



# Procurement of AI Community

## ● PUBLIC BUYERS COMMUNITY

**Proposal Ettepanek avaliku sektori  
organisatsioonide tehisintellekti hankimise lepingu  
tüüptingimuste kohta, 2023. aasta septembri  
versioon**

**DRAFT High Risk version**

#### **Lahtiütlus**

**Tegemist on dokumendi kavandiga, mis on mõeldud üksnes arutamiseks ja mille eesmärk on koguda sidusrühmadelt esialgset tagasisidet. Selle dokumendi on koostanud Jeroen Naves (Pels Rijcken). See ei ole ELi ametlik dokument ega kajasta Euroopa Komisjoni ametlikku seisukohta. Euroopa Komisjon ega ükski komisjoni nimel tegutsev isik ei vastuta käesoleva dokumendi võimaliku kasutamise eest. Käesolev dokument ei ole lõplik. Sellest dokumendist ei tulene mingeid õigusi.**

## Sissejuhatavad märkused

Need lepingu tüüptingimused on koostatud avaliku sektori organisatsioonide jaoks, kes soovivad hankida välistarnija välja töötatud tehisintellektisüsteemi. Nende tüüptingimuste aluseks on algoritmiliste süsteemide hankimise tüüptingimused, mille Amsterdami linn töötas välja 2018. aastal (<https://www.amsterdam.nl/innovatie/digitalisering-technologie/algoritmen-ai/contractual-terms-for-algorithms/>).

Siinses kavandis esitatud lepingu tüüptingimused põhinevad peamiselt suure riskiga tehisintellektisüsteemide suhtes kehtestatud nõuetel ja kohustustel, mis on sätestatud tehisintellektimääruse ettepaneku\* III jaotises. Selle ettepaneku üle peetakse veel läbirääkimisi, mistõttu tuleb tüüptingimused hiljem läbi vaadata, et kajastada kõiki tehtud muudatusi ning viia tüüptingimused täielikult kooskõlla nõukogu ja Euroopa Parlamendi poolt vastu võetud lõpliku määrusega.

Kuna kavandatava tehisintellektimääruse üle peetakse veel läbirääkimisi, võivad avaliku sektori organisatsioonid soovi korral neid tüüptingimusi vabatahtlikult kasutada, hinnates igal üksikjuhul eraldi, kas need lepingu tüüptingimused on konkreetse tehisintellektisüsteemi hankimiseks piisavad ja proportsionaalsed. Lepingu tüüptingimused on suunatud eelkõige tehisintellektisüsteemidele, mida käsitatakse suure riskiga tehisintellektisüsteemidena artikli 6 tähenduses ja mida kasutatakse mõnes kavandatava tehisintellektimääruse II või III lisas loetletud valdkonnas. Muu kui suure riskiga tehisintellekti korral ei ole nende nõuete kohaldamine tehisintellektimääruse kohaselt kohustuslik, kuid see on soovitatav, et suurendada avaliku sektori organisatsioonide hangitud tehisintellektirakenduste usaldusvärsust. Kui see on asjakohane ja põhjendatud, pidades silmas süsteemi mõju üksikisikutele ja ühiskonnale, võivad avaliku sektori organisatsioonid laiendada siinsete tüüptingimuste kohaldamisala ka muudele algoritmilistele süsteemidele, mis ei pruugi tingimata kvalifitseeruda tehisintellektiks, et hõlmata lihtsamaid reeglipõhiseid tarkvarasüsteeme, võttes arvesse, et nende kasutamine avalikus sektoris võib teataval juhul samuti nõuda suuremat vastutust, kontrolli ja läbipaistvust.

Selleks et rahuldada nende avaliku sektori organisatsioonide vajadusi, kes soovivad kasutada neid lepingu tüüptingimusi muude kui suure riskiga tehisintellektisüsteemide puhul, tehakse kättesaadavaks ka nende tüüptingimuste lühem versioon.

Lepingu tüüptingimused sisaldavad üksnes konkreetseid sätteid tehisintellektisüsteemide ja kavandatavas tehisintellektimääruses käsitletavate küsimuste kohta ega hõlma seega muid kohustusi ega nõudeid, mis võivad tuleneda asjakohastest kohaldatavatest õigusaktidest, näiteks isikuandmete kaitse üldmäärusest. Lisaks ei kujuta need lepingu tüüptingimused endast täielikku lepingupõhist kokkulepet. Näiteks ei sisalda need tingimusi, mis käsitlevad intellektuaalomandit, vastuvõtmist, maksmist, tarnetähtaegu, kohaldatavat õigust ja vastutust. Lepingu tüüptingimused on koostatud nii, et need saab lisada lepingule, milles asjaomaseid küsimusi käsitletakse.

\* Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ja muudetakse teatavaid liidu õigusakte (COM(2021)206 final).

## A jagu. Mõisted

### Article 1 Mõisted

1.1. Käesolevates tingimustes kasutatakse allpool määratletud mõisteid:

- leping – kogu leping, mille lahutamatuks osaks on käesolevad tingimused;
- tehisintellektisüsteem – **A lisas** osutatud tehisintellektisüsteem(id), sealhulgas selle (nende) võimalik(ud) uus (uued) versioon(id);
- tingimused – käesolevad avaliku sektori organisatsioonide tehisintellekti hankimise lepingu tüüptingimused;
- avaliku sektori organisatsiooni andmestikud – andmestikud (või nende osad), i) mille avalik organisatsioon edastab tarnijale lepingu alusel või ii) mis luuakse või kogutakse lepingu raames, sealhulgas punktides i) ja ii) osutatud andmestike muudetud või laiendatud (näiteks kommenteerimise, märgendamise, puhastamise, rikastamise ja koondamise teel) versioonid;
- andmestikud – kõik tehisintellektisüsteemi väljatöötamisel kasutatavad andmestikud, sealhulgas **B lisas** kirjeldatud andmestik(ud);
- tarnimine – etapp, mil tarnija teatab avaliku sektori organisatsioonile, et tehisintellektisüsteem vastab kõigile kokkulepitud tingimustele ja on kasutusvalmis;
- sihtotstarve – kasutus, kaasa arvatud B lisas täpsustatud kasutamise konkreetne kontekst ja tingimused, mille jaoks avaliku sektori organisatsioon on tehisintellektisüsteemi kasutusjuhendis, reklaam- või müügitmaterjalides ja avaldustes esitatud teabe ning tehnilises dokumentatsioonis esitatud teabe kohaselt ette näinud;
- mõistlikult prognoositav väärkasutamine – tehisintellektisüsteemi kasutamine viisil, mis ei ole kooskõlas selle sihtotstarbega, kuid mis võib tuleneda põhjendatult prognoositavast inimkäitumisest või koostoimest muude süsteemidega;
- oluline muudatus – tehisintellektisüsteemis pärast selle tarnimist tehtud muudatus, mis mõjutab tehisintellektisüsteemi vastavust käesolevates tingimustes sätestatud nõuetele või mille tulemusena muutub süsteemi sihtotstarve;
- tarnija – füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes tarnib lepingu alusel tehisintellektisüsteemi avaliku sektori organisatsioonile;
- tarnija andmestikud ja kolmandate isikute andmestikud – andmestikud (või nende osad), mis ei kvalifitseeru avaliku sektori organisatsiooni andmestikeks.

