

Eesti seisukohad Euroopa Liidu pilvetehnoloogiate ja tehisaru arendamise õigusakti eelnõu kohta

Lisa 1. Kaasamise käigus esitatud tagasiside arvestamise tabel

Ettepaneku esitaja	Ettepanek	Arvestamine
Amazon Web Services	Reorient the framework from origin-based restrictions toward outcome-based requirements. Rather than prescribing who a provider must be, the regulation should define what a provider must demonstrably deliver: verifiable data control, operational continuity, jurisdictional safeguards, and transparency.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.2
	Ensure coherence between the investment framework (Title II/III) and the sovereignty framework (Title IV). The regulation should reward long-term investment, favour collaboration with all providers demonstrating verifiable compliance with technical security, operational continuity, and sustainability requirements.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.2
	CADA should establish harmonised minimum designation criteria at EU level, preserving Member State flexibility to add incentives above the baseline while ensuring cross-border consistency. Zone criteria must incorporate demand-side signals — customer proximity, workload geography, connectivity to existing digital infrastructure — alongside supply-side factors such as grid capacity, renewable potential, and brownfield availability.	Osaliselt arvestatud seisukohapunktis 6.8
	Harmonized minimum sustainability thresholds should be set at EU level, anchored in the DC Rating Scheme methodology, ensuring consistent treatment across Member States. Eligibility should be conditioned only on KPIs with agreed definitions and mature calculation methodologies — excluding metrics still under development or lacking cross-facility comparability.	Osaliselt arvestatud seisukohapunktis 6.8
	CADA must provide exhaustive documentation checklists, explicit procedural steps with defined responsibilities at each stage, and clear rules on completeness assessment to prevent indefinite pre-application cycles. CADA, the Environmental Omnibus, and the Energy Grid Package must function as a synchronized delivery system, with implementing guidance specifying how timelines across these instruments interact within acceleration zones.	Osaliselt arvestatud seisukohapunktis 6.8
	Designation criteria must reward what a project delivers — investment scale, grid contribution, sustainability performance, local economic value, skills development — not where components originate or where a provider is headquartered. Strategic autonomy is demonstrated through operational integration, contractual commitments, and economic contribution to the EU — not through supply chain mandates that reduce competition and increase costs without improving security of supply.	Osaliselt arvestatud seisukohapunktis 6.8
	Aggregate EU capacity gap monitoring should rely on anonymized, Commission-collected infrastructure data — not operator-level workload disclosure that exposes competitive positioning. Where performance-based indicators are needed to supplement infrastructure metrics, the framework should	Arvestatud seisukohapunktis 6.1 / 6.8

reference methodologies under active development through recognized standardization bodies (such as SPEC) designed for cross-facility comparability without requiring workload-level transparency.	
Redefine UALs 3–4 around verifiable risk mitigation controls rather than corporate nationality. Sovereign operating models, dedicated EU regions, and disconnected solutions should be recognized as legitimate pathways to the highest assurance levels. Introduce data classification guidance that prevents the 'high-water mark' effect — requiring contracting authorities to segment workloads by actual data sensitivity rather than applying the highest applicable UAL across an entire system.	Osaliselt arvestatud seisukohapunktis 6.1
Redefine UALs 3–4 around verifiable risk mitigation controls rather than corporate nationality. Sovereign operating models, dedicated EU regions, and disconnected solutions should be recognized as legitimate pathways to the highest assurance levels. The feasibility of a fully EU-controlled software supply chain at Level 4 should be critically assessed — no cloud service operates on a purely EU-origin stack, and the requirement creates a paradox with CADA's own innovation objectives under Title II.	Osaliselt arvestatud seisukohapunktis 6.1
Data residency requirements should be proportionate to data sensitivity and address a risk. For non-sensitive or public data, there should be a UAL 0, whereby customers can continue to use public cloud services without any additional restrictions. The data residency requirements could require maintaining a copy of customer data available in the EU for sovereignty and operational continuity. For data residency requirements at higher assurance levels, the scope of data should be made explicit as the customer content and all metadata as processed by customers.	Osaliselt arvestatud seisukohapunktis 6.9
Requirements regarding technical and organizational measures to mitigate risks related to extra-territorial reach of foreign jurisdictions should be the same for EU and non-EU providers to align with proportionality and non-discrimination principles. Required evidence in Annex III should provide clarity for providers and auditors as regards what is considered sufficient. The 'prove a negative' burden should be reframed as a positive demonstration of implemented safeguards, with a rebuttable presumption that providing listed Annex III evidence is sufficient unless a specific, documented gap is identified.	Osaliselt arvestatud seisukohapunktis 6.9
Include GPA/FTA partners by default in UAL-3, with the Commission retaining power to suspend recognition where specific conditions are met (opt-out model, consistent with the Industrial Accelerator Act and Chips Act 2). Alternatively, revise criteria (b)–(d) to focus on whether adequate procedural safeguards and judicial oversight exist — not on the absence of any legal mechanism for government access or administrative action, which most democratic countries maintain.	Osaliselt arvestatud seisukohapunktis 6.1
SBOM and source code audit requirements should be scoped to components material to service delivery through a risk-based threshold. Equivalent assurance mechanisms should be accepted; scope SBOM to runtime components material to service delivery. Source code audit requirement for third-country software components should be replaced with assurance-based evidence. Scope migration planning to components material to service delivery.	Osaliselt arvestatud seisukohapunktis 6.9
Implementing guidance should establish that provision of all listed Annex III evidence creates a rebuttable presumption of compliance; any request for additional evidence must be justified with reference to a specific criterion and a documented gap, and alternative evidence demonstrating equivalent	Arvestatud seisukohapunktis 6.9

	assurance must be accepted where a listed item is unavailable in the prescribed form. The evaluating NCA's role should be scoped proportionately to the UAL tier: at UAL-2 and above, limited to reviewing the auditor's opinion, methodology, and conclusions rather than re-examining underlying provider evidence; at UAL-1, reflecting the tier's self-assessment nature.	
	Clarify that the evidence in Annex III constitutes the defined standard; auditors should assess compliance against these listed criteria. Any request for additional evidence beyond Annex III should be justified with reference to a specific criterion and a documented gap. Accept alternative evidence demonstrating equivalent assurance where a prescribed form is unavailable.	Arvestatud seisukohapunktis 6.9
	Include the risk assessment methodology as an Annex to the regulation rather than delegating it to a post-adoption implementing act. This ensures the methodology is subject to full co-legislative scrutiny, stakeholder consultation during the ordinary legislative procedure, and democratic accountability — rather than being determined unilaterally by the Commission after the political negotiations have concluded. Remove or limit the Commission's override power in Article 29(5) to cases with a demonstrated, specific risk and a proportionality test.	Osaliselt arvestatud seisukohapunktis 6.2
	Remove or limit the Commission's override power in Article 29(5) to cases with a demonstrated, specific risk and a proportionality test. Member States are best placed to assess the sensitivity of their data and the specific risks to their public order.	Osaliselt arvestatud seisukohapunktis 6.2
	Introduce a risk mitigation menu in Article 30 that allows contracting authorities to deploy alternative or complementary mitigation measures — including multi-cloud strategies, contractual exit plans, continuity commitments, and technical controls — as legitimate alternatives to mandating a higher UAL. Provider restriction should be a last-resort measure, applied only where a specific risk cannot be adequately mitigated through other means.	Osaliselt arvestatud seisukohapunktis 6.2
	Delete Article 31(3) or convert to ordinary legislative procedure. If retained, require: (i) mandatory public consultation; (ii) quantified impact assessment covering costs to affected sectors, effects on competition and competitiveness, and coherence with existing frameworks (NIS2, DORA, CSA); (iii) materiality threshold — act only where a specific demonstrated risk exists.	Arvestatud seisukohapunktis 6.10
	Critical design elements that determine market access — particularly the risk assessment methodology and the criteria for extending requirements to the private sector — should be included in the base regulation text or its Annexes, subject to ordinary legislative procedure. Where delegation is genuinely necessary for technical updates, require mandatory public consultation and impact assessment before adoption.	Arvestatud seisukohapunktis 6.10
Eesti Teadusagentuur	Teadusandmete (eriti tundlike, nt terviseandmete) turvaline taaskasutamine on teadustööks ja innovatsiooniks suure tähtsusega. Samas tuleb tagada, et uued tehnilised või regulatiivsed nõuded ei tekitaks teadlastele ja teadusasutustele ebamõistlikku haldus- ega finantskoormust.	Arvestatud seisukohapunktis 6.1
	Ülikoolidest võrsuvate süvatehnoloogia idu- ja hargettevõtete (spin-offide) toetamine on Eesti teadmussiirde vaatest võtmetähtsusega. Peame vajalikuks rõhutada, et loodavad AI kiirenduskeskused	Osaliselt arvestatud seisukohapunktis 6.1 / 6.7

	teeksid tihedat institutsionaalset koostööd just ülikoolide ja teadusasutustega, et toetada teaduspõhise majanduse kasvu.	
	Kuna CADA algatusi toetatakse osaliselt programmi Horizon Europe eelarvest, on oluline jälgida, et uued eesmärgid ja suured väljakutsed ei vähendaks fundamentaalselt teiste oluliste teadusvaldkondade rahastust programmi siseselt, vaid looksid uut lisandväärtust. Samuti tuleb tagada 'grand challenges' tingimuste seadmisel väikeriikide teadusasutustele võrdsed osalemisvõimalused.	Arvestatud seisukohapunktis 6.1 / 6.7
	ETAG toetab piiriüleste teadusprojektide edendamist ressursside koondamise teel. Kuid juhime tähelepanu, et suurprojektides ja EDIC-ites nõutav omafinantseering või ressursside maht võib osutuda Eesti-suguse väikeriigi ja meie teadusasutuste jaoks osalemisbarjääriks. Kriteeriumites ja rahastusmodelites peab arvestama väiksemate riikide osalemisvõimekusega.	Arvestatud seisukohapunktis 6.7
	Rangete suveräänsusnõuete (eriti usaldusväärsuse tasemetel 3 ja 4) ja riskihindamiste laiendamine teadusasutuste infosüsteemidele võib tuua kaasa ulatusliku haldus- ja finantskoormuse. Ranged piirangud andmete majutamisele või kolmandate riikide teenuste kasutamisele võivad negatiivselt mõjutada rahvusvahelist teaduskoostööd (sh riikidega väljaspool EL-i, näiteks USA-ga). Riskihindamiste raamistikus tuleb teadustegevuse (va riigisaladus/kaitsevaldkond vms) puhul säilitada paindlikkus.	Arvestatud seisukohapunktis 6.2
	Oluline on aga tagada, et uue repositooriumiga liitumine oleks tehniliselt lihtne ning teadusasutustele pakutaks selleks vajalikku tehnilist ja õiguslikku tuge.	Arvestatud seisukohapunktis 6.5
Google	Üldine: toetada täpsustustega. Google tervitab meetmeid, mis aitavad kiirendada jätkusuutliku andmekeskuste taristu loomist ja toetada Euroopa tehisintellekti ja pilveteenuste mahutavuse vajadusi. On oluline, et kiirendustsoonid toetaksid elujõulisi projekte, mis aitavad edendada nii andmetaristu kui ka jätkusuutlikkuse eesmärgi. Google toetab kiirendustsoonide kontseptsiooni, tingimusel et neid kasutatakse elujõuliste ja jätkusuutlike andmekeskuste projektide hõlbustamiseks. Kiirendustsoonide olemasolu ei tohiks aga piirata uute asukohtade geograafilist asukohta. Artikli 10(1)(f) kohta – Google tervitab meetmeid andmekeskuste projektide lubade andmise sujuvamaks muutmiseks. Kiirem ja prognoositavam lubade andmine saab toetada kiiresti vajalikke investeeringuid Euroopa andmetaristusse. Artikli 10(1)(h) kohta – asukoha/piirkonna jätkusuutlikkus – toetada selgitustega – Google toetab andmekeskuste jätkusuutlikkuse eesmärgi. Jätkusuutlikkuse kriteeriumid peaksid olema kooskõlas tulevase ELi-ülese jätkusuutlikkuse hindamissüsteemiga ega tohiks karistada tõhusaid tehnoloogiaid.	Arvestatud seisukohapunktis 6.8
	Google toetab andmekeskuste projektide energiavajaduse paremat planeerimist. Võrgu planeerimine ja jätkusuutlik taristu on Euroopa tehisintellekti ja pilveteenuste võimsuse jaoks kriitilise tähtsusega. Google tervitab keskendumist võrgu planeerimisele ja ühendustele. Võrgule juurdepääsu hõlbustamine, paindlikud ühenduslepingud ja PPA-de kasutuselevõtt kiirendustsoonides aitavad kaasa jätkusuutlikele investeeringutele andmekeskustesse.	Osaliselt arvestatud seisukohapunktis 6.8
	Toetada selgitustega – Google toetab andmekeskuste ruumilise planeerimise ja taristu planeerimise paremat koordineerimist. Toetusmeetmed ei tohiks piirduda ainult kiirendustsoonides asuvate projektidega.	Osaliselt arvestatud seisukohapunktis 6.8

