Stockholm 2026-09-21
Finansdepartementet
fi.remissvar@regeringskansliet.se
Kopia: fi.ofa.dis.remisser@regeringskansliet.se
Er referens: Fi2026/01676
Vår referens: ELX 2026-01

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

Elastx AB (nedan Elastx) lämnar följande synpunkter på förslaget. Elastx är inte remissinstans; synpunkterna lämnas med stöd av att var och en får yttra sig över remitterade förslag.

Elastx är en svensk leverantör av molninfrastruktur (IaaS och CaaS) med cirka 35 anställda och kunder inom bland annat SaaS, finanssektorn och offentlig sektor. Elastx vision är att möjliggöra en digitalt suverän och hållbar framtid för Sverige och Europa. Tjänsterna levereras från tre georedundanta datacenter i Stockholmsregionen, där Elastx i colocation driftar sin egen utrustning och har full rådighet över hela hårdvaru- och mjukvaruplattformen. Bolaget är svenskägt, verkar under svensk jurisdiktion och bygger hela sin tjänsteplattform på öppna standarder och öppen källkod. Verksamheten är certifierad enligt ISO/IEC 27001, 27017 och 27018 samt ISO 14001.

Elastx lämnar synpunkterna ur perspektivet av just den typ av leverantör som förordningen syftar till att stärka: en svenskägd liten leverantör som redan idag uppfyller huvuddelen av de krav som ställs på de övre tillitsnivåerna. Det gör Elastx till både tänkt förmånstagare av ramverket och föremål för dess krav. Synpunkterna är därför inriktade på vad som krävs för att ramverket ska få avsedd verkan i praktiken.

Sammanfattning

Elastx tillstyrker förslaget i dess huvuddrag, inklusive suveränitetsramverket i avdelning IV och att ägande och kontroll utgör centrala kriterier. Digital suveränitet avgörs av vem som har faktisk kontroll över tjänsten, inte av var datan lagras. Fyra frågor avgör enligt Elastx om ramverket får avsedd verkan eller blir ytterligare ett verktyg för suveränitetstvätt:

- Tredjelandserkännandet i artikel 18 måste utformas snävt, tillämpas strikt och omprövas löpande. Klausulen är förordningens viktigaste enskilda bestämmelse: generöst tillämpad blir nivå 3 en bakdörr för strukturer som ytterst kontrolleras av utländska koncerner.
- Bevisbördan ska ligga på leverantören och efterlevnad ska kunna verifieras områdesvis. Självdeklarationer på nivå 1 behöver förenas med tillsyn.
- Ramverket måste vara uppnåeligt för små och medelstora europeiska leverantörer, och kapacitetsbygget i accelerationszonerna måste komma en mångfald av aktörer till del, med suveränitetsnivåerna som prioriteringskriterium när knapp nätkapacitet och eleffekt fördelas. Annars ersätts dagens koncentration med en ny, och diversifieringsmålet motverkas.

– Nivåerna bör kompletteras med krav på portabilitet, prövad exitförmåga och villkorstransparens, så att ramverket motverkar både teknisk och kommersiell inlåsning oavsett leverantörens ursprung.

Synpunkterna utvecklas nedan och bygger bland annat på Elastx operativa erfarenhet av kundmigrationer till och från andra molnplattformar. En sammanställning av förslagen finns i avsnitt 10.

1. Utgångspunkter: regler bygger inga datacenter

Dataförordningen (Data Act) ger kunder rätt att flytta system och data mellan leverantörer, fasar ut bytesavgifter och kräver portabilitet. Ändå kvarstår inlåsningen i praktiken, eftersom den drivs av friktion: långa bindningstider, kostnaden för att få ut sin egen data och framför allt att verksamheter byggts på leverantörsspecifika tjänster som saknar exakta motsvarigheter någon annanstans. Ett byte blir därför ofta en ombyggnad snarare än en flytt. Även när det blir lätt att lämna lutar marknaden mot de största leverantörerna, eftersom europeiska alternativ behöver skala och bredd för att kunna ta över de mest verksamhetskritiska systemen, och den skalan uppstår inte förrän tillräcklig efterfrågan flyttar. Kunderna väljer de etablerade för att alternativen ännu är för små, och alternativen förblir för små för att kunderna inte kommer. Försprånget från att ha varit först på marknaden konserveras därmed av inlåsningen. Konkurrensen sker inte på lika villkor: kundens val står aldrig mellan två leverantörers pris och kvalitet, utan mellan att stanna och att bära hela kostnaden för att lämna. Det gör inlåsningen dyr för kunderna och gör det svårt för alternativ att konkurrera på egna meriter, oavsett hur väl tjänsterna står sig i en jämförelse.

