EUROOPA
KOMISJON

Brüssel, 3.6.2026
COM(2026) 502 final

ANNEXES 1 to 3

LISAD

järgmise dokumendi juurde:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

millega kehtestatakse meetmete raamistik Euroopa pilvandmetöötluse ja tehisintellekti ökosüsteemi tugevdamiseks (pilvandmetöötluse ja tehisintellekti arendamise määrus)

{SEC(2026) 502 final} - {SWD(2026) 502 final} - {SWD(2026) 503 final}

I LISA

SUURED ÜLESANDED

1. Suur ülesanne nr 1. Liidu andmekeskuste keskkonnakestlikkus, toimivus ja turvalisus

Katsetada andmekeskuste tehnoloogiaid ja võtta need kogu liidus kasutusele, et ületada energia- ja ressursitõhususe tipptaset.

See hõlmab madalama elektrienergia kasutamise tõhususe näitaja (PUE) saavutamist ja serverite oluliselt suurema kasutusmäära võimaldamist. Näited on muu hulgas järgmised.

(1) ***Madalam elektrienergia kasutamise tõhususe keskmine näitaja.*** Liidu pilv- ja servandmetöötluse andmekeskuste keskkonnakestlikkuse ja toimivuse parandamine nii, et kogu liidus oleks keskmine energiakasutuse tõhusus (PUE) 1,15. Peamiselt keskendutakse järgmiste valdkondade arendamise võimaldamisele:

(a) andmekeskuste energiatõhususe tehnoloogiate, näiteks jahutuse ja heitsoojuse taaskasutamise täiustamine;

(b) kvantandmetöötluse tehnoloogiad pilve- ja andmetöötlustaristu käitamiseks;

(c) võrkude lõimimine ja energiajuhtimissüsteemide täiustamine;

(d) katseliinid järgmise põlvkonna energiatõhusate tehnoloogiate valideerimiseks käitamismahus.

(2) ***Andmekeskuste serverite keskmise kasutusmäära suurendamine.*** Serverite keskmise kasutusmäära suurendamine liidu andmekeskustes ligikaudu 50 %-ni, integreerides näiteks tehisintellektipõhiseid tehnoloogiaid serverite kasutusmäärade dünaamiliseks haldamiseks, käitusaegse töökoormuse haldamiseks ja ajastamiseks ning kasutusmäärade, energiakulude, termiliste piirangute ja nõutava latentsuse tasakaalustamiseks.

(3) ***Andmekeskuste turvalisuse ja vastupidavuse suurendamine.*** Andmekeskuste väärtus- ja tarneahelate turvalisuse ja vastupidavuse suurendamine, integreerides liidus projekteeritud ja toodetud pooljuht- ja kvanttehnoloogiaid ning parandades nende vastupanuvõimet füüsilistele ja küberohtudele, sealhulgas sihtrünnetele.

2. Suur ülesanne nr 2. Pilve tehnoloogiavirnad

Luua kogu pilve katvad riist- ja tarkvaralised tehnoloogiavirnad, sealhulgas tehisintellektivahendid, taristud, teenused ja halduskihid liidu kriitiliste võimsuspuudujääkide ületamiseks.

See hõlmab liidus projekteeritud ja toodetud pooljuhtidel ja kvanttehnoloogial põhinevate tehisintellektiserverite ehitamist tehisintellekti jaoks mõeldud hajutatud ja detsentraliseeritud pilv- ja servandmetöötluse jaoks.

Katseprogrammid võiksid aidata demonstreerida Euroopa avatud pilve tehnoloogiavirnade suutlikkust strateegiliselt olulistes sektorites.

3. Suur ülesanne nr 3. Eesliini tehisintellekt

Töötada välja järgmise põlvkonna multimodaalseid eesliini tehisintellekti mudeleid ja -süsteeme ning uudseid teedrajavaid võimeid.

Keskendutakse praeguse algoritmilise suutlikkuse piire nihutavate järgmise põlvkonna multimodaalsete mudelite ja süsteemide arhitektuuri projekteerimisele ja arendamisele, et saavutada parem toimivus keerulise loogika, modaalsustevahelise arusaamise ja agentsuse

valdkonnas; uuritakse uusi lähenemisviise mudelite tõhususe, kognitiivse modelleerimise, alternatiivsete arvutusstruktuuride jne jaoks.

Võimalikud rakendused võiksid hõlmata alusteadusi, näiteks teadusavastusi ja keerulisi andmetõlgendusi, ning maailmamudelite väljatöötamist keerulise loogika rakendamiseks, automatiseeritud juhtimissimulatsiooniks ja planeerimiseks.

4. Suur ülesanne nr 4. Füüsiline tehisintellekt

Töötada välja täiustatud füüsilise tehisintellekti mudelid ja süsteemid, mis töötavad autonoomselt ja ohutult, et tagada töökindel esemete käsitsemine ja navigeerimine struktureerimata keskkonnas.

Keskendutakse tarkvara ja selle alusriistvara arhitektuuri ühisele kavandamisele ning eesliini tehisintellekti meetodite kombineerimisele füüsilist loogikat toetavate maailmamudelitega, et tagada tugev käsitsemis-, navigeerimis- ja suhtlusvõime minimaalse inimjärelevalvega.

Võimalikud rakendused võiksid hõlmata autonoomseid roboteid, tööstussüsteeme ja droone, mis töötavad tegelikus dünaamilises keskkonnas.

5. Suur ülesanne nr 5. Tööstuslik tehisintellekt

Kiirendada Euroopa tööstusliku tehisintellekti väljatöötamist ja kasutuselevõtmist kõigis liidu strateegilistes sektorites.

Keskendutakse selliste Euroopa tööstusliku tehisintellekti mudelite ja süsteemide väljatöötamisele, mis suudavad teenindada väärtuslikke tööstusrakendusi. Sellised mudelid ja süsteemid peaksid olema kohandatavad sektoripõhiste kasutusjuhtumitega ja võimaldama turvalist kasutuselevõttu.

Selle suure ülesande raames käivitatud algatused peaksid tuginema spetsiaalsetele andmetöötlusressurssidele ja katsetamisvahenditele, mis on vajalikud tehisintellektisüsteemide valideerimiseks tegelikes keskkondades, enne nende ulatusliku väljatöötamise ja kasutuselevõtu toetamist, sealhulgas piirkondlikul ja kohalikul tasandil.

Autotööstuses võivad need algatused hõlbustada uuenduslike tarkvaraplatvormide ja tehisintellektimudelite väljatöötamist ja kasutuselevõttu automaatsõidusüsteemide jaoks, tootmises võivad need võimaldada luua spetsiaalseid mudeleid, mis optimeerivad tootmisprotsesse. Muud strateegilised sektorid, mis võiksid saada kasu tööstuslikust tehisintellektist, võivad olla tervishoid, energeetika, põllumajanduslik toidutööstus ja kaitse.

6. Suur ülesanne nr 6. Euroopa koostööpõhised tööstusmudelid

Töötada strateegiliste sektorite jaoks välja Euroopa koostööpõhised tööstusliku tehisintellekti mudelid ja süsteemid, võimaldades koostööd Euroopa tööstuse tasandil ilma osalejate tundliku äriteabe avaldamiseta.

Keskendutakse konfidentsiaalsust säilitavale tehnoloogiale. Nende mehhanismide hulka kuuluvad liidendatud ja hajutatud treeningmeetodid, mille puhul algoritmid tuuakse andmete juurde, selle asemel et andmeid kekselt edastada, turvalised täitmiskeskkonnad, krüpteerimispõhine töötlemine, anonüümimis- ja pseudonüümimismeetodid, juurdepääsu lahterdamine ning kaitse treenitud mudelitest tundliku äriteabe ekstraheerimise eest.

Strateegilised sektorid, mis võiksid saada kasu Euroopa koostööpõhistest tööstusliku tehisintellekti mudelitest ja süsteemidest, võivad olla lennundus ja kosmonautika, ravimid, küberturvalisus, liikuvus, autonoomsed sõidukid ja droonid, energeetika ja kaitse.

7. Suur ülesanne nr 7. Tehisaruagentide platvorm

Töötada välja Euroopa tehisaruagentide orkestreerimisraamistik, mis pakub olulist vahevara autonoomsete agentide vastupidavaks, turvaliseks ja ulatuslikuks kasutuselevõtuks.

Keskendutakse i) uuenduslike tehnoloogiliste paradigmade uurimisele, et võimaldada mitme tehisaruagendi tulemuslikku koostööd, mis ületab eraldiseisvate süsteemide suutlikkust, kuid samas järgib rangeid turvanõudeid, ning ii) tehisaruagentide suuremahuliseks haldamiseks mõeldud vastupidavate pilvepõhiste avatud platvormide loomisele.

Võimalikud rakendused võiksid hõlmata tervishoidu (näiteks kliiniliste otsuste tegemise toetamist ja teadusuuringute koordineerimist), küberturvalisust (näiteks ohtude avastamist ja neile reageerimist) ning alusteadusi.

8. Suur ülesanne nr 8. Avaliku sektori tehisintellekt

Töötada välja avaliku sektori kvaliteetsetel andmetel põhinevate ja esmatähtsatele valdkondadele (näiteks tervishoiule, avalikule haldusele, õigusele, kriisiohjele ja samuti avalikele teenustele) suunatud tehisintellektimudelid ja -süsteemid.

Keskendutakse avalike teenuste lahendustele, millel on eeldatavasti suur positiivne mõju kõige elutähtsamatele avalikele teenustele ja mida jagatakse avaliku sektori organisatsioonide eri tasandite vahel.