Google toetab ametiasutuste, põhivõrguettevõtjate ja jaotusvõrguettevõtjate vahelist koostööd, kuna võrgule juurdepääs on andmekeskuste juurutamise peamine praktiline tegur.	Osaliselt arvestatud seisukohapunktis 6.8
Toetada selgitustega – Google toetab andmekeskuste jätkusuutlikkuse nõudeid, tingimusel, et need on kooskõlas tulevase ELi-ülese jätkusuutlikkuse hindamissüsteemiga. Raamistik ei tohiks karistada kõige energiatõhusamaid jahutustehnoloogiaid, näiteks vesijahutust, kui need on asjakohased.	Osaliselt arvestatud seisukohapunktis 6.8
Artikkel 12 üldiselt – Google tervitab haldusmeetmeid, mis lihtsustavad andmekeskuste projektide elluviimist, sealhulgas lubade ja võrguga ühendamise menetluste koordineerimist. Artikkel 12(1) – Google toetab ühtset teabepunkti, mis saab andmekeskuste operaatoreid kogu projekti elutsükli vältel abistada.	Osaliselt arvestatud seisukohapunktis 6.8
Artikkel 12(2)(a) – ruumiline planeerimine ja ehitusload – Google toetab andmekeskuste projektide ruumilise planeerimise ja ehituslubade menetluste koordineerimist. Artikkel 12(2)(b) – keskkonnamõju hindamine – Google toetab koordineeritud keskkonnamõju hindamise menetlusi, tingimusel et need jäävad prognoositavaks ja proportsionaalseks. Artikkel 12(2)(c) – vesi, reovesi, soojuse kasutamine ja taaskasutamine – toetada selgitustega – Google toetab andmekeskuste jätkusuutlikkusega seotud lubade, sealhulgas vee kasutamise ja soojuse taaskasutamise, koordineerimist. Jätkusuutlikkuse eeskirjad ei tohiks karistada tõhusaid jahutustehnoloogiaid, näiteks vesijahutust. Artikkel 12(2)(d) – haldus- ja aruandluskohustused – Google toetab koordineerimist, mis vähendab andmekeskuste projektide halduslikku keerukust. Artikkel 12(2)(f) – elektri-, soojus- ja sidevõrgud – Google tervitab keskendumist võrgu planeerimise ja ühenduste hõlbustamisele andmekeskuste projektide puhul.	Arvestatud seisukohapunktis 6.1 / 6.8
Artikkel 13 üldiselt – toetada koos selgitustega – Google tervitab kavatsust kasutada strateegilise projekti staatust lubade andmise ja võrgule juurdepääsu sujuvamaks muutmiseks. Need eelised tuleks reserveerida elujõulistele projektidele, mis toetavad Euroopa jätkusuutlikkuse ja andmetaristu vajadusi. Artikkel 13(1) – toetada koos selgitustega – Google toetab kiirendustsoonides asuvate andmekeskuste projektide strateegilise projekti staatust, tingimusel et see ei piira uute asukohtade geograafilist asukohta. Sarnaseid toetavaid meetmeid tuleks vajaduse korral laiendada ka väljaspool kiirendustsoone tegutsevatele andmekeskustele.	Osaliselt arvestatud seisukohapunktis 6.8
Google toetab meetmeid, mis lihtsustavad andmekeskuste projektide lubade väljastamist.	Osaliselt arvestatud seisukohapunktis 6.8
Google toetab andmekeskuste projektidele õigeaegset ja prognoositavat lubade väljastamist.	Osaliselt arvestatud seisukohapunktis 6.8
Artikkel 16 üldiselt - muuta - Google tervitab Euroopa lähenemisviisi ühtlustamist pilvesuveräänsuse suhtes. Liidu usaldusväärse tasemed ei tohiks aga luua ülemaailmsetele pakkujatele suuri takistusi ega eirata seda, kuidas ülemaailmsed tarneahelad ja küberturvalisuse funktsioonid praktikas toimivad. Artikkel 16(1) - muuta - suveräänsuse raamistik peaks põhinema avatud suveräänsusel, partnerlusel ja ausal konkurentsil. Nõuded peaksid võimaldama usaldusväärsetel globaalsetel partneritel panustada Euroopa kontrolli ja vastupidavusse, mitte jätma nad olulistest turuosadest välja.	Osaliselt arvestatud seisukohapunktis 6.1

	<p>Muuta – kõik liidu usaldusväärse tasemete ja nendega seotud tõendusnõuete muudatused peaksid jätma ruumi innovatsioonile ja alternatiivsetele tehnilistele leevendusmeetmetele. Google soovib binaarsete jah/ei kriteeriumide asemel punktisüsteemil põhinevat lähenemisviisi.</p>	<p>Osaliselt arvestatud seisukohapunktis 6.1 / 6.9 / 6.10</p>
	<p>Artikkel 18 - muuta - Google on mures ettepaneku piirava lähenemisviisi pärast ELi-väliste riikide suhtes suveräänse sertifitseerimise raamistikus. Koostöö usaldusväärsete globaalsete partneritega on Euroopa heaolu, turvalisuse, innovatsiooni ja tehisintellekti suutlikkuse jaoks kriitilise tähtsusega. Artikkel 18(1) - muuta - raamistik ei tohiks luua usaldusväärsete ELi-väliste teenusepakkujate välistamist. Piirangud peaksid olema sihipärased ja riskipõhised, mitte aga laiaulatuslike tõkete kehtestamine ülemaailmsetele teenusepakkujatele. Artikkel 18(1)(b) - vajab muutmist - kolmandate riikide juurdepääsu ja jurisdiktsioonilise riski hindamisel tuleks arvesse võtta tehnilisi kontrollimeetmeid ja leevendusmeetmeid. Google soovib punktisüsteemi, mis tunnustab alternatiivseid viise suveräänsusprobleemide lahendamiseks, sealhulgas kliendi kontrollitavaid krüpteerimisvõtmeid. Artikkel 18(1)(c) - muuta - teenuse katkemise riski hindamine peaks võimaldama teenusepakkujatel näidata tõhusaid tehnilisi ja operatiivseid leevendusmeetmeid. Raamistik ei tohiks tugineda ainult teenusepakkuja päritolule või kolmanda riigi kontrollile. Artikkel 18(1)(d) - Google toetab juurdepääsu tagamist tippasemel tehnoloogiatele ja teenustele. Välistav lähenemisviis võib Euroopat innovatsioonist ja andmeinfrastruktuuri kasvust isoleerida. Artikkel 18(1)(e) – Google toetab avatust ja partnerlust osana Euroopa tehnoloogilise suveräänsuse strateegiast.</p>	<p>Arvestatud seisukohapunktis 6.7</p>
	<p>Artikkel 20 üldiselt - vajab muutmist - kuivõrd auditiprotsess rakendab liidu usaldusväärse tasemeid binaarsete jah/ei kriteeriumidena, soovib Google punktisüsteemil põhinevat lähenemisviisi. Teenusepakkujad peaksid suutma demonstreerida erinevaid ja tõhusaid leevendusmeetmeid sõltumatusena seotud probleemide lahendamiseks. Artikkel 20(1) - vajab muutmist - Google on mures, et kumulatiivsed kriteeriumid erinevate usaldusväärse tasemete vahel ei pruugi jätta piisavalt ruumi innovatsioonile või alternatiivsetele tehnilistele kontrollidele. Kõrgemat usaldusväärset peaks olema võimalik demonstreerida tõhusate tehniliste, organisatsiooniliste ja lepinguliste kaitsemeetmete abil.</p>	<p>Arvestatud seisukohapunktis 6.1 / 6.9</p>
	<p>Artikli 20 lõike 5 punktid g–i – muuta – Google soovib vältida puhtalt binaarset jah/ei hindamismudelit. Suveräänse kontrolli ja kolmandate isikute juurdepääsu ning jurisdiktsioonilise riski vahelist seost tuleks hinnata hindamiskriteeriumide abil, mis tunnustavad tõhusaid tehnilisi leevendusmeetmeid.</p>	<p>Osaliselt arvestatud seisukohapunktis 6.9</p>
	<p>Artikkel 29 üldiselt - vajab muutmist - Google on mures, et suveräänse sertifitseerimise raamistik võib takistada liikmesriikide võimet korraldada hankeid oma riigi julgeolekuhuvides. Liikmesriikidel peaks olema kaalutusõigus hinnata oma vajadusi, eriti tundlikes valdkondades. Artikkel 29(1)(b) - vajab muutmist - Liidu usaldusväärse taseme valik peaks olema riskipõhine ja peaks tunnustama tehnilisi leevendusmeetmeid. See ei tohiks automaatselt kaasa tuua usaldusväärsete globaalsete partnerite välistamist, kui suveräänseid probleeme saab lahendada tehniliste kontrollimeetmete abil.</p>	<p>Osaliselt arvestatud seisukohapunktis 6.2</p>
	<p>Artikkel 29(2)(b) - vajab muutmist - kolmandate riikide juurdepääsuriski tuleks hinnata hindamiskriteeriumide abil ja see peaks arvestama tehniliste kontrollimeetmetega, näiteks kliendi</p>	<p>Osaliselt arvestatud seisukohapunktis 6.2</p>