Det är detta moment 22 som förslaget angriper, från båda hållen samtidigt: det underlättar kapacitetsbygge och riktar den samlade offentliga köpkraften mot leverantörer som uppfyller suveränitetskraven. Elastx anser att den ansatsen är riktig. Kommissionens preliminära ställningstagande den 25 juni 2026, att AWS och Azure bör pekas ut som grindvakter enligt Förordningen om digitala marknader (DMA), bekräftar samtidigt problembilden: inlåsningseffekter och gateway-position är strukturella drag på molnmarknaden, inte undantag. Konkurrensregleringen och kapacitetsbygget är två spår mot samma mål och förstärker varandra.

Förslagets största förtjänst är enligt Elastx erfarenhet oberoende av dess slutliga utformning: det gör kontrollfrågorna till standard. I dag kräver nästan varje upphandling att data lagras inom EU, men få ställer frågorna om vem som ytterst äger leverantören, var personer med administrativ åtkomst finns och vilka länders lagar som når tjänsten genom ägarkedjan. Ramverket flyttar dessa frågor från undantag till norm.

2. Nivåmodellen och kontrollkriterierna tillstyrks

Elastx tillstyrker att ägande och kontroll utgör kärnan i kriterierna för de övre tillitsnivåerna. Var datan lagras är en nödvändig men inte tillräcklig fråga: två leverantörer med datacenter i Sverige kan ha helt olika riskprofil beroende på ägarkedja, var administratörer och eskaleringsvägar finns och vilken extraterritoriell lagstiftning som når tjänsten genom ägarstrukturen. Lagstiftning av den typ som amerikanska CLOUD Act representerar följer leverantören, inte servern.

Elastx vill samtidigt bemöta en vanlig missuppfattning: ramverket stänger inte ute utländska leverantörer från marknaden. De lägre nivåerna är öppna för alla som uppfyller kraven. Det

som begränsas är tillgången till de mest känsliga uppdragen, inte marknaden som sådan. Elastx anser att den avvägningen är riktig och proportionerlig.

En viktig effekt av ramverket är att bevisbördan flyttas. Tidigare har köpare fått försöka genomskåda leverantörers påståenden om suveränitet; med ramverket ska leverantören visa hur kontrollen faktiskt ser ut. Suveränitet blir därmed inte en etikett utan något som ska kunna verifieras. Kommissionens egen upphandling av suveräna molntjänster våren 2026, där ramverkets kriterier tillämpades, visar att modellen fungerar i praktiken.

3. Artikel 18 avgör om ramverket får verkan

Nivå 3 är den nivå där ramverkets trovärdighet avgörs. Endast där bland de substantiella nivåerna finns en mekanism för att genom genomförandeakt erkänna tredjeländer vars leverantörer bedöms erbjuda tillräckliga garantier (artikel 18), en konstruktion som liknar dataskyddsförordningens adekvansbeslut. Hur villkoren i artikeln tolkas och tillämpas är enligt Elastx förordningens viktigaste enskilda fråga.

Tillämpas villkoren generöst blir nivå 3 en bakdörr för EU-baserade strukturer som ytterst kontrolleras av utländska koncerner, och den jurisdiktionella skillnaden mellan nivå 2 och 3 försvinner. Tillämpas de strikt blir nivån ett verkligt suveränitetskrav. Villkoren pekar i praktiken direkt på förhållanden som CLOUD Act skapar: så länge ett tredjelands lagstiftning ger dess myndigheter rätt att begära ut data från leverantörer under landets jurisdiktion oavsett var datan lagras, bör erkännande inte kunna komma i fråga. Elastx anser att detta bör framgå tydligare av grundakten eller skälen, så att bedömningen inte lämnas helt till kommittéförfarandet.

