Euroopa Liidu
Nõukogu

Brüssel, 25. november 2022
(OR. en)

14954/22

Institutsioonidevaheline dokument: 2021/0106(COD)

LIMITE

TELECOM 472
JAI 1494
COPEN 396
CYBER 374
DATAPROTECT 320
EJUSTICE 89
COSI 293
IXIM 267
ENFOPOL 569
RELEX 1556
MI 843
COMPET 918
CODEC 1773

MÄRKUS

Saatja:	Alaliste esindajate komitee (COREPER I)
Saaja:	Nõukogu
Eelmise dok nr:	14336/22
Komisjoni dok nr:	8115/21
Teema:	Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte – Üldine lähenemisviis

I. SISSEJUHATUS

1. Komisjon võttis 21. aprillil 2021 vastu määruse ettepaneku, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (**tehisintellekti käsitlev õigusakt**).

2. Komisjoni ettepaneku eesmärk on tagada, et liidu turule lastavad ja liidus kasutatavad tehisintellektisüsteemid oleksid ohutud ning kooskõlas kehtiva põhiõigusi käsitleva õigusega ja liidu väärtustega, tagada õiguskindlus tehisintellekti tehtavate investeeringute ja innovatsiooni soodustamiseks, tugevdada juhtimist ja tõhustada põhiõigusi ja ohutust käsitleva kehtiva õiguse täitmist ning hõlbustada seaduslike, ohutute ja usaldusväärsete tehisintellektirakenduste ühtse turu väljatöötamist ja vältida turu killustumist.

II. TÖÖ TEISTES INSTITUTSIOONIDES

3. Euroopa Parlamendis juhivad arutelu komisjonide ühiste koosolekutega menetluse kohaselt siseturu- ja tarbijakaitsekomisjon (IMCO) (raportöör: Brando Benifei, S& D, Itaalia) ning kodanikuvabaduste, justiits- ja siseasjade komisjon (LIBE) (raportöör: Dragos Tudorache, Renew, Rumeenia). Õigusloomealasesse töösse on jagatud ja/või ainupädevuse alusel kaasatud õiguskomisjon (JURI), tööstuse, teadusuuringute ja energeetikakomisjon (ITRE) ning kultuuri- ja hariduskomisjon (CULT). Kaks kaasraportööri avaldasid oma raporti projekti 2022. aasta aprillis ning IMCO ja LIBE ühise raporti hääletus on kavandatud 2023. aasta esimesse kvartalisse.

4. Euroopa Majandus- ja Sotsiaalkomitee esitas ettepaneku kohta oma arvamuse 22. septembril 2021 ning Regioonide Komitee 2. detsembril 2021.

5. 18. juunil 2021 esitasid Euroopa Andmekaitsenõukogu ja Euroopa Andmekaitseinspektor ettepaneku kohta ühisarvamuse.

6. Euroopa Keskpank (EKP) esitas oma arvamuse 29. detsembril 2021 ja tutvustas seda telekommunikatsiooni ja infoühiskonna töörühma (edaspidi TELECOMi töörühm) 10. veebruari 2022. aasta koosolekul.

III. NÕUKOGU TÖÖ HETKESEIS

1. Nõukogus vaadati ettepanek läbi TELECOMi töörühmas. Nimetatud töörühm alustas ettepaneku arutamist Portugali eesistumise ajal, korraldades 2021. aasta aprillist juunini mitmeid koosolekuid ja seminare. Töö ettepanekuga jätkus Sloveenia eesistumise ajal, kes koostas esimese osalise kompromissettepaneku, mis hõlmas **artikleid 1–7 ja I–III lisa**. Lisaks korraldas eesistujariik Sloveenia telekommunikatsooniministrite nõukogu mitteametliku poolepäevase kohtumise, mis oli pühendatud ainult tehisintellekti käsitleva õigusakti ettepaneku käsitlemisele ja mille käigus ministrid kinnitasid, et toetavad horisontaalset ja inimkeskset lähenemisviisi tehisintellekti reguleerimisele. Eesistujariik Prantsusmaa jätkas läbivaatamisprotsessi ja sõnastas oma eesistumisperioodi lõpuks teksti ülejäänud osad **(artiklid 8–85 ja IV–IX lisa)** ümber ning esitas 17. juunil 2022 esimese konsolideeritud kompromissettepaneku kogu tehisintellekti käsitleva õigusakti kohta.

2. Eesistujariik Tšehhi pidas 5. juulil 2022 TELECOMi töörühmas poliitilise mõttevahetuse poliitikavalikuid käsitleva dokumendi alusel, mille tulemusi kasutati **teise kompromissteksti** ettevalmistamiseks. Võttes aluseks delegatsioonide vastused nimetatud kompromissile, koostas eesistujariik Tšehhi **kolmanda kompromissteksti**, mida esitleti ja arutati TELECOMi töörühmas 22. ja 29. septembril 2022. Pärast neid arutelusid paluti delegatsioonidel esitada täiendavad kirjalikud märkused, mida eesistujariik Tšehhi kasutas **neljanda kompromissettepaneku** koostamisel. Tuginedes TELECOMi töörühmas 25. oktoobril 2022 ja 8. novembril 2022 toimunud neljanda kompromissettepaneku aruteludele ning võttes arvesse liikmesriikide lõplikke kirjalikke märkusi, koostas eesistujariik Tšehhi lisas esitatud **kompromissteksti lõpliku versiooni**. COREPER vaatas 18. novembril kõnealuse kompromissettepaneku läbi ja **leppis ühehäälselt kokku, et see esitatakse ilma muudatusteta transpordi, telekommunikatsiooni ja energeetika nõukogule (telekommunikatsioon) üldise lähenemisviisi saavutamiseks** selle 6. detsembri 2022. aasta istungil.

IV. KOMPROMISSETTEPANEKU PÕHIELEMENDID

1. **Tehisintellektisüsteemi määratlus, tehisintellekti keelatud kasutusviisid, III lisas esitatud suure riskiga tehisintellektisüsteemide kasutusjuhtumite loetelu ja tehisintellektisüsteemi liigitamine suure riskiga tehisintellektisüsteemiks**

1.1 Tagamaks, et tehisintellektisüsteemi määratluses esitatakse piisavalt selged kriteeriumid tehisintellekti eristamiseks klassikalisematest tarkvarasüsteemidest, kitsendatakse kompromisstekstis **artikli 3 punktis 1** esitatud määratlust süsteemidele, mis on välja töötatud masinõppe lähenemisviiside ning loogika- ja teadmistepõhiste lähenemisviiside abil.

1.2 Seoses tehisintellektisüsteemi määratluse ajakohastamise volituste delegeerimisega komisjonile on välja jäetud **I lisa** ja vastav komisjonile antud õigus seda delegeeritud õigusaktidega ajakohastada. Selle asemel on lisatud uued **põhjendused 6a ja 6b**, et selgitada, mida tuleks mõista masinõppe lähenemisviiside ning loogika- ja teadmistepõhiste lähenemisviiside all. Selleks et tagada tehisintellekti käsitleva õigusakti paindlikkus ja tulevikukindlus, on **artiklisse 4** lisatud võimalus võtta vastu rakendusakte, et täiendavalt täpsustada ja ajakohastada masinõppe lähenemisviisi ning loogika- ja teadmistepõhiste lähenemisviiside meetodeid.

1.3 Seoses tehisintellekti keelatud kasutusviisidega on kompromissteksti **artiklis 5** laiendatud keeldu kasutada tehisintellekti sotsiaalseks hindamiseks ka erasektori osalejatele. Lisaks hõlmab säte, millega keelatakse kasutada tehisintellektisüsteeme, mis kasutavad ära konkreetse isikute rühma haavatavust, nüüd ka isikuid, kes on haavatavad oma sotsiaalse või majandusliku olukorra tõttu. Seoses keeluga õiguskaitseasutustele kasutada reaalajas toimuva biomeetrilise kaugtuvastamise süsteeme avalikult juurdepääsetavas ruumis selgitatakse kompromisstekstis eesmärke, mille korral peetakse sellist kasutamist õiguskaitse eesmärkidel rangelt vajalikuks ja mille puhul tuleks õiguskaitseasutustel seetõttu erandkorras lubada selliseid süsteeme kasutada.

1.4 **III lisa** suure riskiga tehisintellektisüsteemide kasutusjuhtumite loetelust on välja jäetud kolm juhtumit (süvavõltsingute avastamine õiguskaitseasutuste poolt, kuritegude analüüs, reisidokumentide autentsuse kontrollimine), lisatud on kaks juhtumit (kriitilise tähtsusega digitaristu ning elu- ja tervisekindlustus) ja teisi on täpsustatud. Samal ajal on muudetud **artikli 7 lõiget 1**, et näha ette võimalus delegeeritud aktide abil suure riskiga kasutusjuhtumite asjakohasesse loetellu lisamine kui ka sellest välja jätmine. Selleks et tagada selliste väljajätmiste korral põhiõiguste piisav kaitse, on **artikli 7 lõikesse 3** lisatud täiendavad sätted, milles täpsustatakse tingimused, mis peavad olema täidetud enne delegeeritud õigusakti vastuvõtmist.

1.5 Seoses tehisintellektisüsteemide liigitamisega suure riskiga süsteemideks sisaldab kompromissettepanek nüüd peale **III lisa** suure riskiga liigituse täiendavat horisontaalset tasandit tagamaks, et ei oleks hõlmatud tehisintellektisüsteemid, mis tõenäoliselt ei põhjusta tõsiseid põhiõiguste rikkumisi ega muid märkimisväärseid riske. Täpsemalt sisaldab **artikli 6 lõige 3** uusi sätteid, mille kohaselt tuleks suure riskiga tehisintellektisüsteemide liigitamisel arvesse võtta ka tehisintellektisüsteemi väljundi olulisust seoses asjaomase meetme või tehtava otsusega. Tehisintellektisüsteemi väljundi olulisust hinnatakse selle põhjal, kas see on asjaomase meetme või tehtava otsuse suhtes puhtalt täiendav või mitte.

2. Nõuded suure riskiga tehisintellektisüsteemidele ja tehisintellekti väärtusahela eri osalejate kohustused

2.1 Paljusid suure riskiga tehisintellektisüsteemidele esitatavaid nõudeid, mis on sätestatud ettepaneku **III jaotise 2. peatükis**, on selgitatud ja kohandatud nii, et need on tehniliselt teostatavamad ja sidusrühmade jaoks vähem koormavad, näiteks seoses andmete kvaliteediga või tehnilise dokumentatsiooniga, mille VKEd peaksid koostama tõendamaks, et nende suure riskiga tehisintellektisüsteemid vastavad nõuetele.

2.2 Kuna tehisintellektisüsteeme arendatakse ja levitatakse keerukate väärtusahelate raames, sisaldab kompromisstekst muudatusi, millega selgitatakse kohustuste ja rollide jaotust. Näiteks on **artiklitesse 13 ja 14** lisatud mõned täiendavad sätted, mis võimaldavad tõhusamat koostööd tehisintellektisüsteemide pakkujate ja kasutajate vahel. Kompromissteksti eesmärk on ka selgitada tehisintellekti käsitlevast õigusaktist tulenevate kohustuste ja selliste kohustuste vahelist seost, mis on juba sätestatud teiste õigusaktidega, näiteks asjakohaste liidu andmekaitsealaste või valdkondlike õigusaktidega, sealhulgas seoses finantsteenuste sektoriga. Lisaks osutatakse uues **artiklis 23a** selgemalt olukordadele, kus teised väärtusahelas osalejad on kohustatud võtma pakkuja kohustused.

3. Üldotstarbelised tehisintellektisüsteemid

3.1 Lisatud on uus **IA jaotis**, et võtta arvesse olukordi, kus tehisintellektisüsteeme saab kasutada paljudel erinevatel eesmärkidel (üldotstarbeline tehisintellekt), ja võimalikke olukordi, kus üldotstarbeline tehisintellektitehnoloogia integreeritakse teise süsteemi, mis võib muutuda suure riskiga süsteemiks. Kompromisstekstis täpsustatakse **artikli 4b lõikes 1**, et teatavaid suure riskiga tehisintellektisüsteemidele esitatavaid nõudeid kohaldatakse ka üldotstarbeliste tehisintellektisüsteemide suhtes. Nende nõuete otsese kohaldamise asemel täpsustatakse rakendusaktis, kuidas neid tuleks kohaldada üldotstarbeliste tehisintellektisüsteemide suhtes, tuginedes konsulteerimisele ja üksikasjalikule mõjuhinnangule ning võttes arvesse nende süsteemide ja nendega seotud väärtusahela eriomadusi, tehnilist teostatavust ning turu ja tehnoloogia arengut. Rakendusakti kasutamine tagab liikmesriikide nõuetekohase kaasamise ja neile jääb lõplik sõnaõigus nõuete kohaldamise kohta selles kontekstis.

3.2 Lisaks sisaldab **artikli 4b lõike 5** kompromisstekst ka võimalust võtta vastu täiendavaid rakendusakte, milles sätestatakse reeglid koostööks üldotstarbeliste tehisintellektisüsteemide pakkujate ja muude selliste pakkujate vahel, kes kavatsevad sellised süsteemid kasutusele võtta või liidu turule lasta suure riskiga tehisintellektisüsteemidena, eelkõige seoses teabe esitamisega.

4. **Kavandatava tehisintellekti käsitleva õigusakti kohaldamisala ja õiguskaitseasutusi käsitlevate sätete täpsustamine**

4.1 **Artiklis 2** on sõnaselgelt viidatud riikliku julgeoleku, kaitse- ja sõjaliste eesmärkide väljajätmisele tehisintellekti käsitleva õigusakti kohaldamisalast. Samuti on selgitatud, et tehisintellekti käsitlevat õigusakti ei tuleks kohaldada tehisintellektisüsteemide ja nende väljundite suhtes, mida kasutatakse üksnes teadus- ja arendustegevuse eesmärgil, ning tehisintellekti muul otstarbel kui tööülesannete täitmiseks kasutavate inimeste kohustuste suhtes, mis jääksid tehisintellekti käsitleva õigusakti kohaldamisalast välja, välja arvatud läbipaistvuskohustused.

4.2 Selleks et võtta arvesse õiguskaitseasutuste eripära, tehti mitu muudatust sätetes, mis on seotud tehisintellektisüsteemide kasutamisega õiguskaitse eesmärkidel. Eeskätt on täpsustatud mõningaid **artiklis 3** esitatud seotud mõisteid, nagu „biomeetrilise kaugtuvastamise süsteem“ ja „reaalajas toimuva biomeetrilise kaugtuvastamise süsteem“, et selgitada, millised olukorrad kuuluksid asjaomase keelu ja suure riskiga kasutusjuhtumi alla ning millised mitte. Kompromissettepanek sisaldab ka muid muudatusi, mille suhtes kohaldatakse asjakohaseid kaitsemeetmeid ja mille eesmärk on tagada õiguskaitseasutuste poolt suure riskiga tehisintellektisüsteemide kasutamisel piisav paindlikkus või kaaluda vajadust austada oma tegevusega seotud tundlike operatiivandmete konfidentsiaalsust.

5. **Vastavushindamine, juhtimise raamistik, turujärelevalve, jõustamine ja karistused**

5.1 Tehisintellekti käsitleva õigusakti vastavusraamistiku lihtsustamiseks on kompromisstekstis täpsustatud ja lihtsustatud mitut vastavushindamismenetlust käsitlevat sätet. Samuti on selgitatud ja lihtsustatud turujärelevalvet käsitlevaid sätteid, et muuta need tõhusamaks ja hõlpsamini rakendatavaks, võttes arvesse vajadust järgida selles küsimuses proportsionaalset lähenemisviisi. Lisaks on põhjalikult läbi vaadatud **artikkel 41**, et piirata komisjoni kaalutlusõigust selliste rakendusaktide vastuvõtmisel, millega kehtestatakse suure riskiga tehisintellektisüsteemide ja üldotstarbeliste tehisintellektisüsteemide nõuete ühtsed tehnilised kirjeldused.

5.2 Kompromisstekstis on oluliselt muudetud ka sätteid, mis käsitlevad tehisintellekti nõukoda (edaspidi „nõukoda“), et tagada selle suurem autonoomsus ja tugevdada selle rolli tehisintellekti käsitleva õigusakti juhtimisstruktuuris. Sellega seoses on läbi vaadatud **artiklid 56 ja 58**, et tugevdada nõukoja rolli nii, et tal oleksid paremad võimalused toetada liikmesriike tehisintellekti käsitleva õigusakti rakendamisel ja jõustamisel. Täpsemalt on laiendatud nõukoja ülesandeid ja täpsustatud selle koosseisu. Selleks et tagada sidusrühmade kaasamine kõigisse tehisintellekti käsitleva õigusakti rakendamisega seotud küsimustesse, sealhulgas rakendusaktide ja delegeeritud õigusaktide ettevalmistamisse, on lisatud uus nõue, et nõukoda looks alalise allrühma, mis toimiks platvormina paljude sidusrühmade jaoks. Samuti tuleks luua turujärelevalveasutuste ja teavitavate asutuste jaoks veel kaks alalist allrühma, et tugevdada tehisintellekti käsitleva õigusakti juhtimise ja täitmise tagamise järjepidevust kogu liidus.

5.3 Juhtimise raamistiku edasiseks parandamiseks sisaldab kompromisstekst uusi **artikleid 68a ja 68b. Artiklis 68a** on nõue, et komisjon määraks tehisintellekti valdkonnas ühe või mitu liidu katserajatist, mis peaksid nõukoja või turujärelevalveasutuste taotlusel andma sõltumatut tehnilist või teaduslikku nõu, ning **artikliga 68b** kehtestatakse komisjonile kohustus luua keskne sõltumatute ekspertide reserv, et toetada tehisintellekti käsitleva õigusakti alusel nõutavaid jõustamistoiminguid. Lisaks on olemas ka uus **artikkel 58a**, milles on sätestatud komisjoni kohustus koostada suunised tehisintellekti käsitleva õigusakti kohaldamise kohta.

5.4 Tehisintellekti käsitleva õigusakti sätete rikkumise eest määratavate karistuste osas nähakse kompromissteksti **artiklis 71** VKEdele ja idufirmadele ette proportsionaalsemad haldustrahvide piirmäärad. Samuti on **artikli 71 lõikesse 6** lisatud veel neli kriteeriumi, mille alusel otsustada haldustrahvide suuruse üle, et veelgi enam tagada nende üldine proportsionaalsus.

6. **Läbipaistvus ja muud sätted mõjutatud isikute toetamiseks**

6.1 Kompromissettepanek sisaldab mitut suure riskiga tehisintellektisüsteemide kasutamise läbipaistvust suurendavat muudatust. Eeskätt on ajakohastatud **artiklit 51**, osutamaks sellele, et teatavatel suure riskiga tehisintellektisüsteemi kasutajatel, kes on avaliku sektori asutused, ametid või organid, on samuti kohustus end registreerida III lisas loetletud suure riskiga tehisintellektisüsteemide ELi andmebaasis. Lisaks rõhutatakse uues **artikli 52 lõikes 2a** emotsioonituvastussüsteemi kasutajate kohustust teavitada füüsilisi isikuid, kui nad sellise süsteemiga kokku puutuvad.

6.2 Kompromissettepanekus selgitatakse ka uues artikli **63 lõikes 11**, et füüsiline või juriidiline isik, kellel on põhjust arvata, et tehisintellekti käsitleva õigusakti sätteid on rikutud, võib esitada kaebuse asjaomasele turujärelevalveasutusele ja võib eeldada, et sellist kaebust käsitletakse kooskõlas selle asutuse erimenetlustega.

7. **Innovatsiooni toetavad meetmed**

7.1 Innovatsioonisõbralikuma õigusraamistiku loomiseks ja tõenduspõhise regulatiivse õppimise edendamiseks on **artikli 53** sätteid innovatsiooni toetavate meetmete kohta kompromisstekstis oluliselt muudetud. Eeskätt on selgitatud, et tehisintellekti regulatsiooni testkeskkonnad, mis peaksid looma kontrollitud keskkonna innovatiivsete tehisintellektisüsteemide arendamiseks, testimiseks ja valideerimiseks riiklike pädevate asutuste otsese järelevalve ja juhendamise all, peaksid võimaldama innovatiivsete tehisintellektisüsteemide testimist ka tegelikes tingimustes. Samuti on lisatud uued **artiklid 54a ja 54b**, mille sätted võimaldavad tehisintellektisüsteemide järelevalveta testimist tegelikes tingimustes, kohaldades eritingimusi ja kaitsemeetmeid. Mõlemal juhul selgitatakse kompromisstekstis, kuidas neid uusi norme tuleb tõlgendada võrreldes selle valdkonna muude kehtivate regulatsiooni testkeskkondi käsitlevate õigusaktidega.

7.2 Selleks et kergendada väiksemate ettevõtjate halduskoormust, on kompromissteksti **artiklis 55** loetelu meetmetest, mida komisjon peab võtma selliste operaatorite toetamiseks, ning **artiklis 55a** on ette nähtud mõned piiratud ja selgelt määratletud erandid.

V. KOKKUVÕTE

1. Eeltoodut silmas pidades palutakse nõukogul:
   - vaadata läbi käesoleva dokumendi lisas esitatud kompromisstekst;
   - Kinnitada transpordi, telekommunikatsiooni ja energeetika nõukogu 6. detsembri 2022. aasta istungil (telekommunikatsioon) üldine lähenemisviis seoses määrusega, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt).

_____

LISA

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

MILLEGA NÄHAKSE ETTE TEHISINTELLEKTI KÄSITLEVAD ÜHTLUSTATUD ÕIGUSNORMID (TEHISINTELLEKTI KÄSITLEV ÕIGUSAKT) JA MUUDETAKSE TEATAVAID LIIDU ÕIGUSAKTE

(EMPs kohaldatav tekst)

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artikleid 16 ja 114,

võttes arvesse Euroopa Komisjoni ettepanekut,

olles edastanud seadusandliku akti eelnõu liikmesriikide parlamentidele,

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust[1],

võttes arvesse Regioonide Komitee arvamust[2],

võttes arvesse Euroopa Keskpanga arvamust[3],

toimides seadusandliku tavamenetluse kohaselt

ning arvestades järgmist:

[1] ELT C […], […], lk […].
[2] ELT C […], […], lk […].
[3] Viide EKP arvamusele.

(1) Käesoleva määruse eesmärk on parandada siseturu toimimist ühtse õigusraamistiku kehtestamisega eeskätt tehisintellekti arendamise, turustamise ja kasutamise jaoks kooskõlas liidu väärtustega. Käesolev määrus on ajendatud mitmest kaaluka üldise huvi eesmärgist, nagu kõrgetasemeline tervise, ohutuse ja põhiõiguste kaitse, ning sellega tahetakse tagada tehisintellektil põhinevate kaupade ja teenuste vaba piiriülene liikumine, vältides seega liikmesriikide kehtestatavaid piiranguid tehisintellektisüsteemide arendamisele, turustamisele ja kasutamisele, kui selleks pole just käesoleva määrusega antud selget luba.

(2) Tehisintellektisüsteeme on lihtne mitmesugustes majanduse ja ühiskonna sektorites kasutusele võtta, sh piiriüleselt, ning need võivad levida kogu liidus. Teatavad liikmesriigid on juba uurinud võimalust võtta vastu siseriiklikke õigusnorme, et tagada tehisintellekti ohutus ning selle arendamine ja kasutamine kooskõlas põhiõigustega seotud kohustustega. Siseriiklike õigusnormide vahelised erinevused võivad tuua kaasa siseturu killustumise ja vähendada tehisintellektisüsteemide arendamise, impordi ja kasutamisega tegelevate operaatorite õiguskindlust. Seepärast tuleks kõikjal liidus tagada kaitse järjekindlus ja kõrge tase ning ühtlasi vältida erinevusi, mis kahjustavad tehisintellektisüsteemide ja nendega seotud toodete ja teenuste vaba ringlust siseturul. Selleks tuleks operaatoritele kehtestada ühetaolised kohustused ja kindlustada kaalukate üldiste huvide ja isikute õiguste ühtne kaitse siseturul, lähtudes Euroopa Liidu toimimise lepingu (edaspidi „ELi toimimise leping“) artiklist 114. Kuivõrd käesolev määrus sisaldab konkreetseid õigusnorme, mis puudutavad üksikisikute kaitset seoses isikuandmete töötlemisega ja millega piiratakse tehisintellektisüsteemide kasutamist avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil reaalajas toimuva biomeetrilise kaugtuvastamise jaoks, on asjakohane võtta nende konkreetsete normide puhul käesoleva määruse aluseks ELi toimimise lepingu artikkel 16. Neid konkreetseid õigusnorme ja ELi toimimise lepingu artiklile 16 tuginemist silmas pidades on asjakohane konsulteerida Euroopa Andmekaitsenõukoguga.

(3) Tehisintellekt on kiirelt arenev tehnoloogiaharu, mis võib aidata saavutada mitmesuguseid majanduslikke ja ühiskondlikke hüvesid kõigis tööstusharudes ja ühiskondlikes tegevustes. Tänu täpsemale prognoosimisele, tegevuse ja ressursijaotuse optimeerimisele ning üksikisikutele ja organisatsioonidele kättesaadavate digilahenduste personaliseerimisele võib tehisintellekti kasutamine anda ettevõtjatele olulise konkurentsieelise ning toetada ühiskonna ja keskkonna jaoks positiivsete tulemuste saavutamist näiteks sellistes valdkondades nagu tervishoid, põllumajandus, haridus ja koolitus, taristuhaldus, energeetika, transport ja logistika, avalikud teenused, turvalisus, õigus, ressursi- ja energiatõhusus ning kliimamuutuste leevendamine ja nendega kohanemine.

(4) Samas võib tehisintellekt olenevalt konkreetse rakenduse ja kasutuse asjaoludest tekitada ka riske ning kahjustada avalikke huve ja liidu õigusega kaitstud õigusi. Selline kahju võib olla varaline või mittevaraline.

(5) Seepärast on vaja liidu õigusraamistikku, millega nähtaks ette tehisintellekti käsitlevad ühtlustatud õigusnormid, et edendada siseturul tehisintellekti arendamist, kasutamist ja levikut, mille puhul oleks ühtlasi tagatud liidu õigusega tunnustatud ja kaitstud üldiste huvide, näiteks tervise ja ohutuse ning põhiõiguste kõrgetasemeline kaitse. Selle eesmärgi saavutamiseks tuleks kehtestada teatavate tehisintellektisüsteemide turule laskmist ja kasutusele võtmist reguleerivad õigusnormid, et seeläbi tagada siseturu sujuv toimimine ja võimaldada neil süsteemidel saada kasu kaupade ja teenuste vaba liikumise põhimõttest. Kõnealuste õigusnormide kehtestamisega ja tuginedes kõrgetasemelise tehisintellekti eksperdirühma tööle, mis on kajastatud suunistes usaldusväärse tehisintellekti arendamiseks ELis, toetab käesolev määrus Euroopa Ülemkogu sõnastatud liidu eesmärki[4] olla maailmas turvalise, usaldusväärse ja eetilise tehisintellekti arendamisel liidripositsioonil ning samas aitab see tagada eetiliste põhimõtete kaitse, mida on eraldi nõudnud Euroopa Parlament[5].

---

4 Euroopa Ülemkogu, Euroopa Ülemkogu erakorraline kohtumine (1. ja 2. oktoober 2020) – Järeldused, EUCO 13/20, 2020, lk 6.

5 Euroopa Parlamendi 20. oktoobri 2020. aasta resolutsioon soovitustega komisjonile tehisintellekti, robotitehnoloogia ja seonduva tehnoloogia eetiliste aspektide raamistiku kohta, 2020/2012(INL).

(5a) Käesolevas määruses sätestatud tehisintellektisüsteemide turule laskmise, kasutusele võtmise ja kasutamise ühtlustatud õigusnorme tuleks kohaldada kõigis sektorites ning kooskõlas uue õigusraamistiku lähenemisviisiga ei tohiks need piirata kehtivat liidu õigust, eeskätt andmekaitset, tarbijakaitset, põhiõigusi, tööhõivet ja tooteohutust käsitlevaid õigusakte, mida käesolev määrus täiendab. Sellest tulenevalt jäävad muutumatuks ja täielikult kohaldatavaks kõik õigused ja õiguskaitsevahendid, mis on liidu õigusega ette nähtud tarbijatele ja muudele isikutele, keda tehisintellektisüsteemid võivad negatiivselt mõjutada, sealhulgas seoses võimaliku kahju hüvitamisega vastavalt nõukogu 25. juuli 1985. aasta direktiivile 85/374/EMÜ liikmesriikide tootevastutust käsitlevate õigus- ja haldusnormide ühtlustamise kohta. Lisaks sellele on käesoleva määruse eesmärk tugevdada selliste olemasolevate õiguste ja õiguskaitsevahendite tõhusust, kehtestades konkreetsed nõuded ja kohustused, sealhulgas seoses tehisintellektisüsteemide läbipaistvuse, tehnilise dokumenteerimise ja andmete säilitamisega. Samuti ei tohiks käesoleva määruse alusel tehisintellekti väärtusahelas osalevatele eri operaatoritele pandud kohustuste kohaldamine mõjutada liidu õigusega kooskõlas olevate teatavate tehisintellektisüsteemide kasutamist piiravate siseriiklike õigusaktide kohaldamist, kui sellised õigusaktid jäävad käesoleva määruse kohaldamisalast välja või kui nendega taotletakse muid õiguspäraseid avaliku huvi eesmärke kui need, mida taotletakse käesoleva määrusega. Näiteks ei tohiks käesolev määrus mõjutada siseriiklikku tööõigust ja alaealiste (st alla 18-aastaste isikute) kaitset käsitlevaid õigusakte, võttes arvesse ÜRO üldist märkust nr 25 (2021) laste õiguste kohta, niivõrd, kuivõrd need ei ole tehisintellektisüsteemidele eriomased ja taotlevad muid õiguspäraseid avaliku huvi eesmärke.

(6) Õiguskindluse tagamiseks tuleks tehisintellektisüsteemi mõiste selgelt määratleda, kuid samas tuleks säilitada paindlikkus, et jääks ruumi tehnika edasiseks arenguks. Määratlus peaks põhinema tehisintellekti peamistel funktsionaalsetel omadustel, nagu selle õppimis-, arutlus- või modelleerimisvõime, eristades seda lihtsamatest tarkvarasüsteemidest ja programmeerimisviisidest. Eelkõige peaks tehisintellektisüsteemidel käesoleva määruse kohaldamisel olema võimalik masin- ja/või inimpõhiste andmete ja sisendite põhjal tuletada, kuidas saavutada neile inimeste poolt seatud lõppeesmärke, kasutades masinõpet ja/või loogika- ja teadmistepõhiseid lähenemisviise, ning toota selliseid väljundeid nagu sisu generatiivsete tehisintellektisüsteemide jaoks (nt tekst, video või pildid), prognoosid, soovitused või otsused, mis mõjutavad keskkonda, millega süsteem suhtleb kas füüsilises või digitaalses plaanis. Süsteemi, mis kasutab toimingute automaatseks sooritamiseks üksnes füüsiliste isikute määratletud reegleid, ei tohiks käsitada tehisintellektisüsteemina. Tehisintellektisüsteeme saab projekteerida töötama erineval autonoomsuse tasemel ning neid võib kasutada eraldiseisvatena või mõne teise toote komponentidena, olenemata sellest, kas süsteem on füüsiliselt tootesse integreeritud (sisseehitatud) või teenib toote funktsionaalsust ilma, et oleks sellesse integreeritud (sisseehitamata). Tehisintellektisüsteemi autonoomia kontseptsioon on seotud sellega, mil määral toimib selline süsteem ilma inimese osaluseta.

(6a) Masinõppe lähenemisviisid keskenduvad selliste süsteemide väljatöötamisele, mis on võimelised õppima ja tegema andmete põhjal järeldusi rakendusprobleemi lahendamiseks, ilma et neid oleks selgelt programmeeritud sammsammuliste juhistega sisendist väljundini. Õppimine tähendab arvutusprotsessi, mille käigus optimeeritakse andmete põhjal mudeli parameetrid; tegemist on matemaatilise konstruktsiooniga, mis annab sisendandmetel põhineva väljundi. Masinõppe abil lahendatavad probleemid hõlmavad tavaliselt ülesandeid, mille puhul teiste lähenemisviiside kasutamine ei õnnestu kas seetõttu, et probleemi ei ole sobivalt formaliseeritud, või on probleemi lahendamine mitteõppiva lähenemisviisiga keeruline. Masinõppe lähenemisviisid hõlmavad näiteks juhendatud õpet, juhendamata õpet ja stiimulõpet, kasutades mitmesuguseid meetodeid, sh süvaõpet neurovõrkudega, statistilisi õppimis- ja järeldamismeetodeid (sealhulgas logistiline regressioon, Bayesi hinnang) ning otsingu- ja optimeerimismeetodeid.

(6b) Loogika- ja teadmistepõhiseid lähenemisviisid keskenduvad selliste süsteemide arendamisele, millel on rakendusprobleemi lahendamiseks olemas teadmistel põhinev loogiline arutlusvõime. Sellised süsteemid hõlmavad tavaliselt teadmusbaasi ja järeldusmootorit, mis loob teadmusbaasil põhineva arutluskäiguga väljundeid. Teadmusbaas, mille tavaliselt kodeerivad inimeksperdid, koosneb üksustest ja loogilistest seostest, mis on rakendusprobleemi seisukohast olulised, lähtudes skeemidest, mis põhinevad reeglitel, ontoloogiatel või teadmiste graafikutel. Järeldusmootor töötab teadmusbaasiga ja tekitab uut teavet selliste toimingute kaudu nagu sortimine, otsimine, sobitamine või järeldamine. Loogika- ja teadmistepõhised lähenemisviisid hõlmavad näiteks teadmuste esitamist, induktiivset (loogilist) programmeerimist, teadmusbaase, järeldavaid ja deduktiivseid masinaid, (sümbol)arutlust, eksperdisüsteeme ning otsingu- ja optimeerimismeetodeid.

(6c) Selleks et tagada käesoleva määruse ühetaolised rakendamistingimused masinõppe lähenemisviiside ning loogika- ja teadmistepõhiste lähenemisviiside osas ning võtta arvesse turu ja tehnoloogia arengut, tuleks komisjonile anda rakendamisvolitused.

(6d) Käesolevas määruses osutatud mõistet „kasutaja“ tuleks tõlgendada kui tehisintellektisüsteemi kasutavat mis tahes füüsilist või juriidilist isikut, sealhulgas ametiasutust, ametkonda või muud organit, kelle volitusel süsteemi kasutatakse. Olenevalt tehisintellektisüsteemi tüübist võib süsteemi kasutamine mõjutada lisaks kasutajale ka muid isikuid.

(7) Käesolevas määruses kasutatavat biomeetriliste andmete mõistet tuleks tõlgendada kooskõlas biomeetriliste andmete mõistega, mis on määratletud Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679[6] artikli 4 punktis 14, Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725[7] artikli 3 punktis 18 ja Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/680[8] artikli 3 punktis 13.

[6] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

[7] Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39).

[8] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK (õiguskaitsedirektiiv) (ELT L 119, 4.5.2016, lk 89).

(8) Käesolevas määruses kasutatav biomeetrilise kaugtuvastamise süsteemi mõiste tuleks määratleda funktsioonidest lähtuvalt kui tehisintellektisüsteem, mis on mõeldud füüsiliste isikute tavaliselt eemalt tuvastamiseks ilma nende aktiivse osaluseta, võrreldes isiku biomeetrilisi andmeid võrdlusandmehoidlas sisalduvate biomeetriliste andmetega, olenemata sellest, milliseid konkreetseid tehnoloogiaid ja protseduure või mis liiki biomeetrilisi andmeid selleks kasutatakse. Selliseid biomeetrilise kaugtuvastamise süsteeme kasutatakse tavaliselt mitme isiku või nende käitumise samaaegseks tajumiseks, et oluliselt hõlbustada paljude isikute tuvastamist ilma nende aktiivse osaluseta. Selline määratlus ei hõlma kontrolli-/autentimissüsteeme, mille ainus eesmärk on kinnitada, et konkreetne füüsiline isik on see, kes ta väidab end olevat, ega süsteeme, mida kasutatakse füüsilise isiku isikusamasuse kinnitamiseks üksnes selleks, et saada juurdepääs teenusele, seadmele või ruumidele. Kõnealune väljajätmine on põhjendatud asjaoluga, et sellistel süsteemidel on tõenäoliselt väike mõju füüsiliste isikute põhiõigustele võrreldes biomeetrilise kaugtuvastamise süsteemidega, mida võidakse kasutada suure hulga isikute biomeetriliste andmete töötlemiseks. Reaalajas kasutatavate süsteemide puhul toimub biomeetriliste andmete hõive, võrdlemine ja isiku identifitseerimine kõik hetkega, peaaegu hetkega või igal juhul ilma märkimisväärse viivituseta. Siinjuures ei tohiks jääda võimalust hoida väikeste viivituste kasutamisega kõrvale käesoleva määruse sätetest, mis käsitlevad tehisintellektisüsteemi kasutamist reaalajas. Reaalajalistes süsteemides kasutatakse kaamera või muu sarnase funktsiooniga seadmega tehtud otse edastatavat või peaaegu otse edastatavat materjali, näiteks videosalvestisi. Tagantjärele kasutatavate süsteemide puhul on aga biomeetriliste andmete hõive juba toimunud ning võrdlemine ja isikute identifitseerimine toimub alles pärast olulist viivitust. Sealjuures kasutatakse selliseid materjale nagu videovalvesüsteemi või isikliku seadmega tehtud pildid või videosalvestised, mis on tehtud enne, kui süsteemi kasutatakse konkreetse füüsilise isiku puhul.

(9) Käesoleva määruse kohaldamisel tuleks avalikult juurdepääsetava ruumina käsitada mis tahes füüsilist kohta, mis on määratlemata arvu füüsiliste isikute jaoks juurdepääsetav, olenemata sellest, kas kõnealune koht on era- või avalik-õiguslikus omandis, ning tegevusest, mille jaoks kohta võidakse kasutada, nagu kaubandus (näiteks kauplused, restoranid, kohvikud), teenused (näiteks pangad, ametialane tegevus, majutus), sport (näiteks ujumisbasseinid, võimlad, staadionid), transport (näiteks bussi-, metroo- ja raudteejaamad, lennujaamad, transpordivahendid), meelelahutus (näiteks kinod, teatrid, muuseumid, kontserdi- ja konverentsisaalid), vaba aja veetmine või muu (näiteks avalikud teed ja väljakud, pargid, metsad, mänguväljakud). Koht tuleks liigitada avalikult juurdepääsetavaks ka siis, kui olenemata võimalikest mahtuvuspiirangutest või turvapiirangutest on juurdepääs seotud teatud eelmääratletud tingimustega, mida saab täita määratlemata arv isikuid, näiteks pääsme või sõidupileti ostmine, eelnev registreerimine või isikute teatav vanus. Seevastu ei tohiks kohta pidada avalikult juurdepääsetavaks, kui juurdepääs on piiratud konkreetsete ja kindlaksmääratud füüsiliste isikutega kas liidu või liikmesriigi õiguse alusel, mis on otseselt seotud avaliku turvalisuse või julgeolekuga, või koha suhtes asjaomaseid volitusi omava isiku selge tahteavalduse alusel. Ainuüksi juurdepääsu faktiline võimalus (nt lukustamata uks, avatud aiavärav) ei tähenda, et koht on avalikult juurdepääsetav, kui on olemas vastupidisele viitavad tähised või asjaolud (nt juurdepääsu keelavad või piiravad märgid). Ettevõtete ja tehaste ruumid ning kontorid ja töökohad, millele on juurdepääs ainult asjaomastel töötajatel ja teenuseosutajatel, on kohad, mis ei ole avalikult juurdepääsetavad. Avalikult juurdepääsetavad ruumid ei tohiks hõlmata vanglaid ega piirikontrollialasid. Mõned muud alad võivad koosneda nii avalikult mitte juurdepääsetavatest kui ka avalikult juurdepääsetavatest aladest, näiteks eraomanduses oleva eluhoone koridor, mis on vajalik arstikabinetti pääsemiseks, või lennujaam. Selle mõiste alla ei käi küberruum, sest see ei ole füüsiline ruum. See, kas konkreetne ruum on avalikult juurdepääsetav, tuleks siiski otsustada igal üksikjuhul eraldi, võttes arvesse vaadeldava olukorra iseärasusi.

(10) Selleks et tagada võrdsed tingimused ning üksikisikute õiguste ja vabaduste tulemuslik kaitse kogu liidus, tuleks käesoleva määrusega kehtestatud õigusnorme kohaldada tehisintellektisüsteemide pakkujate suhtes, diskrimineerimata pakkujaid selle põhjal, kas nad tegutsevad liidus või mõnes kolmandas riigis, ja liidus tegutsevate tehisintellektisüsteemide kasutajate suhtes.

(11) Arvestades tehisintellektisüsteemide digitaalset olemust, peaksid teatavad tehisintellektisüsteemid kuuluma käesoleva määruse kohaldamisalasse isegi siis, kui neid ei ole liidus turule lastud ega kasutusele võetud ja kui neid liidus ei kasutata. See kehtib näiteks siis, kui tegemist on liidus tegutseva operaatoriga, kes sõlmib väljaspool liitu tegutseva operaatoriga lepingu teatavate teenuste kohta, mis on seotud sellise tehisintellektisüsteemi teostatava tegevusega, mis kvalifitseeruks suure riskiga tehisintellektisüsteemiks. Sellisel juhul võib väljaspool liitu asuva operaatori kasutatav tehisintellektisüsteem töödelda andmeid, mis on seaduslikult liidus kogutud ja mida liidust edastatakse, ning anda liidus asuvale lepingu sõlminud operaatorile väljundi, mille see tehisintellektisüsteem kõnealuse töötlemise tulemusena genereeris, ilma et see tehisintellektisüsteem oleks liidus turule lastud, kasutusele võetud või kasutatav. Et hoida ära käesoleva määruse sätetest kõrvalehoidmist ja tagada liidus asuvate füüsiliste isikute tulemuslik kaitse, tuleks käesolevat määrust kohaldada ka tehisintellektisüsteemide kolmandas riigis tegutsevate pakkujate ja kasutajate suhtes niivõrd, kuivõrd nende süsteemide genereeritud väljundit kasutatakse liidus. Võtmaks siiski arvesse olemasolevaid kokkuleppeid ja erivajadusi, mis puudutavad tulevast koostööd välispartneritega, kellega vahetatakse teavet ja tõendeid, ei tuleks käesolevat määrust kohaldada kolmanda riigi ametiasutuste ja rahvusvaheliste organisatsioonide suhtes, kui tegutsetakse selliste rahvusvaheliste lepingute alusel, mis on riigi või Euroopa tasandil sõlmitud liidu või selle liikmesriikidega tehtava õiguskaitse- ja õigusalase koostöö kohta. Selliseid lepinguid on sõlmitud kahepoolselt liikmesriikide ja kolmandate riikide vahel, aga ka Euroopa Liidu, Europoli ja muude ELi asutuste ning kolmandate riikide ja rahvusvaheliste organisatsioonide vahel. Vastuvõtjatest liikmesriikide ametiasutused ning liidu institutsioonid, organid ja asutused ning selliseid väljundeid liidus kasutavad asutused vastutavad selle eest, et nende kasutamine oleks kooskõlas liidu õigusega. Kui kõnealused rahvusvahelised lepingud vaadatakse läbi või sõlmitakse tulevikus uusi, peaksid lepinguosalised tegema kõik endast oleneva, et viia need lepingud vastavusse käesoleva määruse nõuetega.

(12) Käesolevat määrust tuleks kohaldada ka liidu institutsioonide, organite ja asutuste suhtes, kui need tegutsevad tehisintellektisüsteemi pakkuja või kasutajana.

(-12a) Juhul kui ja sel määral mil tehisintellektisüsteeme lastakse turule, võetakse kasutusele või kasutatakse muudetud või muutmata kujul sõjalisel, kaitse- või riikliku julgeoleku eesmärgil, tuleks need käesoleva määruse kohaldamisalast välja jätta, olenemata neid tegevusi teostava üksuse (nt avalik-õiguslik või eraõiguslik üksus) liigist. Sõjalisel ja kaitse-eesmärgil on selline väljajätmine põhjendatud nii ELi lepingu artikli 4 lõikega 2 kui ka ELi lepingu V jaotise 2. peatükiga hõlmatud liikmesriikide ja ühise liidu kaitsepoliitika eripäradega, mille suhtes kohaldatakse rahvusvahelist avalikku õigust ning mis on seega sobivam õigusraamistik, et reguleerida tehisintellektisüsteeme surmava jõu kasutamise kontekstis ja muid tehisintellektisüsteeme sõjalise ja kaitsetegevuse kontekstis. Mis puudutab riigi julgeolekuga seotud eesmärke, siis on väljajätmine põhjendatud nii asjaoluga, et riigi julgeolek kuulub ELi lepingu artikli 4 lõike 2 kohaselt jätkuvalt liikmesriikide ainuvastutusse, kui ka riikliku julgeolekualase tegevuse eripära ja operatiivvajadustega ning selle tegevuse suhtes kohaldatavate konkreetsete siseriiklike õigusnormidega. Kui aga sõjalisel, kaitse- või riikliku julgeoleku eesmärgil välja töötatud, turule lastud, kasutusele võetud või kasutatavat tehisintellektisüsteemi kasutatakse ajutiselt või alaliselt muudel eesmärkidel (näiteks tsiviil- või humanitaareesmärkidel, õiguskaitse või avaliku julgeoleku eesmärgil), kuulub selline süsteem käesoleva määruse kohaldamisalasse. Sellisel juhul peaks üksus, kes kasutab süsteemi muul kui sõjalisel, kaitse- või riikliku julgeoleku eesmärgil, tagama süsteemi vastavuse käesolevale määrusele, välja arvatud juhul, kui süsteemi vastavus on juba tagatud. Tehisintellektisüsteemid, mis on turule lastud või kasutusele võetud määruse kohaldamisalast välja jäetud eesmärgil (st sõjaline, kaitse- või riikliku julgeoleku eesmärk) ja ühel või mitmel määruse kohaldamisalasse kuuluval eesmärgil (nt tsiviileesmärgid, õiguskaitse jne), kuuluvad käesoleva määruse kohaldamisalasse ning nende süsteemide pakkujad peaksid tagama vastavuse käesolevale määrusele. Sellistel juhtudel ei tohiks asjaolu, et tehisintellektisüsteem võib kuuluda käesoleva määruse kohaldamisalasse, mõjutada riikliku julgeoleku, kaitse- ja sõjalise tegevusega tegelevate üksuste – olenemata seda tegevust teostava üksuse liigist – võimalust kasutada tehisintellektisüsteeme riikliku julgeoleku, sõjalisel ja kaitseotstarbel, mis on käesoleva määruse kohaldamisalast välja jäetud. Tsiviil- või õiguskaitse eesmärkidel turule lastud tehisintellektisüsteem, mida kasutatakse muudetud või muutmata kujul sõjalisel, kaitse- või riikliku julgeoleku eesmärgil, ei peaks kuuluma käesoleva määruse kohaldamisalasse, olenemata seda tegevust teostava üksuse liigist.

(12a) Käesolev määrus ei tohiks mõjutada Euroopa Parlamendi ja nõukogu direktiivi 2000/31/EÜ vahendajatest teenuseosutajate vastutust käsitlevate sätete [asendatakse digiteenuste õigusakti vastavate sätetega] kohaldamist.

(12b) Käesolev määrus ei tohiks kahjustada teadus- ja arendustegevust ning selles tuleks austada teadusvabadust. Seepärast on vaja jätta selle kohaldamisalast välja tehisintellektisüsteemid, mis on spetsiaalselt välja töötatud ja kasutusele võetud üksnes teadusliku uurimis- ja arendustegevuse eesmärgil, ning tagada, et määrus ei mõjuta muul viisil tehisintellektisüsteemidega seotud teadus- ja arendustegevust. Käesoleva määruse sätteid ei tuleks kohaldada ka pakkujate tootealase teadustegevuse suhtes. See ei piira käesoleva määruse järgimise kohustust, kui sellise teadus- ja arendustegevuse tulemusena lastakse turule või võetakse kasutusele käesoleva määruse kohaldamisalasse kuuluv tehisintellektisüsteem, ega regulatsiooni testkeskkondade ja tegelikes tingimustes katsetamise sätete kohaldamist. Käesoleva määruse kohaldamisalasse peaksid jääma kõik muud tehisintellektisüsteemid, mida võidakse kasutada mis tahes teadus- ja arendustegevuseks, ilma et see piiraks eespool nimetatut seoses tehisintellektisüsteemidega, mis on spetsiaalselt välja töötatud ja kasutusele võetud üksnes teadusliku uurimis- ja arendustegevuse eesmärgil. Teadus- ja arendustegevus peaks igal juhul toimuma kooskõlas teadusuuringute tunnustatud eetiliste ja kutsestandarditega.

(12c) Võttes arvesse tehisintellektisüsteemide väärtusahela laadi ja keerukust, on oluline selgitada nende osalejate rolli, kes võivad aidata kaasa tehisintellektisüsteemide, eeskätt suure riskiga tehisintellektisüsteemide arendamisele. Eelkõige on vaja selgitada, et üldotstarbelised tehisintellektisüsteemid on pakkuja poolt mõeldud täitma üldkohaldatavaid funktsioone, nagu kujutise või kõne tuvastus, ja on kasutatavad mitmesugustes kontekstides. Neid võib kasutada eraldi suure riskiga tehisintellektisüsteemidena või muude suure riskiga tehisintellektisüsteemide komponentidena. Seepärast tuleks selliste süsteemide suhtes nende eripära tõttu ja selleks, et tagada vastutuse õiglane jagamine tehisintellekti väärtusahelas, kohaldada käesoleva määruse alusel proportsionaalseid ja konkreetsemaid nõudeid ja kohustusi, tagades samal ajal põhiõiguste, tervise ja ohutuse kõrgetasemelise kaitse. Samuti peaksid üldotstarbeliste tehisintellektisüsteemide pakkujad, olenemata sellest, kas teised pakkujad võivad neid kasutada eraldi suure riskiga tehisintellektisüsteemidena või suure riskiga tehisintellektisüsteemide komponentidena, tegema asjakohasel juhul koostööd vastavate suure riskiga tehisintellektisüsteemide pakkujatega, et võimaldada neil täita käesolevast määrusest tulenevaid asjakohaseid kohustusi, ja käesoleva määruse alusel loodud pädevate asutustega. Selleks et võtta arvesse üldotstarbeliste tehisintellektisüsteemide eripära ning kiiresti arenevat turgu ja tehnoloogia arengut selles valdkonnas, tuleks komisjonile anda rakendamisvolitused, et täpsustada ja kohandada käesoleva määruse alusel kehtestatud nõuete kohaldamist üldotstarbeliste tehisintellektisüsteemide suhtes ning täpsustada teavet, mida üldotstarbeliste tehisintellektisüsteemide pakkujad peavad jagama, et vastava suure riskiga tehisintellektisüsteemi pakkujad saaksid täita käesolevast määrusest tulenevaid kohustusi.

(13) Selleks et tagada järjekindel ja kõrgetasemeline avalike huvide kaitse tervishoiu, ohutuse ja põhiõiguste vallas, tuleks kõigi suure riskiga tehisintellektisüsteemide jaoks kehtestada ühised normatiivsed standardid. Need standardid peaksid olema kooskõlas Euroopa Liidu põhiõiguste hartaga (edaspidi „põhiõiguste harta“) ning ühtlasi peaksid need olema mittediskrimineerivad ja kooskõlas liidu rahvusvaheliste kaubanduskohustustega.

(14) Selleks et kehtestada tehisintellektisüsteemide suhtes proportsionaalsed, mõjusad ja siduvad õigusnormid, tuleks järgida selgelt määratletud riskipõhist lähenemisviisi. Sellise lähenemisviisi kohaselt tuleks nende õigusnormide liiki ja sisu kujundada vastavalt tehisintellektisüsteemide põhjustatavate riskide intensiivsusele ja ulatusele. Seepärast tuleb keelata teatavad tehisintellektisüsteemide kasutusviisid, näha ette suure riskiga tehisintellektisüsteemide suhtes kohaldatavad nõuded ja asjaomaste operaatorite kohustused ning kehtestada teatavate tehisintellektisüsteemide puhul läbipaistvuskohustused.