kontrollitavate krüpteerimisvõtmetega. Google märgib, et tema krüpteerimismeetod võib võimaldada klientidel võtmeid pilveväliselt salvestada, mistõttu on Google'il tehniliselt võimatu võtit nõudmisel anda. Artikkel 29(2)(c) - vajab muutmist - teenuse katkemise riski tuleks hinnata tegelike tehniliste ja operatiivsete leevendusmeetmete valguses, mitte ainult päritolupõhiste kriteeriumide alusel.	
Muuta – Komisjoni metoodika peaks jätma ruumi liikmesriikide hindamiseks ega tohiks sundida rakendama liiga jäika või vaikumisi suurima kindluse nõudvat lähenemisviisi.	Osaliselt arvestatud seisukohapunktis 6.2
Kustutada / oluliselt piirata – Google soovib kaotada komisjoni volitused tühistada liikmesriikide otsuseid riigiriski hindamise raames. Varuvariandina peaks see volitus olema rangelt piiratud ning selle suhtes tuleks läbi viia ulatuslikud konsultatsioonid ja nõuetekohane menetlus.	Arvestatud seisukohapunktis 6.2
Artikkel 30 üldiselt - muuta - Google on mures, et kavandatud suveräänsed kriteeriumid võivad jätta ELi-välised teenusepakkujad märkimisväärselt turuosast välja ning vähendada avaliku sektori ja kriitiliste teenuste kasutajate valikuvõimalusi. Riigihanke-eeskirjad peaksid toetama avatust, koostalitlusvõimet ja konkurentsi.	Osaliselt arvestatud seisukohapunktis 6.2
Muuta - kui avaliku sektori asutused on kohustatud hankima UAL 1 teenuseid, ei tohi UAL 1 sisaldada nõudeid, mis häirivad olulisi globaalseid küberturvalisuse funktsioone, näiteks telemeetria ja küberohtude mustrite lokaliseerimist	Arvestatud seisukohapunktis 6.2
Muuta – UAL 2, 3 või 4 teenuste kohustuslik kasutamine tundlike avaliku sektori tegevuste jaoks võib luua kahetasandilise turu, kus avaliku sektori ja avaliku julgeoleku organisatsioonidel on innovatsioonile piiratud juurdepääs. Nõuded ei tohiks vaikumisi välistada usaldusväärseid globaalseid partnereid.	Osaliselt arvestatud seisukohapunktis 6.2
Muuta – erandid peaksid olema praktilised ja võimaldama hankijatel hankida asjakohaseid teenuseid olukorras, kus UAL-i tunnustatud alternatiivid ei ole kättesaadavad, ei sobi või tekitaksid ebaproportsionaalseid piiranguid innovatsioonile, turvalisusele või konkurentstile. Artikli 30 lõike 4 punkt a – muuta – piisava alternatiivi olemasolu hindamisel tuleks arvestada funktsionaalsuse, turvalisuse, innovatsiooni, koostalitlusvõime ja tipptasemel tehnoloogiale juurdepääsuga, mitte ainult UAL-i ametliku tunnustusega.	Arvestatud seisukohapunktis 6.7
Artikkel 31 üldiselt – selgitada/muuta – Google on mures, et suveräänsusnõuete ulatus on ebaselge ja võib hõlmata eraettevõtteid, millel on potentsiaalne mõju avalikule korrale. See võib hõlmata suurt osa Euroopa majandusest, sealhulgas pangandust, energeetikat ja kommunaalteenuseid.	Arvestatud seisukohapunktis 6.10
Muuta – kui komisjon saab laiendada mõju hindamise või leevendamise nõudeid erasektori üksustele kriitilise tähtsusega sektorites, tuleks seda selgitada ja hoolikalt piirata. Vastasel juhul võib ettepanek tekitada ebakindlust ülemaailmsete tarneahelatega Euroopa ettevõtete jaoks.	Arvestatud seisukohapunktis 6.10
Artikkel 32 üldiselt – toetada ja tugevdada – Google toetab riigihangete reforme, mis väärtustavad hinnaväliseid kriteeriume, nagu innovatsioon, jätkusuutlikkus ja koostalitlusvõime. CADA peaks hankeid kasutama avatud tehnoloogia kasutuselevõtu ja avaliku sektori ümberkujundamise edendamiseks. Artikkel 32(1) – toetada ja tugevdada – hinnavälised hankekriteeriumid peaksid hõlmama koostalitlusvõimet, kaasaskantavust, turvalisust, jätkusuutlikkust, innovatsiooni ja võimet toetada mitme pilve arhitektuuri. See aitaks vältida tarnija seotust ja võimaldaks moderniseerimist. CADA peaks võtma	Osaliselt arvestatud seisukohapunktis 6.6

rangemaid meetmeid tarkvaralitsentside seotuse vastu võitlemiseks. See peaks hõlmama litsentside täielikku kaasaskantavust domineerivatelt pilvedelt konkureerivatele pilvedele, domineerivate pilvede tarkvaralitsentside mittediskrimineerivat hinnakujundust ning tarkvara ja turvalisuse samaväärsust olenemata kasutatavast pilveplatvormist. Riigihanked peaksid tegelema kontsentratsiooniriskiga struktuurilisel tasandil koostalitlusvõime ja avatud tehnoloogia kaudu. Geograafilised või päritolupõhised kriteeriumid ei tohiks olla peamine tee suveräänse kontrolli saavutamiseks.	
Google toetab CADA raames avatud ja koostalitlusvõimelise ökosüsteemi edendamise meetmeid.	Osaliselt arvestatud seisukohapunktis 6.6
Artikkel 37 üldiselt – toetada ja tugevdada – Google toetab riigihangete reforme, mis edendavad avatud tehnoloogia kasutuselevõttu, koostalitlusvõimet ja avaliku sektori ümberkujundamist. Ühis- või tsentraliseeritud hanked peaksid vältima tarnija seotust ja toetama mitme-pilve arhitektuure. Artikkel 37(1) – toetada koos selgitustega – kui komisjon hangib pilve-, tarkvara- või tehisintellekti süsteeme, peaksid hankekriteeriumid hõlmama innovatsiooni, jätkusuutlikkust, koostalitlusvõimet ja turvalisust, mitte tuginema peamiselt geograafilistele kriteeriumidele.	Osaliselt arvestatud seisukohapunktis 6.6 / 6.12
Liidu usaldusväärsuse taseme kriteeriumid peaksid jätma ruumi innovatsioonile ja pakkuma teenusepakkujatele erinevaid ja tõhusaid leevendusi suveräänsusprobleemidele. Google soovib tehniliste kriteeriumide puhul binaarse jah/ei lähenemisviisi asemel punktisüsteemi.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.9
Muuta – suveräänse kontrolli ja kolmandate osapoolte juurdepääsu vahelise seose ning jurisdiktsioonilise riski hindamine peaks toimuma punktisüsteemi alusel. Raamistik peaks tunnustama tehnilisi meetmeid, näiteks kliendi kontrollitavaid krüpteerimisvõtmeid, sealhulgas mudeleid, kus kliendid salvestavad krüpteerimisvõtmeid pilveväliselt.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.2 / 6.9
Muuta – kriteeriumid ei tohiks välistada usaldusväärsete globaalsete partnerite osalemist Euroopa turu olulistest osades. Koostöö usaldusväärsete globaalsete partneritega on Euroopa heaolu, turvalisuse ja tehisintellekti kasvu jaoks kriitilise tähtsusega.	Osaliselt arvestatud seisukohapunktis 6.1
Muuta – kriteeriumid peaksid kajastama, kuidas globaalsed tarneahelad ja küberturvalisuse funktsioonid praktikas toimivad. Liiga jäigad nõuded võivad häirida nii ELi-väliseid ettevõtjaid kui ka Euroopa teenusepakkujaid, kes sõltuvad ülemaailmsetest tarneahelatest.	Osaliselt arvestatud seisukohapunktis 6.1
Muuta – UAL 1 ei tohiks takistada oluliste küberturvalisuse funktsioonide täitmist kogu maailmas. Isegi madalaima usaldusväärsuse taseme korral võib ettepanek häirida ülemaailmseid küberturvalisuse toiminguid.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.9
Kustutada/kitsendada– Google soovib eemaldada UAL 1 ja UAL 2 metaandmete ja telemeetria lokaliseerimise nõuded. Nõue, et kogu telemeetria, sealhulgas küberohtude mustrid, jääksid Euroopasse, takistaks oluliste küberturvalisuse funktsioonide täitmist kogu maailmas.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.2
Muuta – UAL 2 peaks võimaldama usaldusväärsetel teenusepakkujatel demonstreerida tõhusaid suveräänsuse leevendamise meetmeid tehniliste ja korralduslike kontrollide abil. Hindamisel tuleks kasutada punktikriteeriume, mitte binaarseid tehnilisi kriteeriume.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.2 / 6.9

	Kustutada/kitsendada – Google soovib UAL 2-s metaandmete ja telemeetria lokaliseerimisnõuded eemaldada. Küberturvalisus sõltub võimest analüüsida globaalseid ohumustreid ja hallata globaalseid turbefunktsioone.	Osaliselt arvestatud seisukohapunktis 6.1
	Kustutada/muuta – Google soovib UAL 2-st eemaldada nõuded kolmandate riikide operaatoritele. Sellised nõuded tuleks kehtestada ainult erandkorras, kui komisjon seab konkreetse teenusepakkuja puhul piirangu kolmandale päritoluriigile.	Osaliselt arvestatud seisukohapunktis 6.1
	Muuta – Google soovib asendada binaarsed kriteeriumid punktisüsteemiga, mis võimaldab teenusepakkujatel näidata samaväärseid või tõhusamaid meetmeid suveräänsusprobleemide leevendamiseks.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.2 / 6.9
	Oluliselt muuta – Google on mures, et UAL 3 loob vaikimisi keelu ELi mittekuuluvate riikide operaatoritele, mille tühistada saab ainult komisjon. See lähenemisviis tuleks ümber pöörata.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.9
	Vaikimisi sätete ümberpööramine – Google soovib komisjoni erandi tegemise volituse ümber pöörata, nii et usaldusväärsed ELi-välised partnerid oleksid UAL 3-s vaikimisi lubatud, kusjuures komisjon saaks põhjendatud juhtudel loa rakendusaktidega tühistada.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.9
	Muuta – UAL 3 peaks võimaldama usaldusväärsel globaalsetel partneritel toetada Euroopa suveräänseid lahendusi, kui on olemas asjakohased tehnilised ja operatiivsed kontrollimeetmed.	Osaliselt arvestatud seisukohapunktis 6.1
	Muuta – Google märgib, et kavandatav UAL 3 lähenemisviis tundub piiravam kui olemasolevad ranged liikmesriikide suveräänsusraamistikud, mis on võimaldanud usaldusväärsel globaalsetel partneritel pakkuda ranget kontrolli toetavaid tehnilisi ja operatiivseid lahendusi.	Osaliselt arvestatud seisukohapunktis 6.1
	Oluliselt muuta – Google on mures, et UAL 4 takistaks ülemaailmsel operaatoritel igas olukorras Euroopa oluliste kaitseteenuste toetamist. See läheks kaugemale kehtivatest rangetest suveräänsetest raamistikest ja võiks piirata juurdepääsu tiptasemel tehnoloogiale.	Arvestatud seisukohapunktis 6.7
	Muuta – Google soovib lubada usaldusväärsel ELi-välistel operaatoritel toetada rangelt sõltumatuid, Euroopa hallatavaid suveräänseid lahendusi, sealhulgas pakkudes alustarkvara.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.9
	Muuta – Google märgib, et Google Cloud on Euroopa partneritega välja töötanud Google Distributed Cloud Airgapped, et rahuldada Euroopa riikide kaitsejõudude vajadusi, kuid tundub, et see ei vastaks kavandatava UAL 4 kohasele nõutavale kontrollile.	Arvestatud seisukohapunktis 6.1 / 6.2
	Muuta – Google soovib ühendada UAL 3 ja UAL 4 üheks tasemeks, mis võimaldab usaldusväärsel ELi-välistel operaatoritel toetada rangelt sõltumatuid, Euroopa poolt hallatavaid suveräänseid lahendusi, sealhulgas alustarkvara pakkumise kaudu.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.9
ITL	Lisada art 1 lõikesse 1 eraldi punkt: aja lühendamine liitumiseni ja loa saamiseni ning andmekeskuse projektide rahastamisele ligipääsu parandamine. Ilma selleta jääb p b deklaratiivseks.	Osaliselt arvestatud seisukohapunktis 6.8
	Parandada nummerdus. Lisada definitsioonid: 'colocation data centre', 'data centre developer', 'acceleration zone', 'flexible connection agreement', 'anticipatory investment'. Art 2 p 11 viide delegeeritud määrusele 2024/1364 katab operaatorit, mitte arendajat/väljaüürijat, kes on III jaotise tegelik adressaat.	Arvestatud seisukohapunktis 6.1 / 6.2