Üks eesmärk on võimaldada andmete jagamist ja eesliinimudelite väljatöötamist riiklike avalike teenuste jaoks, et suurendada mõju kogu liidu avalikule sektorile, sealhulgas tundlikke andmeid käitlevates valdkondades. Selle eesmärgi saavutamisele aitavad kaasa ka eraelu puutumatuse säilitamise raamistikud (näiteks liitõpe ja loomutruude sünteetiliste andmete genereerimine), mis võimaldavad treenida mudeleid ilma alusandmestike konfidentsiaalsust kahjustamata, ning meetmed nende mudelite laialdase kasutuselevõtu kiirendamiseks, sealhulgas piirkondlikul ja kohalikul tasandil.

II LISA

LIIDU TASANDI USALDUSVÄÄRSUSE TASEMETE KRITEERIUMID

Käesolevas lisas sätestatakse kriteeriumid, millele pilvandmetöötlusteenuse osutaja ja tema pilvandmetöötlusteenused peavad vastama, et teda tunnustataks liidu tasandi usaldusväärsuse 1., 2., 3. ja 4. taseme teenuste osutajana. Liidu tasandi usaldusväärsuse 1., 2., 3. ja 4. taseme kriteeriumide kohaldamisel kuulub „tarkvara“ määruse (EL) 2024/2847 artikli 3 punkti 4 tähenduses käesoleva lisa ja III lisa kohaldamisalasse. „Riistvara“ määruse (EL) 2024/2847 artikli 3 punkti 5 tähenduses ei kuulu kohaldamisalasse.

1. Liidu tasandi usaldusväärsuse 1. tase

1.1. Liidu tasandi usaldusväärsuse 1. taseme puhul peab pilvandmetöötlusteenuse osutaja vastama järgmistele kumulatiivsetele kriteeriumidele:

(a) pilvandmetöötlusteenuse osutaja on asutatud liidus;

(b) pilvandmetöötlusteenuse osutaja taristu ja vara, sealhulgas teenuse osutamises osalevate alltöövõtjate taristu ja vara, paiknevad liidus, välja arvatud juhul, kui avaliku sektori asutus nõuab selgesõnaliselt teisiti;

(c) kliendiandmed, sealhulgas metaandmed ja telemeetriaandmed, mida töötlevad, talletavad ja edastavad pilvandmetöötlusteenuse osutaja ja teenuse osutamises osalevad alltöövõtjad, jäävad igal ajal, sealhulgas enne või pärast teenuse konfigureerimist või kasutamist või selle ajal, eranditult liitu, välja arvatud juhul, kui avaliku sektori asutus nõuab selgesõnaliselt teisiti;

(d) kui pilvandmetöötlusteenuse osutaja tellib tehnilise ja operatiivtoe või -abi väljaspool liitu paiknevalt kolmandast isikust teenuseosutajalt, sealhulgas ka siis, kui see tellitakse omakorda väljastpoolt, rakendatakse vajalikke õiguslikke, tehnilisi ja korralduslikke meetmeid nende toimingute jälgitavuse, turvalisuse ja juhtimise tagamiseks, ning need toimingud ei tohi mingil viisil kahjustada pilvandmetöötlusteenuse osutaja tegevusautonoomiat;

(e) pilvandmetöötlusteenuse osutaja tõendab, et teenus vastab küberturvalisuse tippstandarditele;

(f) pilvandmetöötlusteenuse osutaja tagab alltöövõtjate kasutamise täieliku läbipaistvuse. Pilvandmetöötlusteenuse osutaja kohaldab alltöövõtjate suhtes hoolsuskohustust, lepingulisi kohustusi ja pidevat järelevalvet, et täita liidu õigusnormidest tulenevaid kohustusi;

(g) kui pilvandmetöötlusteenuse osutaja on kolmanda riigi või kolmandas riigis asutatud juriidilise isiku kontrolli all, tagab pilvandmetöötlusteenuse osutaja sõltumatutele allikatele tuginedes, et selles kolmandas riigis ei ole õigusakte ega tavasid, mis nõuaksid pilvandmetöötlusteenuse osutajalt tarkvara nõrkusi käsitleva teabe esitamist kõnealuse kolmanda riigi ametiasutustele enne, kui on teada, et neid nõrkusi on ära kasutatud.

1.2. Liidu tasandi usaldusväärsuse 1. taseme korral peab esimeses lõigus osutatud alltöövõtja olema selline kolmas isik, kellel on pilvandmetöötlusteenuse osutajaga otsene lepinguline suhe ja kes aitab kaasa pilvandmetöötlusteenuse pakkumisele ja osutamisele.

2. Liidu tasandi usaldusväärsuse 2. tase

2.1. Liidu tasandi usaldusväärsuse 2. taseme puhul peab pilvandmetöötlusteenuse osutaja vastama järgmistele kumulatiivsetele kriteeriumidele:

(a) auditeeritav teenuseosutaja ja auditeeritava teenuse osutamisega seotud alltöövõtjad on asutatud liidus;

(b) auditeeritava teenuseosutaja, sealhulgas teenuse osutamises osalevate alltöövõtjate taristu, vara ja töötajad paiknevad liidus;

(c) kliendiandmed, sealhulgas metaandmed ja telemeetriaandmed, mida töötlevad, talletavad ja edastavad auditeeritav teenuseosutaja ja teenuse osutamises osalevad alltöövõtjad, jäävad igal ajal, sealhulgas enne või pärast teenuse konfigureerimist või kasutamist või selle ajal, eranditult liitu, välja arvatud juhul, kui avaliku sektori asutus nõuab selgesõnaliselt teisiti;

(d) kui avaliku sektori asutus määrab, et on vaja kehtestada täiendavaid nõudeid töötajate taustakontrollile ja liidu kodakondsusele, peab auditeeritav teenuseosutaja tagama nendele nõuetele vastavate töötajate olemasolu;

(e) auditeeritav teenus saab määruse (EL) 2019/881 alusel loodava pilvandmetöötlusteenuseid hõlmava Euroopa küberturvalisuse sertifitseerimise kava alusel Euroopa küberturvalisuse sertifikaadi vähemalt märkimisväärse usaldusväärsuse taseme kohta tingimusel, et kava on selle määruse alusel vastu võetud ja pilvandmetöötlusteenuse osutajatele kättesaadav. Kuni sellise kava vastuvõtmiseni tuleb kohaldada riiklikke küberturvalisuse sertifitseerimise kavasid, kui need on olemas. Kui liidu või liikmesriigi küberturvalisuse sertifitseerimise kava puudub, peab auditeeritav teenuseosutaja tõendama, et teenus vastab kohaldatava liidu õiguse kohastele kõrgeimatele küberturvalisuse standarditele;

(f) auditeeritava teenuse kasutamisel genereeritud andmeid ei kasutata kolmanda riigi või kolmandas riigis asutatud juriidilise isiku käitatava tehisintellektisüsteemi treenimiseks ega peenhäälestamiseks ning neid ei edastata ühelgi juhul väljapoole liitu;

(g) kui auditeeritav teenuseosutaja ja auditeeritava teenuse osutamises osalevad alltöövõtjad on kolmanda riigi või kolmandas riigis asutatud juriidilise isiku kontrolli all, tõendavad nad, et on rakendatud vajalikke õiguslikke, tehnilisi ja korralduslikke meetmeid tagamaks, et:

i) on välistatud kolmanda riigi või kolmandas riigis asutatud juriidilise isiku kontroll auditeeritava teenuseosutaja üle viisil, mis piirab teenuseosutaja suutlikkust teenust pakkuda ja osutada, seab piiranguid teenuse osutamiseks vajalikule taristule, varale ja töötajatele või halvendab auditeeritava teenuse osutamiseks vajalikku suutlikkust ja standardeid;

ii) on välistatud kolmanda riigi või kolmandas riigis asutatud juriidilise isiku juurdepääs kliendiandmetele;

iii) on välistatud võimalus, et kolmas riik või kolmandas riigis asutatud juriidiline isik häirib teenuse järjepidevust ja/või halvendab teenuse kvaliteeti;

iv) on välistatud kolmanda riigi või kolmandas riigis asutatud juriidilise isiku kontroll auditeeritava teenuseosutaja üle viisil, mis kohustab auditeeritavat teenuseosutajat rakendama, jõustama, kohaldama või järgima kolmanda riigi kehtestatud piiravaid meetmeid, nagu sanktsioonirežiimid, embargod või mis tahes samaväärsed õiguslikud või haldusmeetmed, välja arvatud juhul, kui sellised meetmed on liikmesriikide või liidu õiguse kohaselt õiguspärased;

(h) auditeeritava teenusega seotud tehnilist ja operatiivtuge või -abi, sealhulgas ka siis, kui sisseostetud teenuse osutaja tellib seda omakorda väljastpoolt, algatatakse ja osutatakse eranditult üksnes liidus;