Skäl 48 konstaterar korrekt att de anpassade "suveräna" erbjudanden som marknaden tagit fram, exempelvis partnerskaps- och förvaltarmodeller där driften läggs i en europeisk struktur medan den faktiska kontrollen kvarstår hos en tredjelandskoncern, inte löser grundproblemet. Den slutsatsen bör få uttryckligt genomslag i tillämpningen av artikel 18 och i revisionskriterierna i bilaga III: avgörande ska vara var den faktiska kontrollen ligger, inte var driften är paketerad.

Elastx föreslår att erkännandebeslut föregås av en offentlig, motiverad analys mot samtliga villkor, att beslut omprövas när tredjelandets relevanta lagstiftning ändras och att en övergångsperiod regleras för löpande avtal vid återkallelse, så att en ändrad bedömning inte slår ut pågående leveranser över en natt.

4. Bevisbörda, verifierbarhet och tillsyn

Självdeklaration som väg till nivå 1 (artikel 19) är rimlig som insteg, men en deklaration med unionsomfattande verkan som ingen myndighet granskar riskerar att undergräva förtroendet för hela registret. Elastx föreslår att självdeklarationer förenas med stickprovstillsyn och kännbara sanktioner vid oriktiga uppgifter. Seriösa leverantörer har inget att förlora på granskning; det är frånvaron av granskning som gynnar oseriösa påståenden.

Kraven på samtliga nivåer bör vara formulerade så att de kan visas med underlag: ägarkedja till yttersta ägare, var personal med administrativ åtkomst finns inklusive eskaleringsvägar, samt beroenden i leveranskedjan. Elastx har själv genomfört en självskattning mot Cloud Sovereignty Frameworks åtta områden och kan konstatera att övningen är fullt genomförbar för ett bolag med 35 anställda, samtidigt som den ger en ärlig bild av var beroenden

kvarstår. Den erfarenheten talar för att efterlevnad bör redovisas områdesvis snarare än enbart som en sammanvägd nivå: en områdesvis redovisning visar både var kontrollen finns och var beroenden återstår, vilket ger upphandlande organisationer ett bättre beslutsunderlag än en etikett.

5. Ramverket måste vara uppnåeligt för små och medelstora leverantörer

Förslagets syfte är att bredda den europeiska leverantörsbasen. Om certifierings- och revisionskostnaderna för nivå 2 och 3 blir så höga att endast de största europeiska aktörerna når dem, ersätts dagens koncentration med en ny och förslagets eget diversifieringsmål motverkas. Kravnivåerna bör därför utformas med uttrycklig hänsyn till proportionalitet: revisionens omfattning bör stå i rimlig proportion till leverantörens storlek och riskprofil, och bevis bör kunna återanvändas mellan ordningar, exempelvis befintliga certifikat, oberoende bestyrkanden och SBOM-dokumentation.

Nivå 2 till 4 förutsätter certifiering enligt en europeisk certifieringsordning för molntjänster som ännu inte antagits. Fram till dess att en sådan ordning finns bör etablerade internationella standarder kunna erkännas som interimsbevis för nivå 2 och 3, exempelvis ISO/IEC 27001 med tilläggen 27017 och 27018, kompletterat med oberoende bestyrkande. För en liten leverantör är dessa certifieringar redan en betydande men hanterbar investering. Ett krav på en ytterligare certifiering som inte går att erhålla får inte bli det som i praktiken håller nivåerna stängda under åren fram till att ordningen antagits.

Elastx vill även peka på en svensk konsekvens: en stor del av de SaaS-tjänster som svensk offentlig sektor använder levereras av små och medelstora svenska bolag som idag bygger på utomeuropeisk infrastruktur. Deras möjlighet att nå de högre nivåerna avgörs av valet av underliggande infrastrukturleverantör. Rimliga migrationsfrister och övergångsstöd för dessa bolag avgör om kravbilden bygger en bredare europeisk marknad eller i praktiken utestänger dem som skulle kunna bära den.

