bör verka för att

- unionsassuransnivåerna uttryckligen tillämpas på en specifik molntjänst och inte på leverantören,
- kravet på state of the art preciseras genom objektiva, riskbaserade och verifierbara kriterier samt presumptioner för erkända standarder, certifieringar och likvärdiga kontrollramverk,
- leverantörens ansvar för underleverantörer begränsas till direkt anlitade och andra materiellt kritiska leverantörer som leverantören rimligen kan identifiera, påverka och kontrollera,
- kodgranskning endast krävs när den är riskmässigt motiverad och rättsligt samt praktiskt möjlig, samt att likvärdiga compliance-mekanismer uttryckligen godtas,
- befintliga granskningar, certifieringar och dokumentationskrav enligt andra unionsrättsliga regelverk ska kunna återanvändas,
- materiella ändringar av kraven i bilagorna inte ska kunna genomföras utan samråd och tillräckliga övergångsperioder,
- varje utvidgning av skyldigheterna till privata verksamhetsutövare enligt artikel 31 beslutas i grundakten eller genom ordinarie lagstiftningsförfarande, och
- krav vid offentlig upphandling begränsas till vad som är proportionerligt utifrån den berörda verksamhetens och informationens faktiska skyddsbehov.

2. Tillämpningsområdet måste avgränsas till den granskade tjänsten

Artikel 16 anger att molntjänstleverantörer ska uppfylla kriterierna i bilaga II för att tillhandahålla sina molntjänster till unionsorgan och offentliga organ. Bilaga II anger samtidigt att kriterierna ska uppfyllas av både "cloud computing service providers" och deras molntjänster. I andra bestämmelser används däremot uttryck som "audited service", och bilaga III knyter bevisningen till de komponenter, resurser och dataflöden som används för den granskade tjänsten. Ordalydelsen ger därför inte ett entydigt svar på om kraven gäller tjänsten, den organisatoriska enhet som tillhandahåller tjänsten eller hela den juridiska personen.

Denna oklarhet är särskilt problematisk för en aktör som bedriver blandad verksamhet där molntjänsterna är en del av den tillhandahållna portföljen. Infrastruktur, personalsystem, nätverksfunktioner, inköp och säkerhetsprocesser kan vara gemensamma för flera verksamheter, samtidigt som endast vissa avgränsade resurser används för den molntjänst som ska erkännas. En tolkning som omfattar hela företaget skulle kunna föra in elektroniska kommunikationsnät, stödsystem och leverantörer utan relevant koppling till den granskade tjänsten i assurancesbedömningen. Detta skulle gå utöver det tjänstespecifika syfte som framgår av reglerna om erkännande och granskning och motverka en proportionerlig tillämpning.

Telia föreslår därför att artikel 16 kompletteras med en bestämmelse som tydliggör detta. I sammanhanget är det viktigt att framföra att gemensamma företagsfunktioner bör få granskas endast i den utsträckning de faktiskt styr eller påverkar den aktuella tjänsten. En leverantör bör dessutom kunna certifiera separata tjänstevarianter, regioner eller särskilt avskilda miljöer utan att samma krav automatiskt utsträcks till företagets övriga erbjudanden.

3. Kravet på "state of the art" behöver göras förutsebart och riskbaserat

För assurancesnivå 1 kräver bilaga II punkt 1.1 (e) att leverantören visar att tjänsten uppfyller "state-of-the-art cybersecurity standards". Begreppet är dynamiskt och kan fylla en viktig funktion genom att regelverket inte låses till viss teknik. I nuvarande lydelse saknas emellertid kriterier för vilka standarder som avses, vid vilken tidpunkt bedömningen ska göras, hur snabbt en tjänst måste anpassas till teknisk utveckling och hur kostnader och riskreduktion ska vägas mot varandra.

Som jämförelse föreskriver artikel 21.1 NIS2-direktivet att hänsyn ska tas till relevanta europeiska och internationella standarder och genomförandekostnaden samt att åtgärderna ska vara proportionerliga i förhållande till exponering, storlek, sannolikhet och incidenternas samhällsrelaterade och ekonomiska konsekvenser. NIS2 tillhandahåller därmed en betydligt tydligare rättslig proportionalitetsram än den som nu återfinns i CADA:s bilaga II. Telia föreslår därför att motsvarande kriterier införs i CADA.

