Stockholm 2026-08-05

Finansdepartementet

Er referens: Fi2026/01676

Vår referens: 26-028

Netnod fick från Finansdepartementet möjlighet att komma med synpunkter på *Europeiska kommissionens förslag till förordning om utveckling av moln och AI KOM(2026)502*.

Netnod är operatör av Sveriges största internetknutpunkter (IXP) och driver kritisk DNS-infrastruktur för Sverige och delar av norra Europa, inklusive en av världens tretton rotnamnservrar (i-root). Netnod ansvarar även för tillhandahållande av tids- och frekvenssignaler i Sverige — en tjänst som utgör ett grundläggande beroende för elektroniska kommunikationsnät, finansiella transaktioner, elnätsstyrning och en lång rad andra samhällskritiska system. Netnod är verksam på det infrastrukturlager som utgör grunden för alla molntjänster — det lager som gör att molntjänster faktiskt är nåbara, tidsstämplade och synkroniserade. Det ger Netnod en specifik och praktisk erfarenhet av de beroende- och motståndskraftsfrågor som förordningen adresserar, och en direkt insikt om vad som saknas i dess nuvarande utformning.

Netnod välkomnar kommissionens ambition att stärka Europas motståndskraft och skapa en konkurrenskraftig marknad för moln- och AI-tjänster — särskilt SBOM-kraven i Bilaga II och öppen källkod-bestämmelserna i artiklarna 43–44.

Netnods huvudsakliga invändning är att förslaget i alltför hög grad fokuserar på **egenskaper hos leverantörer** — framför allt var de är etablerade och vem som kontrollerar dem (tillitsnivåer) — snarare än på den **förmåga** som organisationer behöver för att upprätthålla sina kritiska funktioner. Unionen har redan förmåge- och riskbaserade instrument för detta: NIS2-direktivet (direktiv (EU) 2022/2555) och CER-direktivet (direktiv (EU) 2022/2557).

Netnod anser att förordningen bör bygga vidare på deras funktionslogik i stället för att lägga en parallell, ursprungsbaserad regim ovanpå — med risk för dubbelreglering och konflikt.

Netnod AB
Greta Garbos väg 13
169 40 Solna

Motståndskraft skapas genom **redundans, diversifiering och verifierad återställningsförmåga**, inte genom enskilda egenskaper hos en leverantör. En förordning som koncentrerar kritisk infrastruktur till en gemensam europeisk certifieringsram skapar en ny monokultur med ett gemensamt angreppsmönster; icke-europeiska leverantörer måste därför förbli ett tillåtet inslag i en diversifierad beroendeprofil. Offentlig sektor bör dessutom i första hand driva kvalitet och motståndskraft som **krävande kund**, exempelvis genom innovationsupphandling; tvingande reglering och tillsyn bör förbehållas fall där marknaden inte bedöms kunna lösa problemet.

Netnods viktigaste rekommendationer:

- Riskbedömning enligt artikel 29 leder till en tillitsnivå, men kan i praktiken inte reduceras till att ta fram och formellt kontrollera den. För att på ett adekvat sätt bedöma risken för tjänsteavbrott måste analysen utgå från den funktion som ska upprätthållas och dess beroenden, inklusive DNS, BGP-routning, tidssynkronisering och internetutbytespunkter. En hög tillitsnivå är i sig ingen garanti för avbrottsfri drift.
- Krav bör knytas till den kritiska funktionen, inte automatiskt till hela verksamhetsutövarens verksamhet, och kunna föras vidare kontraktuellt till underleverantörer.
- Förordningen bör kräva **verifierad** — inte enbart dokumenterad — kontinuitetförmåga och uttryckligen harmonisera med CER- och NIS2-ramverken.
- Icke-europeiska leverantörer ska förbli tillåtna som del av en dokumenterad diversifieringsstrategi; en EU-certifieringsmonokultur är inte ett resiliensmål.
- Öppna standarder, interoperabilitet och portabilitet bör ges en tydligare roll (artiklarna 43–44 är ett välkommet steg).
- Det industripolitiska målet bör uppnås via **innovationsupphandling**, inte via subventionerade demonstrationsprojekt som inte överlever på marknaden.

Netnod utvecklar dessa synpunkter i den bifogade bilagan (kapitel 1–10).

Patrik Fältström
Senior Security Consultant
Tel: +46-76 70 605 9051
Email: paf@netnod.se

Bilaga 1 - Detaljerade kommentarer

1. Regelverket bör utgå från den funktion som ska upprätthållas

Netnod delar kommissionens bedömning att Europas motståndskraft behöver stärkas och att beroenden av kritiska digitala tjänster behöver analyseras och hanteras. Förordningens övergripande syfte — att hantera beroenden och stärka motståndskraften som framgår av skäl 4–6 i COM(2026)502 — är välmotiverat.

Netnod anser samtidigt att regelverket i högre grad bör utgå från den funktion som ska upprätthållas, snarare än från egenskaper hos enskilda leverantörer eller tekniska lösningar. Bilaga II:s kriterier för tillitsnivåerna 1–4 — vilka utgör kärnan i förordningens suveränitetsramverk och som upphandlande myndigheter ska tillämpa via riskbedömningar enligt artikel 29 — fokuserar på var leverantören är etablerad, var personal och infrastruktur finns, var data lagras och om leverantören kontrolleras av ett tredjeland. Dessa faktorer är viktiga riskfaktorer, men de utgör inte i sig en garanti för att den upphandlande organisationen faktiskt kan upprätthålla sina kritiska funktioner om tjänsten blir otillgänglig.

Den organisation som ansvarar för en samhällsviktig eller annan kritisk funktion har även ansvaret för att denna funktion kan upprätthållas när störningar inträffar. Detta ansvar kan inte överföras till en leverantör genom avtal eller genom att välja en viss kategori av tjänster. Förordningen bör därför utformas så att den stärker organisationens egen förmåga att hantera störningar, oberoende av var dessa uppstår.