Samma proportionalitetsfråga gäller förordningens kapacitetsbyggande del. De accelerationszoner för datacenter som förslaget inrättar, med förenklade tillståndsprocesser och prioriterad nätanslutning, får inte utformas så att de i praktiken enbart gynnar de största aktörernas egna anläggningar. Europeiska utmanare bygger ofta sin leverans i oberoende colocationanläggningar med egen utrustning; tilldelningen av samhällsresurser i zonerna, särskilt eleffekt och nätanslutning, bör därför uttryckligen även omfatta sådana anläggningar. Om de största aktörerna tillåts ta hela den tillgängliga kapaciteten i anspråk driver det upp el- och lokalkostnaderna för colocation och stryper tillväxtmöjligheterna för just de små och medelstora leverantörer som förordningen syftar till att stärka.

Tilldelningen av eleffekt och nätkapacitet sker idag i praktiken enligt först till kvarn-principen, där enskilda kommuner konkurrerar om etableringar och där frågan om vilket värde en etablering skapar i Sverige och Europa sällan ställs. Knapp fossilfri el och nätkapacitet är en nationell strategisk resurs, och beslut om dess tilldelning bör fattas utifrån nationella och europeiska intressen snarare än avgöras av lokal konkurrens om kortsiktiga arbetstillfällen och skatteintäkter. Här kan förordningens egna suveränitetsnivåer bli ett konkret verktyg: om tjänster på de högre nivåerna, exempelvis nivå 3 eller högre, fick användas som prioriteringskriterium vid tilldelning av knapp nätkapacitet och eleffekt i accelerationszonerna skulle suveränitetsramverket kopplas till den fysiska resurs som avgör var kapacitet faktiskt byggs. Inget i det nuvarande förslaget gör den kopplingen. Elastx föreslår att Sverige driver

detta som ett ändringsförslag i förhandlingarna i rådet och Europaparlamentet: medlemsstaterna bör ges uttrycklig möjlighet att prioritera nätanslutning och eleffekt för datacenter som levererar, eller kontrakterats för att leverera, tjänster på de högre suveränitetsnivåerna.

6. Portabilitet och prövad exitförmåga bör komplettera nivåerna

Tillitsnivåerna mäter jurisdiktion, ägande och kontroll. De mäter inte kundens faktiska möjlighet att lämna leverantören. Utan krav på portabilitet riskerar ramverket att flytta inlåsningen snarare än att minska den: en kund som migrerat till en erkänd leverantör ska inte vara mer bunden till den än till sin tidigare.

Dataförordningen tar bort de formella hindren, men den kan inte tvinga nästa leverantör att erbjuda exakt samma tjänster. Elastx operativa erfarenhet av migrationer är att det sällan är datamängden i sig som är det svåraste, utan att bygga om applikationer och integrationer som utformats mot leverantörsspecifika tjänster. Svårast är tillståndsbärande data i leverantörsspecifika databastjänster, särskilt data som ändras kontinuerligt, samt transaktionssystem med hårda krav på tillgänglighet och svarstider, där en flytt måste ske utan avbrott. Det som i praktiken minskar friktionen är öppna standarder och dokumenterade gränssnitt, containerteknik och orkestrering enligt öppna standarder, infrastruktur som kod samt etablerade verktyg för replikering och kontrollerad överflyttning.

Elastx föreslår därför att kraven på de erkända nivåerna kompletteras med krav på dokumenterad och regelbundet prövad exit- och migrationsförmåga: dataexport i användbart och dokumenterat format, öppna gränssnitt där sådana finns etablerade samt genomförda migrationstester. En plan som aldrig prövats är inte bevis för förmåga. Offentliga upphandlingar bör dessutom ställa portabilitetskrav redan vid anskaffning i stället för först när en flytt ska ske; det är då kraven kostar minst. Kraven gynnar kunderna oavsett vilken leverantör de väljer och gör att ramverket motverkar inlåsning i alla led, inte bara i förhållande till dagens dominerande aktörer.

