EUROOPA LIIT

EUROOPA PARLAMENT **NÕUKOGU**

Brüssel, 13. juuni 2024
(OR. en)

2021/0106(COD)
LEX 2363

PE-CONS 24/1/24
REV 1

TELECOM 54
JAI 238
COPEN 69
CYBER 37
DATAPROTECT 76
EJUSTICE 11
COSI 16
IXIM 49
ENFOPOL 63
RELEX 180
MI 151
COMPET 154
CODEC 412

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, MILLEGA NÄHAKSE ETTE TEHISINTELLEKTI KÄSITLEVAD ÜHTLUSTATUD ÕIGUSNORMID NING MUUDETAKSE MÄÄRUSEID (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 JA (EL) 2019/2144 NING DIREKTIIVE 2014/90/EL, (EL) 2016/797 JA (EL) 2020/1828 (TEHISINTELLEKTI KÄSITLEV MÄÄRUS)

EUROOPA PARLAMENDI JA NÕUKOGU
MÄÄRUS (EL) 2024/…,

13. juuni 2024,

millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ning muudetakse määruseid (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ning direktiive 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828 (tehisintellekti käsitlev määrus)

(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 Euroopa Keskpanga arvamust[2],

võttes arvesse Regioonide Komitee arvamust[3],

toimides seadusandliku tavamenetluse kohaselt[4]

---

1 ELT C 517, 22.12.2021, lk 56.
2 ELT C 115, 11.3.2022, lk 5.
3 ELT C 97, 28.2.2022, lk 60.
4 Euroopa Parlamendi 13. märtsi 2024. aasta seisukoht (*Euroopa Liidu Teatajas* seni avaldamata) ja nõukogu 21. mai 2024. aasta otsus.

ning arvestades järgmist:

(1) Käesoleva määruse eesmärk on parandada siseturu toimimist ühtse õigusraamistiku kehtestamisega eeskätt tehisintellektisüsteemide arendamiseks, turule laskmiseks, kasutusele võtmiseks ja kasutamiseks liidus kooskõlas liidu väärtustega, et edendada inimkeskse ja usaldusväärse tehisintellekti levikut, tagades samal ajal tervise, turvalisuse, Euroopa Liidu põhiõiguste hartas (edaspidi „põhiõiguste harta“) sätestatud põhiõiguste, sealhulgas demokraatia ja õigusriigi kõrgetasemelise kaitse ning keskkonnakaitse, kaitsta tehisintellekti süsteemide kahjuliku mõju vastu liidus, ning toetada innovatsiooni. Käesoleva määrusega tagatakse tehisintellektil põhinevate kaupade ja teenuste vaba piiriülene liikumine, takistades seega liikmesriikidel kehtestamast piiranguid tehisintellektisüsteemide arendamisele, turustamisele ja kasutamisele, välja arvatud juhul, kui see käesoleva määrusega selgesõnaliselt lubatakse.

(2) Käesolevat määrust tuleks kohaldada kooskõlas põhiõiguste hartas sätestatud liidu väärtustega, hõlbustades füüsiliste isikute, ettevõtjate, demokraatia ja õigusriigi kaitset ning keskkonnakaitset, edendades samal ajal innovatsiooni ja tööhõivet ning viies liidu usaldusväärse tehisintellekti laialdaselt kasutuselevõtmises juhtpositsioonile.

(3) Tehisintellektisüsteeme saab kergesti juurutada paljudes erinevates majandussektorites ja ühiskonna osades, sealhulgas piiriüleselt, ning need saavad kergesti levida kogu liidus. Teatavad liikmesriigid on juba uurinud võimalust võtta vastu riigisisesed õigusnormid, et tagada tehisintellekti usaldusväärsus ja ohutus ning selle arendamine ja kasutamine kooskõlas põhiõigustealaste kohustustega. Erinevad riigisisesed õigusnormid võivad tuua kaasa siseturu killustumise ja võivad vähendada tehisintellektisüsteemide arendamise, impordi või kasutamisega tegelevate operaatorite õiguskindlust. Seepärast tuleks usaldusväärse tehisintellekti saavutamiseks tagada kõikjal liidus kaitse järjekindlus ja kõrge tase ning ühtlasi hoida ära erinevusi, mis kahjustavad tehisintellektisüsteemide ja nendega seotud toodete ja teenuste vaba ringlust, innovatsiooni, juurutamist ja levikut siseturul; selleks tuleks operaatoritele kehtestada ühetaolised kohustused ja tagada kaalukate üldiste huvide ja isikute õiguste ühtne kaitse siseturul, lähtudes Euroopa Liidu toimimise lepingu (ELi toimimise leping) artiklist 114. Kuivõrd käesolev määrus sisaldab konkreetseid õigusnorme, mis puudutavad üksikisikute kaitset isikuandmete töötlemisel ja millega piiratakse tehisintellektisüsteemide kasutamist õiguskaitse eesmärgil toimuva biomeetrilise kaugtuvastamise jaoks, tehisintellektisüsteemide kasutamist õiguskaitse eesmärgil toimuva füüsiliste isikutega seotud riskihindamise jaoks ja tehisintellektisüsteemide kasutamist õiguskaitse eesmärgil toimuva biomeetrilise liigitamise 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.

(4) Tehisintellekt on kiiresti arenev tehnoloogiaharu, mis aitab saavutada mitmesuguseid majanduslikke, keskkondlikke 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 soodsate tulemuste saavutamist näiteks sellistes valdkondades nagu tervishoid, põllumajandus, toiduohutus, haridus ja koolitus, meedia, sport, kultuur, taristuhaldus, energeetika, transport ja logistika, avalikud teenused, turvalisus, õigus, ressursi- ja energiatõhusus, keskkonnaseire, elurikkuse ja ökosüsteemide säilitamine ja taastamine ning kliimamuutuste leevendamine ja nendega kohanemine.

(5) Samas võib tehisintellekt olenevalt konkreetse rakenduse asjaoludest, kasutusest ja tehnoloogilise arengu tasemest tekitada ka riske ning kahjustada avalikke huve ja liidu õigusega kaitstud põhiõigusi. Selline kahju võib olla varaline või mittevaraline, sealhulgas füüsiline, psühholoogiline, ühiskondlik või majanduslik.

(6) Võttes arvesse suurt mõju, mida tehisintellekt võib ühiskonnale avaldada, ja vajadust suurendada usaldust, on äärmiselt oluline, et tehisintellekti arendamisel ja selle õigusraamistiku väljatöötamisel järgitaks Euroopa Liidu lepingu (ELi lepingu) artiklis 2 sätestatud liidu väärtusi ning aluslepingutes ja ELi lepingu artikli 6 kohaselt põhiõiguste hartas sätestatud põhiõigusi ja -vabadusi. Tuleks seada eeltingimuseks, et tehisintellekt peab olema inimkeskne tehnoloogia. See peaks olema vahend, mis teenib inimesi ja mille lõppeesmärk on suurendada inimeste heaolu.