(15) Lisaks sellele, et tehisintellektil on mitmeid kasulikke rakendusvõimalusi, on seda tehnoloogiat võimalik ka kurjasti kasutada ning luua uudseid ja võimsaid manipuleerimise, ärakasutamise ja sotsiaalse kontrolli vahendeid. Sellised kasutusviisid on eriti kahjulikud ning tuleks ära keelata, sest need on vastuolus selliste liidu väärtustega nagu inimväärikuse austamine, vabadust, võrdsus, demokraatia ja õigusriik ning liidu põhiõigustega, kaasa arvatud õigusega mittediskrimineerimisele, andmekaitsele ja privaatsusele, aga ka lapse õigustega.

(16) Tehisintellektil põhinevaid manipuleerimistehnikaid saab kasutada selleks, et veenda isikuid käituma soovimatult ja neid petta, suunates neid tegema otsuseid, mis pärsivad ja kahjustavad nende sõltumatust, otsuste tegemist ja valikuvabadust. Teatavad tehisintellektisüsteemid, mis moonutavad olulisel viisil inimeste käitumist ja millega võib tõenäoliselt põhjustada füüsilist või psühholoogilist kahju, on eriti ohtlikud ja seetõttu tuleks nende turule laskmine, kasutusele võtmine ja kasutamine keelata. Sellistes tehisintellektisüsteemides kasutatakse alalävisele tajule suunatud elemente, nagu audio-, pildi- ja videostiimuleid, mida inimesed ei suuda tajuda, sest need stiimulid jäävad inimese tajust väljapoole, või muid alalävisele tajule suunatud võtted, mis vähendavad või kahjustavad isiku sõltumatust, otsuste tegemist või vaba valikut viisil, millest inimesed ei ole teadlikud, või isegi kui nad on teadlikud, ei ole nad võimelised seda kontrollima või sellele vastu seisma, näiteks aju ja arvuti vaheliste liideste või virtuaalreaalsuse korral. Lisaks võivad tehisintellektisüsteemid muul viisil kasutada ära konkreetse isikute rühma haavatavusi, mis tulenevad nende vanusest, puudest direktiivi (EL) 2019/882 tähenduses või konkreetsest sotsiaalsest või majanduslikust olukorrast, mis tõenäoliselt muudab need isikud ärakasutamise suhtes haavatavamaks, näiteks äärmises vaesuses elavad isikud, etnilised või usuvähemused. Selliseid süsteeme võidakse turule lasta, kasutusele võtta või kasutada selliselt, et nende eesmärk või tagajärg on isiku käitumise oluline moonutamine viisil, mis kahjustab või mõistliku tõenäosusega kahjustab füüsiliselt või psühholoogiliselt seda või mõnd teist isikut või isikute rühma, sealhulgas kahjustamine, mis võib tekkida aja jooksul. Käitumise moonutamise kavatsust ei saa eeldada, kui moonutus tuleneb tehisintellektisüsteemi välistest teguritest, mis ei ole pakkuja või kasutaja kontrolli all, mis tähendab tegureid, mida tehisintellektisüsteemi pakkuja või kasutaja ei pruugi mõistlikult ette näha ega leevendada. Igal juhul ei pruugi pakkujal või kasutajal olla kavatsust põhjustada füüsilist või psühholoogilist kahju, kui selline kahju tuleneb manipuleerivatest või ekspluateerivatest tehisintellektil põhinevatest tavadest. Sellised tehisintellekti kasutusviise käsitlevad keelud täiendavad direktiivi 2005/29/EÜ sätteid, eelkõige seda, et ebaausad kaubandustavad, mis põhjustavad tarbijatele majanduslikku või rahalist kahju, on igal juhul keelatud, olenemata sellest, kas need on kehtestatud tehisintellektisüsteemide kaudu või muul viisil. Käesolevas määruses sätestatud manipuleerivate ja ekspluateerivate tavade keeld ei tohiks mõjutada õiguspärast ravi, näiteks psüühikahäire psühholoogiline ravi või füüsiline rehabilitatsioon, kui see toimub kooskõlas kohaldatavate meditsiinistandardite ja -õigusaktidega. Samuti ei tohiks tavapäraseid ja õiguspäraseid kaubandustavasid, mis on kooskõlas kohaldatava õigusega, pidada iseenesest kahjulikeks manipuleerivateks tehisintellektiga seotud tavadeks.

(17) Tehisintellektisüsteemid, mida kasutatakse avalike võimude või erasektori osalejate poolt füüsiliste isikute sotsiaalseks hindamiseks, võivad tuua kaasa diskrimineerimise ja teatavate rühmade kõrvalejätmise. Need süsteemid võivad rikkuda õigust väärikusele ja mittediskrimineerimisele ning olla vastuolus võrdsuse ja õigluse väärtustega. Sellised tehisintellektisüsteemid hindavad või liigitavad füüsilisi isikuid, tuginedes nende sotsiaalsele käitumisele eri kontekstides või prognoositud isiku- või iseloomuomadustele. Selliste tehisintellektisüsteemide antud sotsiaalne hinne võib tuua kaasa füüsilisi isikuid või terveid inimrühmi kahjustavat või nende suhtes ebasoodsat kohtlemist sotsiaalses kontekstis, mis ei ole seotud kontekstiga, kus andmed algselt genereeriti või koguti, või kahjustavat kohtlemist, mis ei ole nende sotsiaalse käitumise problemaatilisusega võrreldes proportsionaalne või põhjendatud. Selliseid vastuvõetamatuid hinnangu andmisi sisaldavad tehisintellektisüsteemid tuleks seetõttu keelata. See keeld ei tohiks mõjutada füüsiliste isikute seaduslikku hindamist, mida tehakse ühel või mitmel konkreetsel eesmärgil kooskõlas seadusega.

(18) Tehisintellektisüsteemide kasutamist avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil reaalajas toimuva füüsiliste isikute biomeetrilise kaugtuvastamise jaoks peetakse eriti tõsiseks sekkumiseks asjaomaste isikute õigustesse ja vabadustesse, sest see võib mõjutada suure osa elanikkonna eraelu, tekitada pideva jälgimise tunde ning kaudselt veenda loobuma kogunemisvabaduse ja muude põhiõiguste kasutamisest. Kuna selliste reaalajas töötavate süsteemide kasutamise mõju on vahetu ja täiendava kontrolli või parandamise võimalused piiratud, seab selliste süsteemide kasutamine suuremasse ohtu õiguskaitsetoimingute mõjuvälja jäävate isikute õigused ja vabadused.

(19) Seepärast peaks selliste süsteemide kasutamine õiguskaitse eesmärgil olema keelatud, välja arvatud ammendavalt loetletud ja kitsalt määratletud olukordades, kus nende süsteemide kasutamine on rangelt vajalik selleks, et saavutada olulise avaliku huvi eesmärk, mille tähtsus kaalub riskid üles. Selliste olukordade hulka kuuluvad võimalike kuriteoohvrite, kaasa arvatud kadunud laste otsimine, teatavad füüsiliste isikute elu või füüsilist turvalisust ähvardavad ohud või terrorirünnaku oht ning nõukogu raamotsuses 2002/584/JSK[9] osutatud kuritegude toimepanijate või sellistes kuritegudes kahtlustatavate avastamine, nende asukohta kindlaks tegemine, nende tuvastamine või neile süüdistuse esitamine, kui sellise kuriteo eest karistatakse asjaomases liikmesriigis vabadusekaotuse või vabadust piirava julgeolekumeetmega, mille maksimaalne pikkus on vähemalt kolm aastat, nagu selle liikmesriigi õigusaktides kindlaks määratud. Sellise ajalise piiri seadmine siseriikliku õiguse kohasele vabadusekaotusele või vabadust piiravale julgeolekumeetmele aitab tagada, et reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine oleks õigustatud vaid piisavalt tõsiste rikkumiste korral. Peale selle on nõukogu raamotsuses 2002/584/JSK loetletud 32 kuriteost mõned praktikas tõenäoliselt teistest asjakohasemad, sest reaalajas toimuva biomeetrilise kaugtuvastamise kasutamise eeldatav vajalikkus ja proportsionaalsus varieeruvad märkimisväärselt, kui tegemist on loetelus nimetatud kuriteo toimepanija või sellises kuriteos kahtlustatava reaalse avastamise, tema asukoha kindlaks tegemise, tema tuvastamise või talle süüdistuse esitamisega ja kui võetakse arvesse võimalike negatiivsete tagajärgede raskusastme, tõenäosuse ja ulatuse tõenäolisi erinevusi. Lisaks tuleks käesoleva määrusega säilitada õiguskaitse-, piirivalve-, rände- ja varjupaigaasutuste suutlikkus kontrollida isikusamasust asjaomase isiku juuresolekul vastavalt liidu ja liikmesriigi õiguses sellise kontrolli jaoks sätestatud tingimustele. Eelkõige peaks õiguskaitse-, piirivalve-, rände- ja varjupaigaasutustel olema võimalik kasutada liidu või liikmesriigi õiguse kohaselt infosüsteeme, et tuvastada isik, kes isikusamasuse kontrolli käigus kas keeldub isiku tuvastamisest või ei suuda oma isikut avaldada või tõendada, ilma et neilt nõutaks käesoleva määruse kohaselt eelneva loa taotlemist. Tegemist võib olla näiteks kuriteoga seotud isikuga, isikuga, kes ei soovi või kes õnnetuse või tervisliku seisundi tõttu ei suuda avaldada oma isikut õiguskaitseasutustele.

[9] Nõukogu 13. juuni 2002. aasta raamotsus 2002/584/JSK Euroopa vahistamismääruse ja liikmesriikidevahelise üleandmiskorra kohta (EÜT L 190, 18.7.2002, lk 1).

(20) Lisaks sellele on nende süsteemide vastutustundliku ja proportsionaalse kasutamise tagamiseks oluline panna paika, et kõigi kõnealuste ammendavalt loetletud ja kitsalt määratletud olukordade puhul tuleks arvesse võtta teatavaid elemente, eeskätt mis puudutab taotluse aluseks oleva olukorra olemust ja kasutamise tagajärgi seoses kõigi asjaomaste isikute õiguste ja vabadustega, ning kasutamise korral ettenähtud kaitsemeetmeid ja tingimusi. Peale selle peaks reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil olema ajas ja ruumis asjakohaselt piiratud, võttes eelkõige arvesse tõendeid või viiteid ohu, ohvrite või toimepanija kohta. Isikute võrdlusandmebaas peaks olema kõigi eespool nimetatud olukordade puhul iga kasutusmalli jaoks sobiv.

(21) Iga kord, kui reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutatakse avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil, peaks selleks olema liikmesriigi õigusasutuse või sõltumatu haldusasutuse selge ja konkreetne luba. Põhimõtteliselt tuleks selline luba saada enne süsteemi kasutamist isiku või isikute tuvastamiseks. Erandeid sellest reeglist tuleks lubada nõuetekohaselt põhjendatud kiireloomulistes olukordades, see tähendab olukordades, kus vajadus kõnealuste süsteemide kasutamise järele on selline, et enne kasutamise algust ei ole reaalselt ega objektiivselt võimalik luba saada. Selliste kiireloomuliste juhtumite korral peaks kasutamine piirduma hädavajaliku miinimumiga ning selle suhtes peaksid kehtima asjakohased kaitsemeetmed ja tingimused, mis on kindlaks määratud siseriiklikus õiguses ja mida õiguskaitseasutus iga individuaalse kiireloomulise kasutusjuhtumi korral täpsustab. Lisaks sellele peaks õiguskaitseasutus sellistel juhtudel püüdma saada loa nii pea kui võimalik ja põhjendama, miks ta ei saanud luba varem taotleda.

(22) Ühtlasi on käesoleva määrusega kehtestatavas ammendavas raamistikus otstarbekas ette näha, et selline kasutamine liikmesriigi territooriumil kooskõlas käesoleva määrusega peaks olema võimalik üksnes siis ja niivõrd, kuivõrd kõnealune liikmesriik on otsustanud oma siseriikliku õiguse üksikasjalikes õigusnormides selgelt sätestada võimaluse sellist kasutamist lubada. Seega jääb liikmesriikidele käesoleva määruse alusel vabadus sellist võimalust üldse mitte ette näha või näha selline võimalus ette üksnes mõne eesmärgi jaoks, mille puhul on käesolevas määruses kirjeldatud lubatud kasutamine õigustatud.

(23) Tehisintellektisüsteemide kasutamine avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil reaalajas toimuva füüsiliste isikute biomeetrilise kaugtuvastamise jaoks eeldab igal juhul biomeetriliste andmete töötlemist. Käesoleva määruse sätted, millega keelatakse selline kasutamine teatavate eranditega ja mis põhinevad ELi toimimise lepingu artiklil 16, peaksid direktiivi (EL) 2016/680 artiklis 10 sätestatud biomeetriliste andmete töötlemist käsitlevate õigusnormide suhtes kehtima erinormina (*lex specialis*), nii et selline kasutamine ja sellega kaasnev biomeetriliste andmete töötlemine oleksid ammendavalt reguleeritud. Seega peaks selline kasutamine ja töötlemine olema võimalik üksnes siis, kui see on kooskõlas käesoleva määrusega kehtestatud raamistikuga, ning väljaspool seda raamistikku ei tohiks pädevatel asutustel olla võimalik õiguskaitse eesmärgil tegutsedes kasutada selliseid süsteeme ja töödelda sellega seoses selliseid andmeid direktiivi (EL) 2016/680 artiklis 10 loetletud põhjustel. Seoses sellega ei ole käesoleva määruse eesmärk anda õiguslikku alust isikuandmete töötlemiseks direktiivi 2016/680 artikli 8 alusel. Käesoleva määrusega loodud eriraamistik, mis käsitleb sellist kasutamist õiguskaitse eesmärgil, ei peaks siiski hõlmama reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamist avalikult juurdepääsetavas ruumis muul otstarbel kui õiguskaitse eesmärgil, ka siis, kui seda teevad pädevad asutused. Seega ei peaks selliseks kasutamise suhtes muul otstarbel kui õiguskaitse eesmärgil kehtima käesoleva määruse kohase loa nõue ega selle jõustamiseks kohaldatavad üksikasjalikud siseriiklikud õigusnormid.

(24) Igasugune biomeetriliste ja muude isikuandmete töötlemine, mis on seotud tehisintellektisüsteemide kasutamisega biomeetrilise tuvastamise jaoks, välja arvatud juhul, kui see toimub seoses käesoleva määrusega reguleeritud reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamisega avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil, peaks ka edaspidi vastama kõigile direktiivi (EL) 2016/680 artiklist 10 tulenevatele nõuetele. Muul otstarbel kui õiguskaitse eesmärgil kasutamise puhul on määruse (EL) 2016/679 artikli 9 lõike 1 ja määruse (EL) 2018/1725 artikli 10 lõikega 1 keelatud töödelda füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid, välja arvatud kõnealuste artiklite lõikes 2 kirjeldatud olukordades.

(25) ELi lepingule ja ELi toimimise lepingule lisatud protokolli nr 21 (Ühendkuningriigi ja Iirimaa seisukoha kohta vabadusel, turvalisusel ja õigusel rajaneva ala suhtes) artikli 6a kohaselt ei ole ELi toimimise lepingu artikli 16 põhjal vastu võetud käesoleva määruse artikli 5 lõike 1 punktis d ning lõigetes 2, 3 ja 4 normid füüsiliste isikute kaitse kohta isikuandmete töötlemisel liikmesriikide poolt ELi toimimise lepingu kolmanda osa V jaotise 4. ja 5. peatüki kohaldamisalasse kuuluva tegevuse puhul Iirimaa suhtes siduvad, kui Iirimaa suhtes ei ole siduvad normid, mis käsitlevad õigusalast koostööd kriminaalasjades või politseikoostööd, mille raames tuleb järgida ELi toimimise lepingu artikli 16 alusel kehtestatud sätteid.

(26) ELi lepingule ja ELi toimimise lepingule lisatud protokolli nr 22 (Taani seisukoha kohta) artiklite 2 ja 2a kohaselt ei ole ELi toimimise lepingu artikli 16 põhjal vastu võetud käesoleva määruse artikli 5 lõike 1 punktis d ning lõigetes 2, 3 ja 4 sätestatud normid füüsiliste isikute kaitse kohta isikuandmete töötlemisel liikmesriikide poolt ELi toimimise lepingu kolmanda osa V jaotise 4. ja 5. peatüki kohaldamisalasse kuuluva tegevuse puhul Taani suhtes siduvad ega kohaldatavad.

(27) Suure riskiga tehisintellektisüsteem tuleks liidus turule lasta või kasutusele võtta üksnes siis, kui see vastab teatavatele kohustuslikele nõuetele. Need nõuded peaksid tagama, et liidus kättesaadavad suure riskiga tehisintellektisüsteemid või tehisintellektisüsteemid, mille väljundit kasutatakse liidus muul viisil, ei kujuta endast vastuvõetamatut riski liidu õigusega tunnustatud ja kaitstud liidu oluliste avalike huvide suhtes. Suure riskiga tehisintellektisüsteemideks tuleks pidada üksnes selliseid tehisintellektisüsteeme, millel on liidus oluline kahjulik mõju inimeste tervisele, ohutusele ja põhiõigustele, ning selline piirang minimeerib kõik võimalikud rahvusvahelise kaubanduse piirangud, kui neid peaks olema.

(28) Tehisintellektisüsteemid võivad kahjustada inimeste tervist ja ohutust, eriti juhul, kui sellised süsteemid on toodete komponendid. Kooskõlas liidu ühtlustamisõigusaktide eesmärkidega hõlbustada toodete vaba liikumist siseturul ja tagada, et siseturule saabuvad ainult ohutud ja muul viisil nõuetele vastavad tooted, on oluline tõhusalt ära hoida ja leevendada riske, mille toode kui tervik võib põhjustada oma digitaalsete komponentide, sh tehisintellektisüsteemide tõttu. Näiteks üha autonoomsemad robotid peaksid suutma ohutult töötada ja täita oma ülesandeid keerukates keskkondades, seda nii tootmise kui ka isikliku abi ja hoolduse valdkonnas. Sama moodi peaksid usaldusväärsed ja täpsed olema tervishoiusektoris kasutatavad üha keerulisemad diagnostikasüsteemid ja inimeste otsuseid toetavad süsteemid, sest seal on tegemist elu ja tervise seisukohast eriti oluliste otsustega. Tehisintellektisüsteemi liigitamisel suure riskiga tehisintellektisüsteemiks on eriti oluline see, kui ulatuslik on tehisintellektisüsteemi kahjulik mõju põhiõiguste hartaga kaitstud põhiõigustele. Nende õiguste hulka kuuluvad õigus inimväärikusele, era- ja perekonnaelu austamine, isikuandmete kaitse, väljendus- ja teabevabadus, kogunemis- ja ühinemisvabadus, mittediskrimineerimine, tarbijakaitse, töötajate õigused, puuetega inimeste õigused, õigus tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele, õigus kaitsele, süütuse presumptsioon ja õigus heale haldusele. Lisaks nimetatud õigustele on oluline rõhutada, et lastel on eraldi õigused, mis on sätestatud ELi harta artiklis 24 ja ÜRO lapse õiguste konventsioonis (mida on põhjalikumalt käsitletud ÜRO lapse õiguste komitee üldises märkuses nr 25 digikeskkonna kohta), kusjuures mõlema dokumendi kohaselt tuleb arvesse võtta laste haavatavust ja näha ette nende heaoluks vajalik kaitse ja hoolitsus. Hinnates, kui tõsist kahju võib tehisintellektisüsteem põhjustada, muu hulgas inimeste tervise ja ohutuse vallas, tuleks kaaluda ka põhiõiguste hartas sätestatud ja liidu põhimõtetega rakendatud põhiõigust kõrgetasemelisele keskkonnakaitsele.

(29) Mis puudutab suure riskiga tehisintellektisüsteeme, mis on toodete või süsteemide turvakomponendid või mis on ise tooted või süsteemid, mis kuuluvad Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 300/2008,[10] Euroopa Parlamendi ja nõukogu määruse (EL) nr 167/2013,[11] Euroopa Parlamendi ja nõukogu määruse (EL) nr 168/2013,[12] Euroopa Parlamendi ja nõukogu direktiivi 2014/90/EL,[13] Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/797,[14] Euroopa Parlamendi ja nõukogu määruse (EL) 2018/858,[15] Euroopa Parlamendi ja nõukogu määruse (EU) 2018/1139[16] ning Euroopa Parlamendi ja nõukogu määruse (EL) 2019/2144[17] kohaldamisalasse, siis on otstarbekas muuta kõnealuseid õigusakte tagamaks, et kui komisjon võtab nimetatud õigusaktide põhjal edaspidi vastu asjaomaseid delegeeritud või rakendusakte, võtab ta arvesse käesolevas määruses suure riskiga tehisintellektisüsteemide kohta sätestatud kohustuslikke nõudeid, tuginedes iga sektori tehnilistele ja regulatiivsetele iseärasustele ja ilma, et ta sekkuks nende õigusaktidega kehtestatud olemasolevatesse juhtimis-, vastavushindamis- ja jõustamismehhanismidesse või -asutustesse.

---

10 Euroopa Parlamendi ja nõukogu 11. märtsi 2008. aasta määrus (EÜ) nr 300/2008, mis käsitleb tsiviillennundusjulgestuse ühiseeskirju ja millega tunnistatakse kehtetuks määrus (EÜ) nr 2320/2002 (ELT L 97, 9.4.2008, lk 72).

11 Euroopa Parlamendi ja nõukogu 5. veebruari 2013. aasta määrus (EL) nr 167/2013 põllu- ja metsamajanduses kasutatavate sõidukite kinnituse ja turujärelevalve kohta (ELT L 60, 2.3.2013, lk 1).

12 Euroopa Parlamendi ja nõukogu 15. jaanuari 2013. aasta määrus (EL) nr 168/2013 kahe-, kolme- ja neljarattaliste sõidukite kinnituse ja turujärelevalve kohta (ELT L 60, 2.3.2013, lk 52).

13 Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta direktiiv 2014/90/EL, milles käsitletakse laevavarustust ja millega tunnistatakse kehtetuks nõukogu direktiiv 96/98/EÜ (ELT L 257, 28.8.2014, lk 146).

14 Euroopa Parlamendi ja nõukogu 11. mai 2016. aasta direktiiv (EL) 2016/797 Euroopa Liidu raudteesüsteemi koostalitluse kohta (ELT L 138, 26.5.2016, lk 44).

15 Euroopa Parlamendi ja nõukogu 30. mai 2018. aasta määrus (EL) 2018/858 mootorsõidukite ja mootorsõidukite haagiste ning nende jaoks ette nähtud süsteemide, osade ja eraldi seadmestike tüübikinnituse ja turujärelevalve kohta, ning millega muudetakse määruseid (EÜ) nr 715/2007 ja (EÜ) nr 595/2009 ning tunnistatakse kehtetuks direktiiv 2007/46/EÜ (ELT L 151, 14.6.2018, lk 1).

16 Euroopa Parlamendi ja nõukogu 4. juuli 2018. aasta määrus (EL) 2018/1139, mis käsitleb tsiviillennunduse valdkonna ühisnorme ja millega luuakse Euroopa Liidu Lennundusohutusamet ning millega muudetakse Euroopa Parlamendi ja nõukogu määrusi (EÜ) nr 2111/2005, (EÜ) nr 1008/2008, (EL) nr 996/2010, (EL) nr 376/2014 ja Euroopa Parlamendi ja nõukogu direktiive 2014/30/EL ning 2014/53/EL ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrused (EÜ) nr 552/2004 ja (EÜ) nr 216/2008 ning nõukogu määrus (EMÜ) nr 3922/91 (ELT L 212, 22.8.2018, lk 1).

17 Euroopa Parlamendi ja nõukogu 27. novembri 2019. aasta määrus (EL) 2019/2144, mis käsitleb mootorsõidukite ja nende haagiste ning mootorsõidukite jaoks ette nähtud süsteemide, osade ja eraldi seadmestike tüübikinnituse nõudeid seoses nende üldise ohutuse ning sõitjate ja vähekaitstud liiklejate kaitsega, ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) 2018/858 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrused (EÜ) nr 78/2009, (EÜ) nr 79/2009 ja (EÜ) nr 661/2009 ning komisjoni määrused (EÜ) nr 631/2009, (EL) nr 406/2010, (EL) nr 672/2010, (EL) nr 1003/2010, (EL) nr 1005/2010, (EL) nr 1008/2010, (EL) nr 1009/2010, (EL) nr 19/2011, (EL) nr 109/2011, (EL) nr 458/2011, (EL) nr 65/2012, (EL) nr 130/2012, (EL) nr 347/2012, (EL) nr 351/2012, (EL) nr 1230/2012 ja (EL) 2015/166 (ELT L 325, 16.12.2019, lk 1).

(30) Mis puudutab tehisintellektisüsteeme, mis on toodete turvakomponendid või mis on ise tooted, mis kuuluvad teatavate liidu ühtlustamisõigusaktide kohaldamisalasse, siis on otstarbekas liigitada need tehisintellektisüsteemid käesoleva määruse alusel suure riskiga tehisintellektisüsteemideks, kui nende asjaomaste liidu õigusaktide alusel teeb kõnealuse toote vastavushindamise kolmandast isikust vastavushindamisasutus. Sellised tooted on eeskätt masinad, mänguasjad, liftid, plahvatusohtlikus keskkonnas kasutatavad seadmed ja kaitsesüsteemid, raadioseadmed, surveseadmed, lõbusõidulaevade varustus, köisteed, küttegaasiseadmed, meditsiiniseadmed ja *in vitro* diagnostika meditsiiniseadmed.

(31) See, kui tehisintellektisüsteem liigitatakse käesoleva määruse alusel suure riskiga tehisintellektisüsteemiks, ei peaks ilmtingimata tähendama, et toodet, mille turvakomponent see tehisintellektisüsteem on, või tehisintellektisüsteemi ennast kui toodet peetakse suure riskiga tooteks vastavalt selle toote suhtes kohaldatavate asjaomaste liidu ühtlustamisõigusaktidega kehtestatud kriteeriumidele. Esmajoones puudutab see Euroopa Parlamendi ja nõukogu määrust (EL) 2017/745[18] ja Euroopa Parlamendi ja nõukogu määrust (EL) 2017/746,[19] kui keskmise ja suure riskiga toodete puhul on ette nähtud kolmanda isiku tehtav vastavushindamine.

[18] Euroopa Parlamendi ja nõukogu 5. aprilli 2017. aasta määrus (EL) 2017/745, milles käsitletakse meditsiiniseadmeid, millega muudetakse direktiivi 2001/83/EÜ, määrust (EÜ) nr 178/2002 ja määrust (EÜ) nr 1223/2009 ning millega tunnistatakse kehtetuks nõukogu direktiivid 90/385/EMÜ ja 93/42/EMÜ (ELT L 117, 5.5.2017, lk 1).

[19] Euroopa Parlamendi ja nõukogu 5. aprilli 2017. aasta määrus (EL) 2017/746 in vitro diagnostikameditsiiniseadmete kohta ning millega tunnistatakse kehtetuks direktiiv 98/79/EÜ ja komisjoni otsus 2010/227/EL (ELT L 117, 5.5.2017, lk 176).

(32) Suure riskiga tehisintellektisüsteemid, mis ei ole toodete turvakomponendid või ise tooted, on otstarbekas liigitada suure riskiga tehisintellektisüsteemideks, kui need põhjustavad oma sihtotstarbe tõttu suure riski ja ähvardavad kahjustada inimeste tervist ja ohutust või põhiõigusi, võttes arvesse nii võimaliku kahju tõsidust kui ka selle tekkimise tõenäosust, ja kui neid kasutatakse määruses eelnevalt täpselt kindlaks määratud valdkondades. Nende süsteemide kindlakstegemine põhineb samadel meetoditel ja kriteeriumidel, mida kavatsetakse kasutada suure riskiga tehisintellektisüsteemide loetelu tulevaste võimalike muudatuste jaoks. Lisaks on oluline selgitada, et III lisas osutatud suure riskiga stsenaariumid võivad hõlmata süsteeme, mis ei ohusta märkimisväärselt nende stsenaariumide kohaselt kaitstavaid õiguslikke huve, võttes arvesse tehisintellektisüsteemi väljundit. Seepärast tuleks sellise väljundiga tehisintellektisüsteemi pidada suure riskiga süsteemiks üksnes juhul, kui kõnealune väljund on asjaomase meetme või otsusega seoses väga oluline (st ei ole ainuüksi täiendavat laadi) ning ohustab seega märkimisväärselt kaitstavaid õiguslikke huve. Näiteks kui tehisintellektisüsteemide poolt inimesele esitatav teave seisneb füüsiliste isikute profiilianalüüsis määruse (EL) 2016/679 artikli 4 punkti 4 ja direktiivi (EL) 2016/680 artikli 3 punkti 4 ning määruse (EL) 2018/1725 artikli 3 punkti 5 tähenduses, ei tohiks sellist teavet tavaliselt pidada III lisas osutatud suure riskiga tehisintellektisüsteemide kontekstis täiendavat laadi teabeks. Kui aga tehisintellektisüsteemi väljund on inimtegevuse või -otsuse seisukohast tähtsusetu või väheoluline, võib selle laadi pidada ainuüksi täiendavaks; muu hulgas hõlmab see näiteks tehisintellektisüsteeme, mida kasutatakse tõlkimiseks teavitamise eesmärgil või dokumentide haldamiseks.

(33) Füüsiliste isikute biomeetrilise kaugtuvastamise jaoks mõeldud tehisintellektisüsteemide tehniline ebatäpsus võib kaasa tuua tulemuste kallutatuse ja põhjustada diskrimineerimist. Eriti oluline on see vanuse, etnilise päritolu, rassi, soo või puuete puhul. Seepärast tuleks nii reaalajas kui ka tagantjärele toimuva biomeetrilise kaugtuvastamise süsteemid liigitada suure riskiga süsteemideks. Arvestades, milliseid riske need süsteemid põhjustavad, tuleks mõlemat liiki biomeetrilise kaugtuvastamise süsteemide suhtes kohaldada logimisvõimekuse ja inimjärelevalve erinõudeid.

(34) Elutähtsa taristu juhtimise ja käitamisega seoses on otstarbekas liigitada suure riskiga tehisintellektisüsteemiks need tehisintellektisüsteemid, mis on mõeldud kasutamiseks kriitilise tähtsusega üksuste vastupidavusvõime direktiivi I lisa punktis 8 loetletud elutähtsa digitaristu, maanteeliikluse ning vee, gaasi, kütteenergia ja elektri tarnimise korraldamise ja käitamise turvakomponentidena, sest nende tõrge või talitlushäire võib seada ohtu paljude inimeste elu ja tervise ning põhjustada märgatavaid häireid tavapärases sotsiaalses ja majandustegevuses. Elutähtsa taristu, sealhulgas elutähtsa digitaristu turvakomponendid on süsteemid, mida kasutatakse elutähtsa taristu füüsilise puutumatuse või inimeste tervise ja ohutuse ning vara otseseks kaitsmiseks, kuid mis ei ole süsteemi toimimiseks vajalikud. Selliste komponentide rike või talitlushäire võib otseselt ohustada elutähtsa taristu füüsilist puutumatust ning võib seega kujutada ohtu inimeste tervisele ja ohutusele ning varale. Üksnes küberturvalisuse tagamiseks mõeldud komponente ei tohiks käsitada turvakomponentidena. Sellise elutähtsa taristu turvakomponendid on näiteks veesurve seiresüsteemid ja tulekahjuhäire juhtimissüsteemid pilvandmetöötluse keskustes.

(35) Suure riskiga süsteemidena tuleks käsitada tehisintellektisüsteeme, mida kasutatakse hariduses või kutseõppes eelkõige selleks, et määrata kindlaks isikute juurdepääs kõikide tasemete haridus- ja kutseõppeasutustele või -programmidele, teha otsuseid nende vastuvõtmise kohta või määrata isikuid õppekohtadele või hinnata isikute õpiväljundeid, sest need süsteemid võivad ära määrata inimeste haridusliku ja kutsealase käekäigu ning mõjutada seega nende toimetulekut. Kui sellised süsteemid ei ole korralikult projekteeritud või kui neid ei kasutata korralikult, võivad need rikkuda õigust haridusele ja koolitusele, aga ka õigust mitte olla diskrimineeritud, ning põlistada aegade jooksul välja kujunenud diskrimineerimismustreid.

(36) Suure riskiga tehisintellektisüsteemideks tuleks liigitada ka tehisintellektisüsteemid, mida kasutatakse tööhõive, töötajate juhtimise ja füüsilisest isikust ettevõtjana tegutsemise võimaluste valdkonnas, eeskätt inimeste töölevõtmiseks ja valikuks, edutamise ja töösuhte lõpetamise otsuste tegemiseks ning ülesannete jagamiseks isiku käitumise või isikuomaduste või erijoonte põhjal, seire või inimeste hindamise jaoks tööga seotud lepingulistes suhete kontekstis, sest need süsteemid võivad märkimisväärselt mõjutada nende isikute tulevasi karjääriväljavaateid ja toimetulekut. Asjaomased tööga seotud lepingulised suhted peaksid käima ka selliste töötajate ja isikute kohta, kes osutavad teenuseid platvormide kaudu, nagu on nimetatud komisjoni 2021. aasta tööprogrammis. Põhimõtteliselt ei tuleks selliseid isikuid käsitada kasutajatena käesoleva määruse tähenduses. Värbamisprotsessi käigus ning isikute hindamisel, edutamisel ja ametisse jäämisel tööga seotud lepinguliste suhete kontekstis võivad sellised süsteemid põlistada aegade jooksul välja kujunenud diskrimineerimismustreid, mis on suunatud näiteks naiste, teatavate vanuserühmade, puuetega inimeste või teatava rassilise või etnilise päritolu või seksuaalse sättumusega isikute vastu. Tehisintellektisüsteemid, mida kasutatakse nende isikute töötulemuste ja käitumise seireks, võivad mõjutada ka nende õigust andmekaitsele ja privaatsusele.

(37) Veel üks valdkond, milles tuleks tehisintellektisüsteemide kasutamisele erilist tähelepanu pöörata, on teatavate selliste oluliste era- ja avalik-õiguslike teenuste ja hüvede juurdepääsetavus ja kasutamine, mida inimesed vajavad, et ühiskonnas täielikult osaleda või oma elatustaset parandada. Eeskätt tuleks suure riskiga tehisintellektisüsteemideks liigitada tehisintellektisüsteemid, mida kasutatakse füüsilistele isikutele krediidihinnangu andmiseks või nende krediidivõimelisuse hindamiseks, sest need panevad paika inimese juurdepääsu finantsvahenditele või olulistele teenustele, nagu kinnisvara, elekter ja telekommunikatsiooniteenused. Sel otstarbel kasutatavad tehisintellektisüsteemid võivad põhjustada inimeste või rühmade diskrimineerimist ja põlistada aegade jooksul välja kujunenud diskrimineerimismustreid, mille aluseks on näiteks rassiline või etniline päritolu, puuded, vanus, seksuaalne sättumus, või avaldada uut liiki diskrimineerivat mõju. Arvestades mõju väga piiratud ulatust ja turul kättesaadavaid alternatiive, on otstarbekas teha erand tehisintellektisüsteemidele, mille eesmärk on krediidivõimelisuse hindamine ja krediidihindamine, kui sellised süsteemid võtavad oma tarbeks kasutusele mikro- või väikesed ettevõtjad, nagu need on määratletud komisjoni soovituse 2003/361/EÜ lisas. Füüsilised isikud, kes taotlevad või saavad avaliku sektori asutustelt hädavajalikke sotsiaaltoetusi ja -teenuseid, sõltuvad tavaliselt nendest toetustest ja teenustest ning on vastutavate asutustega võrreldes haavatavas olukorras. Kui tehisintellektisüsteeme kasutatakse selleks, et teha kindlaks, kas ametiasutus peaks sellise toetuse andmisest või teenuse osutamisest keelduma, seda vähendama, selle tühistama või tagasi nõudma, sealhulgas selleks, et teha kindlaks, kas abisaajatel on sellistele toetustele või teenustele seaduslik õigus, võib neil süsteemidel olla märkimisväärne mõju inimese toimetulekule ning need süsteemid võivad rikkuda inimeste põhiõigusi, näiteks õigust sotsiaalkaitsele, mittediskrimineerimisele, inimväärikusele või tõhusale õiguskaitsevahendile. Seepärast tuleks need süsteemid liigitada suure riskiga tehisintellektisüsteemideks. Samas ei tohiks käesolev määrus takistada uuenduslike lähenemisviiside väljatöötamist ja kasutamist avalikus halduses, kus oleks nõuetekohaste ja ohutute tehisintellektisüsteemide laialdasemast kasutamisest rohkelt kasu tingimusel, et need süsteemid ei põhjusta juriidilistele ja füüsilistele isikutele suuri riske. Lisaks eelnimetatule tuleks suure riskiga tehisintellektisüsteemideks liigitada ka tehisintellektisüsteemid, mida kasutatakse kiirabi ja päästeteenistuse väljasaatmiseks ja väljakutsete prioriseerimiseks, sest need teevad otsuseid olukordades, mis on inimeste elu, tervise ja vara seisukohast väga kriitilised. Tehisintellektisüsteeme kasutatakse üha enam ka füüsiliste isikutega seotud riskihindamiseks ning hinnakujunduseks elu- ja tervisekindlustuses, mis võib, kui selle kavandamine, arendamine ja kasutamine ei ole nõuetekohane, põhjustada tõsiseid tagajärgi inimeste elule ja tervisele, sealhulgas majanduslikku tõrjutust ja diskrimineerimist. Selleks et tagada finantsteenuste sektoris ühtne lähenemisviis, tuleks kohaldada eespool nimetatud erandit mikro- või väikeste ettevõtjate poolt oma tarbeks kasutatavate süsteemide suhtes niivõrd, kuivõrd nad ise pakuvad tehisintellektisüsteemi ja võtavad selle kasutusele oma kindlustustoodete müümiseks.

(38) Õiguskaitseasutuste toiminguid, millega kaasneb tehisintellektisüsteemide teatav kasutamine, iseloomustab võimu väga ebavõrdne jaotumine ja nende tulemuseks võib olla jälgimine, arreteerimine või füüsilise isiku vabaduse võtmine, aga ka muu kahjulik mõju põhiõiguste hartaga tagatud põhiõigustele. Tehisintellektisüsteem võib olla inimeste valikul diskrimineeriv või muul moel ebatäpne või ebaõiglane, eriti juhul, kui selle treenimiseks ei ole kasutatud kvaliteetseid andmeid, kui süsteemi täpsus või stabiilsus ei ole piisavad või kui seda ei ole enne turule laskmist või muul moel kasutusele võtmist korralikult projekteeritud ja testitud. Kahjustatud võib saada ka võimalus kasutada selliseid olulisi menetluslikke põhiõigusi, nagu õigus tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele, õigus kaitsele ja süütuse presumptsioon, seda eriti juhul, kui sellised tehisintellektisüsteemid ei ole piisavalt läbipaistvad, selgitatavad ja dokumenteeritud. Seepärast on asjakohane liigitada suure riskiga tehisintellektisüsteemiks hulk tehisintellektisüsteeme, mis on mõeldud kasutamiseks õiguskaitses, kus täpsus, usaldusväärsus ja läbipaistvus on eriti olulised, et hoida ära kahjulikku mõju, säilitada üldsuse usaldus ning tagada aruandekohustus ja tõhus õiguskaitse. Arvestades kõnealuste toimingute olemust ja nendega seotud riske, peaksid selliste suure riskiga tehisintellektisüsteemide hulka kuuluma eeskätt need tehisintellektisüsteemid, mis on mõeldud õiguskaitseasutustele kasutamiseks individuaalsete riskihindamiste, valedetektorite ja samalaadsete vahendite jaoks või füüsilise isiku emotsionaalse seisundi tuvastamiseks, tõendite usaldusväärsuse hindamiseks kriminaalmenetluses, tegeliku või potentsiaalse kuriteo esinemise või kordumise prognoosimiseks füüsiliste isikute profiilianalüüsi põhjal või füüsiliste isikute või rühmade isikuomaduste, erijoonte või varasema kuritegeliku käitumise hindamiseks ning kuritegude avastamise, uurimise või nende eest vastutusele võtmise käigus tehtavaks profiilianalüüsiks. Tehisintellektisüsteeme, mis on mõeldud kasutamiseks spetsiaalselt maksu- ja tolliasutustele haldusmenetlustes ning rahapesu andmebüroodele, kes täidavad liidu rahapesuvastaste õigusaktide kohaseid teabe analüüsimises seisnevaid haldusülesandeid, ei tuleks käsitada suure riskiga tehisintellektisüsteemidena, mida õiguskaitseasutused kasutavad süütegude tõkestamise, avastamise, uurimise ja nende eest vastutusele võtmise eesmärgil.

(39) Rände-, varjupaiga- ja piirkontrollihalduses kasutatavad tehisintellektisüsteemid mõjutavad inimesi, kes on tihtipeale eriti haavatavas olukorras ja sõltuvad pädevate asutuste tegevuse tulemustest. Seepärast on sellises kontekstis kasutatavate tehisintellektisüsteemide täpsus, mittediskrimineeriv olemus ja läbipaistvus eriti oluline, et tagada mõjutatud isikute põhiõiguste austamine, eeskätt nende õigus vabale liikumisele, mittediskrimineerimisele, eraelu ja isikuandmete kaitsele, rahvusvahelisele kaitsele ja heale haldusele. Seepärast on otstarbekas liigitada suure riskiga tehisintellektisüsteemiks sellised tehisintellektisüsteemid, mis on mõeldud rände-, varjupaiga- ja piirikontrollihaldusega tegelevatele pädevatele asutustele kasutamiseks valedetektorite ja samalaadsete vahenditena või füüsilise isiku emotsionaalse seisundi tuvastamiseks; teatavate liikmesriigi territooriumile siseneva või viisat või varjupaika taotleva füüsilise isiku põhjustatavate riskide hindamiseks; pädevate asutuste abistamiseks varjupaiga-, viisa- ja elamisloataotluste ja nendega seotud kaebuste läbivaatamisel, et teha kindlaks sellist staatust taotlevate füüsiliste isikute vastavus tingimustele. Rände-, varjupaiga- ja piirikontrollihalduse valdkonna tehisintellektisüsteemid, mis kuuluvad käesoleva määruse kohaldamisalasse, peaksid vastama Euroopa Parlamendi ja nõukogu direktiivis 2013/32/EL,[20] Euroopa Parlamendi ja nõukogu määruses (EÜ) nr 810/2009[21] ja muudes asjaomastes õigusaktides sätestatud asjaomastele menetlusnõuetele.

[20] Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta direktiiv 2013/32/EL rahvusvahelise kaitse seisundi andmise ja äravõtmise menetluse ühiste nõuete kohta (ELT L 180, 29.6.2013, lk 60).

[21] Euroopa Parlamendi ja nõukogu 13. juuli 2009. aasta määrus (EÜ) nr 810/2009, millega kehtestatakse ühenduse viisaeeskiri (viisaeeskiri) (ELT L 243, 15.9.2009, lk 1).

(40) Teatavad õigusemõistmise ja demokraatlike protsesside jaoks mõeldud tehisintellektisüsteemid tuleks liigitada suure riskiga tehisintellektisüsteemideks, arvestades nende võimalikku märkimisväärset mõju demokraatiale, õigusriigile, üksikisiku vabadustele ning õigusele tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele. Eeskätt võimalikust kallutatusest, vigadest ja läbipaistmatusest tulenevate riskidega toimetulemiseks on otstarbekas liigitada suure riskiga tehisintellektisüsteemideks need tehisintellektisüsteemid, mis on mõeldud abistama õigusasutusi faktide ja õiguse tõlgendamisel ning õiguse kohaldamisel konkreetse faktide kogumi suhtes. Samas ei tohiks selline liigitamine siiski laieneda tehisintellektisüsteemidele, mis on mõeldud puhtalt halduslikeks abitegevusteks, mis ei mõjuta tegelikku õigusemõistmist konkreetsetel juhtudel, nagu kohtuotsuste, dokumentide või andmete anonüümimine või pseudonüümimine, töötajatevaheline suhtlus ja haldusülesanded.

(41) Kui tehisintellektisüsteem on käesoleva määruse alusel liigitatud suure riskiga tehisintellektisüsteemiks, ei tuleks seda tõlgendada nii, et süsteemi kasutamine on seaduslik muude liidu õigusaktide või liidu õigusega kooskõlas olevate siseriiklike õigusaktide alusel, mis käsitlevad näiteks isikuandmete kaitset, valedetektorite või samalaadsete toodete kasutamist või muude süsteemide kasutamist füüsiliste isikute emotsionaalse seisundi tuvastamiseks. Edaspidi peaks igasugune selline kasutamine toimuma üksnes kooskõlas kohaldatavate nõuetega, mis tulenevad põhiõiguste hartast ja kohaldatavatest liidu teisese õiguse aktidest ja siseriiklikust õigusest. Käesolevat määrust ei tohiks käsitada isikuandmete, sealhulgas asjakohasel juhul isikuandmete eriliikide töötlemise õigusliku alusena, kui käesolevas määruses ei ole sõnaselgelt ette nähtud teisiti.

(42) Et leevendada riske, mida põhjustavad liidus turule lastud või muul moel kasutusele võetud suure riskiga tehisintellektisüsteemid, tuleks kohaldada teatavaid kohustuslikke nõudeid, võttes arvesse süsteemi kasutamise sihtotstarvet ja toimides pakkuja kehtestatud riskijuhtimissüsteemi kohaselt. Eelkõige peaks riskijuhtimissüsteem seisnema pidevalt korduvas protsessis, mida kavandatakse ja käitatakse suure riskiga tehisintellektisüsteemi kogu olelusringi jooksul. See protsess peaks tagama, et pakkuja teeb kindlaks riskid nende isikute tervisele, ohutusele ja põhiõigustele, keda süsteem võib selle sihtotstarvet silmas pidades mõjutada, sealhulgas võimalikud riskid, mis tulenevad tehisintellektisüsteemi ja selle töökeskkonna vastasmõjust, analüüsib neid riske ning võtab sellest tulenevalt tehnika taset silmas pidades sobivad riskijuhtimismeetmed.

(43) Suure riskiga tehisintellektisüsteemide suhtes tuleks kohaldada nõudeid seoses kasutatavate andmestike kvaliteedi, tehnilise dokumentatsiooni ja andmete säilitamise, läbipaistvuse ja kasutajate teavitamise, inimjärelevalve, stabiilsuse, täpsuse ja küberturvalisusega. Sellised nõuded on vajalikud, et tulemuslikult leevendada riske tervisele, ohutusele ja põhiõigustele, nagu on asjakohane süsteemi sihtotstarvet arvestades ning kuna muud kaubandust vähem piiravad meetmed ei ole mõistlikult kättesaadavad, et seega vältida põhjendamatuid kaubanduspiiranguid.

(44) Kvaliteetsed andmed on paljude tehisintellektisüsteemide toimimiseks hädavajalikud, eriti kui kasutatakse mudelite treenimise meetodeid, et tagada suure riskiga tehisintellektisüsteemide sihipärane ja ohutu töö ja see, et neist ei saa liidu õigusega keelatud diskrimineerimise allikas. Kvaliteetsete treenimis-, valideerimis- ja testimisandmestike olemasolu eeldab asjakohaste andmehalduse ja juhtimistavade rakendamist. Treenimis-, valideerimis- ja testimisandmestikud peaksid olema piisavalt asjakohased ja representatiivsed ning neil peaksid olema asjakohased statistilised omadused, sealhulgas mis puudutab selliseid isikuid või isikute rühmi, kelle peal kavatsetakse suure riskiga tehisintellektisüsteemi kasutada. Samuti peaksid need andmestikud olema võimalikult vigadeta ja täielikud, pidades silmas tehisintellektisüsteemi sihtotstarvet, võttes proportsionaalselt arvesse tehnilist teostatavust ja tehnika taset, andmete kättesaadavust ja asjakohaste riskijuhtimismeetmete rakendamist, et andmestike võimalikke puudusi nõuetekohaselt käsitleda. Nõue, et andmestikud peavad olema täielikud ja vigadeta, ei tohiks mõjutada eraelu puutumatuse säilitamise meetodite kasutamist tehisintellektisüsteemide arendamise ja testimise kontekstis. Treenimis-, valideerimis- ja testimisandmestikes tuleks võtta sihtotstarbe jaoks nõutavas ulatuses arvesse funktsioone, omadusi või elemente, mis iseloomustavad konkreetset geograafilist, käitumuslikku või funktsionaalset olukorda või konteksti, kus kavatsetakse suure riskiga tehisintellektisüsteemi kasutada. Et kaitsta teiste õigust tehisintellektisüsteemide kallutatusest tuleneda võiva diskrimineerimise eest, peaksid pakkujad saama töödelda isikuandmete eriliike seoses olulise avaliku huviga määruse (EL) 2016/679 artikli 9 lõike 2 punkti g ning määruse (EL) 2018/1725 artikli 10 lõike 2 punkti g tähenduses, et tagada suure riskiga tehisintellektisüsteemide puhul kallutatuse seire, avastamine ja korrigeerimine.

(44a) Määruse (EL) 2016/679 artikli 5 lõike 1 punktis c ja määruse (EL) 2018/1725 artikli 4 lõike 1 punktis c osutatud põhimõtete, eelkõige võimalikult väheste andmete kogumise põhimõtte kohaldamisel seoses käesoleva määruse kohaste treenimis-, valideerimis- ja testimisandmestikega tuleks nõuetekohaselt arvesse võtta tehisintellektisüsteemi kogu elutsüklit.

(45) Suure riskiga tehisintellektisüsteemide arendamiseks peaks teatavatel asjaosalistel, näiteks pakkujatel, teavitatud asutustel ja muudel asjaomastel üksustel, näiteks digitaalse innovatsiooni keskustel, testimis- ja eksperimenteerimisrajatistel ja teadlastel, olema oma käesoleva määrusega seotud tegevusvaldkondades juurdepääs kvaliteetsetele andmestikele ja nad peaksid saama neid kasutada. Komisjoni loodud Euroopa ühised andmeruumid ning avaliku huvi nimel hõlpsam andmete jagamine ettevõtete vahel ja valitsustega on äärmiselt tähtis, et pakkuda tehisintellektisüsteemide treenimiseks, valideerimiseks ja testimiseks usaldusväärset, vastutustundlikku ja mittediskrimineerivat juurdepääsu kvaliteetsetele andmetele. Näiteks tervishoiu valdkonnas hõlbustab tervishoiu Euroopa andmeruum mittediskrimineerivat juurdepääsu terviseandmetele ja tehisintellekti algoritmide treenimist selliste andmestikega privaatsust tagaval, turvalisel, õigeaegsel, läbipaistval ja usaldusväärsel viisil ning asjakohase institutsioonilise juhtimise tingimustes. Asjaomased pädevad asutused, sealhulgas valdkondlikud asutused, kes pakuvad või toetavad juurdepääsu andmetele, võivad toetada ka kvaliteetsete andmete pakkumist tehisintellektisüsteemide treenimiseks, valideerimiseks ja testimiseks.

(46) Selleks, et kontrollida vastavust käesoleva määruse kohastele nõuetele, on äärmiselt oluline omada teavet selle kohta, kuidas on suure riskiga tehisintellektisüsteemid välja töötatud ja kuidas need oma elutsükli jooksul töötavad. Selleks on vaja säilitada andmeid ja tagada sellise tehnilise dokumentatsiooni kättesaadavus, mis sisaldab tehisintellektisüsteemi asjakohastele nõuetele vastavuse hindamiseks vajalikku teavet. Sellise teabe hulka peaksid kuuluma süsteemi üldised omadused, võimekused ja piirid, algoritmid, andmed, kasutatud treenimis-, testimis- ja valideerimisprotsessid ning dokumentatsioon asjaomase riskijuhtimissüsteemi kohta. Tehniline dokumentatsioon peaks olema ajakohane. Lisaks peaksid pakkujad või kasutajad säilitama suure riskiga tehisintellektisüsteemi poolt automaatselt loodud logisid, sealhulgas näiteks väljundandmeid, alustamise kuupäeva ja kellaaega jne niivõrd, kuivõrd selline süsteem ja sellega seotud logid on nende kontrolli all, ajavahemiku jooksul, mis on asjakohane, et võimaldada neil oma kohustusi täita.