	<p>Ettepanek salastatud teave defineerida CADA määruse artiklis 2. Juhul, kui kindlustasemete 3 ja 4 korral on salastatud teabe töötlemisel siiski erisused, tuleks neid CADA määruse temaatilises põhjenduspunktis avada.</p>	
	<p>Tuua selle punkti sisu III jaotisesse loamenetluse õigusena: kiirendustsoonid näevad ette kaasneva kindla (firm) puhta tootmisvõimsuse ja salvestuse asukohad ning liikmesriik loob nendele eelloostamise tee. Vt ka ettepanekud art 12 lg 2 ja art 13 lg 2 juurde.</p>	<p>Osaliselt arvestatud seisukohapunktis 6.1 / 6.7</p>
	<p>Kustutada tingimuslik sissejuhatus. Siduda tsoonide arv ja maht art 15 alusel tuvastatud võimsuselüngaga; ülevaatamine iga 2 aasta järel. Lisada arendaja õigus esitada ala kandidaadiks (bottom-up nomineerimine) koos haldusorgani põhjendamiskohustusega. Tagada, et juba kehtiva planeeringu, ehitusloa või liitumispakkumisega objektid saavad tsooni arvata ilma omandatud õigusi kaotamata.</p> <p>Võrdlusalus: netonullitööstuse määruse (EL) 2024/1735 art 18 netonulli-kiirendusorud on CADA kiirendustsoonist igas mõttes tugevamad - tsoonitasandi eelnev strateegiline keskkonnamõju hindamine, oma ühtne kontaktpunkt ning art 15-16 prioriteetne staatus ja kiirendatud kohtukäsitus. Lihtsaim parandus on kirjutada sama tööriistakomplekt CADA-sse.</p> <p>Kõige odavam üksik parandus kogu ettepanekus: siduda kiirendustsooni määramine taastuvenergia kiirendusala määramisega. CADA ütleb praegu ainult põhjenduspunktis, et lähedus taastuvenergia kiirendusaladele 'võiks olla asjakohane tegur'. Palume siduvat sätet: kiirendustsooni määramisel määrab liikmesriik samal ajal kattuva või külgneva TAASTUVENERGIA JA SALVESTUSE KIIRENDUSALA direktiivi (EL) 2018/2001 art 15c tähenduses, nii et tootmine pärib RED III tööriistakasti (vaikimisi nõusolek, projektitasandi KMH erand kiirendusalal, ülekaaluka avaliku huvi eeldus). See ei loo uut menetlust, vaid ühendab kaks olemasolevat.</p>	<p>Osaliselt arvestatud seisukohapunktis 6.8</p>
	<p>Asendada sõnastus selliselt, et liikmesriigid tagavad andmekeskuste kiirendustsoonide ja nendega seotud taristu käsitlemise asjakohastes ruumilistes ja arengukavades, kui see on vajalik kiirendustsooni eesmärgi saavutamiseks. See võimaldab siduvat planeerimiskohustust seal, kus see on sisuliselt vajalik, kuid ei loo ebaproportsionaalset üldkohustust kõigile planeeringutele. Seega ei toeta sellisel viisil kohustuslikuks muutmist.</p>	<p>Osaliselt arvestatud seisukohapunktis 6.8</p>
	<p>Kui KPI-sid kasutatakse siduvate nõuetena, peab komisjon rakendusaktiga kehtestama ühtlustatud, tehnoloogianeutraalsed vahemikud ja mõõtmismetoodika. Mõõta 12 kuu libiseval keskmisel alates kokkulepitud täiskoormuse saavutamisest. ERF ei ole nõue, kui soojusvõrk ja siduva kohustusega ostja puuduvad. Nõudeid ei kohaldata tagasiulatuvalt juba loastatud või ehituses olevatele objektidele.</p>	<p>Osaliselt arvestatud seisukohapunktis 6.8</p>
	<p>Lisada teine lõik: liikmesriigid tagavad, et kiirendustsoonis eraldatud võrguvõimsusele kohalduvad verstepostipõhised säilitamistingimused (maa kontroll, sõlmitud rendi- või mahuleping, seadmete tellimused, finantssulgemine) ning et neile mittevastav võimsus tagastatakse järjekorda. Liitumisõiguste ülekandmine sama tsooni projektide vahel tuleb lubada.</p>	<p>Osaliselt arvestatud seisukohapunktis 6.8</p>

Lisada 'and small mid-caps (SMCs)' VKE-de kõrvale.	Osaliselt arvestatud seisukohapunktis 6.8
Säilitada muutmata. Laiendada sama õigus sõnaselgelt ka art 14 alusel määratud strateegilistele projektidele, mis ei asu kiirendustsoonis (vt art 14 kommentaari).	Osaliselt arvestatud seisukohapunktis 6.8
<p>Kustutada võrguliitumise väljajätt põhjenduspunktist 41 ja piirata lg 2 väljajätt üksnes tõeliselt seadmespetsiifiliste lubadega. Liitumispunkti, alajaama ja ühenduskaabli trassi load peavad olema koondbaasloaga kaetud. Alternatiivina lisada eraldi artikkel 13a siduvate tähtaegadega liitumispakkumisele (3 kuud) ja siduva pingestamise kuupäevaga koos hüvitisega selle ületamisel. Täna kannab võrgu viivituse riski ainuisikuliselt arendaja, kes on samal ajal rentniku ees seotud viivistega - see riskiasümmeetria on üks peamisi põhjuseid, miks AI-rentnikud eelistavad kindlama tarnetähtajaga turge.</p> <p>Samas rõhutame, et tähtaeg ja pingestamise ajakava peaksid olema siduvad ulatuses, milles nende täitmine on võrguettevõtja kontrolli all, ning arvestama objektiivseid võrguohutuse, süsteemi töökindluse, vajalike võrguinvesteeringute ja kolmandatest isikutest sõltuvate menetluste piiranguid.</p> <p>Töötav eeskuju EL-i: Itaalia 20.02.2026 dekreetseaduse nr 21 artikkel 8 kehtestab andmekeskustele ühtse loa, mis hõlmab IPPC, KMH, maastiku-, muinsuskaitse-, vee- ja heitmeload ning igapäringelised võrguühenduse võrgud, tähtajaga 10 kuud (erandkorras +3) ja poole lühemate KMH tähtaegadega. See tõestab, et võrguühenduse ühtsesse loamenetlusse toomine on ELis juba tehtud ja teostatav.</p> <p>Sama probleem kehtib tootmise kohta: koondbaasluba peab katma ka kaasneva elektritootmise ja salvestuse tsooni tasandil hinnatud mahu ulatuses (nt X MW päikest, Y MWh salvestust, Z MW dispetšeeritavat võimsust). Üksikprojekt esitab selle piires teavituse, mitte uue taotluse.</p>	Osaliselt arvestatud seisukohapunktis 6.8
<p>Lisada uus artikkel 14a 'Effects of strategic project status': (a) käsitatakse strateegilise projektina keskkonnamõju hindamise määruse mõttes ja saab tööriistakasti, sõltumata sellest, kas projekt asub kiirendustsoonis; (b) kohaldub art 13 lg 5 tähtaeg ja art 12 ühtse infopunkti tugi; (c) ülekaaluka avaliku huvi eeldus; (d) eelisjärjekord TSO/DSO liitumismenetluses ja arvestamine võrgu arengukavas kindla koormusena; (e) automaatne konkurentsivõime märgis ja toetuskõlblikkus liidu programmides ning art 14b instrumentides. Menetlus: jooksev taotlemine 90-päevase otsustustähtajaga voorude asemel; liikmesriigi kaudu esitamise tee (liikmesriik esitab, komisjon võib vastu vaielda), nagu kriitiliste toorainete määruks. Selgitada, et erakapitaliga rahastatud kolokatsiooniprojekt eraõigusliku rentnikuga on toetuskõlblik. Lisada kriteerium: asukoht, kus on võrguvõimsuse ülejääk ja madal elektri süsinikumahukus ning kus projekt ankurdatakse uut puhast tootmisvõimsust. P d ei tohi muutuda de facto eeltingimuseks enne, kui ELis on AI-kiirendite mahutootmine olemas.</p> <p>Lisaks: (1) lg 1 p c sõnastada 'kindla (firm) võimsuse ja võrgu stabiilsuse' panusena, mitte ainult 'võrgu stabiilsusena' - AI-koormus on baaskoormus ja vajab kindlat võimsust. (2) Lisada kriteerium, mis</p>	Osaliselt arvestatud seisukohapunktis 6.8

	<p>tunnustab, et pikaajalise elektriostulepinguga andmekeskus RAHASTAB uut puhast tootmist, mida riik muidu peaks oksjonile panema: 100 MW kampus katab ostukohustusega suurusjärgus 300 MW uut tootmisvõimsust ja ca 390 mln EUR investeringut ehk ca 17% Eesti kogu praegusest tuule- ja päikeseparkide mahust, ja asendab suurusjärgus 40 mln EUR aastas riiklikku taastuvenergia toetust, mida tarbijad muidu kannaksid.</p>	
	<p>Lisada lg 1 punktid: '(d) the available and planned grid capacity for large loads per Member State and, where available, per connection point, the size of the connection queue and the average and median lead times actually achieved for the connection of large loads; (e) the duration of permit-granting procedures actually achieved for data centre projects, per Member State, distinguishing projects inside and outside acceleration zones.' Lisada lõige: kui komisjon tuvastab võimsuselünga, PEAB asjaomane liikmesriik 12 kuu jooksul määrama täiendavaid kiirendustsoone või oma tegevusetust põhjendama. Praegu on seire ainus tagajärg võimalik soovitus.</p>	<p>Osaliselt arvestatud seisukohapunktis 6.1 / 6.9</p>
	<p>Taseme 3-4 puhul on keelatud EL välise kodakondsusega töötajad. Kodakondsusnõue võib olla ebaproportsionaalne, sest turvariski seisukohast on tähtsam kontrollitud ligipääs, taustakontroll, asukoht ja juurdepääsu logitavus kui kodakondsus ise. Omandi- ja kontrollikriteeriumid võivad piirata legitiimseid partnerlusi, näiteks kui pakkuja kasutab valitud komponentides või tugiteenustes mitte-ELi tehnoloogiat, kuid kontroll kliendiandmete ja teenuse järjepidevuse üle jääb ELi üksusele. Ka muudes valdkondades on sarnaseid piiranguid ja siin võiks olla need ühtlustatud - keelatud on töötajad riskiriikide kodakondsusega (vene, hinna, valgevene, põhja-korea jt) või siis läheneda riskipõhiselt: „Personnel citizenship requirements shall be replaced by risk-based personnel assurance requirements, including location in the Union, security screening, least-privilege access, privileged access monitoring, contractual independence and enforceable refusal mechanisms against unlawful third-country access.” Funktsionaalne kontrollimudel saavutab sama avaliku korra kaitse vähem diskrimineerivalt ning on paremini kooskõlas proportsionaalsuse ja teenuste vaba liikumise põhimõtetega.</p> <p>Omandi- ja kontrollitestid ei tohi külge hakata FÜÜSILISELE TARISTUKIHILE ega kiirendustsooni või strateegilise projekti kõlblikkusele. Kui see joon hoitakse, on võimsuse-samba kasu suveräänsusdebati lahendusest sõltumatu. Enamik ELi andmekeskuste arendust rahastatakse rahvusvahelise infrastruktuurikapitaliga; kui selle osalus muudaks rajatise kõrgema taseme jaoks kõlbmatuks, tõstaks CADA ELi andmekeskuste kapitalikulu ja töötaks oma võimsuse kolmekordistamise eesmärgi vastu.</p>	<p>Arvestatud seisukohapunktis 6.1 / 6.2</p>
	<p>Lisada: iga art 16 lg 2 alusel tehtava muudatuse puhul vähemalt 36-kuuline üleminekuaeg ning juba kasutuses olevate rajatiste ja kehtivate tunnistuste grandfathering. Muudatusi ei kohaldata tagasiulatuvalt kehtivatele lepingutele.</p>	<p>Osaliselt arvestatud seisukohapunktis 6.9</p>
	<p>„Recognition shall be service-family based and reusable across materially equivalent services, locations and configurations. Existing European cybersecurity certificates, national cloud qualifications and NIS2-</p>	<p>Arvestatud seisukohapunktis 6.9</p>