(7) Selleks et tagada järjekindel ja kõrgetasemeline avalike huvide kaitse tervise, turvalisuse ja põhiõiguste vallas, tuleks suure riskiga tehisintellektisüsteemide jaoks kehtestada ühised õigusnormid. Need õigusnormid peaksid olema kooskõlas põhiõiguste hartaga, mittediskrimineerivad ja järgima liidu rahvusvahelisi kaubanduskohustusi. Samuti tuleks nende õigusnormide puhul arvesse võtta Euroopa deklaratsiooni digiõiguste ja -põhimõtete kohta digikümnendiks ja kõrgetasemelise tehisintellekti eksperdirühma suuniseid usaldusväärse tehisintellekti arendamiseks.

(8) Seepärast on vaja liidu õigusraamistikku, milles nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid, et edendada siseturul tehisintellekti arendamist, kasutamist ja levikut, mille puhul oleks ühtlasi tagatud liidu õigusega tunnustatud ja kaitstud avalike huvide, näiteks tervise ja ohutuse ning põhiõiguste, sealhulgas demokraatia ja õigusriigi kõrgetasemeline kaitse ning keskkonnakaitse. Selle eesmärgi saavutamiseks tuleks kehtestada teatavate tehisintellektisüsteemide turule laskmist, kasutusele võtmist ja kasutamist reguleerivad õigusnormid, et seeläbi tagada siseturu sujuv toimimine ja võimaldada neil süsteemidel saada kasu kaupade ja teenuste vaba liikumise põhimõttest. Nimetatud normid peaksid olema põhiõiguste kaitsmisel selged ja töökindlad, toetades uusi innovatiivseid lahendusi ning võimaldades avaliku ja erasektori osalejate Euroopa ökosüsteemil luua tehisintellektisüsteeme kooskõlas liidu väärtustega ja vallandades digipöörde potentsiaali kõigis liidu piirkondades. Nimetatud õigusnormide kehtestamisega, samuti meetmete võtmisega innovatsiooni toetamiseks, keskendudes eriti väikestele ja keskmise suurusega ettevõtjatele (VKEd), sealhulgas idufirmadele, toetab käesolev määrus eesmärki edendada Euroopa inimkeskset lähenemisviisi tehisintellektile ning seda, et liidul oleks turvalise, usaldusväärse ja eetilise tehisintellekti arendamises ülemaailmne juhtroll, nagu sõnastati Euroopa Ülemkogul[5], ning samas aitab see tagada eetiliste põhimõtete kaitse, mida on eraldi nõudnud Euroopa Parlament[6].

---

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

6 Euroopa Parlamendi 20. oktoobri 2020. aasta resolutsioon soovitustega komisjonile tehisintellekti, robootika, robotitehnoloogia ja seonduva tehnoloogia eetiliste aspektide raamistiku kohta (ELT C 404, 6.10.2021, lk 63).

(9) Suure riskiga tehisintellektisüsteemide turule laskmise, kasutusele võtmise ja kasutamise suhtes kohaldatavad ühtlustatud õigusnormid tuleks kehtestada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EÜ) nr 765/2008[7], Euroopa Parlamendi ja nõukogu otsusega nr 768/2008/EÜ[8] ning Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/1020[9] (edaspidi „uus õigusraamistik“). Käesolevas määruses sätestatud ühtlustatud õigusnorme tuleks kohaldada kõigis sektorites ning kooskõlas uue õigusraamistikuga ei tohiks need piirata kehtivat liidu õigust, eeskätt andmekaitset, tarbijakaitset, põhiõigusi, tööhõivet ja töötajate kaitset ning tooteohutust käsitlevaid õigusakte, mida käesolev määrus täiendab. Sellest tulenevalt jäävad muutumatuks ja täielikult kohaldatavaks kõik õigused ja õiguskaitsevahendid, mis on liidu õiguses ette nähtud tarbijatele ja muudele isikutele, keda tehisintellektisüsteemid võivad negatiivselt mõjutada, sealhulgas seoses võimaliku kahju hüvitamisega vastavalt nõukogu direktiivile 85/374/EMÜ[10].

---

7 Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta määrus (EÜ) nr 765/2008, millega sätestatakse akrediteerimisnõuded ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93 (ELT L 218, 13.8.2008, lk 30).

8 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).

9 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).

10 Nõukogu 25. juuli 1985. aasta direktiiv 85/374/EMÜ liikmesriikide tootevastutust käsitlevate õigus- ja haldusnormide ühtlustamise kohta (EÜT L 210, 7.8.1985, lk 29).

Lisaks ei tohiks käesolev määrus tööhõive ja töötajate kaitse kontekstis mõjutada sotsiaalpoliitikat käsitlevat liidu õigust ega liidu õigusega kooskõlas olevat riigisisest tööõigust, mis käsitleb tööhõivet ja töötingimusi, sealhulgas töötervishoidu ja -ohutust ning tööandjate ja töötajate vahelisi suhteid. Käesolev määrus ei tohiks samuti mõjutada liikmesriikides ja liidu tasandil tunnustatud põhiõiguste, sealhulgas streigiõiguse või -vabaduse teostamist või õigust või vabadust võtta muid liikmesriikide töösuhete erisüsteemidega hõlmatud meetmeid, samuti õigust pidada läbirääkimisi kollektiivlepingute üle, neid sõlmida ja jõustada või kollektiivselt tegutseda kooskõlas riigisisese õigusega. Käesolev määrus ei tohiks mõjutada sätteid, mille eesmärk on parandada platvormitöö tingimusi, mis on sätestatud Euroopa Parlamendi ja nõukogu direktiivis platvormitöö tingimuste parandamise kohta. Lisaks sellele on käesoleva määruse eesmärk tugevdada nimetatud kehtivate õiguste ja õiguskaitsevahendite tõhusust, kehtestades konkreetsed nõuded ja kohustused, sealhulgas seoses tehisintellektisüsteemide läbipaistvuse, tehnilise dokumentatsiooni 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 riigisiseste 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 riigisisest tööõigust ja alaealiste, nimelt alla 18-aastaste isikute kaitset käsitlevaid õigusakte, võttes arvesse ÜRO lapse õiguste komitee üldist märkust nr 25 (2021) laste õiguste kohta seoses digikeskkonnaga, niivõrd, kuivõrd need ei ole tehisintellektisüsteemidele eriomased ja taotlevad muid õiguspäraseid avaliku huvi eesmärke.