(47) Seoses läbipaistmatusega, mis võib muuta teatavad tehisintellektisüsteemid füüsiliste isikute jaoks arusaamatuks või liiga keeruliseks, tuleks suure riskiga tehisintellektisüsteemide puhul nõuda teatavat läbipaistvust. Kasutajad peaksid suutma süsteemi väljundit tõlgendada ja asjakohaselt kasutada. Seepärast peaks suure riskiga tehisintellektisüsteemidega olema kaasas asjaomane dokumentatsioon ja kasutusjuhendid, mis peaksid sisaldama täpset ja selget teavet muu hulgas võimalike riskide kohta, mis võivad esineda seoses nende isikute põhiõiguste ja diskrimineerimisega, keda süsteem võib selle sihtotstarvet silmas pidades mõjutada, kui see on asjakohane. Selleks et kasutajatel oleks lihtsam kasutusjuhendist aru saada, peaks see vajaduse korral sisaldama illustreerivaid näiteid.

(48) Suure riskiga tehisintellektisüsteeme tuleks projekteerida ja arendada selliselt, et füüsilised isikud saavad teha järelevalvet nende toimimise üle. Selleks peaks süsteemi pakkuja tegema enne süsteemi turule laskmist või kasutusele võtmist kindlaks asjakohased inimjärelevalve meetmed. Kui see on asjakohane, tuleks selliste meetmetega eeskätt tagada, et süsteemi on sisse ehitatud käitamisega seotud piirangud, mida süsteem ise ei saa tühistada, et süsteem reageerib inimoperaatori käskudele ning et järelevalvega tegelema määratud füüsilised isikud on selle ülesande täitmiseks piisavalt pädevad ning neil on vajalik koolitus ja õigused. Võttes arvesse märkimisväärseid tagajärgi isikutele, kui teatavad biomeetrilise tuvastamise süsteemid annavad valesid tulemusi, on asjakohane näha nende süsteemide puhul ette tõhusama inimjärelevalve nõue, et kasutaja ei saaks süsteemist tuleneva tuvastamise põhjal midagi ette võtta ega otsust teha, kui tuvastamist ei ole eraldi kontrollinud ja kinnitanud vähemalt kaks füüsilist isikut. Need isikud võivad olla pärit ühest või mitmest üksusest ning nende hulka võib kuuluda süsteemi käitav või kasutav isik. See nõue ei tohiks põhjustada tarbetut koormust ega tarbetuid viivitusi ning piisata võib sellest, kui eri isikute tehtud eraldi kontrollid registreeritakse automaatselt süsteemi loodud logides.

(49) Suure riskiga tehisintellektisüsteemid peaksid toimima kogu oma elutsükli jooksul järjepidevalt ning nende täpsus, stabiilsus ja küberturvalisus peaks olema asjakohasel tasemel vastavalt tehnika üldtunnustatud tasemele. Täpsusaste ja täpsuse parameetrid tuleks kasutajatele teatavaks teha.

(50) Suure riskiga tehisintellektisüsteemide üks peamisi nõudeid on tehniline stabiilsus. Sellised süsteemid peaksid olema vastupidavad kahjuliku või muul viisil soovimatu käitumise suhtes, mis võib tuleneda süsteemide või nende töökeskkonna piirangutest (nt vead, rikked, ebakõlad, ootamatud olukorrad). Seepärast tuleks suure riskiga tehisintellektisüsteeme projekteerida ja arendada nii, et neil oleks asjakohased tehnilised lahendused, mille abil saab vältida või minimeerida sellist kahjulikku või muul viisil soovimatut käitumist, näiteks mehhanismid, mis võimaldavad süsteemil oma töö ohutult katkestada (tõrkekindluse plaanid) teatavate kõrvalekallete esinemisel või juhul, kui käitamine toimub väljaspool teatavaid eelnevalt kindlaks määratud piire. Suutmatus kaitsta nende riskide eest võib mõjutada ohutust või kahjustada põhiõigusi näiteks ekslike otsuste või tehisintellektisüsteemi genereeritud ekslike või kallutatud väljundite tõttu.

(51) Küberturvalisusel on oluline roll, et tagada tehisintellektisüsteemide vastupidavus pahatahtlike kolmandate isikute katsetele muuta süsteemi nõrku kohti ära kasudes süsteemi kasutust, käitumist või toimimist või kahjustada selle turvaomadusi. Tehisintellektisüsteemide vastu suunatud küberrünnetes võidakse ära kasutada tehisintellektispetsiifilisi ressursse, näiteks treeningandmestikke (nt andmemürgitus, i.k. *data poisoning*) või treenitud mudeleid (nt vastandründed, i.k. *adversarial attacks*), või tehisintellektisüsteemi digivarade või IKT alustaristu nõrkusi. Seega peaksid suure riskiga tehisintellektisüsteemide pakkujad võtma riskidele vastava küberturvalisuse taseme tagamiseks sobivaid meetmeid, arvestades sealjuures vastavalt vajadusele ka IKT alustaristuga.

(52) Suure riskiga tehisintellektisüsteemide turule laskmise, kasutusele võtmise ja kasutamise suhtes kohaldatavad õigusnormid kui liidu ühtlustamisõigusaktide osa tuleks kehtestada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EÜ) nr 765/2008,[22] millega sätestatakse akrediteerimise ja turujärelevalve nõuded, Euroopa Parlamendi ja nõukogu otsusega nr 768/2008/EÜ[23] toodete turustamise ühise raamistiku kohta ning Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/1020[24] turujärelevalve ja toodete vastavuse kohta (edaspidi „uus toodete turustamise õigusraamistik“).

(52a) Kooskõlas uue õigusraamistiku põhimõtetega tuleks tehisintellekti väärtusahela asjaomaste operaatorite jaoks kehtestada spetsiifilised kohustused, et tagada õiguskindlus ja hõlbustada käesoleva määruse järgimist. Teatavates olukordades võivad need operaatorid tegutseda samal ajal rohkem kui ühes rollis ja peaksid seetõttu kumulatiivselt täitma kõik nende rollidega seotud asjakohased kohustused. Näiteks võib operaator tegutseda samal ajal turustaja ja importijana.

(53) On otstarbekas, et suure riskiga tehisintellektisüsteemi turule laskmise või kasutusele võtmise eest võtab vastutuse konkreetne füüsiline või juriidiline isik, kes on määratletud kui pakkuja, olenemata sellest, kas see füüsiline või juriidiline isik on süsteemi projekteerija või arendaja.

---

22 Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta määrus (EÜ) nr 765/2008, millega sätestatakse akrediteerimise ja turujärelevalve nõuded seoses toodete turustamisega ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93 (ELT L 218, 13.8.2008, lk 30).

23 Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta otsus nr 768/2008/EÜ toodete turustamise ühise raamistiku kohta ja millega tunnistatakse kehtetuks nõukogu otsus 93/465/EMÜ (ELT L 218, 13.8.2008, lk 82).

24 Euroopa Parlamendi ja nõukogu 20. juuni 2019. aasta määrus (EL) 2019/1020 turujärelevalve ja toodete vastavuse kohta ning millega muudetakse direktiivi 2004/42/EÜ ja määruseid (EÜ) nr 765/2008 ja (EL) nr 305/2011 (ELT L 169, 25.6.2019, lk 1–44).

(54) Pakkuja peaks kehtestama usaldusväärse kvaliteedijuhtimissüsteemi, tagama nõutava vastavushindamismenetluse teostamise, koostama asjakohase dokumentatsiooni ja kehtestama stabiilse turustamisjärgse seire süsteemi. Avaliku sektori asutused, kes võtavad suure riskiga tehisintellektisüsteemi kasutusele oma tarbeks, võivad võtta vastu kvaliteedijuhtimissüsteemi reeglid ja neid rakendada olenevalt asjaoludest riigi või piirkonna tasemel vastuvõetud kvaliteedijuhtimissüsteemi osana, võttes arvesse sektori iseärasusi ning asjaomase avaliku sektori asutuse pädevust ja töökorraldust.

(54a) Õiguskindluse tagamiseks on oluline selgitada, et teatavatel konkreetsetel tingimustel tuleks iga füüsilist või juriidilist isikut käsitada uue suure riskiga tehisintellektisüsteemi pakkujana ning tal peaksid seega olema kõik asjaomased kohustused. Nii oleks see näiteks juhul, kui isik lisab juba turule lastud või kasutusele võetud suure riskiga tehisintellektisüsteemile oma nime või kaubamärgi või kui see isik muudab sellise tehisintellektisüsteemi sihtotstarvet, mis ei ole suure riskiga süsteem ja on juba turule lastud või kasutusele võetud, nii et muudetud süsteem on suure riskiga tehisintellektisüsteem. Neid sätteid tuleks kohaldada, ilma et see piiraks selliste konkreetsemate sätete kohaldamist, mis on kehtestatud teatavates uue õigusraamistiku valdkondlikes õigusaktides, millega koos tuleks käesolevat määrust kohaldada. Näiteks määruse (EL) 745/2017 artikli 16 lõiget 2, milles on sätestatud, et teatavaid muudatusi ei tohiks käsitada seadme muutmisena viisil, mis võib mõjutada selle vastavust kohaldatavatele nõuetele, tuleks jätkuvalt kohaldada suure riskiga tehisintellektisüsteemide suhtes, mis on kõnealuse määruse tähenduses meditsiiniseadmed.

(55) Kui uue õigusraamistiku asjaomase valdkondliku õigusakti kohaldamisalasse kuuluva toote turvakomponendiks olevat suure riskiga tehisintellektisüsteemi ei lasta turule ega võeta kasutusele tootest sõltumatult, peaks uue õigusraamistiku asjakohases õigusaktis määratletud toote tootja täitma käesolevas määruses pakkujale kehtestatud kohustusi ja eeskätt tagama selle, et lõpptootesse integreeritud tehisintellektisüsteem vastab käesoleva määruse nõuetele.

(56) Et võimaldada käesoleva määruse täitmine ja luua operaatoritele võrdsed tingimused, võttes sealjuures arvesse digitoodete kättesaadavaks tegemise eri vorme, on oluline tagada, et mõni liidus tegutsev isik saab igas olukorras esitada ametiasutustele kogu vajaliku teabe tehisintellektisüsteemi nõuetele vastavuse kohta. Seepärast peab väljaspool liitu asuv pakkuja juhul, kui importijat ei ole võimalik kindlaks teha, enne oma süsteemi liidu turul kättesaadavaks tegemist määrama kirjaliku volitusega liidus asuva volitatud esindaja.

(56a) Selliste pakkujate puhul, kes ei asu liidus, on volitatud esindajal esmatähtis roll kõnealuste pakkujate poolt liidus turule lastud või kasutusele võetud suure riskiga tehisintellektisüsteemide nõuetele vastavuse tagamisel ja nende liidus asuva kontaktisikuna tegutsemisel. Pidades silmas kõnealust esmatähtsat rolli ja tagamaks, et võetakse vastutus käesoleva määruse täitmise tagamiseks, on asjakohane määrata volitatud esindaja pakkujaga solidaarselt vastutavaks defektsete suure riskiga tehisintellektisüsteemide eest. Käesoleva määrusega ette nähtud volitatud esindaja vastutus ei piira tootevastutust käsitleva direktiivi 85/374/EMÜ sätete kohaldamist.

(57) [välja jäetud]

(58) Arvestades tehisintellektisüsteemide olemust ning nende kasutamisega potentsiaalselt seotud riske ohutusele ja põhiõigustele, muu hulgas seoses vajadusega tagada reaalsetes oludes tehisintellektisüsteemi toimimise nõuetekohane seire, on otstarbekas näha kasutajatele ette konkreetsed kohustused. Esmajoones peaksid kasutajad kasutama suure riskiga tehisintellektisüsteeme kasutusjuhendi kohaselt ning vastavalt vajadusele tuleks kehtestada teatavad muud kohustused seoses tehisintellektisüsteemide töö seire ja andmete säilitamisega. Need kohustused ei tohiks piirata kasutajate jaoks liidu või liikmesriikide õigusest tulenevaid muid kohustusi seoses suure riskiga tehisintellektisüsteemidega ning neid ei tuleks kohaldada, kui kasutamine toimub isikliku, mitte kutselise tegevuse käigus.

(58a) On asjakohane selgitada, et käesolev määrus ei mõjuta tehisintellektisüsteemide pakkujate ja kasutajate jaoks liidu õigusest tulenevaid kohustusi, mis on seotud nende rolliga vastutava töötlejana või volitatud töötlejana ning mis käsitlevad isikuandmete kaitset, niivõrd, kuivõrd tehisintellektisüsteemide projekteerimine, arendamine või kasutamine hõlmab isikuandmete töötlemist. Samuti on asjakohane selgitada, et andmesubjektide jaoks säilivad kõik sellisest liidu õigusest tulenevad õigused ja tagatised, sealhulgas üksnes automatiseeritud üksikotsuste tegemisega (ka profiilianalüüsiga) seotud õigused. Käesoleva määruse alusel kehtestatud tehisintellektisüsteemide turule laskmist, kasutusele võtmist ja kasutamist käsitlevad ühtlustatud õigusnormid peaksid hõlbustama andmesubjektide õiguste ja teiste liidu õiguse kohaselt isikuandmete kaitse ja muude põhiõigustega seoses tagatud õiguskaitsevahendite tulemuslikku rakendamist ning võimaldama nende kasutamist.

(59) [välja jäetud]

(60) [välja jäetud]

(61) Oluline roll peaks olema standardimisel, et anda pakkujatele tehnilised lahendused käesoleva määruse nõuete täitmiseks kooskõlas tehnika tasemega. Euroopa Parlamendi ja nõukogu määruses (EL) nr 1025/2012[25] määratletud harmoneeritud standardite – mis üldiselt peaksid kajastama tehnika taset – järgimine peaks olema pakkujate jaoks vahend, millega tõendada käesoleva määruse nõuete täitmist. Kui asjakohased viited harmoneeritud standarditele puuduvad, peaks komisjonil siiski olema võimalik kehtestada rakendusaktidega erakorralise varulahendusena teatavate käesoleva määruse kohaste nõuete ühtsed kirjeldused, et hõlbustada pakkuja kohustust täita käesoleva määruse nõudeid, kui standardimisprotsess on blokeeritud või kui asjakohase harmoneeritud standardi kehtestamisel esineb viivitusi. Kui selline viivitus on tingitud kõnealuse standardi tehnilisest keerukusest, peaks komisjon seda enne ühtsete kirjelduste kehtestamist kaaluma. Väikeste ja keskmise suurusega ettevõtjate asjakohane kaasamine käesoleva määruse rakendamist toetavate standardite väljatöötamisse on oluline, et edendada liidus tehisintellekti valdkonnas innovatsiooni ja konkurentsivõimet. Selline kaasamine tuleks nõuetekohaselt tagada kooskõlas määruse 1025/2012 artiklitega 5 ja 6.

[25] Euroopa Parlamendi ja nõukogu 25. oktoobri 2012. aasta määrus (EL) nr 1025/2012, mis käsitleb Euroopa standardimist ning millega muudetakse nõukogu direktiive 89/686/EMÜ ja 93/15/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 94/9/EÜ, 94/25/EÜ, 95/16/EÜ, 97/23/EÜ, 98/34/EÜ, 2004/22/EÜ, 2007/23/EÜ, 2009/23/EÜ ja 2009/105/EÜ ning millega tunnistatakse kehtetuks nõukogu otsus 87/95/EMÜ ning Euroopa Parlamendi ja nõukogu otsus nr 1673/2006/EÜ (ELT L 316, 14.11.2012, lk 12).

(61a) Ilma et see piiraks harmoneeritud standardite ja ühtsete kirjelduste kasutamist, on asjakohane, et pakkujad võivad eeldada vastavust asjakohasele andmenõudele, kui nende suure riskiga tehisintellektisüsteemi on treenitud ja testitud andmetega, mis peegeldavad konkreetset geograafilist, käitumuslikku või funktsionaalset olukorda, milles kasutamiseks tehisintellektisüsteem on mõeldud. Samamoodi tuleks kooskõlas Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 54 lõikega 3 eeldada, et suure riskiga tehisintellektisüsteemid, mis on sertifitseeritud või mille kohta on välja antud vastavusdeklaratsioon nimetatud määruse kohase küberturvalisuse sertifitseerimise kava alusel ning mille viited on avaldatud *Euroopa Liidu Teatajas*, vastavad käesoleva määruse kohasele küberturvalisuse nõudele. See ei piira kõnealuse küberturvalisuse kava vabatahtlikkust.

(62) Selleks et tagada suure riskiga tehisintellektisüsteemide usaldusväärsuse kõrge tase, peaksid need süsteemid enne turule laskmist või kasutuselevõtmist läbima vastavushindamise.

(63) Operaatorite koormuse minimeerimiseks ja võimaliku dubleerimise vältimiseks on otstarbekas hinnata uue õigusraamistiku lähenemisviisi järgi olemasolevate liidu ühtlustamisõigusaktide kohaldamisalasse kuuluvate toodetega seotud suure riskiga tehisintellektisüsteemide vastavust käesoleva määruse nõuetele osana kõnealuste õigusaktidega juba ette nähtud vastavushindamisest. Seega ei tohiks käesoleva määruse nõuete kohaldatavus mõjutada uue õigusraamistiku konkreetsete asjaomaste õigusaktide kohaselt tehtava vastavushindamise eriomast loogikat, metoodikat või üldist ülesehitust. Käesoleva määruse ja [masinamääruse] vastastikune mõju kajastab täielikult sellist lähenemisviisi. Masinates turvafunktsioone täitvate tehisintellektisüsteemide ohutusriske käsitletakse käesoleva määruse nõuetes, kuid tehisintellektisüsteemi ohutu integreerimine üldisse masinavärki tagatakse [masinamääruse] teatavate konkreetsete nõuetega, et mitte seada ohtu masina kui terviku ohutust. [Masinamääruses] on kasutatud sama tehisintellektisüsteemi määratlust kui käesolevas määruses. Suure riskiga tehisintellektisüsteemide osas, mis on seotud meditsiiniseadmeid käsitlevate määrustega (EL) 745/2017 ja (EL) 746/2017 hõlmatud toodetega, ei tohiks käesoleva määruse nõuete kohaldatavus piirata ja peaks võtma arvesse riskijuhtimise loogikat ning meditsiiniseadmete raamistiku alusel tehtud kasulikkuse ja riski hindamist.

(64) Kuna kutselistel turustamiseelsetel sertifitseerijatel on tooteohutuse valdkonnas laialdasemad kogemused ja kaasnevad riskid on oma olemuselt erinevad, on otstarbekas vähemalt käesoleva määruse kohaldamise algjärgus piirata kolmanda isiku tehtava vastavushindamise kohaldamise ulatust muude kui toodetega seotud suure riskiga tehisintellektisüsteemide puhul. Seepärast peaks selliste süsteemide vastavushindamise üldjuhul tegema pakkuja omal vastutusel; ainsaks erandiks on tehisintellektisüsteemid, mis on mõeldud kasutamiseks isikute biomeetrilise kaugtuvastamise jaoks ja mille puhul tuleks ette näha teavitatud asutuse osalemine vastavushindamises, eeldusel, et sellised süsteemid ei ole keelatud.

(65) Selleks, et isikute biomeetrilises kaugtuvastamises kasutamiseks mõeldud tehisintellektisüsteem saaks läbida kolmanda isiku tehtava vastavushindamise, peaksid riikide pädevad asutused käesoleva määruse alusel teatama teavitatud asutustest, tingimusel et need vastavad teatavatele nõuetele eeskätt sõltumatuse, pädevuse ja huvide konflikti puudumise vallas. Riikide pädevad asutused peaksid saatma teavituse kõnealuste asutuste kohta komisjonile ja teistele liikmesriikidele komisjoni poolt otsuse 768/2008 artikli R23 alusel väljaarendatud ja hallatava elektroonilise teavitamise vahendi kaudu.

(66) Liidu ühtlustamisõigusaktidega reguleeritud toodete olulise muudatuse laialdaselt juurdunud mõistega kooskõlas on otstarbekas, et kui tehakse muudatus, mis võib mõjutada suure riskiga tehisintellektisüsteemi vastavust käesolevale määrusele (nt operatsioonisüsteemi või tarkvaraarhitektuuri muudatus), või kui muutub süsteemi sihtotstarve, tuleks kõnealust tehisintellektisüsteemi käsitada uue tehisintellektisüsteemina, mis peaks läbima uue vastavushindamise. Siiski ei peaks muudatuste puhul, mis tehakse selliste tehisintellektisüsteemide algoritmis või toimimises, mis n-ö õpivad edasi ka pärast turule laskmist või kasutusele võtmist (st nad kohandavad funktsioonide täitmist automaatselt), olema tegemist olulise muudatusega, kui pakkuja on kõnealused muudatused eelnevalt kindlaks määranud ja kui neid on vastavushindamise ajal hinnatud.

(67) Suure riskiga tehisintellektisüsteemidel peaks olema CE-märgis, mis näitab nende vastavust käesolevale määrusele, et nad saaksid siseturul vabalt liikuda. Liikmesriigid ei tohiks luua põhjendamatuid tõkkeid käesolevas määruses sätestatud nõuetele vastavate ja CE-märgisega suure riskiga tehisintellektisüsteemide turule laskmisele või kasutusele võtmisele.

(68) Teatavatel tingimustel võib uuenduslike tehnoloogiate kiire kättesaadavus olla inimeste tervise ja ohutuse ning ühiskonna kui terviku jaoks olla äärmiselt tähtis. Seepärast on otstarbekas, et teatavatel erandlikel põhjustel, mis on seotud avaliku julgeoleku või füüsiliste isikute elu ja tervise kaitse ning tööstus- ja kaubandusomandi kaitsega, võiksid liikmesriigid lubada selliste tehisintellektisüsteemide turule laskmist või kasutusele võtmist, mis ei ole vastavushindamist läbinud.

(69) Et hõlbustada tööd, mida komisjon ja liikmesriigid tehisintellekti vallas teevad, ja suurendada avalikkuse jaoks läbipaistvust, peaksid muude kui asjaomaste olemasolevate liidu ühtlustamisõigusaktide kohaldamisalasse kuuluvate toodetega seotud suure riskiga tehisintellektisüsteemide pakkujad olema kohustatud registreerima ennast ja teabe oma suure riskiga tehisintellektisüsteemi kohta ELi andmebaasis, mille loob ja mida haldab komisjon. Enne III lisas loetletud suure riskiga tehisintellektisüsteemi kasutamist registreerivad suure riskiga tehisintellektisüsteemide kasutajad, kes on avaliku sektori asutused, ametid või organid (välja arvatud õiguskaitse-, piirkontrolli-, rände- või varjupaigaasutused) ning ametiasutused, kes on suure riskiga tehisintellektisüsteemide kasutajad elutähtsa taristu valdkonnas, end samuti sellises andmebaasis ja valivad välja süsteemi, mida nad kavatsevad kasutada. Selle andmebaasi vastutav töötleja peaks olema komisjon vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2018/1725[26]. Et andmebaas oleks kasutuselevõtmisel täielikult toimiv, peaks andmebaasi loomise protseduur hõlmama funktsionaalsete kirjelduste väljatöötamist komisjoni poolt ja sõltumatut auditiaruannet.

[26] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

(70) Teatavate tehisintellektisüsteemide puhul, mis on mõeldud suhtlema füüsiliste isikutega või sisu looma, võib esineda kellenagi esinemise või pettuse spetsiifilisi riske olenemata sellest, kas süsteemid on liigitatud suure riskiga süsteemideks või mitte. Seepärast peaks nende süsteemide kasutamise suhtes teatavates olukordades kehtima spetsiifilised läbipaistvuskohustused, ilma et see piiraks suure riskiga tehisintellektisüsteemide suhtes kehtivate nõuete ja kohustuste kohaldamist. Eelkõige tuleks füüsilistele isikutele anda teada, et nad suhtlevad tehisintellektisüsteemiga, välja arvatud juhul, kui see on mõistlikult informeeritud, tähelepaneliku ja aruka füüsilise isiku jaoks ilmne, võttes arvesse asjaolusid ja kasutamise konteksti. Sellise kohustuse rakendamisel tuleks arvesse võtta nende isikute omadusi, kes kuuluvad oma vanuse või puude tõttu haavatavatesse rühmadesse, niivõrd kui tehisintellektisüsteem on mõeldud ka nende rühmadega suhtlemiseks. Peale selle tuleks füüsilisi isikuid teavitada, kui nad puutuvad kokku süsteemidega, mis suudavad nende biomeetrilisi andmeid töödeldes tuvastada või tuletada nende emotsioone või kavatsusi või liigitada kõnealused isikud konkreetsesse kategooriasse. Kõnealused konkreetsed kategooriad võivad olla seotud selliste aspektidega nagu sugu, vanus, juuksevärv, silmade värv, tätoveeringud, isikuomadused, etniline päritolu, isiklikud eelistused ja huvid, või muude aspektidega, nagu seksuaalne või poliitiline sättumus. Selline teave ja teavitused tuleks edastada vormingus, mis on puuetega inimestele juurdepääsetaval kujul. Lisaks peaks kasutaja, kes kasutab tehisintellektisüsteemi, et luua või manipuleerida kujutisi või audio- või videosisu, mis sarnanevad märgatavalt olemasolevate isikute, kohtade või sündmustega ja võib inimesele ekslikult tunduda ehtne, avalikustama, et see sisu on kunstlikult loodud või seda on manipuleeritud, tähistades tehisintellekti väljundi vastavalt ja avalikustades selle tehisliku päritolu. Eespool osutatud teavitamiskohustuste täitmist ei tohiks tõlgendada nii, et süsteemi või selle väljundi kasutamine on seaduslik käesoleva määruse või liidu ja liikmesriikide muu õiguse alusel, ning see ei tohiks piirata tehisintellektisüsteemide kasutajate muid läbipaistvuskohustusi, mis on sätestatud liidu või siseriiklikus õiguses. Seda ei tohiks ka tõlgendada nii, et süsteemi või selle väljundi kasutamine takistab ELi põhiõiguste hartaga tagatud väljendusvabaduse ning kunsti ja teaduse vabaduse õiguse teostamist, eelkõige kui sisu moodustab osa ilmselgelt loomingulisest, satiirilisest, kunstilisest või väljamõeldud teosest või programmist, tingimusel et kolmandate isikute õiguste ja vabaduste kaitseks kohaldatakse asjakohaseid kaitsemeetmeid.

(71) Tehisintellekt on kiirelt arenev tehnoloogiaharu, mis eeldab uudset regulatiivset järelevalvet ja turvalist eksperimenteerimisruumi, aga ka seda, et tagatud oleks vastutustundlik innovatsioon ning asjakohaste kaitsemeetmete ja riskileevendusmeetmete integreerimine. Innovatsioonisõbraliku, tulevikukindla ja häirete suhtes vastupanuvõimelise õigusraamistiku tagamiseks tuleks ühe või mitme liikmesriigi pädevaid asutusi julgustada looma tehisintellekti regulatsiooni testkeskkondi, mis hõlbustaksid innovatiivsete tehisintellektisüsteemide arendamist ja testimist range regulatiivse järelevalve all, enne kui need süsteemid turule lastakse või muul moel kasutusele võetakse.

(72) Tehisintellekti regulatsiooni testkeskkondade eesmärk peaks olema edendada tehisintellekti alast innovatsiooni kontrollitud eksperimenteerimis- ja testimiskeskkonna loomisega arendamisetapis ja turustamiseelses etapis, et tagada innovatiivsete tehisintellektisüsteemide vastavus käesolevale määrusele ning muudele asjakohastele liidu ja liikmesriikide õigusaktidele; parandada novaatorite õiguskindlust ja pädevate asutuste järelevalvet ning arusaamist tehisintellekti kasutamise võimalustest, tekkivatest riskidest ja mõjudest ning kiirendada turulepääsu muu hulgas sellega, et kaotatakse tõkked, mis piiravad väikeseid ja keskmise suurusega ettevõtjaid, sealhulgas idufirmasid. Tehisintellekti regulatsiooni testkeskkonnas osalemisel tuleks keskenduda küsimustele, mis tekitavad pakkujatele ja võimalikele pakkujatele õiguskindlusetust seoses innovatsiooni, liidus tehisintellektiga eksperimenteerimise ja tõenduspõhisele regulatiivsele õppimisele kaasaaitamisega. Tehisintellektisüsteemide järelevalve tehisintellekti regulatsiooni testkeskkonnas peaks seega hõlmama süsteemide arendamist, treenimist, testimist ja valideerimist enne nende turule laskmist või kasutusele võtmist, samuti sellise olulise muudatuse mõistet ja tegemist, mis võib nõuda uut vastavushindamismenetlust. Kui see on asjakohane, peaksid tehisintellekti regulatsiooni testkeskkondi loovad riikide pädevad asutused tegema koostööd teiste asjaomaste asutustega, sealhulgas nendega, kes teevad järelevalvet põhiõiguste kaitse üle, ning võiksid lubada kaasata muid tehisintellekti ökosüsteemis osalejaid, nagu riiklikud või Euroopa standardiorganisatsioonid, teavitatud asutused, testimis- ja eksperimenteerimisrajatised, teadus- ja eksperimenteerimislaborid, innovatsioonikeskused ning asjaomased sidusrühmad ja kodanikuühiskonna organisatsioonid. Selleks, et tagada ühetaoline rakendamine kogu liidus ja mastaabisääst, on otstarbekas kehtestada regulatsiooni testkeskkondade rakendamise ühised eeskirjad ja testkeskkondade järelevalvega tegelevate asjaomaste ametiasutusete vahelise koostöö raamistik. Käesoleva määruse alusel loodud tehisintellekti regulatsiooni testkeskkonnad ei tohiks piirata selliste muude õigusaktide kohaldamist, mis võimaldavad luua muid testkeskkondi, mille eesmärk on tagada kooskõla muude õigusaktidega kui käesolev määrus. Kui see on asjakohane, peaksid nende muude regulatsiooni testkeskkondade eest vastutavad asjaomased pädevad asutused kaaluma, millised eelised on sellel, kui neid testkeskkondi kasutatakse ka eesmärgiga tagada tehisintellektisüsteemide vastavus käesolevale määrusele. Riikide pädevate asutuste ja tehisintellekti regulatsiooni testkeskkonnas osalejate vahelisel kokkuleppel võib tehisintellekti regulatsiooni testkeskkonna raames korraldada ja kontrollida ka testimist tegelikes tingimustes.

(-72a) Käesoleva määrusega tuleks tehisintellekti regulatsiooni testkeskkonnas osalejatele ette näha õiguslik alus muul otstarbel kogutud isikuandmete kasutamiseks, et arendada tehisintellekti regulatsiooni testkeskkonnas avalikes huvides teatavaid tehisintellektisüsteeme kooskõlas määruse (EL) 2016/679 artikli 6 lõikega 4 ja artikli 9 lõike 2 punktiga g ning määruse (EL) 2018/1725 artiklitega 5 ja 10 ning ilma, et see piiraks direktiivi (EL) 2016/680 artikli 4 lõike 2 ja artikli 10 kohaldamist. Kõik muud vastutavate töötlejate kohustused ja andmesubjektide õigused, mis tulenevad määrusest (EL) 2016/679, määrusest (EL) 2018/1725 ja direktiivist (EL) 2016/680, jäävad kehtima. Eelkõige ei tohiks käesolev määrus olla õiguslik alus määruse (EL) 2016/679 artikli 22 lõike 2 punkti b ja määruse (EL) 2018/1725 artikli 24 lõike 2 punkti b tähenduses. Testkeskkonnas osalejad peaksid tagama asjakohased kaitsemeetmed ja tegema koostööd pädevate asutustega, järgides muu hulgas nende juhiseid ning tegutsedes viivitusteta ja heas usus, et leevendada ohutust ja põhiõigusi ähvardavaid suuri riske, mis võivad testkeskkonnas arendustegevuse ja eksperimenteerimise käigus tekkida. Kui pädevad asutused otsustavad, kas määrata haldustrahv määruse 2016/679 artikli 83 lõike 2 ja direktiivi 2016/680 artikli 57 alusel, tuleks osalejate käitumist testkeskkonnas arvesse võtta.

(72a) Selleks et kiirendada III lisas loetletud suure riskiga tehisintellektisüsteemide arendamist ja turule laskmist, on oluline, et selliste süsteemide pakkujad või võimalikud pakkujad saaksid kasutada ka erikorda nende süsteemide testimiseks tegelikes tingimustes, ilma et nad osaleksid tehisintellekti regulatsiooni testkeskkonnas. Sellistel juhtudel ja võttes arvesse sellise testimise võimalikke tagajärgi üksikisikutele, tuleks siiski tagada, et määrusega kehtestatakse pakkujatele ja võimalikele pakkujatele asjakohased ja piisavad tagatised ja tingimused. Sellised tagatised peaksid muu hulgas hõlmama füüsilistelt isikutelt teadva nõusoleku taotlemist tegelikes tingimustes testimises osalemiseks, välja arvatud õiguskaitse puhul sellistel juhtudel, kus teadva nõusoleku taotlemine takistaks tehisintellektisüsteemi testimist. Subjektide nõusolek sellises testimises osalemiseks käesoleva määruse alusel erineb andmesubjektide nõusolekust oma isikuandmete töötlemiseks asjakohase andmekaitseõiguse alusel ega piira kõnealuse õiguse kohaldamist.

(73) Innovatsiooni edendamiseks ja kaitsmiseks on oluline pöörata erilist tähelepanu tehisintellektisüsteemide VKEdest pakkujate ja kasutajate huvidele. Liikmesriigid peaksid selle eesmärgi nimel välja töötama nimetatud operaatoritele suunatud algatusi, muu hulgas teadlikkuse suurendamise ja teabe edastamise teemal. Ühtlasi tuleb VKEdest pakkujate konkreetsete huvide ja vajadustega arvestada, kui teavitatud asutused panevad paika vastavushindamise tasud. Kohustusliku dokumentatsiooni ja ametiasutustega suhtlemisega seotud tõlkekulud võivad osutuda pakkujate ja muude operaatorite jaoks märkimisväärseks, eriti juhul, kui tegemist on väiksemate ettevõtjatega. Liikmesriigid peaksid võimaluse korral tagama, et üks nende poolt asjaomaste pakkujate dokumentatsiooni ja operaatoritega suhtlemise jaoks kindlaks määratud ja neile vastuvõetavatest keeltest on keel, mis on üldjoontes arusaadav võimalikult suurele arvule piiriülestele kasutajatele.

(73a) Innovatsiooni edendamiseks ja kaitsmiseks peaksid tehisintellekti nõudeplatvorm, kõik asjakohased ELi rahastamisprogrammid ja -projektid, nagu programm „Digitaalne Euroopa“ ja programm „Euroopa horisont“, mida rakendavad komisjon ja liikmesriigid riiklikul või ELi tasandil, aitama kaasa käesoleva määruse eesmärkide saavutamisele.

(74) Selleks, et minimeerida rakendamisega seotud riske, mis tulenevad teadmiste ja oskusteabe puudumisest turul, ja muuta käesolevast määrusest tulenevate kohustuste täitmine pakkujate, eelkõige VKEde ning teavitatud asutuste jaoks hõlpsamaks, peaksid eeskätt tehisintellekti nõudeplatvorm, Euroopa digitaalse innovatsiooni keskused ning komisjoni ja liikmesriikide poolt riigi või ELi tasandil loodud testimis- ja eksperimenteerimisrajatised võimaluse korral aitama kaasa käesoleva määruse rakendamisele. Need asutused võivad pakkuda teavitatud asutustele ja pakkujatele oma vastavate ülesannete ja pädevusvaldkondade piires eeskätt tehnilist ja teaduslikku tuge.

(74a) Selleks et tagada proportsionaalsus seoses innovatsioonikuludega, võttes arvesse mõne operaatori väga väikest suurust, on asjakohane vabastada mikroettevõtjad kõige kulukamatest kohustustest, näiteks kohustusest kehtestada kvaliteedijuhtimise süsteem, kuna see vähendaks nende ettevõtjate halduskoormust ja kulusid, ilma et see mõjutaks kaitse taset ja vajadust täita suure riskiga tehisintellektisüsteemidele kehtestatud nõudeid.

(75) On otstarbekas, et komisjon hõlbustab võimaluste piires asjaomaste liidu ühtlustamisõigusaktide kohaselt loodud või akrediteeritud ning nende liidu ühtlustamisõigusaktide kohaldamisalasse kuuluvate toodete või seadmete vastavushindamise raames ülesandeid täitvate organite, rühmade või laborite juurdepääsu testimis- ja eksperimenteerimisrajatistele. Eeskätt kehtib see meditsiiniseadmete valdkonna eksperdirühmade, eksperdilaborite ja referentlaborite kohta vastavalt määrusele (EL) 2017/745 ja määrusele (EL) 2017/746.

(76) Et hõlbustada käesoleva määruse sujuvat, tulemuslikku ja ühtset rakendamist, tuleks luua Euroopa tehisintellekti nõukoda. Nõukoda peaks kajastama tehisintellekti ökosüsteemi erinevaid huve ja koosnema liikmesriikide esindajatest. Selleks et tagada asjaomaste sidusrühmade kaasamine, tuleks luua nõuandekoja alaline allrühm. Nõukoda peaks vastutama mitmesuguste nõustamisalaste ülesannete eest, sh arvamuste, soovituste ja nõuannete väljaandmine või osalemine suuniste andmises käesoleva määruse rakendamisega seotud küsimustes, muu hulgas jõustamise, tehniliste kirjelduste või kehtivate standardite kohta, mis puudutavad käesoleva määrusega kehtestatud nõudeid, ning komisjonile ja liikmesriikidele ning nende riigi pädevatele asutustele nõu andmine konkreetsetes tehisintellektiga seotud küsimustes. Selleks et anda liikmesriikidele teatav paindlikkus oma esindajate nimetamisel tehisintellekti nõukotta, võivad sellised esindajad olla avaliku sektori üksustesse kuuluvad mis tahes isikud, kellel peaksid olema asjakohased pädevused ja volitused, et hõlbustada koordineerimist riiklikul tasandil ja aidata kaasa nõukoja ülesannete täitmisele. Nõukoda peaks looma kaks alalist allrühma, et luua platvorm turujärelevalveasutuste ja teavitavate asutuste vaheliseks koostööks ja teabevahetuseks vastavalt turujärelevalve ja teavitatud asutustega seotud küsimustes. Turujärelevalve alaline allrühm peaks tegutsema käesoleva määruse kohaldamisel haldustegevuse koordineerimisrühmana määruse (EL) 2019/1020 artikli 30 tähenduses. Kooskõlas komisjoni rolli ja ülesannetega vastavalt määruse (EL) 2019/1020 artiklile 33 peaks komisjon toetama turujärelevalve alalise allrühma tegevust, viies läbi turuhindamisi või -uuringuid, eelkõige selleks, et teha kindlaks käesoleva määruse aspektid, mis nõuavad turujärelevalveasutuste vahelist konkreetset ja kiiret koordineerimist. Nõukoda võib vastavalt vajadusele moodustada konkreetsete küsimuste uurimiseks muid alalisi või ajutisi allrühmi. Nõukoda peaks tegema vajaduse korral koostööd ka asjakohaste ELi õigusaktide kontekstis tegutsevate asjaomaste ELi asutuste, eksperdirühmade ja võrgustikega, sealhulgas eelkõige nendega, kes tegutsevad andmeid, digitooteid ja -teenuseid käsitlevate asjakohaste ELi õigusaktide alusel.

(76a) Komisjon peaks aktiivselt toetama liikmesriike ja operaatoreid käesoleva määruse rakendamisel ja täitmise tagamisel. Sellega seoses peaks komisjon välja töötama suunised konkreetsete teemade kohta, mille eesmärk on hõlbustada käesoleva määruse kohaldamist, pöörates samal ajal erilist tähelepanu VKEde ja idufirmade vajadustele kõige tõenäolisemalt mõjutatavates sektorites. Selleks et toetada piisavat täitmise tagamist ja liikmesriikide suutlikkust, tuleks luua liidu tehisintellekti testimisrajatised ja asjaomaste ekspertide reserv ning teha need liikmesriikidele kättesaadavaks.

(77) Liikmesriikidel on käesoleva määruse kohaldamisel ja täitmise tagamisel tähtis roll. Seoses sellega peaks iga liikmesriik määrama ühe või mitu riigi pädevat asutust tegelema käesoleva määruse kohaldamise ja rakendamise järelevalvega. Liikmesriigid võivad otsustada määrata vastavalt oma riiklikele organisatsioonilistele iseärasustele ja vajadustele mis tahes avalik-õigusliku üksuse täitma käesoleva määruse tähenduses riigi pädeva asutuse ülesandeid.

(78) Tagamaks, et suure riskiga tehisintellektisüsteemide pakkujad saavad võtta oma süsteemide ja projekteerimis- ja arendusprotsessi parandamiseks arvesse suure riskiga tehisintellektisüsteemide kasutamise käigus saadud kogemusi või võtta õigeaegselt võimalikke parandusmeetmeid, peaks kõigil pakkujatel olema sisse seatud turustamisjärgse seire süsteem. Selline süsteem on oluline ka selleks, et saaks tõhusamalt ja õigeaegsemalt tegeleda riskidega, mis tulenevad tehisintellektisüsteemidest, mis n-ö õpivad edasi ka pärast turule laskmist või kasutusele võtmist. Seoses sellega tuleks pakkujatelt nõuda ka seda, et neil oleks olemas süsteem, et teatada asjaomastele asutustele mis tahes tõsistest intsidentidest, mille on põhjustanud nende tehisintellektisüsteemi kasutamine.

(79) Selleks et kindlustada liidu ühtlustamisõigusaktide hulka kuuluvas käesolevas määruses sätestatud nõuete ja kohustuste täitmise asjakohane ja tulemuslik tagamine, tuleks määrusega (EL) 2019/1020 kehtestatud toodete turujärelevalve ja nõuetele vastavuse süsteemi kohaldada täies ulatuses. Käesoleva määruse kohaselt määratud turujärelevalveasutustel peaksid olema kõik käesoleva määruse ja määruse (EL) 2019/1020 kohased täitmise tagamise volitused ning nad peaksid kasutama oma volitusi ja täitma oma kohustusi sõltumatult, erapooletult ja eelarvamusteta. Kuigi enamiku tehisintellektisüsteemide suhtes ei kohaldata käesoleva määruse kohaseid konkreetseid nõudeid ja kohustusi, võivad turujärelevalveasutused võtta meetmeid kõigi tehisintellektisüsteemide suhtes, kui need kujutavad endast ohtu vastavalt käesolevale määrusele. Käesoleva määruse kohaldamisalasse kuuluvate liidu institutsioonide, asutuste ja organite eripära tõttu on asjakohane määrata nende jaoks pädevaks turujärelevalveasutuseks Euroopa Andmekaitseinspektor. See ei tohiks piirata riikide pädevate asutuste määramist liikmesriikide poolt. Turujärelevalvetoimingud ei tohiks mõjutada järelevalve alla kuuluvate üksuste võimet täita oma ülesandeid sõltumatult, kui selline sõltumatus on nõutav liidu õigusega.

(79a) Käesolev määrus ei piira põhiõigusi kaitsva liidu õiguse kohaldamise järelevalvega tegelevate asjaomaste riiklike ametiasutuste või organite, sealhulgas võrdõiguslikkust edendavate asutuste ja andmekaitseasutuste pädevust, ülesandeid, volitusi ega sõltumatust. Kui see on nende volituste täitmiseks vajalik, peaks neil riiklikel ametiasutustel või organitel olema samuti juurdepääs kõigile käesoleva määruse alusel loodud dokumentidele. Tuleks kehtestada konkreetne kaitsemenetlus, et tagada piisav ja õigeaegne täitmise tagamine tehisintellektisüsteemide suhtes, mis kujutavad endast ohtu tervisele, ohutusele ja põhiõigustele. Selliste endast ohtu kujutavate tehisintellektisüsteemide jaoks kehtestatud menetlust tuleks kohaldada suure riskiga tehisintellektisüsteemide suhtes, mis kujutavad endast ohtu, keelatud süsteemide suhtes, mis on turule lastud, kasutusele võetud või mida kasutatakse käesolevas määruses sätestatud keelatud tavasid rikkudes, ning tehisintellektisüsteemide suhtes, mis on tehtud kättesaadavaks käesolevas määruses sätestatud läbipaistvusnõudeid rikkudes ja kujutavad endast ohtu.

(80) Finantsteenuseid käsitlevad liidu õigusaktid sisaldavad sisemise juhtimissüsteemi ja riskihalduse kohta käivaid õigusnorme ja nõudeid, mida kohaldatakse reguleeritud finantsasutuste suhtes kõnealuste teenuste pakkumise käigus, kaasa arvatud siis, kui nad kasutavad tehisintellektisüsteeme. Käesolevast määrusest tulenevate kohustuste ja finantsteenuseid käsitlevate liidu õigusaktide asjaomaste õigusnormide ja nõuete sidusa kohaldamise ja täitmise tagamiseks tuleks finantsteenuseid käsitlevate õigusaktide järelevalve ja täitmise tagamise eest vastutavad ametiasutused määrata pädevateks asutusteks, kes tegelevad käesoleva määruse rakendamise järelevalvega, sealhulgas turujärelevalvega, seoses reguleeritud ja järelevalve all olevate finantsasutuste pakutavate või kasutatavate tehisintellektisüsteemidega, välja arvatud juhul, kui liikmesriigid otsustavad määrata kõnealuseid turujärelevalveülesandeid täitma mõne muu asutuse. Kõnealustel pädevatel asutustel peaksid olema kõik käesolevast määrusest ja turujärelevalvet käsitlevast määrusest (EL) 2019/1020 tulenevad volitused tagada käesoleva määruse nõuete ja kohustuste täitmine, sealhulgas õigus viia läbi tagantjärele tehtavaid turujärelevalvetoiminguid, mida saab vajaduse korral integreerida nende olemasolevatesse, asjaomastest finantsteenuseid käsitlevatest liidu õigusaktidest tulenevatesse järelevalvemehhanismidesse ja -menetlustesse. Otstarbekas on näha ette, et käesoleva määruse alusel turujärelevalveasutusena tegutsevad riiklikud asutused, kes vastutavad direktiivi 2013/36/EL alusel reguleeritud krediidiasutuste järelevalve eest ja osalevad nõukogu määrusega (EL) nr 1024/2013 loodud ühtses järelevalvemehhanismis, peaksid viivitamata esitama Euroopa Keskpangale turujärelevalvetoimingute käigus kindlaks tehtud teabe, mis võib pakkuda huvi seoses kõnealuses määruses sätestatud Euroopa Keskpanga usaldatavusnõuete täitmise järelevalve ülesannetega. Et veelgi suurendada käesoleva määruse ning Euroopa Parlamendi ja nõukogu direktiivi 2013/36/EL[27] alusel reguleeritud krediidiasutuste suhtes kohaldatavate õigusnormide sidusust, on ühtlasi otstarbekas integreerida pakkujate mõned riskijuhtimise, turustamisjärgse seire ja dokumentatsiooniga seotud menetluslikud kohustused direktiivi 2013/36/EL kohaste olemasolevate kohustuste ja menetlustega. Kattuvuse vältimiseks tuleks ette näha ka piiratud erandid seoses pakkujate kvaliteedijuhtimissüsteemidega ja seirekohustusega, mis on pandud suure riskiga tehisintellektisüsteemide kasutajatele, niivõrd kuivõrd neid kohaldatakse direktiiviga

[27] Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta direktiiv 2013/36/EL, mis käsitleb krediidiasutuste tegevuse alustamise tingimusi ning krediidiasutuste ja investeerimisühingute usaldatavusnõuete täitmise järelevalvet, millega muudetakse direktiivi 2002/87/EÜ ning millega tunnistatakse kehtetuks direktiivid 2006/48/EÜ ja 2006/49/EÜ (ELT L 176, 27.6.2013, lk 338).

2013/36/EL reguleeritud krediidiasutuste suhtes. Sama korda tuleks kohaldada direktiivi 2009/138/EÜ (Solventsus II) kohaste kindlustus- ja edasikindlustusandjate ning kindlustusvaldusettevõtjate ning direktiivi (EL) 2016/97 kohaste kindlustusvahendajate suhtes ning muud liiki finantsasutuste suhtes, kelle suhtes kohaldatakse liidu finantsteenuseid käsitlevate asjakohaste õigusaktide kohaselt kehtestatud sisemise juhtimise, korra või protsessidega seotud nõudeid, et tagada järjepidevus ja võrdne kohtlemine finantssektoris.

(81) Muude tehisintellektisüsteemide kui suure riskiga tehisintellektisüsteemide arendamine kooskõlas käesoleva määruse nõuetega võib tuua kaasa usaldusväärse tehisintellekti laialdasema kasutamise liidus. Muude kui suure riskiga tehisintellektisüsteemide pakkujaid tuleks julgustada koostama käitumisjuhendeid, mille eesmärk on soodustada suure riskiga tehisintellektisüsteemide suhtes kohaldatavate nõuete vabatahtlikku kohaldamist ja mida on kohandatud süsteemide sihtotstarvet ja väiksemat riski arvesse võttes. Samuti tuleks pakkujaid julgustada kohaldama vabatahtlikult täiendavaid nõudeid, mis on seotud näiteks keskkonnasäästlikkusega, juurdepääsetavusega puuetega inimeste jaoks, sidusrühmade osalemisega tehisintellektisüsteemide projekteerimises ja arendamises ning arendusmeeskondade mitmekesisusega. Komisjon võib töötada välja algatusi, sh valdkondlikke algatusi, et aidata vähendada tehnilisi tõkkeid, mis takistavad tehisintellekti arendamise jaoks toimuvat piiriülest andmevahetust, keskendudes muu hulgas andmetele juurdepääsu taristule ning eri andmeliikide semantilisele ja tehnilisele koostalitlusvõimele.

(82) On oluline, et tehisintellektisüsteemid, mis on seotud toodetega, mis ei ole käesoleva määruse alusel suure riskiga ja mis seega ei pea vastama selles sätestatud nõuetele, oleksid siiski ohutud, kui need turule lastakse või kasutusele võetakse. Selle eesmärgi saavutamiseks kohaldatakse turvaabinõuna Euroopa Parlamendi ja nõukogu direktiivi 2001/95/EÜ[28].

(83) Pädevate asutuste usaldusliku ja konstruktiivse koostöö tagamiseks liidu ja riikide tasandil peaksid kõik käesoleva määruse kohaldamises osalejad austama oma ülesannete täitmise käigus saadud teabe ja andmete konfidentsiaalsust kooskõlas liidu või liikmesriigi õigusega.

[28] Euroopa Parlamendi ja nõukogu 3. detsembri 2001. aasta direktiiv 2001/95/EÜ üldise tooteohutuse kohta (EÜT L 11, 15.1.2002, lk 4).

(84) Liikmesriigid peaksid võtma kõik vajalikud meetmed, et tagada käesoleva määruse sätete rakendamine, sealhulgas kehtestades tõhusad, proportsionaalsed ja hoiatavad karistused nende rikkumise eest, järgides *ne bis in idem* põhimõtet. Teatavate konkreetsete rikkumiste puhul peaksid liikmesriigid võtma arvesse käesolevas määruses sätestatud piire ja kriteeriume. Euroopa Andmekaitseinspektoril peaks olema õigus määrata trahve käesoleva määruse kohaldamisalasse kuuluvatele liidu institutsioonidele, asutustele ja organitele.

(85) Tagamaks, et õigusraamistikku saab vajaduse korral kohandada, peaks komisjonil olema õigus võtta kooskõlas ELi toimimise lepingu artikliga 290 vastu delegeeritud õigusakte, et muuta II lisas loetletud liidu ühtlustamisõigusakte, III lisas loetletud suure riskiga tehisintellektisüsteeme, IV lisas loetletud tehnilist dokumentatsiooni käsitlevaid sätteid, V lisas esitatud ELi vastavusdeklaratsiooni sisu, VI ja VII lisas esitatud vastavushindamismenetlusi käsitlevaid sätteid ja sätteid, millega määratakse kindlaks need suure riskiga tehisintellektisüsteemid, mille suhtes tuleks kohaldada kvaliteedijuhtimissüsteemi ja tehnilise dokumentatsiooni hindamisel põhinevat vastavushindamist. On eriti oluline, et komisjon viiks oma ettevalmistava töö käigus läbi asjakohaseid konsultatsioone, sealhulgas ekspertide tasandil, ja et kõnealused konsultatsioonid viidaks läbi kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes[29] sätestatud põhimõtetega. Eelkõige selleks, et tagada delegeeritud õigusaktide ettevalmistamises võrdne osalemine, saavad Euroopa Parlament ja nõukogu kõik dokumendid liikmesriikide ekspertidega samal ajal ning nende ekspertidel on pidev juurdepääs komisjoni eksperdirühmade koosolekutele, millel arutatakse delegeeritud õigusaktide ettevalmistamist. Selliseid konsultatsioone ja nõustamistuge tuleks korraldada ka tehisintellekti nõukoja ja selle allrühmade tegevuse raames.