Europeiska cybersäkerhetscertifieringar bygger redan på en formell bedömning mot definierade kriterier och assurancesnivåer. EUCS för molntjänster är fortfarande under utveckling, medan EUCC gäller produkter. CADA bör därför inte förutsätta att en viss certifiering alltid finns tillgänglig för den aktuella tjänsten, utan ge möjlighet att kombinera certifikat, standarder och annat verifierbart stöd för bedömningen.

4. Ansvar för underleverantörer och leverantörskedjor

Bilaga II kräver bland annat full transparens om underleverantörer, due diligence, avtalsvillkor och löpande kontroll. För högre assurancesnivåer tillkommer krav på etableringsort, kontroll, support, personal, programvaruberoenden och möjligheten att motstå tredjelandsinflytande. Bilaga III kräver dessutom uppgifter om bland annat leverantörernas identitet, ägar- och kontrollstruktur, tjänster, personal, dataåtkomst och säkerhetsarrangemang.

Förslaget anger på vissa ställen att kraven avser underleverantörer som är direkt avtalsbundna till molntjänstleverantören. Samtidigt används uttryck som "subsequent sub-outsourcing arrangements", "dependencies" och hela programvarutillverkar- och undertillverkarkedjan. Det är därför oklart hur långt ansvaret sträcker sig och om leverantören förväntas garantera förhållanden i flera led där den saknar direkt avtalsrelation och faktisk möjlighet att erhålla information eller revisionsrätt. Telia anser därmed att ansvaret behöver tydliggöras.

5. Assurancesnivå 2 och kraven på kodgranskning

Bilaga II punkt 2.1(i) ii. kräver för vissa programvarukomponenter från tredjelandslieferantörer bland annat kontroller mot fjärrfunktioner, säkerhetsgranskning av säkerhetsrelevanta komponenters källkod och en migrationsplan. Bilaga III, granskningskriterium I, kräver att en oberoende granskare kan få tillgång till och granska den relevanta källkoden samt tillhörande dokumentation.

Bilaga II anger visserligen att hårdvara enligt artikel 3.5 cyberresiliensförordningen ligger utanför bilagans tillämpningsområde medan programvara omfattas. Bilaga III kräver emellertid ändrings- och underhållskontroller som uttryckligen omfattar firmware och BIOS. Det är därför inte klart om kraven kan omfatta firmware eller mikrokod i exempelvis lagringsenheter, controllers, nätverkskort och andra hårdvarukomponenter som molntjänstleverantören inte utvecklar och normalt inte har tillgång till i källkodsform.

En skyldighet att säkerställa tillgång till all sådan kod kan i praktiken göra etablerad standardutrustning och kommersiell programvara oanvändbar, även när komponenten är certifierad, signerad, uppdaterad och föremål för oberoende leverantörsgranskning. Den kan även minska säkerheten om revisioner dupliceras utan tydlig riskprioritering eller om känslig källkod behöver spridas till ytterligare aktörer.

Cyberresiliensförordningen använder i stället en riskbaserad due diligence-modell för integrerade tredjepartskomponenter och nämner bland annat kontroll av CE-märkning, säkerhetsuppdateringar, kända sårbarheter och kompletterande säkerhetstester.

Telia anser mot denna bakgrund att kodgranskningskraven ersätts med ett funktions- och riskbaserat resultatkrav. Direkt källkodsgranskning bör krävas endast för säkerhetskritisk programvara som leverantören själv utvecklar eller över vilken leverantören har faktisk och rättslig kontroll. För proprietär tredjepartsprogramvara, firmware och mikrokod bör andra erkända mekanismer kunna godtas.

Kraven bör uttryckligen begränsas till komponenter som är relevanta för den granskade tjänstens säkerhet eller kontinuitet och inte omfatta kod som leverantören saknar rättslig eller faktisk möjlighet att anskaffa. En SBOM bör vara ett medel för insyn och sårbarhetshantering, inte en presumtion för att leverantören har kontroll över eller revisionsrätt till samtliga komponenters källkod. Cyberresiliensförordningen definierar

SBOM som en formell förteckning över komponenter och deras leveranskedjereationer, vilket är förenligt med en sådan avgränsning.