compliant audited controls shall be accepted as evidence to the extent they cover equivalent requirements.”	
CADA võiks sätestada ka selle, milliste rikkumiste eest konkreetselt on võimalik karistusi määrata. Peaksime vältima olukordi, kus avalik sektor paneb kogu vastutuse erasektori pakkujale.	Arvestatud seisukohapunktis 6.9
CADA art 29 tuleks muuta nii, et 12 kuud ei oleks absoluutne lagi, vaid vaikumisi maksimum lihtsamatele migratsioonidele; keerukate, kriitiliste või telco-integrated pilveteenuste puhul peaks olema võimalik 24–36 kuud, kui see on vajalik teenuse järjepidevuse, küberturbe või sõltuvuste tõttu.	Arvestatud seisukohapunktis 6.3
„Contracting authorities shall require Union assurance level 1 only where the nature, sensitivity, criticality and operational impact of the cloud computing service justify such requirement. For low-risk or publicly available workloads, equivalent safeguards based on recognised Union or national cybersecurity frameworks may be accepted.”	Arvestatud seisukohapunktis 6.2
arusaamatu ja vajaks täpsustamist.	Arvestatud seisukohapunktis 6.2
Peaks vältima seda, et NIS 2 subjektidele nt on mitme õigusakti aluselmitmed erinevad sertifitseerimisohustused sama valdkonna osas (nt küberturvalisus).	Arvestatud seisukohapunktis 6.9
CADA eesmärk võik olla tagada, et 25% eesmärk ei välistaks suurettevõtjaid konsortsiumijuhtidena ega karistaks skaleeritavaid lahendusi selle sättega, vaid lubada SME-de kaasamine allhankes/partnerluses.	Arvestatud seisukohapunktis 6.6
Peame vajalikuks täpsustada EuroCloud Federation'i rolli selliselt, et see ei tooks kaasa erasektori pilve-, andmekeskus- ja sideettevõtjate väljatõrjumist ega konkurentsimoontust. Avaliku sektori üksuste vaheline teenuste jagamine peaks olema lubatud üksnes selgelt piiritletud avaliku huvi või tõendatud turutõrke korral ning tingimustel, mis tagavad kulude läbipaistvuse, ristsubsideerimise vältimise ja võrdse konkurentsi kommertsteenuse pakkujatega. Tuleks rõhutada pigem meetmeid, mis ergutaks vastava kommerts-teenuse turu tekkimist Euroopas (stabiilne nõudlus, soodsad finantseerimismudelid jms.) Kuigi praegusel hetkel võib väita, et meil on turutõrge kvaliteetsete pilveteenuste osutamisel, siis siin on sellise tõrke tekkimise põhjuseks pigem sobiva ärikeskkonna puudumine olukorras, kus US suured tehnoloogiafirmad oma finantsjõuga lihtsalt investeerivad Euroopa ettevõtteid selliselt turult välja. Mastaabiefekti puudumise tõttu on Euroopas raske on olnud hoida võrreldavat hinna-kvaliteedi suhet. Kui EL on administratiivsete vahenditega sellist turgu tekitamas, kus Euroopa firmadel oleks võimalik vastavat äri välja arendada, siis on vaja vältida igasugust võimalust, et teise käega nullitakse selline motivaator erasektori jaoks kohe ära läbi riikliku isetegemise ambitsiooni. Kui avaliku sektori üksused saavad teenuseid jagada kulupõhiselt ja väljaspool tavapärase hankeõigust, võib see moonutada konkurentsi eraoperaatoritega, kes peavad kandma kapitalikulu, sertifitseerimiskulu, küberturbe kulu ja tururiske.	Arvestatud seisukohapunktis 6.11 / 6.12
Selleks, et selliste hangete puhul ei koonduks pakkujateks ainult üksikud suured pakkujad, peaks lisama tingimused, mis soodustaksid ka väiksemate ja lokaalsete pakkujate kaasamist: „Common procurement shall be designed as multi-award, multi-lot and multi-cloud by default, including regional lots, security-assurance lots, data-centre services lots and managed-service lots. Award criteria shall preserve	Arvestatud seisukohapunktis 6.6 / 6.12

	competition, avoid over-concentration and enable EU-based telecom, cloud and data centre providers to participate either directly or in consortia.”	
KAM	Toetame, kuna vähendab kriitilisi sõltuvusi ja samas suurendab EL-i suveräänsust pilve- ja AI-võimekust.	Arvestatud seisukohapunktis 6.1
	Toetame üldises raamis, kuid hetkel tekib küsimus, kuidas arevistatakse kaitsevaldkonna erisustega nt andmete, kriitiliste teenuste, tarneahela usaldusväärsuses ja riigikaitse toimepidavuse nõuetega.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.7
	Toetame sätte üldist suunda, kuid tuleb rõhutada vajadust arvestada kaitsevaldkonna erisustega, sh tundlike andmete, kriitiliste teenuste, tarneahela usaldusväärsuse ja riigikaitse toimepidavuse nõuetega.	Arvestatud seisukohapunktis 6.1 / 6.7
	Toetame andmekeskuste arendamise kiirendamist, kuid lisada Eesti seisukohta vajadus hinnata andmekeskuste asukoha, elektri- ja sideühenduste, füüsilise turbe, tarneahela ning kriisiolukorra toimepidavuse mõju riigikaitsele.	Arvestatud seisukohapunktis 6.8
	Toetame ühtset EL-i suveräänsuse raamistikku, kuid kaitsevaldkonna kasutusjuhtude puhul peab olema võimalik nõuda kõrgemaid suveräänsus-, kontrolli-, auditi- ja andmepaiknemise tingimusi.	Arvestatud seisukohapunktis 6.1 / 6.2
	Toetame ainult siis sellist tunnustamismehhanismi, mis välistab kaitsevaldkonna tundlike kasutusjuhtude puhul ebapiisava kontrolli kolmandate riikide jurisdiktsiooni, andmetele ligipääsu ja teenusekatkestuse riskide üle. Kaitsevaldkonnas võib kolmanda riigi kontroll ja jurisdiktsioon olla oluline risk.	Arvestatud seisukohapunktis 6.1 / 6.2
	Toetame ühtset EL-i suveräänsuse raamistikku, kuid kaitsevaldkonna kasutusjuhtude puhul peab olema võimalik nõuda kõrgemaid suveräänsus-, kontrolli-, auditi- ja andmepaiknemise tingimusi.	Arvestatud seisukohapunktis 6.1 / 6.9
	Toetame sõltumatu auditi nõuet, kuid täpsustada, et kaitsevaldkonna teenuste puhul peavad auditorganisatsioonidele, audititööenditele ja juurdepääsule kehtima täiendavad julgeoleku-, taustakontrolli- ja konfidentsiaalsusnõuded.	Arvestatud seisukohapunktis 6.1 / 6.9
	Toetame registri loomist, kuid rõhutaks üle, et registris peaks olema piisav teave teenuse suveräänsustaseme, kehtivuse, piirangute ja auditi ulatuse kohta, mis võimaldab kaitsevaldkonnal teha teadlikuid valikuid.	Arvestatud seisukohapunktis 6.1 / 6.9
	Toetame ühtset EL-i suveräänsuse raamistikku, kuid kaitsevaldkonna kasutusjuhtude puhul peab olema võimalik nõuda kõrgemaid suveräänsus-, kontrolli-, auditi- ja andmepaiknemise tingimusi.	Arvestatud seisukohapunktis 6.1 / 6.9
	Toetame tõhusaid ja hoiatavaid sanktsioone, kuid riigikaitse seisukohalt oluliste ja kriitiliste teenuste puhul peab rikkumise mõju hindamisel arvestama ka toimepidavuse, julgeoleku ja usalduskahjuga.	Arvestatud seisukohapunktis 6.1 / 6.9
	Toetame pädevate asutuste selget rollijaotust, kuid samas tuleb rõhutada vajadust tagada julgeolekuastute ja kaitsevaldkonna kaasamine juhtudel, kus järelvalve puudutab riigikaitse, salastatud või kriitilisi teenuseid.	Arvestatud seisukohapunktis 6.1
	Toetame riskihindamise kohustust, kuid Eesti seisukohas tuleb rõhutada, et kaitsevaldkonna puhul peab meetodika võimaldama hinnata ka riigikaitse mõju, salastatust, operatiivset autonoomiat, kriisi- ja sõjaaja toimepidavust, sõltuvust kolmandatest riikidest ning vajadusel kasutada kõrgemaid kindlustasemeid.	Arvestatud seisukohapunktis 6.2