(10) Põhiõigus isikuandmete kaitsele on tagatud eelkõige Euroopa Parlamendi ja nõukogu määrustega (EL) 2016/679[11] ja (EL) 2018/1725[12] ning Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2016/680[13]. Euroopa Parlamendi ja nõukogu direktiiviga 2002/58/EÜ[14] kaitstakse lisaks eraelu puutumatust ja side konfidentsiaalsust, sealhulgas isikuandmete ja isikustamata andmete lõppseadmesse talletamist ja andmetele lõppseadmest juurdepääsu käsitlevate tingimuste sätestamise kaudu. Need liidu õigusaktid on aluseks kestlikule ja vastutustundlikule andmetöötlusele, sealhulgas juhtudel, kui andmestikud sisaldavad nii isikuandmeid kui ka isikustamata andmeid. Käesoleva määruse eesmärk ei ole mõjutada isikuandmete töötlemist reguleeriva kehtiva liidu õiguse kohaldamist, sealhulgas selliste sõltumatute järelevalveasutuste ülesandeid ja volitusi, kes on pädevad jälgima kõnealuste õigusaktide järgimist.

---

11 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).

12 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).

13 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 (ELT L 119, 4.5.2016, lk 89).

14 Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37).

Samuti ei mõjuta käesolev määrus tehisintellektisüsteemide pakkujate ja juurutajate jaoks liidu või liikmesriikide 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 (k.a 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.

(11) Käesolev määrus ei tohiks mõjutada Euroopa Parlamendi ja nõukogu määruse (EL) 2022/2065[15] vahendajatest teenuseosutajate vastutust käsitlevate sätete kohaldamist.

[15] Euroopa Parlamendi ja nõukogu 19. oktoobri 2022. aasta määrus (EL) 2022/2065, mis käsitleb digiteenuste ühtset turgu ja millega muudetakse direktiivi 2000/31/EÜ (digiteenuste määrus) (ELT L 277, 27.10.2022, lk 1)..

(12) Tehisintellektisüsteemi mõiste tuleks käesolevas määruses selgelt määratleda ja see peaks olema tihedalt kooskõlas tehisintellekti valdkonnas tegutsevate rahvusvaheliste organisatsioonide tööga, et tagada õiguskindlus, hõlbustada rahvusvahelist lähenemist ja laialdast aktsepteerimist, võimaldades samal ajal paindlikkust, et võtta arvesse tehnoloogia kiiret arengut selles valdkonnas. Lisaks peaks see mõiste põhinema tehisintellektisüsteemide põhiomadustel, mis eristavad neid lihtsamatest traditsioonilistest tarkvarasüsteemidest või programmeerimisviisidest ega peaks hõlmama süsteeme, mis kasutavad toimingute automaatseks sooritamiseks üksnes füüsiliste isikute määratletud reegleid. Tehisintellektisüsteemide põhiomadus on nende võime teha järeldusi. See järelduste tegemise võime viitab protsessile, mis toodab selliseid väljundeid nagu prognoosid, sisu, soovitused või otsused, mis võivad mõjutada füüsilist ja virtuaalset keskkonda, ning tehisintellektisüsteemide võimele tuletada sisenditest või andmetest mudeleid või algoritme või mõlemaid. Meetodid, mis aitavad tehisintellektisüsteemi loomisel saavutada selle järelduste tegemise võime, hõlmavad masinõppemeetodeid, mis õpivad andmete põhjal, kuidas saavutada teatavaid eesmärke, ning loogika- ja teadmistepõhiseid lähenemisviise, mis teevad järeldusi kodeeritud teadmiste või lahendatava ülesande sümboolse esituse põhjal. Tehisintellektisüsteemi võime teha järeldusi ulatub kaugemale vaid andmete töötlemisest, võimaldades õppimist, arutlust või modelleerimist. Mõiste „masinpõhine“ viitab asjaolule, et tehisintellektisüsteemid kasutavad oma tööks masinaid.

Viide otsestele või kaudsetele eesmärkidele rõhutab, et tehisintellektisüsteemid võivad toimida vastavalt selgetele määratletud eesmärkidele või kaudsetele eesmärkidele. Tehisintellektisüsteemi eesmärgid võivad teatud kontekstis erineda tehisintellektisüsteemi kasutusotstarbest. Käesoleva määruse kohaldamisel tuleks keskkondade all mõista konteksti, milles tehisintellektisüsteemid toimivad, samas kui tehisintellektisüsteemi loodud väljundid kajastavad tehisintellektisüsteemide erinevaid funktsioone ning hõlmavad prognoose, sisu, soovitusi ja otsuseid. Tehisintellektisüsteemid on projekteeritud töötama erinevatel autonoomsuse tasemetel, mis tähendab, et neil on teatav inimesest sõltumatu tegevusvabadus ja suutlikkus toimida ilma inimsekkumiseta. Kohanemisvõime, mida tehisintellektisüsteem võib pärast juurutamist demonstreerida, viitab iseõppimisvõimele, mis võimaldab süsteemil kasutamise ajal muutuda. Tehisintellektisüsteeme võib kasutada autonoomselt või mingi toote komponentidena, olenemata sellest, kas süsteem on füüsiliselt tootesse integreeritud (sisseehitatud) või teenib toote funktsionaalsust ilma, et oleks sellesse integreeritud (sisseehitamata).

(13) Käesolevas määruses osutatud juurutaja mõistet tuleks tõlgendada kui tehisintellektisüsteemi kasutavat mis tahes füüsilist või juriidilist isikut, sealhulgas avaliku sektori asutust, ametit või muud organit, kelle volitusel süsteemi kasutatakse, välja arvatud juhul, kui tehisintellektisüsteemi kasutatakse isikliku, mitte kutselise tegevuse jaoks. Olenevalt tehisintellektisüsteemi tüübist võib süsteemi kasutamine mõjutada lisaks juurutajale ka muid isikuid.

(14) Käesolevas määruses kasutatavat biomeetriliste andmete mõistet tuleks tõlgendada lähtudes määruse (EL) 2016/679 artikli 4 punktis 14, määruse (EL) 2018/1725 artikli 3 punktis 18 ja direktiivi (EL) 2016/680 artikli 3 punktis 13 määratletud biomeetriliste andmete mõistest. Biomeetrilised andmed võivad võimaldada füüsiliste isikute autentimist, tuvastamist või liigitamist ning füüsiliste isikute emotsioonide tuvastamist.

(15) Käesolevas määruses osutatud biomeetrilise tuvastamise mõiste tuleks määratleda kui inimeste füüsiliste, füsioloogiliste ja käitumuslike tunnuste, nagu nägu, silmade liikumine, kehakuju, hääl, prosoodia, kõnnak, kehahoiak, südame löögisagedus, vererõhk, lõhn, klahvivajutuste erijooned, automaatseks tuvastamiseks isiku isikusamasuse kindlakstegemise eesmärgil, võrreldes selle isiku biomeetrilisi andmeid isikute võrdlusandmebaasi salvestatud biomeetriliste andmetega, sõltumata sellest, kas isik on andnud selleks nõusoleku või mitte. See ei hõlma tehisintellektisüsteeme, mis on ette nähtud biomeetriliseks kontrolliks, kaasa arvatud autentimiseks, mille ainus eesmärk on kinnitada, et konkreetne füüsiline isik on see, kes ta väidab end olevat, ning füüsilise isiku isikusamasuse kinnitamiseks üksnes selleks, et saada juurdepääs teenusele, avada seade või saada juurdepääsuluba ruumidesse sisenemiseks.