(i) auditeeritav teenuseosutaja tõendab, et kehtestatud on järgmised tarkvara tarneahela meetmed:

i) määruse (EL) 2024/2847 artikli 3 punktis 39 määratletud täielik ja ajakohane tarkvara koostenimekiri ning teenuse osutamisega seoses kindlaks tehtud sõltuvuste loetelu dokumenteeritakse ja tehakse auditeerivale organisatsioonile kättesaadavaks;

ii) kui määruse (EL) 2024/2847 artikli 3 punktis 6 määratletud tarkvarakomponente või tooteid pakub, omab ja litsentsib kolmandas riigis asutatud juriidiline isik, rakendatakse ja dokumenteeritakse kontrollimeetmed, et blokeerida kõik kaugfunktsioonid, mis võivad seadet, süsteemi või tarkvara oluliselt rikkuda või häirida (sealhulgas uuenduste ajal), ning tagatakse, et kolmanda riigi ja määruse (EL) 2024/2847 artikli 3 punkti 13 määratlusele vastava tarkvaratootja valmistatud ja turvalisusega seotud komponentidele tehakse lähtekoodi auditid, ja et on olemas dokumenteeritud üleviimiskava juhuks, kui müüja ei suuda oma kohustusi täita või kui kolmas riik kehtestab piirangud;

iii) kui pilvandmetöötlusteenuse osutaja on kolmanda riigi või kolmandas riigis asutatud juriidilise isiku kontrolli all, tagab pilvandmetöötlusteenuse osutaja sõltumatutele allikatele tuginedes, et selles kolmandas riigis ei ole õigusakte ega tavasid, mis nõuaksid pilvandmetöötlusteenuse osutajalt tarkvara nõrkusi käsitleva teabe esitamist kõnealuse kolmanda riigi ametiasutustele enne, kui on teada, et neid nõrkusi on ära kasutatud;

(j) kui teenuse osutamiseks kasutatakse avatud lähtekoodi litsentsi alusel välja antud tarkvara, tõendab auditeeritav teenuseosutaja, et ta on rakendanud ja dokumenteerinud asjakohased kontrollimeetmed, et välistada kaugfunktsioonid või -mehhanismid, mida saaks kasutada seadme, süsteemi või tarkvara oluliseks rikkumiseks või häirimiseks;

(k) kui auditeeritav teenuseosutaja osutab oma teenuseid kogu maailmas ja tal on kolmandas riigis tütarettevõtja, on auditeeritav teenuseosutaja rakendanud vajalikud meetmed, et tagada ja jõustada liidus paikneva emaettevõtja ja iga sellise kolmanda riigi tütarettevõtja tõhus õiguslik, tehniline ja organisatsiooniline eraldamine.

2.2. Liidu tasandi usaldusväärsuse 2. taseme korral peab esimeses lõigus osutatud alltöövõtja olema selline kolmas isik, kellel on pilvandmetöötlusteenuse osutajaga otsene lepinguline suhe ja kes aitab kaasa pilvandmetöötlusteenuse pakkumisele ja osutamisele.

3. Liidu tasandi usaldusväärsuse 3. tase

3.1. Liidu tasandi usaldusväärsuse 3. taseme puhul peab pilvandmetöötlusteenuse osutaja vastama järgmistele kumulatiivsetele kriteeriumidele:

(a) auditeeritav teenuseosutaja ja auditeeritava teenuse osutamisega seotud alltöövõtjad on asutatud liidus;

(b) auditeeritava teenuseosutaja, sealhulgas teenuse osutamises osalevate alltöövõtjate taristu, vara ja töötajad paiknevad liidus;

(c) kliendiandmed, sealhulgas metaandmed ja telemeetriaandmed, mida töötlevad, talletavad ja edastavad auditeeritav teenuseosutaja ja teenuse osutamises osalevad

alltöövõtjad, jäävad igal ajal, sealhulgas enne või pärast teenuse konfigureerimist või kasutamist või selle ajal, eranditult liitu, välja arvatud juhul, kui avaliku sektori asutus nõuab selgesõnaliselt teisiti;

(d) töötajad, sealhulgas auditeeritava teenuse osutamisega seotud alltöövõtjate töötajad, on liidu kodanikud, ja kui töötajad käitlevad määruse (EL) 2021/697 artikli 2 punktis 21 määratletud salastatud teavet, peavad nad asjakohasel juhul olema läbinud ka liikmesriigis vajaliku riikliku julgeolekukontrolli;

(e) auditeeritav teenus saab määruse (EL) 2019/881 alusel loodava pilvandmetöötlusteenuseid hõlmava Euroopa küberturvalisuse sertifitseerimise kava alusel Euroopa küberturvalisuse sertifikaadi vähemalt märkimisväärse usaldusväärsuse taseme kohta tingimusel, et kava on selle määruse alusel vastu võetud ja pilvandmetöötlusteenuse osutajatele kättesaadav. Kuni sellise kava vastuvõtmiseni tuleb kohaldada riiklikke küberturvalisuse sertifitseerimise kavasid, kui need on olemas. Kui liidu või liikmesriigi küberturvalisuse sertifitseerimise kava puudub, peab auditeeritav teenuseosutaja tõendama, et teenus vastab kohaldatava liidu õiguse kohastele kõrgeimatele küberturvalisuse standarditele;

(f) auditeeritava teenuse kasutamisel genereeritud andmeid ei kasutata kolmanda riigi või kolmandas riigis asutatud juriidilise isiku käitatava tehisintellektisüsteemi treenimiseks ega peenhäälestamiseks ning neid ei edastata ühelgi juhul väljapoole liitu;

(g) auditeeritav teenuseosutaja ja auditeeritava teenuse osutamises osalevad alltöövõtjad ei ole kolmanda riigi või kolmandas riigis asutatud juriidilise isiku kontrolli all. Erandina sellest kriteeriumist võib pilvandmetöötlusteenuse osutajat ja auditeeritava teenuse osutamises osalevaid alltöövõtjaid, kes on kolmanda riigi või kolmandas riigis asutatud juriidilise isiku kontrolli all, auditeerida liidu tasandi usaldusväärsuse 3. taseme saamiseks siis, kui komisjon on võtnud vastu artikli 19 kohase rakendusakti. Kui komisjon on vastu võtnud artikli 19 kohase rakendusakti, peavad auditeeritav teenuseosutaja ja auditeeritava teenuse osutamises osalevad alltöövõtjad samuti tõendama, et on rakendatud vajalikud õiguslikud, tehnilised ja korralduslikud meetmed tagamaks, et:

i) on välistatud kolmanda riigi või kolmandas riigis asutatud juriidilise isiku kontroll auditeeritava teenuseosutaja üle viisil, mis piirab teenuseosutaja suutlikkust teenust pakkuda ja osutada, seab piiranguid teenuse osutamiseks vajalikule taristule, varale ja töötajatele või halvendab auditeeritava teenuse osutamiseks vajalikku suutlikkust ja standardeid. Auditeeritav teenuseosutaja peab võimaldama mõistliku juurdepääsu lähtekoodile;

ii) on välistatud kolmanda riigi või kolmandas riigis asutatud juriidilise isiku juurdepääs kliendiandmetele;

iii) on välistatud võimalus, et kolmas riik või kolmandas riigis asutatud juriidiline isik häirib teenuse järjepidevust ja/või halvendab teenuse kvaliteeti;

iv) on välistatud kolmanda riigi või kolmandas riigis asutatud juriidilise isiku kontroll auditeeritava teenuseosutaja üle viisil, mis kohustab auditeeritavat teenuseosutajat rakendama, jõustama, kohaldama või järgima kolmanda riigi kehtestatud piiravaid meetmeid, nagu sanktsioonirežiimid, embargod või mis tahes samaväärsed õiguslikud või haldusmeetmed, välja arvatud juhul, kui sellised meetmed on liikmesriikide või liidu õiguse kohaselt õiguspärased;

(h) auditeeritava teenusega seotud tehnilist ja operatiivtuge või -abi, sealhulgas ka siis, kui sisseostetud teenuse osutaja tellib seda omakorda väljastpoolt, algatab ja osutab

eranditult liidus üksnes selline töötaja, kes on liidu resident, või kolmas isik, kes ei ole kolmanda riigi või kolmandas riigis asutatud juriidilise isiku kontrolli all;

(i) auditeeritav teenuseosutaja tõendab, et kehtestatud on järgmised tarkvara tarneahela meetmed:

i) täielik ja ajakohane tarkvara koostenimekiri ning teenuse osutamisega seoses kindlaks tehtud sõltuvuste loetelu dokumenteeritakse ja tehakse auditeerivale organisatsioonile kättesaadavaks;

ii) kui tarkvarakomponente või tooteid pakub, omab ja litsentsib kolmandas riigis asutatud juriidiline isik, rakendatakse ja dokumenteeritakse kontrollimeetmed, et blokeerida kõik kaugfunktsioonid, mis võivad seadet, süsteemi või tarkvara oluliselt rikkuda või häirida (sealhulgas uuenduste ajal), ning tagatakse, et kolmanda riigi tootja valmistatud ja turvalisusega seotud komponentidele tehakse lähtekoodi auditid, ja et on olemas dokumenteeritud üleviimiskava juhuks, kui tarnija ei suuda oma kohustusi täita või kui kolmas riik kehtestab piirangud;

iii) kui pilvandmetöötlusteenuse osutaja on kolmanda riigi või kolmandas riigis asutatud juriidilise isiku kontrolli all, tagab pilvandmetöötlusteenuse osutaja sõltumatutele allikatele tuginedes, et selles kolmandas riigis ei ole õigusakte ega tavasid, mis nõuaksid pilvandmetöötlusteenuse osutajalt tarkvara nõrkusi käsitleva teabe esitamist kõnealuse kolmanda riigi ametiasutustele enne, kui on teada, et neid nõrkusi on ära kasutatud;

(j) kui teenuse osutamiseks kasutatakse avatud lähtekoodi litsentsi alusel välja antud tarkvara, tõendab auditeeritav teenuseosutaja, et ta on rakendanud ja dokumenteerinud asjakohased kontrollimeetmed, et välistada kaugfunktsioonid või -mehhanismid, mida saaks kasutada seadme, süsteemi või tarkvara oluliseks rikkumiseks või häirimiseks;

(k) kui auditeeritav teenuseosutaja osutab oma teenuseid väljaspool liitu ja tal on kolmandas riigis tütarettevõtja, tõendab auditeeritav teenuseosutaja, et ta on rakendanud vajalikud meetmed, et tagada ja jõustada liidus paikneva emaettevõtja ja iga sellise kolmanda riigi tütarettevõtja tõhus õiguslik, tehniline ja organisatsiooniline eraldamine.

