Torup 2026-08-28

Finansdepartementet
fi.remissvar@regeringskansliet.se
Kopia: fi.ofa.dis.remisser@regeringskansliet.se

Er referens: Fi2026/01676
Vår referens: ELM 2026-03

Yttrande över Europeiska kommissionens förslag till förordning om utveckling av moln och AI, KOM(2026) 502

Elmhav Sweden AB (nedan Elmhav) lämnar följande synpunkter på förslaget. Elmhav är inte remissinstans; synpunkterna lämnas med stöd av att var och en får yttra sig över remitterade förslag. Elmhav är ett konsultföretag inom informationssäkerhet, dataskydd och IT-rätt i Torup, Hylte kommun, som arbetar som extern säkerhetschef och dataskyddsombud åt företag och offentliga verksamheter, reviderar ledningssystem enligt ISO/IEC 27001 och undervisar inom yrkeshögskolan. Synpunkterna lämnas ur tillämparens perspektiv: den som ska omsätta förordningen i riskbedömningar, kravspecifikationer, avtal och revisioner, ofta i små organisationer med begränsade resurser.

Sammanfattning

Elmhav tillstyrker förslagets syfte och dess huvuddelar om datacenterkapacitet, gemensam upphandling, EuroCloud-federationen och öppen källkod. Elmhav avstyrker suveränitetsramverket i avdelning IV i dess nuvarande utformning, eftersom det inte kan tillämpas som det är skrivet, och tillstyrker det under förutsättning att det byggs om på följande fem punkter.

1. **Ramverket förutsätter en certifieringsordning som inte finns.** Nivå 2 till 4 kräver certifikat enligt den europeiska certifieringsordningen för molntjänster (EUCS), som varit blockerad sedan 2020. Tillämpningen av avdelning IV bör knytas till att ordningen antagits, och grundakten bör ange vad som gäller under mellantiden.
2. **Nivåmodellen blandar tre skyddsintressen i en enda skala.** Cybersäkerhet, kontinuitet och jurisdiktionsexponering har olika hotbilder och olika botemedel. En linjär, kumulativ skala tvingar upphandlare att köpa jurisdiktionskrav för att få cybersäkerhet, och gör nivå 4 omöjlig bokstavligt tolkad. Elmhav föreslår att kriterierna i bilaga II struktureras i tre spår.
3. **Steget från nivå 1 till nivå 2 skapar övergångs- och systemrisk.** Nivå 1 är uppnåeligt för dagens marknad; nivå 2 kräver infrastruktur och personal i unionen och en leverantörsbas som ännu inte finns i den bredd offentlig sektor behöver. Utan övergångsregler, grandfathering och migrationsstöd blir undantaget i art. 30(4) huvudregel, och koncentrationsrisken flyttas snarare än minskas.
4. **Unionsmervärdeskriteriet i art. 32 är svårförenligt med upphandlingsrätten och Världshandelsorganisationens avtal om offentlig upphandling (GPA).** Var en leverantör bedriver forskning eller köper hårdvara saknar anknytning till kontraktsföremålet. Kriteriet bör utgå, eller åtminstone preciseras med viktning i artikeltexten och en uttrycklig GPA-grund.
5. **Styrningen i art. 18, 29(5) och 31(3) brister i förutsebarhet och rättssäkerhet.** Tredjelandserkännande genom genomförandeakt, kommissionens rätt att åsidosätta medlemsstatens nivåval och delegeringen att göra ramverket obligatoriskt för privata

aktörer avgör ramverkets faktiska räckvidd utan lagstiftarens medverkan och utan övergångsregler för löpande avtal. För Sverige tillkommer att art. 29 förutsätter en central statlig kompetens som kommunalt självstyre inte medger utan nationell lag.

Elmhav utvecklar synpunkterna i bilaga 1. Övriga synpunkter där avser rättsgrundens räckvidd, definitioner, förhållandet till cybersäkerhetsdirektivet (NIS2) och direktivet om kritiska entiteters motståndskraft (CER), personalkrav, revisorer, sanktioner, datacenterreglerna, öppen källkod, dataskydd, översynsfristen och redaktionell kvalitet. En sammanställning av förslagen finns i bilagans avsnitt 5.

Tova Elmhav
Jurist & GRC-specialist
Elmhav Sweden AB (org.nr 559475-9952)
Tel: 0763-400 900
E-post: tova@elmhav.se

Bilaga 1. Detaljerade synpunkter

1. Allmänna synpunkter

Förslagets problembeskrivning är riktig. Beroendet av ett fåtal leverantörer under tredjelandsjurisdiktion är en reell risk för kontinuitet, konfidentialitet och handlingsfrihet, och de anpassade "suveräna" erbjudanden som marknaden tagit fram löser inte grundproblemet, vilket skäl 48 korrekt konstaterar. Att EU tar ett samlat grepp i stället för att låta nationella märkningar som SecNumCloud och C5 fragmentera marknaden är i sig ett framsteg.