## ***B jagu. Tehisintellektisüsteemiga seotud olulised nõuded***

### Article 2 Riskijuhtimissüsteem

- 2.1. Tarnija tagab, et enne tehisintellektisüsteemi tarnimist luuakse ja võetakse kasutusele tehisintellektisüsteemiga seotud riskijuhtimissüsteem.
- 2.2. Riskijuhtimissüsteem peab hõlmama vähemalt järgmisi etappe:
  - a. nende teadaolevate ja mõistlikult prognoositavate tervist, ohutust ja Euroopa Liidu põhiõigusi mõjutavate riskide kindlakstegemine, prognoosimine ja hindamine, mis tõenäoliselt tekivad, arvestades tehisintellektisüsteemi sihtotstarvet ja mõistlikult prognoositavat väärkasutamist;
  - b. muude tekkida võivate riskide hindamine;
  - c. asjakohaste ja sihipäraste riskijuhtimismeetmete vastuvõtmine käesoleva lõike punktide a ja b kohaselt kindlaks tehtud riskide maandamiseks kooskõlas järgmiste lõigetega.
- 2.3. Lõike 2.2 punktis c osutatud riskijuhtimismeetmed peavad olema sellised, et tarnija käsitleb iga ohuga seotud asjakohaseid jääkriske ja tehisintellektisüsteemi üldist jääkriski põhjendatult vastuvõetavana, tingimusel et tehisintellektisüsteemi kasutatakse vastavalt selle sihtotstarbele või mõistlikult prognoositava väärkasutamise tingimustes.
- 2.4. Lõike 2.2 punktis c osutatud kõige asjakohasemate riskijuhtimismeetmete kindlaksmääramisel tagatakse järgmine:
  - a. tuvastatud riskide kõrvaldamine või vähendamine niivõrd, kuivõrd see on tehniliselt teostatav tehisintellektisüsteemi sobiva projekteerimise ja väljatöötamise kaudu;
  - b. asjakohasel juhul sobivate riskimaandamis- ja kontrollimeetmete rakendamine selliste riskide puhul, mida ei saa kõrvaldada;
  - c. avaliku sektori organisatsioonile piisava teabe andmine.
- 2.5. Tarnija tagab, et enne tehisintellektisüsteemi tarnimist testitakse tehisintellektisüsteemi, et kontrollida, kas see vastab käesolevatele tingimustele ja kas lõike 2.2 punktis c osutatud riskijuhtimismeetmed on kavandatud sihtotstarvet ja mõistlikult prognoositavat väärkasutamist silmas pidades tõhusad. Kui avaliku sektori organisatsioon seda nõuab, on tarnija kohustatud testima tehisintellektisüsteemi avaliku sektori organisatsiooni keskkonnas.
- 2.6. Tarnija peab dokumenteerima kõik käesoleva artikli järgimisega seoses tuvastatud riskid, võetud meetmed ja tehtud testid. Tarnija peab tegema vastavad dokumendid avaliku sektori organisatsioonile kättesaadavaks vähemalt tehisintellektisüsteemi tarnimise ajal. Need dokumendid võivad olla osa tehnilisest dokumentatsioonist ja/või kasutusjuhendist.
- 2.7. Riskijuhtimissüsteem peab seisnema lepingu kogu kehtivusaja jooksul pidevalt korduvas protsessis. Seetõttu peab tarnija pärast tehisintellektisüsteemi tarnimist tegema järgmist:
  - a. riskijuhtimisprotsessi regulaarselt läbi vaatama ja ajakohastama, et tagada selle jätkuv tõhusus;
  - b. ajakohastama lõikes 2.6 osutatud dokumentatsiooni ja
  - c. tegema kõik lõikes 2.6 osutatud dokumentide uued versioonid avaliku sektori organisatsioonile viivitamata kättesaadavaks.

- 2.8. Kui tarnija seda riskijuhtimise süsteemi nõuetekohaseks rakendamiseks põhjendatult vajab, annab avaliku sektori organisatsioon tarnijale viimase nõudmisel teavet, mis ei ole konfidentsiaalne.
- 2.9. **<Vabatahtlik>** Kui avaliku sektori organisatsioon jätkab tehisintellektisüsteemi kasutamist ka pärast lepingu kehtivusaja lõppu, esitab tarnija avaliku sektori organisatsioonile lepingu kehtivusaja lõpus teabe, mis on vajalik riskijuhtimissüsteemi toimivana hoidmiseks.