[29] ELT L 123, 12.5.2016, lk 1.

(86) Selleks et tagada käesoleva määruse ühetaolised rakendamistingimused, tuleks komisjonile anda rakendamisvolitused. Neid volitusi tuleks teostada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 182/2011[30]. On eriti oluline, et kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes sätestatud põhimõtetega kasutaks komisjon alati, kui rakendusaktide eelnõude ettevalmistamise varases etapis on vaja laiemaid eksperditeadmisi, vastavalt vajadusele eksperdirühmi, konsulteeriks sihtrühma kuuluvate sidusrühmadega või korraldaks avalikke konsultatsioone. Selliseid konsultatsioone ja nõustamistuge tuleks korraldada ka tehisintellekti nõukoja ja selle allrühmade tegevuse raames, sealhulgas artiklitega 4, 4b ja 6 seotud rakendusaktide ettevalmistamisel.

(87) Kuna käesoleva määruse eesmärki ei suuda liikmesriigid piisalt saavutada, küll aga saab seda meetmete ulatuse ja toime tõttu paremini saavutada liidu tasandil, võib liit võtta meetmeid kooskõlas ELi lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev määrus nimetatud eesmärgi saavutamiseks vajalikust kaugemale.

(87a) Selleks et tagada õiguskindlus, tagada operaatoritele asjakohane kohanemisaeg ja vältida turuhäireid, sealhulgas tagades tehisintellektisüsteemide kasutamise järjepidevuse, on asjakohane, et käesolevat määrust kohaldatakse suure riskiga tehisintellektisüsteemide suhtes, mis on turule lastud või kasutusele võetud enne käesoleva määruse üldist kohaldamiskuupäeva, ainult juhul, kui pärast nimetatud kuupäeva muudetakse oluliselt nende projekti või sihtotstarvet. On asjakohane selgitada, et sellega seoses tuleks olulise muutmise mõistet käsitada sisuliselt samaväärsena olulise muudatuse mõistega, mida kasutatakse ainult suure riskiga tehisintellektisüsteemide puhul, nagu need on käesolevas määruses määratletud.

[30] Euroopa Parlamendi ja nõukogu 16. veebruari 2011. aasta määrus (EL) nr 182/2011, millega kehtestatakse eeskirjad ja üldpõhimõtted, mis käsitlevad liikmesriikide läbiviidava kontrolli mehhanisme, mida kohaldatakse komisjoni rakendamisvolituste teostamise suhtes (ELT L 55, 28.2.2011, lk 13).

(88) Käesolevat määrust tuleks kohaldada alates … [*väljaannete talitus – palun sisestada artiklis 85 sätestatud kuupäev*]. Juhtimise ja vastavushindamissüsteemiga seotud taristu peaks hakkama toimima siiski juba enne nimetatud kuupäeva ning seepärast tuleks teavitatud asutusi ja juhtimisstruktuuri käsitlevaid sätteid kohaldada alates … [*väljaannete talitus – palun sisestada kuupäev: kolm kuud pärast käesoleva määruse jõustumist*]. Lisaks peaksid liikmesriigid nägema ette õigusnormid karistuste, kaasa arvatud haldustrahvide kohta, teatama neist komisjonile ning tagama, et need õigusnormid on käesoleva määruse kohaldamise kuupäevaks nõuetekohaselt ja tulemuslikult rakendatud. Seepärast tuleks karistusi käsitlevaid sätteid hakata kohaldama alates [*väljaannete talitus – palun sisestada kuupäev: kaksteist kuud pärast käesoleva määruse jõustumist*].

(89) Vastavalt määruse (EL) nr 2018/1725 artikli 42 lõikele 2 on konsulteeritud Euroopa Andmekaitseinspektori ja Euroopa Andmekaitsenõukoguga, kes esitasid oma arvamuse [...],

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I JAOTIS

ÜLDSÄTTED

Artikkel 1

Reguleerimisese

Käesoleva määrusega nähakse ette:

a) ühtlustatud õigusnormid, mis reguleerivad tehisintellektisüsteemide turule laskmist, kasutusele võtmist ja kasutamist liidus;

a) teatavate tehisintellekti kasutusviiside keelustamine;

b) erinõuded suure riskiga tehisintellektisüsteemidele ja selliste süsteemide operaatorite kohustused;

c) ühtlustatud läbipaistvusnormid teatavate tehisintellektisüsteemide jaoks;

d) turuseire, turujärelevalve ja juhtimise normid;

e) innovatsiooni toetavad meetmed.

Artikkel 2

Kohaldamisala

1. Käesolevat määrust kohaldatakse järgmise suhtes:

a) pakkujad, kes tegelevad liidus tehisintellektisüsteemide liidus turule laskmise või kasutusele võtmisega olenemata sellest, kas pakkuja füüsiline asukoht või tegevuskoht on liidus või kolmandas riigis;

b) tehisintellektisüsteemide kasutajad, kelle füüsiline asukoht või tegevuskoht on liidus;

c) tehisintellektisüsteemide pakkujad ja kasutajad füüsilise asukoha või tegevuskohaga kolmandas riigis, kui süsteemi väljundit kasutatakse liidus.

d) tehisintellektisüsteemide importijad ja turustajad;

e) toote valmistajad, kes lasevad tehisintellektisüsteemi turule või võtavad selle kasutusele koos oma tootega ja oma nime või kaubamärgi all;

f) liidus asuvad pakkujate volitatud esindajad.

2. Artikli 6 lõigete 1 ja 2 kohaste suure riskiga tehisintellektisüsteemide puhul, mis on seotud II lisa B jaos loetletud liidu ühtlustamisõigusaktidega hõlmatud toodetega, kohaldatakse üksnes käesoleva määruse artiklit 84. Artiklit 53 kohaldatakse üksnes niivõrd, kuivõrd käesoleva määruse kohased suure riskiga tehisintellektisüsteemidele esitatavad nõuded on nendesse liidu ühtlustamisõigusaktidesse integreeritud.

3. Käesolevat määrust ei kohaldata tehisintellektisüsteemide suhtes, juhul ja sel määral mil need lastakse turule, võetakse kasutusele või neid kasutatakse muudetud või muutmata kujul sellise tegevuse eesmärgil, mis ei kuulu liidu õiguse kohaldamisalasse, ning igal juhul sõjalise, kaitse- või riikliku julgeolekuga seotud tegevuse suhtes, olenemata seda tegevust teostava üksuse liigist.

   Lisaks ei kohaldata käesolevat määrust tehisintellektisüsteemide suhtes, mida ei lasta turule ega võeta kasutusele liidus, kui väljundit kasutatakse liidus tegevuseks, mis ei kuulu liidu õiguse kohaldamisalasse, ning igal juhul sõjalise, kaitse- või riikliku julgeolekuga seotud tegevuseks, olenemata seda tegevust teostava üksuse liigist.

4. Käesolevat määrust ei kohaldata kolmanda riigi ametiasutuste ega vastavalt lõikele 1 käesoleva määruse kohaldamisalasse kuuluvate rahvusvaheliste organisatsioonide suhtes, kui need asutused või organisatsioonid kasutavad tehisintellektisüsteeme liidu või ühe või mitme liikmesriigiga õiguskaitse ja õigusalase koostöö jaoks sõlmitud rahvusvaheliste lepingute raames.

5. Käesolev määrus ei mõjuta Euroopa Parlamendi ja nõukogu direktiivi 2000/31/EÜ[31] II peatüki 4. jaos sätestatud vahendajatest teenuseosutajate vastutust käsitlevate sätete [*asendatakse digiteenuste õigusakti vastavate sätetega*] kohaldamist.

6. Käesolevat määrust ei kohaldata tehisintellektisüsteemide, sealhulgas nende väljundite suhtes, mis on spetsiaalselt välja töötatud ja kasutusele võetud üksnes teadus- ja arendustegevuse eesmärgil.

7. Käesolevat määrust ei kohaldata tehisintellektisüsteemidega seotud teadus- ja arendustegevuse suhtes.

8. Käesolevat määrust ei kohaldata isikliku, mitte kutselise tegevuse käigus tehisintellektisüsteeme kasutavate füüsiliste isikute kohustuste suhtes, välja arvatud artikkel 52.

---

[31] Euroopa Parlamendi ja nõukogu 8. juuni 2000. aasta direktiiv 2000/31/EÜ infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul (direktiiv elektroonilise kaubanduse kohta) (EÜT L 178, 17.7.2000, lk 1).

Artikkel 3

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) „tehisintellektisüsteem“ – süsteem, mis on projekteeritud töötama teatava autonoomsusega ning mis teeb masina ja/või inimese antud andmete ja sisendite alusel järeldusi, kuidas saavutada masinõppe ja/või loogika- ja teadmistepõhiseid lähenemisviise kasutades teatavaid eesmärke, ning mis toodab süsteemi genereeritud väljundeid, nagu sisu (generatiivsed tehisintellektisüsteemid), prognoosid, soovitused või otsused, mis mõjutavad keskkonda, millega tehisintellektisüsteem suhtleb;

1a) „tehisintellektisüsteemi elutsükkel“ – tehisintellektisüsteemi kestus projekteerimisest kuni kasutusest kõrvaldamiseni. Ilma et see mõjutaks turujärelevalveasutuste volitusi, võib selline kasutusest kõrvaldamine toimuda pakkuja otsuse alusel mis tahes ajahetkel turustamisjärgse seire etapi jooksul ning see tähendab, et süsteemi ei tohi enam kasutada. Tehisintellektisüsteemi elutsükkel lõpeb ka siis, kui pakkuja või mis tahes muu füüsiline või juriidiline isik teeb tehisintellektisüstemi olulise muudatuse, millisel juhul peetakse oluliselt muudetud tehisintellektisüsteemi uueks tehisintellektisüsteemiks.

1b) „üldotstarbeline tehisintellektisüsteem“ – tehisintellektisüsteem, mis olenemata sellest, kuidas see turule lastakse või kasutusele võetakse, sealhulgas avatud lähtekoodiga tarkvarana, on pakkuja poolt mõeldud täitma üldkohaldatavaid funktsioone, nagu kujutise ja kõne tuvastus, audio ja video loomine, mustrite tuvastamine, küsimustele vastamine, tõlkimine ja muud; üldotstarbeline tehisintellektisüsteem on kasutatav mitmesugustes kontekstides ja integreeritav paljudesse teistesse tehisintellektisüsteemidesse;

2) „pakkuja“ – füüsiline või juriidiline isik, ametiasutus, ametkond või muu organ, kes töötab välja tehisintellektisüsteemi või laseb tehisintellektisüsteemi välja töötada ning laseb selle turule või võtab kasutusele oma nime või kaubamärgi all kas tasu eest või tasuta;

3) [välja jäetud]

3a) „väikesed ja keskmise suurusega ettevõtjad“ (VKEd) – ettevõtjad, nagu need on määratletud komisjoni soovituse 2003/361/EÜ (mikroettevõtjate, väikeste ja keskmise suurusega ettevõtjate määratluse kohta) lisas;

4) „kasutaja“ – füüsiline või juriidiline isik, sealhulgas ametiasutus, ametkond või muu organ, kelle volituste alusel süsteemi kasutatakse;

5) „volitatud esindaja“ – füüsiline või juriidiline isik, kelle füüsiline asukoht või tegevuskoht on liidus ja kes on saanud tehisintellektisüsteemi pakkujalt kirjaliku volituse täita käesoleva määrusega kehtestatud kohustusi ja sooritada menetlusi tema nimel ning on selle volituse vastu võtnud;

5a) „toote valmistaja“ – tootja II lisas loetletud liidu ühtlustamisõigusaktide tähenduses;

6) „importija“ – füüsiline või juriidiline isik, kelle füüsiline asukoht või tegevuskoht on liidus ja kes laseb turule väljaspool liitu asuva füüsilise või juriidilise isiku nime või kaubamärki kandva tehisintellektisüsteemi;

7) „turustaja“ – füüsiline või juriidiline isik tarneahelas, välja arvatud pakkuja või importija, kes teeb tehisintellektisüsteemi liidu turul kättesaadavaks;

8) „operaator“ – pakkuja, toote valmistaja, kasutaja, volitatud esindaja, importija või turustaja;

9) „turule laskmine“ – tehisintellektisüsteemi liidu turul esmakordselt kättesaadavaks tegemine;

10) „turul kättesaadavaks tegemine“ – tehisintellektisüsteemi tasu eest või tasuta tarnimine liidu turule kaubandustegevuse käigus kas turustamiseks või kasutamiseks;

11) „kasutusele võtmine“ – tehisintellektisüsteemi tarnimine esmakordseks kasutamiseks otse kasutajale või oma tarbeks, et kasutada seda sihtotstarbeliselt liidus;

12) „sihtotstarve“ – kasutus, kaasa arvatud kasutamise konkreetne kontekst ja tingimused, mille jaoks pakkuja on tehisintellektisüsteemi kasutusjuhendis, reklaam- või müügimaterjalides või avaldustes ning tehnilistes dokumentides esitatud teabe kohaselt ette näinud;

13) „mõistlikult prognoositav väärkasutamine“ – tehisintellektisüsteemi kasutamine viisil, mis ei ole kooskõlas selle sihtotstarbega, kuid mis võib tuleneda põhjendatult prognoositavast inimkäitumisest või interaktsioonist muude süsteemidega;

14) „toote või süsteemi turvakomponent“ – toote või süsteemi komponent, mis täidab selle toote või süsteemi ohutusfunktsiooni või mille tõrge või talitlushäire ohustab inimeste tervist ja ohutust või vara;

15) „kasutusjuhend“ – teave, mille pakkuja esitab, et teavitada kasutajat eeskätt tehisintellektisüsteemi kasutusotstarbest ja nõuetekohasest kasutamisest;

16) „tehisintellektisüsteemi tagasikutsumine“ – mis tahes meede, mille eesmärk on saavutada kasutajatele kättesaadavaks tehtud tehisintellektisüsteemi tagastamine pakkujale või selle kasutusest kõrvaldamine või selle kasutamise keelamine;

17) „tehisintellektisüsteemi turult kõrvaldamine“ – mis tahes meede, mille eesmärk on hoida ära tarneahelas oleva tehisintellektisüsteemi turul kättesaadavaks tegemist;

18) „tehisintellektisüsteemi toimimine“ – tehisintellektisüsteemi suutlikkus täita talle seatud sihtotstarvet;

19) „vastavushindamine“ – protsess, mille käigus kontrollitakse, kas suure riskiga tehisintellektisüsteemi kohta käesoleva määruse III jaotise 2. peatükis sätestatud nõuded on täidetud;

20) „teavitav asutus“ – riigi ametiasutus, kes vastutab vastavushindamisasutuste hindamise, määramise ja neist teavitamise ning nende seire jaoks vajalike menetluste väljatöötamise ja läbiviimise eest;

21) „vastavushindamisasutus“ – asutus, kes teeb kolmanda isikuna vastavushindamise toiminguid, sealhulgas testimist, sertifitseerimist ja kontrollimist;

22) „teavitatud asutus“ – käesoleva määruse ja liidu muude asjaomaste ühtlustamisalaste õigusaktide kohaselt määratud vastavushindamisasutus;

23) „oluline muudatus“ – tehisintellektisüsteemis pärast selle turule laskmist või kasutusele võtmist tehtud muudatus, mis mõjutab tehisintellektisüsteemi vastavust käesoleva määruse III jaotise 2. peatükis sätestatud nõuetele, või muudatus kasutusotstarbes, mida silmas pidades on tehisintellektisüsteemi hinnatud. Kui tegemist on suure riskiga tehisintellektisüsteemiga, mis õpib edasi ka pärast turule laskmist või kasutusele võtmist, ei käsitata oluliste muudatustena tehisintellektisüsteemi ja selle toimimise muudatusi, mis on pakkuja poolt esialgse vastavushindamise ajal paika pandud ja mis sisalduvad IV lisa punkti 2 alapunktis f osutatud tehnilises dokumentatsioonis.

24) „CE-vastavusmärgis“ või „CE-märgis“ – märgis, millega pakkuja annab teada, et tehisintellektisüsteem vastab käesoleva määruse III jaotise 2. peatükis või artiklis 4b ja muudes kohaldatavates toodete turustamise tingimusi ühtlustavates liidu õigusaktides (edaspidi „liidu ühtlustamisõigusaktid“) sätestatud märgise paigaldamist käsitlevatele nõuetele;

25) „turustamisjärgse seire süsteem“ – igasugune tehisintellektisüsteemi pakkuja tegevus, et koguda ja läbi vaadata tema poolt turule lastud või kasutusele võetud tehisintellektisüsteemide kasutamise käigus saadud kogemusi, eesmärgiga teha kindlaks juhud, kui tuleb viivitamata võtta vajalikke parandus- või ennetusmeetmeid;

26) „turujärelevalveasutus“ – riigi ametiasutus, kes teeb toiminguid ja võtab meetmeid vastavalt määrusele (EL) 2019/1020;

27) „harmoneeritud standard“ – määruse (EL) nr 1025/2012 artikli 2 lõike 1 punktis c määratletud Euroopa standard;

28) „ühtne kirjeldus“ – kogum tehnilistest spetsifikatsioonidest, nagu on määratletud määruse (EL) nr 1025/2012 artikli 2 punktis 4, mille abil täita teatavaid käesoleva määrusega kehtestatud nõudeid;

29) „treeningandmed“ – andmed, mida kasutatakse tehisintellektisüsteemi treenimiseks läbi õpiparameetrite sobituse;

30) „valideerimisandmed“ – andmed, mida kasutatakse treenitud tehisintellektisüsteemi hindamiseks ning selle mitteõpitavate parameetrite ja õppimisprotsessi reguleerimiseks, muu hulgas selleks, et hoiduda ülesobitamisest; sealjuures võib valideerimisandmestik olla kas eraldi andmestik või treeningandmestiku osa kindlaksmääratud või muutuva jaotuse alusel;

31) „testandmed“ – andmed, mida kasutatakse sõltumatu hinnangu andmiseks treenitud ja valideeritud tehisintellektisüsteemile, et kinnitada selle süsteemi toimimise eeldustekohasust, enne kui süsteem lastakse turule või võetakse kasutusele;

32) „sisendandmed“ – andmed, mis esitatakse tehisintellektisüsteemile või mille tehisintellektisüsteem vahetult saab ning mille põhjal süsteem genereerib väljundi;

33) „biomeetrilised andmed“ – konkreetse tehnilise töötlemise abil saadavad isikuandmed füüsilise isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, näiteks näokujutis ja sõrmejälgede andmed;

34) „emotsioonituvastussüsteem“ – tehisintellektisüsteem, mille eesmärk on tuvastada või tuletada füüsiliste isikute psühholoogilisi seisundeid, emotsioone või kavatsusi nende biomeetriliste andmete põhjal;

35) „biomeetrilise liigitamise süsteem“ – tehisintellektisüsteem, mille eesmärk on jagada füüsilisi isikuid nende biomeetriliste andmete põhjal teatavatesse kategooriatesse;

36) „biomeetrilise kaugtuvastamise süsteem“ – tehisintellektisüsteem, mille eesmärk on tuvastada füüsilisi isikuid tavaliselt eemalt ilma nende aktiivse osaluseta, võrreldes isiku biomeetrilisi andmeid võrdlusandmehoidlas sisalduvate biomeetriliste andmetega;

37) „reaalajas toimuva biomeetrilise kaugtuvastamise süsteem“ – biomeetrilise kaugtuvastamise süsteem, milles biomeetriliste andmete hõive, võrdlemine ja tuvastamine toimub hetkega või peaaegu hetkega;

38) [välja jäetud]

39) „avalikult juurdepääsetav ruum“ – avalikus või eraomandis füüsiline koht, millele on juurdepääs määramatul arvul füüsilistel isikutel, olenemata sellest, kas eelnevalt on kindlaks määratud teatavad juurdepääsutingimused või -asjaolud, ja olenemata võimalikest mahutavuspiirangutest;

40) „õiguskaitseasutus“ –

a) ametiasutus, kes on pädev kuritegusid tõkestama, uurima, avastama või nende eest vastutusele võtma või kriminaalkaristusi täitmisele pöörama, sealhulgas kaitsma avalikku julgeolekut ähvardavate ohtude eest ja neid ohte ennetama, või

b) muu asutus või üksus, kes teostab liikmesriigi õiguse kohaselt avalikku võimu kuritegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil;

41) „õiguskaitse“ – tegevus, mida õiguskaitseasutus teostab või mida teostatakse õiguskaitseasutuse nimel kuritegude tõkestamiseks, uurimiseks, avastamiseks või nende eest vastutusele võtmiseks või kriminaalkaristuse täitmisele pööramiseks, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmiseks ja nende ohtude ennetamiseks;

42) [välja jäetud]

43) „riigi pädev asutus“ – üks järgmistest: teavitav asutus või turujärelevalveasutus. ELi institutsioonide, ametite, asutuste, ja organite poolt kasutusele võetud või kasutatavate tehisintellektisüsteemide puhul täidab neid ülesandeid, mis liikmesriikides on antud riikide pädevatele asutustele, Euroopa Andmekaitseinspektor ning kui see on asjakohane, käsitatakse käesolevas määruses toodud mis tahes viiteid riikide pädevatele asutustele või turujärelevalveasutustele viidetena Euroopa Andmekaitseinspektorile;

44) „tõsine intsident“ – juhtum või tõrge tehisintellektisüsteemis, mis otseselt või kaudselt põhjustab ühe järgmistest tagajärgedest:

a) inimese surm või tõsine kahju inimese tervisele;

b) elutähtsa taristu juhtimise ja käitamise tõsine ja pöördumatu katkemine;

c) põhiõiguste kaitsmiseks loodud liidu õigusest tulenevate kohustuste rikkumine;

d) tõsine kahju varale või keskkonnale.

45) „elutähtis taristu“ – vara, süsteem või selle osa, mis on vajalik sellise teenuse osutamiseks, mis on hädavajalik elutähtsate ühiskondlike funktsioonide või majandustegevuse säilitamiseks kriitilise tähtsusega üksuste vastupidavusvõimet käsitleva direktiivi …/... artikli 2 lõigete 4 ja 5 tähenduses;

46) „isikuandmed“ – määruse (EL) 2016/679 artikli 4 punktis 1 määratletud andmed;

47) „isikustamata andmed“ – muud andmed kui isikuandmed, mis on määratletud määruse (EL) 2016/679 artikli 4 punktis 1;

48) „tegelikes tingimustest testimine“ – tehisintellektisüsteemi ajutine testimine selle sihtotstarbe jaoks tegelikes tingimustes väljaspool laborit või muul moel simuleeritud keskkonda, eesmärgiga koguda usaldusväärseid ja stabiilseid andmeid ning hinnata ja kontrollida tehisintellektisüsteemi vastavust käesoleva määruse nõuetele; tegelikes tingimustes testimist ei peeta tehisintellektisüsteemi turule laskmiseks või kasutusele võtmiseks käesoleva määruse tähenduses, eeldusel et täidetud on kõik artikli 53 või 54a kohased tingimused;

49) „tegelikes tingimustes testimise kava“ – dokument, milles kirjeldatakse tegelikes tingimustes testimise eesmärke, meetodeid, geograafilist, rahvastikuga seotud ja ajalist ulatust, järelevalvet, korraldust ja läbiviimist;

50) „subjekt“ – tegelikes tingimustes testimise kontekstis füüsiline isik, kes osaleb tegelikes tingimustes testimises;

51) „teadev nõusolek“ – subjekti vaba ja vabatahtlik väljendus oma tahtest osaleda teatavas tegelikes tingimustes toimuvas testimises pärast seda, kui teda on teavitatud testimise kõikidest aspektidest, mis on subjekti osalemisotsuse jaoks asjakohased; alaealiste ja piiratud teovõimega subjektide puhul annab teadva nõusoleku nende seaduslik esindaja;

52) „tehisintellekti regulatsiooni testkeskkond“ – riigi pädeva asutuse loodud konkreetne raamistik, mis pakub tehisintellektisüsteemide pakkujatele või võimalikele pakkujatele võimalust arendada, treenida, valideerida ja testida innovatiivset tehisintellektisüsteemi asjakohastel juhtudel tegelikes tingimustes ning konkreetse kava kohaselt piiratud aja jooksul regulatiivse järelevalve all.

Artikkel 4

Rakendusaktid

Selleks et tagada käesoleva määruse ühetaolised rakendamistingimused masinõppe lähenemisviiside ning loogika- ja teadmistepõhiste lähenemisviiside osas, millele on viidatud artikli 3 punktis 1, võib komisjon võtta vastu rakendusakte, et täpsustada nende lähenemisviiside tehnilisi elemente, võttes arvesse turu ja tehnoloogia arengut. Need rakendusaktid võetakse vastu kooskõlas artikli 74 lõikes 2 osutatud kontrollimenetlusega.

IA JAOTIS

ÜLDOTSTARBELISED TEHISINTELLEKTISÜSTEEMID

Artikkel 4a

Üldotstarbeliste tehisintellektisüsteemide vastavus käesolevale määrusele

1. Ilma et see mõjutaks käesoleva määruse artiklite 5, 52, 53 ja 69 kohaldamist, peavad üldotstarbelised tehisintellektisüsteemid vastama üksnes artiklis 4b sätestatud nõuetele ja kohustustele.

2. Selliseid nõudeid ja kohustusi kohaldatakse olenemata sellest, kas üldotstarbeline tehisintellektisüsteem lastakse turule või võetakse kasutusele eeltreenitud mudelina või kas üldotstarbelise tehisintellektisüsteemi kasutaja viimistleb mudelit täiendavalt.

Artikkel 4b

Nõuded üldotstarbelistele tehisintellektisüsteemidele ning selliste süsteemide pakkujate kohustused

1. Üldotstarbelised tehisintellektisüsteemid, mida võib kasutada suure riskiga tehisintellektisüsteemidena või suure riskiga tehisintellektisüsteemide komponentidena artikli 6 tähenduses, peavad vastama käesoleva määruse III jaotise 2. peatükis kehtestatud nõuetele alates kuupäevast, millal hakatakse kohaldama komisjoni poolt kooskõlas artikli 74 lõikes 2 osutatud kontrollimenetlusega vastu võetud rakendusakte, ning mitte hiljem kui 18 kuud pärast käesoleva määruse jõustumist. Nendes rakendusaktides täpsustatakse ja kohandatakse III jaotise 2. peatükis kehtestatud nõuete kohaldamist üldotstarbeliste tehisintellektisüsteemide suhtes, võttes arvesse nende eriomadusi, tehnilist teostatavust, tehisintellekti väärtusahela ja turu iseärasusi ning tehnoloogia arengut. Nende nõuete täitmise puhul võetakse arvesse tehnika üldtunnustatud taset.

2. Lõikes 1 osutatud üldotstarbeliste tehisintellektisüsteemide pakkujad peavad alates lõikes 1 osutatud rakendusaktide kohaldamise alguskuupäevast täitma kohustusi, mis on sätestatud artiklites 16aa, 16e, 16f, 16g, 16i, 16j, 25, 48 ja 61.

3. Artiklis 16e sätestatud kohustuste täitmiseks järgivad pakkujad sisekontrollil põhinevat vastavushindamist, nagu on sätestatud VI lisa punktides 3 ja 4.

4. Selliste süsteemide pakkujad hoiavad artiklis 11 osutatud tehnilist dokumentatsiooni riikide pädevatele asutustele kättesaadavana kuni kümme aastat pärast üldotstarbelise tehisintellektisüsteemi liidu turule laskmist või liidus kasutusele võtmist.

5. Üldotstarbeliste tehisintellektisüsteemide pakkujad teevad koostööd teiste pakkujatega, kes kavatsevad selliseid süsteeme suure riskiga tehisintellektisüsteemidena või suure riskiga tehisintellektisüsteemide komponentidena kasutusele võtta või liidu turule lasta, ning edastavad neile vajalikku teavet, eesmärgiga võimaldada teistel pakkujatel täita oma kohustusi, mis tulenevad käesolevast määrusest. Sellise pakkujatevahelise koostöö puhul kaitstakse, kui see on asjakohane, intellektuaalomandiõigusi ning konfidentsiaalset äriteavet ja ärisaladusi kooskõlas artikliga 70. Selleks et tagada käesoleva määruse ühetaolised rakendamistingimused seoses üldotstarbeliste tehisintellektisüsteemide pakkujate jagatava teabega, võib komisjon võtta kooskõlas artikli 74 lõikes 2 osutatud kontrollimenetlusega vastu rakendusakte.

6. Lõigetes 1, 2 ja 3 osutatud nõuete ja kohustuste järgimise puhul:

- käsitatakse mis tahes viidet sihtotstarbele viitena üldotstarbeliste tehisintellektisüsteemide võimalikule kasutamisele suure riskiga tehisintellektisüsteemidena või suure riskiga tehisintellektisüsteemide komponentidena artikli 6 tähenduses;

- käsitatakse mis tahes viidet suure riskiga tehisintellektisüsteemidele esitatavatele nõuetele III jaotise II peatükis viitena üksnes käesolevas artiklis sätestatud nõuetele.

Artikkel 4c

Erandid artiklist 4b

1. Artiklit 4b ei kohaldata, kui pakkuja on üldotstarbelise tehisintellektisüsteemi kasutusjuhendis või süsteemiga kaasnevas teabes sõnaselgelt välistanud kõik suure riskiga kasutusviisid.

2. Selline erand tehakse heas usus ning seda ei peeta õigustatuks, kui pakkujal on piisavalt põhjuseid uskuda, et süsteemi võib väärkasutada.

3. Kui pakkuja avastab väärkasutamise turul või kui talle sellest teatatakse, võtab ta kõik vajalikud ja proportsionaalsed meetmed sellise väärkasutamise ennetamiseks tulevikus, võttes eeskätt arvesse väärkasutamise ulatust ning kaasnevate riskide tõsidust.

II JAOTIS

TEHISINTELLEKTI KEELATUD KASUTUSVIISID

Artikkel 5

1. Järgmised tehisintellekti kasutusviisid on keelatud:

a) selliste tehisintellektisüsteemide turule laskmine, kasutusele võtmine või kasutamine, milles on kasutatud inimese teadvusest kaugemale ulatuvale alalävisele tajule suunatud võtteid ning mille eesmärk või tagajärg on oluliselt moonutada isiku käitumist viisil, mis põhjustab või mõistliku tõenäosusega põhjustab sellele või mõnele teisele isikule füüsilist või psühholoogilist kahju;

b) selliste tehisintellektisüsteemide turule laskmine, kasutusele võtmine või kasutamine, mis kasutavad ära konkreetse isikute rühma mis tahes haavatavusi, mis tulenevad nende vanusest, puudest või konkreetsest sotsiaalsest või majanduslikust olukorrast ning mille eesmärk või tagajärg on oluliselt moonutada sellesse rühma kuuluva isiku käitumist viisil, mis põhjustab või mõistliku tõenäosusega põhjustab sellele või mõnele teisele isikule füüsilist või psühholoogilist kahju;

c) selliste tehisintellektisüsteemide turule laskmine, kasutusele võtmine või kasutamine, millega hinnatakse või liigitatakse füüsilisi isikuid teatava aja jooksul, lähtudes nende sotsiaalsest käitumisest või teadaolevatest või prognoositud iseloomulikest või isikuomadustest, kusjuures ühiskondliku reitingu tulemuseks on üks või mõlemad järgmisest:

i) teatavaid füüsilisi isikuid või füüsiliste isikute rühmi kahjustav või nende suhtes ebasoodne kohtlemine sotsiaalses kontekstis, mis ei ole seotud kontekstiga, milles andmed algselt loodi või koguti;

ii) teatavaid füüsilisi isikuid või füüsiliste isikute rühmi kahjustav või nende suhtes ebasoodne kohtlemine, mis ei ole põhjendatud või on ebaproportsionaalne võrreldes nende sotsiaalse käitumise või selle kaalukusega;

d) avalikult juurdepääsetavas ruumis reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine õiguskaitseasutuste poolt või nende nimel õiguskaitse jaoks, välja arvatud juhul, kui selline kasutamine on vajalik rangelt ainult ühel järgmistest eesmärkidest, ja ainult selleks vajalikus ulatuses:

i) konkreetsete võimalike kuriteoohvrite sihipärane otsimine;

ii) elutähtsat taristut, füüsiliste isikute elu, tervist või füüsilist turvalisust ähvardava konkreetse ja suure ohu või terrorirünnaku ärahoidmine;

iii) füüsilise isiku asukoha või isikusamasuse kindlaks tegemine nõukogu raamotsuse 2002/584/JSK[32] artikli 2 lõikes 2 osutatud sellise kuriteo uurimise, selle eest süüdistuse esitamise või kriminaalkaristuse täitmisele pööramise eesmärgil, mille eest karistatakse asjaomases liikmesriigis vabadusekaotuse või vabadust piirava julgeolekumeetmega, mille maksimaalne pikkus on vähemalt kolm aastat, või muude spetsiifiliste kuritegude puhul, mille eest karistatakse asjaomases liikmesriigis vabadusekaotuse või vabadust piirava julgeolekumeetmega, mille maksimaalne pikkus on vähemalt viis aastat, nagu selle liikmesriigi õigusaktides kindlaks määratud.

2. Kui reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutatakse avalikult juurdepääsetavas ruumis õiguskaitse jaoks ükskõik millisel lõike 1 punktis d osutatud eesmärgil, võetakse arvesse järgmisi elemente:

a) millist laadi on olukord, kus süsteemi võidakse kasutada; eeskätt see, milline oleks kahju raskusaste, tõenäosus ja ulatus juhul, kui süsteemi ei kasutata;

[32] Nõukogu 13. juuni 2002. aasta raamotsus 2002/584/JSK Euroopa vahistamismääruse ja liikmesriikidevahelise üleandmiskorra kohta (EÜT L 190, 18.7.2002, lk 1).

b) millised on süsteemi kasutamise tagajärjed kõigi asjaomaste isikute õiguste ja vabaduste seisukohast; eeskätt see, milline on tagajärgede raskusaste, tõenäosus ja ulatus.

Ühtlasi peab reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine avalikult juurdepääsetavas ruumis õiguskaitse jaoks ükskõik millisel lõike 1 punktis d osutatud eesmärgil olema vastavuses kasutamise suhtes kehtivate vajalike ja proportsionaalsete kaitsemeetmete ja tingimustega ning seda eeskätt ajaliste, geograafiliste ja isikutega seotud piirangute osas.

3. Lõike 1 punkti d ja lõike 2 puhul on reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi igaks kasutamiseks avalikult juurdepääsetavas ruumis vaja eelnevat luba, mille annab selle liikmesriigi õigusasutus või sõltumatu haldusasutus, kus kasutamine hakkab toimuma, ja mis antakse põhjendatud taotluse põhjal kooskõlas lõikes 4 osutatud üksikasjalike siseriiklike õigusnormidega. Nõuetekohaselt põhjendatud kiireloomulistel juhtudel võib siiski hakata süsteemi kasutama ilma loata, eeldusel et sellist luba taotletakse põhjendamatu viivituseta tehisintellektisüsteemi kasutamise ajal ning, kui loa andmisest keeldutakse, lõpetatakse süsteemi kasutamine viivitamatult.

Pädev õigus- või haldusasutus annab loa üksnes juhul, kui on talle esitatud objektiivsete tõendite või selgete asjaolude valguses veendunud, et kõnealuse reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine on vajalik ja proportsionaalne mõne lõike 1 punktis d täpsustatud ja taotluses nimetatud eesmärgi saavutamiseks. Pädev õigus- või haldusasutus teeb taotluse kohta otsuse, võttes arvesse lõikes 2 osutatud elemente.

4. Liikmesriik võib otsustada näha ette võimaluse osaliselt või täielikult lubada reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamist avalikult juurdepääsetavas ruumis õiguskaitse jaoks lõike 1 punktis d ning lõigetes 2 ja 3 loetletud piirides ja tingimustel. Selline liikmesriik kehtestab oma siseriiklikus õiguses lõikes 3 osutatud lubade taotlemise, andmise ja kasutamise ning nende lubadega seotud järelevalve ja aruandluse jaoks vajalikud üksikasjalikud õigusnormid. Kõnealustes õigusnormides tuleb täpsustada, milliste lõike 1 punktis d loetletud eesmärkide, sealhulgas milliste selle punkti alapunktis iii osutatud kuritegude puhul võib anda pädevatele asutustele loa kasutada neid süsteeme õiguskaitse jaoks.

III JAOTIS

SUURE RISKIGA TEHISINTELLEKTISÜSTEEMID

1. PEATÜKK

TEHISINTELLEKTISÜSTEEMI LIIGITAMINE SUURE RISKIGA TEHISINTELLEKTISÜSTEEMIKS

Artikkel 6

Suure riskiga tehisintellektisüsteemide liigitamise reeglid

1. Tehisintellektisüsteemi, mis on ise toode, mille suhtes kehtivad II lisas loetletud liidu ühtlustamisõigusaktid, käsitatakse suure riskiga süsteemina, kui see peab läbima kolmanda isiku tehtava vastavushindamise, et toote saaks turule lasta või kasutusele võtta vastavalt eespool nimetatud õigusaktidele.

2. Tehisintellektisüsteemi, mis on mõeldud kasutamiseks lõikes 1 osutatud õigusaktidega hõlmatud toote turvakomponendina, käsitatakse suure riskiga süsteemina, kui see peab läbima kolmanda isiku tehtava vastavushindamise, et toote saaks turule lasta või kasutusele võtta vastavalt eespool nimetatud õigusaktidele. Seda sätet kohaldatakse olenemata sellest, kas tehisintellektisüsteem lastakse turule või võetakse kasutusele tootest sõltumatult.

3. III lisas osutatud tehisintellektisüsteeme peetakse suure riskiga süsteemideks, välja arvatud siis, kui süsteemi väljund on asjaomase tegevuse või tehtava otsuse suhtes üksnes täiendav ning ei too seega tõenäoliselt kaasa olulist riski tervisele, ohutusele või põhiõigustele.

Selleks et tagada käesoleva määruse rakendamiseks ühetaolised tingimused, võtab komisjon hiljemalt üks aasta pärast käesoleva määruse jõustumist vastu rakendusaktid, et täpsustada tingimusi, mille puhul oleks III lisas osutatud tehisintellektisüsteemide väljund asjaomase tegevuse või tehtava otsuse suhtes üksnes täiendav. Need rakendusaktid võetakse vastu kooskõlas artikli 74 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 7

III lisa muutmine

1. Komisjonil on õigus võtta kooskõlas artikliga 73 vastu delegeeritud õigusakte, et muuta III lisas esitatud loetelu ja lisada sellesse suure riskiga tehisintellektisüsteeme, kui täidetud on mõlemad järgmised tingimused:

a) tehisintellektisüsteemid on mõeldud kasutamiseks mõnes III lisa punktides 1–8 loetletud valdkonnas;

b) tehisintellektisüsteemid võivad kahjustada tervist ja ohutust või avaldada negatiivset mõju põhiõigustele ning sellise riski raskusaste ja esinemise tõenäosus on samaväärne või suurem kui III lisas juba osutatud suure riskiga tehisintellektisüsteemide põhjustatud kahju või negatiivse mõju riski puhul.

2. Kui lõike 1 kohaldamisel hinnatakse, kas tehisintellektisüsteem võib kahjustada tervist ja ohutust või avaldada negatiivset mõju põhiõigustele ning sellise riski raskusaste ja esinemise tõenäosus on samaväärne või suurem kui III lisas juba osutatud suure riskiga tehisintellektisüsteemide põhjustatud kahju riski puhul, võtab komisjon arvesse järgmisi kriteeriume:

a) mis on tehisintellektisüsteemi sihtotstarve;

b) millises ulatuses on tehisintellektisüsteemi kasutatud või tõenäoliselt kasutatakse;

c) millises ulatuses on tehisintellektisüsteemi kasutamine juba teinud kahju tervisele ja ohutusele või avaldanud negatiivset mõju põhiõigustele või tekitanud tõsist muret, et selline kahju või negatiivne mõju võib tekkida, nagu on näidanud riikide pädevatele asutustele esitatud aruanded või dokumenteeritud väited;

d) milline oleks sellise kahju või negatiivse mõju võimalik ulatus, eeskätt intensiivsus ja võime mõjutada paljusid isikuid;

e) millises ulatuses sõltuvad potentsiaalselt kahjustatud või negatiivselt mõjutatud isikud tulemusest, milleni on jõutud tehisintellektisüsteemi abil, eeskätt seetõttu, et praktilistel või õiguslikel põhjustel ei ole mõistlikult võimalik loobuda selle tulemuse rakendamisest;

f) millises ulatuses on potentsiaalselt kahjustatud või negatiivselt mõjutatud isikud haavatavas olukorras võrreldes tehisintellektisüsteemi kasutajaga, eeskätt võimu, teadmiste, majanduslike või sotsiaalsete olude või vanusega seotud ebavõrdsuse tõttu;

g) millises ulatuses ei ole tehisintellektisüsteemi abil saavutatud tulemus kergesti tagasipööratav, kusjuures tulemust, millel on mõju inimeste tervisele või ohutusele, ei peeta kergesti tagasipööratavaks;

h) millises ulatuses on kehtivate liidu õigusaktidega ette nähtud:

i) mõjusad õiguskaitsevahendid seoses tehisintellektisüsteemist tulenevate riskidega, välja arvatud kahjunõuded;

ii) mõjusad meetmed, et neid riske ära hoida või neid oluliselt vähendada;

i) tehisintellekti kasutamisest üksikisikutele, rühmadele või ühiskonnale laiemalt tuleneva kasu suurus ja tõenäosus.

3. Komisjonil on õigus võtta kooskõlas artikliga 73 vastu delegeeritud õigusakte, et muuta III lisas esitatud loetelu ja jätta sellest välja suure riskiga tehisintellektisüsteeme, kui täidetud on mõlemad järgmised tingimused:

a) asjaomane suure riskiga tehisintellektisüsteem või sellised süsteemid ei tekita enam märkimisväärseid riske põhiõigustele, tervisele või ohutusele, võttes arvesse lõikes 2 loetletud kriteeriume;

b) väljajätmine ei vähenda liidu õiguse kohase tervise, ohutuse ja põhiõiguste kaitse üldist taset.

2. PEATÜKK

SUURE RISKIGA TEHISINTELLEKTISÜSTEEMIDELE ESITATAVAD NÕUDED

Artikkel 8

Nõuetelevastavus

1. Suure riskiga tehisintellektisüsteemid peavad vastama käesolevas peatükis kehtestatud nõuetele, võttes arvesse tehnika üldtunnustatud taset.

2. Neile nõuetele vastavuse tagamisel võetakse arvesse suure riskiga tehisintellektisüsteemi sihtotstarvet ja artiklis 9 osutatud riskijuhtimissüsteemi.

Artikkel 9

Riskijuhtimissüsteem

1. Suure riskiga tehisintellektisüsteemide jaoks luuakse riskijuhtimissüsteem, seda rakendatakse ja see dokumenteeritakse ning seda hooldatakse.

2. Riskijuhtimissüsteemi käsitatakse pidevalt korduva protsessina, mida kavandatakse ja käitatakse suure riskiga tehisintellektisüsteemi kogu olelusringi jooksul ning mida tuleb korrapäraselt ja süstemaatiliselt ajakohastada. See peab sisaldama järgmisi etappe:

   a) selliste teadaolevate ja prognoositavate riskide kindlakstegemine ja analüüsimine, mis võivad tekkida tervisele, ohutusele ja põhiõigustele suure riskiga tehisintellektisüsteemi sihtotstarvet silmas pidades;

   b) [välja jäetud]

   c) muude tekkida võivate riskide hindamine artiklis 61 osutatud turustamisjärgse seire süsteemist saadud andmete analüüsi põhjal;

   d) sobivate riskijuhtimismeetmete vastuvõtmine kooskõlas järgmiste lõigete sätetega.

   Käesolevas lõikes osutatud riskid hõlmavad ainult neid riske, mida on võimalik mõistlikult maandada või kõrvaldada suure riskiga tehisintellektisüsteemi arendamise või projekteerimise või piisava tehnilise teabe esitamise kaudu.

3. Lõike 2 punktis d osutatud riskijuhtimismeetmetes võetakse nõuetekohaselt arvesse käesolevas 2. peatükis sätestatud nõuete kombineeritud kohaldamisest tulenevat mõju ja võimalikku koostoimet, pidades silmas riskide tõhusamat minimeerimist, saavutades samas asjakohase tasakaalu nende nõuete täitmiseks võetavate meetmete rakendamisel.

4. Lõike 2 punktis d osutatud riskijuhtimismeetmed on sellised, et iga ohuga seotud mistahes jääkriski ja suure riskiga tehisintellektisüsteemide üldist jääkriski peetakse vastuvõetavaks.

Kõige otstarbekamate riskijuhtimismeetmete kindlaksmääramisel tuleb tagada järgmine:

a) lõike 2 kohaselt tuvastatud ja hinnatud riskide kõrvaldamine või vähendamine nii palju kui võimalik suure riskiga tehisintellektisüsteemi sobiva projekteerimise ja arendamise kaudu;

b) asjakohasel juhul sobivate riskimaandamis- ja kontrollimeetmete rakendamine selliste riskide puhul, mida ei saa kõrvaldada;

c) piisava teabe andmine vastavalt artiklile 13, eeskätt seoses käesoleva artikli lõike 2 punktis b osutatud riskidega, ning asjakohasel juhul kasutajate koolitamine.

Suure riskiga tehisintellektisüsteemi kasutamisega seotud riskide kõrvaldamiseks või vähendamiseks võetakse nõuetekohaselt arvesse kasutajalt eeldatavaid tehnilisi teadmisi, kogemusi, haridust ja koolitust, ning keskkonda, milles kasutamiseks on süsteem mõeldud.

5. Suure riskiga tehisintellektisüsteeme testitakse eesmärgiga tagada, et suure riskiga tehisintellektisüsteemid töötavad oma sihtotstarbega kooskõlas oleval moel ning vastavad käesolevas peatükis sätestatud nõuetele.

6. Testimismenetlused võivad hõlmata tegelikes tingimustes testimist kooskõlas artikliga 54a.

7. Suur riskiga tehisintellektisüsteemide testimine toimub vastavalt vajadusele mistahes ajal kogu arendusprotsessi jooksul ja igal juhul enne selle turule laskmist või kasutusele võtmist. Testimiseks kasutatakse eelnevalt kindlaks määratud parameetreid ja tõenäosuskünniseid, mis on suure riskiga tehisintellektisüsteemi sihtotstarbe seisukohast sobivad.

8. Lõigetes 1–7 kirjeldatud riskijuhtimissüsteemi puhul pööratakse erilist tähelepanu sellele, kas on tõenäoline, et suure riskiga tehisintellektisüsteemile pääsevad juurde alla 18-aastased isikud või et selline süsteem mõjutab alla 18-aastaseid isikuid.

9. Suure riskiga tehisintellektisüsteemide pakkujate jaoks, kelle suhtes kohaldatakse asjaomaste valdkondlike liidu õigusaktide alusel sisemisi riskijuhtimisprotsesse käsitlevaid nõudeid, võivad lõigetes 1–8 kirjeldatud aspektid olla kõnealuse õiguse kohaselt loodud riskijuhtimisprotseduuride osa.

Artikkel 10

Andmed ja andmehaldus

1. Kui tegemist on suure riskiga tehisintellektisüsteemidega, milles kasutatavad meetodid hõlmavad mudelite treenimist andmetega, tuleb nende süsteemide arendamiseks kasutada treenimis-, valideerimis- ja testimisandmestikke, mis vastavad lõigetes 2–5 osutatud kvaliteedikriteeriumidele.

2. Treenimis-, valideerimis- ja testimisandmestike suhtes kohaldatakse asjakohaseid andmehaldus- ja juhtimistavasid. Need tavad puudutavad eeskätt järgmist:

   a) asjakohased projekteerimise käigus tehtavad valikud;

   b) andmete kogumise protsessid;

   c) andmete ettevalmistamiseks tehtavad asjakohased töötlemistoimingud, näiteks kommenteerimine, märgendamine, puhastamine, rikastamine ja koondamine;

d) asjakohaste eelduste sõnastamine, eeskätt seoses teabega, mida andmed peaksid mõõtma ja kajastama;

e) vajalike andmestike kättesaadavuse, koguste ja sobivuse eelhindamine;

f) läbivaatamine võimaliku kallutatuse seisukohast, mis võib mõjutada füüsiliste isikute tervist ja ohutust või põhjustada liidu õigusega keelatud diskrimineerimist;

g) võimalike andmelünkade või puuduste kindlakstegemine ja võimalused nende lünkade ja puuduste kõrvaldamiseks.

3. Treenimis-, valideerimis- ja testimisandmestikud peavad olema asjakohased, representatiivsed ning võimalikult suurel määral vigadeta ja täielikud. Neid peavad iseloomustama asjakohased statistilised omadused, sealhulgas vajaduse korral seoses isikute või isikute rühmadega, kelle peal kavatsetakse suure riskiga tehisintellektisüsteemi kasutada. Need andmestiku omadused võivad olla täidetud üksikute andmestike või nende kombinatsiooni tasandil.

4. Treenimis-, valideerimis- ja testimisandmestikes tuleb sihtotstarbe jaoks vajalikus ulatuses võtta arvesse omadusi või elemente, mis iseloomustavad konkreetset geograafilist, käitumuslikku või funktsionaalset olukorda, kus kavatsetakse suure riskiga tehisintellektisüsteemi kasutada.

5. Niivõrd, kuivõrd see on rangelt vajalik kallutatuse seire, avastamise ja parandamise jaoks suure riskiga tehisintellektisüsteemide puhul, võivad selliste süsteemide pakkujad töödelda määruse (EL) 2016/679 artikli 9 lõikes 1, direktiivi (EL) 2016/680 artiklis 10 ja määruse (EL) 2018/1725 artikli 10 lõikes 1 osutatud isikuandmete eriliike, tingimusel et füüsiliste isikute põhiõiguste ja vabaduste kaitseks kohaldatakse asjakohaseid kaitsemeetmeid, sh tehnilisi piiranguid, mis puudutavad tipptasemel turvalisuse tagamise ja privaatsuse säilitamise meetmete, näiteks pseudonüümimise taaskasutamist ja kasutamist või krüpteerimist, kui anonüümimine võib avaldada olulist mõju taotletavale eesmärgile.

6. Nende suure riskiga tehisintellektisüsteemide arendamisel, mille puhul ei kasutata mudelite treenimist hõlmavaid meetodeid, kohaldatakse lõikeid 2–5 üksnes testimisandmestike suhtes.

Artikkel 11

Tehniline dokumentatsioon

1. Suure riskiga tehisintellektisüsteemi tehniline dokumentatsioon koostatakse enne süsteemi turule laskmist või kasutusele võtmist ning see hoitakse ajakohasena.

   Tehniline dokumentatsioon koostatakse selliselt, et see tõendaks suure riskiga tehisintellektisüsteemi vastavust käesolevas peatükis sätestatud nõuetele ja annaks riikide pädevatele asutustele ja teavitatud asutustele selgel ja terviklikul kujul kogu teabe, mis on vajalik, et hinnata tehisintellektisüsteemi vastavust neile nõuetele. Dokumentatsioon peab sisaldama vähemalt IV lisas loetletud elemente või VKEde, sealhulgas idufirmade puhul samaväärset dokumentatsiooni, mis vastab samadele eesmärkidele, välja arvatud juhul, kui pädev asutus seda ebasobivaks peab.

2. Kui turule lastakse või kasutusse võetakse suure riskiga tehisintellektisüsteem, mis on seotud tootega, mille suhtes kohaldatakse II lisa A jaos loetletud õigusakte, koostatakse üks ühtne tehniline dokumentatsioon, mis sisaldab nii kogu IV lisas kirjeldatud teavet kui ka nimetatud õigusaktide kohaselt nõutavat teavet.

3. Komisjonil on õigus võtta kooskõlas artikliga 73 vastu delegeeritud õigusakte, et muuta IV lisa, kui see on vajalik, et tagada, et tehniline dokumentatsioon sisaldab tehnika arengut arvestades kogu vajalikku teavet, et hinnata süsteemi vastavust käesolevas peatükis sätestatud nõuetele.

Artikkel 12

Andmete säilitamine

1. Suure riskiga tehisintellektisüsteemid võimaldavad tehniliselt sündmuste automaatset registreerimist („logid“) süsteemi kogu elutsükli jooksul.