Elmhav stödjer särskilt: den riskbaserade grundidén att de flesta offentliga verksamheter ska klara sig med nivå 1 (skäl 52); den gemensamma upphandlingen i art. 37 till 40 och EuroCloud-federationen, som ger små kommuner tillgång till kapacitet de aldrig kan upphandla själva; det centrala registret i art. 22; transparenskraven i art. 23; nätverket av programkontor för öppen källkod (OSPO) i art. 44; och att förslaget tar datacenterkapacitet och nätanslutning på allvar som en förutsättning för allt annat.

Elmhav delar de utgångspunkter regeringen redovisar i faktapromemoria 2025/26:FPM99: att förslaget inte får överlappa eller stå i konflikt med annan EU-lagstiftning, att befintliga regleringar och strukturer bör användas så långt möjligt, att medlemsstaternas ansvar för säkerhetsbedömningar måste värnas och kommissionens befogenheter vara tydligt avgränsade, att de upphandlande myndigheternas handlingsutrymme vid valet av tilldelningskriterier ska värnas, och att reglerna ska vara enkla att tillämpa även för små upphandlande myndigheter. Synpunkterna nedan är avsedda som konkreta förslag till hur dessa utgångspunkter kan omsättas i rådsförhandlingen.

Elmhavs kritik gäller därför inte riktningen utan konstruktionen. Ett ramverk som ska styra offentlig sektors molnanvändning i 27 medlemsstater under lång tid måste kunna tillämpas från dag ett, ge förutsebara utfall och inte skapa nya beroenden i stället för de gamla.

2. Huvudsynpunkter

2.1 Avdelning IV kan inte tillämpas förrän EUCS finns

Nivå 2 och 3 kräver europeiskt cybersäkerhetscertifikat på nivån "substantial" och nivå 4 på nivån "high", enligt en ordning för molntjänster antagen under cybersäkerhetsakten (EU) 2019/881. Motiveringen medger att ordningen inte antagits och att "arbetet kommer att återupptas". Fram till dess hänvisar bilaga II till nationella ordningar "där de finns" och annars till "de högsta cybersäkerhetsstandarderna enligt tillämplig unionsrätt". Sverige har ingen nationell ordning, och den senare formuleringen pekar inte ut någon identifierbar standard.

Konsekvensen är att de tre övre nivåerna inte kan uppnås i Sverige när förordningen börjar tillämpas, samtidigt som riskbedömningen enligt art. 29 ska peka ut verksamheter som måste använda dem. Tidsplanen förstärker problemet: förordningen ska tillämpas ett år efter ikraftträdandet (art. 48), riskbedömningen ska vara klar vid samma tidpunkt (art. 29(1)), och en migration som riskbedömningen kräver ska vara genomförd inom högst tolv månader därefter (art. 29(6)). Två år efter ikraftträdandet ska alltså verksamheter av allmän ordning ha flyttat till tjänster på en nivå som kräver ett certifikat som ännu inte går att få. Verksamheterna hamnar då antingen på nivå 1 i strid med bedömningen eller i undantaget enligt art. 30(4). Elmhav noterar också att EUCS blockerades av precis den

suveränitetsfråga som förslaget nu flyttar in i sin egen text; förslaget löser inte blockeringen utan flyttar den till ett instrument där konsekvenserna av oenighet är större. Cybersäkerhetsakten är därtill under revidering (CSA2), vilket gör hänvisningen till en rörlig måltavla.

Elmhav föreslår att regeringen i rådet verkar för att tillämpningen av avdelning IV kopplas till att en EUCS-ordning antagits, och att grundakten under mellantiden anger vilka erkända standarder som får användas som ersättning, till exempel ISO/IEC 27001 med 27017 och 27018, för nivå 2 och 3. Nivå 4 bör inte kunna erkännas förrän "high" finns.

2.2 Nivåmodellen blandar tre skyddsintressen

Kriterierna i bilaga II mäter samtidigt cybersäkerhet (certifieringsnivå, programvaruförteckning (SBOM), källkodsrevision), kontinuitet (infrastruktur och support i unionen, migrations- och omställningsplaner) och jurisdiktionsexponering (etablering, ägande, kontroll, medborgarskap). Nivåerna är kumulativa. En verksamhet som behöver hög cybersäkerhet men saknar jurisdiktionsproblem måste ändå köpa jurisdiktionskraven, och en verksamhet med akut kontinuitetsrisk får inga starkare kontinuitetskrav på nivå 1 än utan erkännande.

De tre intressena har olika botemedel. Cybersäkerhet verifieras genom certifiering och revision. Kontinuitet verifieras genom att exit, failover och drift utan leverantörens medverkan faktiskt övas. Jurisdiktionsexponering verifieras genom rättslig analys av vilka utländska lagar leverantören lyder under, och kan inte kompenseras med teknisk förmåga. Att pressa in dem i en linjär skala ger två synliga fel: nivå 4:s krav på att inget tredjeland ska kunna påverka mjukvarukomponenternas utveckling, underhåll och kontinuitet är omöjligt att uppfylla bokstavligt (operativsystemkärnor, orkestrering, firmware, processorer), och nivå 2 och 3 kräver samma cybersäkerhetsnivå ("substantial") så att skillnaden mellan dem enbart är jurisdiktion, vilket bilagan inte redovisar.