3.2. Liidu tasandi usaldusväärsuse 3. taseme korral peab esimeses lõigus osutatud alltöövõtja olema kolmas isik, kellel on pilvandmetöötlusteenuse osutajaga otsene lepinguline suhe, kes aitab kaasa pilvandmetöötlusteenuse pakkumisele ja osutamisele ning kes võib vajada juurdepääsu salastatud või tundlikule teabele, nagu on määratletud määruse (EL) 2021/697 artikli 2 punktis 22.

4. Liidu tasandi usaldusväärsuse 4. tase

4.1. Liidu tasandi usaldusväärsuse 4. taseme puhul peab pilvandmetöötlusteenuse osutaja vastama järgmistele kumulatiivsetele kriteeriumidele:

(a) auditeeritav teenuseosutaja ja auditeeritava teenuse osutamisega seotud alltöövõtjad on asutatud liidus;

(b) auditeeritava teenuseosutaja taristu, vara ja töötajad, sealhulgas teenuse osutamisega seotud alltöövõtjad, paiknevad liidus;

(c) kliendiandmed, sealhulgas riskihindamise tulemusel tundliku teabena määratletud metaandmed ja telemeetriaandmed, mida töötlevad, talletavad ja edastavad auditeeritav teenuseosutaja ja tema teenuse osutamises osalevad alltöövõtjad, jäävad

igal ajal, sealhulgas enne või pärast teenuse konfigureerimist või kasutamist või selle ajal, eranditult liitu;

(d) töötajad, sealhulgas auditeeritava teenuse osutamisega seotud alltöövõtjate töötajad, on liidu kodanikud, ja kui töötajad käitlevad salastatud teavet, peavad nad asjakohasel juhul olema läbinud ka liikmesriigis vajaliku riikliku julgeolekukontrolli;

(e) auditeeritav teenus saab määruse (EL) 2019/881 alusel loodava pilvandmetöötlusteenuseid hõlmava Euroopa küberturvalisuse sertifitseerimise kava alusel Euroopa küberturvalisuse sertifikaadi vähemalt kõrge usaldusväärsuse taseme kohta tingimusel, et kava on selle määruse alusel vastu võetud ja pilvandmetöötlusteenuse osutajatele kättesaadav. Kuni sellise kava vastuvõtmiseni tuleb kohaldada riiklikke küberturvalisuse sertifitseerimise kavasid, kui need on olemas. Kui liidu või liikmesriigi küberturvalisuse sertifitseerimise kava puudub, peab auditeeritav teenuseosutaja tõendama, et teenus vastab kohaldatava liidu õiguse kohastele kõrgeimatele küberturvalisuse standarditele;

(f) auditeeritava teenuse kasutamisel genereeritud andmeid ei kasutata kolmanda riigi või kolmandas riigis asutatud juriidilise isiku käitatava tehisintellektisüsteemi treenimiseks ega peenhäälestamiseks ning neid ei edastata ühelgi juhul väljapoole liitu;

(g) auditeeritav teenuseosutaja ja auditeeritava teenuse osutamises osalevad alltöövõtjad ei ole kolmanda riigi või kolmandas riigis asutatud juriidilise isiku kontrolli all;

(h) auditeeritava teenusega seotud tehnilist ja operatiivtuge või -abi, sealhulgas ka siis, kui sisseostetud teenuse osutaja tellib seda omakorda väljastpoolt, algatab ja osutab eranditult liidus üksnes selline töötaja, kes on liidu resident, või kolmas isik, kes ei ole kolmanda riigi või kolmandas riigis asutatud juriidilise isiku kontrolli all;

(i) auditeeritav teenuseosutaja tõendab, et kehtestatud on järgmised tarkvara tarneahela meetmed:

  i) täielik ja ajakohane tarkvara koostenimekiri ning teenuse osutamisega seoses kindlaks tehtud sõltuvuste loetelu dokumenteeritakse ja tehakse auditeerivale organisatsioonile kättesaadavaks;

  ii) on rakendatud meetmed tegeliku kontrolli säilitamiseks tarkvarakomponentide või toodete üle, tõendades, et kolmas riik või kolmandas riigis asutatud juriidiline isik ei oma ega teosta tegelikku kontrolli nende komponentide või toodete projekteerimise, väljatöötamise, hooldamise ega arendamise üle. Tegelik kontroll hõlmab võimet oluliselt mõjutada komponendi tehnilist arendamist, hooldusprioriteete, turvalisuse parandamist ja pikaajalist järjepidevust;

(j) kui kasutatakse avatud lähtekoodi litsentsi alusel välja antud tarkvara, tõendab auditeeritav teenuseosutaja, et ta on rakendanud ja dokumenteerinud asjakohased kontrollimeetmed, et välistada kaugfunktsioonid või -mehhanismid, mida saaks kasutada seadme, süsteemi või tarkvara oluliseks rikkumiseks või häirimiseks;

(k) kui auditeeritav teenuseosutaja osutab oma teenuseid väljaspool liitu ja tal on kolmandas riigis tütarettevõtja, tõendab auditeeritav teenuseosutaja, et ta on rakendanud vajalikud meetmed, et tagada ja jõustada liidus paikneva emaettevõtja ja iga sellise kolmanda riigi tütarettevõtja tõhus õiguslik, tehniline ja organisatsiooniline eraldamine.

4.2. Liidu tasandi usaldusväärsuse 4. taseme korral peab esimeses lõigus osutatud alltöövõtja olema kolmas isik, kellel on pilvandmetöötlusteenuse osutajaga otsene lepinguline suhe, kes aitab kaasa pilvandmetöötlusteenuse pakkumisele ja osutamisele

ning kes teenuse osutamiseks võib vajada juurdepääsu salastatud või tundlikule teabele.

III LISA

AUDITI TÕENDUSMATERJAL AUDITIPROTSEDUURI JAOKS

Kui auditeerivad organisatsioonid hindavad auditeeritava teenuse vastavust II lisas sätestatud auditi kriteeriumidele, peaksid nad auditeeritavalt teenuseosutajalt nõudma käesolevas lisas loetletud auditi tõendusmaterjale.

Käesolev lisa on soovituslik ega sea piiranguid tõendusmaterjalidele, mida auditeerivad organisatsioonid võivad nõuda või arvesse võtta. Audiitorid võivad küsida mis tahes lisateavet, et auditi tegemisel tagada nõuetele vastavuse põhjalik ja täpne hindamine. Kuigi nõutavad tõendid võivad olla samad, erinevad analüüsitavad aspektid sõltuvalt usaldusväärsuse taseme kriteeriumidest ja nende rangusest.

1. Auditi kriteerium A: asutamine liidus

Auditeeriv organisatsioon peaks hindama II lisas loetletud liidu tasandi usaldusväärsuse 2., 3. ja 4. taseme punktis a nimetatud auditi kriteeriumeid järgmise põhjal.

(1) Tõendid selle kohta, et auditeeritav teenuseosutaja on asutatud liidus liikmesriigi õiguse alusel või on moodustatud muul viisil kooskõlas liidu liikmesriigi äriühinguõigusega.

(2) Tõendid selle kohta, et auditeeritava teenuseosutaja registrijärgne asukoht, juhatuse asukoht ja peamine tegevuskoht on liidus.

(3) Auditeeriv organisatsioon peaks kontrollima, kas auditeeritava teenuseosutaja suhtes kohaldatakse liidu õigusraamistikku ja tema tegevuskoht on tõeline ja püsiv või kvalifitseerub auditeeritav teenuseosutaja üksnes ELi-väliseks teenuseosutajaks, kes pakub teenuseid liidus.

(4) Auditeeriv organisatsioon peaks kontrollima, kas teenuseosutaja on seaduslikult asutatud liidu liikmesriigis. Tõendid selle kohta võivad muu hulgas hõlmata äriregistri väljavõtteid, maksuresidentsuse dokumente, tegevuslube, käibemaksukohustuslasena registreerimist, kontrollimist, kas teenuseosutaja on registreeritud registrite sidestamise süsteemis ja käibemaksuteabe vahetamise süsteemis.

(5) Auditeeriv organisatsioon peaks kontrollima auditeeritava teenuseosutaja püsivat ja tegelikku kohalolekut liidus. Auditeeriv organisatsioon peaks seetõttu kontrollima, et:

   (a) ELis on olemas füüsilised kontorid või tööruumid (näiteks rendilepingute, kommunaalteenuste arvete või kinnisvaradokumentide põhjal);

   (b) alalised töötajad paiknevad liidus ja klienditoega seotud toiminguid tehakse liidus (näiteks töölepingute, palgaarvestuse, tööajatabelite põhjal);

   (c) lepingutega seotud toiminguid tehakse liidus (näiteks tegevuspõhise halduse andmete, intsidentidest teatamise andmete põhjal);

   (d) pangandus- ja raamatupidamisfunktsioonid on üksnes liidus (näiteks finantsaruannete ja kohustusliku auditi aruannete põhjal).