(16) Käesolevas määruses osutatud biomeetrilise liigitamise mõiste tuleks määratleda kui füüsiliste isikute jagamine teatud kategooriatesse nende biomeetriliste andmete alusel. Kõnealused konkreetsed kategooriad võivad olla seotud selliste aspektidega nagu sugu, vanus, juuksevärv, silmade värv, tätoveeringud, käitumine või isikuomadused, keel, usk, rahvusvähemusse kuulumine, seksuaalne või poliitiline sättumus. See ei hõlma biomeetrilise liigitamise süsteeme, mis on puhtalt lisafunktsioonid, mis on lahutamatult seotud teise äriteenusega, mis tähendab, et seda funktsiooni ei saa objektiivsetel tehnilistel põhjustel kasutada ilma põhiteenuseta ning selle funktsiooni või funktsioonistiku integreerimine ei ole vahend käesoleva määruse normide kohaldamisest kõrvalehoidmiseks. Sellised lisafunktsioonid võivad olla näiteks internetipõhistes kauplemiskohtades kasutatavad filtrid näojoonte või kehaehituse liigitamiseks, kuna neid saab kasutada ainult seoses põhiteenusega, mis seisneb toote müümises sellisel viisil, mis võimaldab tarbijal toote virtuaalset proovimist enda peal ja aidates selle abil tarbijal teha ostuotsust. Lisafunktsiooniks võib pidada ka veebipõhistes sotsiaalvõrgustike teenustes kasutatavaid filtreid, millega liigitatakse näojooned või kehaehitus, et võimaldada kasutajatel lisada või muuta pilte või videoid, kuna sellist filtrit ei saa kasutada ilma sotsiaalvõrgustiku teenuste põhiteenuseta, mis seisneb veebisisu jagamises.

(17) Käesolevas määruses osutatud biomeetrilise kaugtuvastamise süsteemi mõiste tuleks määratleda funktsioonidest lähtuvalt kui tehisintellektisüsteem, mis on mõeldud füüsiliste isikute tuvastamiseks ilma nende aktiivse osaluseta, tavaliselt eemalt, võrreldes isiku biomeetrilisi andmeid võrdlusandmebaasis 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 füüsiliste isikute tuvastamist ilma nende aktiivse osaluseta. See ei hõlma tehisintellektisüsteeme, mis on ette nähtud biomeetriliseks kontrolliks, kaasa arvatud autentimiseks, mille ainus eesmärk on kinnitada, et konkreetne füüsiline isik on see, kes ta väidab end olevat, ning füüsilise isiku isikusamasuse kinnitamiseks üksnes selleks, et saada juurdepääs teenusele, avada seade või saada juurdepääsuluba ruumidesse sisenemiseks. Kõnealune väljajätmine on põhjendatud asjaoluga, et sellistel süsteemidel on tõenäoliselt väike mõju füüsiliste isikute põhiõigustele võrreldes selliste biomeetrilise kaugtuvastamise süsteemidega, mida võidakse kasutada suure hulga isikute biomeetriliste andmete töötlemiseks ilma nende aktiivse osaluseta. Reaalajaliste süsteemide puhul toimub nii biomeetriliste andmete hõive, võrdlemine kui ka isikutuvastus koheselt, peaaegu koheselt või igal juhul ilma märkimisväärse viivituseta. Siinjuures ei tohiks jääda võimalust hoida väikeste viivituste kasutamisega kõrvale käesoleva määruse sätetest, mis käsitlevad asjaomaste tehisintellektisüsteemide 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 isikutuvastus toimub alles pärast olulist viivitust. Sealjuures kasutatakse sellist materjali nagu videovalvesüsteemi või isikliku seadmega tehtud pildid või videosalvestised, mis on tehtud enne, kui süsteemi konkreetse füüsilise isiku puhul kasutatakse.

(18) Käesolevas määruses osutatud emotsioonituvastussüsteemi mõiste tuleks määratleda kui tehisintellektisüsteem, mille eesmärk on tuvastada või tuletada füüsiliste isikute emotsioone või kavatsusi nende biomeetriliste andmete põhjal. Selle mõistega viidatakse sellistele emotsioonidele või kavatsustele nagu õnnetunne, kurbus, viha, üllatus, vastikus, piinlikkus, elevus, häbi, põlgus, rahulolu ja lõbustatus. See ei hõlma füüsilisi seisundeid, nagu valu või väsimus, sealhulgas näiteks süsteeme, mida kasutatakse kutseliste pilootide või sõidukijuhtide väsimuse avastamiseks, et õnnetusi ära hoida. See ei hõlma ka pelgalt kergesti arusaadavate ilmete, žestide või liigutuste kindlakstegemist, välja arvatud juhul, kui neid kasutatakse emotsioonide tuvastamiseks või tuletamiseks. Nimetatud ilmed võivad olla tavalised näoilmed, näiteks kulmukortsutus või naeratus, või žestid, nagu käte- või pealiigutused, või isiku hääle erijooned, näiteks vali hääl või sosistamine.

(19) Käesoleva määruse kohaldamisel tuleks avalikult juurdepääsetava ruumina käsitada mis tahes füüsilist ruumi, mis on määratlemata arvu füüsiliste isikute jaoks juurdepääsetav, olenemata sellest, kas kõnealune ruum on era- või avalik-õiguslikus omandis, olenemata tegevusest, mille jaoks ruumi 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. Ruumi tuleks liigitada ka avalikult juurdepääsetavaks, kui olenemata võimalikest mahtuvus- või turvapiirangutest sõltub juurdepääs teatud eelmääratletud tingimustest, mida saab täita määratlemata arv isikuid, näiteks pääsme või sõidupileti ostmine, eelnev registreerimine või isikute teatav vanus. Seevastu ei tohiks ruumi 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 ruumi suhtes asjaomaseid volitusi omava isiku selge tahteavalduse alusel. Ainuüksi juurdepääsu faktiline võimalus, näiteks lukustamata uks, avatud aiavärav, ei tähenda, et ruum on avalikult juurdepääsetav, kui on olemas vastupidisele viitavad tähised või asjaolud, näiteks juurdepääsu keelavad või piiravad märgid. Ettevõtete ja tehaste ruumid ning kontorid ja töökohad, millele on juurdepääs ainult asjaomastel töötajatel ja teenuseosutajatel, on ruumid, mis ei ole avalikult juurdepääsetavad. Avalikult juurdepääsetavate ruumide hulka ei tohiks kuuluda vanglad ega piirikontrolliala. Mõned muud ruumid võivad koosneda nii avalikult juurdepääsetavatest kui ka avalikult mitte juurdepääsetavatest ruumidest, näiteks eraomandis oleva eluhoone koridor, mille kaudu on vaja minna arstikabinetti, 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 asjaomase olukorra iseärasusi.