**Article 3 <Artikkel 3 on asjakohane üksnes tehisintellektisüsteemide puhul, milles kasutatakse meetodeid, mis hõlmavad mudelite treenimist andmetega. Artikkel 3 eeldab, et tarnijal (või tema alltöövõtjatel) on täielik juurdepääs andmestikele. Kui andmestikud on üksnes avaliku sektori organisatsiooni valduses, tuleb sõlmida teistsugused kokkulepped.>** Andmed ja andmehaldus

- 3.1. Tarnija tagab, et tehisintellektisüsteemi väljatöötamisel, sealhulgas treenimisel, valideerimisel ja testimisel kasutatavate andmestike suhtes on kohaldatud ja kohaldatakse andmehaldust, mis on nii tehisintellektisüsteemi kasutamise kui ka sihtotstarbe kontekstis asjakohane. Asjaomased meetmed puudutavad eeskätt järgmist:
- andmete kogumise algse eesmärgi läbipaistvus;
  - asjakohased projekteerimise käigus tehtavad valikud;
  - andmete kogumise protsessid;
  - andmete ettevalmistamiseks tehtavad töötlemistoimingud, näiteks kommenteerimine, märgendamine, puhastamine, rikastamine ja koondamine;
  - asjakohaste eelduste sõnastamine, eeskätt seoses teabega, mida andmed peaksid mõõtma ja kajastama;
  - läbivaatamine, pidades silmas võimalikku kallutatust, mis võib mõjutada füüsiliste isikute tervist ja ohutust või põhjustada Euroopa Liidu õigusaktidega keelatud diskrimineerimist;
  - asjakohased meetmed võimaliku kallutatuse avastamiseks, ennetamiseks ja vähendamiseks;
  - käesolevate tingimuste täitmist takistavate asjakohaste andmelünkade või puuduste ning nende lünkade ja puuduste kõrvaldamise võimaluste kindlakstegemine.
- 3.2. Tarnija tagab, et tehisintellektisüsteemi väljatöötamisel kasutatavad andmestikud on süsteemi sihtotstarvet silmas pidades asjakohased, representatiivsed, võimalikult suures ulatuses vigadeta ja võimalikult täielikud. Tarnija tagab, et andmestikel on asjakohased statistilised omadused, sealhulgas vajaduse korral seoses isikutega või isikute rühmadega, kelle puhul tehisintellektisüsteemi kavatsetakse kasutada. Need andmestike omadused peavad olema tagatud üksikute andmestike või nende kombinatsiooni tasandil.
- 3.3. Tarnija tagab, et tehisintellektisüsteemi väljatöötamisel kasutatavate andmestike puhul võetakse süsteemi sihtotstarbest või mõistlikult prognoositavast väärkasutamisest tulenevas vajalikus ulatuses arvesse omadusi või elemente, mis iseloomustavad konkreetset geograafilist, käitumuslikku või funktsionaalset konteksti, milles tehisintellektisüsteemi kavatsetakse kasutada.

- 3.4. Käesolevast artiklist tulenevaid kohustusi ei kohaldata mitte ainult tehisintellektisüsteemi väljatöötamise suhtes enne selle tarnimist, vaid ka tarnijapoolse andmestike kasutamise suhtes, mis võib mõjutada tehisintellektisüsteemi toimimist mis tahes muul ajal lepingu kehtivusaja jooksul.

#### Article 4 Tehniline dokumentatsioon ja kasutusjuhend

- 4.1. Tehisintellektisüsteemi tarnimine hõlmab tehnilise dokumentatsiooni ja kasutusjuhendi üleandmist tarnija poolt.
- 4.2. Tehniline dokumentatsioon peab võimaldama avaliku sektori organisatsioonil või kolmandal isikul hinnata tehisintellektisüsteemi vastavust käesolevates tingimustes sätestatud nõuetele ja olema kooskõlas vähemalt **C lisas** kirjeldatud tingimustega.
- 4.3. Kasutusjuhend peab sisaldama kokkuvõtlikku, täielikku, täpset ja selget teavet, mis on avaliku sektori organisatsioonile oluline, juurdepääsetav ja mõistetav. Kasutusjuhend peab vastama vähemalt **D lisas** kirjeldatud tingimustele.
- 4.4. Tarnija peab neid dokumente ajakohastama vähemalt iga olulise muudatuse tegemisel lepingu kehtivusaja jooksul ja seejärel tegema need avaliku sektori organisatsioonile kättesaadavaks.
- 4.5. **<Vabatahtlik>** Tehniline dokumentatsioon ja kasutusjuhend tuleb koostada inglise keeles.
- 4.6. **<Vabatahtlik>** Avaliku sektori organisatsioonil on õigus teha tehnilisest dokumentatsioonist ja kasutusjuhendist koopiaid organisatsioonisiseseks kasutamiseks vajalikus ulatuses, ilma et see piiraks artiklite 6 ja 13 kohaldamist.

#### Article 5 Andmete säilitamine

- 5.1. Tarnija tagab, et tehisintellektisüsteem on projekteeritud ja välja töötatud või projekteeritakse ja töötatakse välja nii, et süsteemi toimimise käigus on võimalik sündmusi automaatselt registreerida (nn logid). Need logimisfunktsioonid peavad vastama tehnilistele nõuetele ja olemasolu korral tunnustatud standarditele või ühtsetele kirjeldustele. **<Vabatahtlik: olemasolu korral lisage konkreetne standard>**
- 5.2. Logimisfunktsioonid peavad tagama tehisintellektisüsteemi toimimise jälgitavuse süsteemi kogu kasutusaja jooksul süsteemi sihtotstarbe ja mõistlikult prognoositava väärkasutamise seisukohast otstarbekal tasemel. Eeskätt peavad logimisfunktsioonid võimaldama registreerida sündmusi, mis on olulised selliste olukordade tuvastamiseks,
- mille tulemusena võib tehisintellektisüsteem ohustada tervist või ohutust või isikute põhiõiguste kaitset või
  - mis võivad põhjustada olulise muudatuse.
- 5.3. **<Vabatahtlik>** Tarnija võimaldab avaliku sektori organisatsioonile reaalajas juurdepääsu tehisintellektisüsteemi poolt automaatselt loodud logidele.
- 5.4. Tarnija säilitab tehisintellektisüsteemi poolt automaatselt loodud logisid lepingu kehtivusaja jooksul, kui need logid on lepingu kohaselt tema kontrolli all. Lepingu kehtivusaja lõpul edastab tarnija need logid viivitamata avaliku sektori organisatsioonile.

#### Article 6 Tehisintellektisüsteemi läbipaistvus

- 6.1. Tarnija tagab, et tehisintellektisüsteem on projekteeritud ja välja töötatud või projekteeritakse ja töötatakse välja nii, et süsteemi toimimine on piisavalt läbipaistev, võimaldamaks avaliku sektori organisatsioonil süsteemi toimimisest mõistlikult aru saada.
- 6.2. Asjakohase läbipaistvuse tagamiseks rakendab tarnija enne tehisintellektisüsteemi tarnimist vähemalt **E lisas** kirjeldatud tehnilisi ja korralduslikke meetmeid. Nende meetmete tulemusel peaks avaliku sektori organisatsioonil olema võimalik tehisintellektisüsteemi õigesti mõista ja kasutada, saades aru, kuidas tehisintellektisüsteem töötab ja milliseid andmeid see töötleb, mis võimaldab avaliku sektori organisatsioonil selgitada tehisintellektisüsteemi tehtud otsuseid isikutele või isikute rühmale, kelle puhul tehisintellektisüsteemi kasutatakse (kavatsetakse kasutada).