Det innebär att riskbedömningar bör utgå från verksamhetens uppdrag och de konsekvenser som uppstår om den aktuella funktionen inte längre kan upprätthållas. Artikel 29(1)(b) föreskriver att riskbedömningen ska fastställa vilken tillitsnivå som är lämplig för verksamheten. Nivån är alltså bedömningens resultat, inte dess utgångspunkt. Netnod noterar vidare att artikel 29(1)(c) redan kräver att risken för och konsekvenserna av ett eventuellt tjänsteavbrott beaktas. Artikeln stannar dock där, den kräver inte att verksamhetens beroenden kartläggs, att återställningskrav fastslås eller att alternativa sätt att uppnå förmåga vidmakthålls. Bedömningarna är primärt inriktade på leverantörens egenskaper snarare än på verksamhetens kritiska beroenden och den faktiska förmågan att fungera vid störningar. Därmed finns en praktisk risk att bedömningen blir en klassificeringsövning där en hög tillitsnivå uppfattas som svaret på kontinuitetsfrågan.

Netnod anser att artikel 29 bör kompletteras med ett krav på att riskbedömningen även ska identifiera vilka funktioner som är beroende av tjänsten, vilka konsekvenser ett avbrott medför och vilken alternativ förmåga organisationen har.

Netnod anser därför att följande princip bör vara vägledande vid tillämpningen av förordningen:

> **Skyddsvärdet ligger i den funktion som ska upprätthållas, inte i den tekniska lösning eller den leverantör som används för att tillhandahålla funktionen.**

Leverantörens etableringsland, ägarstruktur och tillämpliga jurisdiktion är viktiga faktorer vid en riskbedömning. Netnod anser dock att dessa bör betraktas som en del av den samlade riskbilden och vägas samman med andra faktorer, såsom tekniska beroenden, koncentrationsrisker, möjlighet till diversifiering, interoperabilitet, portabilitet samt organisationens förmåga att upprätthålla verksamheten vid störningar.

Ett regelverk som utgår från den funktion som ska skyddas blir mer teknikneutralt och bättre anpassat till framtida teknikutveckling. Det ger också verksamhetsutövare möjlighet att välja de lösningar som bäst uppfyller verksamhetens krav på säkerhet, robusthet och kontinuitet, samtidigt som de hålls ansvariga för att den nödvändiga förmågan verkligen finns.

Netnod vill i detta sammanhang framhålla att unionens befintliga resiliensreglering redan följer denna funktionslogik. CER-direktivet (direktiv (EU) 2022/2557) och NIS2-direktivet (direktiv (EU) 2022/2555) ålägger verksamhetsutövare att göra riskbedömningar och vidta åtgärder för motståndskraft utifrån den tjänst som ska upprätthållas, inte utifrån leverantörens ursprung. Netnod anser att COM(2026)502 bör vila på samma grund. En svaghet i de befintliga ramverken är dock att skyldigheterna som utgångspunkt omfattar hela verksamhetsutövarens verksamhet, även när den kritiska tjänsten utgör en avgränsad och mindre del. Förordningen bör undvika denna oproportionerliga räckvidd och i stället knyta krav till den kritiska funktionen — kombinationen av verksamhet och den tjänst som faktiskt är skyddsvärd.

2. Riskbedömningar bör utgå från verksamhetens beroenden

En förutsättning för att kunna bedöma risk är att först identifiera vilka beroenden en verksamhet har. Netnod anser därför att riskbedömningar enligt artikel 29 bör utgå från en systematisk analys av de resurser och tjänster som är nödvändiga för att den aktuella funktionen ska kunna upprätthållas. I nuvarande utformning är artikel 29(1) primärt inriktad på att fastställa tillitsnivå för den identifierade verksamheten, snarare än på att kartlägga de beroenden som verksamheten faktiskt har.

Digitala tjänster bygger sällan på ett enskilt beroende. Tvärtom består de normalt av ett stort antal tekniska, organisatoriska och externa beroenden som tillsammans möjliggör den funktion som användaren uppfattar som en enda tjänst.

För en molnbaserad tjänst kan sådana beroenden exempelvis omfatta nätanslutning, DNS, BGP-routning, Internetutbytespunkter, tids- och frekvensinfrastruktur, identitets- och behörighetshantering, certifikatinfrastruktur, elförsörjning, kylning, logistik, fysisk infrastruktur, programvara, underleverantörer samt personal med rätt kompetens. Varje sådant beroende kan utgöra en kritisk felpunkt om det inte analyseras och hanteras på ett systematiskt sätt.

Netnod välkomnar att Bilaga II (punkt 2(i), 3(i) och 4(i)) redan kräver en fullständig och aktuell SBOM (Software Bill of Materials) och dokumentation av identifierade beroenden i programvaruleveranskedjan. Netnod föreslår att detta krav utvidgas till att även omfatta operativa nätverksberoenden — exempelvis DNS-tjänster, routing, Internetknutpunkter och

nätanslutning — som i dag faller utanför förordningens tillämpningsområde men som är avgörande för molntjänsters faktiska tillgänglighet (se vidare kapitel 7).

Konsekvensanalysen (SWD(2026)502, avsnitt 2.2) identifierar beroendet av ett fåtal leverantörer som ett strukturellt problem och konstaterar att tre icke-europeiska hyperscalers kontrollerar över 70 procent av den europeiska molnmarknaden. Analysen adresserar dock inte de underliggande nätverksberoendena. Netnod rekommenderar att riskbedömningar enligt artikel 29 uttryckligen ska inkludera dessa beroenden, även när den berörda infrastrukturen inte i sig utgör en molntjänst enligt förordningens definition.

Netnod vill särskilt understryka att regleringen — och den tillitsnivå som väljs — endast når den leverantör som organisationen har avtal med. Underleverantörsledet, där AI-accelererade angrepp ofta får sin hävstång, faller utanför. En verklig beroendeanalys måste därför omfatta även underleverantörer, och de krav som ställs på den direkta leverantören måste kunna föras vidare kontraktuellt nedåt i kedjan. En etablerad förebild finns i säkerhetsskyddslagstiftningens krav på säkerhetsskyddsavtal, där en aktör förpliktas att binda sina leverantörer vid motsvarande krav. Förordningen bör möjliggöra och uppmuntra en sådan kontraktuell nedförning av krav i leverantörskedjan, så att skyddet inte upphör vid den första avtalsparten.