2. Selleks et tagada tehisintellektisüsteemi toimimise jälgitavus süsteemi sihtotstarbe seisukohast otstarbekal tasemel, võimaldavad logimisfunktsioonid registreerida sündmusi, mis on asjakohased

i) olukordade tuvastamiseks, mille tulemuseks võib olla riski tekitav tehisintellektisüsteem artikli 65 lõike 1 tähenduses või oluline muudatus;

ii) artiklis 61 osutatud turustamisjärgse seire hõlbustamiseks

iii)artikli 29 lõikes 4 osutatud suure riskiga tehisintellektisüsteemide töö seireks.

4. III lisa punkti 1 alapunktis a osutatud suure riskiga tehisintellektisüsteemide logimisfunktsioonid peavad pakkuma vähemalt järgmist:

a) süsteemi iga kasutuskorra ajavahemiku registreerimine (iga kasutuskorra alguse ja lõpu kuupäev ja kellaaeg);

b) võrdlusandmebaas, millega süsteem sisendandmeid võrdleb;

c) sisendandmed, mille otsimine on andnud vastuseks tulemuse;

d) tulemuste kontrollimises osalenud füüsiliste isikute isikusamasuse kontroll, nagu on viidatud artikli 14 lõikes 5.

Artikkel 13

Läbipaistvus ja kasutajate teavitamine

1. Suure riskiga tehisintellektisüsteeme tuleb projekteerida ja arendada selliselt, et oleks tagatud nende töö piisav läbipaistvus selleks, et saavutada käesoleva jaotise 3. peatükis sätestatud kasutaja ja pakkuja asjaomaste kohustuste täitmine ning et kasutajad saaksid süsteemi asjakohaselt mõista ja kasutada.

2. Suure riskiga tehisintellektisüsteemiga peab kaasas olema sobivas digivormingus või muus vormis kasutusjuhend, mis sisaldab kokkuvõtlikku, täielikku, täpset ja selget teavet, mis on kasutajatele oluline, juurdepääsetav ja mõistetav.

3. Lõikes 2 osutatud teabest peavad selguma järgmised asjaolud:

   a) pakkuja ning asjakohasel juhul tema volitatud esindaja nimi ja kontaktandmed;

   b) suure riskiga tehisintellektisüsteemi omadused, funktsioonid ja toimimispiirangud, muu hulgas:

      i) selle sihtotstarve, sealhulgas konkreetne geograafiline, käitumuslik ja funktsionaalne raamistik, milles kasutamiseks suure riskiga tehisintellektisüsteem on ette nähtud;

      ii) artiklis 15 osutatud täpsuse (sealhulgas selle parameetrite), stabiilsuse ja küberturvalisuse tase, mille põhjal on suure riskiga tehisintellektisüsteem testitud ja valideeritud ja mida võib eeldada, ning kõik teadaolevad ja prognoositavad asjaolud, mis võivad seda täpsuse, stabiilsuse ja küberturvalisuse taset mõjutada;

      iii) kõik teadaolevad või prognoositavad asjaolud, mis on seotud suure riskiga tehisintellektisüsteemi kasutamisega vastavalt selle sihtotstarbele ja mis võivad kaasa tuua riskid tervisele ja ohutusele või põhiõigustele, millele on osutatud artikli 9 lõikes 2;

iv) kui see on asjakohane, siis süsteemi käitumine, mis puudutab isikuid või isikute rühmi, kelle peal kavatsetakse suure riskiga tehisintellektisüsteemi kasutada;

v) kui see on asjakohane, siis sisendandmete spetsifikatsioonid või muu asjakohane teave kasutatud treenimis-, valideerimis- ja testimisandmestike kohta, võttes arvesse tehisintellektisüsteemi sihtotstarvet;

vi) kui see on asjakohane, siis süsteemi eeldatava väljundi kirjeldus;

c) suure riskiga tehisintellektisüsteemi ja selle toimimise muudatused, mille pakkuja on esialgse vastavushindamise ajal ette kindlaks määranud, kui neid on;

d) artiklis 14 osutatud inimjärelevalve meetmed, kaasa arvatud tehnilised meetmed, mis on kehtestatud selleks, et kasutajatel oleks lihtsam tehisintellektisüsteemide väljundit tõlgendada;

e) vajalikud arvutus- ja riistvararessursid, suure riskitasemega tehisintellektisüsteemi eeldatav eluiga ning mistahes hooldus- ja hoolikusmeetmed, mis on vajalikud, et tagada tehisintellektisüsteemi nõuetekohane toimimine, muu hulgas tarkvarauuenduste vallas, ning nende meetmete sagedus;

f) sellise tehisintellektisüsteemi kuuluva mehhanismi kirjeldus, mis võimaldab kasutajatel logisid nõuetekohaselt koguda, salvestada ja tõlgendada, kui see on asjakohane.

Artikkel 14

Inimjärelevalve

1. Suure riskiga tehisintellektisüsteeme tuleb projekteerida ja arendada selliselt, kasutades muu hulgas asjakohaseid inimene-masin kasutajaliideseid, et füüsilised isikud saaksid teha tehisintellektisüsteemi kasutamise ajal selle üle reaalset järelevalvet.

2. Inimjärelevalve eesmärk on hoida ära või minimeerida tervist, ohutust või põhiõigusi ähvardavaid riske, mis võivad tekkida, kui suure riskiga tehisintellektisüsteemi kasutatakse vastavalt selle sihtotstarbele või mõistlikult prognoositava väärkasutamise tingimustes, eeskätt juhul, kui sellised riskid jäävad alles ka siis, kui kohaldatakse muid käesolevas peatükis sätestatud nõudeid.

3. Inimjärelevalve tagatakse kas ühe järgmist liiki meetme või kõigi järgmist liiki meetmete kaudu:

   a) meetmed, mille pakkuja on enne suure riskiga tehisintellektisüsteemi turule laskmist või kasutusele võtmist kindlaks teinud ja, kui see on tehniliselt teostatav, sellisesse süsteemi sisse ehitanud;

   b) meetmed, mille pakkuja on enne suure riskiga tehisintellektisüsteemi turule laskmist või kasutusele võtmist kindlaks teinud ja mis sobivad selleks, et kasutaja saaks neid rakendada.

4. Lõigete 1–3 rakendamiseks antakse suure riskiga tehisintellektisüsteem kasutajale sellisel viisil, et füüsilistel isikutel, kellele on antud ülesanne tegeleda inimjärelevalvega, oleks võimalik, kui see on olenevalt asjaoludest asjakohane ja proportsionaalne, teha järgmist:

   a) mõista suure riskiga tehisintellektisüsteemi võimekusi ja piiranguid ning suuta tegeleda sellise süsteemi nõuetekohase seirega;

   b) olla pidevalt teadlik võimalusest, et tekib kalduvus hakata automaatselt tuginema või liigselt tuginema suure riskiga tehisintellektisüsteemi toodetud väljundile (nn kalduvus eelistada automatiseerimist);

   c) korrektselt tõlgendada suure riskiga tehisintellektisüsteemi väljundit, võttes arvesse näiteks kättesaadavaid tõlgendamisvahendeid ja -meetodeid;

   d) otsustada igas konkreetses olukorras, et suure riskiga tehisintellektisüsteemi ei kasutata, või jätta suure riskiga tehisintellektisüsteemi väljund muul moel kõrvale, sürjutada või tagasi võtta;

   e) sekkuda suure riskiga tehisintellektisüsteemi töösse või katkestada süsteemi töö stopp-nupu või muu sarnase protseduuriga.

5. III lisa punkti 1 alapunktis a osutatud suure riskiga tehisintellektisüsteemide puhul tuleb lõikes 3 osutatud meetmetega tagada, et lisaks sellele ei tee ega otsusta kasutaja süsteemist saadud tuvastamise põhjal midagi, kui seda ei ole eraldi kontrollinud ja kinnitanud vähemalt kaks füüsilist isikut. Vähemalt kahe füüsilise isiku teostatava eraldi kontrollimise nõuet ei kohaldata nende suure riskiga tehisintellektisüsteemide suhtes, mida kasutatakse õiguskaitse, rände, piirikontrolli või varjupaigaga seotud eesmärgil, juhtumite puhul, kui liidu või riigi õiguse kohaselt peetakse selle nõude kohaldamist ebaproportsionaalseks.

Artikkel 15

Täpsus, stabiilsus ja küberturvalisus

1. Suure riskiga tehisintellektisüsteeme tuleb projekteerida ja arendada selliselt, et nad saavutaksid oma sihtotstarbe seisukohast asjakohase täpsuse, stabiilsuse ja küberturvalisuse taseme ning et nende sooritus oleks kolmes nimetatud aspektis kogu elutsükli jooksul järjekindel.

2. Suure riskiga tehisintellektisüsteemide täpsuse tasemed ja asjakohased täpsuse parameetrid tuleb deklareerida süsteemiga kaasas olevas kasutusjuhendis.

3. Suure riskiga tehisintellektisüsteemid peavad olema süsteemis või süsteemi töökeskkonnas tekkida võivate vigade, rikete või ebakõlade suhtes vastupidavad, eriti juhul, kui põhjuseks on süsteemi interaktsioon füüsiliste isikute või muude süsteemidega.

   Suure riskiga tehisintellektisüsteemide stabiilsuse võib saavutada tehnilise liiasuse lahendustega, mis võivad hõlmata varuplaane või tõrkekindluse plaane.

   Suure riskiga tehisintellektisüsteeme, mis õpivad edasi ka pärast turule laskmist või kasutusele võtmist, tuleb projekteerida ja arendada selliselt, et asjakohaste leevendusmeetmete kaudu kõrvaldada või vähendada niipalju kui võimalik potentsiaalselt kallutatud väljundite võimalikku mõju edasistele toimingutele („tagasisideahelad“).

4. Suure riskiga tehisintellektisüsteemid peavad pidama vastu volitamata kolmandate isikute katsetele muuta süsteemi kasutamist või toimimist, kasutades ära süsteemi nõrkusi.

Suure riskiga tehisintellektisüsteemide küberturvalisuse tagamiseks kasutatavad tehnilised lahendused peavad vastama asjaomastele asjaoludele ja riskidele.

Tehisintellektile iseloomulike nõrkustega toimetulemiseks kasutatavad tehnilised lahendused hõlmavad olenevalt asjaoludest meetmeid, millega hoida ära ja kontrollida ründeid, millega püütakse manipuleerida treenimisandmestikku („andmemürgitus“), sisendeid, mille eesmärk on panna mudel viga tegema („vastandnäited“), või mudelivigu.

3. PEATÜKK

SUURE RISKIGA TEHISINTELLEKTISÜSTEEMIDE PAKKUJATE JA KASUTAJATE NING MUUDE OSALISTE KOHUSTUSED

Artikkel 16

Suure riskiga tehisintellektisüsteemide pakkujate kohustused

Suure riskiga tehisintellektisüsteemide pakkujad peavad:

a) tagama, et nende suure riskiga tehisintellektisüsteemid vastavad käesoleva jaotise 2. peatükis sätestatud nõuetele;

aa) märkima oma nime, registreeritud kaubanime või registreeritud kaubamärgi ja kontaktaadressi kas suure riskiga tehisintellektisüsteemile või, kui see ei ole võimalik, selle pakendile või kaasasolevatesse dokumentidesse, nagu on asjakohane;

b) võtma kasutusele kvaliteedijuhtimissüsteemi, mis vastab artikli 17 nõuetele;

c) säilitama dokumentatsiooni, millele on osutatud artikli 18;

d) säilitama oma suure riskiga tehisintellektisüsteemide automaatselt loodud logisid, kui need on nende kontrolli all, nagu on osutatud artiklis 20;

e) tagama, et suure riskiga tehisintellektisüsteem läbib enne turule laskmist või kasutusele võtmist asjakohase vastavushindamise, nagu on osutatud artiklis 43;

f) täitma artikli 51 lõikes 1 osutatud registreerimiskohustusi;

g) võtma artiklis 21 osutatud vajalikud parandusmeetmed, kui suure riskiga tehisintellektisüsteem ei ole vastavuses käesoleva jaotise 2. peatükis sätestatud nõuetega;

h) teatama mittevastavusest ja võetud parandusmeetmetest sellele liikmesriigi asjaomasele pädevale asutusele, kus nad on tehisintellektisüsteemi kättesaadavaks teinud või kasutusele võtnud, ja vajaduse korral teavitatud asutusele;

i) kinnitama kooskõlas artikliga 49 oma suure riskiga tehisintellektisüsteemile CE-märgise, et näidata vastavust käesolevale määrusele;

j) tõendama riigi pädeva asutuse taotlusel suure riskiga tehisintellektisüsteemi vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele.

Artikkel 17

Kvaliteedijuhtimissüsteem

1. Suure riskiga tehisintellektisüsteemide pakkujad võtavad kasutusele kvaliteedijuhtimissüsteemi, mis tagab käesoleva määruse järgimise. Kvaliteedijuhtimissüsteem peab olema kirjalike põhimõtete, menetluste ja juhendite kujul süsteemselt ja nõuetekohaselt dokumenteeritud ning sisaldama vähemalt järgmisi aspekte:

   a) strateegia õigusnormidele vastavuse tagamiseks, sealhulgas vastavushindamise ja suure riskiga tehisintellektisüsteemis tehtavate muudatuste haldamismenetluste järgimiseks;

b) meetodid, protseduurid ja süstemaatilised meetmed, mida kasutatakse suure riskiga tehisintellektisüsteemi projekteerimiseks, projekteerimise järelevalveks ja projektide kontrollimiseks;

c) meetodid, protseduurid ja süstemaatilised meetmed, mida kasutatakse suure riskiga tehisintellektisüsteemi arendamiseks, kvaliteedi kontrollimiseks ja kvaliteedi tagamiseks;

d) enne suure riskiga tehisintellektisüsteemi arendamist, 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, siis ka vahendid, mida kasutatakse, et tagada suure riskiga tehisintellektisüsteemi vastavus käesoleva jaotise 2. peatükis sätestatud nõuetele;

f) andmehalduse süsteemid ja protseduurid, sh andmete kogumine, andmeanalüüs, andmete märgendamine, andmete talletamine, andmete filtreerimine, andmekaeve, andmete agregeerimine, andmesäilitus ja mis tahes muud andmetega seotud toimingud, mida teostatakse suure riskiga tehisintellektisüsteemide turule laskmise või kasutusele võtmise eel ja eesmärgil;

g) artiklis 9 osutatud riskijuhtimissüsteem;

h) turustamisjärgse seire süsteemi loomine, rakendamine ja toimivana hoidmine vastavalt artiklile 61;

i) protseduurid, mis on seotud tõsisest intsidendist teatamisega vastavalt artiklile 62;

j) suhtlemine riikide pädevate asutustega, pädevate asutustega, sh valdkondlike pädevate asutustega, kes pakuvad või toetavad juurdepääsu andmetele, teavitatud asutustega, teiste operaatoritega, klientidega või muude huvitatud isikutega;

k) kõigi vajalike dokumentide ja teabega seotud andmete säilitamise süsteemid ja protseduurid;

l) ressursside haldamine, sh varustuskindlusega seotud meetmed;

m) aruandekohustuse raamistik, millega nähakse ette juhtkonna ja muude töötajate vastutus seoses kõigi käesolevas lõikes loetletud aspektidega.

2. Lõikes 1 osutatud aspektide rakendamine peab olema proportsionaalne pakkuja organisatsiooni suurusega.

2a. Suure riskiga tehisintellektisüsteemide pakkujate jaoks, kelle suhtes kohaldatakse asjaomase valdkondliku liidu õiguse alusel kvaliteedijuhtimissüsteeme käsitlevaid kohustusi, võivad lõikes 1 kirjeldatud aspektid olla osa kõnealuse õiguse kohastest kvaliteedijuhtimissüsteemidest.

3. Finantsasutustest pakkujate puhul, kelle suhtes kohaldatakse finantsteenuseid käsitlevate liidu õigusaktide kohaseid nõudeid seoses nende sisemise juhtimise, korra või protsessidega, loetakse kvaliteedijuhtimissüsteemi loomise kohustus, välja arvatud lõike 1 punktide g, h ja i osas, täidetuks, kui järgitakse nõudeid seoses sisemise juhtimise, korra või protsessidega vastavalt finantsteenuseid käsitlevatele asjaomastele liidu õigusaktidele. Seoses sellega võetakse arvesse käesoleva määruse artiklis 40 osutatud harmoneeritud standardeid.

Artikkel 18

Dokumentatsiooni säilitamine

1. Pakkuja säilitab järgmisi dokumente riigi pädevate asutuste jaoks kättesaadavana kümne aasta jooksul pärast seda, kui tehisintellektisüsteem on turule lastud või kasutusele võetud:

a) artiklis 11 osutatud tehniline dokumentatsioon;

b) artiklis 17 osutatud kvaliteedijuhtimissüsteemi käsitlev dokumentatsioon;

c) kui see on asjakohane, siis dokumendid muudatuste kohta, mille teavitatud asutused on heaks kiitnud;

d) kui see on asjakohane, siis teavitatud asutuste tehtud otsused ja välja antud muud dokumendid;

e) artiklis 48 osutatud ELi vastavusdeklaratsioon.

1a. Iga liikmesriik määrab kindlaks tingimused, mille kohaselt jääb lõikes 1 osutatud dokumentatsioon riikide pädevate asutuste jaoks kättesaadavaks kõnealuses lõikes märgitud ajavahemikuks sellistel juhtudel, kui pakkuja või tema volitatud esindaja riigi territooriumil läheb pankrotti või lõpetab oma tegevuse enne selle ajavahemiku lõppu.

2. Finantsasutustest pakkujad, kelle suhtes kohaldatakse finantsteenuseid käsitlevate liidu õigusaktide kohaseid nõudeid seoses nende sisemise juhtimise, korra või protsessidega, säilitavad tehnilise dokumentatsiooni osana dokumentatsioonist, mida tuleb säilitada vastavalt finantsteenuseid käsitlevatele asjaomastele liidu õigusaktidele.

Artikkel 19

Vastavushindamine

1. Suure riskiga tehisintellektisüsteemide pakkujad peavad tagama, et nende süsteemid läbivad enne turule laskmist või kasutusele võtmist asjakohase vastavushindamise vastavalt artiklile 43. Kui sellise vastavushindamise kohaselt tõendatakse, et tehisintellektisüsteemid vastavad käesoleva jaotise 2. peatüki nõuetele, koostavad pakkujad ELi vastavusdeklaratsiooni vastavalt artiklile 48 ja kinnitavad tootele CE-vastavusmärgise vastavalt artiklile 49.

2. [välja jäetud]

Artikkel 20

Automaatselt genereeritud logid

1. Suure riskiga tehisintellektisüsteemide pakkujad säilitavad oma suure riskiga tehisintellektisüsteemide automaatselt genereeritud logisid, millele on osutatud artikli 12 lõikes 1, niivõrd, kuivõrd sellised logid on nende kontrolli all tulenevalt lepingupõhisest kokkuleppest kasutajaga või muul õiguslikul alusel. Nad säilitavad neid vähemalt kuus kuud, kui kohaldatavas liidu või liikmesriigi õiguses, eeskätt isikuandmete kaitset käsitlevas liidu õiguses ei ole sätestatud teisiti.

2. Finantsasutustest pakkujad, kelle suhtes kohaldatakse finantsteenuseid käsitlevate liidu õigusaktide kohaseid nõudeid seoses nende sisemise juhtimise, korra või protsessidega, säilitavad suure riskiga tehisintellektisüsteemide automaatselt genereeritud logisid osana dokumentatsioonist, mida tuleb säilitada vastavalt finantsteenuseid käsitlevatele asjaomastele õigusaktidele.

Artikkel 21

Parandusmeetmed

Suure riskiga tehisintellektisüsteemide pakkujad, kes arvavad või kellel on põhjust arvata, et suure riskiga tehisintellektisüsteem, mille nad on turule lasknud või kasutusele võtnud, ei vasta käesolevale määrusele, uurivad, kui see on asjakohane, viivitamatult koos teatanud kasutajaga põhjuseid ning võtavad viivitamatult vajalikud parandusmeetmed, et viia süsteem vastavusse, võtta see turult tagasi või kutsuda tagasi, nagu on asjakohane. Nad teavitavad sellest asjaomase suure riskiga tehisintellektisüsteemi levitajaid ning vajaduse korral volitatud esindajat ja importijaid.

Artikkel 22

Teavitamiskohustus

Kui suure riskiga tehisintellektisüsteem kujutab endast riski artikli 65 lõike 1 tähenduses ja see risk on süsteemi pakkujale teada, peab see pakkuja viivitamata teavitama nende liikmesriikide pädevaid asutusi, kus ta on süsteemi kättesaadavaks teinud, ja vajaduse korral teavitatud asutust, kes andis selle suure riskiga tehisintellektisüsteemi jaoks välja sertifikaadi, eeskätt tuleb teave esitada mittevastavuse ja võetud parandusmeetmete kohta.

Artikkel 23

Koostöö pädevate asutustega

Suure riskiga tehisintellektisüsteemide pakkujad peavad riigi pädeva asutuse taotluse peale esitama sellele asutusele selle liikmesriigi pädeva asutuse jaoks kergesti arusaadavas keeles kogu teabe ja dokumentatsiooni, mis on vajalik, et tõendada suure riskiga tehisintellektisüsteemi vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele. Riigi pädeva asutuse põhjendatud taotluse peale annavad pakkujad sellele asutusele juurdepääsu suure riskiga tehisintellektisüsteemi automaatselt genereeritud logidele, millele on osutatud artikli 12 lõikes 1, niivõrd, kuivõrd sellised logid on nende kontrolli all tulenevalt lepingupõhisest kokkuleppest kasutajaga või muul õiguslikul alusel.

Artikkel 23a

Tingimused, mille korral muude isikute suhtes kohaldatakse pakkuja kohustusi

1. Mis tahes füüsilist või juriidilist isikut käsitatakse käesoleva määruse kohaldamisel uue suure riskiga tehisintellektisüsteemi pakkujana ning tema suhtes kohaldatakse artiklist 16 tulenevaid pakkuja kohustusi millisel tahes järgmisel juhul:

   a) ta lisab juba turule lastud või kasutusele võetud suure riskiga tehisintellektisüsteemile oma nime või kaubamärgi, ilma et see piiraks selliste lepinguliste kokkulepete kohaldamist, milles sätestatakse, et kohustused on jaotatud muul viisil;

b) [välja jäetud]

c) ta teeb olulise muudatuse juba turule lastud või kasutusele võetud suure riskiga tehisintellektisüsteemi;

d) ta muudab sellise tehisintellektisüsteemi sihtotstarvet, mis ei ole suure riskiga ning mis on juba turule lastud või kasutusele võetud, nii et muudetud süsteemist saab suure riskiga tehisintellektisüsteem;

e) ta laseb turule või võtab kasutusele üldotstarbelise tehisintellektisüsteemi suure riskiga tehisintellektisüsteemina või suure riskiga tehisintellektisüsteemid komponendina.

2. Lõike 1 punktis a või c osutatud asjaolude ilmnemise korral ei käsitata suure riskiga tehisintellektisüsteemi algselt turule lasknud või kasutusele võtnud pakkujat enam käesoleva määruse kohaldamisel pakkujana.

3. Suure riskiga tehisintellektisüsteemide puhul, mis on selliste toodete turvakomponendid, mille suhtes kohaldatakse II lisa A jaos loetletud õigusakte, käsitatakse nende toodete tootjat suure riskiga tehisintellektisüsteemi pakkujana ja tema suhtes kohaldatakse artikli 16 kohaseid kohustusi ühel järgmistest juhtudest:

i) suure riskiga tehisintellektisüsteem lastakse turule koos tootega toote valmistaja nime või kaubamärgi all;

ii) suure riskiga tehisintellektisüsteem võetakse kasutusele toote valmistaja nime või kaubamärgi all pärast toote turule laskmist.

Artikkel 24

[välja jäetud]

Artikkel 25

Volitatud esindajad

1. Väljaspool liitu asuv pakkuja peab enne oma süsteemi liidu turul kättesaadavaks tegemist määrama kirjaliku volitusega liidus asuva volitatud esindaja.

2. Volitatud esindaja täidab pakkujalt saadud volituses kindlaksmääratud ülesandeid. Käesoleva määruse kohaldamisel annab volitus volitatud esindajale õiguse täita ainult järgmisi ülesandeid:

-a) kontrollida, et koostatud on ELi vastavusdeklaratsioon ja tehniline dokumentatsioon ning et pakkuja on teostanud asjakohase vastavushindamismenetluse;

a) säilitada riigi pädevate asutuste ja artikli 63 lõikes 7 osutatud riiklike asutuste jaoks kättesaadavana 10 aasta jooksul pärast suure riskiga tehisintellektisüsteemi turule laskmist või kasutusele võtmist pakkuja kontaktandmed, mida kasutades on volitatud esindaja nimetatud, ELi vastavusdeklaratsiooni koopia, tehnilise dokumentatsiooni ning, kui see on asjakohane, teavitatud asutuse väljastatud sertifikaadi;

b) esitada riigi pädevale asutusele põhjendatud taotluse peale kogu teave ja dokumentatsioon, sealhulgas punkti b kohaselt säilitatud teave ja dokumentatsioon, mis on vajalik, et tõendada suure riskiga tehisintellektisüsteemi vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele, sealhulgas pakkuda juurdepääsu suure riskiga tehisintellektisüsteemi automaatselt genereeritud logidele, millele on osutatud artikli 12 lõikes 1, niivõrd, kuivõrd sellised logid on pakkuja kontrolli all tulenevalt lepingupõhisest kokkuleppest kasutajaga või muul õiguslikul alusel;

c) teha riikide pädevate asutustega põhjendatud taotluse peale koostööd kõigis toimingutes, mida riigi pädev asutus seoses suure riskiga tehisintellektisüsteemiga ette võtab;

d) täita artikli 51 lõikes 1 osutatud registreerimiskohustusi ning, kui süsteemi registreerimise teeb pakkuja ise, kontrollida, et VIII lisa II osa punktides 1–11 osutatud teave on õige.

Volitatud esindaja lõpetab volituse, kui tal on piisavalt põhjust arvata, et pakkuja rikub oma käesolevast määrusest tulenevaid kohustusi. Sellisel juhul teatab ta volituse lõpetamisest ja selle põhjustest ka viivitamata oma asukohaliikmesriigi turujärelevalveasutusele ning, kui see on asjakohane, asjaomasele teavitatud asutusele.

Volitatud esindaja on defektsete tehisintellektisüsteemide eest pakkujaga samadel alustel ja solidaarselt juriidiliselt vastutav seoses tema potentsiaalse vastutusega nõukogu direktiivi 85/374/EMÜ kohaselt.

Artikkel 26

Importijate kohustused

1. Enne suure riskiga tehisintellektisüsteemi turule laskmist peavad sellise süsteemi importijad tagama süsteemi vastavuse käesolevale määrusele, kontrollides, et:

a) selle tehisintellektisüsteemi pakkuja on teostanud artiklis 43 osutatud asjakohase vastavushindamise;

b) pakkuja on koostanud tehnilise dokumentatsiooni kooskõlas IV lisaga;

c) süsteemil on nõutav CE-vastavusmärgis ning sellega on kaasas ELi vastavusdeklaratsioon ja kasutusjuhendid;

d) pakkuja on kindlaks määranud artiklis 25 osutatud volitatud esindaja.

2. Kui importijal on piisavalt põhjuseid arvata, et suure riskiga tehisintellektisüsteem ei ole käesoleva määrusega vastavuses või on võltsitud või sellega on kaasas võltsitud dokumentatsioon, ei vii ta seda süsteemi turule enne, kui see tehisintellektisüsteem on viidud määrusega vastavusse. Kui suure riskiga tehisintellektisüsteem kujutab endast riski artikli 65 lõike 1 tähenduses, teavitab importija sellest tehisintellektisüsteemi pakkujat, volitatud esindajaid ja turujärelevalveasutusi.

3. Importijad märgivad oma nime, registreeritud kaubanime või registreeritud kaubamärgi ja kontaktaadressi kas suure riskiga tehisintellektisüsteemile või, kui see ei ole võimalik, selle pakendile või kaasasolevatesse dokumentidesse, nagu on asjakohane.

4. Importija tagab vastavalt asjaoludele, et sel ajal, kui suure riskiga tehisintellektisüsteem on tema vastutuse all, ei ohusta ladustamise ega transpordi tingimused selle vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele.

4a. Importijad säilitavad 10 aasta jooksul pärast tehisintellektisüsteemi turule laskmist või kasutusele võtmist koopia teavitatud asutuse väljastatud sertifikaadist, kui see on asjakohane, kasutusjuhendist ning ELi vastavusdeklaratsioonist.

5. Importijad esitavad riigi pädevale asutusele põhjendatud taotluse peale selle riigi pädeva asutuse jaoks kergesti arusaadavas keeles kogu teabe ja dokumentatsiooni, sealhulgas lõike 5 kohaselt säilitatud teabe ja dokumentatsiooni, mis on vajalik, et tõendada suure riskiga tehisintellektisüsteemi vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele. Seda silmas pidades tagavad nad ka selle, et nendele asutustele saab kättesaadavaks teha tehnilise dokumentatsiooni.

5a. Importijad teevad riikide pädevate asutustega koostööd kõigis toimingutes, mida need asutused võtavad ette seoses tehisintellektisüsteemiga, mille importijad nad on.

Artikkel 27

Turustajate kohustused

1. Enne suure riskiga tehisintellektisüsteemi turul kättesaadavaks tegemist kontrollivad turustajad, et suure riskiga tehisintellektisüsteem kannab nõutavat CE-vastavusmärgist, et sellega on kaasas koopia ELi vastavusdeklaratsioonist ja kasutusjuhend ning et olenevalt asjaoludest on kas süsteemi pakkuja või importija täitnud oma kohustused, mis on sätestatud vastavalt artikli 16 punktis b ja artikli 26 lõikes 3.

2. Kui turustaja arvab või tal on põhjust arvata, et suure riskiga tehisintellektisüsteem ei ole vastavuses käesoleva jaotise 2. peatükis sätestatud nõuetega, ei tee ta seda suure riskiga tehisintellektisüsteemi turul kättesaadavaks enne, kui see süsteem on viidud nende nõuetega vastavusse. Peale selle, kui suure riskiga tehisintellektisüsteem kujutab endast riski artikli 65 lõike 1 tähenduses, teavitab turustaja sellest süsteemi pakkujat või importijat, nagu on asjakohane.

3. Turustaja tagab vastavalt asjaoludele, et sel ajal, kui suure riskiga tehisintellektisüsteem on tema vastutuse all, ei ohusta ladustamise ega transpordi tingimused süsteemi vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele.

4. Turustaja, kes arvab või kellel on põhjust arvata, et suure riskiga tehisintellektisüsteem, mille ta on turul kättesaadavaks teinud, ei vasta käesoleva jaotise 2. peatüki nõuetele, võtab parandusmeetmeid, mis on vajalikud, et viia süsteem nende nõuetega vastavusse, võtta see turult tagasi või kutsuda tagasi, või tagab, et olenevalt asjaoludest, kas pakkuja, importija või mõni asjaomane operaator võtab sellised parandusmeetmed. Kui suure riskiga tehisintellektisüsteem kujutab endast riski artikli 65 lõike 1 tähenduses, teavitab turustaja sellest viivitamata riigi pädevaid asutusi nendes liikmesriikides, kus ta on toote kättesaadavaks teinud, esitades eelkõige üksikasjad mittevastavuse ja võimalike võetud parandusmeetmete kohta.

5. Riigi pädeva asutuse põhjendatud taotluse peale esitab suure riskiga tehisintellektisüsteemi turustaja sellele asutusele kogu teabe ja dokumentatsiooni oma tegevuse kohta, nagu on kirjeldatud lõigetes 1–4.

5a. Turustajad teevad riikide pädevate asutustega koostööd kõigis toimingutes, mida need asutused võtavad ette seoses tehisintellektisüsteemiga, mille turustajad nad on.

Artikkel 28

[välja jäetud]

Artikkel 29

Suure riskiga tehisintellektisüsteemide kasutajate kohustused

1. Suure riskiga tehisintellektisüsteemide kasutajad kasutavad selliseid süsteeme vastavalt süsteemiga kaasas olevale kasutusjuhendile kooskõlas käesoleva artikli lõigetega 2 ja 5.

1a. Kasutajad annavad inimjärelevalve ülesande sellistele füüsilistele isikutele, kellel on vajalik pädevus, koolitus ja volitus.

2. Lõigetes 1 ja 1a sätestatud kohustused ei piira muid liidu või liikmesriigi õigusest tulenevaid kasutaja kohustusi ega kasutaja kaalutlusõigust oma vahendite ja tegevuse korraldamisel, et rakendada pakkuja märgitud inimjärelevalve meetmeid.

3. Niivõrd, kuivõrd kasutajal on kontroll sisendandmete üle, tagab see kasutaja, et sisendandmed on suure riskiga tehisintellektisüsteemi sihtotstarbe seisukohast asjakohased, ilma et see piiraks lõike 1 kohaldamist.

4. Kasutajad rakendavad inimjärelevalvet ja tegelevad suure riskiga tehisintellektisüsteemi töö seirega kasutusjuhendi alusel. Kui neil on põhjust arvata, et kasutusjuhendi kohase kasutamise tulemusena võib tehisintellektisüsteem tekitada riski artikli 65 lõike 1 tähenduses, teatab ta sellest pakkujale või turustajale ja peatab süsteemi kasutamise. Pakkujat või turustajat teavitavad nad ka siis, kui on kindlaks teinud tõsise intsidendi, ning nad katkestavad tehisintellektisüsteemi kasutamise. Kui kasutaja ei saa pakkujaga ühendust, kohaldatakse artiklit 62 *mutatis mutandis*. See kohustus ei hõlma õiguskaitseasutustest tehisintellektisüsteemide kasutajate tundlikke operatiivandmeid.

Finantsasutustest kasutajate puhul, kelle suhtes kohaldatakse finantsteenuseid käsitlevate liidu õigusaktide kohaseid nõudeid seoses nende sisemise juhtimise, korra või protsessidega, loetakse esimeses lõigus sätestatud seirekohustus täidetuks, kui vastavalt finantsteenuseid käsitlevatele asjaomastele õigusaktidele on täidetud sisejuhtimise korralduse, protseduuride ja korra alased nõuded.

5. Suure riskiga tehisintellektisüsteemide kasutajad säilitavad selle suure riskiga tehisintellektisüsteemi automaatselt genereeritud logisid, millele on osutatud artikli 12 lõikes 1, niivõrd, kuivõrd sellised logid on nende kontrolli all. Nad säilitavad neid vähemalt kuus kuud, kui kohaldatavas liidu või liikmesriigi õiguses, eeskätt isikuandmete kaitset käsitlevas liidu õiguses ei ole sätestatud teisiti.

Finantsasutustest kasutajad, kelle suhtes kohaldatakse finantsteenuseid käsitlevate liidu õigusaktide kohaseid nõudeid seoses nende sisemise juhtimise, korra või protsessidega, säilitavad logisid osana dokumentatsioonist, mida tuleb säilitada vastavalt finantsteenuseid käsitlevatele asjaomastele liidu õigusaktidele.

5a. Suure riskiga tehisintellektisüsteemide kasutajad, kes on avaliku sektori asutused, ametid või organid, välja arvatud õiguskaitse-, piirkontrolli-, rände- või varjupaigasutused, peavad täitma artiklis 51 osutatud registreerimiskohustused. Kui nad leiavad, et süsteem, mida nad kavatsevad kasutada, ei ole registreeritud ELi andmebaasis, millele on osutatud artiklis 60, siis nad seda süsteemi ei kasuta ning teavitavad pakkujat või turustajat.

6. Suure riskiga tehisintellektisüsteemide kasutajad kasutavad artikli 13 alusel esitatavat teavet, et täita oma kohustust koostada vajaduse korral andmekaitsealane mõjuhinnang vastavalt määruse (EL) 2016/679 artiklile 35 või direktiivi (EL) 2016/680 artiklile 27.

6a. Kasutajad teevad riikide pädevate asutustega koostööd kõigis toimingutes, mida need asutused võtavad ette seoses tehisintellektisüsteemiga, mille kasutajad nad on.

4. PEATÜKK

TEAVITAVAD ASUTUSED JA TEAVITATUD ASUTUSED

Artikkel 30

Teavitavad asutused

1. Iga liikmesriik määrab või loob vähemalt ühe teavitava asutuse, kes vastutab vastavushindamisasutuste hindamise, määramise ja neist teavitamise ning nende seire jaoks vajalike menetluste väljatöötamise ja läbiviimise eest.

2. Liikmesriigid võivad otsustada, et lõikes 1 osutatud hindamist ja seiret teeb riiklik akrediteerimisasutus määruse (EÜ) nr 765/2008 tähenduses ja sellega kooskõlas.

3. Teavitavad asutused tuleb luua, nende töö korraldada ja neid juhtida nii, et ei tekiks huvide konflikti vastavushindamisasutustega ning et oleks kindlustatud nende tegevuse objektiivsus ja erapooletus.

4. Teavitavate asutuste töö korraldatakse nii, et kõik vastavushindamisasutusest teavitamisega seotud otsused teevad pädevad isikud, kes ei ole nende asutuste hindamist läbi viinud isikud.

5. Teavitavad asutused ei tohi pakkuda ega osutada teenuseid, mida osutavad vastavushindamisasutused, ega nõustamisteenuseid ärilisel või konkureerival alusel.

6. Teavitavad asutused tagavad saadud teabe konfidentsiaalsuse kooskõlas artikliga 70.

7. Teavitavatel asutustel on oma ülesannete nõuetekohaseks täitmiseks piisavalt pädevaid töötajaid.

8. [välja jäetud]

Artikkel 31

Vastavushindamisasutuse teavitamistaotlus

1. Vastavushindamisasutus esitab teavitamistaotluse selle liikmesriigi teavitavale asutusele, mille territooriumil ta asub.

2. Teavitamistaotlusega koos esitatakse dokument, kus kirjeldatakse vastavushindamistoiminguid, vastavushindamismoodulit või -mooduleid ja tehisintellektisüsteeme, millega tegelemiseks väidab see vastavushindamisasutus end pädev olevat, ning riikliku akrediteerimisasutuse väljastatud akrediteerimistunnistus (kui see on olemas), mis tõendab, et vastavushindamisasutus vastab artiklis 33 sätestatud nõuetele. Lisatakse mis tahes kehtivad dokumendid, mis on seotud taotlust esitava teavitatud asutuse olemasolevate määramistega mõne muu liidu ühtlustamisõigusakti alusel.

3. Kui vastavushindamisasutus ei saa akrediteerimistunnistust esitada, siis esitab ta teavitavale asutusele kogu dokumentaalse tõestuse, mis on vajalik, et kontrollida, tunnistada ja korrapäraselt jälgida tema vastavust artiklis 33 sätestatud nõuetele. Kui tegemist on teavitatud asutusega, mis on määratud mõne muu liidu ühtlustamisõigusakti alusel, võib vastavalt vajadusele kasutada kõiki kõnealuste määramistega seotud dokumente ja tõendeid nende määramise toetuseks käesoleva määruse alusel. Teavitatud asutus ajakohastab lõigetes 2 ja 3 osutatud dokumentatsiooni alati, kui tehakse asjakohaseid muudatusi, et teavitatud asutuste eest vastutav asutus saaks jälgida ja kontrollida pidevat vastavust kõigile artiklis 33 sätestatud nõudmistele.

Artikkel 32

Teavitamiskord

1. Teavitavad asutused võivad teavitada ainult neist vastavushindamisasutustest, mis vastavad artiklis 33 sätestatud nõuetele.

2. Teavitavad asutused kasutavad komisjoni ja teiste liikmesriikide teavitamiseks nendest asutustest komisjoni välja töötatud ja hallatavat elektroonilist teavitamisvahendit.

3. Lõikes 2 nimetatud teavitus sisaldab täielikku ülevaadet vastavushindamistoimingutest, vastavushindamismoodulist või -moodulitest ja asjaomastest tehisintellektisüsteemidest ning asjakohast pädevuse tõendamist. Kui teavitus ei põhine artikli 31 lõikes 2 osutatud akrediteerimistunnistusel, esitab teavitav asutus komisjonile ja teistele liikmesriikidele dokumentaalsed tõendid, mis kinnitavad, et vastavushindamisasutus on pädev ja et on kehtestatud asutuse korrapärast järelevalvet tagav kord, millega tagatakse ka edaspidi vastavus artiklis 33 sätestatud nõuetele.

4. Asjaomane vastavushindamisasutus võib teavitatud asutuse toiminguid teha ainult juhul, kui komisjon või teised liikmesriigid ei esita vastuväiteid kahe nädala jooksul alates teavitava asutuse poolsest teavitamisest, kui teatis sisaldab artikli 31 lõikes 2 osutatud akrediteerimistunnistust, või kahe kuu jooksul alates teavitava asutuse poolsest teavitamisest, kui teatis sisaldab artikli 31 lõikes 3 osutatud dokumentaalseid tõendeid.

5. [välja jäetud]

Artikkel 33

Teavitatud asutustega seotud nõuded

1. Teavitatud asutus asutatakse liikmesriigi õiguse alusel ning ta on juriidiline isik.

2. Teavitatud asutused täidavad organisatsioonilisi, kvaliteedijuhtimise, ressursside ja protsessidega seotud nõudeid, mis on vajalikud nende ülesannete täitmiseks.

3. Teavitatud asutuste organisatsiooniline struktuur, vastutusalade jaotus, aruandlusahelad ja tegevus peavad olema sellised, et oleks võimalik tagada usaldus teavitatud asutuste tegevuse ja nende teostatud vastavushindamistoimingute tulemuste suhtes.

4. Teavitatud asutused peavad olema sõltumatud suure riskiga tehisintellektisüsteemi pakkujast, mille vastavushindamisega nad tegelevad. Samuti peavad teavitatud asutused olema sõltumatud mis tahes muust operaatorist, kellel on majanduslik huvi hinnatava suure riskiga tehisintellektisüsteemi vastu, ja kõigist pakkuja konkurentidest.

5. Teavitatud asutused korraldatakse ja neid juhitakse nii, et kindlustada nende tegevuse sõltumatus, objektiivsus ja erapooletus. Teavitatud asutused dokumenteerivad ja rakendavad struktuuri ja menetlused, millega kindlustada erapooletus ning mille abil edendada ja kohaldada erapooletuse põhimõtteid, mis hõlmavad kogu organisatsiooni, personali ja hindamistoiminguid.

6. Teavitatud asutustel peavad olema dokumenteeritud menetlused, millega tagatakse, et nende töötajad, komiteed, tütarettevõtjad, alltöövõtjad ja kõik nendega seotud asutused või väliste asutuste töötajad austavad vastavushindamistoimingute teostamise käigus saadud teabe konfidentsiaalsust kooskõlas artikliga 70, välja arvatud juhul, kui avalikustamine on seadusega nõutud. Teavitatud asutuste töötajad on kohustatud kaitsma ametisaladusena teavet, mille nad on saanud käesoleva määruse alusel oma ülesandeid täites, välja arvatud suhetes selle liikmesriigi teavitavate asutustega, kus teavitatud asutus tegutseb.

7. Teavitatud asutustel peavad olema menetlused toimingute teostamiseks, mis võtavad asjakohaselt arvesse ettevõtja suurust, tegutsemisvaldkonda, tema struktuuri ning kõnealuse tehisintellektisüsteemi keerukuse astet.

8. Teavitatud asutused peavad võtma endale asjakohase vastutuskindlustuse seoses oma vastavushindamistoimingutega, välja arvatud juhul, kui vastutust kannab liikmesriik, mille territooriumil nad asuvad vastavalt selle liikmesriigi siseriiklikele õigusaktidele, või kui see liikmesriik vastutab ise otseselt vastavushindamise eest.

9. Teavitatud asutused peavad olema võimelised täitma kõiki oma käesoleva määruse kohaseid ülesandeid suurima erialase usaldusväärsuse ja nõutava erialase pädevusega nii siis, kui neid ülesandeid täidavad teavitatud asutused ise, kui ka siis, kui seda tehakse nende nimel ja nende vastutusel.

10. Teavitatud asutustel peab olema piisav sisepädevus, et tulemuslikult hinnata väliste isikute poolt nende nimel täidetud ülesandeid. Teavitatud asutusele peab olema alaliselt kättesaadav piisavalt haldus-, tehnilisi, õigus- ja teadustöötajaid, kellel on kogemused ja teadmised asjaomaste tehisintellektitehnoloogiate, andmete ja andmetöötluse ja käesoleva jaotise 2. peatükis sätestatud nõuete alal.

11. Teavitatud asutused osalevad artiklis 38 osutatud koordineerimistegevuses. Samuti osalevad nad otseselt või esindajate kaudu Euroopa standardiorganisatsioonides või tagavad, et nad on asjakohastest standarditest teadlikud ja värskeima arenguga kursis.

12. [välja jäetud]

Artikkel 33a

Eeldatav vastavus teavitatud asutustega seotud nõuetele

Kui vastavushindamisasutus tõendab, et ta vastab sellistes asjakohastes harmoneeritud standardites või nende osades sätestatud kriteeriumidele, mille viitenumbrid on avaldatud *Euroopa Liidu Teatajas*, eeldatakse, et ta vastab artiklis 33 sätestatud nõuetele niivõrd, kuivõrd kohaldatavad harmoneeritud standardid hõlmavad kõnealuseid nõudeid.

Artikkel 34

Teavitatud asutuste tütarettevõtjad ja alltöövõtjad

1. Kui teavitatud asutus kasutab vastavushindamisega seotud ülesannete täitmiseks alltöövõtjat või tütarettevõtjat, tagab ta, et alltöövõtja või tütarettevõtja vastab artiklis 33 sätestatud nõuetele, ning teatab sellest teavitavale asutusele.

2. Teavitatud asutused vastutavad täielikult oma alltöövõtjate ja tütarettevõtjate täidetud ülesannete eest, olenemata sellest, kus need asuvad.

3. Alltöövõtjat või tütarettevõtjat võib kasutada ainult pakkuja nõusolekul.

4. Asjakohaseid dokumente, mis puudutavad alltöövõtja või tütarettevõtja kvalifikatsiooni hindamist ja nende poolt käesoleva määruse alusel tehtud tööd, hoitakse teavitavale asutusele kättesaadavana viie aasta jooksul alates alltöövõtutegevuse lõpetamise kuupäevast.

Artikkel 34a

Teavitatud asutuste tegevuskohustused

1. Teavitatud asutused kontrollivad suure riskiga tehisintellektisüsteemi vastavust artiklis 43 osutatud vastavushindamismenetluse kohaselt.

2. Teavitatud asutused väldivad toimingute teostamisel pakkujate liigset koormamist, võttes asjakohaselt arvesse ettevõtja suurust, tegutsemisvaldkonda, tema struktuuri ning kõnealuse suure riskiga tehisintellektisüsteemi keerukuse astet. Seejuures peab teavitatud asutus siiski silmas, millist rangust ja kaitse taset on vaja, et tagada suure riskiga tehisintellektisüsteemi vastavus käesoleva määruse nõuetele.

3. Teavitatud asutused teevad kättesaadavaks ja esitavad taotluse korral kogu asjakohase dokumentatsiooni, sealhulgas pakkuja dokumentatsiooni, artiklis 30 osutatud teavitavale asutusele, et sellel asutusel oleks võimalik teostada hindamis-, määramis-, teavitamis- ja seiretoiminguid ning hõlbustada käesolevas peatükis kirjeldatud hindamist.

Artikkel 35

Käesoleva määruse alusel määratud teavitatud asutuste identifitseerimisnumbrid ja loetelud

1. Komisjon määrab teavitatud asutustele identifitseerimisnumbrid. Komisjon määrab üheainsa identifitseerimisnumbri, isegi kui asutusest teavitatakse mitme erineva liidu õigusakti alusel.

2. Komisjon teeb üldsusele kättesaadavaks käesoleva määruse alusel teavitatud asutuste loetelu, mis sisaldab ka asutustele määratud identifitseerimisnumbreid ja toiminguid, mille teostamiseks neist on teavitatud. Komisjon tagab, et seda loetelu ajakohastatakse.

Artikkel 36

Muudatused teavitustes

1. Teavitav asutus teavitab komisjoni ja teisi liikmesriike kõigist asjakohastest muudatustest teavitatud asutuse teavituses artikli 32 lõikes 2 osutatud elektroonilise teavitamisvahendi kaudu.

2. Teavituse ulatuse laiendamise suhtes kohaldatakse artiklites 31 ja 32 kirjeldatud menetlusi. Muude kui teavituse ulatuse laiendamisega seotud muudatuste puhul kohaldatakse järgmistes lõigetes sätestatud menetlusi.

Kui teavitatud asutus otsustab vastavushindamisalase tegevuse lõpetada, teatab ta sellest teavitavale asutusele ja asjaomastele pakkujatele nii kiiresti kui võimalik ning ettekavatsetud lõpetamise korral üks aasta enne tegevuse lõpetamist. Sertifikaadid võivad pärast teavitatud asutuse tegevuse lõpetamist jääda ajutiselt kehtima üheksaks kuuks tingimusel, et mõni teine teavitatud asutus on kirjalikult kinnitanud, et ta võtab nende sertifikaatidega hõlmatud tehisintellektisüsteemide eest vastutuse üle. Enne asjaomastele tehisintellektisüsteemidele uute sertifikaatide väljastamist viib uus teavitatud asutus selle ajavahemiku lõpuks läbi nende süsteemide täieliku hindamise. Kui teavitatud asutus on oma tegevuse lõpetanud, tühistab teavitav asutus määramise.

3. Kui teavitaval asutusel on piisavalt põhjust arvata, et teavitatud asutus ei vasta enam artiklis 33 sätestatud nõuetele või ta ei täida oma kohustusi, siis teavitav asutus, tingimusel et teavitatud asutusele anti võimalus oma seisukohti esitada, seab vastavalt vajadusele teavitusele piirangud või peatab või tühistab selle sõltuvalt nõuetele mittevastavuse või kohustuste täitmata jätmise raskusastmest. Ta teatab sellest viivitamata komisjonile ja teistele liikmesriikidele.

4. Kui määramine on peatatud, piiratud või täielikult või osaliselt tühistatud, peab teavitatud asutus asjaomaseid tootjaid sellest teavitama hiljemalt kümne päeva jooksul.

5. Teavituse piiramise, peatamise või tühistamise korral võtab teavitav asutus asjakohaseid meetmeid tagamaks, et asjaomase teavitatud asutuse toimikud hoitakse alles ja tehakse teistes liikmesriikides asuvatele teavitavatele asutustele ja turujärelevalveasutustele nende nõudmisel kättesaadavaks.

6. Määramise piiramise, peatamise või tühistamise korral teavitav asutus:

   a) hindab mõju teavitatud asutuse väljastatud sertifikaatidele;

   b) esitab komisjonile ja teistele liikmesriikidele kolme kuu jooksul pärast teavituse muudatustest teatamist aruande oma järelduste kohta;

   c) nõuab, et teavitatud asutus peataks või tühistaks riikliku asutuse määratud mõistliku aja jooksul kõik alusetult väljastatud sertifikaadid, et tagada turul olevate tehisintellektisüsteemide nõuetele vastavus;

   d) teavitab komisjoni ja liikmesriike sertifikaatidest, mille peatamist või tühistamist ta on nõudnud;

e) esitab selle liikmesriigi pädevatele asutustele, kus on pakkuja registreeritud tegevuskoht, kogu asjakohase teabe sertifikaatide kohta, mille peatamist või tühistamist ta on nõudnud. Pädev asutus võtab vajaduse korral asjakohaseid meetmeid, et ära hoida võimalik risk tervisele, ohutusele või põhiõigustele.

7. Välja arvatud alusetult väljastatud sertifikaatide puhul ning kui teavitus on peatatud või piiratud, jäävad sertifikaadid kehtima järgmistel tingimustel:

a) teavitav asutus on ühe kuu jooksul alates peatamisest või piirangu kehtestamisest kinnitanud, et nende sertifikaatide puhul, mida peatamine või piirang puudutab, puudub risk tervisele, ohutusele või põhiõigustele, ning teavitav asutus on esitanud ajakava ja kavandatud meetmed peatamise või piirangu tühistamiseks; või

b) teavitav asutus on kinnitanud, et peatamisega seoses ei anta välja, ei muudeta ega anta uuesti välja ühtegi sertifikaati peatamise või piirangu kehtivuse jooksul, ning märgib, kas teavitatud asutus on suuteline järelevalvet jätkama ja jätkuvalt vastutama olemasolevate sertifikaatide eest, mis on välja antud peatamise või piirangu kehtivuse ajaks. Juhul kui teavitatud asutuste eest vastutav asutus teeb kindlaks, et teavitatud asutus ei ole suuteline olemasolevaid väljastatud sertifikaate toetama, esitab sertifikaadiga hõlmatud süsteemi pakkuja oma registreeritud tegevuskoha liikmesriigi pädevatele asutustele kolme kuu jooksul alates peatamisest või piirangu kehtestamisest kirjaliku kinnituse, et mõni teine kvalifitseeritud teavitatud asutus võtab peatamise või piirangu kehtimise ajaks ajutiselt üle teavitatud asutuse järelevalve ja sertifikaatide eest vastutamisega seotud ülesanded.