#### Article 7 Inimjärelevalve

- 7.1. Tarnija tagab, et tehisintellektisüsteem on projekteeritud ja välja töötatud või projekteeritakse ja töötatakse välja nii (kasutades muu hulgas asjakohaseid inimene-masin kasutajaliideseid), et füüsilised isikud saaksid teha süsteemi üle tõhusat järelevalvet, mis on proportsionaalne süsteemiga seotud riskidega.
- 7.2. Tarnija tagab, et enne tarnimist lõimitakse tehisintellektisüsteemi ja rakendatakse asjakohased inimjärelevalve tagamiseks vajalikud meetmed. Need meetmed, mis võivad muu hulgas hõlmata avaliku sektori organisatsiooni töötajate koolitust, peavad võimaldama isikutel, kelle ülesandeks on teostada inimjärelevalvet, teha vastavalt asjaoludele järgmist:
  - a. teada ja piisavalt mõista tehisintellektisüsteemi asjakohaseid võimeid ja piiranguid ning olla võimeline nõuetekohaselt jälgima süsteemi toimimist, et võimalikult kiiresti avastada märke kõrvalekalletest, väärtalitlusest ja ootamatust toimimisest ning need kõrvaldada;
  - b. olla alati teadlik võimalikust kalduvusest automaatselt või liigselt tugineda tehisintellektisüsteemi toodetud väljundile (nn kalduvus eelistada automatiseerimist), eelkõige juhul, kui tehisintellektisüsteemi kasutatakse selleks, et saada teavet või soovitusi füüsiliste isikute tehtavate otsuste jaoks;
  - c. osata tehisintellektisüsteemi väljundit õigesti tõlgendada, võttes arvesse eeskätt süsteemi omadusi ning kättesaadavaid tõlgendamisevahendeid ja -meetodeid;
  - d. suuta igas konkreetsetes olukorras otsustada tehisintellektisüsteemi mitte kasutada või selle väljund muul moel kõrvale jätta, sürjutada või tagasi pöörata;
  - e. osata sekkuda tehisintellektisüsteemi töösse või katkestada süsteemi töö stoppnupu või muu sarnase protseduuriga.
- 7.3. **<Vabatahtlik>** Asjakohase inimjärelevalve tagamiseks rakendab tarnija enne tehisintellektisüsteemi tarnimist vähemalt **F lisas** kirjeldatud tehnilisi ja korralduslikke meetmeid.

#### Article 8 Täpsus, stabiilsus ja küberturvalisus

- 8.1. Tarnija tagab, et tehisintellektisüsteem on projekteeritud ja välja töötatud või projekteeritakse ja töötatakse välja sisseprojekteeritud turbe ja vaiketurbe põhimõtet



järgides. Süsteem peaks saavutama oma sihtotstarbe seisukohast asjakohasel tasemel täpsuse, stabiilsuse ja küberturvalisuse ning toimima nendes aspektides järjepidevalt kogu oma kasutusaja jooksul.

- 8.2. Tehisintellektisüsteemi täpsuse tasemeid ja asjakohaseid täpsuse parameetreid kirjeldatakse **G lisas**.
- 8.3. Asjakohasel tasemel stabiilsuse, ohutuse ja küberturvalisuse tagamiseks rakendab tarnija enne tehisintellektisüsteemi tarnimist vähemalt **H lisas** kirjeldatud tehnilisi ja korralduslikke meetmeid.

### ***C jagu. Tarnija kohustused seoses tehisintellektisüsteemiga***

#### Article 9 Vastavus B jaole

Tarnija peab tagama, et tehisintellektisüsteem vastab käesolevate tingimuste B jaos sätestatud nõuetele alates tehisintellektisüsteemi tarnimisest kuni lepingu kehtivusaja lõpuni.

#### Article 10 **<Vabatahtlik>** Kvaliteedijuhtimissüsteem

- 10.1. Enne tehisintellektisüsteemi tarnimist võtab tarnija kasutusele kvaliteedijuhtimissüsteemi, mis tagab käesolevate tingimuste järgimise. Kvaliteedijuhtimissüsteem peab olema kirjalike põhimõtete, menetluste ja juhendite kujul süsteemselt ja nõuetekohaselt dokumenteeritud ning sisaldama vähemalt järgmisi aspekte:
  - a. strateegia õigusnormidele vastavuse tagamiseks;
  - b. meetodid, protseduurid ja süstemaatilised meetmed, mida kasutatakse tehisintellektisüsteemi projekteerimiseks, projekteerimise üle tehtavaks järelevalveks ja projektide kontrollimiseks;
  - c. meetodid, protseduurid ja süstemaatilised meetmed, mida kasutatakse tehisintellektisüsteemi väljatöötamiseks, kvaliteedi kontrollimiseks ja kvaliteedi tagamiseks;
  - d. enne tehisintellektisüsteemi väljatöötamist, selle ajal ja pärast seda teostatavad läbivaatamis-, testimis- ja valideerimisprotseduurid ning nende teostamise sagedus;
  - e. kohaldatavad tehnilised kirjeldused, sh standardid, ja juhul, kui asjaomaseid harmoneeritud standardeid ei kohaldata täies mahus või need ei hõlma kõiki asjakohaseid nõudeid, siis ka vahendid, mida kasutatakse selleks, et tagada tehisintellektisüsteemi vastavus käesolevate tingimuste B jaos sätestatud nõuetele;
  - f. andmehalduse süsteemid ja protseduurid, sh andmete kogumine, andmeanalüüs, andmete märgendamine, andmete talletamine, andmete filtreerimine, andmekaeve, andmete agregeerimine, andmete säilitamine ja mis tahes muud andmetega seotud toimingud, mida tehakse enne tehisintellektisüsteemi tarnimist;
  - g. artiklis 2 osutatud riskijuhtimissüsteem;
  - h. protseduurid, mis on seotud tõsistest intsidentidest ja tõrgetest teatamisega;

- i. kõigi vajalike dokumentide ja teabega seotud andmete säilitamise süsteemid ja protseduurid;
- j. ressursside haldamine, sh varustuskindlusega seotud meetmed;
- k. aruandekohustuse raamistik, millega nähakse ette juhtkonna ja muude töötajate vastutus seoses kõigi käesolevas lõikes loetletud aspektidega.