(6) Auditeeriv organisatsioon peaks kontrollima ELi liikmesriikide üksuste või filiaalide olemasolu (näiteks rendilepingute, kommunaalteenuste arvete, kinnisvaradokumentide, töölepingute, tööajatabelite, palgaarvestuse või ostutellimuste põhjal).

2. Auditi kriteerium B: taristu, vara ja töötajate asukoht

Auditeeriv organisatsioon peaks hindama II lisas loetletud liidu tasandi usaldusväärsuse 2., 3. ja 4. taseme punktis b nimetatud auditi kriteeriumeid järgmise põhjal.

(1) Taristu asukoht

(a) Auditeeritava teenuse osutamiseks kasutatava taristu asukohtade ja andmetalletuskohtade loetelu koos asjakohaste üksikasjadega. See loetelu peaks sisaldama taristu täpset asukohta (hoone number, tänav, linn, sihtnumber ja riik), mis näitab, et auditeeritava teenuse osutamisel püsivad kõik elemendid liidus. See hõlmab põhitalletuskohta ning varukoopiate, avariitaaste andmete ja logide talletamise asukohta.

(b) Mis tahes muud tõendid selle kohta, et IT-taristu paikneb liidus, näiteks rendilepingud, omandiõigust tõendavad dokumendid, hooldusleping, teenuslepingud, rajatiste pääsulogid.

(c) Võrguskeemid ja arhitektuuridokumendid, mis näitavad, et andmete talletamiseks ja töötlemiseks, sealhulgas varundamiseks ja kopeerimiseks, kasutatakse ainult liidus paiknevat taristut.

(2) Vara asukoht

(a) Auditeeritava teenuse osutamisel kasutatava vara loetelu ja asjakohased üksikasjad, näiteks vararegister.

(b) Tõendid selle kohta, et serverid, seadmed ja tegevuseks vajalikud varad paiknevad liidus, näiteks serveri ja selle asukoha andmed, ostuarved, saatelehed, litsentsilepingud, tellimislepingud või tarkvaraostude või -tellimuste arved, riistvara korral arved koos tarnetõenditega.

(c) Tõendid selle kohta, et teenuste osutamise suutlikkus paikneb liidus, näiteks kasutuselevõtu andmed, paigaldusandmed, teenuse oleku aruanded, konfiguratsiooniaruanded, järelevalveväljundid, teenuse kasutamist näitavad halduslogid.

(3) Töötajate asukoht

(a) Auditeeritava teenuse osutamises osalevate töötajate nimekiri ja asjakohased üksikasjad.

(b) Tõendid selle kohta, et auditeeritava teenuse osutamises osalevad töötajad paiknevad liidus, sealhulgas töölepingud, palgaarvestusdokumendid, tööajatabelid, tegevusdokumendid ja organisatsiooni skeemid, millel on näidatud liidus paiknevad töötajad, kellel on tegevuskohustused.

(4) Taristu, vara ja töötajatega seotud kaalutlused

(a) Auditeeriv organisatsioon peaks hindama ka seda, kus selline taristu, vara või töötajad:

i) kliendiandmeid talletavad, edastavad, töötlevad või käitlevad muul viisil või pääsevad neile juurde;

ii) tagavad, võimaldavad või võiksid võimaldada halduslikku juurdepääsu kliendiandmetele, kontrolli nende üle, nende konfigureerimist või nähtavust;

iii) võivad rikkumise, valesti konfigureerimise, kättesaamatuks muutmise või katkemise korral põhjendatult kaasa tuua auditeeritava teenuse katkemise või kättesaamatuse.

NB! *„Taristu“ – füüsiline taristu, sealhulgas andmekeskuse taristu või koospaiknemistaristu, võrk, jahutus ja IT-süsteemid, mis võimaldavad andmekeskust hallata.*

„Vara“ – riist- ja tarkvara, mis võimaldab osutada pilvandmetöötlusteenust, sealhulgas teegid, krüptomaterjalid ja tarkvarakomponentide suhtlemiseks vajalik sisevõrk.

„Töötajad“, sealhulgas alltöövõtjate hallatavad töötajad – isikud, kes toetavad auditeeritava teenuse osutamist, haldamist, turvalisust, kättesaadavust või toimimist.

3. Auditi kriteerium C: andmete paiknemine liidus

Auditeeriv organisatsioon peaks hindama II lisas loetletud liidu tasandi usaldusväärsuse 2., 3. ja 4. taseme punktis c nimetatud auditi kriteeriumeid järgmise põhjal.

(1) Tõendid selle kohta, et kliendiandmeid talletatakse ja töödeldakse üksnes liidus ning kolmas isik või alltöövõtja, kes ei vasta käesolevas lisas sätestatud tingimustele, ei ole ühelgi juhul tehniliselt ega tegevuslikult ilma eelneva loata võimeline kliendiandmetele juurde pääsema, neid hankima, kättesaamatuks muutma, hävitama või üldisemalt töötlema. Näiteks pääsulogid, pääsupoliitika tugiteenuste osutajatele, eelispääsukirjed, varundatud andmete talletamise põhimõtted ning andmevooskeem, mis näitab, kus kliendiandmeid talletatakse, töödeldakse, kopeeritakse ja varundatakse. Isikuandmete töötlemisel määruse (EL) 2016/679 järgimist tõendavad lepingud alltöövõtjatega.

(2) Logide ja järelevalveandmete põhised tõendid, mis näitavad, et kõiki andmeid talletatakse ja töödeldakse üksnes liidus. Näiteks teenuste raamlepingud, andmetöötluslepingud, andmete asukohta reguleerivad lepingud või ELi andmepiirid.

(3) Tõendid (näiteks avaliku sektori asutustele pakutavad lepingulised kokkulepped, logid ja menetlused), mis näitavad, et auditeeritav teenuseosutaja ja auditeeritava teenuse osutamises osalevad alltöövõtjad on võtnud vajalikud meetmed tagamaks, et:

   (a) kliendiandmeid, sealhulgas krüpteeritud andmeid, ei edastata väljapoole liitu ilma avaliku sektori asutuse heakskiiduta;

   (b) andmeid ei edastata ühelegi kolmandale isikule peale teenuse osutamises osalevate alltöövõtjate ja avaliku sektori asutuse poolt selgesõnaliselt volitatud vastuvõtjate.

(4) Andmevooskeem, mis näitab andmevooge pilvandmetöötlusteenuse osutaja ja kliendiandmete, kolmanda isiku teenuste ja alltöövõtjate vahel. Skeemil peab olema selgelt märgitud andmete allikas ja sihtkoht ning peab olema näidatud, et andmed ei lahku liidust.

NB! Käesoleva lisa kohaldamisel tähendab klient avaliku sektori asutust, kes on sõlminud pilvandmetöötlusteenuse osutajaga lepingu või muu õiguslikult siduva kokkuleppe pilvandmetöötlusteenusele juurdepääsuks või selle kasutamiseks.

„Kliendiandmed“ võivad olla mis tahes andmed, mis on pilvandmetöötlusteenuse kliendi kontrolli all kas õiguslikul, lepingulisel või muul alusel ning mis on:

   (a) pilvandmetöötlusteenusesse sisestatud kliendi poolt või nimel, sealhulgas autentimismandaadiga;

   (b) toodetud, kui klient kasutab pilvandmetöötlusteenust.

Kliendiandmed võivad hõlmata ka auditeeritavate teenuseosutajate kontrolli all olevaid andmeid, mis on saadud pilvteenuse kliendi ja auditeeritava teenuse suhtluse tulemusena. See

hõlmab kliendiandmeid ja pilvandmetöötlusteenuste kasutamisest tulenevaid andmeid (st telemeetria, metaandmed).

„Pilvandmetöötlusteenuse abil saadud andmed“ – see osa logiandmetest, mis sisaldab andmeid selle kohta, kes, millal ja milliste funktsioonidega teenust kasutas, mis liiki andmetega on tegemist jne. See võib sisaldada ka teavet volitatud kasutajate arvu ja nende identiteedi kohta. See võib hõlmata ka konfiguratsiooni- või kohandamisandmeid, kui pilvandmetöötlusteenusel on sellised konfiguratsiooni- või kohandamisfunktsioonid.

4. Auditi kriteerium D: liidu kodakondsus

Auditeeriv organisatsioon peaks hindama II lisas loetletud liidu tasandi usaldusväärsuse 2., 3. ja 4. taseme punktis d nimetatud auditi kriteeriumeid järgmise põhjal.

(1) Auditeeritav teenuseosutaja peaks esitama auditeerivale organisatsioonile tõendid selle kohta, et ta on rakendanud meetmeid tagamaks, et kui avaliku sektori asutus seab liidu kodakondsuse nõude, on auditeeritava teenuse osutamises osalevad töötajad liidu kodanikud. Seda saab tõendada valitsuse väljastatud kehtivate ametlike dokumentidega (näiteks kehtiv pass ja liikmesriigi isikutunnistus).

(2) Auditeeritav teenuseosutaja peaks esitama organisatsiooni skeemid ja ametijuhendid, mis kinnitavad, et ta suudab nõudmise korral tagada, et auditeeritava teenuse toimimisele, juhtimisele, hooldusele ja toele on juurdepääs ainult liidu kodakondsusega töötajatel.