7. Parallell användning och kommersiell inlåsning

Att använda flera leverantörer parallellt är den mest robusta formen av diversifiering och den flerleverantörsstrategi som förslaget självt lyfter fram. I praktiken motverkas den av tre faktorer. Den första är löpande avgifter för utgående datatrafik: dataförordningen fasar ut engångsavgifterna vid byte, men avgifter för kontinuerlig synkronisering, replikering och backup mellan leverantörer kvarstår och gör parallell drift löpande dyrare än koncentration till en leverantör. Den andra är svarstidskrav mellan tjänster som ska spänna över flera leverantörer. Den tredje är kostnaden för att bygga och underhålla kompetens på flera plattformar. Om diversifieringsmålet ska nås behöver den löpande parallella användningen samma uppmärksamhet som engångsbytet; annars premierar kostnadsbilden fortsatt koncentration.

Gränsdragningen mellan byte och parallell användning skapar dessutom ett kryphål. Avgiftsfriheten vid byte förutsätter i praktiken att kunden lämnar helt, men de största leverantörernas utbud omfattar hundratals deltjänster och en fullständig utflytt i ett steg är sällan realistisk. En kund som flyttar huvuddelen av sin miljö men under en övergångstid behåller enstaka deltjänster hos den tidigare leverantören riskerar att behandlas som parallell användare i stället för som bytande kund, och går då miste om avgiftsskyddet. Ju

bredare tjänsteutbud en leverantör har, desto lättare blir avgiftsfriheten att kringgå. Elastx föreslår att en dokumenterad stegvis migration omfattas av samma avgiftsskydd som ett fullständigt byte, bedömt per tjänst och arbetslast, så att skyddet inte urholkas av tjänsteutbudets bredd.

Prismodellernas komplexitet är i sig ett byteshinder. Modellerna skiljer sig åt i vad som mäts och hur, avgifter för utgående datatrafik är svåra att uppskatta i förväg och blir därmed en osäkerhetsfaktor i varje byteskalkyl, och det saknas ofta en dokumenterad bild av vilka tjänster hos en leverantör som motsvarar vilka hos en annan. Elastx föreslår att transparenskraven i artikel 23 utvidgas till att omfatta prismodeller: kostnader, inklusive avgifter för utgående datatrafik, ska kunna förutses och jämföras före ett byte, och erkända leverantörer bör tillhandahålla dokumenterade tjänstebeskrivningar som gör jämförelser mellan leverantörer möjliga.

Vid sidan av tekniken och priset låser avtalsvillkoren. Återkommande exempel är volymåtaganden, automatiska förlängningar med korta uppsägningsfönster, rabatter som kopplar samman i övrigt orelaterade tjänster så att ett byte av en tjänst fördyrar en annan, licensvillkor som gör det dyrare att köra samma programvara hos en annan molnleverantör än i programvaruleverantörens eget moln, samt tillgodohavanden, exempelvis vid SLA-brott, som förverkas vid uppsägning och därmed skapar incitament att stanna hos en leverantör som brustit i leverans. Sådana villkor bör redovisas öppet för erkända tjänster. Ett alternativ värt att pröva är krav på avtalad exithjälp vid allvarliga avtalsbrott, så att bristande leverans underlättar ett byte i stället för att försvåra det.

För AI-tjänster gäller samma inlåsningsdynamik, förstärkt av två faktorer: proprietära gränssnitt som gör byten till ombyggnadsprojekt och koncentrationen av specialiserad beräkningshårdvara till ett fåtal aktörer, vilket begränsar antalet oberoende leverantörer. Eftersom förslaget uttryckligen omfattar AI-kapacitet bör öppna gränssnitt och tillgång till beräkningskapacitet behandlas som portabilitets- och konkurrensfrågor även på AI-området.

Ett närliggande skydd gäller användningen av kunddata. Kunddata ska inte kunna användas för träning av leverantörens AI-modeller utan kundens uttryckliga och specifika förhandsgodkännande. Ett sådant förbud bör gälla generellt för erkända tjänster, oavsett nivå och oavsett leverantörens ursprung, och utgångspunkten bör vara särskilt strikt för offentlig sektors data. Frågan är i grunden en förtroendefråga för hela molnmarknaden: en kund som inte kan lita på att den egna datan stannar i den egna tjänsten kommer att tveka inför både moln och AI.