Elmhav noterar att bilaga II och III redan innehåller kontinuitetskrav i de övre nivåerna, men de avser leverantörens egna beroenden: dokumenterad migrationsplan om en programvaruleverantör i tredjeland faller bort eller ett tredjeland inför restriktioner, blockering av fjärrfunktioner som kan störa tjänsten, och testad omställning till alternativ programvara eller minimal fungerande funktionalitet (bilaga III, kriterium I och J). Det finns inget motsvarande krav som avser kundens kontinuitet: att det offentliga organet kan få ut sina data i användbart format, återställa driften hos en annan leverantör inom bestämd tid eller driva verksamheten vidare utan leverantörens medverkan. Kraven förekommer dessutom enbart på nivå 2 och uppåt, där jurisdiktionskraven också gäller.

Från revisorns och upphandlarens håll finns ett konkret problem med det. En riskbedömning enligt art. 29 vars enda utfall är en nivå ger upphandlaren ingenting att skriva in i kravspecifikation, avtal eller SLA, och ger revisorn ingenting att pröva utöver leverantörens egenskaper vid revisionstillfället. Art. 29(1)(c) kräver visserligen att risken för och konsekvenserna av avbrott beaktas, men bedömningen mynnar inte ut i några kontinuitetskrav. I varje ledningssystem för informationssäkerhet och kontinuitet är det självklart att en riskbedömning ska resultera i mätbara krav: maximal acceptabel avbrottstid och maximal acceptabel dataförlust per funktion, vilka alternativ som finns om tjänsten upphör, och vilka beroenden funktionen vilar på. Det är sådana parametrar som kan läggas till grund för ett avtal och som en revisor kan verifiera. Ett nivåerkännande kan det inte.

En plan som aldrig prövats är inte bevis för förmåga. Bilaga III kräver test av leverantörens omställning till alternativ programvara; samma princip bör gälla kundens exit. Revisionsbevisningen bör omfatta protokoll från genomförda prov av dataexport, återställning hos annan leverantör och drift utan leverantörens medverkan, inte bara att planerna finns. Samma sak bör gälla på kundsidan: den som åberopar undantaget i art. 30(4) bör kunna visa att den har övat vad som händer om den tjänst undantaget avser upphör. I den delen delar Elmhav den kritik Netnod framfört i sitt yttrande över förslaget den 5 augusti 2026, om att kontinuitet ska vara verifierad och inte bara dokumenterad.

Som alternativ struktur föreslår Elmhav att bilaga II delas i tre spår med separata kriterier: ett cybersäkerhetsspår (via EUCS eller interimsstandard), ett kontinuitetsspår (tillgängligt från nivå 1, med prövade planer och med avbrottstid, dataförlust och exitförmåga som kontraktsparametrar) och ett jurisdiktionsspår (för nivå 3 och 4). Riskbedömningen enligt art. 29 skulle då ange krav per spår i stället för en sammansatt nivå. Art. 29(9) anger att medlemsstaterna ska överväga om en flerleverantörs- eller multimolnstrategi är lämplig. Elmhav föreslår att den bestämmelsen skärps till ett obligatoriskt element: riskbedömningen ska omfatta koncentrationsrisk oavsett leverantörens ursprung, i linje med skäl 65 och med den metod förordningen om digital operativ motståndskraft för finanssektorn (DORA) redan tillämpar. Om lagstiftaren väljer att behålla en enhetlig skala bör åtminstone kontinuitetskraven göras oberoende av nivå och formuleras som krav på prövad förmåga med revisionsbevis enligt bilaga III.

2.3 Steget till nivå 2 skapar övergångs- och systemrisk

Nivå 1 är byggd för att vara uppnåelig: tredjelandskontroll är tillåten och ska redovisas, kunddata inklusive metadata och telemetri ska stanna i unionen om inte det offentliga organet uttryckligen begär annat, och leverantören ska garantera att ingen tredjelandslag kräver rapportering av sårbarheter innan de exploaterats. Kommissionens konsekvensanalys (SWD(2026) 502) antar att 70 procent av offentlig sektors användningsfall stannar på nivå 1, 20 procent kräver nivå 2, 9 procent nivå 3 och 1 procent nivå 4. Fördelningen är ett antagande, inte en mätning, men den visar var tyngdpunkten ligger: de omkring 30 procent som ska passera gränsen till nivå 2 och uppåt är vård, energi, vatten, transport och andra verksamheter av allmän ordning. Nivå 2 kräver därutöver att infrastruktur, tillgångar och personal finns i unionen, oberoende revision och certifiering.