(3) Auditeeritav teenuseosutaja peaks esitama dokumendid, milles on pääsupoliitika, ja kontrolljäljed, mis näitavad, et teenuse süsteemidele ja andmetele on juurdepääs ainult volitatud töötajatel, kes on liidu kodanikud.

(4) Auditeeritav teenuseosutaja peaks tõendama, et tal on juhendid, milles kirjeldatakse, kuidas kontrollitakse kodakondsust enne tööle määramist ja kuidas säilitatakse vastavus sellele auditi kriteeriumile kogu töösuhte jooksul.

***NB!** Auditeeritava teenuse osutamises osalevate töötajate hulka võivad kuuluda töötajad, kellel on loogiline või füüsiline juurdepääs pilvandmetöötlusteenuse osutamiseks kasutatavale taristule ja varale, samuti klienditoe eest vastutavad töötajad ning kõik töötajad, kellel on kontroll pilvandmetöötlusteenuse osutaja juhtimise üle.*

5. Auditi kriteerium E: määruse (EL) 2019/881 alusel vastu võetud Euroopa küberturvalisuse sertifitseerimise kava

Auditeeriv organisatsioon peaks hindama II lisas loetletud liidu tasandi usaldusväärsuse 2., 3. ja 4. taseme punktis e nimetatud auditi kriteeriumeid järgmise põhjal.

(1) Kehtiv Euroopa küberturvalisuse sertifikaat, mille on välja andnud pädev vastavushindamisasutus ja mis tõendab, et auditeeritavat teenust on hinnatud ja see vastab määruse (EL) 2019/881 alusel vastu võetud Euroopa küberturvalisuse sertifitseerimise kava kohase usaldusväärsuse baastaseme, märkimisväärse taseme või kõrge taseme nõuetele, tingimusel et selline kava on kehtestatud.

(2) Sertifitseerimisaruanne, mis sisaldab auditisertifikaadiga hõlmatud pilvandmetöötlusteenuse väljatöötamiseks ja käitamiseks kasutatud peamiste komponentide kirjeldust.

(3) Kuni pilvandmetöötlusteenuseid hõlmava Euroopa küberturvalisuse sertifitseerimise kava kehtestamiseni saab auditeeritav teenuseosutaja tõendada nõuetele vastavust kehtivate küberturvalisuse sertifikaatide abil. See võib hõlmata muu hulgas järgmist:

(a) kehtiv sertifikaat, mille on välja andnud pädev vastavushindamisasutus (kooskõlas standardiga CEN/CLC/TS 18072:2025), ja mis tõendab, et pilvandmetöötlusteenust on hinnatud ja see vastab standardis CEN/TS 18026:2024 määratletud usaldusväärsuse baastasemele, märkimisväärsele tasemele või kõrgele tasemele;

(b) asjaomase riigi pädeva asutuse väljastatud kehtiv sertifikaat, mis tõendab, et pilvandmetöötlusteenust on hinnatud ja see vastab liikmesriigis praegu kehtiva riikliku küberturvalisuse kava nõuetele;

(c) riikliku kava puudumise korral tõendid, mis näitavad turul kättesaadavate küberturvalisuse standardite kõrgeima taseme järgimist.

6. Auditi kriteerium F: kolmanda riigi või kolmanda riigi juriidilise isiku käitatavad tehisintellektisüsteemid

Auditeeriv organisatsioon peaks hindama II lisas loetletud liidu tasandi usaldusväärsuse 2., 3. ja 4. taseme punktis f nimetatud auditi kriteeriumeid järgmise põhjal.

(1) Lepingutingimused, milles sätestatakse, et auditeeritava teenuse kasutamisel töödeldud või genereeritud andmeid, sealhulgas klientidelt saadud andmeid, logisid ja telemeetriat, ei kasutata ühegi kolmanda riigi või kolmanda riigi õigussubjekti käitatava tehisintellektimudeli või -süsteemi treenimiseks või peenhäälestamiseks ning neid ei edastata ühelgi juhul väljapoole liitu.

(2) Lepingutingimused, milles täpsustatakse, et andmeid töödeldakse üksnes auditeeritava teenuse osutamiseks, mitte teenuse täiustamiseks või mudeli või süsteemi täiustamiseks või muul teisesel eesmärgil.

(3) Andmevooskeemid, mis dokumenteerivad andmete liikumist otspunktide vahel ning hõlmavad andmete valmendamist, talletamist, töötlemist ja kustutamist. Skeemid peaksid näitama ka seda, kus tehisintellekti töövood või masinõppeoperatsioonid puutuvad kokku kliendiandmetega.

(4) Masinõppeoperatsioonide või kasutuselevõtu andmed, mis näitavad, et kompileerimise, testimise ja väljalaskmise kohad paiknevad ELis.

(5) Mudeli- või süsteemikaardid, millel on mudeli või süsteemi nimi, versioon, treenimis- ja valideerimisallikad, sealhulgas kinnitused selle kohta, et auditeeritava teenuse kasutamisel genereeritud andmed ei lahku liidust.

(6) Andmete päritoluga seotud põhimõtted ja rakendusdokumendid, mis näitavad, et teenuseosutaja kasutab vahendeid andmete päritolu ja ajaloo kindlakstegemiseks ning suudab (iga kirje kohta) tõendada, milleks andmeid on kasutatud.

(7) Loetelu alltöövõtjatest (märkida nende asukohariik), kellel on juurdepääs auditeeritava teenuse kasutamisel loodud andmetele.

7. Auditi kriteerium G: kolmanda riigi kontrolli või kolmanda riigi üksuse kontrolli puudumine

Auditeeriv organisatsioon peaks hindama II lisas loetletud liidu tasandi usaldusväärsuse 2., 3. ja 4. taseme punktis g nimetatud auditi kriteeriumeid järgmise põhjal.

(1) Auditeeriv organisatsioon peaks kindlaks tegema ja analüüsima järgmist:

(a) kõik otsesed ja kaudsed aktsionärid kuni tegelike omanikeni;

(b) äriühingu omandistruktuuri kajastav tabel;

(c) organ või organid, kellel on õigus teha strateegilisi otsuseid (aktsionäride üldkoosolek, nõukogu, juhatus jne);

(d) juhtorganite määramise/valimise/tagasikutsumise kord ja juhtorganite tegelik koosseis (näiteks selleks, et teha kindlaks, kas mõnel aktsionäril on õigus nimetada esindaja juhatusse või kas tal on juhatuses häälteenamus);

(e) strateegiliste otsuste vastuvõtmiseks vajalik kvoorum ja häälteenamus, et teha kindlaks, kas aktsionär saab teha strateegilise otsuse (kas seetõttu, et tal on sellise otsuse heakskiitmiseks vajalik häälteenamus, või seetõttu, et ta saab blokeerida sellise otsuse veto või muude eriõigustega, isegi kui ta ei saa sellist otsust ise peale suruda jne);

(f) võimalik mõju strateegilistele otsustele ärisidemete, finantssidemete või muude vahendite kaudu jne.

(2) Auditeeritav teenuseosutaja peaks nõudma kogu eespool nimetatud teavet oma alltöövõtjatelt ja tegema selle auditeerivale organisatsioonile kättesaadavaks.

7.1. Omandiõiguse ja kontrolli hindamine

(1) Auditeeritav teenuseosutaja peaks esitama auditeerivale organisatsioonile järgmised peakorteriga seotud tõendid:

(a) ülemaailmse peakorteri ja/või peakontori asukoht ja täielik aadress;

(b) juhtimisstruktuuride asukohad.

(2) Auditeeritav teenuseosutaja peaks esitama auditeerivale organisatsioonile omandistruktuuri ja eriõiguste kohta järgmised tõendid.

(a) Üksikasjalik loetelu omanikest

i) kes omavad otseselt või kaudselt, sealhulgas mis tahes sisu, kokkuleppe, suhte või vahendaja kaudu vähemalt 5 % kapitalist või vähemalt 5 % hääleõigusest. See hõlmab aktsionäride vahelisi hääletamiskokkuleppeid, mis kokku annaksid üle 5 % hääleõigusest või 5 % kapitalist;

ii) kellel on seoses oma omandiõigusega seoses üks või mitu järgmistest eriõigustest: a) aktsiate üleandmist puudutav vetoõigus; b) ostueesõigus; c) õigus osta teatavatel tingimustel täiendavaid aktsiaid või investeeringuid.

(b) Auditeeriv organisatsioon peaks lõike 2 punktis a nimetatud elementide hindamiseks nõudma järgmisi tõendavaid dokumente:

i) äriregistri väljavõtted, aktsiaraamat ning organisatsiooniga seotud muud asjakohased dokumendid, milles on selgelt märgitud aktsionärid ja nende hääleõigus või osaluse protsendimäär;

ii) aktsionäride leping, aktsionäride vastastikuse mõistmise memorandum, põhikiri, asutamisleping või muud asjakohased dokumendid, mis käsitlevad otsuste tegemise korda juriidilises isikus, aktsionäride vahelised investeerimislepingud jne;

iii) juriidilistest isikutest aktsionäride puhul, kellele kuulub vähemalt 5 % kapitalist või vähemalt 5 % hääleõigusest:

(1) skeem, mis kirjeldab erinevaid omandikihte / kontrolliahelat kuni tegelike omanikeni;

(2) põhikiri, asutamisleping või samaväärsed asutamisdokumendid;

(3) juhatuse liikmete, ametiisikute ja allkirjaõiguslike isikute register.

(3) Auditeeritav teenuseosutaja peaks esitama auditeerivale organisatsioonile äriühingu üldjuhtimise kohta järgmised tõendid.