8. Välja arvatud alusetult väljastatud sertifikaatide puhul ja kui määramine on tühistatud, jäävad sertifikaadid kehtima üheksaks kuuks järgmistel tingimustel:

a) selle liikmesriigi pädev asutus, kus on sertifikaadiga hõlmatud tehisintellektisüsteemi pakkuja registreeritud tegevuskoht, on kinnitanud, et kõnealuste süsteemidega ei kaasne riski tervisele, ohutusele ega põhiõigustele; ning

b) mõni teine teavitatud asutus on kirjalikult kinnitanud, et ta võtab üle otsese vastutuse nende süsteemide eest ning viib nende hindamise lõpule 12 kuu jooksul alates määramise tühistamisest.

Esimeses lõigus osutatud tingimustel võib selle liikmesriigi pädev asutus, kus on sertifikaadiga hõlmatud tehisintellektisüsteemi pakkuja registreeritud tegevuskoht, pikendada sertifikaatide ajutist kehtivust kolme kuu kaupa, kusjuures kokku ei tohi pikendamise kestus ületada 12 kuud.

Liikmesriigi pädev asutus või teavitatud asutus, kes täidab selle teavitatud asutuse ülesandeid, keda teavituse muutmine puudutab, teavitab sellest viivitamata komisjoni, teisi liikmesriike ja teisi teavitatud asutusi.

Artikkel 37

Teavitatud asutuste pädevuse vaidlustamine

1. Komisjon uurib vajaduse korral kõiki juhtumeid, mille puhul on põhjust kahelda, kas teavitatud asutus vastab artiklis 33 sätestatud nõuetele.

2. Teavitav asutus annab komisjonile taotluse alusel kogu teabe asjaomase teavitatud asutuse teavitamise kohta.

3. Komisjon tagab, et käesoleva artikli kohase uurimise käigus omandatud konfidentsiaalset teavet käsitatakse konfidentsiaalsena kooskõlas artikliga 70.

4. Kui komisjon on veendunud, et teavitatud asutus ei täida või on lakanud täitmast artiklis 33 sätestatud nõudeid, teavitab ta teavitavat asutust sellise veendumuse põhjustest ning nõuab, et teavitav asutus võtaks vajalikud parandusmeetmed, sealhulgas vajaduse korral määramise peatamine, piiramine või tühistamine. Kui teavitav asutus ei rakenda vajalikke parandusmeetmeid, võib komisjon rakendusaktiga teavituse peatada või tühistada või seda piirata. Kõnealune rakendusakt võetakse vastu artikli 74 lõikes 2 osutatud kontrollimenetluse kohaselt.

Artikkel 38

Teavitatud asutuste koordineerimine

1. Komisjon tagab, et suure riskiga tehisintellektisüsteemide puhul kehtestatakse asjakohane koordineerimine ja koostöö teavitatud asutuste vahel, kes tegelevad vastavushindamisega vastavalt käesolevale määrusele, ning et see toimub nõuetekohaselt teavitatud asutuste valdkondliku rühma vormis.

2. Teavitav asutus tagab oma teavitatud asutuste osalemise nimetatud rühma töös otseselt või määratud esindajate vahendusel.

Artikkel 39

Kolmandate riikide vastavushindamisasutused

Sellise kolmanda riigi õiguse alusel asutatud vastavushindamisasutusel, kellega liit on sõlminud lepingu, võidakse lubada tegutseda teavitatud asutusena käesoleva määruse alusel, tingimusel et ta täidab artiklis 33 sätestatud nõuded.

5. PEATÜKK

STANDARDID, VASTAVUSHINDAMINE, SERTIFIKAADID, REGISTREERIMINE

Artikkel 40

Harmoneeritud standardid

1. Eeldatakse, et suure riskiga tehisintellektisüsteemid või üldotstarbelised tehisintellektisüsteemid, mis vastavad harmoneeritud standarditele või nende osadele, mille viited on avaldatud *Euroopa Liidu Teatajas*, on vastavuses käesoleva jaotise 2. peatükis sätestatud nõuetega, või kui see on asjakohane, artiklites 4a ja 4b sätestatud nõuetega niivõrd, kuivõrd nimetatud standardid hõlmavad neid nõudeid.

2. Kui komisjon esitab Euroopa standardiorganisatsioonidele standardimistaotluse kooskõlas määruse (EL) 1025/2012 artikliga 10, täpsustab ta, et standardid on sidusad, selged ja koostatud nii, et nende eesmärk on täita eelkõige järgmisi eesmärke:

   a) tagada, et liidus turule lastud või kasutusele võetud tehisintellektisüsteemid on ohutud ja austavad liidu väärtusi ning tugevdavad liidu avatud strateegilist autonoomiat;

   b) edendada tehisintellektialaseid investeeringuid ja innovatsiooni, sealhulgas õiguskindluse suurendamise kaudu, ning liidu turu konkurentsivõimet ja kasvu;

   c) tõhustada mitmel sidusrühmal põhinevat juhtimist, esindades kõiki asjaomaseid Euroopa sidusrühmi (nt tööstus, VKEd, kodanikuühiskond ja teadlased);

   d) aidata tugevdada tehisintellekti valdkonnas ülemaailmset standardimisalast koostööd, mis on kooskõlas liidu väärtuste ja huvidega.

Komisjon palub Euroopa standardiorganisatsioonidel esitada tõendid selle kohta, et nad on andnud endast parima eespool nimetatud eesmärkide täitmiseks.

Artikkel 41

Ühtsed kirjeldused

1. Komisjonil on õigus võtta pärast artiklis 56 osutatud tehisintellekti nõukojaga konsulteerimist ja kooskõlas artikli 74 lõikes 2 osutatud kontrollimenetlusega vastu rakendusakte, millega kehtestatakse ühtsed tehnilised kirjeldused käesoleva jaotise 2. peatükis sätestatud nõuete või, kui see on asjakohane, artiklites 4a ja 4b sätestatud nõuete kohta, kui on täidetud järgmised tingimused:

   a) *Euroopa Liidu Teatajas* ei ole avaldatud ühtegi määruse (EL) nr 1025/2012 kohast viidet harmoneeritud standarditele, mis hõlmaks asjakohaseid olulisi ohutuse või põhiõigustega seotud probleeme;

   b) komisjon on esitanud määruse (EL) 1025/2012 artikli 10 lõike 1 kohaselt taotluse ühele või mitmele Euroopa standardiorganisatsioonile koostada harmoneeritud standard käesoleva jaotise 2. peatükis sätestatud nõuete kohta;

   c) ükski Euroopa standardiorganisatsioon ei ole punktis b osutatud taotlust vastu võtnud või selle taotlusega seotud harmoneeritud standardeid ei ole esitatud määruse (EL) 1025/2012 artikli 10 lõikes 1 sätestatud tähtaja jooksul või need standardid ei vasta taotlusele.

1a. Enne rakendusakti eelnõu koostamist teavitab komisjon määruse (EL) nr 1025/2012 artiklis 22 osutatud komiteed sellest, et ta leiab, et lõikes 1 sätestatud tingimused on täidetud.

2. Ühtse kirjelduse kehtestamist käsitleva rakendusakti eelnõu ettevalmistamise varases etapis täidab komisjon artikli 40 lõikes 2 osutatud eesmärgid ja kogub kokku asjaomaste valdkondlike liidu õigusaktide alusel loodud asjaomaste asutuste või eksperdirühmade arvamused. Komisjon koostab rakendusakti eelnõu selle konsultatsiooni põhjal.

3. Eeldatakse, et suure riskiga tehisintellektisüsteemid või üldotstarbelised tehisintellektisüsteemid, mis vastavad lõikes 1 osutatud ühtsetele kirjeldustele, on vastavuses käesoleva jaotise 2. peatükis sätestatud nõuetega, või kui see on asjakohane, artiklites 4a ja 4b sätestatud nõuetega niivõrd, kuivõrd nimetatud ühtsed kirjeldused hõlmavad neid nõudeid.

4. Kui harmoneeritud standardi viited avaldatakse *Euroopa Liidu Teatajas*, tunnistatakse kehtetuks lõikes 1 osutatud rakendusaktid, mis hõlmavad käesoleva jaotise 2. peatükis sätestatud nõudeid või artiklites 4a ja 4b sätestatud nõudeid, kui see on asjakohane.

5. Kui liikmesriik leiab, et ühtne kirjeldus ei vasta täielikult käesoleva jaotise 2. peatükis sätestatud nõuetele või, kui see on asjakohane, artiklites 4a ja 4b sätestatud nõuetele, teatab ta sellest komisjonile ja lisab üksikasjaliku selgituse ning komisjon hindab seda teavet ja muudab vajaduse korral rakendusakti, millega kõnealune ühtne kirjeldus kehtestatakse.

Artikkel 42

Eeldatav vastavus teatavatele nõetele

1. Eeldatakse, et kui suure riskiga tehisintellektisüsteeme on treenitud ja testitud andmetega, mis peegeldavad konkreetset geograafilist, käitumuslikku ja funktsionaalset olustikku, milles kasutamiseks on need süsteemid mõeldud, vastavad need süsteemid artikli 10 lõike 4 vastavatele nõuetele.

2. Eeldatakse, et suure riskiga tehisintellektisüsteemid või üldotstarbelised tehisintellektisüsteemid, mis on sertifitseeritud või mille kohta on välja antud vastavusdeklaratsioon Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881[33] kohase küberturvalisuse sertifitseerimise kava alusel ning mille viited on avaldatud *Euroopa Liidu Teatajas*, vastavad käesoleva määruse artiklis 15 sätestatud küberturvalisuse nõuetele niivõrd, kuivõrd küberturvalisuse sertifikaat või vastavusdeklaratsioon või nende osad hõlmavad neid nõudeid.

Artikkel 43

Vastavushindamine

1. Kui pakkuja on rakendanud artiklis 40 osutatud harmoneeritud standardeid või, kui see on asjakohane, artiklis 41 osutatud ühtset kirjeldust, et tõendada III lisa punktis 1 loetletud suure riskiga tehisintellektisüsteemide vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele, valib pakkuja ühe järgmistest menetlustest:

   a) VI lisas osutatud sisekontrollil põhinev vastavushindamine; või

   b) VII lisas osutatud vastavushindamine, mis põhineb kvaliteedijuhtimissüsteemi ja tehnilise dokumentatsiooni hindamisel ning milles osaleb teavitatud asutus.

   Kui selle tõendamiseks, et suure riskiga tehisintellektisüsteem vastab käesoleva jaotise 2. peatükis sätestatud nõuetele, ei ole pakkuja rakendanud artiklis 40 osutatud harmoneeritud standardeid või on neid rakendanud vaid osaliselt või kui selliseid harmoneeritud standardeid ei ole olemas ja artiklis 41 osutatud ühtsed kirjeldused ei ole kättesaadavad, järgib pakkuja VII lisas sätestatud vastavushindamist.

[33] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 1).

VII lisas osutatud vastavushindamise jaoks võib pakkuja valida mistahes teavitatud asutuse. Kui aga süsteemi kavatsevad kasutusele võtta õiguskaitse-, rände- või varjupaigaasutused või ELi institutsioonid, organid või asutused, tegutseb teavitatud asutusena olenevalt asjaoludest artikli 63 lõikes 5 või kui see on asjakohane, lõikes 6 osutatud turujärelevalveasutus.

2. III lisa punktides 2–8 osutatud suure riskiga tehisintellektisüsteemide puhul ning jaotises 1a osutatud üldotstarbeliste tehisintellektisüsteemide puhul järgivad pakkujad VI lisas osutatud sisekontrollil põhinevat vastavushindamist, mille korral ei ole teavitatud asutuse osalemist ette nähtud.

3. Suure riskiga tehisintellektisüsteemide puhul, mille suhtes kohaldatakse II lisa A jaotises loetletud õigusakte, järgib pakkuja nende õigusaktide kohaselt nõutavat asjaomast vastavushindamist. Selliste suure riskiga tehisintellektisüsteemide suhtes kohaldatakse käesoleva jaotise 2. peatükis sätestatud nõudeid ning need nõuded on vastavushindamise osa. Kohaldatakse ka VII lisa punkte 4.3, 4.4, 4.5 ja punkti 4.6 viiendat lõiku.

Teavitatud asutustel, kellest on teavitatud nende õigusaktide alusel, on selliseks hindamiseks õigus kontrollida, kas suure riskiga tehisintellektisüsteemid vastavad käesoleva jaotise 2. peatükis sätestatud nõuetele, tingimusel et nende teavitatud asutuste vastavust artikli 33 lõigetes 4, 9 ja 10 sätestatud nõuetele on hinnatud nende õigusaktide kohase teavitamismenetluse raames.

Kui II lisa A jaos loetletud õigusaktid võimaldavad toote valmistajal loobuda kolmanda isiku tehtavast vastavushindamisest, tingimusel et see valmistaja on rakendanud kõiki harmoneeritud standardeid, mis hõlmavad kõiki olulisi nõudeid, võib see valmistaja nimetatud võimalust kasutada ainult siis, kui ta rakendab ka harmoneeritud standardeid või, kui see on asjakohane, artiklis 41 osutatud ühtseid kirjeldusi, mis hõlmavad käesoleva jaotise 2. peatükis sätestatud nõudeid.

4. [välja jäetud]

5. Komisjonil on õigus võtta kooskõlas artikliga 73 vastu delegeeritud õigusakte, et ajakohastada VI ja VII lisa, arvestades tehnika arenguga.

6. Komisjonil on õigus võtta vastu delegeeritud õigusakte, et muuta lõikeid 1 ja 2, et kohaldada III lisa punktides 2–8 osutatud suure riskiga tehisintellektisüsteemide suhtes VII lisas osutatud vastavushindamist või selle osi. Komisjon arvestab sellised delegeeritud õigusakte vastu võttes seda, kui mõjus on VI lisas osutatud sisekontrollil põhinev vastavushindamine, et hoida ära või minimeerida tervist, ohutust ja põhiõiguste kaitset ähvardavaid riske, mida sellised süsteemid põhjustavad, ning piisava suutlikkuse ja ressursside kättesaadavust teavitatud asutustes.

Artikkel 44

Sertifikaadid

1. Teavitatud asutuste poolt VII lisa kohaselt välja antavad sertifikaadid koostatakse keeles, mis on teavitatud asutuse asukoha liikmesriigi asjaomastele asutustele kergesti arusaadav.

2. Sertifikaat kehtib selles märgitud ajavahemiku jooksul, mis ei ületa viit aastat. Pakkuja taotlusel võib sertifikaadi kehtivust pikendada korraga mitte rohkem kui viie aasta kaupa, võttes aluseks kohaldatavate vastavushindamismenetluste kohaselt tehtava uue hindamise. Sertifikaadi mis tahes lisade kehtivusaeg on võrdne sertifikaadi kehtivusajaga.

3. Kui teavitatud asutus leiab, et tehisintellektisüsteem ei vasta enam käesoleva jaotise 2. peatükis sätestatud nõuetele, peatab ta väljastatud sertifikaadi, tunnistab selle kehtetuks või kehtestab selle suhtes piirangud, võttes seejuures arvesse proportsionaalsuse põhimõtet, kui süsteemi pakkuja ei taga nimetatud nõuete täitmist asjakohaste parandusmeetmete võtmisega teavitatud asutuse poolt kindlaks määratud tähtajaks. Teavitatud asutus põhjendab oma otsust.

Artikkel 45

Teavitatud asutuste otsuste vaidlustamine

Teavitatud asutuse otsuste vaidlustamiseks nähakse ette edasikaebamise kord.

Artikkel 46

Teavitatud asutuste teavitamiskohustused

1. Teavitatud asutused informeerivad teavitavat asutust järgmisest:

   a) kõik VII lisa nõuete kohaselt välja antud liidu tehnilise dokumentatsiooni hindamise sertifikaadid, nende sertifikaatide lisad, kvaliteedijuhtimissüsteemi kinnitused;

   b) kõik VII lisa nõuete kohaselt välja antud liidu tehnilise dokumentatsiooni hindamise sertifikaadi või kvaliteedijuhtimissüsteemi kinnituse tagasilükkamise, piiramise, peatamise või kehtetuks tunnistamise juhtumid;

   c) teavitamise ulatust või tingimusi mõjutavad asjaolud;

   d) turujärelevalveasutustelt saadud teabenõuded vastavushindamistoimingute kohta;

   e) taotluse korral vastavushindamistoimingud, mida nad teavituse sihtvaldkonnas on teinud, ja muu tegevus, sealhulgas piiriülesed toimingud ja alltöövõtt.

2. Iga teavitatud asutus informeerib teisi teavitatud asutusi järgmisest:

   a) kvaliteedijuhtimissüsteemi kinnitamised, mille andmisest ta keeldus, mille ta peatas või tunnistas kehtetuks, ja taotluse korral ka välja antud kvaliteedisüsteemide kinnitamised;

b) ELi tehnilise dokumentatsiooni hindamise sertifikaadid või nende lisad, mille andmisest ta keeldus, mille ta tunnistas kehtetuks, peatas või mida ta muul moel piiras, ning taotluse korral sertifikaadid ja/või nende lisad, mis ta on välja andnud.

3. Iga teavitatud asutus esitab teistele samu tehisintellektisüsteeme puudutavate samalaadsete vastavushindamistoimingutega tegelevatele teavitatud asutustele asjakohase teabe negatiivsete ja taotluse korral ka positiivsete vastavushindamistulemuste kohta.

4. Lõigetes 1–3 osutatud kohustused täidetakse kooskõlas artikliga 70.

Artikkel 47

Erand vastavushindamisest

1. Erandina artiklist 43 nõuetekohaselt põhjendatud taotluse korral võib mis tahes turujärelevalveasutus anda loa lasta asjaomase liikmesriigi territooriumil turule või võtta kasutusele konkreetne suure riskiga tehisintellektisüsteem, kui selleks on erandkorras põhjust avaliku julgeoleku või inimeste elu ja tervise kaitse, keskkonnakaitse või oluliste tööstus- ja taristuvarade kaitse tõttu. Selline luba antakse piiratud ajaks, kuni toimuvad vajalikud vastavushindamismenetlused, võttes arvesse erandi aluseks olevaid erandlikke põhjuseid. Need menetlused võetakse ette viivitamata.

1a. Nõuetekohaselt põhjendatud hädaolukorras avaliku julgeoleku erandlikel põhjustel või konkreetse, olulise ja vahetu ohu korral füüsiliste isikute elule või füüsilisele turvalisusele võivad õiguskaitseasutused või elanikkonnakaitse asutused võtta kasutusele konkreetse suure riskiga tehisintellektisüsteemi ilma lõikes 1 nimetatud loata tingimusel, et sellist luba taotletakse kasutamise ajal või pärast seda ilma põhjendamatu viivituseta ja kui selline luba lükatakse tagasi, peatatakse selle süsteemi kasutamine viivitamatult ning kõik sellise kasutamise tulemused ja väljundid kõrvaldatakse viivitamata.

2. Lõikes 1 osutatud luba antakse üksnes juhul, kui turujärelevalveasutus järeldab, et suure riskiga tehisintellektisüsteem vastab käesoleva jaotise 2. peatüki nõuetele. Turujärelevalveasutus teavitab komisjoni ja teisi liikmesriike kõigist lõike 1 kohaselt antud lubadest. See kohustus ei hõlma õiguskaitseasutuste tegevusega seotud tundlikke operatiivandmeid.

3. [välja jäetud]

4. [välja jäetud]

5. [välja jäetud]

6. Suure riskiga tehisintellektisüsteemide suhtes, mis on seotud II lisa A jaos osutatud liidu ühtlustamisõigusaktidega hõlmatud toodetega, kohaldatakse üksnes nendes õigusaktides sätestatud menetlusi vastavushindamisest erandite tegemiseks.

Artikkel 48

ELi vastavusdeklaratsioon

1. Pakkuja koostab iga tehisintellektisüsteemi kohta käsitsi või elektrooniliselt allkirjastatud ELi vastavusdeklaratsiooni ja säilitab seda riigi pädevate asutuste jaoks kättesaadavana vähemalt kümne aasta jooksul pärast tehisintellektisüsteemi turule laskmist või kasutusele võtmist. ELi vastavusdeklaratsioonis nimetatakse, millise tehisintellektisüsteemi kohta see on koostatud. Taotluse korral esitatakse ELi vastavusdeklaratsiooni koopia riigi asjaomastele pädevatele asutustele.

2. ELi vastavusdeklaratsioonis kinnitatakse, et kõnealune suure riskiga tehisintellektisüsteem vastab käesoleva jaotise 2. peatükis sätestatud nõuetele. ELi vastavusdeklaratsioon sisaldab V lisas sätestatud teavet ning see tõlgitakse keelde, mis on kergesti arusaadav selle liikmesriigi või nende liikmesriikide pädevatele asutustele, kus suure riskiga tehisintellektisüsteem kättesaadavaks tehakse.

3. Kui suure riskiga tehisintellektisüsteemide suhtes kohaldatakse muid liidu ühtlustamisõigusakte, mille kohaselt on samuti nõutav ELi vastavusdeklaratsioon, koostatakse kõigi suure riskiga tehisintellektisüsteemi suhtes kohaldatavate liidu õigusaktide jaoks üks ainus ELi vastavusdeklaratsioon. Vastavusdeklaratsioon sisaldab kogu vajalikku teavet deklaratsiooniga seotud liidu ühtlustamisõigusaktide kindlakstegemiseks.

4. ELi vastavusdeklaratsiooni koostamisega võtab pakkuja vastutuse käesoleva jaotise 2. peatükis sätestatud nõuete täitmise eest. Pakkuja ajakohastab ELi vastavusdeklaratsiooni vastavalt vajadusele.

5. Komisjonil on õigus võtta kooskõlas artikliga 73 vastu delegeeritud õigusakte, et ajakohastada V lisas sätestatud ELi vastavusdeklaratsiooni sisu, et lisada sinna elemente, mis muutuvad vajalikuks tehnika arengust tulenevalt.

Artikkel 49

CE-vastavusmärgis

1. CE-vastavusmärgise suhtes kohaldatakse määruse (EÜ) nr 765/2008 artiklis 30 sätestatud üldpõhimõtteid.

2. Suure riskiga tehisintellektisüsteemi CE-märgis kinnitatakse nähtaval, loetaval ja kustutamatul viisil. Kui see ei ole suure riskiga tehisintellektisüsteemi olemuse tõttu võimalik või otstarbekas, kinnitatakse märgis olenevalt asjaoludest kas pakendile või süsteemiga kaasas olevatele dokumentidele.

3. Vajaduse korral järgneb CE-märgisele artiklis 43 sätestatud vastavushindamismenetluste eest vastutava teavitatud asutuse identifitseerimisnumber. Identifitseerimisnumber esitatakse ka kõigis reklaammaterjalides, kus on öeldud, et suure riskiga tehisintellektisüsteem vastab CE-märgise nõuetele.

Artikkel 50

[välja jäetud]

Artikkel 51

Asjaomaste operaatorite ja III lisas loetletud suure riskiga tehisintellektisüsteemide registreerimine

1. Enne III lisas loetletud suure riskiga tehisintellektisüsteemi, välja arvatud III lisa punktides 1, 6 ja 7 osutatud õiguskaitse-, rände-, varjupaiga- ja piirikontrollihalduse valdkonna suure riskiga tehisintellektisüsteemide ning III lisa punktis 2 osutatud suure riskiga tehisintellektisüsteemide turule laskmist või kasutusele võtmist registreerib pakkuja ja kui see on asjakohane, volitatud esindaja end artiklis 60 osutatud ELi andmebaasis. Pakkuja, või kui see on asjakohane, volitatud esindaja registreerib selles andmebaasis ka oma süsteemid.

2. Enne III lisas loetletud suure riskiga tehisintellektisüsteemi kasutamist registreerivad suure riskiga tehisintellektisüsteemide kasutajad, kes on avaliku sektori asutused, ametid või organid või nende nimel tegutsevad üksused, end artiklis 60 osutatud ELi andmebaasis ja valivad välja süsteemi, mida nad kavatsevad kasutada.

   Eelmises lõigus sätestatud kohustusi ei kohaldata õiguskaitse-, piirikontrolli-, rände- või varjupaigaasutuste, -ametite või -organite, III lisa punktis 2 osutatud suure riskiga tehisintellektisüsteeme kasutavate asutuste, ametite või organite ega nende nimel tegutsevate üksuste suhtes.

IV JAOTIS

TEATAVATE TEHISINTELLEKTISÜSTEEMIDE PAKKUJATE JA KASUTAJATE LÄBIPAISTVUSKOHUSTUSED

Artikkel 52

Teatavate tehisintellektisüsteemide pakkujate ja kasutajate läbipaistvuskohustused

1. Pakkujad tagavad, et füüsiliste isikutega suhtlema mõeldud tehisintellektisüsteeme projekteeritakse ja arendatakse selliselt, et füüsilistele isikutele antakse teada, et nad suhtlevad tehisintellektisüsteemiga, välja arvatud juhul, kui see on mõistlikult informeeritud, tähelepaneliku ja aruka füüsilise isiku jaoks ilmne, võttes arvesse asjaolusid ja kasutamise konteksti. See kohustus ei kehti tehisintellektisüsteemide suhtes, mida on seadusega lubatud kasutada kuritegude avastamiseks, tõkestamiseks ja uurimiseks ning nende eest vastutusele võtmiseks, tingimusel, et kolmandate isikute õiguste ja vabaduste kaitseks kohaldatakse asjakohaseid kaitsemeetmeid, välja arvatud juhul, kui sellised süsteemid on üldsusele kättesaadavad, et kuritegudest teatada.

2. Biomeetrilise liigitamise süsteemi kasutajad annavad selle süsteemi tööst teada füüsilistele isikutele, kes selle süsteemiga kokku puutuvad. Seda kohustust ei kohaldata biomeetriliseks liigitamiseks kasutatavate tehisintellektisüsteemide suhtes, mida on seadusega lubatud kasutada kuritegude avastamiseks, tõkestamiseks ja uurimiseks, tingimusel et kolmandate isikute õiguste ja vabaduste kaitseks kohaldatakse asjakohaseid kaitsemeetmeid.

2a. Emotsioonituvastussüsteemi kasutajad annavad selle süsteemi tööst teada füüsilistele isikutele, kes selle süsteemiga kokku puutuvad. Seda kohustust ei kohaldata emotsioonide tuvastamiseks kasutatavate tehisintellektisüsteemide suhtes, mida on seadusega lubatud kasutada kuritegude avastamiseks, tõkestamiseks ja uurimiseks, tingimusel et kolmandate isikute õiguste ja vabaduste kaitseks kohaldatakse asjakohaseid kaitsemeetmeid.

3. Kasutaja, kes kasutab tehisintellektisüsteemi, mis loob või manipuleerib pildi-, audio-või videosisu, mis märkimisväärselt sarnaneb olemasolevate isikute, objektide, kohtade või muude olemite või sündmustega ja võib inimesele ekslikult tunduda ehtne või tõene (nn süvavõltsing), peab avalikustama, et sisu on kunstlikult loodud või seda on manipuleeritud.

Esimest lõiku ei kohaldata siiski juhul, kui kasutamine on seadusega lubatud kuritegude avastamiseks, tõkestamiseks, uurimiseks ja nende eest vastutusele võtmiseks või kui sisu moodustab osa ilmselgelt loomingulisest, satiirilisest, kunstilisest või väljamõeldud teosest või programmist, tingimusel et kolmandate isikute õiguste ja vabaduste kaitseks kohaldatakse asjakohaseid kaitsemeetmeid.

3a. Lõigetes 1–3 osutatud teave esitatakse füüsilistele isikutele selgel ja eristataval viisil hiljemalt esimese suhtlemise või kokkupuute ajal.

4. Lõiked 1, 2, 2a, 3 ja 3a ei mõjuta käesoleva määruse III jaotises sätestatud nõudeid ja kohustusi ega piira liidu või liikmesriigi õiguses sätestatud tehisintellektisüsteemide kasutajate muid läbipaistvuskohustusi.

V JAOTIS

INNOVATSIOONI TOETAVAD MEETMED

Artikkel 53

Tehisintellekti regulatsiooni testkeskkonnad

–1a. Riigi pädevad asutused võivad luua tehisintellekti regulatsiooni testkeskkondi innovatiivsete tehisintellektisüsteemide arendamiseks, treenimiseks, testimiseks ja valideerimiseks riigi pädeva asutuse otsese järelevalve, juhendamise ja toe all enne nende süsteemide turule laskmist või kasutusele võttu. Sellised regulatsiooni testkeskkonnad võivad hõlmata tegelikes tingimustes testimist, mille üle teostavad järelevalvet riigi pädevad asutused.

–1b. [välja jäetud]

-1c Kui see on asjakohane, teevad riigi pädevad asutused koostööd teiste asjaomaste asutustega ja võivad võimaldada muude tehisintellekti ökosüsteemis osalejate kaasamist.

–1d. Käesolev artikkel ei mõjuta muid liikmesriigi või liidu õiguse alusel loodud regulatsiooni testkeskkondi, sealhulgas juhtudel, kui neis testitavad tooted või teenused on seotud innovatiivsete tehisintellektisüsteemide kasutamisega. Liikmesriigid tagavad asjakohasel tasemel koostöö nende muude testkeskkondade üle järelevalvet teostavate asutuste ja riigi pädevate asutuste vahel.

1. [välja jäetud]

1a. [välja jäetud]

1b. Käesoleva määruse alusel tehisintellekti regulatsiooni testkeskkondade loomise eesmärk on aidata kaasa ühe või mitme järgmise eesmärgi saavutamisele:

a) edendada innovatsiooni ja konkurentsivõimet ning hõlbustada tehisintellekti ökosüsteemi arendamist;
b) hõlbustada ja kiirendada tehisintellektisüsteemide juurdepääsu liidu turule, eelkõige siis, kui seda pakuvad väikesed ja keskmise suurusega ettevõtjad (VKEd), sealhulgas idufirmad;
c) parandada õiguskindlust ja aidata kaasa parimate tavade jagamisele tehisintellekti regulatsiooni testkeskkonnas osalevate asutustega tehtava koostöö kaudu, et tagada tulevikus vastavus käesolevale määrusele ning kui see on asjakohane, muudele liidu ja liikmesriikide õigusaktidele;
d) aidata kaasa tõenduspõhisele regulatiivsele õppimisele.

2. [välja jäetud]

2a. Juurdepääs tehisintellekti regulatsiooni testkeskkondadele on avatud igale tehisintellektisüsteemi pakkujale või võimalikule pakkujale, kes vastab lõike 6 punktis a osutatud kõlblikkus- ja valikukriteeriumidele ning kelle riigi pädevad asutused on valinud lõike 6 punktis b osutatud valikumenetluse kohaselt. Pakkujad või võimalikud pakkujad võivad esitada taotlusi ka partnerluses kasutajate või muude asjaomaste kolmandate isikutega.

Tehisintellekti regulatsiooni testkeskkonnas osalemine piirdub ajavahemikuga, mis on projekti keerukuse ja ulatuse seisukohast asjakohane. Riigi pädev asutus võib seda ajavahemikku pikendada.

Tehisintellekti regulatsiooni testkeskkonnas osalemine põhineb käesoleva artikli lõikes 6 osutatud konkreetsel kaval, milles lepivad kokku osaleja(d) ja vajaduse korral riigi pädev(ad) asutus(ed).

3. Tehisintellekti regulatsiooni testkeskkondades osalemine ei mõjuta testkeskkonna üle järelevalvet teostavate pädevate asutuste järelevalve- ja parandusvolitusi. Need asutused kasutavad oma järelevalvevolitusi paindlikult ja asjakohaste õigusaktidega ettenähtud piirides, kasutades konkreetse tehisintellekti testkeskkonna projekti suhtes õigussätete rakendamisel oma kaalutlusõigust, et toetada tehisintellektialast innovatsiooni liidus.

Kui osaleja(d) järgib/järgivad lõike 6 punktis c osutatud testkeskkonna kava ja oma osalemise tingimusi ning järgib/järgivad heauskselt ametiasutuste antud juhiseid, ei määra ametiasutused haldustrahve testkeskkonnas jälgitava tehisintellektisüsteemi suhtes kohaldatavate liidu või liikmesriikide õigusaktide, sealhulgas käesoleva määruse sätete rikkumise eest.

4. Osalejad vastutavad kohaldatavate liidu ja liikmesriikide vastutusalaste õigusaktide alusel igasuguse kahju eest, mida nad on tekitanud tehisintellekti regulatsiooni testkeskkonnas osalemise käigus.

4a. Tehisintellektisüsteemi pakkuja või võimaliku pakkuja taotlusel esitab riigi pädev asutus vajaduse korral kirjaliku tõendi testkeskkonnas edukalt läbi viidud tegevuste kohta. Riigi pädev asutus esitab ka väljumisaruande, milles kirjeldatakse üksikasjalikult testkeskkonnas toimunud tegevusi ning sellega seotud tulemusi ja õpiväljundeid. Turujärelevalveasutused või teavitatud asutused võivad sellist kirjalikku tõendit ja väljumisaruannet vajaduse korral arvesse võtta vastavushindamismenetluste või turujärelevalve kontrollide raames.

Vastavalt artikli 70 konfidentsiaalsussätetele ja testkeskkonnas osalejate nõusolekul on Euroopa Komisjonil ja tehisintellekti nõukojal õigus saada juurdepääs väljumisaruannetele ning nad võtavad neid vajaduse korral arvesse oma käesolevast määrusest tulenevate ülesannete täitmisel. Kui nii osaleja kui ka riigi pädev asutus on sellega sõnaselgelt nõus, võib väljumisaruande teha artikli 55 lõike 3 punktis b osutatud ühtse teabeplatvormi kaudu üldsusele kättesaadavaks.

4b. Tehisintellekti regulatsiooni testkeskkonnad kavandatakse ja rakendatakse nii, et need hõlbustavad piiriülest koostööd riikide pädevate asutuste vahel, kui see on asjakohane.

5. Riigi pädevad asutused teevad üldsusele kättesaadavaks aastaaruanded tehisintellekti regulatsiooni testkeskkondade rakendamise kohta, kirjeldades muu hulgas nende ülesehitusega seotud häid tavasid, saadud kogemusi ja soovitusi, ning, kui see on asjakohane, ka käesoleva määruse ja muude testkeskkonnas jälgitavate liidu õigusaktide kohaldamise kohta. Need aastaaruanded esitatakse tehisintellekti nõukojale, kes teeb üldsusele kättesaadavaks kokkuvõtte kõigist headest tavadest, saadud kogemustest ja soovitustest. Kohustus teha aastaaruanded üldsusele kättesaadavaks ei hõlma õiguskaitse-, piirikontrolli-, rände- või varjupaigaasutuste tegevusega seotud tundlikke operatiivandmeid. Komisjon ja tehisintellekti nõukoda võtavad vajaduse korral aastaaruandeid arvesse oma käesolevast määrusest tulenevate ülesannete täitmisel.

5b. Komisjon tagab, et teave tehisintellekti regulatsiooni testkeskkondade, sealhulgas käesoleva artikli alusel loodud testkeskkondade kohta tehakse kättesaadavaks artikli 55 lõike 3 punktis b osutatud ühtse teabeplatvormi kaudu.

6. Käesoleva määruse kohaste tehisintellekti regulatsiooni testkeskkondade loomise ja toimimise kord ja tingimused võetakse vastu rakendusaktidega kooskõlas artikli 74 lõikes 2 osutatud kontrollimenetlusega.

Kord ja tingimused peavad võimalikult suures ulatuses toetama riigi pädevate asutuste paindlikkust oma tehisintellekti regulatsiooni testkeskkondade loomisel ja käitamisel, soodustama innovatsiooni ja regulatiivset õppimist ning võtma eelkõige arvesse osalevate VKEde, sealhulgas idufirmade eriolukorda ja suutlikkust.

Nimetatud rakendusaktid sisaldavad ühiseid peamisi põhimõtteid järgmistes küsimustes:

a) kõlblikkus ja valik tehisintellekti regulatsiooni testkeskkonnas osalemiseks;
b) tehisintellekti regulatsiooni testkeskkonna taotlemise, selles osalemise, selle seire, sellest väljumise ja selle lõpetamise kord, sealhulgas testkeskkonna kava ja väljumisaruanne;
c) osalejate suhtes kohaldatavad tingimused.

7. Kui riigi pädevad asutused kaaluvad tegelikes tingimustes testimise lubamist, mida jälgitakse käesoleva artikli alusel loodud tehisintellekti regulatsiooni testkeskkonna raames, lepivad nad osalejatega konkreetselt kokku sellise testimise tingimustes, eelkõige asjakohastes kaitsemeetmetes, et kaitsta põhiõigusi, tervist ja ohutust. Vajaduse korral teevad nad koostööd teiste riikide pädevate asutustega, et tagada ühtsed tavad kogu liidus.

Artikkel 54

Isikuandmete täiendav töötlemine tehisintellekti regulatsiooni testkeskkonnas teatavate tehisintellektisüsteemide arendamiseks avalikes huvides

1. Tehisintellekti regulatsiooni testkeskkonnas võidakse töödelda muuks otstarbeks seaduslikult kogutud isikuandmeid testkeskkonnas innovatiivsete tehisintellektisüsteemide arendamiseks, testimiseks ja treenimiseks järgmistel kumulatiivsetel tingimustel:

   a) innovatiivseid tehisintellektisüsteeme arendatakse selleks, et avaliku sektori asutus või muu avalik-õiguslik või eraõiguslik füüsiline või juriidiline isik saaks kaitsta olulisi avalikke huve ühes või mitmes järgmises valdkonnas:

      i) [välja jäetud]

      ii) avalik julgeolek ja rahvatervis, kaasa arvatud haiguste ennetamine, tõrje ja ravi ning tervishoiusüsteemide parandamine;

      iii) keskkonna kvaliteedi kaitse ja parandamine, sealhulgas rohepööre, kliimamuutuste leevendamine ja nendega kohanemine;

      iv) energiasäästlikkus, transport ja liikuvus;

      v) avaliku halduse ja avalike teenuste tõhusus ja kvaliteet;

      vi) küberturvalisus ja elutähtsa taristu vastupidavusvõime.

   b) töödeldud andmeid on vaja, et täita üht või mitut III jaotise 2. peatükis osutatud nõuet, kui neid nõudeid ei saa tulemuslikult täita anonüümitud andmete, tehisandmete või muude isikustamata andmete töötlemisega;

c) olemas on mõjusad seiremehhanismid, et teha kindlaks, kas testkeskkonnas toimuvate eksperimentide ajal võib tekkida suuri riske seoses andmesubjektide õiguste ja vabadustega, nagu on osutatud määruse (EL) 2016/679 artiklis 35 ja määruse (EL) 2018/1725 artiklis 39, ning reageerimismehhanism, mis võimaldab neid riske kiiresti leevendada ja vajaduse korral andmete töötlemise peatada;

d) testkeskkonnas töödeldavad isikuandmed paiknevad funktsionaalselt eraldiseisvas, isoleeritud ja kaitstud andmetöötluskeskkonnas osaliste kontrolli all ning neile on juurdepääs ainult volitatud isikutel;

e) töödeldud isikuandmeid ei tohi edastada ega üle anda ning need ei tohi olla testkeskkonnas mitteosalevatele isikutele muul moel kättesaadavad, välja arvatud juhul, kui selline avalikustamine toimub kooskõlas määrusega (EL) 2016/679, või kui see on asjakohane, määrusega (EL) 2018/1725, ja kui kõik osalejad on sellega nõustunud;

f) isikuandmete töötlemine testkeskkonnas ei mõjuta isikuandmete kaitset käsitlevas liidu õiguses, eelkõige määruse (EL) 2016/679 artiklis 22 ja määruse (EL) 2018/1725 artiklis 24 sätestatud andmesubjektide õiguste kohaldamist;

g) testkeskkonnas töödeldud isikuandmed on kaitstud asjakohaste tehniliste ja korralduslike meetmetega ja need kustutatakse, kui osalemine testkeskkonnas lõpeb või isikuandmete säilitamisperiood saab läbi;

h) isikuandmete testkeskkonnas töötlemise logisid hoitakse alles testkeskkonnas osalemise ajal, kui liidu või liikmesriigi õiguses ei ole sätestatud teisiti;

i) tehisintellektisüsteemi treenimise, testimise ja valideerimise protsessi ja põhjenduste täielikku ja üksikasjalikku kirjeldust säilitatakse koos testimistulemustega IV lisas osutatud tehnilises dokumentatsioonis;

j) testkeskkonnas arendatud tehisintellektiprojekti, selle eesmärkide ja eeldatavate tulemuste lühiülevaade avaldatakse pädevate asutuste veebisaidil. See kohustus ei hõlma õiguskaitse-, piirikontrolli-, rände- või varjupaigaasutuste tegevusega seotud tundlikke operatiivandmeid.

1a. Kuritegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil, õiguskaitseasutuste kontrolli all ja vastutusel, toimub isikuandmete töötlemine tehisintellekti regulatsiooni testkeskkondades konkreetse liikmesriigi või liidu õiguse alusel ja samadel kumulatiivsetel tingimustel, millele on osutatud lõikes 1.

2. Lõige 1 ei piira liidu või liikmesriikide selliste õigusaktide kohaldamist, millega kehtestatakse innovatiivsete tehisintellektisüsteemide arendamiseks, testimiseks ja treenimiseks vajalike isikuandmete töötlemise alus või mis tahes muu õiguslik alus kooskõlas isikuandmete kaitset käsitleva liidu õigusega.

Artikkel 54a

Suure riskiga tehisintellektisüsteemide testimine tegelikes tingimustes väljaspool tehisintellekti regulatsiooni testkeskkondi

1. Tehisintellektisüsteemide testimist tegelikes tingimustes väljaspool tehisintellekti regulatsiooni testkeskkondi võivad teostada III lisas loetletud suure riskiga tehisintellektisüsteemide pakkujad või võimalikud pakkujad kooskõlas käesoleva artikli sätetega ja vastavalt käesolevas artiklis osutatud tegelikes tingimustes testimise kavale.

Tegelikes tingimustes testimise kava üksikasjalikud elemendid täpsustatakse rakendusaktides, mille komisjon võtab vastu kooskõlas artikli 74 lõikes 2 osutatud kontrollimenetlusega.

Käesolev säte ei piira liidu või liikmesriikide õigusaktide kohaldamist, mis käsitlevad II lisas loetletud õigusaktidega hõlmatud toodetega seotud suure riskiga tehisintellektisüsteemide tegelikes tingimustes testimist.

2. Pakkujad või võimalikud pakkujad võivad teostada III lisas osutatud suure riskiga tehisintellektisüsteemide tegelikes tingimustes testimist igal ajal enne tehisintellektisüsteemi turule laskmist või kasutusele võtmist kas iseseisvalt või partnerluses ühe või mitme võimaliku kasutajaga.

3. Suure riskiga tehisintellektisüsteemide tegelikes tingimustes testimine käesoleva artikli alusel ei piira eetikaalast hindamist, mida võidakse nõuda liikmesriikide või liidu õiguse kohaselt.

4. Pakkujad või võimalikud pakkujad võivad teostada tegelikes tingimustes testimist ainult siis, kui on täidetud kõik järgmised tingimused:

a) pakkuja või võimalik pakkuja on koostanud tegelikes tingimustes testimise kava ja esitanud kõnealuse kava selle liikmesriigi või nende liikmesriikide turujärelevalveasutusele, kus tegelikes tingimustes testimine teostatakse;

b) selle liikmesriigi või nende liikmesriikide turujärelevalveasutus, kus tegelikes tingimustes testimine teostatakse, ei ole 30 päeva jooksul pärast plaani esitamist testimisele vastuväiteid esitanud;

c) pakkuja või võimalik pakkuja, välja arvatud III lisa punktides 1, 6 ja 7 osutatud õiguskaitse-, rände-, varjupaiga- ja piirikontrollihalduse valdkonna suure riskiga tehisintellektisüsteemide ning III lisa punktis 2 osutatud suure riskiga tehisintellektisüsteemide puhul, on registreerinud tegelikes tingimustes testimise artikli 60 lõikes 5a osutatud ELi andmebaasis üleliidulise kordumatu ühtse identifitseerimisnumbriga ja VIIIa lisas täpsustatud teabega;

d) tegelikes tingimustes testimist teostav pakkuja või võimalik pakkuja asub liidus või on määranud tegelikes tingimustes testimise jaoks liidus asuva seadusliku esindaja;

e) tegelikes tingimustes testimiseks kogutud ja töödeldud andmeid ei edastata väljaspool liitu asuvatele riikidele, välja arvatud siis, kui edastamine ja töötlemine toimub liidu õiguses ette nähtud kaitsemeetmetega samaväärsete kaitsemeetmete tingimustes;

f) tegelikes tingimustes testimine ei kesta kauem, kui on vaja selle eesmärkide saavutamiseks, ja igal juhul mitte kauem kui 12 kuud;

g) isikud, kes oma vanuse, füüsilise või vaimse puude tõttu kuuluvad haavatavatesse rühmadesse, on asjakohaselt kaitstud;

h) [välja jäetud]

i) kui pakkuja või võimalik pakkuja korraldab tegelikes tingimustes testimise koostöös ühe või mitme võimaliku kasutajaga, on neid teavitatud kõigist testimise aspektidest, mis on nende osalemisotsuse seisukohast olulised, ning neile on antud artiklis 13 osutatud asjakohased juhised tehisintellektisüsteemi kasutamise kohta; pakkuja või võimalik pakkuja ja kasutaja(d) sõlmivad lepingu, milles on täpsustatud nende rollid ja kohustused, et tagada vastavus käesoleva määruse ning muude kohaldatavate liidu ja liikmesriikide õigusaktide sätetele tegelikes tingimustes testimise kohta;

j) tegelikes tingimustes testimises osalejad on andnud teadva nõusoleku vastavalt artiklile 54b, või õiguskaitse puhul, kui teadva nõusoleku taotlemine takistaks tehisintellektisüsteemi testimist, ei mõjuta tegelikes tingimustes testimine ega selle tulemused testimises osalejat negatiivselt;

k) tegelikes tingimustes testimise üle teostavad reaalset järelevalvet pakkuja või võimalik pakkuja ja kasutaja(d) koos isikutega, kellel on sobiv kvalifikatsioon asjaomases valdkonnas ning oma ülesannete täitmiseks vajalik suutlikkus ja väljaõpe ning vastavad õigused;

l) tehisintellektisüsteemi prognoose, soovitusi või otsuseid saab tulemuslikult tagasi võtta või kõrvale jätta.

5. Iga tegelikes tingimustes testimises osaleja või asjakohasel juhul tema seaduslik esindaja võib testimisest igal ajal, kahju kandmata ja selgitusi andmata lahkuda, tühistades oma teadva nõusoleku. Teadva nõusoleku tagasivõtmine ei mõjuta juba tehtud tegevusi ega teadva nõusoleku alusel enne tagasivõtmist saadud andmete kasutamist.

6. Igast tegelikes tingimustes testimise käigus tuvastatud tõsisest intsidendist teatatakse riiklikule turujärelevalveasutusele kooskõlas käesoleva määruse artikliga 62. Pakkuja või võimalik pakkuja võtab viivitamata leevendusmeetmeid, või kui see ei ole võimalik, siis peatab tegelikes tingimustes testimise kuni leevendamiseni, või lõpetab selle muul viisil. Pakkuja või võimalik pakkuja kehtestab sellise tegelikes tingimustes testimise lõpetamise puhuks menetluse tehisintellektisüsteemi viivitamatuks tagasikutsumiseks.

7. Pakkujad või võimalikud pakkujad teavitavad selle liikmesriigi või nende liikmesriikide turujärelevalveasutust, kus tegelikes tingimustes testimine teostatakse, tegelikes tingimustes testimise peatamisest või lõpetamisest ja selle lõpptulemustest.

8. Pakkuja ja võimalik pakkuja vastutavad kohaldatavate liidu ja liikmesriikide vastutust käsitlevate õigusaktide alusel igasuguse kahju eest, mida nad on tekitanud tegelikes tingimustes testimises osalemise käigus.

Artikkel 54b

Teadev nõusolek osalemiseks testimises tegelikes tingimustes väljaspool tehisintellekti regulatsiooni testkeskkondi

1. Artikli 54a kohaseks tegelikes tingimustes testimiseks annab testimises osaleja vabal tahtel teadva nõusoleku, tehes seda enne sellises testimises osalemist ja pärast seda, kui talle on nõuetekohaselt antud täpset, selget, asjakohast ja arusaadavat teavet järgmise kohta:

i) tegelikes tingimustes testimise laad ja selle eesmärgid ning võimalikud ebamugavused, mis võivad olla tema osalemisega seotud;

ii) tingimused, mille alusel tegelikes tingimustes testimine teostatakse, sealhulgas testimises osaleja osalemise eeldatav kestus;

iii) osaleja osalemisega seotud õigused ja tagatised, eelkõige õigus igal ajal keelduda tegelikes tingimustes testimises osalemisest ja testimisest lahkuda, ilma et ta kannaks kahju või peaks andma selgitusi;

iv) tehisintellektisüsteemi prognooside, soovituste või otsuste tagasivõtmise või kõrvalejätmise kord;

v) artikli 54a lõike 4 punkti c kohane tegelikes tingimustes testimise üleliiduline kordumatu ühtne identifitseerimisnumber ning selle pakkuja või tema seadusliku esindaja kontaktandmed, kellelt on võimalik saada lisateavet.

2. Teadev nõusolek peab olema kuupäevastatud ja dokumenteeritud ning selle koopia antakse testimises osalejale või tema seaduslikule esindajale.

Artikkel 55

Toetusmeetmed operaatoritele, eelkõige VKEdele, sealhulgas idufirmadele

1. Liikmesriigid teevad järgmist:

a) annavad VKEdele, sealhulgas idufirmadele eelisjuurdepääsu tehisintellekti regulatsiooni testkeskkonnale, eeldusel et nad vastavad kõlblikkus- ja valikukriteeriumidele;

b) korraldavad just VKEde, sealhulgas idufirmade ja kui see on asjakohane, kohalike ametiasutuste vajadustest lähtuvaid konkreetseid teadlikkuse suurendamise üritusi ja koolitusi käesoleva määruse kohaldamise kohta;

c) loovad asjakohasel juhul spetsiaalse kanali VKEde, sealhulgas idufirmadega, ja kui see on asjakohane, kohalike ametiasutustega suhtlemiseks, et anda nõu ja vastata päringutele käesoleva määruse rakendamise kohta, sealhulgas seoses osalemisega tehisintellekti regulatsiooni testkeskkondades.

2. Artikli 43 kohase vastavushindamise tasude kehtestamisel võetakse arvesse VKEdest pakkujate, sealhulgas idufirmade konkreetseid huve ja vajadusi ning vähendatakse neid tasusid proportsionaalselt, lähtudes nende suurusest, turumahust ja muudest asjaomastest näitajatest.

3. Komisjon teeb järgmist:

a) esitab tehisintellekti nõukoja taotlusel standardvormid käesoleva määrusega hõlmatud valdkondade jaoks;

b) töötab välja ühtse teabeplatvormi, mis pakub kõigile operaatoritele kogu liidus hõlpsasti kasutatavat teavet käesoleva määruse kohta, ja haldab seda platvormi;

c) korraldab asjakohaseid teavituskampaaniaid, et suurendada teadlikkust käesolevast määrusest tulenevatest kohustustest;

d) hindab ja edendab tehisintellektisüsteemidega seotud riigihankemenetluste parimate tavade lähendamist.

Artikkel 55a

Erandid konkreetsete operaatorite suhtes

1. Käesoleva määruse artiklis 17 sätestatud kohustusi ei kohaldata mikroettevõtjate suhtes, nagu on määratletud komisjoni soovituse 2003/361/EÜ (mikro-, väikeste ja keskmise suurusega ettevõtjate määratluse kohta) lisa artikli 2 lõikes 3, tingimusel et neil ettevõtjatel ei ole sama lisa artiklis 3 määratletud partnerettevõtjaid ega sidusettevõtjaid.