	Hetkel teadmata, millised oleksid need kehtestatud miinimumnõuded pilveteenuste hankimisel, seega peab arvestama, et kaitsevaldkonna puhul peab olema jankijal õigus nõuda rangemaid tingimusi, sh andmete paiknemist EL-is või Eestis, kriitilise sõltuvuse maandamist ning eraldi turva- ja toimepidavusnõudeid.	Osaliselt arvestatud seisukohapunktis 6.2
	Toetame innovatsiooni ja Euroopa lisandväärtust soodustavaid hankekriteeriume, kuid samas tuleb rõhutada, et kaitsevaldkonna hangetes ei tohi need vähendada võimalust seada rangemaid julgeoleku-, salastatuse, tarneahela usaldusväärsuse ja operatiivse autonoomia nõudeid.	Arvestatud seisukohapunktis 6.6
	Toetame avaliku sektori pilveföderatsiooni arendamist, kuid Eesti seisukohas tuleks rõhutada, et kaitsevaldkonna kasutusjuhtude kaasamine peab olema vabatahtlik ja võimalik ainult juhul, kui on tagatud piisav suveräänsus, turvalisus, andmete kontroll, audit, kriisiaegne kätesaadavus ja vastutuse selgus.	Arvestatud seisukohapunktis 6.11
	Toetame ühishangete võimalust, kuid tuleb rõhutada, et kaitsevaldkonnale peab jääma õigus teha eraldiseisvaid või piiratud menetlusega hankeid, kui seda nõuavad riigikaitsele vajadused, tarneahela usaldusväärsus või teabe kaitse.	Arvestatud seisukohapunktis 6.6 / 6.12
	Üldjoontes toetame avatud standardite ja avatud lähtekoodid põhimõtet, kuid tuleb rõhutada, et kaitsevaldkonnas peab kasutamine põhinema turvahindamisel, haavatuste haldamisel, komponentide päritolu kontrollil ning vajadusel piiratud levitamise või erandite võimalusel.	Arvestatud seisukohapunktis 6.5
	Vastuväited puuduvad, kuid Eesti seisukohast tuleks rõhutada vajadust kaasata rakendusaktide ja delegeeritud aktide ettevalmistamisse liikmesriikide julgeoleku- ja/või kaitsevaldkonna eksperdid ning tagada piisav üleminekuage.	Arvestatud seisukohapunktis 6.10
MKM	Selleks, et vältida investeringute ja turuvõimaluste koondumist üksikutesse suurematesse EL liikmesriikidesse võiks lisada ühe eesmärgina "võrdse ja mittediskrimineeriva juurdepääsu tagamine kõigi liikmesriikide ettevõtjatele". Nt "The measures established under this Regulation shall be implemented in a manner that ensures equal and non-discriminatory access for eligible entities from all MS"	Arvestatud seisukohapunktis 6.1 / 6.7
	Art 3(2) võiks lisada uue lõike " The Commission shall ensure open, transparent and geographically balanced participation of undertakings, including SMEs and start-ups, from all Member States ". See vältiks olukorda, kus rahastus ja projektid koonduvad üksikutesse liikmesriikidesse.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.7
	Tuleks seista selle eest, et vältida ebaproportsionaalset koormust VKEdele. Võimalusel lisada kusagile "reporting obligations" alla "Reporting obligations for SMEs shall be proportionate to their size, risk profile and participation under this Regulation".	Osaliselt arvestatud seisukohapunktis 6.8
RAM	Lisada Artiklisse 2 "avaliku korra" definitsioon või vähemalt mitteammendav loetelu kriteeriumidest/valdkondadest, mida mõiste hõlmab.	Arvestatud seisukohapunktis 6.2 / 6.10
	Täiendada Artikli 4(7)(d) sõnastust selgesõnalise viitega Euroopa terviseandmeruumi määrusele (EHDS) ja sätestada, et käesoleva määruse alusel toimuv terviseandmete taaskasutus AI mudelite jaoks peab vastama EHDS-is sätestatud sekundaarse kasutuse tingimustele.	Arvestatud seisukohapunktis 6.1

	Pikendada tähtaega vähemalt 18 kuule.	Osaliselt arvestatud seisukohapunktis 6.4
	Pikendada tähtaega (nt 12 kuule) ja/või näha ette komisjoni tehniline tugi (juhendmaterjal, näidismetoodika) tsoonide kriteeriumide hindamiseks, et väikeriigid saaksid tähtajast reaalselt kinni pidada.	Osaliselt arvestatud seisukohapunktis 6.8
	Selgesõnaliselt lubada liikmesriikidel määrata olemasolev asutus ilma täiendava institutsionaalse loomiseta.	Arvestatud seisukohapunktis 6.1
	Lisada võimalus tähtaega mõjuval põhjusel pikendada.	Arvestatud seisukohapunktis 6.3
	Täpsustada määruses (a) mõõtmismetoodika (kas 25% arvestatakse hankelepingute arvust või rahalisest mahust), (b) aruandluskohustuse sisu ja sagedus, ning (c) näha ette proportsionaalsuse/erandi mehhanism liikmesriikidele, kelle siseturul napib vastava suurusega ja profiiliga innovaatilisi VKE-sid.	Arvestatud seisukohapunktis 6.6
RIA	Säilitada eesmärgid; tagada sidusus olemasoleva EL küberraamistikuga (vt art 16).	Arvestatud seisukohapunktis 6.1
	Komisjoni õigus teha lõplik otsus peaks hõlmama mingeid garantiisid nende riikide jaoks, kes hoiduksid nõusoleku andmisest. Näiteks kohustus hinnata vastulauseid seoses avaliku korra või julgeolekuga või nõue, et konsulteeritakse vastu oleva riigi pädeva asutusega.	Osaliselt arvestatud seisukohapunktis 6.9
	Soovitame kaaluda lisada, et tegevuskoha/teenuse osutamise asukoha riigi pädeval asutusel oleks õigus võtta samuti mingeid ajutisi meetmeid. Nt olukorras, kus ilmneb, et mingi nõuete rikkumine kujutab endast ohtu avalikule korrale või julgeolekule.	Arvestatud seisukohapunktis 6.1
	Avaldada metoodika kavand menetluse käigus, et oleks võimaliks hinnata regulatsiooni reaalselt mõju; säilitada liikmesriigi kaalutlusruum julgeolekutundlikes hinnangutes.	Arvestatud seisukohapunktis 6.10
	Jätta lõplik tagatistaseme määramine liikmesriigile; Komisjoni roll piirata metoodika ja soovitustega, mitte siduva ümberotsustamisega. Tegemist riigi julgeoleku ja siseturvalisuse küsimusega.	Arvestatud seisukohapunktis 6.2
	Näha ette pikem tähtaeg ja/või võimalus põhjendatud juhul tähtaega pikendada.	Arvestatud seisukohapunktis 6.3
	Täpsustada Komisjoni volitusi täiendavatele üksustele kohustuslike nõuete kehtestamisel, anda liikmesriikidele suurem roll.	Arvestatud seisukohapunktis 6.10
	Täpsustada tasude arvutamise metoodika ja läbipaistvus.	Arvestatud seisukohapunktis 6.11 / 6.12
RIT	AI arvutusvõimsust tuleb allokeerida Frontier AI arendus projektidesse. Kas see tähendab tasuta või võib siin raha küsida? Kas siin on ette nähtud ka võimekuse suurendamist? Kui meil võimekust pole, siis kas on kohustus see luua?	Arvestatud seisukohapunktis 6.7
	Article 15 ei selgita, kes on selle gap-i target kliendid.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.8

	Kas Article 17 puhul säilib igal liikmesriigil kohustus suurettevõtete puhul hinnang eraldi teha? Samas Article 19 ütleb, et self-assessmentit saab teha UA1 puhul. Hetkel on ebaselge, mis puhkudel peab riik seda hindama ja mis juhul tuleb see teenusepakkuvalt endalt.	Osaliselt arvestatud seisukohapunktis 6.9
	Kas article 22 on riigi või EL põhine? Kas keskne register on ELi tasandi register ning milline roll jääb liikmesriigi pädevale asutusele andmete sisestamisel/uuendamisel?	Arvestatud seisukohapunktis 6.1 / 6.9
	Article 30 puhul jääb ebaselgeks millistel puhkudel on kohustus osta pilvteenust. Kas igal juhul ja p2 ning p3 sätestavad ainult taseme?	Arvestatud seisukohapunktis 6.2
	Mis on Article 34 - 36 eesmärk? Ühtpidi on see variant kuidas erinevate riikide avaliku sektori asutused saavad teistele oma ressursi müüa, teistpidi tundub CADA eesmärk olevat ikkagi innovaatilistele pilvteenustele avalikku sektorit suunata. Kas on mõeldud, et riigid hakkavad oma DC-sid kuidagi omavahel jagama? Kas Eesti peab võimaldama oma DC-des teiste riikide asutustel oma infrat hoida?	Arvestatud seisukohapunktis 6.11
	P3 tähendab, et "komisjon" saab EU üleseks keskseks raamhankijaks, kelle käest on võimalik siis asju otse osta/hankida? Kuidas selline raamhankija rolli võtmine konkurentsi soosib ning kas on kooskõlas EL hangetealaste direktiividega?	Arvestatud seisukohapunktis 6.6 / 6.12
	Article 44 räägib OSPO-st. Kuhu see luuakse?	Arvestatud seisukohapunktis 6.1 / 6.5
RTK	Artiklite 2 ja 30 kogumis on küsimus, kas hallatavad tehisaru keelemudeliteenused (LLM API-d, hosted model endpoints) on käsitletavad pilvandmetöötlusteenusena (NIS 2 direktiivi (EL) 2022/2555 artikkel 6 p 30). Avalikku korda, julgeolekut või õiguskaitset toetavatele asutustele rakendub käesoleva eelnõu kohaselt nõue kasutada üksnes usaldustasemega 2-4 sertifitseeritud teenuseid. Kui tehisaru keelemudeliteenuseid käsitleda pilvandmetöötlusteenusena, siis kuivõrd turul puuduvad praegu CADA või EUCSi tasemetele 2-4 vastavad kommerts LLM teenused, siis tekiks juriidiline hallala ning avaliku sektori tehisarulahenduste hankimine ja kasutus oleks takistatud. Lähtuvalt sellest leiame, et nimetatud määratlus tuleks eelnõus selgelt sätestada.	Arvestatud seisukohapunktis 6.1 / 6.2
	Leiame, et lisaks sellele, et nimetatud keskused ehitatakse Euroopa digitaalse innovatsiooni keskuste baasile, peaks selgelt ka eelnõus sätestatud olema, et keskuse pädevus katab andmekaitse, õigusraamistiku, infoturbe ning keelemudelite arhitektuuri. See võimaldaks välistada tänase olukorra, mil iga riigiasutus lahendab neid valdkondi eraldist, dubleerib. Vt ka järgneval sheedil toodud kommentaari.	Arvestatud seisukohapunktis 6.7
	Tunnustatud pilveteenuste kohustus laieneb kogu avalikule sektorile. Kohustuse jõustumisel tekib risk, et sobivaid teenusepakkujaid veel ei ole, mis halvab hanked. Avalik-õiguslik kohustus peab olema objektiivselt täidetav. Kui määrusega nõutakse hankijalt registreeritud / tunnustatud pilveteenuse hankimist, kuid pakkujaid ei ole või sertifitseerimisasutuste võimekus on puudulik, tekib ummikseis.	Osaliselt arvestatud seisukohapunktis 6.2
	Nõue, et hindamiskriteerium peab olema samal ajal kohustuslik, kuid "kõrvalise tähtsusega ega ole lepingu sõlmimisel otsustav", on sisemiselt vastuoluline. Riigihangete direktiivi 2014/24/EL artikli 67 ja RHS § 85 kohaselt peavad hindamiskriteeriumid oleva läbipaistvad, eristatavad ning pakkumuste hindamisel punktide kaalutud. Iga kriteerium, millele omistatakse osakaal (ka nt 1%), muutub piirjuhul otsustavaks, kui pakkujate tulemused ülejäänud kriteeriumites on võrdsed. Formulatsioon "ei tohi olla	Osaliselt arvestatud seisukohapunktis 6.6