(20) Selleks et saada tehisintellektisüsteemidest võimalikult suur kasu, kaitstes samal ajal põhiõigusi, tervist ja ohutust, ning võimaldada demokraatlikku kontrolli, peaks tehisintellektipädevus andma pakkujatele, juurutajatele ja mõjutatud isikutele vajalikud mõisted tehisintellektisüsteemide kohta teadlike otsuste tegemiseks. Nimetatud mõisted võivad asjaomase konteksti poolest erineda ja võivad hõlmata arusaamist tehniliste elementide nõuetekohasest kohaldamisest tehisintellektisüsteemi arendusetapis, selle kasutamisel kohaldatavaid meetmeid, sobivaid viise tehisintellektisüsteemi väljundi tõlgendamiseks ja mõjutatud isikute puhul teadmisi, mis on vajalikud, et mõista, kuidas tehisintellekti abil tehtud otsused neid mõjutavad. Käesoleva määruse kohaldamisel peaks tehisintellektipädevus andma kõigile tehisintellekti väärtusahela asjaomastele osalejatele vajalikud teadmised, et tagada määruse asjakohane järgimine ja selle korrektne jõustamine. Lisaks võib tehisintellektipädevusega seotud meetmete laialdane rakendamine ja asjakohaste järelmeetmete kehtestamine aidata parandada töötingimusi ning lõppkokkuvõttes toetada usaldusväärse tehisintellekti konsolideerimist ja innovatsiooni liidus. Euroopa tehisintellekti nõukoda (edaspidi „nõukoda“) peaks toetama komisjoni, et edendada tehisintellektipädevusega seotud vahendeid, üldsuse teadlikkust ja arusaamist tehisintellektisüsteemide kasutamisega seotud kasust, riskidest, kaitsemeetmetest, õigustest ja kohustustest. Komisjon ja liikmesriigid peaksid koostöös asjaomaste sidusrühmadega hõlbustama vabatahtlike käitumisjuhendite koostamist, et edendada tehisintellektipädevust tehisintellekti arendamise, käitamise ja kasutamisega tegelevate isikute seas.

(21) Selleks et tagada võrdsed tingimused ning üksikisikute õiguste ja vabaduste tõhus kaitse kogu liidus, tuleks käesoleva määrusega kehtestatud õigusnorme kohaldada tehisintellektisüsteemide pakkujate suhtes mittediskrimineerival viisil, olenemata sellest, kas nad on asutatud liidus või mõnes kolmandas riigis, ja liidus asutatud tehisintellektisüsteemide juurutajate suhtes.

(22) Kuna tehisintellektisüsteemid on digitaalsed, peaksid teatavad tehisintellektisüsteemid kuuluma käesoleva määruse kohaldamisalasse isegi siis, kui neid ei ole liidus turule lastud ega kasutusele võetud või kui neid liidus ei kasutata. See kehtib näiteks siis, kui liidus asutatud operaator sõlmib kolmandas riigis asutatud operaatoriga lepingu, et see osutaks teatavaid teenuseid, mis on seotud sellise tehisintellektisüsteemi teostatava tegevusega, mida peetakse suure riskiga tehisintellektisüsteemiks. Sellisel juhul võib operaatori kolmandas riigis 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 asutatud pakkujate ja juurutajate suhtes niivõrd, kuivõrd nende süsteemide genereeritud väljundit kavatsetakse liidus kasutada.

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 koostöö või selliste rahvusvaheliste lepingute alusel, mis on liidu või riigi tasandil sõlmitud liidu või liikmesriikidega tehtava õiguskaitse- ja õigusalase koostöö kohta, tingimusel et asjaomane kolmas riik või rahvusvaheline organisatsioon pakub piisavaid kaitsemeetmeid üksikisikute põhiõiguste ja -vabaduste kaitseks. Vajaduse korral võib see hõlmata selliste üksuste tegevust, kellele kolmandad riigid on usaldanud konkreetsete ülesannete täitmise sellise õiguskaitse- ja õigusalase koostöö toetamiseks. Selliseid koostööraamistikke või lepinguid on sõlmitud kahepoolselt liikmesriikide ja kolmandate riikide vahel, aga ka Euroopa Liidu, Europoli ja muude liidu asutuste ning kolmandate riikide ja rahvusvaheliste organisatsioonide vahel. Pädevad asutused, kes vastutavad käesoleva määruse alusel õiguskaitse- ja õigusasutuste järelevalve eest, peaksid hindama, kas need koostööraamistikud või rahvusvahelised lepingud sisaldavad piisavaid kaitsemeetmeid üksikisikute põhiõiguste ja -vabaduste kaitseks. Vastuvõtvad riiklikud ametiasutused ning liidu institutsioonid, organid ja asutused, kes selliseid väljundeid liidus kasutavad, vastutavad selle tagamise eest, et väljundite 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.

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

(24) 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 sellest, mis liiki üksus neid tegevusi teostab, näiteks kas tegemist on avalik-õigusliku või eraõigusliku üksusega. 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 riigisiseste 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 tehisintellektisüsteemi muul kui sõjalisel, kaitse- või riikliku julgeoleku eesmärgil, tagama tehisintellektisüsteemi 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, nimelt sõjalisel, kaitse- või riikliku julgeoleku eesmärgil, ja ühel või mitmel määruse kohaldamisalasse kuuluval eesmärgil, näiteks tsiviileesmärgil või õiguskaitse eesmärgil, 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 sellest, mis liiki üksus seda tegevust teostab – võimalust kasutada tehisintellektisüsteeme riikliku julgeoleku, sõjalisel ja kaitseotstarbel, mis on käesoleva määruse kohaldamisalast välja jäetud. Tsiviileesmärgil või õiguskaitse eesmärgil turule lastud tehisintellektisüsteem, mida kasutatakse muudetud või muutmata kujul sõjalisel, kaitse- või riikliku julgeoleku eesmärgil, ei peaks kuuluma käesoleva määruse kohaldamisalasse, olenemata sellest, mis liiki üksus seda tegevust teostab.