2. Lõiget 1 ei tõlgendata nii, et see vabastaks need operaatorid muude käesolevas määruses sätestatud nõuete ja kohustuste täitmisest, sealhulgas artiklites 9, 61 ja 62 sätestatud nõuete ja kohustuste täitmisest.

3. Artiklis 4b sätestatud üldotstarbeliste tehisintellektisüsteemide nõudeid ja kohustusi ei kohaldata mikro-, väikeste ja keskmise suurusega ettevõtjate suhtes, tingimusel et neil ettevõtjatel ei ole partnerettevõtjaid ega sidusettevõtjaid, nagu on määratletud komisjoni soovituse 2003/361/EÜ (mikro-, väikeste ja keskmise suurusega ettevõtjate määratluse kohta) lisa artiklis 3.

VI JAOTIS

JUHTIMINE

1. PEATÜKK

EUROOPA TEHISINTELLEKTI NÕUKODA

Artikkel 56

Euroopa tehisintellekti nõukoja loomine ja selle struktuur

1. Luuakse Euroopa tehisintellekti nõukoda (edaspidi „nõukoda“).

2. Nõukoda koosneb ühest esindajast iga liikmesriigi kohta. Euroopa Andmekaitseinspektor osaleb vaatlejana. Komisjon osaleb samuti nõukoja koosolekutel, kuid hääletamisest osa ei võta.

   Nõukoda võib kutsuda koosolekutele muid riiklikke ja liidu asutusi, organeid või eksperte iga juhtumi puhul eraldi, kui arutlusel olevad küsimused on nende jaoks olulised.

2a. Liikmesriik nimetab oma esindaja kolmeks aastaks ja seda perioodi võib ühe korra pikendada.

2aa. Liikmesriigid tagavad, et nende esindajad nõukojas:

   i) omavad oma liikmesriigis asjakohast pädevust ja volitusi, et aidata aktiivselt kaasa nõukoja artiklis 58 osutatud ülesannete täitmisele;

   ii) määratakse ühtseks kontaktpunktiks nõukojas ja kui see on liikmesriikide vajadusi arvesse võttes asjakohane, siis sidusrühmade ühtseks kontaktpunktiks;

iii) on volitatud hõlbustama oma liikmesriigi pädevate asutuste järjepidevust ja nendevahelist koordineerimist seoses käesoleva määruse rakendamisega, sealhulgas kogudes asjakohaseid andmeid ja teavet, et täita oma ülesandeid nõukojas.

3. Liikmesriikide määratud esindajad võtavad kahekolmandikulise häälteenamusega vastu nõukoja töökorra.

Töökorras sätestatakse eelkõige eesistuja valimise menetluse kord, tema volituste kestus ja tema ülesannete kirjeldus, hääletuskord ning nõukoja ja selle allrühmade tegevuse korraldus.

Nõukoda moodustab alalise allrühma, mis toimib sidusrühmade platvormina, et nõustada nõukoda kõigis käesoleva määruse rakendamisega seotud küsimustes, sealhulgas rakendusaktide ja delegeeritud õigusaktide ettevalmistamisel. Selleks kutsutakse sellesse allrühma osalema organisatsioonid, kes esindavad tehisintellektisüsteemide pakkujate ja kasutajate huve, sealhulgas VKEd ja idufirmad, samuti kodanikuühiskonna organisatsioonid, mõjutatud isikute esindajad, teadlased, standardiorganisatsioonid, teavitatud asutused, laborid ning testimis- ja eksperimenteerimisasutused. Nõukoda moodustab kaks alalist allrühma, et luua platvorm turujärelevalveasutuste ja teavitavate asutuste vaheliseks koostööks ja teabevahetuseks turujärelevalve ja teavitatud asutustega seotud küsimustes.

Nõukoda võib vastavalt vajadusele moodustada konkreetsete küsimuste uurimiseks muid alalisi või ajutisi allrühmi. Kui see on asjakohane, võib sellistesse allrühmadesse või nende allrühmade konkreetsetele koosolekutele vaatlejatena kutsuda eelmises lõigus osutatud sidusrühmi.

3a. Nõukoda on organiseeritud ja seda juhitakse nii, et oleks tagatud tema tegevuse objektiivsus ja erapooletus.

4. Nõukoja eesistuja on üks liikmesriikide esindajatest. Eesistuja taotlusel kutsub komisjon kokku koosolekud ja valmistab ette päevakorra vastavalt nõukoja käesolevast määrusest tulenevatele ülesannetele ja nõukoja töökorrale. Komisjon pakub nõukoja käesoleva määruse kohaseks tegevuseks haldus- ja analüütilist tuge.

Artikkel 57

[välja jäetud]

Artikkel 58

Nõukoja ülesanded

Nõukoda nõustab ja abistab komisjoni ja liikmesriike, et hõlbustada käesoleva määruse järjepidevat ja tõhusat kohaldamist. Selleks võib nõukoda eelkõige:

a) koguda ja jagada tehnilisi ja regulatiivseid eksperditeadmisi ja parimaid tavasid liikmesriikides;

b) aidata kaasa haldustavade ühtlustamisele liikmesriikides, sealhulgas seoses artiklis 47 osutatud erandiga vastavushindamismenetlustest ning seoses artiklites 53, 54 ja 54a osutatud regulatsiooni testkeskkondade toimimisega ja katsetega tegelikes tingimustes;

c) esitada komisjoni taotluse korral või omal algatusel soovitusi ja kirjalikke arvamusi mis tahes asjakohastes küsimustes, mis on seotud käesoleva määruse rakendamise ning selle järjepideva ja tõhusa kohaldamisega, mis hõlmab järgmist:

   i) III jaotise 2. peatükis sätestatud nõudeid käsitlevad tehnilised kirjeldused või kehtivad standardid,

   ii) artiklites 40 ja 41 osutatud harmoneeritud standardite või ühtsete kirjelduste kasutamine,

iii) juhenddokumentide, sh artiklis 71 osutatud haldustrahvide määramise suuniste ettevalmistamine;

d) nõustada komisjoni võimaliku vajaduse osas muuta III lisa kooskõlas artiklitega 4 ja 7, võttes arvesse asjakohaseid kättesaadavaid tõendeid ja uusimaid arenguid tehnoloogias;

e) nõustada komisjoni käesoleva määruse kohase delegeeritud õigusakti või rakendusakti ettevalmistamise;

f) teha vajaduse korral koostööd asjaomaste ELi asutuste, eksperdirühmade ja võrgustikega, eelkõige tooteohutuse, küberturvalisuse, konkurentsi, digi- ja meediateenuste, finantsteenuste, krüptoraha, tarbijakaitse, andmete ja põhiõiguste kaitse valdkonnas;

g) anda komisjonile asjakohast nõu artiklis 58a osutatud suuniste väljatöötamisel või taotleda selliste suuniste väljatöötamist;

h) toetada turujärelevalveasutuste tööd ning koostöös asjaomaste turujärelevalveasutustega ja nende nõusolekul edendada ja toetada piiriüleseid turujärelevalve uurimisi, sealhulgas seoses tehisintellektisüsteemidest tuleneda võivate süsteemsete riskide tekkimisega;

i) aidata hinnata käesoleva määruse rakendamisega seotud liikmesriikide töötajate koolitusvajadusi;

j) nõustada komisjoni tehisintellekti käsitlevates rahvusvahelistes küsimustes.

1A. PEATÜKK

KOMISJONI SUUNISED

Artikkel 58a

Komisjoni suunised käesoleva määruse rakendamise kohta

1. Komisjon annab liikmesriikide või nõukoja taotlusel või omal algatusel välja suunised käesoleva määruse praktilise rakendamise kohta, eelkõige seoses järgmisega:

   i) artiklites 8–15 osutatud nõuete kohaldamine;

   ii) artiklis 5 osutatud keelatud kasutusviisid;

   iii) oluliste muudatustega seotud sätete praktiline rakendamine;

   iv) artikli 6 lõikes 3 osutatud ühtsete tingimuste praktiline rakendamine, sealhulgas näited III lisas osutatud suure riskiga tehisintellektisüsteemide kohta;

   v) artiklis 52 sätestatud läbipaistvuskohustuste praktiline rakendamine;

   vi) käesoleva määruse seos muude asjakohaste liidu õigusaktidega, sealhulgas nende täitmise tagamise järjepidevus.

Selliste suuniste väljaandmisel pöörab komisjon erilist tähelepanu VKEde, sealhulgas idufirmade, kohalike ametiasutuste ja selliste sektorite vajadustele, mida käesolev määrus kõige tõenäolisemalt mõjutab.

2. PEATÜKK

RIIKIDE PÄDEVAD ASUTUSED

Artikkel 59

Riikide pädevate asutuste määramine

1. [välja jäetud]

2. Iga liikmesriik loob või määrab käesoleva määruse kohaldamiseks riiklikeks pädevateks asutusteks vähemalt ühe teavitava asutuse ja vähemalt ühe turujärelevalveasutuse. Need riigi pädevad asutused korraldatakse nii, et kindlustada nende tegevuse ja ülesannete puhul objektiivsuse ja erapooletuse põhimõtete kohaldamine. Tingimusel, et austatakse nimetatud põhimõtteid, võivad selliseid tegevusi ja ülesandeid vastavalt liikmesriigi organisatsioonilistele vajadustele täita üks või mitu määratud asutust.

3. Liikmesriigid teavitavad komisjoni enda määratud asutustest.

4. Liikmesriigid tagavad, et riigi pädevatel asutustel on käesolevast määrusest tulenevate ülesannete tõhusaks täitmiseks piisavad rahalised vahendid, tehnilised seadmed ja kõrge kvalifikatsiooniga inimressursid.

5. Hiljemalt *[üks aasta pärast käesoleva määruse jõustumist]* ja seejärel kuus kuud enne artikli 84 lõikes 2 osutatud tähtaega teavitavad liikmesriigid komisjoni riigi pädevate asutuste rahaliste vahendite, tehniliste seadmete ja inimressursside olukorrast, hinnates sealjuures nende piisavust. Komisjon edastab selle teabe nõukojale arutamiseks ja võimalikeks soovitusteks.

6. Komisjon hõlbustab riikide pädevate asutuste vahelist kogemuste vahetamist.

7. Riigi pädevad asutused võivad anda nõu käesoleva määruse rakendamise kohta, sealhulgas VKEdest pakkujate (sh idufirmad) jaoks kohandatud nõu. Kui riigi pädevad asutused kavatsevad anda juhiseid ja nõu tehisintellektisüsteemi kohta valdkondades, mille suhtes kehtivad ka muud liidu õigusaktid, konsulteeritakse vastavalt vajadusele nende liidu õigusaktide alusel pädevate riiklike asutustega. Liikmesriigid võivad luua operaatoritega suhtlemiseks ka ühe keskse kontaktpunkti.

8. Kui liidu institutsioonid, organid ja asutused kuuluvad käesoleva määruse kohaldamisalasse, tegutseb nende järelevalve teostamisel pädeva asutusena Euroopa Andmekaitseinspektor.

VII JAOTIS

III LISAS LOETLETUD SUURE RISKIGA TEHISINTELLEKTISÜSTEEMIDE ELI ANDMEBAAS

Artikkel 60

III lisas loetletud suure riskiga tehisintellektisüsteemide ELi andmebaas

1. Komisjon loob koostöös liikmesriikidega ELi andmebaasi, mis sisaldab lõikes 2 osutatud teavet asjaomaste operaatorite ja III lisas loetletud suure riskiga tehisintellektisüsteemide kohta, mis on registreeritud vastavalt artiklitele 51 ja 54a, ning haldab seda. Sellise andmebaasi funktsionaalsete kirjelduste määratlemisel konsulteerib komisjon tehisintellekti nõukojaga.

2. VIII lisa I osas loetletud andmed sisestavad ELi andmebaasi vastavalt vajadusele pakkujad, volitatud esindajad ja asjaomased kasutajad nende registreerimisel. VIII lisa II osa punktides 1–11 loetletud andmed sisestavad ELi andmebaasi pakkujad või vajaduse korral volitatud esindaja kooskõlas artikliga 51. VIII lisa II osa punktis 12 osutatud andmed genereerib andmebaas automaatselt asjaomaste kasutajate poolt artikli 51 lõike 2 kohaselt esitatud teabe põhjal. VIIIa lisas loetletud andmed sisestavad andmebaasi võimalikud pakkujad või pakkujad kooskõlas artikliga 54a.

3. [välja jäetud]

4. ELi andmebaas ei sisalda isikuandmeid, välja arvatud VIII lisas loetletud teave, ning see ei piira artikli 70 kohaldamist.

5. ELi andmebaasi vastutav töötleja on komisjon. Komisjon teeb pakkujatele, võimalikele pakkujatele ja kasutajatele kättesaadavaks piisava tehnilise ja haldustoe.

5a. ELi andmebaasis sisalduv teave, mis on registreeritud vastavalt artiklile 51, on üldsusele kättesaadav. Artikli 54a kohaselt registreeritud teave on kättesaadav üksnes turujärelevalveasutustele ja komisjonile, välja arvatud juhul, kui võimalik pakkuja või pakkuja on andnud nõusoleku selle teabe avalikustamiseks.

VIII JAOTIS

TURUSTAMISJÄRGNE SEIRE, TEABE JAGAMINE, TURUJÄRELEVALVE

1. PEATÜKK

TURUSTAMISJÄRGNE SEIRE

Artikkel 61

Pakkujapoolne turustamisjärgne seire ja suure riskiga tehisintellektisüsteemide turustamisjärgse seire kava

1. Pakkujad kehtestavad turustamisjärgse seire süsteemi ja dokumenteerivad selle viisil, mis on proportsionaalne suure riskiga tehisintellektisüsteemi riskidega.

2. Selleks et pakkuja saaks hinnata tehisintellektisüsteemide vastavust III jaotise 2. peatükis sätestatud nõuetele kogu nende olelusringi jooksul, kogub, dokumenteerib ja analüüsib turustamisjärgse seire süsteem asjakohaseid andmeid suure riskiga tehisintellektisüsteemide toimimise kohta, mida võivad esitada kasutajad või mida võidakse koguda muude allikate kaudu. See kohustus ei hõlma õiguskaitseasutustest tehisintellektisüsteemide kasutajate tundlikke operatiivandmeid.

3. Turustamisjärgse seire süsteem peab põhinema turustamisjärgse seire kaval. Turustamisjärgse seire kava on IV lisas osutatud tehnilise dokumentatsiooni osa. Komisjon võtab vastu rakendusakti, millega nähakse ette üksikasjalikud sätted turustamisjärgse seire kava vormi ja kavas sisalduvate elementide loetelu kehtestamise kohta.

4. Kui tegemist on II lisa A osas osutatud õigusaktide kohaldamisalasse kuuluva suure riskiga tehisintellektisüsteemiga, mille turustamisjärgse seire süsteem ja kava on nende õigusaktide alusel juba kehtestatud, loetakse nende õigusaktide alusel koostatud turustamisjärgse seire dokumentatsioon piisavaks tingimusel, et kasutatakse lõikes 3 osutatud vormi.

Esimest lõiku kohaldatakse ka III lisa punktis 5 osutatud suure riskiga tehisintellektisüsteemide suhtes, mille on turule lasknud või kasutusele võtnud finantsasutused, kelle suhtes kohaldatakse finantsteenuseid käsitlevate liidu õigusaktide kohaseid nõudeid seoses nende sisemise juhtimise, korra või protsessidega.

2. PEATÜKK

TEABE JAGAMINE TÕSISTE INTSIDENTIDE KOHTA

Artikkel 62

Tõsistest intsidentidest teatamine

1. Liidu turule lastud suure riskiga tehisintellektisüsteemide pakkujad teatavad igast tõsisest intsidendist nende liikmesriikide turujärelevalveasutustele, kus intsident aset leidis.

Teatamine peab toimuma kohe pärast seda, kui pakkuja on teinud kindlaks, et tehisintellektisüsteemi ja tõsise intsidendi vahel on põhjuslik seos või et selline seos on põhjendatult tõenäoline, ning igal juhul hiljemalt 15 päeva pärast seda, kui pakkuja sai tõsisest intsidendist teadlikuks.

2. Kui asjaomane turujärelevalveasutus saab teate artikli 3 lõike 44 punktis c osutatud tõsise intsidendi kohta, teatab ta sellest artikli 64 lõikes 3 osutatud riiklikele ametiasutustele või organitele. Komisjon töötab välja eraldi juhendi, et hõlbustada lõikes 1 sätestatud kohustuste täitmist. Juhend antakse välja hiljemalt 12 kuud pärast käesoleva määruse jõustumist.

3. III lisa punktis 5 osutatud suure riskiga tehisintellektisüsteemide puhul, mille on turule lasknud või kasutusele võtnud finantsasutustest pakkujad, kelle suhtes kohaldatakse finantsteenuseid käsitlevate liidu õigusaktide kohaseid nõudeid seoses nende sisemise juhtimise, korra või protsessidega, piirdub tõsistest intsidentidest teatamine artikli 3 lõike 44 punktis c osutatud juhtudega.

4. Suure riskiga tehisintellektisüsteemide puhul, mis on selliste seadmete turvakomponendid või mis on ise sellised seadmed, mille suhtes kohaldatakse määrust (EL) 2017/745 ja määrust (EL) 2017/746, teavitatakse tõsistest intsidentidest ainult artikli 3 lõike 44 punktis c osutatud juhtudel ning nendest teatatakse nende liikmesriikide vastavatele pädevatele asutustele, kus intsident aset leidis.

3. PEATÜKK

TÄITMISE TAGAMINE

Artikkel 63

Tehisintellektisüsteemide turujärelevalve ja kontroll liidu turul

1. Käesoleva määruse kohaldamisalasse kuuluvate tehisintellektisüsteemide suhtes kohaldatakse määrust (EL) 2019/1020. Käesoleva määruse tulemusliku täitmise tagamiseks:

   a) käsitatakse kõiki määruse (EL) 2019/1020 kohaseid viiteid ettevõtjatele viidetena, mis hõlmavad kõiki käesoleva määruse artiklis 2 kindlaks määratud operaatoreid;

   b) käsitatakse kõiki määruse (EL) 2019/1020 kohaseid viiteid toodetele viidetena, mis hõlmavad kõiki käesoleva määruse kohaldamisalasse kuuluvaid tehisintellektisüsteeme.

2. Osana määruse (EL) 2019/1020 artikli 34 lõike 4 kohastest aruandluskohustustest esitavad turujärelevalveasutused komisjonile aruande käesoleva määruse kohaste asjakohaste turujärelevalvetoimingute tulemuste kohta.

3. Käesoleva määruse kohaldamisel on II lisa A jaos loetletud õigusaktidega reguleeritud toodetega seotud suure riskiga tehisintellektisüsteemide puhul turujärelevalveasutuseks nende õigusaktide alusel määratud ametiasutus, kes vastutab turujärelevalvetoimingute eest, või põhjendatud asjaoludel ja tingimusel, et tagatud on koordineerimine, liikmesriigi poolt kindlaks määratud muu asjaomane asutus.

   Käesoleva määruse artiklites 65, 66, 67 ja 68 osutatud menetlusi ei kohaldata selliste tehisintellektisüsteemide suhtes, mis on seotud toodetega, mille suhtes kohaldatakse II lisa A jaos loetletud õigusakte, kui selliste õigusaktidega on juba ette nähtud sama eesmärgiga menetlused. Sellisel juhul kohaldatakse selle asemel kõnealuseid valdkondlikke menetlusi.

4. Käesoleva määruse kohaldamisel on finantsteenuseid käsitlevate liidu õigusaktidega reguleeritud finantsasutuste poolt turule lastud, kasutusele võetud või kasutatavate suure riskiga tehisintellektisüsteemide puhul turujärelevalveasutuseks riigi asjaomane ametiasutus, kes vastutab kõnealuste õigusaktide kohaselt nende asutuste finantsjärelevalve eest, niivõrd, kuivõrd tehisintellektisüsteemi turule laskmine, kasutusele võtmine või kasutamine on otseselt seotud kõnealuste finantsteenuste osutamisega.

   Erandina eelmisest lõigust võib liikmesriik põhjendatud asjaoludel ja tingimusel, et tagatud on koordineerimine, määrata käesoleva määruse kohaldamisel turujärelevalveasutuseks mõne teise asjaomase asutuse.

   Riiklikud turujärelevalveasutused, kes teostavad järelevalvet direktiivi 2013/36/EL kohaldamisalasse kuuluvate reguleeritud krediidiasutuste üle ja kes osalevad nõukogu määrusega nr 1024/2013 loodud ühtses järelevalvemehhanismis, peaksid viivitamata esitama Euroopa Keskpangale turujärelevalvetoimingute käigus kindlaks tehtud teabe, mis võib pakkuda huvi seoses kõnealuses määruses sätestatud Euroopa Keskpanga usaldatavusnõuete täitmise järelevalve ülesannetega.

5. Suure riskiga tehisintellektisüsteemide puhul, mis on loetletud III lisa punkti 1 alapunktis a (niivõrd, kuivõrd neid süsteeme kasutatakse õiguskaitse eesmärgil) ning punktides 6, 7 ja 8, määravad liikmesriigid käesoleva määruse kohaldamisel turujärelevalveasutuseks kas riiklikud asutused, kes teostavad järelevalvet õiguskaitse-, piirikontrolli-, rände-, varjupaiga- või õigusasutuste tegevuse üle, või direktiivi (EL) 2016/680 või määruse (EL) 2016/679 kohaselt pädevad andmekaitse järelevalveasutused. Turujärelevalvetoimingud ei mõjuta mingil viisil õigusasutuste sõltumatust ega sekku muul viisil nende tegevusse, kui nad tegutsevad õigusemõistjana.

6. Kui liidu institutsioonid, organid ja asutused kuuluvad käesoleva määruse kohaldamisalasse, tegutseb nende turujärelevalveasutusena Euroopa Andmekaitseinspektor.

7. Liikmesriigid hõlbustavad koordineerimist käesoleva määruse alusel määratud turujärelevalveasutuste ja muude asjaomaste riiklike asutuste või organite vahel, kes teevad järelevalvet II lisas loetletud liidu ühtlustamisõigusaktide või muude III lisas osutatud suure riskiga tehisintellektisüsteemide seisukohast oluliste liidu õigusaktide kohaldamise üle.

8. Ilma et see piiraks määrusega (EL) 2019/1020 antud volitusi, ning kui see on asjakohane ja piiratud nende ülesannete täitmiseks vajalikuga, annab pakkuja turujärelevalveasutustele täieliku juurdepääsu dokumentatsioonile ning suure riskiga tehisintellektisüsteemi arendamiseks kasutatavatele treenimis-, valideerimis- ja testimisandmestikele, sealhulgas, kui see on asjakohane ja kohaldades turvameetmeid, rakendusliideste (API) või muude sobivate kaugjuurdepääsu võimaldavate tehniliste vahendite ja tööriistade kaudu.

9. Juurdepääs suure riskiga tehisintellektisüsteemi lähtekoodile antakse turujärelevalveasutustele põhjendatud taotluse alusel ja ainult juhul, kui on täidetud järgmised kumulatiivsed tingimused:

a) juurdepääs lähtekoodile on vajalik selleks, et hinnata suure riskiga tehisintellektisüsteemi vastavust III jaotise 2. peatükis sätestatud nõuetele, ning

b) pakkuja esitatud andmetel ja dokumentatsioonil põhinevad testimis-/auditeerimismenetlused ja kontrollid on ammendatud või osutunud ebapiisavaks.

10. Turujärelevalveasutuste poolt saadud teabe ja dokumentatsiooni käsitlemisel täidetakse artiklis 70 sätestatud konfidentsiaalsuskohustusi.

11. Iga füüsiline või juriidiline isik, kellel on alust arvata, et käesoleva määruse sätteid on rikutud, võib esitada asjaomasele turujärelevalveasutusele kaebuse.

Kooskõlas määruse (EL) 2019/1020 artikli 11 lõike 3 punktiga e ja lõike 7 punktiga a võetakse kaebusi turujärelevalvetoimingute tegemisel arvesse ja neid käsitletakse turujärelevalveasutuste poolt selleks kehtestatud erimenetluste kohaselt.

Artikkel 63a

Turujärelevalveasutuste järelevalve tegelikes tingimustes testimise üle

1. Turujärelevalveasutustel on pädevus ja volitused tagada, et tegelikes tingimustes testimine on käesoleva määrusega kooskõlas.

2. Kui tehisintellektisüsteeme, mille üle tehakse artikli 54 kohaselt järelevalvet tehisintellekti regulatsiooni testkeskkonnas, testitakse tegelikes tingimustes, kontrollivad turujärelevalveasutused vastavust artikli 54a sätetele osana oma järelevalverollist tehisintellekti regulatsiooni testkeskkonnas. Pakkujale või võimalikule pakkujale tegelikes tingimustes testimise lubamiseks võivad need asutused teha vajaduse korral erandi artikli 54a lõike 4 punktides f ja g sätestatud tingimustest.

3. Kui turujärelevalveasutus on saanud pakkujalt, võimalikult pakkujalt või tõsise intsidendi kolmandalt osapoolelt teavet või kui tal on muud alust arvata, et artiklites 54a ja 54b sätestatud tingimused ei ole täidetud, võib ta vajaduse korral teha oma territooriumil mis tahes järgmise otsuse:

a) peatada või lõpetada testimine tegelikes tingimustes;

b) nõuda pakkujalt või võimalikult pakkujalt ja kasutaja(te)lt tegelikes tingimustes testimise mis tahes aspekti muutmist.

4. Kui turujärelevalveasutus on teinud käesoleva artikli lõikes 3 osutatud otsuse või esitanud vastuväite artikli 54a lõike 4 punkti b tähenduses, märgitakse otsuses või vastuväites selle põhjused ning üksikasjad ja tingimused, mille alusel pakkuja või võimalik pakkuja saab otsuse või vastuväite vaidlustada.

5. Kui turujärelevalveasutus on teinud käesoleva artikli lõikes 3 osutatud otsuse, teavitab ta vajaduse korral selle põhjustest teiste liikmesriikide turujärelevalveasutusi, kus tehisintellektisüsteemi testimise kava kohaselt testiti.

Artikkel 64

Põhiõigusi kaitsvate asutuste volitused

1. [välja jäetud]

2. [välja jäetud]

3. Riiklikel ametiasutustel või organitel, kes tegelevad põhiõiguste, sealhulgas mittediskrimineerimise õiguse kaitse alastest liidu õigusaktidest tulenevate kohustuste täitmise järelevalve või tagamisega seoses III lisas osutatud suure riskiga tehisintellektisüsteemide kasutamisega, on õigus taotleda mis tahes dokumentatsiooni, mis on loodud või mida hoitakse käesoleva määruse alusel, ja saada sellele juurdepääs, kui juurdepääs sellisele dokumentatsioonile on vajalik nende ülesannetest tulenevate kohustuste täitmiseks nende jurisdiktsiooni piires. Asjaomane avaliku sektori asutus või organ teatab igast sellisest taotlusest asjaomase liikmesriigi turujärelevalveasutusele.

4. Hiljemalt kolm kuud pärast käesoleva määruse jõustumist nimetab iga liikmesriik lõikes 3 osutatud ametiasutused või organid ning teeb nende loetelu üldsusele kättesaadavaks. Liikmesriigid teavitavad loetelust komisjoni ja teisi liikmesriike ning ajakohastavad seda.

5. Kui lõikes 3 osutatud dokumentatsioon ei ole piisav, et teha kindlaks, kas põhiõiguste kaitseks mõeldud liidu õiguse kohaseid kohustusi on rikutud, võib lõikes 3 osutatud ametiasutus või organ esitada turujärelevalveasutusele põhjendatud taotluse korraldada suure riskiga tehisintellektisüsteemi testimine tehniliste vahendite abil. Turujärelevalveasutus korraldab testimise mõistliku aja jooksul pärast taotluse esitamist tihedas koostöös taotluse esitanud ametiasutuse või organiga.

6. Lõikes 3 osutatud riiklike ametiasutuste või organite poolt käesoleva artikli sätete kohaselt saadud teabe ja dokumentatsiooni käsitlemisel täidetakse artiklis 70 sätestatud konfidentsiaalsuskohustusi.

Artikkel 65

Riiklikul tasemel riski tekitava tehisintellektisüsteemiga tegelemise menetlus

1. Riski tekitavat tehisintellektisüsteemi käsitatakse määruse (EL) 2019/1020 artikli 3 punktis 19 määratletud ohtliku tootena niivõrd, kuivõrd tegemist on tervise või ohutuse või isikute põhiõigustega seotud riskidega.

2. Kui liikmesriigi turujärelevalveasutusel on piisavalt põhjust uskuda, et tehisintellektisüsteem tekitab lõikes 1 osutatud riski, korraldab ta asjaomase tehisintellektisüsteemi hindamise, et selgitada välja, kas süsteem vastab käesolevas määruses sätestatud nõuetele ja kohustustele. Kui tuvastatakse põhiõigustega seotud riske, teavitab turujärelevalveasutus sellest ka artikli 64 lõikes 3 osutatud asjaomaseid riiklikke ametiasutusi või organeid. Asjaomased operaatorid teevad vastavalt vajadusele koostööd turujärelevalveasutuste ja muude artikli 64 lõikes 3 osutatud riiklike ametiasutuste või organitega.

   Kui turujärelevalveasutus leiab nimetatud hindamise käigus, et tehisintellektisüsteem ei vasta käesolevas määruses sätestatud nõuetele ja kohustustele, nõuab ta põhjendamatu viivituseta, et asjaomane operaator võtaks tema määratava aja jooksul kõik vajalikud parandusmeetmed, et tehisintellektisüsteem nimetatud nõuetega vastavusse viia, turult kõrvaldada või tagasi nõuda.

   Turujärelevalveasutus teavitab sellest asjaomast teavitatud asutust. Teises lõigus osutatud meetmete suhtes kohaldatakse määruse (EL) nr 2019/1020 artiklit 18.

3. Kui turujärelevalveasutus on seisukohal, et nõuetele mittevastavus ei piirdu üksnes tema liikmesriigi territooriumiga, teavitab ta põhjendamatu viivituseta komisjoni ja teisi liikmesriike hindamistulemustest ja meetmetest, mille võtmist ta on operaatorilt nõudnud.

4. Operaator tagab, et kõigi asjaomaste, tema poolt liidu turul kättesaadavaks tehtud tehisintellektisüsteemide suhtes võetakse kõik vajalikud parandusmeetmed.

5. Kui tehisintellektisüsteemi operaator ei võta lõikes 2 osutatud ajavahemiku jooksul piisavaid parandusmeetmeid, võtab turujärelevalveasutus kõik sobivad ajutised meetmed, et keelata või piirata tehisintellektisüsteemi kättesaadavaks tegemist oma siseriiklikul turul, toode turult kõrvaldada või tagasi nõuda. See asutus teavitab komisjoni ja teisi liikmesriike nimetatud meetmetest põhjendamatu viivituseta.

6. Lõikes 5 osutatud teade sisaldab kõiki kättesaadavaid üksikasju, eelkõige nõuetele mittevastava tehisintellektisüsteemi identifitseerimiseks vajalikku teavet, tehisintellektisüsteemi päritolu, väidetava mittevastavuse ja riski olemust, võetud riiklike meetmete olemust ja kestust ning asjaomase operaatori esitatud seisukohti. Turujärelevalveasutused märgivad eelkõige ära, kas nõuetele mittevastavus on tingitud ühest või mitmest järgmisest asjaolust:

-a) artiklis 5 osutatud tehisintellekti kasutusviiside keelu rikkumine;

a) suure riskiga tehisintellektisüsteemi mittevastavus III jaotise 2. peatükis sätestatud nõuetele;

b) puudused artiklites 40 ja 41 osutatud harmoneeritud standardites või ühtsetes kirjeldustes, mille alusel vastavust eeldatakse.

c) artikli 52 sätete rikkumine;

d) üldotstarbeliste tehisintellektisüsteemide mittevastavus artiklis 4a osutatud nõuetele ja kohustustele.

7. Muude liikmesriikide kui menetluse algatanud liikmesriigi turujärelevalveasutused teavitavad komisjoni ja teisi liikmesriike põhjendamatu viivituseta kõigist võetud meetmetest ja muust nende käsutuses olevast täiendavast teabest seoses asjaomase tehisintellektisüsteemi mittevastavusega ning, kui nad ei ole teadaantud riigisisese meetmega nõus, siis ka oma vastuväidetest.

8. Kui kolme kuu jooksul alates lõikes 5 osutatud teate kättesaamisest ei ole teised liikmesriigid ega komisjon esitanud vastuväiteid liikmesriigi ajutise meetme suhtes, loetakse meede põhjendatuks. See ei piira asjaomase operaatori määruse (EL) 2019/1020 artikli 18 kohaseid menetlusõigusi. Käesoleva lõike esimeses lauses osutatud tähtaega lühendatakse 30 päevani, kui rikutud on artiklis 5 osutatud tehisintellekti kasutusviiside keeldu.

9. Kõigi liikmesriikide turujärelevalveasutused tagavad seejärel, et asjaomase tehisintellektisüsteemi suhtes võetakse põhjendamatu viivituseta asjakohased piiravad meetmed, näiteks kõrvaldatakse toode liikmesriigi turult.

Artikkel 66

Liidu kaitsemeetmete menetlus

1. Kui kolme kuu jooksul alates artikli 65 lõikes 5 osutatud teavituse kättesaamisest või 30 päeva jooksul, kui rikutud on artiklis 5 osutatud tehisintellekti kasutusviiside keeldu, esitab mõni liikmesriik vastuväite teise liikmesriigi võetud meetme suhtes või kui komisjon leiab, et meede on liidu õigusega vastuolus, alustab komisjon põhjendamatu viivituseta konsultatsioone asjaomase liikmesriigi turujärelevalveasutuse ja operaatori või operaatoritega ning hindab riiklikku meedet. Selle hindamise tulemuste põhjal otsustab komisjon 9 kuu jooksul (või artiklis 5 osutatud tehisintellekti kasutusviiside keelu rikkumise puhul 60 päeva jooksul) alates artikli 65 lõikes 5 osutatud teate saamisest, kas riiklik meede on põhjendatud või ei. Ta teatab oma otsuse asjaomasele liikmesriigile. Komisjon teavitab sellisest otsusest ka kõiki teisi liikmesriike.

2. Kui komisjon leiab, et asjaomase liikmesriigi turujärelevalveasutuse võetud meede on põhjendatud, tagavad kõikide liikmesriikide turujärelevalveasutused, et asjaomase tehisintellektisüsteemi suhtes võetakse asjakohaseid piiravaid meetmeid, nagu tehisintellektisüsteemi põhjendamatu viivituseta kõrvaldamine oma turult, ning teavitavad sellest komisjoni. Kui komisjon peab riiklikku meedet põhjendamatuks, tühistab asjaomase liikmesriigi turujärelevalveasutus meetme ja teavitab sellest komisjoni.

3. Kui riiklik meede loetakse põhjendatuks ja tehisintellektisüsteemi nõuetele mittevastavus tuleneb puudustest käesoleva määruse artiklites 40 ja 41 osutatud harmoneeritud standardites või ühtsetes kirjeldustes, kohaldab komisjon määruse (EL) nr 1025/2012 artiklis 11 sätestatud menetlust.

Artikkel 67

Nõuetele vastavad suure riskiga või üldotstarbelised tehisintellektisüsteemid, mis põhjustavad riski

1. Kui liikmesriigi turujärelevalveasutus leiab pärast artikli 65 kohast hindamist, et suure riskiga või üldotstarbeline tehisintellektisüsteem, mis on kooskõlas käesoleva määruse nõuetega, põhjustab sellest hoolimata riski isikute tervisele või ohutusele või põhiõigustele, nõuab ta, et asjaomane operaator võtaks tema määratava aja jooksul kõik vajalikud meetmed tagamaks, et asjaomane tehisintellektisüsteem ei põhjusta turule laskmise või kasutusele võtmise korral enam sellist riski, kõrvaldaks asjaomase tehisintellektisüsteemi turult või nõuaks selle tagasi põhjendamatu viivituseta.

2. Pakkuja või muud asjaomased operaatorid tagavad, et parandusmeetmed võetakse kõigi asjaomaste tehisintellektisüsteemide suhtes, mille nad on liidu turul kättesaadavaks teinud, lõikes 1 osutatud liikmesriigi turujärelevalveasutuse ettekirjutuse kohase tähtaja jooksul.

3. Liikmesriik teavitab sellest viivitamata komisjoni ja teisi liikmesriike. Teave peab sisaldama kõiki teadaolevaid üksikasju, eelkõige asjaomase tehisintellektisüsteemi tuvastamiseks vajalikke andmeid, tehisintellektisüsteemi päritolu ja tarneahelat, kaasneva riski olemust ning liikmesriigi võetud meetmete olemust ja kestust.

4. Komisjon alustab põhjendamatu viivituseta konsulteerimist asjaomaste liikmesriikide ja asjaomase operaatoriga ning hindab võetud riiklikke meetmeid. Nimetatud hinnangu tulemuste põhjal otsustab komisjon, kas meede on põhjendatud või mitte, ning teeb vajaduse korral ettepaneku sobivate meetmete kohta.

5. Komisjon adresseerib oma otsuse asjaomastele liikmesriikidele ja teavitab kõiki ülejäänud liikmesriike.

Artikkel 68

Formaalne mittevastavus

1. Kui mõne liikmesriigi turujärelevalveasutus on avastanud ühe järgmistest asjaoludest, nõuab ta, et asjaomane pakkuja lõpetaks tema määratava aja jooksul asjaomase mittevastavuse:

   a) vastavusmärgise kinnitamisel ei ole järgitud artikli 49 nõudeid;

   b) vastavusmärgist ei ole kinnitatud;

   c) ELi vastavusdeklaratsiooni ei ole koostatud;

   d) ELi vastavusdeklaratsioon ei ole koostatud õigesti;

   e) vastavushindamises osaleva teavitatud asutuse identifitseerimisnumbrit ei ole kinnitatud, kui see on asjakohane.

2. Kui lõikes 1 osutatud mittevastavust ei kõrvaldata, võtab asjaomane liikmesriik kõik vajalikud meetmed tehisintellektisüsteemi turul kättesaadavaks tegemise piiramiseks või keelamiseks või tagab selle tagasinõudmise või kõrvaldamise turult.

Artikkel 68a

Liidu katserajatised tehisintellekti valdkonnas

1. Komisjon määrab tehisintellekti valdkonnas määruse (EL) 2019/1020 artikli 21 kohaselt ühe või mitu liidu katserajatist.

2. Ilma et see piiraks määruse (EL) 2019/1020 artikli 21 lõikes 6 osutatud liidu katserajatiste tegevust, annavad lõikes 1 osutatud liidu katserajatised nõukoja või turujärelevalveasutuste taotlusel ka sõltumatut tehnilist või teaduslikku nõu.

Artikkel 68b

Sõltumatute ekspertide keskreserv

1. Tehisintellekti nõukoja taotlusel võtab komisjon rakendusaktiga vastu sätted sõltumatute ekspertide keskreservi loomise, haldamise ja rahastamise kohta, et toetada käesoleva määruse kohast jõustamistegevust.

2. Eksperdid valib välja komisjon ja nad lisatakse keskreservi, lähtuvalt ajakohastest teaduslikest või tehnilistest eksperditeadmistest tehisintellekti valdkonnas, võttes nõuetekohaselt arvesse käesolevas määruses sätestatud nõuete ja kohustustega hõlmatud tehnilisi valdkondi ning turujärelevalveasutuste tegevust vastavalt määruse (EL) 2019/1020 artiklile 11. Komisjon määrab keskreservi ekspertide arvu kindlaks vastavalt vajadustele.

3. Ekspertidel võivad olla järgmised ülesanded:

a) anda turujärelevalveasutustele nende taotluse korral nõu ja toetada nende tööd;

b) toetada artikli 58 punktis h osutatud piiriüleseid turujärelevalveuurimisi, ilma et see piiraks turujärelevalveasutuste volitusi;

c) nõustada ja toetada komisjoni tema kohustuste täitmisel seoses artikli 66 kohase kaitseklausliga.

4. Eksperdid täidavad oma ülesandeid erapooletult ja objektiivselt ning tagavad oma ülesannete ja tegevuse käigus saadud teabe ja andmete konfidentsiaalsuse. Iga ekspert koostab huvide deklaratsiooni, mis tehakse üldsusele kättesaadavaks. Komisjon kehtestab süsteemid ja menetlused võimalike huvide konfliktide aktiivseks haldamiseks ja ennetamiseks.

5. Liikmesriikidelt võidakse nõuda ekspertide pakutava nõustamise ja toe eest tasu. Tasu struktuuri ja suuruse ning hüvitatavate kulude ulatuse ja struktuuri võtab komisjon vastu lõikes 1 osutatud rakendusaktiga, võttes arvesse käesoleva määruse nõuetekohase rakendamise eesmärke, kulutasuvust ja vajadust tagada kõikide liikmesriikide jaoks eksperditeenustele tõhus juurdepääs.

6. Komisjon hõlbustab vajaduse korral liikmesriikide õigeaegset juurdepääsu eksperditeenustele ning tagab, et artikli 68a kohaselt liidu katserajatistes läbiviidava toetustegevuse kombineerimine käesoleva artikli kohaste eksperditeenustega on tõhusalt korraldatud ja annab parima võimaliku lisaväärtuse.

IX JAOTIS

KÄITUMISJUHENDID

Artikkel 69

Käitumisjuhendid erinõuete vabatahtlikuks kohaldamiseks

1. Komisjon ja liikmesriigid hõlbustavad selliste käitumisjuhendite koostamist, mille eesmärk on soodustada käesoleva määruse III jaotise 2. peatükis sätestatud ühe või mitme nõude vabatahtlikku kohaldamist muude tehisintellektisüsteemide suhtes, mis ei ole suure riskiga tehisintellektisüsteemid, võimalikult suures ulatuses, võttes arvesse olemasolevaid tehnilisi lahendusi, mis võimaldavad selliseid nõudeid kohaldada.

2. Komisjon ja liikmesriigid hõlbustavad selliste käitumisjuhendite koostamist, mille eesmärk on edendada selliste erinõuete vabatahtlikku kohaldamist kõigi tehisintellektisüsteemide suhtes, mis on seotud näiteks keskkonnasäästlikkusega, muu hulgas seoses energiatõhusa programmitööga, puuetega inimestele juurdepääsetavusega, sidusrühmade osalemisega tehisintellektisüsteemide projekteerimises ja arendamises ning arendusmeeskondade mitmekesisusega, lähtudes selgetest eesmärkidest ja põhilistest tulemusnäitajatest, millega mõõta kirjeldatud eesmärkide saavutamist. Komisjon ja liikmesriigid hõlbustavad vajaduse korral ka selliste käitumisjuhendite koostamist, mida kohaldatakse vabatahtlikkuse alusel seoses tehisintellektisüsteemidega seonduvate kasutajate kohustustega.

3. Vabatahtlikkuse alusel kohaldatavaid käitumisjuhendeid võivad koostada üksikud tehisintellektisüsteemide pakkujad või nende esindusorganisatsioonid või mõlemad ning sellesse tegevusse võib kaasata ka kasutajaid ja huvitatud sidusrühmi ning nende esindusorganisatsioone, või vajaduse korral kasutajad seoses neid puudutavate kohustustega. Käitumisjuhendid võivad käia ühe või mitme tehisintellektisüsteemi kohta, võttes arvesse asjaomaste süsteemide sihtotstarbe sarnasusi.

4. Käesolevas artiklis osutatud käitumisjuhendite koostamist edendades ja hõlbustades võtavad komisjon ja liikmesriigid arvesse VKEdest pakkujate, kaasa arvatud idufirmade erihuve ja vajadusi.

X JAOTIS

KONFIDENTSIAALSUS JA KARISTUSED

Artikkel 70

Konfidentsiaalsus

1. Käesoleva määruse kohaldamises osalevad riigi pädevad asutused, teavitatud asutused, komisjon, nõukoda ja kõik muud füüsilised ja juriidilised isikud kehtestavad kooskõlas liidu või liikmesriigi õigusega asjakohased tehnilised ja korralduslikud meetmed, et tagada oma ülesannete täitmisel ja tegevuste käigus saadud teabe ja andmete konfidentsiaalsust, et kaitsta eeskätt järgmist:

a) intellektuaalomandiõigused ning füüsilise või juriidilise isiku konfidentsiaalne äriteave või ärisaladused, kaasa arvatud lähtekood, välja arvatud juhtudel, millele on viidatud direktiivi 2016/943 (milles käsitletakse avalikustamata oskusteabe ja äriteabe (ärisaladuste) ebaseadusliku omandamise, kasutamise ja avalikustamise vastast kaitset) artiklis 5;

b) käesoleva määruse tulemuslikku rakendamist, eelkõige inspekteerimise, uurimise ja auditite eesmärgil;

c) avaliku ja riigi julgeolekuga seotud huvid;

d) kriminaal- või haldusmenetluste usaldusväärsus;

e) liidu või liikmesriigi õiguse kohaselt salastatud teabe terviklus.

2. Ilma et see piiraks lõike 1 kohaldamist, ei avaldata riikide pädevate asutuste ning riikide pädevate asutuste ja komisjoni vahel konfidentsiaalselt vahetatud teavet ilma, et oleks eelnevalt konsulteeritud riigi pädevad asutusega, kust teave pärit on, ja kasutajaga, kui III lisa punktides 1, 6 ja 7 osutatud suure riskiga tehisintellektisüsteeme kasutavad õiguskaitse-, piirikontrolli, rände- või varjupaigaasutused ja kui selline avaldamine seaks ohtu avaliku ja riigi julgeolekuga seotud huvid. See kohustus teavet vahetada ei hõlma õiguskaitse-, piirikontrolli-, rände- või varjupaigaasutuste tegevusega seotud tundlikke operatiivandmeid.

Kui õiguskaitse-, rände- või varjupaigaasutused on III lisa punktides 1, 6 ja 7 osutatud suure riskiga tehisintellektisüsteemide pakkujad, peab IV lisas osutatud tehniline dokumentatsioon jääma nende asutuste ruumidesse. Need asutused peavad tagama, et olenevalt asjaoludest võivad artikli 63 lõigetes 5 ja 6 osutatud turujärelevalveasutused taotluse alusel viivitamata tutvuda dokumentatsiooniga või saada selle koopia. Dokumentide ja nende koopiatega on lubatud tutvuda ainult neil turujärelevalveasutuse töötajatel, kellel on asjakohasel tasemel salastatud teabele juurdepääsu luba.

3. Lõiked 1 ja 2 ei mõjuta komisjoni, liikmesriikide ja nende asjaomaste ametiasutuste ning teavitatud asutuste õigusi ja kohustusi vahetada teavet ja edastada hoiatusi, kaasa arvatud piiriülese koostöö kontekstis, ega asjaosaliste kohustusi anda teavet liikmesriikide kriminaalõiguse kohaselt.

Artikkel 71

Karistused

1. Liikmesriigid kehtestavad kooskõlas käesolevas määruses sätestatud tingimustega õigusnormid karistuste, kaasa arvatud haldustrahvide kohta, mida kohaldatakse käesoleva määruse rikkumise korral, ning võtavad kõik vajalikud meetmed, et tagada nende nõuetekohane ja mõjus rakendamine. Kehtestatud karistused peavad olema mõjusad, proportsionaalsed ja hoiatavad. Nende puhul tuleb eriti arvesse võtta VKEdest pakkujate, kaasa arvatud idufirmade suurust ja huve ning nende majanduslikku elujõulisust. Neis tuleb samuti võtta arvesse seda, kas tehisintellektisüsteemi kasutamine toimub isikliku, mitte kutselise tegevuse kontekstis.

2. Liikmesriigid teavitavad komisjoni viivitamata nimetatud normidest ja meetmetest ning nende hilisematest muudatustest.

3. Kui rikutakse artiklis 5 osutatud tehisintellekti kasutusviiside keeldu, kohaldatakse haldustrahvi kuni 30 000 000 eurot või, kui rikkuja on ettevõte, kuni 6 % tema eelmise majandusaasta ülemaailmsest kogukäibest olenevalt sellest, kumb on suurem. VKE, kaasa arvatud idufirma puhul on see trahv kuni 3 % ettevõtte eelmise majandusaasta ülemaailmsest käibest.

4. Järgmiste operaatoreid või teavitatud asutusi puudutavate nõuete rikkumise korral kohaldatakse haldustrahvi kuni 20 000 000 eurot või, kui rikkuja on ettevõte, kuni 4 % tema eelmise majandusaasta ülemaailmsest kogukäibest olenevalt sellest, kumb on suurem:

-a) pakkujate kohustused vastavalt artiklitele 4b ja 4c;

a) pakkujate kohustused vastavalt artiklile 16;

b) teatavate muude isikute kohustused vastavalt artiklile 23a;

c) volitatud esindajate kohustused vastavalt artiklile 25;

d) importijate kohustused vastavalt artiklile 26;

e) turustajate kohustused vastavalt artiklile 27;

f) kasutajate kohustused vastavalt artikli 29 lõigetele 1–6a;

g) teavitatud asutuste nõuded ja kohustused vastavalt artiklile 33, artikli 34 lõikele 1, artikli 34 lõikele 3, artikli 34 lõikele 4 ja artiklile 34a;

h) pakkujate ja kasutajate läbipaistvuskohustused vastavalt artiklile 52.

VKE, kaasa arvatud idufirma puhul on see trahv kuni 2 % ettevõtte eelmise majandusaasta ülemaailmsest käibest.

5. Kui teavitatud asutustele ja riigi pädevatele asutustele on taotluse peale esitatud vale, ebatäielikku või eksitavat teavet, kohaldatakse haldustrahve kuni 10 000 000 eurot või, kui rikkuja on ettevõte, kuni 2 % tema eelmise majandusaasta ülemaailmsest kogukäibest olenevalt sellest, kumb on suurem. VKE, kaasa arvatud idufirma puhul on see trahv kuni 1 % ettevõtte eelmise majandusaasta ülemaailmsest käibest.

6. Kui otsustatakse igal konkreetsel juhul kohaldatava haldustrahvi suuruse üle, võetakse arvesse iga konkreetse olukorra kõiki asjaomaseid asjaolusid ning pööratakse asjakohast tähelepanu järgmisele:

a) rikkumise olemus, raskusaste ja kestus ning selle tagajärjed;

aa) kas rikkumine pandi toime tahtlikult või hooletusest;

ab) igasugune operaatori tegevus rikkumise heastamiseks ja rikkumise võimaliku kahjuliku mõju leevendamiseks;

b) kas muud turujärelevalveasutused on juba kohaldanud sama operaatori suhtes muus liikmesriigis sama rikkumise eest haldustrahve;

ba) kas teised asutused on juba kohaldanud sama operaatori suhtes haldustrahve muu liidu või liikmesriigi õiguse rikkumise eest, kui sellised rikkumised tulenevad samast tegevusest või tegevusetusest, mis kujutab endast käesoleva määruse asjassepuutuvat rikkumist;

c) rikkumise toime pannud operaatori suurus, aastakäive ja turuosa.

d) juhtumi asjaolude suhtes kohaldatavad mis tahes muud raskendavad või kergendavad tegurid, näiteks rikkumisest otseselt või kaudselt saadud finantskasu või välditud kahju.

7. Iga liikmesriik kehtestab õigusnormid selle kohta, kas ja millisel määral võib haldustrahve määrata selles liikmesriigis asutatud avaliku sektori asutustele ja organitele.

8. Olenevalt liikmesriikide õigussüsteemidest võib haldustrahve käsitlevaid õigusnorme kohaldada selliselt, et trahve määravad riigi pädevad kohtud või muud asutused, nii nagu neis liikmesriikides asjakohane. Selliste õigusnormide kohaldamisel neis liikmesriikides on samaväärne mõju.

9. Käesoleva artikli kohaste volituste kasutamise suhtes turujärelevalveasutuse poolt kohaldatakse kooskõlas liidu ja liikmesriigi õigusega asjakohaseid menetluslikke kaitsemeetmeid, sealhulgas tõhusat õiguskaitsevahendit ja nõuetekohast menetlust.