(a) Auditeeritav teenuseosutaja peaks esitama auditeerivale organisatsioonile kirjelduse järgmise kohta:

i) otsustusorganid, nende koosseis ja kodakondsus või tegevuskoht (kui on asjakohane);

ii) otsustusorganite liikmete või muude juhtivate ametiisikute valimist, ametisse nimetamist, kandideerimist või ametiaega käsitlev kord;

iii) otsuste tegemise kord, sealhulgas teave otsuste tegemiseks vajaliku häälteenamuse ja/või kvoorumi kohta;

iv) sisemise juhtimissüsteemi põhimõtted, milles kirjeldatakse omandi- ja kontrolliotsuste registreerimist ja heakskiitmist;

juhatuse ja juhtkonna otsused, mis kajastavad kindlaksmääratud kontrollistruktuuri;

juhatuse protokollid ja otsused kontrollimuudatuste kohta.

(b) Auditeeritav teenuseosutaja peaks esitama auditeerivale organisatsioonile tõendavad dokumendid, milles kehtestatakse või kirjeldatakse järgmist: juriidilise isiku otsustusorganid ja nende valimise, ametisse nimetamise, kandideerimise või ametiaja kord, otsuste tegemise kord, hääleõigus, vetoõigus, ametisse nimetamise õigus, heakskiitmise õigus (näiteks põhikiri, äriühingu üldjuhtimise aruanded jne). Tõendavad dokumendid ja teave tuleks esitada iga vahendava juriidilise isiku kohta, kellele kuulub otseselt või kaudselt 5 % või rohkem kapitalist või hääleõigustest, kuni kõigi asjaomaste kihtide tegelike omanikeni.

(4) Auditeeritav teenuseosutaja peaks esitama auditeerivale organisatsioonile järgmised kontrolliga seotud tõendid.

(a) Auditeeritav teenuseosutaja peaks esitama auditeerivale organisatsioonile tõendid kontrolliõigust andvate ärisidemete kohta. See hõlmab muu hulgas loetelu füüsilistest või juriidilistest isikutest, kellega auditeeritaval teenuseosutajal (või auditeeritava teenuseosutaja omanikel, sealhulgas vahekihtidel kuni tegelike omanikeni) on ärisuhe, mis a) toob kaasa aktsiate või vara omamisele sarnaneva kontrolli juhtimise ja ressursside üle ja b) on väga pikaajaline (näiteks väga olulised pikaajalised tarnelepingud või tarkvaratootjate/klientide pakutavad krediidid koos struktuurse seosega).

(b) Tõendavad dokumendid peaksid sisaldama koostöölepinguid avaliku sektori asutustega, tarkvaratootjatega jne.

(5) Auditeeritav teenuseosutaja peaks esitama auditeerivale organisatsioonile kontrolliõigust andvate finantssidemetega seotud järgmised tõendid.

(a) Auditeeritav teenuseosutaja peaks loetlema füüsilised või juriidilised isikud (sealhulgas kontrollivad aktsionärid või omanikud), kellest auditeeritav

teenuseosutaja (või omanikud) on rahalises sõltuvuses viisil, mis võimaldaks neil saada soodustusi strateegilistes ärivaldkondades.

(b) Tõendavad dokumendid peaksid hõlmama laenudokumente, põhikirju, finantsseost näitavaid dokumente jne.

(6) Auditeeritav teenuseosutaja peaks esitama auditeerivale organisatsioonile kontrolliõiguse muude allikate kohta järgmised tõendid.

(a) Auditeeritav teenuseosutaja peaks auditeerivale organisatsioonile teatama, kas on muid vahendeid, protsesse või seoseid, mis annavad tegeliku kontrolli kolmandale riigile või kolmandas riigis asutatud juriidilisele isikule (juhtimise ja vara kontrolliõigus, mis sarnaneb aktsiate või vara omamisele ja on pikaajaline).

(b) Tõendavates dokumentides tuleks esitada tõendid sellise kontrolli olemasolu kohta või kinnitus sellise kontrolli puudumise kohta (selle kinnituse võib anda teenuseosutaja juhatus).

NB! *Kontrolliõiguse hindamisel tuleks arvesse võtta omandistruktuure ja eriõigusi, äriühingu üldjuhtimist, kontrolliõigust andvaid ärisidemeid, kontrolliõigust andvaid finantssidemeid ja kontrolliõiguse muid allikaid.*

7.2. Omandi- ja kontrolliõiguse kontrollimise järeldustel põhinevad lisaetapid

Kui auditeeriv organisatsioon teeb kindlaks, et auditeeritav pakkuja on kolmanda riigi või kolmanda riigi juriidilise isiku kontrolli all, peaks ta nõudma järgmisi täiendavaid tõendeid:

(c) tõendid, et komisjon on võtnud artikli 19 kohaselt vastu otsuse kolmanda riigi kohta, kellel on kontroll pilvandmetöötlusteenuse osutaja üle;

(d) kõik tõendid, mis näitavad, et auditeeritav teenuseosutaja ja kõik auditeeritava teenuse osutamises osalevad alltöövõtjad on rakendanud vajalikud meetmed, et tagada pilvandmetöötlusteenuse osutaja ja mis tahes kolmanda riigi või kolmandas riigis asutatud juriidilise isiku tõhus õiguslik, tehniline ja organisatsiooniline eraldamine ning tagada, et pilvandmetöötlusteenuse osutajal ei ole õiguslikult, tehniliselt ega tegevuslikult võimalik täita mis tahes nõudmist juurdepääsuks kliendiandmetele, sealhulgas krüpteeritud andmetele, või teenuse järjepidevuse häirimiseks või teenuse kvaliteedi halvendamiseks;

(e) kõik tõendid, mis näitavad, et avaliku sektori asutust teavitatakse sellisest nõudmisest, ja kinnitavad, et nõudmine on tagasi lükatud;

(f) kõik tõendid, mis näitavad, et kolmandast riigist või kolmandas riigis asutatud juriidiliselt isikult tulnud kõik nõudmised kliendiandmetele juurdepääsuks, teenuse järjepidevuse häirimiseks või teenuse kvaliteedi halvendamiseks kantakse ajakohastatud registrisse, mis sisaldab vähemalt nõudmist ja vastust nõudmisele.

8. Auditi kriteerium H: tehnilise toe ja kasutustoe osutamine ei toimu liidust väljaspool

Auditeeriv organisatsioon peaks hindama II lisas loetletud liidu tasandi usaldusväärsuse 2., 3. ja 4. taseme punktis h nimetatud auditi kriteeriumeid järgmise põhjal.

(1) Tõendid selle kohta, et auditeeritav teenuseosutaja on rakendanud siduvaid lepingutingimusi, milles on sätestatud, et kogu tugi-, haldus-, hooldus-, järelevalve-, intsidentidele reageerimise ja operatiivtegevus tuleb algatada ja peab toimuma üksnes liidus. See võiks hõlmata lepingutingimusi, millega nõutakse kõigi alltöövõtjate ja

tugiteenuse osutamise asukohtade eelnevat avalikustamist ja eelnevat kirjalikku nõusolekut uute alltöövõtjate kaasamiseks, ning antakse õigus lükata tagasi kõik väljaspool liitu paiknevad alltöövõtjad.

(2) Tõendid selle kohta, et auditeeritav teenuseosutaja peab ajakohastatud alltöövõtjate registrit.

(3) Tõendid selle kohta, et auditeeritav teenuseosutaja ei sõlmi allhankelepinguid liidust väljaspool olijatega ega anna selliseid tegevusi üle väljapoole liitu.

(4) Tõendid selle kohta, et auditeeritav teenuseosutaja on rakendanud vajalikud õiguslikud, tehnilised ja korralduslikud meetmed tagamaks, et väljastpoolt liitu osutatav tehniline tugi ja operatiivtugi ei saa kaugjuurdepääsu auditeeritavale teenusele.

(5) Tõendid selle kohta, et auditeeritava teenuseosutaja kasutajatoe ja tugiteenuste osutamine, taristu haldamine, infoturbekeskuste või võrgukeskuste toimingud, eelispääs, varundamine ja avariitaastetoimingud, sealhulgas teenuse osutamiseks vajalike juurdepääsuteede andmine, toimub üksnes liidu seest.

(6) Tõendid selle kohta, et auditeeritav teenuseosutaja tagab, et ettevõttest lahkunud töötajatel ei ole enam juurdepääsu auditeeritavale teenusele, ja tühistab kõik nende pääsuõigused.

(7) Tõendid selle kohta, et auditeeritav teenuseosutaja on rakendanud vajalikud tehnilised ja korralduslikud meetmed tagamaks, et haldusjuurdepääs auditeeritava teenuse osutamiseks kasutatavatele süsteemidele antakse liidus paiknevate juurdepääsuteede kaudu. Seda saab tõendada geograafiliste võrgupiirangutega, liidus paikneva haldustaristu kasutamisega, eelispääsu haldamise kontrollimisega ja järelevalvemehhanismide rakendamisega.

(8) Tõendid selle kohta, et auditeeritav teenuseosutaja on kehtestanud korra, mis välistab (sealhulgas ka siis, kui sisseostetud teenuse osutaja tellib seda omakorda väljastpoolt), et tegelik kontroll on kolmanda riigi või kolmandas riigis asutatud juriidilise isiku käes.