Elmhav delar ambitionen att en europeisk leverantörsbas ska växa fram, och ser att ramverket är tänkt att skapa den efterfrågan som gör det möjligt. Problemet är sekvensen. Kravet på nivå 2 börjar gälla när riskbedömningen är klar, vilket är ett år efter ikraftträdande, och en migration som bedömningen kräver ska enligt art. 29(6) vara genomförd inom högst tolv månader, medan marknaden byggs över flera år. Under mellantiden står verksamheter i vård, socialtjänst, energi, vatten och transport inför valet att stanna på nivå 1 i strid med bedömningen eller att åberopa art. 30(4). Undantaget har tre grunder: att ingen erkänd tjänst i registret kan leverera och inget rimligt alternativ finns; att en liknande upphandling under det senaste året inte gett några lämpliga anbud; och att efterlevnad skulle medföra oproportionerlig kostnad. Den tredje grunden är, som den är formulerad, tillämplig på nästan varje migration från en etablerad leverantör, och den andra kan uppfyllas genom att en upphandling genomförs och misslyckas. Erfarenheten från Frankrike, där Health Data Hub trots SecNumCloud blev kvar hos en amerikansk leverantör efter prövning i Conseil d'État, visar att undantaget blir normalläge när marknaden saknas.

Systemrisken är att kravet, när det väl kan uppfyllas, uppfylls av ett fåtal leverantörer. Ett beroende av tre utomeuropeiska hyperscalers ersätts då av ett beroende av färre europeiska aktörer, vilket motverkar både skäl 65 och dataaktens syfte att motverka inlåsning. För svenska förhållanden tillkommer att merparten av de lösningar levererade som programvara som tjänst (SaaS) som offentlig sektor använder levereras av små och medelstora svenska företag som bygger på utomeuropeisk infrastruktur. De kan inte nå nivå 2 om underleverantören inte gör det, och förslaget innehåller inget stöd för deras migration.

Elmhav anser att förslaget bör kompletteras med: uttrycklig grandfathering av avtal som ingåtts före ikraftträdandet, med tillämpning endast vid ny upphandling; en övergångsperiod för nivå 2-kravet räknat från att EUCS antagits; objektiva kriterier för samtliga undantagsgrunder i art. 30(4), där kostnadsgrunden knyts till verksamhetens riskbedömning och inte till enskild upphandling; att migrationsfristen i art. 29(6) räknas från att minst två av varandra oberoende erkända tjänster på den bedömda nivån finns tillgängliga i registret, så att migrationen inte i sig skapar ett nytt enleverantörsberoende; tidsbegränsning, publicering i registret och krav på migrationsplan vid undantag; samt stödåtgärder för SaaS-leverantörer som behöver byta infrastruktur.

2.4 Art. 32 och upphandlingsrätten

Art. 32 ålägger upphandlande myndigheter att vid upphandling av innovativa molntjänster och AI-system tillämpa icke prisbaserade tilldelningskriterier för "unionsmervärde": stärkt digital leveranskedja i unionen, integrering av unionsteknik, innovation som stärker försörjningstryggheten, och hårdvara designad eller tillverkad i unionen. Vad som gör en upphandling "innovativ" definieras inte. Art. 32(2) anger att kriterierna ska ha anknytning till kontraktsföremålet och vara underordnade och inte avgörande; viktningen om 15 av 120 poäng finns endast i skäl 67 som något upphandlande myndigheter "kan överväga".

Tilldelningskriterier ska enligt direktiv 2014/24/EU art. 67(3) och lagen (2016:1145) om offentlig upphandling (LOU) 16 kap. 2 § ha anknytning till kontraktsföremålet. EU-domstolen har slagit fast att kriterier som rör anbudsgivarens verksamhet i allmänhet, utöver det som ska levereras under kontraktet, inte får användas vid tilldelning (EVN och Wienstrom, C-448/01, där ett kriterium om leveransförmåga utöver kontraktsvolymen underkändes), att anbudsgivarens allmänna inköpspolicy inte får läggas till grund för bedömningen (kommissionen mot Nederländerna, C-368/10), och att egenskaper hos anbudsgivaren hör till kvalificeringen, inte tilldelningen (Lianakis, C-532/06). Miljö- och sociala kriterier är tillåtna just därför att de kan knytas till det som upphandlas (Concordia Bus, C-513/99). Var leverantören bedriver forskning, om den "stärker unionens digitala leveranskedja" eller varifrån den köper processorer är egenskaper hos leverantörens verksamhet, inte hos den upphandlade tjänsten. Art. 32(2)(a) föreskriver därmed en anknytning som kriterierna i art. 32(3) till sin natur inte kan ha; artikeln motsäger sig själv. Kriteriet är dessutom svårt att förena med likabehandlingsprincipen och med GPA art. IV, och undantaget för allmän ordning i GPA art. III:2(a), som skäl 64 åberopar för nivåkraven, täcker inte ett industripolitiskt kriterium. Hårdvarukriteriet kan i praktiken ingen leverantör uppfylla i dag, vilket gör det till ett innehållslöst poängkriterium. En mindre kommun saknar förmåga att verifiera påståenden om leveranskedjor och lokalisering av forskning och utveckling, och varje tillämpning öppnar för överprövning.

Elmhav förordar att art. 32 utgår. Om kriteriet behålls bör viktningen anges i artikeln, hårdvarukriteriet strykas, en standardiserad självdeklaration med sanktion vid oriktighet införas och den GPA-grund som åberopas anges uttryckligen.