8. Öppen källkod, öppna standarder och SBOM

Elastx tillstyrker bestämmelserna om öppen källkod och programvarudelning i artiklarna 43 och 44 samt SBOM-kraven i bilaga II. Elastx plattform bygger i sin helhet på öppen källkod, och det är i praktiken detta som gör operativt oberoende och leverantörsbyten möjliga: kompetensen finns brett på marknaden och tjänsterna har motsvarigheter hos andra leverantörer. Öppen källkod och öppna standarder är därmed inte ett sidospår i förordningen utan en förutsättning för att både diversifierings- och portabilitetsmålen ska kunna nås.

Samtidigt bör kraven riktas mot förmåga snarare än enbart tillgång: tillgång till källkod ger inte automatiskt operativt oberoende. Det som bör efterfrågas är leverantörens faktiska förmåga att granska, underhålla och vid behov ersätta de komponenter tjänsten bygger på.

Detta bör även gälla förordningens egna strukturer. Den gemensamma tjänsteplattform som byggs upp inom den europeiska molnfederationen bör strikt baseras på öppen källkod och öppna standarder, med portabilitet som designkrav från början. Annars riskerar federationen att själv bli en ny inlåsningspunkt, tekniskt och organisatoriskt, i stället för det resursutbyte den är avsedd att möjliggöra.

Ett konkret område där öppna standarder behöver kompletteras med praktisk interoperabilitet är identitets- och åtkomsthantering. Etablerade öppna standarder finns, till exempel OIDC och SAML, men roller och behörigheter är utformade olika även mellan standardbaserade lösningar, vilket gör att åtkomstmodeller i praktiken måste byggas om vid varje byte och utgör ett av de större enskilda hindren för både byte och parallell drift. Interoperabel identitets- och åtkomsthantering bör därför pekas ut som ett prioriterat område i det interoperabilitetsarbete som förordningen initierar.

9. Efterfrågesidan: offentlig upphandling och kopplingen till Cybersäkerhetslagen

Elastx tillstyrker att offentlig upphandling används som motor. Det är efterfrågan i skala som ger europeiska leverantörer den volym som gör dem trovärdiga alternativ även för privata kunder; utan efterfrågesidan förblir kapacitetsbygget ett utbud utan marknad. Kravet att upphandlande myndigheter som lägst ska använda tjänster på nivå 1 är en rimlig utgångspunkt.

Möjligheten i artikel 31(3) att utsträcka suveränitetsbedömningarna till privata väsentliga entiteter i sektorer med hög kritikalitet pekar enligt Elastx i rätt riktning. För verksamheter som omfattas av Cybersäkerhetslagen (NIS2) är frågorna om ägande, administration och jurisdiktion lika relevanta som för offentlig sektor, och flera av Elastx kunder ställer redan idag motsvarande krav på eget initiativ. En sådan utvidgning behöver dock förutsebarhet: tydliga kriterier, rimliga övergångstider och skydd för löpande avtal. Berörda verksamheter gör klokt i att genomföra bedömningen frivilligt redan nu; blir den senare obligatorisk är arbetet då redan gjort.

Utvidgningen bör också samordnas med befintliga regelverk. De riskbedömningar och granskningar som verksamheter och leverantörer redan genomför enligt Cybersäkerhetslagen och Lagen om motståndskraft hos kritiska verksamhetsutövare (CER) bör kunna återanvändas som underlag för suveränitetsbedömningen enligt förordningen, så att samma beroende inte behöver dokumenteras flera gånger enligt olika metoder och inför olika myndigheter. Det håller nere den administrativa bördan för både kunder och leverantörer och följer samma princip om återanvändning av bevis som Elastx förordar i avsnitt 5.

10. Sammanställning av förslag

1. Villkoren för tredjelandserkännande enligt artikel 18 förtydligas i grundakten eller skälen så att extraterritoriell lagstiftning som ger tredjelands myndigheter åtkomst till data oavsett lagringsplats utesluter erkännande.
2. Erkännandebeslut enligt artikel 18 föregås av en offentlig, motiverad analys mot samtliga villkor, omprövas när tredjelandets lagstiftning ändras och förenas med en reglerad övergångsperiod för löpande avtal vid återkallelse.