(25) Käesolev määrus peaks toetama innovatsiooni, peaks austama teadusvabadust ega tohiks kahjustada teadus- ja arendustegevust. Seepärast on vaja jätta selle kohaldamisalast välja tehisintellektisüsteemid ja -mudelid, mis on spetsiaalselt välja töötatud ja kasutusele võetud üksnes teadus- ja arendustegevuse eesmärgil. Lisaks on vaja tagada, et käesolev määrus ei mõjuta muul viisil tehisintellektisüsteemide või -mudelitega seotud teadus- ja arendustegevust enne nende turule laskmist või kasutusele võtmist. Samuti ei tohiks käesoleva määruse sätteid kohaldada tehisintellektisüsteemide või -mudelite tootepõhise teadus-, testimis- ja arendustegevuse suhtes enne nende süsteemide ja mudelite kasutusele võtmist või turule laskmist. See väljajätmine ei piira käesoleva määruse järgimise kohustust, kui sellise teadus- ja arendustegevuse tulemusena lastakse turule või võetakse kasutusele käesoleva määruse kohaldamisalasse kuuluv tehisintellektisüsteem, ega tehisintellekti regulatiivliivakasti ja tegelikes tingimustes testimist käsitlevate sätete kohaldamist. Lisaks peaksid käesoleva määruse kohaldamisalasse jääma kõik muud tehisintellektisüsteemid, mida võidakse kasutada mis tahes teadus- ja arendustegevuseks, ilma et see piiraks selliste tehisintellektisüsteemide väljajätmist, mis on spetsiaalselt välja töötatud ja kasutusele võetud üksnes teadus- ja arendustegevuse eesmärgil. Teadus- ja arendustegevus peaks igal juhul toimuma kooskõlas teadusuuringute tunnustatud eetiliste ja kutsestandarditega ning see peaks toimuma kooskõlas kohaldatava liidu õigusega.

(26) 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 nende riskide intensiivsusele ja ulatusele, mida tehisintellektisüsteemid võivad põhjustada. Seepärast tuleb keelata teatavad vastuvõetamatud tehisintellekti kasutusviisid, näha ette suure riskiga tehisintellektisüsteemide suhtes kohaldatavad nõuded ja asjaomaste operaatorite kohustused ning kehtestada teatavatele tehisintellektisüsteemidele läbipaistvuskohustused.

(27) Kuigi riskipõhine lähenemisviis on proportsionaalsete ja tõhusate siduvate õigusnormide alus, on oluline meelde tuletada 2019. aasta eetikasuuniseid usaldusväärse tehisintellekti arendamiseks, mille töötas välja komisjoni määratud sõltumatu kõrgetasemeline tehisintellekti eksperdirühm. Kõrgetasemeline tehisintellekti eksperdirühm töötas nendes suunistes välja seitse mittesiduvat tehisintellekti eetikapõhimõtet, mille eesmärk on aidata tagada, et tehisintellekt on usaldusväärne ja järgib eetikanorme. Nende seitsme põhimõtte seas on: inimese toimevõime ja inimjärelevalve; tehniline töökindlus ja ohutus; privaatsus ja andmehaldus; läbipaistvus; mitmekesisus, mittediskrimineerimine ja õiglus; ühiskondlik ja keskkonnaalane heaolu ning vastutuse võtmine. Ilma et see piiraks käesoleva määruse ja mis tahes muu kohaldatava liidu õiguse õiguslikult siduvate nõuete kohaldamist, aitavad need suunised kujundada sidusat, usaldusväärset ja inimkeskset tehisintellekti kooskõlas põhiõiguste harta ja liidu alusväärtustega. Kõrgetasemelise tehisintellekti eksperdirühma suuniste kohaselt tähendab inimese toimevõime ja inimjärelevalve, et tehisintellektisüsteeme arendatakse ja kasutatakse vahendina, mis teenib inimesi, austab inimväärikust ja isiklikku sõltumatust ning toimib viisil, mille üle inimesed saavad nõuetekohaselt kontrolli ja järelevalvet teostada.

Tehniline töökindlus ja ohutus tähendab seda, et tehisintellektisüsteeme arendatakse ja kasutatakse viisil, mis tagab probleemide esinemisel nende töökindluse ning vastupidavuse katsetele muuta tehisintellektisüsteemi kasutust või toimivust nii, et kolmandad isikud saaksid neid ebaseaduslikult kasutada, ning et minimeerida soovimatut kahju. Privaatsus ja andmehaldus tähendab, et tehisintellektisüsteeme arendatakse ja kasutatakse kooskõlas privaatsus- ja andmekaitsenormidega ning andmetöötlus vastab kõrgetele kvaliteedi ja tervikluse standarditele. Läbipaistvus tähendab, et tehisintellektisüsteeme arendatakse ja kasutatakse viisil, mis võimaldab asjakohast jälgitavust ja selgitatavust, andes samal ajal inimestele teada, et nad suhtlevad tehisintellektisüsteemiga, ning teavitades juurutajaid igakülgselt selle tehisintellektisüsteemi võimetest ja piiridest ning mõjutatud isikuid nende õigustest. Mitmekesisus, mittediskrimineerimine ja õiglus tähendavad, et tehisintellektisüsteeme arendatakse ja kasutatakse viisil, mis hõlmab erinevaid osalejaid ja edendab võrdset ligipääsu, soolist võrdõiguslikkust ja kultuurilist mitmekesisust, vältides samal ajal diskrimineerivat mõju ja ebaõiglast kallutatust, mis on liidu või liikmesriikide õigusega keelatud. Ühiskondlik ja keskkonnaalane heaolu tähendab, et tehisintellektisüsteeme arendatakse ja kasutatakse kestlikul ja keskkonnasõbralikul viisil, samuti viisil, mis toob kasu kõigile inimestele, jälgides ja hinnates samal ajal pikaajalist mõju üksikisikule, ühiskonnale ning demokraatiale. Nimetatud põhimõtete kohaldamine tuleks võimaluse korral üle kanda tehisintellektimudelite projekteerimisse ja kasutamisse. Igal juhul peaksid need olema aluseks käesoleva määruse alusel koostatavatele käitumisjuhenditele. Kõiki sidusrühmi, sealhulgas tööstust, akadeemilisi ringkondi, kodanikuühiskonda ja standardiorganisatsioone, julgustatakse vabatahtlike parimate tavade ja standardite väljatöötamisel võtma vastavalt vajadusele arvesse eetikapõhimõtteid.