	otsustav" tekitab olukorra, kus hankelepingu sõlmimise otsuse saab kohtus vaidlustada väitega, et "kõrvaline kriteerium sai võitja selgitamisel otsustavaks". Ettepanek seega asendada säte kaalu fikseeritud ülempiiriga (nt kuni 10%). Samuti leiame, et vajalik on komisjoni poolt tüüpikriteeriumite juhendi koostamine.	
	Säte on vastuolus võrdse kohtlemise põhimõttega. Direktiiv 2014/24/EL art 18 ning RHS § 3 sätestavad, et hankija on kohustatud tagama pakujate võrdse kohtlemise, vältima diskrimineerimist ning konkurentsi kunstlikult piiramist. Konkurentsi peetakse kunstlikult piiratuks, kui riigihanget kavandatakse kavatsusega teatavaid ettevõtjaid sobimatul viisil soodustada või ebasoodsasse olukorda panna. Lisaks märgime, et Eesti-suurusel turul tehakse aastas vaid üksikuid suuri IT-taristu raamlepinguid. Kui üks mahukas taristuhankeleping sõlmitakse suurtootjaga, võib see rahalises mahus täita või halvata kogu riikliku aastanimetaja. Lahendusena näeme, et VKEd e kaamine saaks toimuda protsessimeetmete kaudu (art 33 lg 5: turukonsultatsioonid, hankelepingute osadeks jaotamine, proportsionaalsed tingimused).	Arvestatud seisukohapunktis 6.6
SIM	Märkus (d) kohta, et kriitilistest tehnoloogiatest sõltuvuse vähendamine ei tohi vähendada teenuste toimepidevust - see tähendab, et sõltuvuse vähendamiseks kehtestatud meetmed ei tohi põhjendamatult piirata teenuste toimepidevust, mitme pilveteenuse kasutamise strateegiaid või juurdepääsu maailmatasemel konkurentsivõimelistele tehnoloogiatele. (e) osa võiks arvestada liikmesriikide arhitektuuri, st. kui see toimib, siis pea ilmtingimata sundima kasutama ühist pilveplatvormi - see on EE arhitektuuri põhimõtete vastu.	Arvestatud seisukohapunktis 6.1
	Lisada sõltumatuse nõue.	Arvestatud seisukohapunktis 6.9
	(b) märkus - Eesmärgiks on andmekeskuste võimekuse suurendamine, kuid mille alusel? Oluline, et see ei muutuks eesmärgiks omaette ning arvestama tegelikku vajadust. Tekitab survet energiataristule - mis on prioriteetsem: andmekeskus, tööstus või kodanik. Suured AI-andmekeskused võivad tarbida väga suuri energiakoguseid ning mõjutada nii elektri hindu kui ka võrgu koormust. (c) märkus: kasutuselevõtmine peab olema seaduslik ja turvaline.	Arvestatud seisukohapunktis 6.7 / 6.8
	Märkus (c) kohta - riigiasutuse eesmärk ei tohiks olla võtta AI-d kasutusele võimalikult palju, vaid kasutada seda õiguspäraselt, turvaliselt ja põhjendatult. AI peaks väärtust lisama.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.7
	Eestis kasutatakse hübriid- ja multi-cloud lahendusi ning täielik tehnoloogiline eraldumine ei ole realistlik?	Osaliselt arvestatud seisukohapunktis 6.1 / 6.7
	Tuleks lubada ka regionaalseid keskuseid nt Balti koostöö, Eesti turu väiksust arvestades.	Arvestatud seisukohapunktis 6.7
	Siin tuleks toetada tootja- või tehnoloogia neutraalseid hankeotsuseid.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.7
	Väiksematel riikidel ei pruugi olla võimalik kõikides algatustes osaleda. EE jaoks väljakutse.	Arvestatud seisukohapunktis 6.1 / 6.7

Ei peaks olema täiesti eraldiseisev strateegia vaid võib olla osana muust strateegiast, nt. DÜAK vms.	Arvestatud seisukohapunktis 6.4
Märkus (g) kohta - vältida avatud lähtekoodi kohustuslikuks muutmist olukorras, kus see ei sobi.	Arvestatud seisukohapunktis 6.5
LR-del tuleb arvestada ka oma riiklikke vajadusi.	Arvestatud seisukohapunktis 6.4
Digikümnenendi eesmärgid on olulised, kuid nende täitmine ei tohiks muutuda liikmesriikidele absoluutseks kohustuseks sõltumata kuludest või tegelikust vajadusest.	Arvestatud seisukohapunktis 6.4
Kolmeaastane kohustuslik ülevaatus võib põhjustada dubleerimist juba olemasolevate aruandluskohustustega - vt. KÜTS näitena jne. Aruandlus ja ülevaatused võiksid toimida olemasolevate aruandlusmehhanismide näol, et vähendada halduskoormust.	Arvestatud seisukohapunktis 6.4
Parimate praktikate jagamine on väga tervitatav. Nõustamine on tervitatav, aga tuleb silmas pidada, et liikmesriikidel peab jääma võimalus kujundada oma digiarhitektuuri.	Arvestatud seisukohapunktis 6.4
Liikmesriikidelt ei tohiks nõuda arvutusvõimsuse reserveerimist EL prioriteetsetele projektidele olukorras, kus see võib mõjutada riigisiseseid teenuseid.	Arvestatud seisukohapunktis 6.7
Andmekeskuste rajamise vajadus peab sõltuma turuolukorrast, elektrivõrgu võimekusest ja investeerimishuvi olemasolust. Eesti jaoks võib olla see kohustus liialt koormav. Andmekeskuste kiirendustsoonid võivad Eestit ebasoodsasse olukorda jätta, kuna määrus eeldab andmekeskuste geograafiliselt tasakaalustatud rajamist ja EL võimsuse kolmekordistamist. Riskikoht on see, et investeringud liiguvad eelkõige: Saksamaale, Prantsusmaale, Põhjamaade piirkonda. Ettepanek on luua: Väikeriikidele eraldi toetusmehhanism või regionaalne tasakaalukriteerium strateegiliste projektide valikul.	Arvestatud seisukohapunktis 6.7 / 6.8
Siin on kindlasti on oluline kaasata ka riigi küberturvalisuse eest vastutavaid, sest andmekeskused on sageli kriitilise infrastruktuuri osa.	Arvestatud seisukohapunktis 6.8
Lisaks VKE-dele tuleks toetada ka avalikku sektorit.	Osaliselt arvestatud seisukohapunktis 6.8
Märkus (d) - võib piirata tehnoloogianeutraalsust olukorras, kus kohustatakse kasutusele võtma lahendusi EL-st.	Osaliselt arvestatud seisukohapunktis 6.8
See on piirav, s.t et tohib kasutada tulevikus ainult kindla suveräänsustasemega teenuseid - otsused peaksid põhinema siiski riskipõhisusel ja tehnoloogia-neutraalsusel.	Arvestatud seisukohapunktis 6.1
Väiksematele Eesti teenusepakkujatele võib menetlus osutuda kulukaks.	Osaliselt arvestatud seisukohapunktis 6.9
Lisaks sanktsioonidele tuleb hinnata tarneahelat, geopoliitilist riski ja võimalikku mõju teenuse toimepidevusele.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.9
Üksnes enesehindamisel põhinev vastavus võib olla ebapiisav kõrgema riskiga avalike teenuste jaoks.	Osaliselt arvestatud seisukohapunktis 6.9

	<p>Auditi põhimõtted peavad olema proportsionaalsed, hindama tegelikku küberturvalisust, toimepidevust ja sõltuvusriske.</p>	<p>Osaliselt arvestatud seisukohapunktis 6.9</p>
	<p>Vältida dubleerivat halduskoormust. Riskihindamise kohustus on põhjendatud, kuid tuleb vältida dubleerimist olemasolevate KüTS-i, NIS2, E-ITS-i, riigi infosüsteemide ja toimepidevuse riskianalüüsidega.</p> <p>Selle järgi tuleb asutustele (sh andmekaitse spetsialistidele) täiendada ajaliselt määratletud kohustused, st koostada tuleb pilveteenuseid kasutavate avaliku sektori tegevuste jaoks riskianalüüse. Artikli 29 lõigete 1 ja 2 kohaselt tuleb neid analüüse läbi viia vähemalt iga kahe aasta tagant ning nendes tuleb hinnata töödeldavate isikuandmete tundlikkust, kolmandate riikide üksuste poolt ebaseadusliku juurdepääsu riski ning võimalikku mõju avalikule korrale ja andmesubjektide õigustele. Tekib küsimus, kas see on midagi erinevat andmekaitsest mõjuhinnangust või selle osa? (GDPR artikkel 35 seosed).</p> <p>Kui see on lisaks (nagu tundub loetelust), siis toob see kaasa täiendava ressursivajaduse. Kas see eeldab ka ühtseid riskihinnanguid (art 29 lg 1 viimase lause aluse)? Nt andmekaitsest mõjuhinnangut peab teostama vastutav töötleja aga kui tehakse CADA alusel riskihinnanguid, siis kas tekib kohustuste konflikt? Kas ühtne riskihinnang on võimalus või kohustus?</p> <p>Lisaks on problemaatilised järjest artikkel 29 ja 30-ga seotud kohustused - kas on kohustus hakata avaldama Komisjonile neid riskianalüüse?</p> <p>Liikmesriikide riskihindamiste harmoniseerimise osas näeb artikkel 29 ette riiklikud riskihindamised avaliku sektori kasutusjuhtudele. Sealt aga tuleneb risk, et üks liikmesriik võib määrata taseme 4. Samas Eesti määrab taseme 2. Tulemuseks on killustunud turg.</p> <p>Ettepanek: ENISA või Euroopa Komisjon (või ka liikmesriigid) peaks avaldama ühise metoodika; referentskasutusjuhtumid; ühised riskikriteeriumid. Need võiks aidata seda metoodikat ühtlustada. Teenused on ka riikide vahel, nt Schengeni Entry-Exit vms.</p>	<p>Arvestatud seisukohapunktis 6.1 / 6.9</p>
	<p>Komisjonile saadetak detailne riskihindamine võib sisaldada tundlikku teavet.</p>	<p>Arvestatud seisukohapunktis 6.2</p>
	<p>12-kuuline migratsioonikohustus võib olla ebarealistlik väga suurte või kriitiliste infosüsteemide puhul. Ettepanek on see viis pikemaks, nt 24 kuud kriitilistel ja/või 36 kuud keskmis eja madala riskiga teenustel.</p> <p>Mis ajast alates hakkab 12 kuud jooksmas?</p>	<p>Arvestatud seisukohapunktis 6.3</p>
	<p>Kas seda informatsiooni saab liikmesriigi asutus ka nõuda? Või kas seda infot avaldatakse ka EL-i liikmesriikidele?</p>	<p>Osaliselt arvestatud seisukohapunktis 6.2</p>
	<p>Viidata riskipõhisusele.</p>	<p>Osaliselt arvestatud seisukohapunktis 6.2</p>