Artikkel 72

Liidu institutsioonide, asutuste ja organite suhtes kohaldatavad haldustrahvid

1. Euroopa Andmekaitseinspektor võib määrata haldustrahve käesoleva määruse kohaldamisalasse kuuluvatele liidu institutsioonidele, asutustele ja organitele. Kui otsustatakse haldustrahvi määramise ja selle konkreetsel juhul kohaldatava suuruse üle, võetakse arvesse iga konkreetse olukorra kõiki asjaomaseid asjaolusid ning pööratakse asjakohast tähelepanu järgmisele:

   a) rikkumise olemus, raskusaste ja kestus ning selle tagajärjed;

   b) Euroopa Andmekaitseinspektoriga rikkumise heastamiseks ja rikkumise võimaliku kahjuliku mõju leevendamiseks tehtav koostöö, kaasa arvatud Euroopa Andmekaitseinspektori poolt varem asjaomase liidu institutsiooni, asutuse või organi suhtes samas küsimuses määratud meetmete järgimine:

   c) liidu institutsiooni, asutuse või organi varasemad sarnased rikkumised.

2. Artiklis 5 osutatud tehisintellekti kasutusviiside keelu rikkumise korral määratakse haldustrahv kuni 500 000 eurot.

3. Kui tehisintellektisüsteem ei vasta ükskõik millisele käesolevast määrusest tulenevale nõudele või kohustusele, välja arvatud need, mis on sätestatud artiklites 5 ja 10, kohaldatakse haldustrahvi kuni 250 000 eurot.

4. Enne käesoleva artikli alusel otsuse tegemist annab Euroopa Andmekaitseinspektor liidu institutsioonile, asutusele või organile, kelle suhtes Euroopa Andmekaitseinspektor on menetluse algatanud, võimaluse olla võimaliku rikkumisega seotud küsimuses ära kuulatud. Euroopa Andmekaitseinspektori otsused toetuvad üksnes sellistele elementidele ja asjaoludele, mille kohta asjaomastel isikutel on olnud võimalik esitada oma seisukoht. Kaebuste esitajate olemasolu korral kaasatakse nad aktiivselt menetlusse.

5. Menetluse käigus tagatakse täielikult asjaomaste isikute õigus kaitsele. Neil on õigus tutvuda Euroopa Andmekaitseinspektori toimikuga tingimusel, et võetakse arvesse üksikisikute ja ettevõtjate õigustatud huvi kaitsta oma isikuandmeid ja ärisaladusi.

6. Käesoleva artikli alusel määratud trahvidega kogutud summad kantakse liidu üldeelarvesse.

XI JAOTIS

VOLITUSTE DELEGEERIMINE JA KOMITEEMENETLUS

Artikkel 73

Delegeeritud volituste rakendamine

1. Komisjonile antakse õigus võtta vastu delegeeritud õigusakte käesolevas artiklis sätestatud tingimustel.

2. Artikli 7 lõigetes 1 ja 3, artikli 11 lõikes 3, artikli 43 lõigetes 5 ja 6 ning artikli 48 lõikes 5 osutatud õigus võtta vastu delegeeritud õigusakte antakse komisjonile viieks aastaks alates [*käesoleva määruse jõustumise kuupäev*].

   Komisjon esitab delegeeritud volituste kohta aruande hiljemalt üheksa kuud enne viieaastase tähtaja möödumist. Volituste delegeerimist pikendatakse automaatselt samaks ajavahemikuks, välja arvatud juhul, kui Euroopa Parlament või nõukogu esitab selle suhtes vastuväite hiljemalt kolm kuud enne iga ajavahemiku lõppemist.

3. Euroopa Parlament ja nõukogu võivad artikli 7 lõigetes 1 ja 3, artikli 11 lõikes 3, artikli 43 lõigetes 5 ja 6 ning artikli 48 lõikes 5 osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas* või selles otsuses nimetatud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.

4. Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, teeb ta selle samal ajal teatavaks Euroopa Parlamendile ja nõukogule.

5. Artikli 7 lõigete 1 ja 3, artikli 11 lõike 3, artikli 43 lõigete 5 ja 6 ning artikli 48 lõike 5 alusel vastu võetud delegeeritud õigusakt jõustub üksnes juhul, kui Euroopa Parlament ega nõukogu ei ole kolme kuu jooksul pärast õigusakti teatavakstegemist Euroopa Parlamendile ja nõukogule esitanud selle kohta vastuväiteid või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväiteid. Euroopa Parlamendi või nõukogu algatusel pikendatakse seda tähtaega kolme kuu võrra.

Artikkel 74

Komiteemenetlus

1. Komisjoni abistab komitee. Nimetatud komitee on komitee määruse (EL) nr 182/2011 tähenduses.

2. Käesolevale lõikele viitamise korral kohaldatakse määruse (EL) nr 182/2011 artiklit 5.

XII JAOTIS

LÕPPSÄTTED

Artikkel 75

Määruse (EÜ) nr 300/2008 muutmine

Määruse (EÜ) nr 300/2008 artikli 4 lõikesse 3 lisatakse järgmine lõik:

„Võttes vastu üksikasjalikke meetmeid julgestusseadmete tehniliste kirjelduste ning nende heakskiitmise ja kasutamise korra kohta, mis on seotud tehisintellektisüsteemidega Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.“

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).“

Artikkel 76

Määruse (EL) nr 167/2013 muutmine

Määruse (EL) nr 167/2013 artikli 17 lõikesse 5 lisatakse järgmine lõik:

„Võttes vastu esimese lõigu kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).“

Artikkel 77

Määruse (EL) nr 168/2013 muutmine

Määruse (EL) nr 168/2013 artikli 22 lõikesse 5 lisatakse järgmine lõik:

„Võttes vastu esimese lõigu kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).“

Artikkel 78

Direktiivi 2014/90/EL muutmine

Direktiivi 2014/90/EL artiklisse 8 lisatakse järgmine lõige:

„4. Tegutsedes vastavalt lõikele 1 ning võttes vastu tehnilisi kirjeldusi ja testimisstandardeid vastavalt lõigetele 2 ja 3 seoses tehisintellektisüsteemidega, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võtab komisjon arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).“.

Artikkel 79

Direktiivi (EL) 2016/797 muutmine

Direktiivi (EL) 2016/797 artiklisse 5 lisatakse järgmine lõige:

„12. Võttes vastu lõike 1 kohaseid delegeeritud õigusakte ja lõike 11 kohaseid rakendusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).“.

Artikkel 80

Määruse (EL) 2018/858 muutmine

Määruse (EL) 2018/858 artiklisse 5 lisatakse järgmine lõige:

„4. Võttes vastu lõike 3 kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).“.

Artikkel 81

Määruse (EL) 2018/1139 muutmine

Määrust (EL) 2018/1139 muudetakse järgmiselt.

1) Artiklisse 17 lisatakse järgmine lõige:

„3. Võttes vastu lõike 1 kohaseid rakendusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid, ilma et see piiraks lõike 2 kohaldamist.

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).“

2) Artiklisse 19 lisatakse järgmine lõige:

„4. Võttes vastu lõigete 1 ja 2 kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid määruse (EL) YYY/XX [tehisintellekti kohta] tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.“

3) Artiklisse 43 lisatakse järgmine lõige:

„4. Võttes vastu lõike 1 kohaseid rakendusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid määruse (EL) YYY/XX [tehisintellekti kohta] tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.“

4) Artiklisse 47 lisatakse järgmine lõige:

„3. Võttes vastu lõigete 1 ja 2 kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid määruse (EL) YYY/XX [tehisintellekti kohta] tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.“

5) Artiklisse 57 lisatakse järgmine lõige:

„Võttes vastu kõnealuseid rakendusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid määruse (EL) YYY/XX [tehisintellekti kohta] tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.“

6) Artiklisse 58 lisatakse järgmine lõige:

„3. Võttes vastu lõigete 1 ja 2 kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid määruse (EL) YYY/XX [tehisintellekti kohta] tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.“.

Artikkel 82

Määruse (EL) 2019/2144 muutmine

Määruse (EL) 2019/2144 artiklisse 11 lisatakse järgmine lõige:

„3. Võttes vastu lõike 2 kohaseid rakendusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).“.

Artikkel 83

Juba turule lastud või kasutusele võetud tehisintellektisüsteemid

1. Käesolevat määrust ei kohaldata tehisintellektisüsteemide suhtes, mis on selliste IX lisas loetletud õigusaktidega loodud suuremahuliste IT-süsteemide komponendid, mis on turule lastud või kasutusele võetud enne *[12 kuud pärast artikli 85 lõikes 2 osutatud kuupäeva, mil käesolevat määrust hakatakse kohaldama]*, välja arvatud juhul, kui nende õigusaktide asendamise või muutmise tulemusena tehakse oluline muudatus asjaomase tehisintellektisüsteemi või asjaomaste tehisintellektisüsteemide projektis või sihtotstarbes.

   Kui see on asjakohane, võetakse käesolevas määruses sätestatud nõudeid arvesse, kui hinnatakse IX lisas loetletud õigusaktidega loodud suuremahulisi IT-süsteeme neis õigusaktides sätestatud korra kohaselt.

2. Käesolevat määrust kohaldatakse suure riskiga tehisintellektisüsteemide suhtes, välja arvatud lõikes 1 osutatud süsteemide suhtes, mis on turule lastud või kasutusele võetud enne *[artikli 85 lõikes 2 osutatud kuupäev, mil käesolevat määrust hakatakse kohaldama]*, ainult juhul, kui pärast nimetatud kuupäeva muudetakse oluliselt nende projekti või sihtotstarvet.

Artikkel 84

Hindamine ja läbivaatamine

1. [välja jäetud]

1b. Komisjon annab pärast käesoleva määruse jõustumist kord kahe aasta tagant ning volituste delegeerimise tähtaja lõpuni hinnangu sellele, kas III lisas esitatud loetelu on vaja muuta. Selle hindamise tulemused esitatakse Euroopa Parlamendile ja nõukogule.

2. Komisjon esitab Euroopa Parlamendile ja nõukogule hiljemalt *[kolm aastat pärast artikli 85 lõikes 2 osutatud kuupäeva, mil käesolevat määrust hakatakse kohaldama,]* ning pärast seda iga nelja aasta järel aruande käesoleva määruse hindamise ja läbivaatamise kohta. Aruanded avalikustatakse.

3. Lõikes 2 osutatud aruannetes pööratakse erilist tähelepanu järgmisele:

   a) riigi pädevate asutuste rahaliste ressursside, tehniliste seadmete ja inimressursside olukord, et nad saaksid tulemuslikult täita neile käesoleva määruse alusel määratud ülesandeid;

   b) olukord seoses artikli 71 lõikes 1 osutatud karistuste ja eriti haldustrahvidega, mida liikmesriigid kohaldavad käesoleva määruse sätete rikkumise korral.

4. Komisjon hindab *[kolme aasta jooksul alates artikli 85 lõikes 2 osutatud kuupäevast, mil käesolevat määrust hakatakse kohaldama,]* ja pärast seda iga nelja aasta järel, kui see on asjakohane, kui mõjusalt ja tulemuslikult on vabatahtlikkusel põhinevad käitumisjuhendid edendanud III jaotise 2. peatükis sätestatud muude kui suure riskiga tehisintellektisüsteemide ja võimaluse korral tehisintellektisüsteemide suhtes kehtivate muude täiendavate nõuete kohaldamist, muu hulgas seose keskkonnasäästlikkusega.

5. Lõigete 1a–4 kohaldamisel esitavad nõukoda, liikmesriigid ja riikide pädevad asutused komisjonile tema taotluse korral teavet.

6. Lõigetes 1a–4 osutatud hindamiste ja läbivaatamiste käigus võtab komisjon arvesse nõukoja, Euroopa Parlamendi, nõukogu ning muude asjaomaste organite ja allikate seisukohti ja tähelepanekuid.

7. Komisjon esitab vajaduse korral asjakohased ettepanekud käesoleva määruse muutmiseks, eelkõige võttes arvesse tehnika ja infoühiskonna arengut.

Artikkel 85

Jõustumine ja kohaldamine

1. Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

2. Käesolevat määrust kohaldatakse alates [36 kuud pärast määruse jõustumist].

3. Erandina lõikest 2 kohaldatakse:

   a) III jaotise 4. peatükki ja VI jaotist alates [12 kuud pärast käesoleva määruse jõustumist];

   b) artiklit 71 alates [12 kuud pärast määruse jõustumist].

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

I LISA

[välja jäetud]

II LISA

LIIDU ÜHTLUSTAMISÕIGUSAKTIDE LOETELU

A jaotis. Uuel õigusraamistikul põhinevate liidu ühtlustamisõigusaktide loetelu

1. Euroopa Parlamendi ja nõukogu 17. mai 2006. aasta direktiiv 2006/42/EÜ, mis käsitleb masinaid ja millega muudetakse direktiivi 95/16/EÜ (ELT L 157, 9.6.2006, lk 24) [kehtetuks tunnistatud masinamäärusega]

2. Euroopa Parlamendi ja nõukogu 18. juuni 2009. aasta direktiiv 2009/48/EÜ mänguasjade ohutuse kohta (ELT L 170, 30.6.2009, lk 1)

3. Euroopa Parlamendi ja nõukogu 20. novembri 2013. aasta direktiiv 2013/53/EL, mis käsitleb väikelaevu ja jette ning millega tunnistatakse kehtetuks direktiiv 94/25/EÜ (ELT L 354, 28.12.2013, lk 90)

4. Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/33/EL lifte ja lifti ohutusseadiseid käsitlevate liikmesriikide õigusaktide ühtlustamise kohta (ELT L 96, 29.3.2014, lk 251)

5. Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/34/EL plahvatusohtlikus keskkonnas kasutatavaid seadmeid ja kaitsesüsteeme käsitlevate liikmesriikide õigusaktide ühtlustamise kohta (ELT L 96, 29.3.2014, lk 309)

6. Euroopa Parlamendi ja nõukogu 16. aprilli 2014. aasta direktiiv 2014/53/EL raadioseadmete turul kättesaadavaks tegemist käsitlevate liikmesriikide õigusaktide ühtlustamise kohta ja millega tunnistatakse kehtetuks direktiiv 1999/5/EÜ (ELT L 153, 22.5.2014, lk 62)

7. Euroopa Parlamendi ja nõukogu 15. mai 2014. aasta direktiiv 2014/68/EL surveseadmete turul kättesaadavaks tegemist käsitlevate liikmesriikide õigusaktide ühtlustamise kohta (ELT L 189, 27.6.2014, lk 164)

8. Euroopa Parlamendi ja nõukogu 9. märtsi 2016. aasta määrus (EL) 2016/424, mis käsitleb köisteid ning millega tunnistatakse kehtetuks direktiiv 2000/9/EÜ (ELT L 81, 31.3.2016, lk 1)

9. Euroopa Parlamendi ja nõukogu 9. märtsi 2016. aasta määrus (EL) 2016/425, mis käsitleb isikukaitsevahendeid ja millega tunnistatakse kehtetuks nõukogu direktiiv 89/686/EMÜ (ELT L 81, 31.3.2016, lk 51)

10. Euroopa Parlamendi ja nõukogu 9. märtsi 2016. aasta määrus (EL) 2016/426, mis käsitleb küttegaasi põletavaid seadmeid ning millega tunnistatakse kehtetuks direktiiv 2009/142/EÜ (ELT L 81, 31.3.2016, lk 99)

11. Euroopa Parlamendi ja nõukogu 5. aprilli 2017. aasta määrus (EL) 2017/745, milles käsitletakse meditsiiniseadmeid, millega muudetakse direktiivi 2001/83/EÜ, määrust (EÜ) nr 178/2002 ja määrust (EÜ) nr 1223/2009 ning millega tunnistatakse kehtetuks nõukogu direktiivid 90/385/EMÜ ja 93/42/EMÜ (ELT L 117, 5.5.2017, lk 1)

12. Euroopa Parlamendi ja nõukogu 5. aprilli 2017. aasta määrus (EL) 2017/746 *in vitro* diagnostikameditsiiniseadmete kohta ning millega tunnistatakse kehtetuks direktiiv 98/79/EÜ ja komisjoni otsus 2010/227/EL (ELT L 117, 5.5.2017, lk 176)

B jaotis. Muude liidu ühtlustamisõigusaktide loetelu

1. Euroopa Parlamendi ja nõukogu 11. märtsi 2008. aasta määrus (EÜ) nr 300/2008, mis käsitleb tsiviillennundusjulgestuse ühiseeskirju ja millega tunnistatakse kehtetuks määrus (EÜ) nr 2320/2002 (ELT L 97, 9.4.2008, lk 72)

2. Euroopa Parlamendi ja nõukogu 15. jaanuari 2013. aasta määrus (EL) nr 168/2013 kahe-, kolme- ja neljarattaliste sõidukite kinnituse ja turujärelevalve kohta (ELT L 60, 2.3.2013, lk 52)

3. Euroopa Parlamendi ja nõukogu 5. veebruari 2013. aasta määrus (EL) nr 167/2013 põllu- ja metsamajanduses kasutatavate sõidukite kinnituse ja turujärelevalve kohta (ELT L 60, 2.3.2013, lk 1)

4. Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta direktiiv 2014/90/EL, milles käsitletakse laevavarustust ja millega tunnistatakse kehtetuks nõukogu direktiiv 96/98/EÜ (ELT L 257, 28.8.2014, lk 146)

5. Euroopa Parlamendi ja nõukogu 11. mai 2016. aasta direktiiv (EL) 2016/797 Euroopa Liidu raudteesüsteemi koostalitluse kohta (ELT L 138, 26.5.2016, lk 44)

6. Euroopa Parlamendi ja nõukogu 30. mai 2018. aasta määrus (EL) 2018/858 mootorsõidukite ja mootorsõidukite haagiste ning nende jaoks ette nähtud süsteemide, osade ja eraldi seadmestike tüübikinnituse ja turujärelevalve kohta, ning millega muudetakse määruseid (EÜ) nr 715/2007 ja (EÜ) nr 595/2009 ning tunnistatakse kehtetuks direktiiv 2007/46/EÜ (ELT L 151, 14.6.2018, lk 1)

7. Euroopa Parlamendi ja nõukogu 27. novembri 2019. aasta määrus (EL) 2019/2144, mis käsitleb mootorsõidukite ja nende haagiste ning mootorsõidukite jaoks ette nähtud süsteemide, osade ja eraldi seadmestike tüübikinnituse nõudeid seoses nende üldise ohutuse ning sõitjate ja vähekaitstud liiklejate kaitsega, ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) 2018/858 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrused (EÜ) nr 78/2009, (EÜ) nr 79/2009 ja (EÜ) nr 661/2009 ning komisjoni määrused (EÜ) nr 631/2009, (EL) nr 406/2010, (EL) nr 672/2010, (EL) nr 1003/2010, (EL) nr 1005/2010, (EL) nr 1008/2010, (EL) nr 1009/2010, (EL) nr 19/2011, (EL) nr 109/2011, (EL) nr 458/2011, (EL) nr 65/2012, (EL) nr 130/2012, (EL) nr 347/2012, (EL) nr 351/2012, (EL) nr 1230/2012 ja (EL) 2015/166 (ELT L 325, 16.12.2019, lk 1)

8. Euroopa Parlamendi ja nõukogu 4. juuli 2018. aasta määrus (EL) 2018/1139, mis käsitleb tsiviillennunduse valdkonna ühisnorme ja millega luuakse Euroopa Liidu Lennundusohutusamet ning millega muudetakse Euroopa Parlamendi ja nõukogu määrusi (EÜ) nr 2111/2005, (EÜ) nr 1008/2008, (EL) nr 996/2010, (EL) nr 376/2014 ja Euroopa Parlamendi ja nõukogu direktiive 2014/30/EL ning 2014/53/EL ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrused (EÜ) nr 552/2004 ja (EÜ) nr 216/2008 ning nõukogu määrus (EMÜ) nr 3922/91 (ELT L 212, 22.8.2018, lk 1), kuivõrd see puudutab selle määruse artikli 2 lõike 1 punktides a ja b osutatud õhusõidukite projekteerimist, tootmist ja turule laskmist, kui tegemist on mehitamata õhusõidukite ja nende mootorite, propellerite, osade ning kaugkontrolliseadmetega

III LISA

ARTIKLI 6 LÕIKES 3 OSUTATUD SUURE RISKIGA TEHISINTELLEKTISÜSTEEMID

Igas punktides 1–8 loetletud valdkonnas käsitatakse iga alapunkti all konkreetselt nimetatud tehisintellektisüsteeme artikli 6 lõike 3 kohaste suure riskiga tehisintellektisüsteemidena.

1. Biomeetria:

   a) biomeetrilise kaugtuvastamise süsteemid.

2. Elutähtis taristu:

   a) tehisintellektisüsteemid, mis on mõeldud kasutamiseks elutähtsa digitaristu, maanteeliikluse ning vee, gaasi, kütteenergia ja elektri tarnimise korraldamise ja käitamise turvakomponentidena.

3. Haridus ja kutseõpe:

   a) tehisintellektisüsteemid, mis on mõeldud kasutamiseks selleks, et määrata kindlaks füüsiliste isikute juurdepääs haridus- ja kutseõppeasutustele või -programmidele või nende vastuvõtmine või määramine nendesse kõigil tasanditel;

   b) tehisintellektisüsteemid, mis on mõeldud kasutamiseks õpiväljundite hindamiseks, muu hulgas juhul, kui neid väljundeid kasutatakse füüsiliste isikute õppeprotsessi suunamiseks haridus- ja kutseõppeasutustes või -programmides, kõigil tasanditel.

4. Tööhõive, töötajate juhtimine ja füüsilisest isikust ettevõtjana tegutsemine:

   a) tehisintellektisüsteemid, mis on mõeldud kasutamiseks füüsiliste isikute värbamiseks või valimiseks, eriti sihipäraste töökuulutuste avaldamiseks, tööle kandideerimise taotluste analüüsimiseks ja filtreerimiseks ning kandidaatide hindamiseks;

b) tehisintellektisüsteemid, mis on mõeldud kasutamiseks selleks, et teha edutamise ja töösuhte lõpetamise otsuseid, jagada isiku käitumise või isikuomaduste või erijoonte põhjal tööülesandeid ning tegeleda selliste suhete kontekstis inimeste töötulemuste ja käitumise seire ja hindamisega.

5. Juurdepääs olulistele era- ja avalik-õiguslikele teenustele ja hüvedele ning nende kasutamine:

a) tehisintellektisüsteemid, mis on mõeldud kasutamiseks ametiasutustele või nende nimel, et hinnata füüsiliste isikute vastavust oluliste sotsiaaltoetuste ja -teenuste saamise tingimustele ning selliseid toetusi ja teenuseid anda, vähendada, tühistada või tagasi nõuda;

b) tehisintellektisüsteemid, mis on mõeldud kasutamiseks selleks, et hinnata füüsiliste isikute krediidikõlblikkust või anda neile krediidihinnang, välja arvatud tehisintellektisüsteemid, mille on enda tarbeks kasutusele võtnud mikro- ja väikestest ettevõtjatest pakkujad, nagu on määratletud komisjoni soovituse 2003/361/EÜ lisas;

c) tehisintellektisüsteemid, mis on mõeldud kasutamiseks kiirabi ja päästeteenistuse, sealhulgas tuletõrje ja arstiabi väljasaatmiseks ja väljasaatmisprioriteetide seadmiseks;

d) tehisintellektisüsteemid, mis on mõeldud kasutamiseks selleks, et hinnata riske ja seada hind seoses füüsiliste isikutega elu- ja tervisekindlustusega seotud juhtudel, välja arvatud tehisintellektisüsteemid, mille on enda tarbeks võtnud kasutusele mikro- ja väikesetest ettevõtjatest pakkujad, nagu on määratletud komisjoni soovituse 2003/361/EÜ lisas.

6. Õiguskaitse:

a) tehisintellektisüsteemid, mis on mõeldud kasutamiseks õiguskaitseasutustele või nende nimel, et hinnata, milline on risk, et füüsiline isik rikub seadust või rikub uuesti seadust, või milline on risk, et füüsiline isik saab kuriteo võimalikuks ohvriks;

b) tehisintellektisüsteemid, mis on mõeldud kasutamiseks õiguskaitseasutustele või nende nimel valedetektorite ja muude samalaadsete vahenditena või füüsilise isiku emotsionaalse seisundi tuvastamiseks;

c) [välja jäetud]

d) tehisintellektisüsteemid, mis on mõeldud kasutamiseks õiguskaitseasutustele või nende nimel, et hinnata tõendite usaldusväärsust kuritegude uurimise või nende eest vastutusele võtmise käigus;

e) tehisintellektisüsteemid, mis on mõeldud kasutamiseks õiguskaitseasutustele või nende nimel tegeliku või potentsiaalse kuriteo esinemise või kordumise prognoosimiseks füüsiliste isikute profiilianalüüsi põhjal direktiivi (EL) 2016/680 artikli 3 punkti 4 tähenduses või füüsiliste isikute või rühmade isikuomaduste, erijoonte või varasema kuritegeliku käitumise hindamiseks;

f) tehisintellektisüsteemid, mis on mõeldud kasutamiseks õiguskaitseasutustele või nende nimel kuritegude avastamise, uurimise või nende eest vastutusele võtmise käigus tehtava füüsiliste isikute profiilianalüüsi jaoks direktiivi (EL) 2016/680 artikli 3 lõike 4 tähenduses.

g) [välja jäetud]

7. Rände-, varjupaiga- ja piirikontrollihaldus:

a) tehisintellektisüsteemid, mis on mõeldud kasutamiseks pädevatele asutustele või nende nimel valedetektorite ja muude samalaadsete vahenditena või füüsilise isiku emotsionaalse seisundi tuvastamiseks;

b) tehisintellektisüsteemid, mis on mõeldud kasutamiseks pädevatele asutustele või nende nimel, et hinnata riske, sh turvariski, ebaseadusliku rände riski või terviseriski, mille põhjustab füüsiline isik, kes kavatseb siseneda või on sisenenud liikmesriigi territooriumile;

c) [välja jäetud]

d) tehisintellektisüsteemid, mis on mõeldud kasutamiseks pädevatele asutustele või nende nimel varjupaiga-, viisa- ja elamisloataotluste ja nendega seotud kaebuste läbivaatamisel seoses sellist staatust taotlevate füüsiliste isikute tingimustele vastavusega.

8. Õigusemõistmine ja demokraatlikud protsessid:

a) tehisintellektisüsteemid, mis on mõeldud kasutamiseks õigusasutusele või selle nimel, et tõlgendada fakte või seadusi ning rakendada seadust konkreetse faktide kogumi suhtes.

IV LISA

Artikli 11 lõikes 1 osutatud TEHNILINE DOKUMENTATSIOON

Artikli 11 lõikes 1 osutatud tehniline dokumentatsioon peab sisaldama vähemalt järgmist teavet, nagu asjaomase tehisintellektisüsteemi puhul kohaldatav.

1. Tehisintellektisüsteemi üldine kirjeldus, sealhulgas:

   a) selle sihtotstarve, süsteemi arendaja(d), süsteemi kuupäev ja versioon;

   b) kuidas tehisintellektisüsteem suhtleb või kuidas seda võidakse kasutada, et suhelda riistvara või tarkvaraga, mis ei ole ise tehisintellektisüsteemi osa, kui see on asjakohane;

   c) asjaomase tarkvara või püsivara versioonid ja kõik versiooniuuendustega seotud nõuded;

   d) ammendav kirjeldus kõigi vormide kohta, milles võidakse tehisintellektisüsteem turule lasta või kasutusele võtta (nt riistvarasse integreeritud tarkvarapakett, allalaaditav tarkvara, API jne);

   e) selle riistvara kirjeldus, millel kasutamiseks on tehisintellektisüsteem mõeldud;

   f) kui tehisintellektisüsteem on toote osa, siis fotod või joonised, mis kujutavad toote välist vormi, märgistust ja sisemist struktuuri;

   g) kasutajale mõeldud kasutusjuhend ja vajaduse korral paigaldusjuhend;

2. Tehisintellektisüsteemi komponentide ja selle arendamise protsessi üksikasjalik kirjeldus:

   a) tehisintellektisüsteemi arendamise meetodid ja etapid, sealhulgas, kui see on asjakohane, eeltreenitud süsteemide või kolmandate isikute pakutud töövahendite kasutamine ning see, kuidas pakkuja on neid kasutanud, need integreerinud või neid muutnud;

b) süsteemi projekti kirjeldus, täpsemalt tehisintellektisüsteemi ja algoritmide üldine loogika; olulisemad konstruktsioonivalikud, sh põhjendused ja eeldused, kaasa arvatud nende isikute või isikute rühmade kohta, kelle peal kasutamiseks on see süsteem mõeldud; peamised liigitamisvalikud; mida on süsteem projekteeritud optimeerima ja milline on eri parameetrite olulisus; süsteemi eeldatava väljundi kirjeldus; otsused võimalike kompromisside kohta seoses kasutatud tehniliste lahendustega, et järgida III jaotise 2. peatükis sätestatud nõudeid;

c) süsteemi arhitektuuri kirjeldus, milles selgitatakse, kuidas tarkvarakomponendid üksteisele toetuvad või üksteisele sisendit annavad ja üldise andmetöötlusega integreeruvad; tehisintellektisüsteemi arendamiseks, treenimiseks, testimiseks ja valideerimiseks kasutatud arvutusressursid;

d) kui see on asjakohane, siis andmetele esitatavad nõuded andmelehtedena, milles kirjeldatakse treenimismeetodeid ja -võtteid ning kasutatud treeningandmestikke, sh nende andmestike üldine kirjeldus ning teave nende päritolu, ulatuse ja peamiste omaduste kohta; kuidas andmed on saadud ja valitud; märgistamismenetlused (nt juhendatud õppe korral), andmete puhastamise metoodikad (nt võõrväärtuste avastamine);

e) hinnang artikli 14 kohaselt vajalikele inimjärelevalve meetmetele, sh hinnang tehnilistele meetmetele, mida on vaja, et kasutajatel oleks lihtsam tehisintellektisüsteemi väljundit tõlgendada, vastavalt artikli 13 lõike 3 punktile d;

f) kui see on asjakohane, siis tehisintellektisüsteemi ja selle toimimise ette kindlaks määratud muudatuste üksikasjalik kirjeldus koos kogu asjaomase teabega nende tehniliste lahenduste kohta, mida on kasutatud, et tagada tehisintellektisüsteemi pidev vastavus III jaotise 2. peatükis sätestatud asjaomastele nõuetele;

g) kasutatud valideerimis- ja testimismenetlused, sh teave kasutatud valideerimis- ja testimisandmete ja nende peamiste omaduste kohta; parameetrid, mida kasutatakse, et mõõta täpsust, stabiilsust ja küberturvalisust ning vastavust muudele III jaotise 2. peatükis sätestatud asjaomastele nõuetele ning võimalikku diskrimineerivat mõju; testilogid ja kõik testiaruanded, mis on varustatud kuupäeva ja vastutavate isikute allkirjadega, sh seoses punktis f osutatud ette kindlaksmääratud muudatustega.

3. Üksikasjalik teave tehisintellektisüsteemi seire, toimimise ja kontrollimise kohta, eeskätt seoses järgmisega: süsteemi funktsioonid ja toimimispiirangud, sh täpsusaste konkreetsete isikute või isikute rühmade puhul, kelle peal süsteemi kavatsetakse kasutada, ning üldine eeldatav täpsusaste võrreldes selle sihtotstarbega; prognoositavad soovimatud tagajärjed ja riskiallikad seoses tervise ja ohutuse, põhiõiguste ja diskrimineerimisega, lähtudes tehisintellektisüsteemi sihtotstarbest; artikli 14 kohaselt vajalikud inimjärelevalve meetmed, kaasa arvatud tehnilised meetmed, mis on kehtestatud selleks, et kasutajatel oleks lihtsam tehisintellektisüsteemide väljundit tõlgendada; sisendandmete kirjeldused, kui see on asjakohane.

4. Riskijuhtimissüsteemi üksikasjalik kirjeldus vastavalt artiklile 9.

5. Süsteemi elutsükli jooksul pakkuja poolt tehtud asjassepuutuvate muudatuste kirjeldus.

6. Loetelu täielikult või osaliselt kohaldatavatest harmoneeritud standarditest, mille viited on avaldatud *Euroopa Liidu Teatajas*; kui selliseid harmoneeritud standardeid ei ole kohaldatud, siis III jaotise 2. peatükis sätestatud nõuete täitmiseks kasutatud lahenduste üksikasjalik kirjeldus, sh muude asjaomaste kohaldatud standardite ja tehniliste kirjelduste loetelu.

7. ELi vastavusdeklaratsiooni koopia.

8. Turustamisjärgse seire etapis tehisintellektisüsteemi toimimise hindamiseks kasutusele võetud süsteemi üksikasjalik kirjeldus vastavalt artiklile 61, sh artikli 61 lõikes 3 osutatud turustamisjärgse seire kava.

V LISA

ELi VASTAVUSDEKLARATSIOON

Artiklis 48 osutatud ELi vastavusdeklaratsioon peab sisaldama järgmist teavet.

1. Tehisintellektisüsteemi nimi ja liik ning muud üheselt mõistetavad lisaviited, mis võimaldavad tehisintellektisüsteemi kindlaks teha ja seda jälgida.

2. Pakkuja või vajaduse korral tema volitatud esindaja nimi ja aadress.

3. Märge, et ELi vastavusdeklaratsioon on väljastatud üksnes pakkuja vastutusel.

4. Kinnitus selle kohta, et asjaomane tehisintellektisüsteem vastab käesoleva määruse nõuetele ja olenevalt asjaoludest muude liidu asjaomaste õigusaktide nõetele, millega on ette nähtud ELi vastavusdeklaratsioon väljastamine.

5. Viited asjaomastele kasutatud harmoneeritud standarditele või muudele ühtsetele kirjeldustele, mille põhjal vastavust deklareeritakse.

6. Kui see on asjakohane, siis teavitatud asutuse nimetus ja tunnusnumber, vastavushindamismenetluse kirjeldus ja väljastatud sertifikaadi tunnusnumber.

7. Deklaratsiooni väljastamise koht ja kuupäev, allakirjutanu nimi ja amet, teave, kelle poolt ja kelle nimel on nimetatud isik allkirja andnud, ning allkiri.

VI LISA

SISEKONTROLLIL PÕHINEV VASTAVUSHINDAMINE

1. Sisekontrollil põhinev vastavushindamine on punktidel 2–4 põhinev vastavushindamine.

2. Pakkuja kontrollib, et kehtestatud kvaliteedijuhtimissüsteem vastab artikli 17 nõuetele.

3. Pakkuja vaatab tehnilises dokumentatsioonis sisalduva teabe läbi, et hinnata tehisintellektisüsteemi vastavust III jaotise 2. peatükis sätestatud asjakohastele olulistele nõuetele.

4. Ühtlasi kontrollib pakkuja, kas tehisintellektisüsteemi projekteerimis- ja arendusprotsess ning artiklis 61 osutatud turustamisjärgne seire on kooskõlas tehnilise dokumentatsiooniga.

VII LISA

KVALITEEDIJUHTIMISSÜSTEEMI JA TEHNILISE DOKUMENTATSIOONI HINDAMISEL PÕHINEV VASTAVUS

1. Sissejuhatus

Kvaliteedijuhtimissüsteemi ja tehnilise dokumentatsiooni hindamisel põhineva vastavuse puhul on tegu punktidel 2–5 põhineva vastavushindamisega.

2. Ülevaade

Tehisintellektisüsteemide projekteerimise, arendamise ja testimise jaoks heakskiidetud artikli 17 kohane kvaliteedijuhtimise süsteem vaadatakse läbi vastavalt punktile 3 ja selle suhtes kohaldatakse punktis 5 sätestatud järelevalvet. Tehisintellektisüsteemi tehniline dokumentatsioon vaadatakse läbi vastavalt punktile 4.

3. Kvaliteedijuhtimissüsteem

3.1. Pakkuja taotlus peab sisaldama järgmist:

a) pakkuja nimi ja aadress ning kui taotluse on esitanud volitatud esindaja, siis ka tema nimi ja aadress;

b) sama kvaliteedijuhtimissüsteemiga hõlmatud tehisintellektisüsteemide loetelu;

c) tehniline dokumentatsioon iga sama kvaliteedijuhtimissüsteemiga hõlmatud tehisintellektisüsteemi kohta;

d) kvaliteedijuhtimissüsteemi käsitlev dokumentatsioon, mis hõlmab kõiki artiklis 17 loetletud aspekte;

e) kvaliteedijuhtimissüsteemi asjakohasuse ja tulemuslikkuse tagamiseks kasutatavate menetluste kirjeldus;

f) kirjalik kinnitus selle kohta, et samasugust taotlust ei ole esitatud mõnele teisele teavitatud asutusele.

3.2. Kvaliteedijuhtimissüsteemi hindab teavitatud asutus, kes teeb kindlaks, kas süsteem vastab artiklis 17 osutatud nõuetele.

Otsusest teatatakse pakkujale või tema volitatud esindajale.

Teade sisaldab kvaliteedijuhtimissüsteemi hindamise järeldusi ning põhjendatud hindamisotsust.

3.3. Pakkuja jätkab heaks kiidetud kvaliteedijuhtimissüsteemi rakendamist ja haldamist, et see oleks jätkuvalt piisav ja tõhus.

3.4. Pakkuja peab teavitatud asutust informeerima kõigist muudatustest, mis kavatsetakse teha heakskiidetud kvaliteedijuhtimissüsteemis või sellega hõlmatud tehisintellektisüsteemide loetelus.

Teavitatud asutus vaatab kavandatud muudatused läbi ja otsustab, kas muudetud kvaliteedijuhtimissüsteem vastab jätkuvalt punktis 3.2 osutatud nõuetele või on vaja uut hindamist.

Teavitatud asutus teatab oma otsusest pakkujale. Teade sisaldab muudatuste hindamise järeldusi ning põhjendatud hindamisotsust.

4. Tehnilise dokumentatsiooni kontrollimine

4.1. Lisaks punktis 3 osutatud taotlusele esitab pakkuja enda valitud teavitatud asutusele taotluse, et hinnataks sellise tehisintellektisüsteemi kohta käivat tehnilist dokumentatsiooni, mille pakkuja kavatseb turule lasta või kasutusele võtta ja mida hõlmab punktis 3 osutatud kvaliteedijuhtimissüsteem.

4.2. Taotlus peab sisaldama järgmist:

a) pakkuja nimi ja aadress;

b) kirjalik kinnitus selle kohta, et samasugust taotlust ei ole esitatud mõnele teisele teavitatud asutusele;

c) IV lisas osutatud tehniline dokumentatsioon.

4.3. Teavitatud asutus vaatab tehnilise dokumentatsiooni läbi. Kui see on asjakohane ja piiratud oma ülesannete täitmiseks vajalikuga, antakse teavitatud asutusele täielik juurdepääs kasutatavatele treenimis-, valideerimis- ja testimisandmestikele, sealhulgas, kui see on asjakohane ja kui kohaldatakse turvameetmeid, rakendusliideste (API) või muude asjakohaste kaugjuurdepääsu võimaldavate tehniliste vahendite ja tööriistade kaudu.

4.4. Tehnilise dokumentatsiooni läbivaatamise käigus võib teavitatud asutus nõuda, et pakkuja esitaks täiendavaid tõendeid või teeks täiendavaid teste, et oleks võimalik nõuetekohaselt hinnata tehisintellektisüsteemi vastavust III jaotise 2. peatükis sätestatud nõuetele. Kui teavitatud asutus ei ole pakkuja tehtud testidega rahul, teeb teavitatud asutus piisavad testid, nagu on asjakohane.

4.5. Juurdepääs tehisintellektisüsteemi lähtekoodile antakse teavitatud asutusele põhjendatud taotluse alusel ja ainult juhul, kui on täidetud järgmised kumulatiivsed tingimused:

a) juurdepääs lähtekoodile on vajalik selleks, et hinnata suure riskiga tehisintellektisüsteemi vastavust III jaotise 2. peatükis sätestatud nõuetele, ning

b) pakkuja esitatud andmetel ja dokumentidel põhinevad testimis-/auditeerimismenetlused ja kontrollid on ammendatud või osutunud ebapiisavaks.

4.6. Otsusest teatatakse pakkujale või tema volitatud esindajale. Teade sisaldab tehnilise dokumentatsiooni hindamise järeldusi ning põhjendatud hindamisotsust.

Kui tehisintellektisüsteem vastab III jaotise 2. peatükis sätestatud nõuetele, väljastab teavitatud asutus ELi tehnilise dokumentatsiooni hindamise sertifikaadi. Sertifikaat sisaldab pakkuja nime ja aadressi, läbivaatamise põhjal tehtud järeldusi, vajaduse korral kehtivustingimusi ja tehisintellektisüsteemi identifitseerimiseks vajalikke andmeid.

Sertifikaat ja selle lisad sisaldavad kogu asjakohast teavet, et oleks võimalik hinnata tehisintellektisüsteemi vastavust ja et tehisintellektisüsteemi saaks kasutamise ajal kontrollida, kui see on asjakohane.

Kui tehisintellektisüsteem ei vasta III jaotise 2. peatükis sätestatud nõuetele, keeldub teavitatud asutus ELi tehnilise dokumentatsiooni hindamise sertifikaadi väljastamisest ja teatab sellest taotlejale, põhjendades keeldumist üksikasjalikult.

Kui tehisintellektisüsteem ei vasta nõuetele, mis on seotud süsteemi treenimiseks kasutatud andmetega, tuleb tehisintellektisüsteem enne uue vastavushindamise taotlemist uuesti treenida. Sellisel juhul peab ELi tehnilise dokumentatsiooni hindamise sertifikaadi väljastamisest keeldunud teavitatud asutuse põhjendatud hindamisotsus sisaldama konkreetseid argumente tehisintellektisüsteemi treenimiseks kasutatud andmete kvaliteedi kohta, eeskätt mittevastavuse põhjuste kohta.

4.7. Teavitatud asutus, kes väljastas ELi tehnilise dokumentatsiooni hindamise sertifikaadi, peab heaks kiitma kõik tehisintellektisüsteemi muudatused, mis võivad mõjutada tehisintellektisüsteemi vastavust nõuetele või süsteemi sihtotstarvet. Pakkuja peab informeerima sellist teavitatud asutust, kui ta kavatseb teha eespool nimetatud muudatusi või kui ta saab muul moel sellistest muudatustest teada. Teavitatud asutus hindab kavandatud muudatusi ja otsustab, kas kavandatud muudatused eeldavad uut vastavushindamist vastavalt artikli 43 lõikele 4 või piisab nende puhul ELi tehnilise dokumentatsiooni hindamise sertifikaadi lisast. Viimasel juhul hindab teavitatud asutus muudatusi, teatab pakkujale oma otsuse ning, juhul kui muudatused heaks kiidetakse, väljastab pakkujale ELi tehnilise dokumentatsiooni hindamise sertifikaadi lisa.

5. Heakskiidetud kvaliteedijuhtimissüsteemide järelevalve

5.1. Punktis 3 osutatud teavitatud asutuse teostatava järelevalve eesmärk on tagada, et pakkuja täidab nõuetekohaselt heakskiidetud kvaliteedijuhtimissüsteemi tingimusi.

5.2. Pakkuja annab teavitatud asutusele hindamise jaoks juurdepääsu ruumidele, kus toimub tehisintellektisüsteemi projekteerimine, arendamine ja testimine. Lisaks jagab pakkuja teavitatud asutusega kogu vajalikku teavet.

5.3. Teavitatud asutus teostab korrapäraselt auditeid tagamaks, et pakkuja säilitab ja rakendab kvaliteedijuhtimissüsteemi, ja esitab pakkujale selle kohta auditeerimisaruande. Seoses nende auditite ga võib teavitatud asutus täiendavalt testida tehisintellektisüsteeme, mille kohta on väljastatud ELi tehnilise dokumentatsiooni hindamise sertifikaat.

VIII LISA

TEAVE, MIS TULEB ESITADA OPERAATORI JA SUURE RISKIGA TEHISINTELLEKTISÜSTEEMI REGISTREERIMISEL VASTAVALT ARTIKLILE 51

Pakkujad, volitatud esindajad ja kasutajad, kes on avaliku sektori asutused, ametid või organid, esitavad I osas osutatud teabe. Pakkujad või asjakohasel juhul volitatud esindajad tagavad, et II osa punktides 1–11 osutatud nende suure riskiga tehisintellektisüsteemide andmed on täielikud, täpsed ja ajakohased. II osa punktis 12 osutatud teabe loob andmebaas automaatselt.

I osa. Operaatoriga seotud teave (operaatori registreerimisel)

-1. Operaatori liik (pakkuja, volitatud esindaja või kasutaja)

1. Pakkuja nimi, aadress ja kontaktandmed.

2. Kui operaatori nimel esitab teabe keegi teine, siis selle isiku nimi, aadress ja kontaktandmed.

II osa. Suure riskiga tehisintellektisüsteemiga seotud teave

1. Pakkuja nimi, aadress ja kontaktandmed.

2. Volitatud esindaja nimi, aadress ja kontaktandmed, kui see on asjakohane.

3. Tehisintellektisüsteemi kaubanimi ning muud täiendavad üheselt mõistetavad viited, mis võimaldavad tehisintellektisüsteemi kindlaks teha ja seda jälgida.

4. Tehisintellektisüsteemi sihtotstarbe kirjeldus.

5. Tehisintellektisüsteemi staatus (turul või kasutuses, ei ole enam turul/kasutuses, tagasi kutsutud).

6. Teavitatud asutuse väljastatud sertifikaadi liik, number ja kehtivusaeg ning selle teavitatud asutuse nimetus või tunnusnumber, kui see on asjakohane.

7. Punktis 6 osutatud sertifikaadi skaneeritud koopia, kui see on asjakohane.

8. Need liikmesriigid, kus tehisintellektisüsteem on liidus turule lastud, kasutusele võetud või kättesaadavaks tehtud.

9. Artiklis 48 osutatud ELi vastavusdeklaratsiooni koopia.

10. Elektrooniline kasutusjuhend.

11. Täiendava teabe URL, kui see on asjakohane.

12. Kasutaja nimi, aadress ja kontaktandmed.

VIIIa LISA

TEAVE, MIS TULEB ESITADA III LISAS LOETLETUD SUURE RISKIGA TEHISINTELLEKTISÜSTEEMI REGISTREERIMISEL SEOSES TESTIMISEGA TEGELIKES TINGIMUSTES KOOSKÕLAS ARTIKLIGA 54A

Tegelikes tingimustes testimise kohta, mis tuleb registreerida vastavalt artiklile 54a, tuleb esitada järgmine teave ning seda edaspidi ajakohastada.

1. Tegelikes tingimustes testimise üleliiduline kordumatu ühtne identifitseerimisnumber.

2. Tegelikes tingimustes testimises osaleva pakkuja või võimaliku pakkuja ja kasutajate nimi ja kontaktandmed.

3. Tehisintellektisüsteemi lühikirjeldus, selle sihtotstarve ja muu süsteemi identifitseerimiseks vajalik teave.

4. Tegelikes tingimustes testimise kava põhiomaduste kokkuvõte.

5. Teave tegelikes tingimustes testimise peatamise või lõpetamise kohta.

IX LISA

LIIDU ÕIGUSAKTID VABADUSEL, TURVALISUSEL JA ÕIGUSEL RAJANEV ALA SUUREMAHULISTE IT-SÜSTEEMIDE KOHTA

1. Schengeni infosüsteem

   a) Euroopa Parlamendi ja nõukogu 28. novembri 2018. aasta määrus (EL) 2018/1860 Schengeni infosüsteemi kasutamise kohta ebaseaduslikult riigis viibivate kolmandate riikide kodanike tagasisaatmiseks (ELT L 312, 7.12.2018, lk 1)

   b) Euroopa Parlamendi ja nõukogu 28. novembri 2018. aasta määrus (EL) 2018/1861, milles käsitletakse Schengeni infosüsteemi (SIS) loomist, toimimist ja kasutamist kontrollide valdkonnas piiril ning millega muudetakse Schengeni lepingu rakendamise konventsiooni ja määrust (EÜ) nr 1987/2006 ning tunnistatakse kehtetuks määrus (EÜ) nr 1987/2006 (ELT L 312, 7.12.2018, lk 14)

   c) Euroopa Parlamendi ja nõukogu 28. novembri 2018. aasta määrus (EL) 2018/1862, milles käsitletakse Schengeni infosüsteemi (SIS) loomist, toimimist ja kasutamist politseikoostöös ja kriminaalasjades tehtavas õigusalases koostöös ning millega muudetakse nõukogu otsust 2007/533/JSK ja tunnistatakse see kehtetuks ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1986/2006 ning komisjoni otsus 2010/261/EL (ELT L 312, 7.12.2018, lk 56)

2. Viisainfosüsteem

   a) EUROOPA PARLAMENDI JA NÕUKOGU määrus, millega muudetakse määrust (EÜ) nr 767/2008, määrust (EÜ) nr 810/2009, määrust (EL) 2017/2226, määrust (EL) 2016/399, määrust XX/2018 [koostalitlusvõimet käsitlev määrus] ja otsust 2004/512/EÜ ning tunnistatakse kehtetuks nõukogu otsus 2008/633/JSK (COM(2018) 302 final). Ajakohastatakse, kui kaasseadusandjad on määruse vastu võtnud (aprill-mai 2021).

3. Eurodac

a) Muudetud ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega kehtestatakse biomeetriliste andmete võrdlemise Eurodac-süsteem määruse (EL) nr XXX/XXX [varjupaiga- ja rändehalduse määrus] ja määruse (EL) nr XXX/XXX [ümberasustamise määrus] tõhusaks kohaldamiseks, et tuvastada ebaseaduslikult riigis viibivad kolmandate riikide kodanikud ja kodakondsuseta isikud, ning mis käsitleb liikmesriikide õiguskaitseasutuste ja Europoli taotlusi sõrmejälgede andmete võrdlemiseks Eurodac-süsteemi andmetega õiguskaitse eesmärgil ning millega muudetakse määrust (EL) 2018/1240 ja määrust (EL) 2019/818 (COM(2020) 614 final)

4. Riiki sisenemise ja riigist lahkumise süsteem

a) Euroopa Parlamendi ja nõukogu 30. novembri 2017. aasta määrus (EL) 2017/2226, millega luuakse riiki sisenemise ja riigist lahkumise süsteem liikmesriikide välispiire ületavate kolmandate riikide kodanike riiki sisenemise ja riigist lahkumise andmete ja sisenemiskeeluandmete registreerimiseks ning määratakse kindlaks riiki sisenemise ja riigist lahkumise süsteemile õiguskaitse eesmärgil juurdepääsu andmise tingimused ning millega muudetakse Schengeni lepingu rakendamise konventsiooni ning määruseid (EÜ) nr 767/2008 ja (EL) nr 1077/2011 (ELT L 327, 9.12.2017, lk 20)

5. Euroopa reisiinfo ja -lubade süsteem

a) Euroopa Parlamendi ja nõukogu 12. septembri 2018. aasta määrus (EL) 2018/1240, millega luuakse Euroopa reisiinfo ja -lubade süsteem (ETIAS) ning muudetakse määrusi (EL) nr 1077/2011, (EL) nr 515/2014, (EL) 2016/399, (EL) 2016/1624 ja (EL) 2017/2226 (ELT L 236, 19.9.2018, lk 1)

b) Euroopa Parlamendi ja nõukogu 12. septembri 2018. aasta määrus (EL) 2018/1241, millega muudetakse määrust (EL) 2016/794 Euroopa reisiinfo ja -lubade süsteemi (ETIAS) loomise eesmärgil (ELT L 236, 19.9.2018, lk 72)

6. Euroopa karistusregistrite infosüsteem kolmandate riikide kodanike ja kodakondsuseta isikute kohta

   a) Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/816, millega luuakse kesksüsteem nende liikmesriikide väljaselgitamiseks, kellel on teavet kolmandate riikide kodanike ja kodakondsuseta isikute suhtes tehtud süüdimõistvate kohtuotsuste kohta, et täiendada Euroopa karistusregistrite infosüsteemi (ECRIS-TCN), ning muudetakse määrust (EL) 2018/1726 (ELT L 135, 22.5.2019, lk 1)

7. Koostalitlusvõime

   a) Euroopa Parlamendi ja nõukogu 20. mai 2019. aasta määrus (EL) 2019/817, millega luuakse ELi infosüsteemide koostalitlusvõime raamistik piiride ja viisade valdkonnas (ELT L 135, 22.5.2019, lk 27)

   b) Euroopa Parlamendi ja nõukogu 20. mai 2019. aasta määrus (EL) 2019/818, millega luuakse ELi infosüsteemide koostalitlusvõime raamistik politsei- ja õiguskoostöö, varjupaiga ja rände valdkonnas (ELT L 135, 22.5.2019, lk 85)