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

(29) Tehisintellektil põhinevaid manipuleerimistehnikaid saab kasutada selleks, et veenda inimesi käituma soovimatult ja neid petta, suunates neid tegema otsuseid, mis pärsivad ja kahjustavad nende sõltumatust, otsuste tegemist ja valikuvabadust. Teatavad tehisintellektisüsteemid, mille eesmärk või tagajärg on inimeste käitumise suurel määral moonutamine, mis võib tõenäoliselt tekitada olulist kahju, eelkõige sellist, millel on piisavalt oluline kahjulik mõju füüsilisele ja psühholoogilisele tervisele või finantshuvidele, 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 manipuleerivaid või petlikke võtteid, mis vähendavad või kahjustavad isiku sõltumatust, otsuste tegemist või vaba valikut viisil, mille puhul inimesed ei ole nendest võtetest teadlikud, või isegi kui nad on teadlikud, on võimalik nad ikka eksiteele viia või nad ei ole võimelised neid kontrollima või nendele vastu seisma. Selleks võidakse kasutada näiteks aju-arvuti liideseid või virtuaalreaalsust, kuna need võimaldavad suuremat kontrolli selle üle, milliseid stiimuleid inimestele esitatakse, kuivõrd need võivad oluliselt moonutada nende käitumist märkimisväärselt kahjulikul viisil. Lisaks võivad tehisintellektisüsteemid muul viisil kasutada ära konkreetse isiku või isikute rühma haavatavusi, mis tulenevad nende vanusest, puudest Euroopa Parlamendi ja nõukogu direktiivi (EL) 2019/882[16] tähenduses või konkreetsest sotsiaalsest või majanduslikust olukorrast, mis tõenäoliselt muudab need isikud ärakasutamise suhtes kaitsetumaks, näiteks äärmises vaesuses elavad isikud, etnilised või usuvähemused.

[16] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta direktiiv (EL) 2019/882 toodete ja teenuste ligipääsetavusnõuete kohta (ELT L 151, 7.6.2019, lk 70).

Selliseid süsteeme võidakse turule lasta, kasutusele võtta või kasutada selliselt, et nende eesmärk või tagajärg on isiku käitumise oluline moonutamine viisil, mis põhjustab või mõistliku tõenäosusega põhjustab olulist kahju sellele või mõnele teisele isikule või isikute rühmale, sealhulgas kahju, mis võib tekkida aja jooksul, ning seetõttu peaksid sellised süsteemid olema keelatud. Käitumise moonutamise kavatsust ei pruugi olla võimalik eeldada, kui moonutus tuleneb tehisintellektisüsteemi välistest teguritest, mis ei ole pakkuja või juurutaja kontrolli all, nimelt teguritest, mis ei pruugi olla mõistlikult prognoositavad ja seetõttu ei ole tehisintellektisüsteemi pakkujal või juurutajal võimalik neid leevendada. Igal juhul ei pruugi pakkujal või juurutajal olla kavatsust põhjustada olulist kahju, kui selline kahju tuleneb manipuleerivatest või ekspluateerivatest tehisintellektil põhinevatest kasutusviisidest. Selliseid tehisintellekti kasutusviise käsitlevad keelud täiendavad Euroopa Parlamendi ja nõukogu direktiivi 2005/29/EÜ[17] sätteid, eelkõige seda, et ebaausad kaubandustavad, mis põhjustavad tarbijatele majanduslikku või rahalist kahju, on igal juhul keelatud, olenemata sellest, kas need on võetud kasutusele tehisintellektisüsteemide abil või muul viisil. Käesolevas määruses sätestatud manipuleerivate ja ekspluateerivate kasutusviiside keeld ei tohiks mõjutada õiguspärast ravi, näiteks psüühikahäire psühholoogiline ravi või füüsiline rehabilitatsioon, kui see toimub kooskõlas kohaldatava õiguse ja meditsiinistandarditega, näiteks üksikisikute või nende seaduslike esindajate selgesõnalisel nõusolekul. Samuti ei tohiks tavapäraseid ja õiguspäraseid kaubandustavasid, näiteks reklaami valdkonnas, mis on kooskõlas kohaldatava õigusega, pidada iseenesest kahjulikeks manipuleerivateks tehisintellektil põhinevateks kasutusviisideks.

---

[17] Euroopa Parlamendi ja nõukogu 11. mai 2005. aasta direktiiv 2005/29/EÜ, mis käsitleb ettevõtja ja tarbija vaheliste tehingutega seotud ebaausaid kaubandustavasid siseturul ning millega muudetakse nõukogu direktiivi 84/450/EMÜ, Euroopa Parlamendi ja nõukogu direktiive 97/7/EÜ, 98/27/EÜ ja 2002/65/EÜ ning Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 2006/2004 (ebaausate kaubandustavade direktiiv) (ELT L 149, 11.6.2005, lk 22).

(30) Biomeetrilise liigitamise süsteemid, mis põhinevad füüsiliste isikute biomeetrilistel andmetel, näiteks isiku näol või sõrmejälgedel, et tuletada või järeldada isikute poliitilisi vaateid, kuulumist ametiühingusse, usulisi või filosoofilisi veendumusi, rassi, seksuaalelu või seksuaalset sättumust, tuleks keelata. See keeld ei tohiks hõlmata selliste biomeetriliste andmestike seaduslikku märgistamist, filtreerimist või liigitamist vastavalt biomeetrilistele andmetele, mis on saadud kooskõlas liidu või liikmesriigi õigusega, nagu kujutiste sorteerimist vastavalt juuksevärvile või silmavärvile, mida saab kasutada näiteks õiguskaitse valdkonnas.

(31) Tehisintellektisüsteemid, mida kasutatakse avaliku või erasektori osalejate poolt füüsilistele isikutele sotsiaalpunktide andmiseks, 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 või nende rühmi, tuginedes paljudele andmepunktidele, mis on seotud nende sotsiaalse käitumisega eri kontekstides, või teadaolevatele, tuletatavatele või prognoositavatele isiku- või iseloomuomadustele teatava aja jooksul. Selliste tehisintellektisüsteemide antud sotsiaalpunktid võivad tuua kaasa füüsilisi isikuid või terveid inimrühmi kahjustavat või nende ebasoodsat kohtlemist sotsiaalses kontekstis, mis ei ole seotud kontekstiga, kus andmed algselt loodi või koguti, või kahjustavat kohtlemist, mis ei ole nende sotsiaalse käitumise problemaatilisusega võrreldes proportsionaalne või põhjendatud. Tehisintellektisüsteemid, millega kaasnevad sellised vastuvõetamatud punktide andmise tavad ja mis viivad selliste kahjustavate või ebasoodsate tulemusteni, tuleks seetõttu keelata. See keeld ei tohiks mõjutada füüsiliste isikute seaduslikku hindamist, mida tehakse konkreetsel eesmärgil kooskõlas liidu või liikmesriigi õigusega.

(32) Tehisintellektisüsteemide kasutamine avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil reaalajas toimuva füüsiliste isikute biomeetrilise kaugtuvastamise jaoks on eriti tõsine sekkumine 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. Füüsiliste isikute biomeetrilise kaugtuvastamise jaoks mõeldud tehisintellektisüsteemide tehniline ebatäpsus võib kaasa tuua tulemuste kallutatuse ja põhjustada diskrimineerimist. Sellised võimalikud kallutatud tulemused ja diskrimineeriv mõju on eriti olulised vanuse, etnilise päritolu, rassi, soo või puuete puhul. 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.