Förordningen bör vidare klargöra hur nivåkravet infogas i upphandlingsdirektivets system: som teknisk specifikation, kvalificeringskrav eller uteslutningsgrund, om det prövas vid anbud, tilldelning eller under avtalstid, och att riskbedömningen enligt art. 29 inte kan angripas i överprövning av enskild upphandling. Utan detta blir varje upphandling ett prejudikat.

2.5 Styrning, förutsebarhet och kommunalt självstyre

Tre bestämmelser avgör ramverkets faktiska räckvidd utanför den ordinarie lagstiftningsprocessen.

Art. 18 låter kommissionen genom genomförandeakt erkänna tredjeländer vars leverantörer får revideras mot nivå 3. Villkoren är sex och kumulativa, och de är i sak väl utformade: adekvansbeslut, inga åtgärder som ger kontroll i strid med dataaktens art. 32(2) och (3), inga åtgärder som tvingar till degradering eller sanktionstillämpning, inga hinder mot modern teknik, öppen marknad och ömsesidigt upphandlingstillträde. Frågan är hur de tillämpas. Tolkas de strikt utesluts sannolikt de flesta tredjeländer och art. 18 blir tom; tolkas de generöst försvinner den jurisdiktionella skillnaden mellan nivå 2 och 3. Var gränsen dras är ramverkets viktigaste enskilda fråga, och den avgörs i kommittéförfarande utan parlamentets medverkan. Kommissionen ska dessutom återkalla, ändra eller tillfälligt upphäva beslutet när ett villkor inte längre är uppfyllt, utan övergångstid. Eftersom adekvansbeslut är ett villkor innebär det att en ogiltigförklaring av det slag EU-domstolen två gånger meddelat skulle kunna slå ut löpande nivå 3-avtal över en natt.

Art. 29(5) ger kommissionen rätt att genom genomförandeakt fastställa en annan nivå än den medlemsstaten valt om den anser att medlemsstatens nivå inte tillräckligt möter hänsynen till allmän ordning. Beslutet fattas i granskningsförfarande, alltså med kvalificerad majoritet av övriga medlemsstater. Det innebär att en svensk bedömning av vilken nivå en verksamhet inom rättsväsende, gränsförvaltning eller försvar behöver kan ändras av andra medlemsstater. Det är svårt att förena med att säkerhetsbedömningar för sådan verksamhet enligt art. 4(2) i fördraget om Europeiska unionen (FEU) är medlemsstatens ansvar, och med regeringens ståndpunkt i faktapromemorian att detta ansvar måste värnas. Befogenheten bör begränsas till att kommissionen får rekommendera en högre nivå, eller åtminstone förenas med samråd med den berörda medlemsstaten före beslut och undantag för verksamhet inom nationell säkerhet och försvar.

Art. 31(3) låter kommissionen genom delegerad akt, efter samråd med medlemsstaterna, göra suveränitetsbedömningarna obligatoriska för privata väsentliga entiteter i sektorer med hög kritikalitet, och föreskriva vilka riskreducerande åtgärder de ska vidta. Skäl 66 uttrycker att spillover till privat sektor är avsedd. Invändningsrätten enligt art. 290 i fördraget om Europeiska unionens funktionssätt (FEUF) finns, men beslutet flyttar gränsen för vilka som omfattas av förordningen, vilket hör till lagstiftaren. För finanssektorn tillkommer att DORA redan har en fullständig tredjepartsregim med register, koncentrationsanalys och tillsyn av kritiska leverantörer.

Elmhav föreslår att erkännande enligt art. 18 sker genom delegerad akt, att artikeln förses med övergångsperiod vid återkallelse och att fortsatt giltighet frikopplas från

adekvansbeslutets giltighet; att art. 29(5) begränsas till rekommendation, eller åtminstone förses med samråd före beslut och undantag för nationell säkerhet och försvar; och att art. 31(3) utgår så att utvidgning till privat sektor kräver ordinarie förfarande, med uttryckligt undantag för sektorer under DORA.

Kommunalt självstyre. Art. 29 ålägger "medlemsstater" att identifiera verksamheter och nivåer med bindande verkan för alla offentliga organ. I Sverige är kommuner och regioner egna rättssubjekt med grundlagsskyddat självstyre (regeringsformen 1 kap. 1 § och 14 kap.). Staten kan inte genom förvaltningsbeslut binda en kommuns upphandling; det kräver lag, och lagen ska enligt regeringsformen 14 kap. 3 § inte gå längre än nödvändigt. Unionen är enligt art. 4(2) FEU skyldig att respektera medlemsstaternas konstitutionella strukturer, uttryckligen inbegripet regionalt och lokalt självstyre. En förordning som förutsätter central statlig styrning av kommunal upphandling utan att ge medlemsstaten ett verktyg för det är svårförenlig med den skyldigheten, och kommissionens befogenhet enligt art. 29(5) skärper problemet. Förordningen är direkt tillämplig, men dess tillämpning förutsätter en nationell lag om vem som gör riskbedömningen, med vilken verkan och med vilka rättsmedel. Problemet delas av förbundsstaterna, och regeringen bör söka gemensam position med dem. Elmhav föreslår att förordningen uttryckligen anger att medlemsstaten får utse en central myndighet vars nivåbeslut binder alla offentliga organ, att ettårsfristen räknas från att kommissionens metod antagits, och att regeringen parallellt förbereder nationell lagstiftning.