	<p>Puudub erand olukorraks, kus nõutud suveräänsustase võib tegelikult halvendada teenuse toimimist või küberturvalisust.</p> <p>See on vastuolus Eesti senise lähenemisega, kus kõige olulisem eesmärk on kriitiliste teenuste toimepidevus (KüTS, NIS2, E-ITS põhimõtted).</p>	Arvestatud seisukohapunktis 6.2
	ELis toodetud ei tähenda automaatselt eelist - lähtuma peab siiski toimepidevusest, innovatsioonist ja toote turvalisusest.	Arvestatud seisukohapunktis 6.6
SOM	<p>Toetame avaliku sektori jaoks mõeldud tehisarumudelite ja -süsteemide arendamist, sealhulgas hariduse, teaduse ja tervishoiu valdkonnas. Säte on siiski väga üldine ega täpsusta, kuidas valitakse prioriteetsed kasutusvaldkonnad, kuidas tagatakse liikmesriikide osalemine ning kellele kuuluvad projektide käigus loodud mudelid, tarkvara ja intellektuaalomandi õigused.</p> <p>Ettepanek: Täpsustada, et prioriteetsete avaliku sektori projektide valimisel kaasatakse valdkonna eest vastutavad liikmesriikide asutused ning tagatakse loodud lahenduste piiriülene taaskasutatavus, koostalitlusvõime ja võimaluse korral avatud lähtekoodiga kättesaadavus. Hariduse, teaduse ja tervishoiu valdkonna lahenduste puhul peab säilima võimalus arvestada liikmesriigi keele-, andme- ja institutsionaalsete eripäradega.</p>	Arvestatud seisukohapunktis 6.7
	Ettepanek: võimaldada riikliku strateegia läbivaatamistsükli (iga 3 aastat) ühildamist juba kehtivate (tervishoiu) digiarengukavade läbivaatamistsükliga, et vähendada dubleerivat aruandluskoormust.	Arvestatud seisukohapunktis 6.4
	<p>Sättest ei selgu, millise korra alusel ja millise hinnaga saavad liikmesriigid, ülikoolid, teadusasutused ja avaliku sektori asutused juurdepääsu arvutusressursile. Samuti pole selge, kuidas tagatakse väiksemate liikmesriikide võrdne ligipääs.</p> <p>Ettepanek: Kehtestada läbipaistvad ja mittediskrimineerivad juurdepääsukriteeriumid ning eraldi võimalus avaliku huvi projektidele, teadusele, haridusele ja väikese keeleruumi mudelite arendamisele. Ressursi jaotamisel ei tohiks lähtuda ainult liikmesriigi rahalisest panusest või projekti mahust.</p>	Arvestatud seisukohapunktis 6.7
	Ettepanek: lisada kriteerium a (olulised avaliku sektori funktsioonid, sh tervishoid) juurde nõue kaasata strateegilise projekti staatuse hindamisse valdkondlikult pädev ministeerium	Osaliselt arvestatud seisukohapunktis 6.8
	<p>Arvutusvõimsuse seire võib hõlmata äri- ja julgeolekutundlikku infot ning tekitada andmekeskustele, teadusasutustele ja avaliku sektori taristu haldajatele täiendavat aruandluskoormust.</p> <p>Ettepanek: Täpsustada kogutavate andmete ulatus, konfidentsiaalsuse tagatised, andmete kasutamise eesmärk ja seos juba olemasoleva energiatõhususe ning digikümneni aruandlusega. Sama infot ei tohiks nõuda mitme ELi õigusakti alusel korduvalt</p>	Arvestatud seisukohapunktis 6.1 / 6.8
	<p>Tähelepanek: Ühtse pilvesuveräänsuse raamistiku loomist võib põhimõtteliselt toetada, kuid neli kindlustaset ja nende kriteeriumid asuvad II lisas, mille kohta tagasisidevormis eraldi ridu ei ole. Kriteeriumid võivad oluliselt piirata teenusepakkujate valikut ning mõjutada teenuste hinda ja kättesaadavust.</p> <p>Ettepanek: Tagada, et nõuded oleksid riskipõhised, tehnoloogianeutraalsed ja proportsionaalsed ning et madalama riskiga avaliku sektori teenustele ei kohalduks põhjendamatult kõrge suveräänsustase. Lisa</p>	Osaliselt arvestatud seisukohapunktis 6.9

muutmisel delegeeritud õigusaktiga peab liikmesriikidel olema piisav mõju ning ettevõtjatele mõistlik üleminekuaeg.	
Tähelepanek (read 82-112): Tunnustamis- ja auditisüsteem on mahukas ning võib tekitada teenusepakujatele märkimisväärsed kulusid. See võib olla eriti koormav väikestele ja keskmise suurusega Euroopa teenusepakujatele ning vähendada konkurentsi. Samuti ei ole selge süsteemi suhe EUCSi, NIS2, andmekaitsealaste auditite ja teiste sertifitseerimissüsteemidega. Ettepanek: Kehtestada võimalus kasutada olemasolevate auditite ja sertifikaatide tulemusi ning järgida põhimõtet „üks kord auditeeritud – kogu ELis tunnustatud“. Väikestele teenusepakujatele tuleks ette näha proportsionaalsed tasud, juhendamine ja võimalusel rahaline toetus. Vältida tuleb samade kontrollide kordamist eri õigusaktide alusel.	Arvestatud seisukohapunktis 6.9
Ettepanek: näha ette kiirendatud (lühendatud tähtajaga) tunnustamismenetlus pilvandmetööstuste teenuse osutajatele, kes teenindavad riiklikke kriitilisi tervishoiusüsteeme, et vältida teenusekatkestusi menetluse ajal.	Osaliselt arvestatud seisukohapunktis 6.9
Ettepanek: näha ette riiklik toetusmehhanism auditikulude osaliseks katmiseks väiksematele tervishoiu-IT lahenduste pakujatele, et kõrgema kindluse taseme nõue ei vähendaks konkurentsi Eesti tervishoiu-IT turul.	Osaliselt arvestatud seisukohapunktis 6.1 / 6.9 / 6.12
Ettepanek: võimaldada iga-aastase auditi läbivaatamise ajastust asutuste muude eelarve ja hooldustsüklitega, et vältida sertifikaadi kehtivuse katkemist tsüklilise koormuse kokkulangemise tõttu.	Osaliselt arvestatud seisukohapunktis 6.9
Kohustus hinnata iga kahe aasta järel avaliku sektori pilvekasutust on väga ulatuslik. Ebaselge on, kas hindamine toimub keskse riikliku hindamisena, valdkondade kaupa või iga asutuse ja infosüsteemi tasandil. Samuti võib Komisjoni võimalus nõuda liikmesriigilt kõrgema kindlustaseme rakendamist oluliselt mõjutada riigi eelarvet ja tehnoloogilisi valikuid. Ettepanek: Täpsustada, et riskihindamine võib tugineda olemasolevatele riiklikele riskijuhtimise, andmekaitse ja küberturvalisuse protsessidele.	Arvestatud seisukohapunktis 6.1 / 6.9
Ettepanek: töötada komisjoni metoodikale lisaks välja tervishoiuvaldkonna eripära (patsiendiohutus, ravi järjepidevus, eriliigilised isikuandmed) arvestav hindamislisa või -juhend.	Osaliselt arvestatud seisukohapunktis 6.2
Ettepanek: näha ette liikmesriigi konsulteerimis- ja vaidlustamisõigus enne, kui komisjon oma rakendusaktiga muudab liikmesriigi poolt määratud kindluse taset.	Arvestatud seisukohapunktis 6.2
Ettepanek: Näha ette erand või pikendamisvõimalus 12-kuulisest üleminekutähtajast eluliselt kriitiliste (tervishoiu)infosüsteemide puhul, koos nõudega faasiliseks, katkestusteta üleminekuks ja paralleeltöö perioodiks. Lisaks: Üleminekuperioodi määramisel tuleb arvesse võtta süsteemi keerukust, andmemahutu, hankemenetluse kestust, teenuse kriitilisust ning eelarvelisi võimalusi. Kohustus ei tohiks rakenduda enne, kui turul on nõutavale tasemele vastav ja majanduslikult mõistlik alternatiiv.	Arvestatud seisukohapunktis 6.3
Tähelepanek: Ebaselge on, kuidas toimida olukorras, kus sobiva kindlustasemega teenuseid ei ole turul piisavalt, nende hind on ebaproportsionaalselt kõrge või teenus ei vasta funktsionaalsetele vajadustele. Ettepanek: Erand peab olema kasutatav lisaks ajutisele hädaolukorrale ka turu puudumise,	Arvestatud seisukohapunktis 6.2

	<p>ebaproportsionaalse maksumuse, tehnilise sobimatuse ja toimepidevusrisi korral. Erandi kasutamise menetlus peab olema lihtne ning liikmesriigi pädeva asutuse otsustada.</p> <p>Ettepanek: lisada erandialuste loetellu selgesõnaliselt olukord, kus nõuetele vastava teenuse hankimine seaks ohtu inimelu (sh ravi järjepidevus jmt), analoogselt olemasolevate turupõhiste eranditega.</p> <p>Suured ühishanked võivad vähendada kulusid, ent samal ajal vähendavad need ka väiksemate pakkujate turulepääsu (puudutab just tarkvara ja AI-süsteeme kus on palju väiksseid ettevõtjaid ja spetsiifilisi tooteid). Ettepanekut sõnastada ei oska, ent komisjonile tuleks selgitada, et nendes teemades peaks vältima kõrgeid käibe ja referentsinõudeid jmt.</p> <p>Ettepanek: Kataloog peaks toimima olemasolevate repositooriumide metaandmete indeksi või födereeritud otsingulahendusena. Tarkvara peaks saama hoida riiklikus või asutuse enda repositooriumis ning ELi kataloogi tuleks edastada üksnes standarditud metaandmed ja viide</p>	<p>Arvestatud seisukohapunktis 6.2</p> <p>Arvestatud seisukohapunktis 6.6 / 6.12</p> <p>Arvestatud seisukohapunktis 6.5</p>
TEHIK	<p>ANNEX 2 level 2 g Kolmanda riigi kontroll pakkuja üle: Alates tasemest 2 peab pakkuja puhul olema õiguslike/tehniliste/organisatsiooniliste meetmetega välisriigi mõju (andmetele juurdepääs, teenuse häirimine, sanktsioonisurve). Selle nõudega ei oleks võimalik kasutada USA või potentsiaalselt teiste suuremate riikide pilvteenuseid. ETTEPANEK: Antud nõue võiks kohalduda tasemest 3 alates VÕI peaks olema sõnastatud oluliselt selgemalt, tehes selle täitmise realistlikumaks.</p> <p>ANNEX 2 level 2 i Lähtekoodi auditid: kolmanda riigi tootjate turvakriitilised komponendid peavad läbima lähtekoodi auditi. Siin on oluline aru saada, kuidas lähtekoodi auditeerimine toimib, kelle ülesanne see on ja mis mahus.</p> <p>ANNEX 2 level 2 i Migratsiooni plaan: määrus nõuab dokumenteeritud plaani, kuidas komponendist loobuda/asendada, kui tootja pankrotistub või kolmas riik kehtestab piirangud (nt ekspordikeeld, sanktsioonid). Oluline on teada, kui detailne peab migratsiooni plaan olema ja mis on selle komponendid, muul juhul võib selle täitmine olla väga keeruline kui mitte võimatu.</p>	<p>Osaliselt arvestatud seisukohapunktis 6.2</p>
	<p>Euroopa Komisjonist saab keskne hankija andmekeskuste, pilvteenuste, tarkvara ja AI-süsteemide ostmiseks. Kuigi Euroopa tasandil hankimine võib pakkuja Eesti hankijatele paremaid tingimusi ja mastaabisäästu, siis uute määruse nõuete valguses muutub see tegelikult ainsaks võimaluseks nõuetele vastav teenusepakkuja ühele eesti IT-majale hankida. Pilvteenuse pakkujad/AI lahenduste pakkujad ei osale Eesti hangetes. Hankijatel on võimalus vaid teenusepakkujate üldtingimustega nõustuda. Läbi Euroopa Komisjoni hangete teostamine on äärmiselt ajakulukas, kallis ja kaugel. Selle asemel võiks CADA määruse kohustused/nõuded seada hoopis Euroopas teenuste pakkujatele, et nende üldtingimused võimaldaksid kohe level 1, 2, 3 või 4 teenuse või muid nõutavaid eritingimusi valida. See tagaks ka Eesti erasektorile turvalised lahendused.</p>	<p>Osaliselt arvestatud seisukohapunktis 6.6 / 6.12</p>