6. Samspel med befintlig unionsrätt

CADA kommer att tillämpas parallellt med bland annat NIS2, cyberresiliensförordningen, cybersäkerhetsakten, AI-förordningen och dataskyddsregleringen. Befintliga dataflödeskartläggningar, personuppgiftsbiträdesavtal, konsekvensbedömningar, NIS2-underlag, produktdokumentation och certifieringar bör därför kunna återanvändas.

Telia föreslår en uttrycklig "once-only"-princip: samma sakförhållande eller kontroll ska inte behöva granskas på nytt om det redan har bedömts av en behörig eller ackrediterad aktör enligt ett unionsrättsligt krav och underlaget fortfarande är relevant. Telia anser vidare att tillsynsmyndigheter bör samordna informationsinhämtning, granskning och sanktioner. Detta är särskilt viktigt eftersom artikel 24 överlåter åt medlemsstaterna att fastställa effektiva, proportionerliga och avskräckande sanktioner utan att närmare lösa risken för parallella förfaranden avseende samma faktiska omständigheter.

7. Ytterligare bestämmelser av materiell betydelse

7.1. Ändringar genom delegerade akter

Artikel 16.2 ger kommissionen befogenhet att ändra assurancesnivåerna i bilaga II och beviskraven i bilaga III genom delegerade akter, och bilagorna ska ses över minst var artonde månad. Kriterierna avgör i praktiken marknadstillträdet till offentlig upphandling och kan kräva betydande förändringar av teknik, organisation och leverantörsavtal.

Väsentliga krav bör enligt Telia därför fastställas i grundakten. Tekniska uppdateringar genom delegerade akter bör begränsas av tydliga mål och principer och föregås av konsekvensanalys, öppet samråd och bedömning av tillgängliga standarder och marknadslösningar. Materiella ändringar bör omfattas av en tillräcklig övergångsperiod och tjänster som redan erkänts bör som huvudregel få behålla erkännandet till nästa ordinarie förnyelse.

7.2. Offentlig upphandling

Artikel 30 innebär att all offentlig upphandling av molntjänster som huvudregel ska uppfylla minst assurancesnivå 1, medan verksamhet med betydelse för allmän ordning ska använda nivå 2–4. Undantag kan medges bland annat om det saknas lämpliga tjänster eller om kostnaden blir oproportionerlig. Kommissionens eget underlag utgår från att olika användningsfall ska mötas av olika nivåer, men den generella miniminivån riskerar ändå att bli oproportionerlig för standardiserade och lågriskbetonade tjänster.

Telia anser att även nivå 1 bör knytas till en dokumenterad riskbedömning, alternativt att likvärdiga säkerhets- och suveränitetskontroller får godtas för lågriskanvändning. Undantagen måste vara transparenta men får inte utformas så att myndigheter tvingas genomföra kostsamma migrationer innan konkurrenskraftiga alternativ faktiskt finns. Tilldelningskriterierna i artikel 32 bör vara objektiva, kontraktsanknutna och teknikneutrala samt premiera säkerhet, resiliens, interoperabilitet, portabilitet, hållbarhet och innovation snarare än enbart utvecklings- eller tillverkningsort.

7.3. Datacenter och öppen källkod

Telia välkomnar åtgärderna i artiklarna 10–15 om samordnade kontaktpunkter och effektivare tillståndprocesser.

Telia stödjer även återanvändning av offentligfinansierad programvara och öppna standarder när detta är ändamålsenligt. Artiklarna 41–44 bör dock inte medföra en generell preferens för öppen källkod eller krav på utlämnande av proprietär kod. Bedömningen måste även omfatta underhåll, ansvar, kompetens, sårbarhetshantering och långsiktig kontinuitet.

8. Avslutande synpunkter

Telia tillstyrker CADA:s övergripande inriktning. Sverige bör dock verka för ett tjänstespecifikt, riskbaserat och teknikneutralt ramverk, med möjlighet att använda certifieringar, tredjepartsassurance och andra likvärdiga kontroller. Det är en förutsättning för att CADA ska kunna stärka Europas säkerhet, innovationsförmåga och konkurrenskraft utan att skapa oproportionerliga hinder för europeiska leverantörer.

Solna som ovan

Sofia Donner
Enhetschef och bolagsjurist