3. Övriga synpunkter

Rättsgrundens räckvidd. Avdelning IV vilar på art. 114 FEUF. Kommissionens argument att nationella suveränitetsmärkningar fragmenterar marknaden är hållbart så långt ramverket ersätter dem. Det bär däremot inte art. 32, och det är osäkert hur långt det bär de kriterier i bilaga II som saknar motsvarighet i någon nationell märkning. Art. 173(3) kan inte åberopas för art. 32: motiveringen och skäl 8 reserverar den grunden för Leadership-initiativen i avdelning II, och art. 173(3) utesluter uttryckligen harmonisering, medan art. 32 är en harmoniserad upphandlingsregel. Elmhav föreslår att regeringen i rådet efterfrågar rättstjänstens analys av räckvidden, och att kommissionen redovisar GPA-förenligheten sektor för sektor; att kräva nivå 2 till 4 i samtliga NIS2-sektorer, inklusive post, avfall och livsmedel, är svårt att försvara som nödvändigt för allmän ordning.

Definitioner. Begreppet "kontroll" bär hela skillnaden mellan nivå 2 och 3. Art. 2(21) hänvisar till definitionen i förordningen om Europeiska försvarsfonden (EU) 2021/697, förmågan att direkt eller indirekt utöva ett avgörande inflytande, medan bilaga III punkt 7 anger en betydligt mer detaljerad prövning med ägande om minst 5 procent, vetorätter, kommersiella och finansiella beroenden som "andra källor till kontroll". Förhållandet mellan den snäva legaldefinitionen och den vida revisionsprövningen är oklart, och försvarsfondens definition är skriven för en annan situation. Elmhav föreslår att kontrollbegreppet ges en egen definition i art. 2 som anger tröskelvärden och vilka former av inflytande som räknas, med koncentrationsförordningen 139/2004 art. 3 som förebild eftersom den har praxis. "Allmän ordning" bör definieras med anknytning till EU-domstolens praxis om ett verkligt och tillräckligt allvarligt hot mot ett grundläggande samhällsintresse, och förhållandet till nationella klassificeringssystem (säkerhetsskyddsklassificering, Myndigheten för samhällsskydd och beredskaps informationsklassning) bör regleras; skäl 62 och 63 pekar i dag åt olika håll. Gränsen mot AI-förordningen för sammansatta tjänster (SaaS med inbäddad AI) bör anges. EES-staternas ställning bör klargöras.

Förhållandet till NIS2 och CER. De verksamheter som art. 29 pekar ut är i huvudsak samma som omfattas av NIS2-direktivet och CER-direktivet (EU) 2022/2557, båda under genomförande i svensk rätt. De direktiven ålägger verksamhetsutövaren att riskbedöma och skydda den tjänst som ska upprätthållas, oavsett leverantörens ursprung. CADA lägger en tredje riskbedömning ovanpå, med annan utgångspunkt (leverantörens egenskaper) och annan tillsynsmyndighet, och för finanssektorn en fjärde via DORA. För en svensk kommun eller ett regionalt energibolag innebär det parallella bedömningar av samma system enligt olika metoder, utan regel om vilken som gäller vid konflikt. Konsekvensanalysen behandlar inte förhållandet till CER alls. Elmhav föreslår en uttrycklig samordningsregel i förordningen: en riskbedömning gjord enligt NIS2 eller CER ska kunna användas som underlag för art. 29, och en verksamhetsutövare ska inte behöva dokumentera samma beroende tre gånger.

Personalkrav. Nivå 3 och 4 kräver att all personal, inklusive underleverantörers, är unionsmedborgare, med nationell säkerhetsprövning endast vid hantering av säkerhetsskyddsklassificerade uppgifter (bilaga II 3.1(d) och 4.1(d)). Medborgarskap är en svag proxy för tillförlitlighet; det relevanta skyddet är prövning till en definierad standard. Elmhav är medveten om att säkerhetsprövning är nationell kompetens, att säkerhetsskyddslagens prövning inte kan exporteras till annan medlemsstats leverantör annat än genom bilaterala säkerhetsskyddsavtal, och att ömsesidigt erkännande på unionsnivå inte är realistiskt. Lösningen finns dock redan i förslaget: på nivå 2 får det offentliga organet självt avgöra om ytterligare personalprövning eller medborgarskapskrav behövs (bilaga II 2.1(d)). Samma konstruktion bör användas på nivå 3, så att det upphandlande organet ställer de personalkrav dess nationella rätt och verksamhet motiverar, i stället för ett generellt medborgarskapskrav som varken är tillräckligt för säkerhetskänslig verksamhet eller nödvändigt för övrig. Behandlingen av medborgarskaps- och prövningsuppgifter saknar därtill angiven rättslig grund enligt dataskyddsförordningen (GDPR). Elmhav föreslår att medborgarskapskravet på nivå 3 ersätts med en rätt för det offentliga organet att föreskriva personalprövning enligt nationell rätt, och att rättslig grund för behandlingen anges i förordningen.