Article 11      **<Vabatahtlik>** Vastavushindamine

- 11.1. Tarnija tagab, et enne tarnimist läbib tehisintellektisüsteem järgmise vastavushindamismenetluse.
- a. Tarnija kontrollib, kas kehtestatud kvaliteedijuhtimissüsteem vastab artikli 10 nõuetele.
  - b. Tarnija vaatab tehnilises dokumentatsioonis sisalduva teabe läbi, et hinnata tehisintellektisüsteemi vastavust käesolevate tingimuste B jaos sätestatud asjakohastele olulistele nõuetele.
  - c. Ühtlasi kontrollib tarnija, kas tehisintellektisüsteemi projekteerimis- ja väljatöötamisprotsess on kooskõlas tehnilise dokumentatsiooniga.
- 11.2. Tarnija tagab, et tehisintellektisüsteem läbib uue vastavushindamismenetluse iga kord, kui tarnija teeb süsteemis lepingu kehtivusaja jooksul olulise muudatuse.

Article 12      Parandusmeetmed

Kui lepingu kehtivusaja jooksul tarnija arvab või tal on põhjust arvata, et tehisintellektisüsteem ei vasta käesolevatele tingimustele, olenemata sellest, kas selleni viis avaliku organisatsiooni märkus või mitte, võtab ta viivitamata vajalikud parandusmeetmed, et viia süsteem käesolevate tingimustega vastavusse. Tarnija teatab sellest avaliku sektori organisatsioonile.

Article 13      Kohustus selgitada tehisintellektisüsteemi toimimist üksikisiku tasandil

- 13.1. Lisaks artiklis 6 kirjeldatud kohustustele on tarnija lepingu kehtivusaja jooksul kohustatud aitama avaliku sektori organisatsioonil tolle esimesel nõudmisel selgitada isikutele või isikute rühmale, kelle puhul tehisintellektisüsteemi kasutatakse (kavatsetakse kasutada), kuidas tehisintellektisüsteem konkreetse otsuse või tulemuseni jõudis. See abi sisaldab vähemalt selget viidet peamistele teguritele, mille tõttu tehisintellektisüsteem jõudis konkreetse tulemuseni, ja muudatuste kohta sisendis, mis tuleb teha, et jõuda teistsuguse tulemuseni.
- 13.2. Lõikes 13.1 kirjeldatud kohustus hõlmab kohustust esitada avaliku sektori organisatsioonile kogu tehniline ja muu teave, mida on vaja selleks, et selgitada, kuidas tehisintellektisüsteem konkreetse otsuse või tulemuseni jõudis, ning pakkuda isikutele või isikute rühmale, kelle puhul tehisintellektisüsteemi kasutatakse (kavatsetakse kasutada), võimalust kontrollida, kuidas tehisintellektisüsteem konkreetse otsuse või tulemuseni jõudis. Käesolevaga annab tarnija avaliku sektori organisatsioonile õiguse seda teavet kasutada, jagada ja avalikustada, kui see on vajalik selleks, et teavitada isikuid või isikute

rühma, kelle puhul tehisintellektisüsteemi kasutatakse (kavatsetakse kasutada) tehisintellektisüsteemi toimimisest, ja/või kui see on vajalik võimalikes kohtumenetlustes.

- 13.3. **<Vabatahtlik>** Lõigetes 13.1 ja 13.2 osutatud kohustused hõlmavad tehisintellektisüsteemi lähtekoodi, tehisintellektisüsteemi väljatöötamisel kasutatud tehnilisi kirjeldusi, andmestikke, tehnilist teavet selle kohta, kuidas tehisintellektisüsteemi väljatöötamiseks kasutatud andmestikud saadi ja kuidas neid redigeeriti, teavet kasutatud väljatöötamismeetodi ja elluviidud väljatöötamisprotsessi kohta, konkreetse mudeli valiku põhjendust ja selle parameetreid ning teavet tehisintellektisüsteemi toimimise kohta.

#### ***D jagu. Andmestike kasutamise õigused***

##### Article 14 Avaliku sektori organisatsiooni andmestikega seotud õigused

- 14.1. Kõik avaliku sektori organisatsiooni andmestikega seotud õigused, sealhulgas intellektuaalomandi õigused, kuuluvad avaliku sektori organisatsioonile või avaliku sektori organisatsiooni määratud kolmandale isikule.
- 14.2. Tarnijal ei ole õigust kasutada avaliku sektori organisatsiooni andmestikke muul eesmärgil kui lepingu täitmiseks, kui B lisas ei ole sätestatud teisiti.
- 14.3. Kui B lisas ei ole sätestatud teisiti, peab tarnija avaliku sektori organisatsiooni esimesel nõudmisel hävitama avaliku sektori organisatsiooni andmestikud. Kui avaliku sektori organisatsioon seda nõuab, peab tarnija esitama mõistlikud tõendid avaliku sektori organisatsiooni andmestike hävitamise kohta.

##### Article 15 Tarnija andmestikega ja kolmandate isikute andmestikega seotud õigused

- 15.1. Kõik tarnija andmestikega ja kolmandate isikute andmestikega seotud õigused, sealhulgas intellektuaalomandi õigused, kuuluvad tarnijale või kolmandale isikule.
- 15.2. Tarnija annab avaliku sektori organisatsioonile mitteainuõigusliku õiguse kasutada tarnija andmestikke ja kolmandate isikute andmestikke, mis on igal juhul piisav lepingu sätete, sealhulgas käesolevate tingimuste täitmiseks, kui B lisas ei ole sätestatud teisiti.
- 15.3. **<Vabatahtlik>** Lõikes 15.2 kirjeldatud kasutusõigus hõlmab õigust kasutada tarnija andmestikke ja kolmandate isikute andmestikke tehisintellektisüsteemi, sealhulgas selle uute versioonide edasiarendamiseks avaliku sektori organisatsiooni või kolmanda isiku poolt.