Netnod anser därför att artikel 29 bör kompletteras med ett krav på att riskbedömningen ska:

- identifiera vilka kritiska funktioner som är beroende av den upphandlade tjänsten och vilka konsekvenser ett avbrott medför,
- identifiera samtliga relevanta beroenden, inklusive nätverksberoenden till till exempel DNS, routning och Internetknutpunkter,
- fastställa maximal acceptabel återställningstid (RTO) och maximal acceptabel dataförlust (RPO) för varje kritisk funktion,
- bedöma vilka alternativa lösningar som finns om tjänsten upphör att vara tillgänglig.

Netnod vill särskilt framhålla att ett beroende inte automatiskt utgör en oacceptabel risk. Digital infrastruktur bygger ofrånkomligen på ett stort antal beroenden. Det avgörande är istället att beroendena är kända, analyserade och hanterade på ett sådant sätt att verksamheten kan fortsätta fungera även när enskilda komponenter eller leverantörer fallerar.

3. Motståndskraft uppnås genom att minska konsekvenserna av störningar

Netnod delar kommissionens uppfattning att Europa behöver minska sårbara beroenden och stärka motståndskraften i den digitala infrastrukturen (skäl 5–6). Motståndskraft uppnås dock inte enbart genom att minska sannolikheten för störningar. Minst lika viktigt är att begränsa konsekvenserna när störningar trots allt inträffar.

Den grundläggande principen bakom Internet är att enskilda komponenter, nät, leverantörer och kommunikationsvägar förr eller senare kommer att fallera. Arkitekturen bygger därför

inte på antagandet att fel kan undvikas, utan på att den övergripande funktionen ska kunna upprätthållas trots att fel uppstår. Netnod anser att samma princip bör genomsyra förordningen.

En verksamhets motståndskraft avgörs inte enbart av valet av leverantör utan av dess samlade förmåga att hantera störningar. Denna förmåga kan uppnås genom flera olika åtgärder:

- användning av flera oberoende leverantörer,
- geografisk och teknisk redundans,
- alternativa kommunikationsvägar,
- möjlighet att flytta data och tjänster mellan olika miljöer,
- oberoende identitets- och behörighetslösningar,
- kontinuitetplanering och återställningsförmåga,
- samt regelbundet verifierade reservrutiner.

Netnod vill i detta sammanhang framhålla att verklig diversifiering kräver att icke-europeiska leverantörer förblir ett tillåtet alternativ som en del av en organisations beroendeprofil. Om all kritisk offentlig verksamhet i Europa koncentreras till leverantörer certifierade inom samma europeiska ram för tillitsnivåer innebär det att dessa leverantörer delar samma regulatoriska krav, samma granskningsprocess, samma tekniska arkitekturval och i många fall samma underleverantörer. En systemisk brist, ett angrepp eller en regulatorisk förändring som påverkar detta gemensamma lager kan potentiellt slå ut kritiska funktioner i hela Europa samtidigt.

En organisation som kombinerar en europeisk leverantör på hög tillitsnivå med en icke-europeisk leverantör på en annan teknisk och regulatorisk grund uppnår en genuint diversifierad beroendeprofil. En organisation som enbart använder EU-certifierade leverantörer kan ha uppfyllt förordningens formella krav utan att ha uppnått reell motståndskraft mot systemiska fel i den europeiska certifieringsramen. Förordningen bör explicit klargöra att icke-europeiska leverantörer, som en del av en dokumenterad och riskbaserad diversifieringsstrategi, inte är oförenliga med kravet på operativ motståndskraft.

Ett konkret och vardagsnära exempel på samma monokulturrisk finns i den svenska identitetsinfrastrukturen. När samhällsviktiga tjänster i praktiken endast accepterar en enda identitetslösning uppstår en de facto-monokultur och en gemensam felkälla: ett bortfall eller en kompromettering av den lösningen slår ut åtkomsten överallt samtidigt. Motståndskraften ökar då inte genom att staten lägger till ännu en enskild lösning som alla i sin tur förlitar sig på, utan genom att tjänsterna godtar flera oberoende och kvalificerade leverantörer. Exakt samma princip gäller det ramverk för tillitsnivåer som förordningen inför: motståndskraft skapas genom diversifiering, inte genom koncentration till en gemensam ram.

Netnod vill uppmärksamma EuroCloud Federation (artiklarna 34–36), som skapar ett ramverk för gemensam upphandling och delning av molnkapacitet. Federationen kan bidra

till att minska individuella organisationers beroenden av enskilda kommersiella leverantörer, men skapar i sin tur ett gemensamt system som kan utgöra en kritisk felkälla om det inte utformas med krav på redundans och oberoende driftsättning.

Netnod vill vidare uppmärksamma att de upphandlingsbestämmelser i Kapitel I, Titel IV som kräver att upphandlande myndigheter som minimum ska använda tjänster på tillitsnivå 1 riskerar att skapa incitament att ersätta ett ensidigt leverantörsberoende med ett annat. Kravet bör kompletteras med krav på att den upphandlande organisationen faktiskt har förmåga att upprätthålla sina kritiska funktioner när den upphandlade tjänsten inte är tillgänglig.

Netnod anser att förordningen tydligare bör betona att motståndskraft skapas genom redundans, diversifiering och återställningsförmåga, snarare än genom enskilda egenskaper hos de leverantörer som används.

4. Regelverket bör ställa krav på förmåga, inte på lösning

Netnod anser att ett långsiktigt hållbart regelverk bör beskriva vilken förmåga en organisation ska ha för att kunna upprätthålla sina kritiska funktioner, snarare än att styra valet av specifika tekniska lösningar eller kategorier av leverantörer.

Digital infrastruktur utvecklas kontinuerligt. Nya tjänster, leveransmodeller och tekniska lösningar tillkommer samtidigt som befintliga förändras eller avvecklas. Ett regelverk som bygger på dagens marknadsstruktur eller dagens teknik riskerar därför att snabbt bli inaktuellt. Ett regelverk som istället beskriver vilken förmåga som ska uppnås är mer teknikneutralt och kan tillämpas även när teknik och marknad förändras.