3. Anpassade erbjudanden där driften paketerats i en europeisk struktur men den faktiska kontrollen kvarstår hos en tredjelandskoncern ska inte kunna kvalificera för nivå 3; prövningen i bilaga III ska avse faktisk kontroll.
4. Självdeklarationer på nivå 1 förenas med stickprovstillsyn och sanktioner vid oriktiga uppgifter.
5. Efterlevnad redovisas områdesvis, inte enbart som en sammanvägd nivå.
6. I väntan på en antagen europeisk certifieringsordning erkänns etablerade internationella standarder, exempelvis ISO/IEC 27001 med 27017 och 27018 kompletterat med oberoende bestyrkande, som interimsbevis för nivå 2 och 3.
7. Certifierings- och revisionskrav utformas proportionerligt i förhållande till leverantörens storlek och riskprofil, med möjlighet att återanvända bevis mellan ordningar.
8. Rimliga migrationsfrister och övergångsstöd införs för små och medelstora SaaS-leverantörer som idag bygger på utomeuropeisk infrastruktur.
9. Reglerna för accelerationszoner för datacenter utformas så att tillstånd, nätanslutning och eleffekt kommer en mångfald av aktörer till del, inklusive oberoende colocationanläggningar, så att kapacitetsbygget inte i praktiken förbehålls de största aktörernas egna anläggningar.
10. Medlemsstaterna ges uttrycklig möjlighet att använda suveränitetsnivåerna som prioriteringskriterium vid tilldelning av knapp nätkapacitet och eleffekt i accelerationszonerna, så att den fysiska resursen styrs mot tjänster som uppfyller ramverkets krav i stället för att fördelas enligt först till kvarn-principen.
11. Nivåkraven kompletteras med krav på dokumenterad och regelbundet prövad exit- och migrationsförmåga, med genomförda tester som revisionsbevis.
12. Transparenskraven i artikel 23 utvidgas till prismodeller och avtalsvillkor: kostnader inklusive avgifter för utgående datatrafik ska kunna förutses och jämföras, och villkor som volymåtaganden, automatiska förlängningar, diskriminerande licensvillkor och tillgodohavanden som förverkas vid uppsägning ska redovisas öppet.
13. Löpande datatrafik mellan leverantörer vid parallell användning behandlas som en portabilitetsfråga, så att diversifiering genom flera leverantörer inte motverkas av löpande överföringskostnader.
14. En dokumenterad stegvis migration omfattas av samma avgiftsskydd som ett fullständigt byte, bedömt per tjänst och arbetslast, så att avgiftsfriheten vid byte inte kan kringgås genom att kunden under en övergångstid behåller enstaka deltjänster hos den tidigare leverantören.
15. Interoperabel identitets- och åtkomsthantering enligt öppna standarder pekas ut som prioriterat område i förordningens interoperabilitetsarbete.
16. Den gemensamma tjänsteplattformen inom den europeiska molnfederationen baseras strikt på öppen källkod och öppna standarder, med portabilitet som designkrav.
17. Öppna gränssnitt och tillgång till beräkningskapacitet behandlas som portabilitets- och konkurrensfrågor även för AI-tjänster.

18. Kunddata får inte användas för träning av leverantörens AI-modeller utan kundens uttryckliga och specifika förhandsgodkännande; skyddet gäller oavsett nivå och oavsett leverantörens ursprung.
19. Nivå 1 som lägsta nivå i offentlig upphandling behålls; en utvidgning till privata väsentliga entiteter enligt artikel 31(3) förenas med tydliga kriterier, rimliga övergångstider och skydd för löpande avtal.
20. Riskbedömningar och granskningar som redan genomförts enligt Cybersäkerhetslagen och Lagen om motståndskraft hos kritiska verksamhetsutövare ska kunna återanvändas som underlag för suveränitetsbedömningen enligt förordningen, så att samma beroende inte dokumenteras flera gånger enligt olika metoder.

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

Joakim Öhman, VD

Elastx AB (org.nr 556906-5617)
Kungsgatan 9, 111 43 Stockholm
E-post: info@elastx.se