##### Article 16 Andmestike üleandmine

- 16.1. Tarnija annab avaliku sektori organisatsiooni esimesel nõudmisel avaliku sektori organisatsioonile üle avaliku sektori organisatsiooni andmestike viimase versiooni.
- 16.2. Tarnija annab avaliku sektori organisatsiooni esimesel nõudmisel avaliku sektori organisatsioonile üle tarnija andmestike ja kolmandate isikute andmestike viimase versiooni, kui B lisas ei ole sätestatud teisiti.
- 16.3. Tarnija peab andmestikud avaliku sektori organisatsioonile üle andma ühtses failivormingus, mille määrab avaliku sektori organisatsioon. **<Vabatahtlik> Andmestikud tagastatakse järgmiselt: [failivorming].**

Article 17 Kaitse nõuete eest

- 17.1. Tarnija kaitseb avaliku sektori organisatsiooni kõigi nõuete eest, mille kolmandad isikud, sealhulgas järelevalveasutused, esitavad seoses oma intellektuaalomandi õiguste või eraelu puutumatuse õiguste võimaliku rikkumisega, ning samaväärsete nõuete eest, mis on seotud teadmistega, ebaseadusliku konkurentsiga jms ning tulenevad tarnija andmestikest ja kolmandate isikute andmestikest.
- 17.2. Avaliku sektori organisatsioon kaitseb tarnijat kõigi nõuete eest, mille kolmandad isikud, sealhulgas järelevalveasutused, esitavad seoses oma intellektuaalomandi õiguste või eraelu puutumatuse õiguste võimaliku rikkumisega, ning samaväärsete nõuete eest, mis on seotud teadmistega, ebaseadusliku konkurentsiga jms ning tulenevad avaliku sektori organisatsiooni andmestikest.

***E jagu. Tehisintellektisüsteemide register ja auditeerimine***

Article 18 <Vabatahtlik> Tehisintellektisüsteemide register

- 18.1. Tarnija esitab avaliku sektori organisatsiooni esimesel nõudmisel avaliku sektori organisatsioonile C lisas ja D lisas kirjeldatud teabe kõige uuema versiooni.
- 18.2. Avaliku sektori organisatsioonil on õigus jagada lõikes 18.1 osutatud teavet kolmandate isikutega ja seda avalikustada, näiteks tehisintellektisüsteemide registris.
- 18.3. Kui avaliku sektori organisatsioon seda nõuab, aitab tarnija tehisintellektisüsteeme registreerida mis tahes asjakohases registris.

Article 19 Tingimustele vastavus ja auditeerimine

- 19.1. Tarnija peab avaliku sektori organisatsiooni esimesel nõudmisel tegema avaliku sektori organisatsioonile kättesaadavaks kogu käesolevatele tingimustele vastavust tõendava teabe.
- 19.2. Tarnija on kohustatud tegema koostööd avaliku sektori organisatsiooni poolt või nimel tehtava auditi või muud liiki kontrolli käigus, mille eesmärk on hinnata, kas tarnija täidab alati käesolevates tingimustes sätestatud kohustusi. See koostöö hõlmab kogu avaliku sektori organisatsiooni nõutud teabe esitamist, rakendatud riskijuhtimissüsteemist ülevaate andmist, tarnijate töötajate vestlusteks kättesaadavaks tegemist ja tarnija asukohtadele juurdepääsu võimaldamist.
- 19.3. Avaliku sektori organisatsioon koostab või laseb koostada aruande, milles dokumenteeritakse auditi järeldused. Aruandes märgib avaliku sektori organisatsioon, mil määral tarnija täidab lepingust tulenevaid kohustusi. Kui avaliku sektori organisatsioon teeb kindlaks, et tarnija ei täida käesolevast artiklist tulenevaid kohustusi, on tarnija kohustatud kõrvaldama avaliku sektori organisatsiooni tuvastatud puudused mõistliku tähtsaja jooksul, mille avaliku sektori organisatsioon on aruandes kindlaks määranud. Kui tarnija ei kõrvalda avaliku sektori organisatsiooni tuvastatud puudusi nende puuduste

kõrvaldamiseks ette nähtud tähtaja jooksul, on tarnija seaduse alusel oma kohustused täitmata jätnud.

- 19.4. Avaliku sektori organisatsioonil on õigus avaldada lõikes 19.3 osutatud aruande järeldused.
- 19.5. Avaliku sektori organisatsioonil on õigus teha või lasta teha audit üks kord kalendriaastas või seoses mis tahes olulise muudatusega.
- 19.6. Avaliku sektori organisatsioon võib otsustada, et kogu auditi või selle osa teeb sõltumatu audiitor.
- 19.7. Avaliku sektori organisatsiooni palgatava audiitori kulud tasub avaliku sektori organisatsioon. Avaliku sektori organisatsioon maksab tarnijale mõistlikku tasu võimalike kulude eest, mis tarnijal seoses auditiga tekivad. Vaidlus sellise tasu suuruse üle ei anna ühelgi juhul tarnijale õigust peatada käesolevatest tingimustest tulenevate kohustuste täitmine. Avaliku sektori organisatsioon ei ole kohustatud nimetatud tasu maksma, kui auditi käigus selgub, et tarnija ei ole täitnud käesolevatest tingimustest tulenevaid kohustusi.

### ***F jagu. Kulud***

#### Article 20      Kulud

Kui lepinguosalisel ei lepi kokku teisiti või kui käesolevates tingimustes ei ole sõnaselgelt sätestatud teisiti, ei ole avaliku sektori organisatsioon kohustatud maksma tarnijale käesolevatest tingimustest tuleneva töö eest lisatasu.

## **A lisa. Tehisintellektisüsteem ja selle sihtotstarve**

### Tehisintellektisüsteemi kirjeldus

Käesolevate tingimuste kohaldamisalasse kuuluvad järgmised süsteemid või nende komponendid.