Netnod anser att regelverket i första hand bör ställa krav på att verksamheten exempelvis ska kunna:

- upprätthålla kritiska funktioner under definierade störningsscenarier,
- återställa verksamheten inom den tid som verksamheten själv bedömt som acceptabel,
- ersätta eller komplettera en leverantör när detta behövs,
- migrera data och tjänster utan oacceptabla avbrott,
- använda öppna och dokumenterade gränssnitt för informationsutbyte,
- samt fortlöpande identifiera och minska sina kritiska beroenden.

Bilaga II:s kriterier för de fyra tillitsnivåerna ställer detaljerade krav på var leverantören är etablerad, var data lagras och hur ägarstrukturen ser ut, men innehåller inga krav på att leverantören ska demonstrera kontinuitetförmåga eller att kunden ska ha en alternativ lösning om tjänsten upphör. Netnod anser att sådan kontinuitetförmåga i första hand bör efterfrågas av upphandlande organisationer som krävande kunder — marknaden kan och bör lösa detta genom kravställning i upphandling. I den mån tillitsnivåerna ändå används som obligatoriskt instrument bör Bilaga II kompletteras med ett krav på att leverantörer på

samtliga nivåer tillhandahåller dokumenterade och testade rutiner för serviceåterställning och kundmigration.

Netnod föreslår att artikel 29 kompletteras med ett krav på att riskbedömningen dokumenterar: (a) vilka kritiska funktioner som är beroende av den upphandlade tjänsten och vilka konsekvenser ett avbrott medför, (b) vilka alternativa lösningar som finns om tjänsten upphör att vara tillgänglig, samt (c) maximal acceptabel återställningstid (RTO) och dataförlust (RPO) för varje kritisk funktion. Dessa parametrar bör väga minst lika tungt som den tillitsnivå som krävs för verksamheten vid upphandlingsbeslut.

Netnod vill vidare framhålla att det legitima industripolitiska målet att stärka europeiska leverantörers konkurrenskraft bör redovisas som sådant — och inte kläs i säkerhets- och resiliensterminologi som det inte fullt ut motiverar. Sammanblandningen försvårar en korrekt analys av vilka åtgärder som faktiskt stärker motståndskraften och vilka som primärt stärker europeiska leverantörers marknadsposition. Risken att en leverantör — oavsett ursprung — av tekniska, kommersiella, rättsliga eller geopolitiska skäl inte kan leverera är en reell risk som åtgärdas genom förmågeuppbyggnad och diversifiering, inte genom att byta ut vilka leverantörskategorier som är obligatoriska.

5. Öppna standarder möjliggör konkurrens, interoperabilitet och minskade beroenden

Netnod anser att öppna standarder utgör en grundläggande förutsättning för ett robust och långsiktigt hållbart digitalt ekosystem. De möjliggör konkurrens mellan leverantörer, minskar risken för inlåsning och skapar förutsättningar för organisationer att anpassa sina lösningar när verksamhetens behov eller omvärldens förutsättningar förändras.

Internet har utvecklats till världens mest robusta digitala infrastruktur genom användningen av öppna och internationellt överenskomna standarder. Netnods verksamhet — från IXP-drift och DNS-infrastruktur till tids- och frekvenssignaler — bygger på dessa standarder och bekräftar dagligen deras betydelse för motståndskraft och interoperabilitet.

Netnod välkomnar att artiklarna 43–44 ger öppen källkod och programvarudelning ett tydligt stöd i förordningen, och att artikel 10 inrättar ett nätverk av nationella kontaktpunkter. Det är viktigt att notera att öppen källkod ger tillgång till kod men inte automatiskt operativt oberoende. Det krävs också kompetens, byggmiljöer, resurser för säkerhetsunderhåll och långsiktig förvaltningskapacitet. Förordningen bör skilja tydligare mellan tillgång till källkod och faktisk förmåga att självständigt underhålla och driva systemet.

Netnod anser att förordningen bör uppmuntra användningen av öppna standarder inom områden där interoperabilitet är avgörande för kontinuitet och motståndskraft: informationsutbyte, identitet och autentisering, säkerhetsfunktioner, administration, övervakning samt migration av data och tjänster. Förordningen bör inte peka ut enskilda standarder, utan skapa incitament för användning av öppna, dokumenterade och allmänt tillgängliga standarder.

6. Förmåga behöver utvecklas, verifieras och följas upp

Netnod anser att ett regelverk för moln- och AI-tjänster bör säkerställa att organisationer fortlöpande utvecklar, verifierar och följer upp sin förmåga att upprätthålla kritiska funktioner.

Netnod konstaterar att förordningen i sin nuvarande utformning saknar specifika krav på att kontinuitetförmåga ska verifieras genom praktiska tester. Riskbedömningsprocessen i artikel 29 och revisionskraven i Bilaga III avser primärt att fastställa och verifiera leverantörens egenskaper vid ett givet tillfälle — de ställer inga krav på att den upphandlande organisationen faktiskt testar sin förmåga att fungera utan den upphandlade tjänsten. Netnod anser att förordningen bör kräva verifierad — inte enbart dokumenterad — kontinuitetförmåga, men överlåta åt verksamheten att välja hur den visas. Offentlig sektor bör i första hand säkerställa detta som krävande kund i upphandling, och på så sätt forma marknader. Ett ändamålsenligt och regelbundet återkommande sätt att visa förmågan är praktiska tester av att kunna återställa kritiska funktioner och, vid behov, migrera till en alternativ leverantör.

Det är särskilt viktigt att skilja mellan dokumenterad och verifierad förmåga. Dokumenterade kontinuitetplaner, återställningsrutiner eller migrationsstrategier ger inte i sig någon garanti för att verksamheten faktiskt kan fortsätta fungera när en störning inträffar. Kontinuitetförmåga bör verifieras genom praktiska tester: att återställa tjänster från säkerhetskopior, migrera data mellan miljöer, simulera bortfall av en leverantör eller verifiera att alternativa kommunikationsvägar fungerar.