Revisorer. Art. 20 och 21 ställer oberoendekrav men inget ackrediteringskrav. Elmhav förordar ackreditering enligt förordning 765/2008, gemensam revisionsmetod i bilaga III, och en regel om vad som gäller när revisorer i olika stater når olika slutsatser.

Erkännandeprocessen. Art. 17 är i huvudsak väl utformad, med frister, invändningsrätt och hänskjutande till kommissionen. Det saknas frist för kommissionens beslut, regel om vad som gäller under hänskjutande, och tillsyn över små och medelstora företags (SMF) självdeklarationer på nivå 1, som erkänns unionsomfattande utan att någon myndighet sett dem. Sverige behöver dessutom besluta vilken myndighet som ska vara behörig och ge den resurser.

Sanktioner och återkallelse. Art. 24 saknar harmoniserat maximibelopp; medlemsstaterna ska själva bestämma sanktioner som är effektiva, proportionella och avskräckande med ledning av en icke uttömmande kriterielista. Skadeståndsrätten i art. 24(3) hänvisar till unionsrätt och nationell rätt utan att precisera ansvarsgrund, kausalitet eller preskription. Det avviker från GDPR, AI-förordningen och NIS2 och öppnar för forumshopping. Förslaget reglerar inte heller vad som händer med löpande avtal när ett erkännande återkallas, till exempel efter ett ägarbyte. Elmhav förordar ett harmoniserat tak, preciserad ansvarsgrund och en lagstadgad avvecklingstid om minst tolv månader med kostnadsansvar hos leverantören vid självförvållad återkallelse.

Datacenter. Tolvmånadersfristen i art. 13(5) gäller tillståndsförfarandet för datacenterprojektet räknat från fullständig ansökan. Det aggregerade grundtillståndet omfattar enligt skäl 41 inte nätanslutningstillstånd, och nätanslutning tar enligt kommissionens egen konsekvensanalys två till tio år i etablerade datacenterregioner. Klockan stannar alltså före det steg som faktiskt avgör. Begreppet aggregerat grundtillstånd saknas i svensk rätt, där plan- och bygglagen, miljöbalken och Svenska kraftnäts anslutningsprocess är separata. Elmhav föreslår att nätanslutning ges en parallell bindande frist, att medlemsstaten får prioritera nätkapacitet mellan datacenter och annan samhällsviktig verksamhet, och att skäl 36 om geografisk balans inte tillåts styra investeringar bort från platser med bäst förutsättningar.

Öppen källkod. Elmhav stödjer inriktningen. Art. 41 ålägger unionen och medlemsstaterna att "uppmuntra" offentliga organ att använda öppna standarder och öppen källkod med beaktande av funktionalitet, säkerhet och totalkostnad. Bestämmelsen bör ges ett konkret innehåll, lämpligen som en motiveringsskyldighet när ett offentligt organ väljer en proprietär lösning, så att förhållandet till LOU:s regler om tekniska specifikationer och likabehandling blir tydligt. Art. 42 innebär ingen skyldighet att publicera kod utan reglerar bara kanalen när ett organ väljer att göra det; det bör framgå av skälen så att bestämmelsen inte läses vidare än den är. Lagstiftaren bör också beakta att offentliga organ som publicerar kod kan få skyldigheter som open source steward enligt cyberresiliensakten.

Dataskydd. Motiveringen beskriver ramverket som en garanti för dataskydd. Nivå 1 vilar på självdeklaration och ramverket ersätter inte överföringsbedömning, biträdesavtal eller konsekvensbedömning enligt GDPR. Förordningen bör uttryckligen ange att ett erkännande enligt art. 17 inte skapar någon presumtion om att behandlingen är förenlig med GDPR eller att överföring till tredjeland enligt kapitel V är tillåten. Utan en sådan regel kommer nivåmärkningen att läsas som en garanti, och EU-domstolens praxis i Schrems-målen visar vad det kostar när en sådan garanti visar sig ogrundad. Förbudet mot att träna AI på kunddata bör gälla alla nivåer, inte bara när systemet drivs av en tredjelandsenhet.

Översyn. Art. 47 föreskriver utvärdering fyra år efter ikraftträdandet och därefter vart femte år. Det är för lång tid för ett ramverk vars marknadsförutsättningar ännu inte finns, särskilt som bilaga II och III ska ses över var 18:e månad (art. 16(3)) medan ramverkets grundkonstruktion ligger fast. Elmhav förordar treårig översyn och årlig rapportering om användningen av art. 30(4), antal erkända tjänster per nivå och medlemsstat, och marknadskoncentration bland erkända leverantörer.