*Esitage tehisintellektisüsteemi(de) kirjeldus. Tegemist võib olla ka algoritmilise süsteemiga, mis ei kvalifitseeru tehisintellektimääruse kohaselt tehisintellektisüsteemiks.*

### Sihtotstarve

*Kirjeldage kasutust, mille tarbeks tehisintellektisüsteem on ette nähtud.*

## B lisa. Andmestikud

*Kirjeldage tehisintellektisüsteemi treenimiseks (vajaduse korral), valideerimiseks ja testimiseks kasutatavaid andmestikke. Eristada tuleb avaliku sektori organisatsiooni andmestikke, tarnija andmestikke ja kolmandate isikute andmestikke. Avaliku sektori organisatsiooni andmestike puhul kirjeldage eesmärke, milleks tarnija võib andmestikke kasutada (peale lepingu täitmise), ja märkige, kas tarnija on kohustatud lepingu kehtivusaja lõpul andmestiku hävitama. Tarnija andmestike ja kolmandate isikute andmestike puhul kirjeldage eesmärke, milleks avaliku sektori organisatsioon võib andmestikke kasutada, ja märkige, kas tarnija on kohustatud andmestikud üle andma.*

### Avaliku sektori organisatsiooni andmestikud

Lepingu raames edastatakse avaliku sektori organisatsiooni poolt tarnijale või luuakse või kogutakse järgmised andmestikud.

Andmestiku kirjeldus	Tarnija kasutusõigused	Kohustus hävitada andmestik lepingu kehtivusaja lõpul
		Jah/ei
		Jah/ei
		Jah/ei
		Jah/ei

### Tarnija andmestikud ja kolmandate isikute andmestikud

Tehisintellektisüsteemi treenimiseks (vajaduse korral), valideerimiseks ja testimiseks kasutatakse või kasutati järgmisi tarnija andmestikke ja kolmandate isikute andmestikke.

Andmestiku kirjeldus	Avaliku sektori organisatsiooni kasutusõigused	Üleandmise kohustus <sup>1</sup>
		Jah/ei
		Jah/ei
		Jah/ei
		Jah/ei

<sup>1</sup> Tarnija andmestike ja kolmandate isikute andmestike üleandmise kohustuse piiramine ei piira tarnija kohustusi, mis on sätestatud artiklites 6 ja 13.

## C lisa. Tehniline dokumentatsioon

Tehniline dokumentatsioon peab sisaldama vähemalt järgmist teavet, kui see on asjaomase tehisintellektisüsteemi puhul kohaldatav.

1. Tehisintellektisüsteemi üldine kirjeldus, sealhulgas:
  - 1.1. süsteemi sihtotstarve, tarnija nimi, kuupäev ja süsteemi versioon;
  - 1.2. nende andmete laad, mida süsteem tõenäoliselt töötleb või mille töötlemiseks süsteem on ette nähtud, ning isikuandmete puhul füüsiliste isikute kategooriad ja rühmad, keda see tõenäoliselt või ette kavatselt mõjutab;
  - 1.3. tehisintellektisüsteemi võimalik koostoime riistvara või tarkvaraga, mis ei ole ise tehisintellektisüsteemi osa, või sellise koostoime eesmärgil kasutamine, kui see on asjakohane;
  - 1.4. asjaomase tarkvara või püsivara versioonid ja kõik versiooniuuendustega seotud nõuded;
  - 1.5. ammendav kirjeldus kõigi vormide kohta, milles tehisintellektisüsteem turule lastakse või kasutusele võetakse;
  - 1.6. selle riistvara kirjeldus, millel kasutamiseks on tehisintellektisüsteem ette nähtud;
  - 1.7. kui tehisintellektisüsteem on toote osa, siis fotod või joonised, mis kujutavad toote välist vormi, märgistust ja sisemist struktuuri;
  - 1.8. süsteemi peamise optimeerimiseesmärgi või -eesmärkide üksikasjalik ja kergesti mõistetav kirjeldus;
  - 1.9. süsteemi eeldatava väljundi ja selle kvaliteedi üksikasjalik ja kergesti mõistetav kirjeldus;
  - 1.10. üksikasjalikud ja kergesti mõistetavad juhtnöörid süsteemi väljundi tõlgendamiseks;
  - 1.11. näited stsenaariumidest, mille puhul süsteemi ei tohiks kasutada.
  
2. Tehisintellektisüsteemi komponentide ja selle väljatöötamise protsessi üksikasjalik kirjeldus, sealhulgas:
  - 2.1. tehisintellektisüsteemi väljatöötamise meetodid ja etapid, sealhulgas, kui see on asjakohane, kolmandate isikute pakutavate eeltreenitud süsteemide või töövahendite kasutamine ning see, kuidas tarnija on neid kasutanud, need integreerinud või neid muutnud, sealhulgas selliste kolmandate isikute sisenditega seotud litsentsilepingute või muude lepinguliste kokkulepete kirjeldus;
  - 2.2. süsteemi projekti kirjeldus, täpsemalt tehisintellektisüsteemi ja algoritmide üldine loogika; olulisemad konstruktsioonivalikud, sh põhjendused ja eeldused, kaasa arvatud nende isikute või isikute rühmade kohta, kelle puhul tehisintellektisüsteemi kavatsetakse kasutada; peamised liigitamisvalikud; mida on süsteem projekteeritud optimeerima ja milline on eri parameetrite olulisus; otsused võimalike kompromisside kohta seoses kasutatud tehniliste lahendustega, et järgida käesolevates tingimustes sätestatud nõudeid;
  - 2.3. süsteemi arhitektuuri kirjeldus, milles selgitatakse, kuidas tarkvarakomponendid üksteisele toetuvad või üksteisele sisendit annavad ja üldise andmetöötlusega



- integreeruvad; tehisintellektisüsteemi väljatöötamiseks, treenimiseks, testimiseks ja valideerimiseks kasutatud arvutusressursid;
- 2.4. kui see on asjakohane, siis andmetele esitatavad nõuded andmelehtedena, milles kirjeldatakse treenimismeetodeid ja -võtteid ning kasutatud treeningandmestikke, sh teave andmestike päritolu, ulatuse ja peamiste omaduste kohta; kuidas andmed on saadud ja valitud; märgistamismenetlused (nt juhendatud õppe korral), andmete puhastamise meetodid (nt võõrväärtuste avastamine);
- 2.5. kui see on asjakohane, siis tehisintellektisüsteemi ja selle toimimise ette kindlaks määratud muudatuste üksikasjalik kirjeldus koos kogu asjaomase teabega nende tehniliste lahenduste kohta, mida kasutatakse selleks, et tagada tehisintellektisüsteemi pidev vastavus käesolevates tingimustes sätestatud asjakohastele nõuetele;
- 2.6. kasutatud valideerimis- ja testimismenetlused, sh teave kasutatud valideerimis- ja testimisandmete ja nende peamiste omaduste kohta; parameetrid, mida kasutatakse selleks, et mõõta täpsust, stabiilsust ja küberturvalisust ning vastavust muudele käesolevates tingimustes sätestatud asjakohastele nõuetele ning võimalikku diskrimineerivat mõju; testilogid ja kõik testiaruanded, mis on dateeritud ja vastutavate isikute allkirjastatud, sh seoses punktis 2.5 osutatud ette kindlaks määratud muudatustega;
- 2.7. kasutusele võetud küberturbemeetmed.