Netnod vill särskilt lyfta fram bortfallstestet som metod: att med jämna mellanrum praktiskt simulera att en leverantör, en komponent eller en hel kategori av tjänster faller bort, och verifiera att den kritiska funktionen ändå kan upprätthållas eller återställas inom den tid verksamheten själv bedömt som acceptabel. Det är först när förmågan prövats mot ett verkligt bortfall — inte enbart genom att återställa en säkerhetskopia — som den kan betraktas som verifierad. Netnod rekommenderar att sådan verifierad förmåga efterfrågas av offentlig sektor i upphandling och ingår i verksamhetens egen uppföljning, snarare än att förordningen detaljstyr testmetod och intervall.

Netnod vill även framhålla vikten av lärande. Resultatet från inträffade incidenter, genomförda övningar och praktiska tester bör återföras till organisationens riskbedömningar och kontinuitetplanering, så att motståndskraften successivt kan utvecklas i takt med att teknik, hotbild och beroenden förändras.

7. Beroenden bortom molntjänsten — en illustration av varför förmågebaserad riskanalys krävs

Förordningens suveränitets- och motståndskraftsbegrepp är i allt väsentligt begränsat till dataskiktet: var data lagras, vem som äger och kontrollerar lagringsinfrastrukturen och vilken jurisdiktion som är tillämplig på leverantören. En organisation kan uppnå full

överensstämmelse med förordningens krav och ändå vara beroende av ett stort antal kritiska resurser som förordningen inte berör alls.

Netnod lyfter detta inte som ett argument för att utvidga förordningens tillämpningsområde till ytterligare lager — det vore varken ändamålsenligt eller proportionerligt. Avsikten är i stället att illustrera varför en riskbedömning som utgår från leverantörens egenskaper är otillräcklig, och varför en förmågebaserad och beroendeorienterad riskanalys är nödvändig. Om artikel 29 kräver att organisationen systematiskt identifierar alla beroenden som är nödvändiga för att en kritisk funktion ska kunna upprätthållas, kommer dessa beroenden naturligt att framgå — oavsett om de faller inom eller utanför förordningens direkta räckvidd.

7.1 Nätverksberoenden som Netnod känner väl till

Netnod driver en av världens tretton rotnamnservrar (i-root), är operatör av kritisk DNS-infrastruktur för Sverige och ett flertal ccTLD:er, driver Sveriges största Internetknutpunkter (IXP) och ansvarar för tillhandahållande av tids- och frekvenssignaler i Sverige. Från dessa positioner ser Netnod dagligen de beroenden som avgör om en molntjänst faktiskt är nåbar, synkroniserad och driftsäker.

DNS är ett sådant beroende. En molntjänst på tillitsnivå 4 är fullständigt onåbar om DNS-uppslag fallerar — för användare, för API-anrop och för återhämtningsprocedurer. DNS-beroenden är tekniskt enkla att ta för givna men kan utgöra en kritisk felkälla om de inte analyseras.

Routing är ett annat. Routing styr hur trafik tar sig från användare till molntjänst. En felaktig eller illvillig ruttannonsering kan omdirigera eller blockera trafik till ett EU-certifierat datacenter utan att detta fångas av förordningens krav.

Tids- och frekvenssynkronisering är ett tredje. Distribuerade system, finansiella transaktioner, kryptografiska protokoll och nätverksutrustning är alla beroende av korrekt tidsreferens. Om den tidsinfrastruktur som en molntjänst förlitar sig på är otillförlitlig, felaktig eller saknar redundans uppstår fel som kan vara svåra att diagnostisera och allvarliga till sina konsekvenser — oavsett om datacentret i sig uppfyller samtliga krav i Bilaga II.

Internetutbytespunkter och transitförbindelser är ytterligare beroenden. En molntjänsts tillgänglighet beror på att det finns fungerande nätvägar hela vägen från användaren till datacentret. Netnods IXP är kritiska knutpunkter för svensk och nordisk Internettrafik. Brister i denna infrastruktur kan göra en i övrigt felfri molntjänst onåbar.

7.2 Beroenden som förordningen inte berör alls

Utöver nätverksberoendena finns ett stort antal andra kritiska beroenden som ingen molncertifiering adresserar. **Elförsörjning** är ett fundamentalt beroende för varje datacenter — redundans, reservkraft och anslutningspunkter till elnätet avgör i praktiken hur länge en tjänst kan hållas igång vid störningar. **Vattenförsörjning** är ett beroende för kylning i storskaliga datacenter. **Logistik och transportförsörjning** avgör möjligheten att snabbt tillföra reservdelar (vilka har sin egen leverantörskedja), ersättningshårdvara och teknisk

personal. **Kompetensförsörjning** — tillgång till personal med rätt kompetens för att driva, underhålla och återställa systemen — är ett beroende som sällan formaliseras i riskbedömningar.

Ingen av dessa faktorer fångas upp av en riskbedömning som primärt syftar till att fastställa den tillitsnivå som krävs för verksamheten.

7.3 Slutsats: rätt svar är förmågebaserad riskanalys, inte utvidgat tillämpningsområde

Netnod anser inte att lösningen är att utvidga förordningens tillämpningsområde till att omfatta DNS-operatörer, tids- och frekvenstjänster, elnät, logistikförsörjning eller personalförsörjning. Det vore att försöka reglera sig fram till ett resultat som bara kan uppnås genom systematisk riskanalys.

Snarare borde artikel 29 kräva att den upphandlande organisationen genomför en fullständig beroendeanalys som utgår från den funktion som ska upprätthållas — och som identifierar samtliga beroenden som är nödvändiga för att den funktionen ska fungera. Nätverksinfrastruktur, tidssynkronisering, elförsörjning, logistik och personal är alla naturliga delar av en sådan analys. Om ett beroende identifieras som kritiskt och inte kan hanteras, bör det framgå av riskbedömningen och leda till åtgärder — oavsett om det faller inom eller utanför förordningens direkta räckvidd.

Förordningens nuvarande utformning, där riskbedömningen primärt syftar till att välja rätt tillitsnivå, ger ingen vägledning för och inget incitament till denna bredare analys. Detta är en central brist i ramverket.

8. Slutsatser

Netnod välkomnar Europeiska kommissionens ambition att stärka Europas digitala motståndskraft och minska sårbara beroenden inom moln- och AI-området. Förslaget COM(2026)502 adresserar viktiga frågor som kommer att få stor betydelse för såväl offentlig sektor som näringsliv och leverantörer av digital infrastruktur.