9. Auditi kriteerium I: tarkvara tarneahela läbipaistvuse tagamine

Auditeeriv organisatsioon peaks hindama II lisas loetletud liidu tasandi usaldusväärsuse 2., 3. ja 4. taseme punktis i nimetatud auditi kriteeriumeid järgmise põhjal.

(1) Auditeeritav teenuseosutaja peaks tegema auditeerivale organisatsioonile kättesaadavaks täieliku ja ajakohase tarkvara koostenimekirja kõigi tarkvarakomponentide, sealhulgas avatud lähtekoodiga tarkvara kohta.

(2) Auditeeritav teenuseosutaja peaks tegema auditeerivale organisatsioonile kättesaadavaks sõltuvuste loetelu. See peaks sisaldama järgmist:

(a) kõik kasutatavad tarkvaramoodulid, teegid või rakendusliidesed ning arendusvahendid;

(b) tarkvara päritolu: kus (päritoluriik) ja kes tarkvara projekteerib, arendab ja hooldab, kus tarkvara levitatakse ja uuendatakse ja milline õigusruum seda reguleerib;

(c) sõltuvuse määr ELi-välistest müüjatest, vahenditest või patenditud tehnoloogiatest; 3. taseme puhul tõendid selle kohta, et kui tarkvaravirna pakub kolmanda riigi üksus, ei ole kehtestatud põhjendamatuid litsentsimispiiranguid;

(d) avatud lähtekoodiga tarkvarale tuginemise määr;

(e) nähtavus kogu tarkvaratootjate ja alltootjate ahelas, sealhulgas auditeerimisõigused.

NB! *Ülalesitatud nõuded tähendavad, et sellele tasemele saavad kvalifitseeruda näiteks ühisettevõtjad, mille on asutanud liidu üksus koos kolmandas riigis asutatud juriidilise isikuga.*

(3) Auditeeritav teenuseosutaja peaks esitama:

(a) tõendid riskipõhise protsessi kohta, millega tehakse kindlaks ja vähendatakse sõltuvust pilvandmetöötlusteenuse toimimisega seotud välistest tarkvaratootjatest;

(b) tõendid selle kohta, et on tuvastatud alternatiivne tarkvaralahendus (alternatiivsed tarkvaralahendused), sealhulgas avatud lähtekoodiga tarkvara. Kui samaväärset tarkvara ei ole võimalik tuvastada, tuleb leida lahendus, mis tagab minimaalse elujõulise funktsionaalsuse. Tuleb teha teste ja koostada üleviimiskava, mis võimaldab üleminekut sellistele alternatiivsetele lahendustele;

(c) tõendid selle kohta, et müüja vea või maksejõuetuse või kolmanda riigi või kolmandas riigis asutatud juriidilise isiku piirangute korral on võimalik üle minna alternatiivsele lahendusele;

(d) loetelu avatud standarditest, mida auditeeritav teenuseosutaja järgib auditeeritava teenusega seotud poliitika osana.

(4) Auditeeritav teenuseosutaja peaks tagama läbipaistvuse kaugpääsu ja lähtekoodi auditeeritavuse kaudu järgmiselt:

(a) tehes auditeerivale organisatsioonile kättesaadavaks loetelu tõenditest, mis tõendavad, et ei kasutata kaugfunktsioone või -mehhanisme, mida saaks kasutada seadme, süsteemi või tarkvara oluliseks rikkumiseks või häirimiseks. See peaks sisaldama järgmist:

i) tarkvarakomponendi testimisega seotud tõendid (testimismenetlus, testimisaruanded, testimisplaan jne), et on välistatud kaugfunktsioonid või -mehhanismid, mida saaks kasutada seadme, süsteemi või tarkvara oluliseks rikkumiseks või häirimiseks;

ii) tõendid selle kohta, et organisatsiooni muudatuste juhtimise kord hõlmab püsivara, BIOSi ja tarkvara uuendamise mis tahes muudatusi ning uute komponentide integreerimist, et välistada ükskõik milliste kaugfunktsioonide või -mehhanismide kasutamine;

iii) tõendid selle kohta, et hooldusmenetlus on ajakohastatud nii, et on välistatud kaugfunktsioonid või -mehhanismid, mida saaks kasutada seadme, süsteemi või tarkvara oluliseks rikkumiseks või häirimiseks.

(b) Auditeeritav teenuseosutaja peab tagama, et kolmandast isikust sõltumatule audiitorile antakse õigus sellise tarkvara lähtekoodile juurde pääseda ja seda auditeerida. Auditeeritav teenuseosutaja peab samuti tagama, et kogu lähtekoodi hindamiseks ja auditeerimiseks vajalik dokumentatsioon, tehniline materjal ja teave tehakse auditeerivale organisatsioonile kättesaadavaks täielikus, täpses ja kättesaadavas vormis.

10. Auditi kriteerium J: avatud lähtekoodiga tarkvara

Auditeeriv organisatsioon peaks hindama II lisas loetletud liidu tasandi usaldusväärsuse 2., 3. ja 4. taseme punktis j nimetatud auditi kriteeriumeid järgmise põhjal.

(1) Auditeeritav teenuseosutaja peaks tagama läbipaistvuse kaugpääsu ja lähtekoodi auditeeritavuse kaudu järgmiselt:

(a) tehes auditeerivale organisatsioonile kättesaadavaks loetelu tõenditest, mis tõendavad, et ei kasutata kaugfunktsioone või -mehhanisme, mida saaks kasutada seadme, süsteemi või tarkvara oluliseks rikkumiseks või häirimiseks. See peaks sisaldama järgmist:

i) tarkvarakomponendi testimisega seotud tõendid (testimismenetlus, testimisaruanded, testimisplaan jne), et on välistatud kaugfunktsioonid või -mehhanismid, mida saaks kasutada seadme, süsteemi või tarkvara oluliseks rikkumiseks või häirimiseks;

ii) tõendid selle kohta, et organisatsiooni muudatuste juhtimise menetlused hõlmavad püsivara, BIOSi ja tarkvara uuendamise mis tahes muudatusi ning uute komponentide integreerimist, et välistada ükskõik milliste kaugfunktsioonide või -mehhanismide kasutamine;

iii) tõendid selle kohta, et hooldusmenetlus on ajakohastatud nii, et on välistatud kaugfunktsioonid või -mehhanismid, mida saaks kasutada seadme, süsteemi või tarkvara oluliseks rikkumiseks või häirimiseks.

(2) Auditeeritav teenuseosutaja peaks esitama:

(a) tõendid riskipõhise protsessi kohta, millega tuvastatakse ja vähendatakse järgmisi riske: i) avatud lähtekoodiga tarkvara nõrk ökosüsteem ja kogukonna toetus; ii) avaldatud uuendusi ei jälgita pidevalt; iii) juhtumid, kus avatud lähtekoodiga tarkvara on aegunuks tunnistatud või seda enam ei hooldata;

(b) tõendid selle kohta, et auditeeritav teenuseosutaja on põhjendamatu viivituseta kasutusele võtnud ajakohase avatud lähtekoodiga tarkvara;

(c) tõendid selle kohta, et auditeeritav teenuseosutaja on kindlaks teinud ühe või mitu alternatiivset avatud lähtekoodiga lahendust. Kui auditeeritav teenuseosutaja ei suuda leida samaväärset tarkvara, tuleb leida lahendus, mis tagab minimaalse elujõulise funktsionaalsuse. Auditeeritav teenuseosutaja peab rakendama teste ja üleviimiskava, mis võimaldavad üleminekut alternatiivsetele lahendustele.

(3) Kui auditeeritav teenuseosutaja kasutab avatud lähtekoodi litsentsi alusel välja antud tarkvara, peaks auditeeritav teenuseosutaja rakendama mehhanisme, et tuvastada tarkvara omandiõiguse või kontrolli üleminek kolmandale riigile või kolmandas riigis asutatud juriidilisele isikule või sihtasutusele, ja teavitada sellest õigeaegselt avaliku sektori asutust.

11. Auditi kriteerium K: üleilmsed teenused ja tütarettevõtjad kolmandas riigis

Auditeeriv organisatsioon peaks hindama II lisas loetletud liidu tasandi usaldusväärsuse 2., 3. ja 4. taseme punktis k nimetatud auditi kriteeriumeid järgmise põhjal.

(1) Auditeeriv organisatsioon peaks kontrollima, et tütarettevõtja on auditeeritavast teenuseosutajast õiguslikult ja tegevuslikult sõltumatu.

(2) Auditeeritav teenuseosutaja peaks tõendama, et tütarettevõtjal puudub juurdepääs kliendiandmeid töötlevatele või talletavatele süsteemidele.

(3) Auditeeritav teenuseosutaja peaks tõendama, et tütarettevõtjal ei ole liidu tootmiskeskkondades eeliskontosid, sealhulgas pilvehalduse, identiteedi- ja pääsuhalduse, eelispääsu halduse ning järelevalve- või andmebaasihalduse privileege.

(4) Auditeeriv organisatsioon peaks kontrollima, et tütarettevõtja töötajatel ei ole juurdepääsu liidu kliendiandmetele.

(5) Auditeeriv organisatsioon peaks kontrollima, et tütarettevõtjal ei ole õigust anda liidu tegevpersonalile juhiseid kliendiandmete avalikustamiseks või turvamenetlustest möödahiilimiseks.

(6) Auditeeriv organisatsioon peaks kontrollima, et kõik välisriigi valitsuse taotlused, mille tütarettevõtja on saanud, suunatakse ametlikult edasi pädevale liidu üksusele liidu ja liikmesriigi õiguse kohaseks õiguslikuks hindamiseks.