Üksikasjalik teave tehisintellektisüsteemi seire, toimimise ja kontrollimise kohta, eeskätt seoses järgmisega: süsteemi funktsioonid ja toimimispiirangud, sh täpsusaste konkreetsete isikute või isikute rühmade puhul, kelle puhul tehisintellektisüsteemi kavatakse kasutada, ning üldine eeldatav täpsusaste võrreldes selle sihtotstarbega; prognoositavad soovimatud tagajärjed ja riskiallikad seoses tervise ja ohutuse, põhiõiguste ja diskrimineerimisega, lähtudes tehisintellektisüsteemi sihtotstarbest.

3. Riskijuhtimissüsteemi üksikasjalik kirjeldus vastavalt artiklile 2.
4. Tarnija poolt süsteemis selle kasutusaja jooksul tehtud asjakohaste muudatuste kirjeldus.

## D lisa. Kasutusjuhend

Kasutusjuhend peab sisaldama vähemalt järgmist teavet, kui see on asjaomase tehisintellektisüsteemi puhul kohaldatav.

1. Tarnija ja vajaduse korral tema volitatud esindajate nimed ja kontaktandmed.
2. Tehisintellektisüsteemi omadused, funktsioonid ja toimimispiirangud, sealhulgas vastavalt vajadusele:
  - 2.1. sihtotstarve;
  - 2.2. artiklis 8 osutatud täpsuse, stabiilsuse ja küberturvalisuse tase, mille suhtes tehisintellektisüsteem on testitud ja valideeritud ning mida võib eeldada, ning võimalikud selgelt teadaolevad ja prognoositavad asjaolud, mis võivad seda eeldatavat täpsuse, stabiilsuse ja küberturvalisuse taset mõjutada;
  - 2.3. võimalikud selgelt teadaolevad või prognoositavad asjaolud, mis on seotud tehisintellektisüsteemi kasutamisega vastavalt selle sihtotstarbele või mõistlikult prognoositava väärkasutamise tingimustes ning mis võivad seada ohtu tervise ja ohutuse või põhiõigused;
  - 2.4. mil määral suudab tehisintellektisüsteem selgitada oma otsuseid;
  - 2.5. süsteemi toimimine seoses isikute või isikute rühmadega, kelle puhul tehisintellektisüsteemi kavatsetakse kasutada;
  - 2.6. asjakohane teave kasutaja toimingute kohta, mis võivad mõjutada süsteemi toimimist, sealhulgas teave sisendandmete liigi või kvaliteedi kohta, või mis tahes muu asjakohane teave kasutatud treenimis-, valideerimis- ja testimisandmestike kohta, võttes arvesse tehisintellektisüsteemi sihtotstarvet.
3. Võimalikud muudatused tehisintellektisüsteemis ja selle toimimises, mille tarnija on ette kindlaks määranud.
4. Artiklis 7 osutatud inimjärelevalve meetmed, sealhulgas tehnilised meetmed, mis on kehtestatud selleks, et hõlbustada tehisintellektisüsteemi väljundite tõlgendamist avaliku sektori organisatsiooni poolt.
5. Tehisintellektisüsteemi eeldatav kasutusiga ning hooldus- ja hoolsusmeetmed, mis on vajalikud selleks, et tagada tehisintellektisüsteemi nõuetekohane toimimine, sealhulgas seoses tarkvarauuendustega.
6. Tehisintellektisüsteemis sisalduvate mehhanismide kirjeldus, mis võimaldavad kasutajatel logisid nõuetekohaselt koguda, salvestada ja tõlgendada.

**E lisa. Läbipaistvuse tagamise meetmed**

*Kirjeldage tehnilisi ja korralduslikke meetmeid, mida tarnija peab rakendama, et tagada läbipaistvus vastavalt käesolevate tingimuste artiklile 6.*

**F lisa. Inimjärelevalve tagamise meetmed**

*Kirjeldage tehnilisi ja korralduslikke meetmeid, mida tarnija peab rakendama, et tagada inimjärelevalve vastavalt käesolevate tingimuste artiklile 7.*

**G lisa. Täpsustasemed**

*Kirjeldage siin nõutavaid täpsustasemeid.*

#### **H lisa. Asjakohasel tasemel stabiilsuse, ohutuse ja küberturvalisuse tagamise meetmed**

*Kirjeldage tehnilisi ja korralduslikke meetmeid, mida tarnija peab rakendama, et tagada asjakohasel tasemel stabiilsus, ohutus ja küberturvalisus vastavalt käesolevate tingimuste artiklile 8.*

*Nende meetmetega tuleb tagada, et tehisintellektisüsteem on võimalikult vastupidav vigade, rikete või ebakõlade suhtes, mis võivad tekkida süsteemis või süsteemi töökeskkonnas, eelkõige süsteemi koostoime tõttu füüsiliste isikutega või muude süsteemidega.*

*Tehisintellektisüsteem peab vastu pidama volitamata kolmandate isikute katsetele muuta selle kasutamist, käitumist, väljundeid või toimimist, kasutades ära süsteemi nõrkusi. Tehisintellektile iseloomulike nõrkustega toimetulemiseks kasutatavad tehnilised lahendused võivad olenevalt asjaoludest hõlmata meetmeid, millega hoida ära, avastada, peatada, lahendada ja ohjata treenimisandmestiku manipuleerimiseks („andmemürgitus“) või treenimisel kasutatavate eeltreenitud komponentide manipuleerimiseks („mudelimürgitus“) tehtavaid ründeid, samuti sisendeid, mille eesmärk on panna mudel viga tegema („vastandnäited“ või „mudelihälbed“), konfidentsiaalsuse vastu suunatud ründeid või mudelivigu, mis võivad viia kahjulike otsuste tegemiseni.*