Netnod välkomnar särskilt SBOM-kraven i Bilaga II (punkt 2(i), 3(i) och 4(i)), öppen källkod-bestämmelserna i artiklarna 43–44 samt EuroCloud Federationens potential att minska individuella beroenden (artiklarna 36–36).

Netnod anser att förordningen måste utgå tydligare från etablerade principer för riskhantering, kontinuitetplanering och Internetarkitektur. Regelverkets syfte bör vara att säkerställa att organisationer har den förmåga som krävs för att upprätthålla sina kritiska funktioner även när enskilda komponenter, leverantörer eller andra beroenden fallerar.

Netnod rekommenderar följande konkreta ändringar:

- **Artikel 29** bör kompletteras med ett krav på att riskbedömningen dokumenterar vilka kritiska funktioner som är beroende av den upphandlade tjänsten, konsekvenserna av avbrott, RTO/RPO-parametrar, alternativa lösningar och samtliga kritiska beroenden — inklusive sådana som faller utanför förordningens tillämpningsområde, som nätverksinfrastruktur, tidssynkronisering, elförsörjning och personalförsörjning.
- **Operativ kontinuitet** bör i första hand efterfrågas av offentlig sektor som krävande kund i upphandling. I den mån **Bilaga II** ändå används bör den kompletteras med

kriterier för operativ kontinuitet och verifierade återställningsrutiner, utöver de nuvarande kriterierna om etablering, datalagring och ägarstruktur.

- Förordningen bör explicit klargöra att icke-europeiska leverantörer, som en del av en dokumenterad och riskbaserad diversifieringsstrategi, är förenliga med kravet på operativ motståndskraft. En monokultur av EU-certifierade leverantörer är inte ett resiliensmål.
- **EuroCloud Federation** (artiklarna 35–36) bör utformas med krav på redundans och oberoende driftsättning för att undvika att en ny koncentrationsrisk skapas på federationsnivå.
- Förordningen bör kräva **verifierad** (inte enbart dokumenterad) kontinuitetförmåga, som utfall snarare än föreskriven metod. Sådan förmåga bör i första hand efterfrågas av offentlig sektor som krävande kund och kan visas genom återkommande bortfallstest, som komplement till de dokumentationsbaserade revisionskraven i Bilaga III.
- Det legitima industripolitiska målet att stärka europeiska leverantörers konkurrenskraft bör uppnås via offentlig **innovationsupphandling** — där krav ställs på funktioner, interoperabilitet och portabilitet snarare än på leverantörens ursprung. Subventionerade demonstrationsprojekt som inte överlever på marknaden när finansieringen upphör — ett mönster som setts i projekt som DNS4EU och WiFi4EU — är inte ett hållbart instrument för att bygga europeisk kapacitet i en marknadsekonomi. Den europeiska offentliga sektorns samlade köpkraft, om den samordnas rätt via innovationsupphandling, är ett mer effektivt och hållbart verktyg.
- Offentlig sektor bör i första hand agera som **krävande kund** och driva kvalitet och motståndskraft genom innovationsupphandling. Tvingande reglering, certifiering och tillsyn bör förbehållas områden där marknaden bevisligen inte kan lösa problemet.
- Förordningen bör uttryckligen linjera med den förmåge- och riskbaserade ansats som redan gäller enligt CER-direktivet (direktiv (EU) 2022/2557) och NIS2-direktivet (direktiv (EU) 2022/2555), och undvika att den ursprungsbaserade skalan för tillitsnivåer skapar dubbelreglering eller står i konflikt med dessa. Krav bör dessutom knytas till den kritiska funktionen, inte automatiskt till hela verksamhetsutövarens verksamhet, och kunna föras vidare kontraktuellt i leverantörskedjan.

Netnod anser att förordningen bör utvecklas med utgångspunkt i följande principer:

- skyddsvärdet är den funktion som ska upprätthållas,
- riskbedömningar enligt artikel 29 ska utgå från funktion och beroenden och täcka samtliga kritiska resurser — inklusive sådana utanför förordningens direkta räckvidd,
- motståndskraft kräver genuint heterogena beroendeprofiler — inklusive en kombination av europeiska och icke-europeiska leverantörer,
- regelverket — inklusive Bilaga II — bör beskriva vilken förmåga som ska uppnås, inte vilken lösning som ska användas,
- öppna standarder och interoperabilitet är centrala för att minska inlåsning och möjliggöra diversifiering,
- och den förmåga som byggs upp bör regelbundet verifieras genom praktiska tester.

9. Brister i konsekvensanalysen

Konsekvensanalysen (SWD(2026)502) utgör det analytiska underlaget för förordningens utformning. Netnod anser att den på flera punkter drar slutsatser som inte följer av det presenterade underlaget.

9.1 Icke-europeiskt ursprung likställs med operativ risk utan tillräckligt stöd

Konsekvensanalysen identifierar följande faktiska problem (avsnitt 2.2): hög marknadskoncentration hos ett fåtal leverantörer, teknisk inlåsning, extraterritoriell lagstiftning i tredjeland och ett begränsat europeiskt utbud. Dessa är välunderbyggda och allvarliga problem.

Analysen drar dock slutsatsen att lösningen är att öka europeisk ägarskaps- och etableringskontroll — utan att visa att leverantörens hemvist är en tillräcklig indikator på sannolikheten för driftsavbrott, eller att en europeisk leverantör skulle ge bättre operativ kontinuitet. En europeisk leverantör kan vara tekniskt beroende av samma globala infrastruktur, samma underleverantörer och samma programvarustackar som en icke-europeisk. Den korrekta slutsatsen av det presenterade underlaget är att verksamheter måste minska kritiska och koncentrerade beroenden — oavsett var leverantören är etablerad.

9.2 Fyra skilda politikmål behandlas som om de hade samma lösning

Förslaget syftar till att uppnå fyra separata mål: industripolitik (bygga upp europeisk kapacitet), riskhantering (säkerställa att kritiska funktioner upprätthålls), dataskydd och jurisdiktion (förhindra obehörig eller lagtvingad åtkomst), och konkurrenspolitik (minska marknadskoncentration och inlåsning).