Redaktionell kvalitet. Artikelnumreringen är bruten: två artiklar bär nummer 44 (nätverket av OSPO:er respektive utövandet av delegeringen), texten fortsätter med art. 46, medan art. 16(2), 20(9) och 31(3) hänvisar till delegerade akter enligt "art. 45" och motiveringen beskriver avdelning V som art. 45 till 48. Definitionerna i art. 2 hoppar från punkt 22 till punkt 25. Art. 30(4) har två led betecknade (a). Bilaga II punkt 3.1(g) och bilaga III punkt 7.2 hänvisar till en genomförandeakt enligt "art. 19" där art. 18 avses. Skälen innehåller ett flertal stavfel. Skäl 62 och 63 behöver samordnas. Elmhav förutsätter juristlingvistisk granskning före rådsbehandling.

4. Konsekvenser för Sverige

Förslaget träffar 290 kommuner, 21 regioner, kommunala bolag, lärosäten och samtliga statliga myndigheter, och indirekt varje leverantör till dem. Kostnaderna redovisas i

konsekvensanalysen som "huvudsakligen" för nationella och lokala myndigheter, utan belopp. Elmhav delar inte kommissionens bedömning att förslagets ekonomiska konsekvenser är begränsade: för svensk offentlig sektor tillkommer riskbedömningar, migrationer med tolvmånadersfrist, tillsynsmyndighet och nationell lagstiftning, och för svenska leverantörer omställning av infrastruktur, utan att någon av posterna är uppskattad. Sverige behöver före ikraftträdandet: en nationell lag om riskbedömning och dess bindande verkan; beslut om behörig myndighet med resurser; en plan för hur befintliga ramavtal hanteras; och en bedömning av vad kravet på nivå 2 betyder för de svenska SaaS-leverantörer som bygger på utomeuropeisk infrastruktur. Elmhav föreslår att regeringen låter göra en nationell konsekvensanalys som omfattar dessa delar, inklusive SMF-stöd, innan Sverige tar ställning i rådet.

5. Sammanställning av förslag

1. Tillämpningen av avdelning IV knyts till att en EUCS-ordning antagits; interimsstandarder anges i grundakten.
2. Bilaga II struktureras i tre spår (cybersäkerhet, kontinuitet, jurisdiktion); kontinuitetskraven görs oberoende av nivå; riskbedömningen enligt art. 29 ska resultera i maximal acceptabel avbrottstid, dataförlust, alternativ och beroenden som kontraktsparametrar; bilaga III ska kräva protokoll från prövad exit och återställning; art. 29(9) skärps till obligatorisk analys av koncentrationsrisk.
3. Grandfathering av befintliga avtal; övergångsperiod för nivå 2 från EUCS; objektiva kriterier, tidsgräns, publicering och migrationsplan för undantag enligt art. 30(4); migrationsfristen i art. 29(6) räknas från att minst två oberoende erkända tjänster finns tillgängliga; migrationsstöd för SaaS-leverantörer.
4. Art. 32 utgår; i andra hand viktning i artikeln, hårdvarukriteriet stryks, GPA-grund anges.
5. Förordningen anger nivåkravets plats i upphandlingsdirektivets system och att riskbedömningen inte kan angripas i enskild överprövning.
6. Erkännande enligt art. 18 genom delegerad akt, med övergångsperiod vid återkallelse och frikoppling från adekvansbeslutets fortsatta giltighet.
7. Art. 29(5) begränsas till rekommendation, eller förses med samråd före beslut och undantag för nationell säkerhet och försvar.
8. Art. 31(3) utgår; sektorer under DORA undantas uttryckligen.
9. Medlemsstaten får utse central myndighet med bindande nivåbeslut; ettårsfristen räknas från antagen metod; regeringen förbereder nationell lag och söker gemensam position med förbundsstaterna.
10. Rättstjänstens analys av art. 114:s räckvidd; GPA-förenlighet redovisas sektor för sektor.
11. Egen definition av kontroll med tröskelvärden; definitioner av allmän ordning, sammansatta tjänster, "innovativ" upphandling och EES-status.
12. Samordningsregel mellan art. 29 och riskbedömningar enligt NIS2 och CER.
13. Medborgarskapskravet på nivå 3 ersätts med rätt för det offentliga organet att föreskriva personalprövning enligt nationell rätt; rättslig grund för behandlingen.
14. Ackreditering av revisorer; gemensam revisionsmetod.
15. Frist för kommissionens beslut vid hänskjutande enligt art. 17; stickprov på SMF-deklarationer.

16. Harmoniserat sanktionstak; preciserad ansvarsgrund; avvecklingstid vid återkallat erkännande.
17. Parallell frist för nätanslutning; nationell prioritering av nätkapacitet.
18. Art. 41 som motiveringsskyldighet; klargörande i skälen att art. 42 inte innebär publiceringsplikt.
19. Erkännande enligt art. 17 skapar ingen presumtion om GDPR-efterlevnad eller om tillåten tredjelandsöverföring; generellt förbud mot AI-träning på offentlig sektors data.
20. Treårig översyn; årlig rapportering om undantag, nivåer och koncentration.
21. Nationell konsekvensanalys inklusive SMF-stöd före svenskt ställningstagande.

Elmhav står gärna till förfogande för fördjupning i någon av punkterna.