Dessa mål är legitima var för sig men har delvis olika lösningar och kan i vissa fall stå i konflikt. Förslaget använder i stor utsträckning samma verktyg — europeisk kontroll och etablering — som svar på samtliga fyra. Det håller inte analytiskt. Inlåsning bryts primärt genom portabilitet och öppna standarder. Kontinuitetsproblem löses genom redundans och förmågeuppbyggnad. Konsekvensanalysen bör tydligare redovisa vilka åtgärder som svarar mot vilket problem.

9.3 Suveränitetsskalan är endimensionell trots att riskerna är flerdimensionella

De fyra tillitsnivåerna ger intrycket att nivå 4 alltid är säkrare än nivå 3. Men de ingående kriterierna ligger på separata riskdimensioner: datalokalisering, åtkomstkontroll, ägarstruktur, jurisdiktion, personalsäkerhet, försörjningskedja, teknisk säkerhet, operativ kontinuitet och möjlighet att byta leverantör. En tjänst kan vara stark i en dimension och svag i en annan. En enda sammanvägd nivå döljer detta och kan leda till felaktiga upphandlingsbeslut.

9.4 Kostnaden och komplexiteten för migration underskattas

Konsekvensanalysen redovisar ett migrationsscenario som Regulatory Scrutiny Board uttryckligen kritiserat. I praktiken kan migration av kritiska system kräva omkonstruktion av applikationsarkitektur, byte av identitets- och säkerhetsmodell, ersättning av proprietära plattformstjänster, ny driftorganisation, parallell drift och uppbyggnad av nya beroenden hos

den mottagande leverantören. Om dessa faktorer underskattas riskerar förordningens effekter att bli en annan än avsedd.

9.5 Öppen källkod ger tillgång till kod, inte automatiskt operativt oberoende

Förslaget beskriver öppen källkod som en hävstång för teknologisk suveränitet. Netnod delar uppfattningen att öppen källkod är ett viktigt verktyg för interoperabilitet och minskad inlåsning. Men analysen bör skilja tydligare mellan tillgång till källkod och faktisk förmåga att självständigt underhålla och driva systemet.

9.6 Utbyggnad av datacenterkapacitet är inte samma sak som ökad resiliens

Förslaget syftar till att tredubbla EU:s datacenterkapacitet. Men fysisk kapacitet i megawatt är inte i sig samma sak som robust tillgänglig kapacitet. Datacenter kräver för sin funktion oberoende nätanslutningar, tillräcklig elförsörjning, kompetent personal och reservkraft. Konsekvensanalysen bör redovisa hur dessa förutsättningar säkras och hur kapacitetstillväxten förväntas stärka möjligheten att upprätthålla kritiska funktioner.

9.7 Förhållandet till CER- och NIS2-direktiven är inte analyserat

Konsekvensanalysen behandlar inte hur den föreslagna skalan för tillitsnivåer förhåller sig till unionens redan antagna resiliensinstrument: CER-direktivet (direktiv (EU) 2022/2557) och NIS2-direktivet (direktiv (EU) 2022/2555). Dessa reglerar motståndskraft och riskhantering utifrån funktion och risk, medan förordningens tillitsnivåer utgår från leverantörens ursprung och kontroll. Utan en analys av överlapp, samspel och möjlig konflikt riskerar förordningen att lägga en andra, delvis motstridig regleringslogik ovanpå den befintliga — med dubbelreglering och otydlighet om vilken norm som gäller som följd. Netnod anser att konsekvensanalysen bör kompletteras med en sådan analys, och att förordningen bör utformas så att den bygger vidare på, snarare än konkurrerar med, CER- och NIS2-ramverken.

10. Synpunkter på enskilda bestämmelser och bilagor

10.1 Artiklarna 16–20: Systemet för tillitsnivåer mäter ursprung och kontroll, inte faktisk förmåga

Artiklarna 16–20 etablerar ett system med fyra tillitsnivåer. Systemet bygger på kriterier som primärt mäter var leverantören är etablerad, var personal och infrastruktur finns och vem som kontrollerar organisationen. Dessa kriterier kan vara relevanta för bedömning av juridisk autonomi och jurisdiktionsrisk, men mäter inte leverantörens förmåga att leverera kontinuerlig drift, kundens förmåga att upprätthålla sina funktioner vid avbrott, eller möjligheten att migrera i praktiken.

Netnod rekommenderar att systemet antingen tydligare benämns som en klassificering av juridisk och organisatorisk autonomi — inte som en generell säkerhets- eller resiliensnivå — eller kompletteras med separata kriterier för verifierad teknisk säkerhet och operativ kontinuitetförmåga. De resilienskriterier som saknas kan med fördel hämtas från den funktions- och riskbaserade ansats som redan gäller enligt CER-direktivet (direktiv (EU) 2022/2557) och NIS2-direktivet (direktiv (EU) 2022/2555), så att förordningen bygger vidare på ett etablerat unionsramverk i stället för att införa en fristående ursprungsskala.

Netnod motsätter sig inte att staten ställer strikta krav på ägande och jurisdiktion för en mycket avgränsad kärna av nationell säkerhet och hemligstämplad information (EUCI).

Däremot vänder vi oss mot att detta konfidentialitetsfokus upphöjs till en generell resiliensmodell för all kritisk infrastruktur, eftersom det i praktiken riskerar försämra den operativa tillgängligheten och kan innebära ett hinder mot teknisk diversifiering.

10.2 Bilaga II, punkt 3(d) och 4(d): Medborgarskap är relevant men otillräckligt som ensamt säkerhetskriterium

På tillitsnivåerna 3 och 4 kräver Bilaga II att personal som deltar i leveransen av den granskade tjänsten ska vara unionsmedborgare, och att nationell säkerhetsprövning ska ha genomförts när klassificerad information hanteras.

Netnod anser att medborgarskap kan vara relevant som en av flera faktorer i en säkerhetsbedömning. En persons jurisdiktionsexponering och lojalitetsbindningar påverkas av medborgarskap och bosättning — en unionsmedborgare bosatt inom unionen är i normalfallet inte underkastad tredjelandslagstiftning med extraterritoriell räckvidd på samma sätt som en person med hemvist utanför unionen. Det kan finnas legitima skäl att beakta dessa faktorer för roller med åtkomst till känsliga system. Netnod vill dock framhålla att medborgare i nära allierade och likasinnade europeiska länder (EES/EFTA såsom Norge och Island, samt Storbritannien) inte utan vidare bör likställas med tredjeländer i allmänhet vid en sådan bedömning.

Medborgarskap är dock inte tillräckligt som ensamt säkerhetskriterium. Det verifierar inte individens faktiska lojalitet, pålitlighet, åtkomstbehov eller säkerhetsmässiga lämplighet. Det säger ingenting om risk för insiderhot, kompromettering eller felaktig hantering av information. Krav på medborgarskap utan kompletterande säkerhetsprövning riskerar dessutom att utestänga kompetent personal i en bransch med begränsat utbud av specialister, utan att det påvisbart minskar säkerhetsriskerna.

För roller med åtkomst till känsliga system och klassificerad information bör kraven explicit inkludera säkerhetsprövning utförd i enlighet med nationell lagstiftning eller EU-rättslig ram, principen om minsta behörighet, separation av ansvar, loggning och granskning av åtkomst, stark autentisering och tvåpersonskontroll för kritiska operationer. Medborgarskap kan beaktas som en komponent i en samlad säkerhetsbedömning, men kan inte ersätta dessa explicita krav.

10.3 Bilaga II, punkt 2(h), 3(h) och 4(h): Förbud mot support utanför EU kan försämra driftkontinuiteten

På tillitsnivåerna 2–4 kräver Bilaga II att all teknisk och operativ support ska initieras och utföras uteslutande inom unionen. Netnod anser att kravet i vissa fall kan uppnå sitt syfte men att det som en generell nivåmarkör kan leda till minskad, inte ökad, motståndskraft. Krav på geografisk avgränsning kan minska tillgången till specialistkompetens vid komplexa incidenter, försvåra dygnet-runt-täckning med tillräcklig personaldjup och koncentrera driftorganisationen geografiskt — vilket i sig skapar en ny sårbarhet. Geografisk avgränsning är ett verktyg för att reducera jurisdiktionsrisk, inte ett generellt mått på operativ kontinuitetförmåga.

Netnod anser vidare att avgränsningen till "inom unionen" är onödigt snäv. Support och driftsamverkan från nära allierade och likasinnade europeiska länder — särskilt EES/EFTA-länder som Norge och Island samt Storbritannien — medför en väsentligt lägre jurisdiktionsrisk än tredjeländer i allmänhet, och möjligheten att samarbeta med dessa

länder är viktig för svenska och europeiska aktörers tillgång till specialistkompetens och för geografisk redundans. Netnod rekommenderar att kravet formuleras om så att det tillåter support från en definierad krets av betrodda länder (EU/EES samt likasinnade partner som Storbritannien), medger riskbaserade undantag och inte hindrar leverantörer från att upprätthålla geografisk redundans i driftorganisationen.

10.4 Bilaga II, punkt 4(i)(ii): Kravet på kontroll över programvarans framtida utveckling är orealistiskt

På tillitsnivå 4 kräver Bilaga II att leverantören demonstrerar att en aktör i tredjeland inte utövar faktisk kontroll över design, utveckling och underhåll av relevanta programvarukomponenter. Kravet på SBOM-dokumentation och transparens om beroenden är välmotiverat och bör behållas. Kravet på kontroll över komponenternas framtida utveckling är dock svårt att motivera riskbaserat och i praktiken omöjligt att uppfylla för moderna system, som i princip alltid innehåller globala beroenden i form av kompilatorer, standardbibliotek, operativsystem och öppen källkod-projekt.

Den relevanta frågan är om leverantören har förmåga att granska, underhålla och vid behov ersätta relevanta komponenter — inte var den ursprungliga utvecklaren är etablerad. Netnod rekommenderar att kriteriet omformuleras till att avse leverantörens faktiska underhålls- och granskningsförmåga.

10.5 Artikel 19: Självdeklaration på nivå 1 är missvisande givet begreppet "tillit" ("assurance")

Artikel 19 tillåter leverantörer att uppnå tillitsnivå 1 genom självdeklaration. Netnod anser att en mekanism baserad på självdeklaration inte motiverar beteckningen "tillitsnivå". Upphandlande organisationer riskerar att uppfatta nivåmärkningen som en verifierad garanti när den i praktiken visar formell självförsäkran om uppfyllelse av etablerings- och lokaliseringskriterier. Netnod rekommenderar att kommunikationen kring nivå 1 tydligare klargör att den avser självdeklarerad formell överensstämmelse, och inte innebär någon bedömning av teknisk säkerhet eller operativ kontinuitetförmåga.

10.6 Artikel 29: Risk för cirkulär riskbedömning

Artikel 29 ålägger upphandlande myndigheter att genomföra riskbedömningar för att fastställa vilken tillitsnivå som är lämplig för en identifierad verksamhet. Netnod noterar att analysen alltså går i rätt riktning — från verksamhet till tillitsnivå. Risken ligger i vad bedömningen mynnar ut i: just en tillitsnivå, och ingenting annat. Netnod anser att artikel 29 i sin nuvarande utformning därför riskerar en cirkulär logik i tillämpningen: riskbedömningen bedömer verksamhetens känslighet, som översätts till ett krav på en viss tillitsnivå, som i sin tur definieras av Bilaga II:s kriterier för leverantörens ursprung och kontrollstruktur. Kopplingen till den faktiska riskbilden — verksamhetens tolerans för avbrott, tillgängliga alternativa lösningar och faktisk förmåga att upprätthålla funktionen — riskerar att gå förlorad.

Artikel 29 bör skrivas om så att riskbedömningen utgår från funktion, konsekvens, beroenden och förmåga. Kriterierna för tillitsnivå kan användas som möjliga riskreducerande åtgärder, men bör inte vara det primära utfallet av bedömningen. En riskbedömning som börjar i frågan "vilken tillitsnivå behöver vi?" i stället för "vad händer om denna funktion upphör och hur hanterar vi det?" stärker inte organisationens faktiska motståndskraft.