(33) 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 teatavate kuriteoohvrite, kaasa arvatud kadunud isikute otsimine, teatavad füüsiliste isikute elu või füüsilist turvalisust ähvardavad ohud või terrorirünnaku oht ning käesoleva määruse lisas loetletud kuritegude toimepanijate või sellistes kuritegudes kahtlustatavate asukoha kindlaks tegemine või nende tuvastamine, kui sellise kuriteo eest karistatakse asjaomases liikmesriigis vabadusekaotuse või vabadust piirava julgeolekumeetmega, mille maksimaalne pikkus on vähemalt neli aastat ning vastavalt kõnealuse kuriteo määratlusele selle liikmesriigi õiguses. Sellise ajalise piiri seadmine riigisisese õiguse kohasele vabadusekaotusele või vabadust piiravale julgeolekumeetmele aitab tagada, et reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine oleks õigustatud vaid piisavalt raskete rikkumiste korral. Peale selle põhineb käesoleva määruse lisas esitatud kuritegude loetelu 32 kuriteoliigil, mis on loetletud nõukogu raamotsuses 2002/584/JSK[18], võttes arvesse, et mõned neist kuritegudest on praktikas tõenäoliselt teistest asjakohasemad, sest reaalajas toimuva biomeetrilise kaugtuvastamise kasutamise eeldatav vajalikkus ja proportsionaalsus võivad märkimisväärselt varieeruda, kui tegemist on loetelus nimetatud kuriteo toimepanija või sellises kuriteos kahtlustatava asukoha kindlaks tegemise või tema tuvastamisega ja kui võetakse arvesse võimalike negatiivsete tagajärgede raskusastme, tõenäosuse ja ulatuse tõenäolisi erinevusi.

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

Vahetu oht füüsiliste isikute elule või füüsilisele turvalisusele võib tuleneda ka Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2557[19] artikli 2 punktis 4 määratletud elutähtsa taristu tõsisest kahjustada saamisest, kui sellise elutähtsa taristu kahjustada saamine või hävimine ohustaks vahetult isiku elu või füüsilist turvalisust, sealhulgas elanikkonna esmatarbekaupadega varustamise või riigi põhiülesannete täitmise tõsise kahjustamise kaudu. 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 isikud, kes isikusamasuse kontrolli käigus kas keelduvad isiku tuvastamisest või ei suuda oma isikut avaldada või tõendada, ilma et neilt nõutaks käesoleva määruse kohaselt eelneva loa saamist. Tegemist võib olla näiteks kuriteoga seotud isikuga, isikuga, kes ei soovi või kes õnnetuse või tervisliku seisundi tõttu ei suuda avaldada oma isikut õiguskaitseasutustele.

[19] Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2557, mis käsitleb elutähtsa teenuse osutajate toimepidevust ja millega tunnistatakse kehtetuks nõukogu direktiiv 2008/114/EÜ (ELT L 333, 27.12.2022, lk 164).

(34) Lisaks sellele on nende süsteemide vastutustundliku ja proportsionaalse kasutamise tagamiseks oluline panna paika, et igaühes neist ammendavalt loetletud ja kitsalt määratletud olukorrast tuleks arvesse võtta teatavaid elemente, eeskätt mis puudutab taotluse aluseks oleva olukorra olemust ja kasutamise tagajärgi kõigi asjaomaste isikute õigustele ja vabadustele ning kasutamise korral ettenähtud kaitsemeetmeid ja tingimusi. Peale selle tuleks reaalajas toimuva biomeetrilise kaugtuvastamise süsteeme kasutada avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil üksnes selleks, et kinnitada konkreetselt sihtmärgiks oleva isiku isikusamasust, ning see peaks piirduma sellega, mis on rangelt vajalik seoses ajavahemiku ning geograafilise ja isikulise kohaldamisalaga, võttes eelkõige arvesse tõendeid või viiteid ohu, ohvrite või toimepanija kohta. Reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine avalikult juurdepääsetavas ruumis peaks olema lubatud üksnes juhul, kui asjaomane õiguskaitseasutus on viinud lõpule põhiõigustele avalduva mõju hindamise, ja kui käesolevas määruses ei ole sätestatud teisiti, on ta süsteemi andmebaasis registreerinud, nagu on sätestatud käesolevas määruses. Isikute võrdlusandmebaas peaks olema igas eespool nimetatud olukorras iga kasutusmalli jaoks sobiv.

(35) Iga kord, kui reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutatakse avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil, peaks liikmesriigi õigusasutus või sõltumatu haldusasutus, kelle otsus on siduv, andma selleks selge ja konkreetse loa. Põhimõtteliselt tuleks selline luba saada enne tehisintellektisüsteemi kasutamist isiku või isikute tuvastamiseks. Erandeid sellest reeglist tuleks lubada põhjendatud kiireloomulistes olukordades, see tähendab olukordades, kus vajadus asjaomaste süsteemide kasutamise järele on selline, et enne tehisintellektisüsteemi kasutamise algust ei ole reaalselt ega objektiivselt võimalik luba saada. Sellistes kiireloomulistes olukordades peaks tehisintellektisüsteemi kasutamine piirduma hädavajaliku miinimumiga ning selle suhtes peaksid kehtima asjakohased kaitsemeetmed ja tingimused, mis on kindlaks määratud riigisiseses õiguses ja mida õiguskaitseasutus iga individuaalse kiireloomulise kasutusjuhtumi korral täpsustab. Lisaks sellele peaks õiguskaitseasutus sellistel juhtudel kõnealust luba taotlema, põhjendades, miks ta ei saanud seda varem, põhjendamatu viivituseta ja hiljemalt 24 tunni jooksul taotleda. Kui selline luba lükatakse tagasi, tuleks selle loaga seotud reaalajas biomeetrilise tuvastamise süsteemide kasutamine viivitamata lõpetada ning kõik sellise kasutamisega seotud andmed tuleks kõrvale jätta ja kustutada. Sellised andmed hõlmavad sisendandmeid, mille tehisintellektisüsteem on sellise süsteemi kasutamise käigus vahetult saanud, ning selle loaga seotud kasutamise tulemusi ja väljundeid. See ei tohiks hõlmata sisendit, mis on saadud seaduslikult muu liidu või riigisisese õiguse kohaselt. Ühelgi juhul ei tohiks isiku suhtes kahjulikke õiguslikke tagajärgi põhjustavat otsust teha üksnes biomeetrilise kaugtuvastamise süsteemi tulemuste põhjal.

(36) Selleks et täita oma ülesandeid kooskõlas käesolevas määruses ja riigisiseses õigusnormides sätestatud nõuetega, tuleks asjaomast turujärelevalveasutust ja riiklikku andmekaitseasutust teavitada igast reaalajas toimuva biomeetrilise tuvastamise süsteemi kasutamisest. Teavitatud turujärelevalveasutused ja riiklikud andmekaitseasutused peaksid esitama komisjonile igal aastal aruande reaalajas toimunud biomeetrilise tuvastamise süsteemide kasutamise kohta.

(37) 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 asjaomane liikmesriik on otsustanud oma riigisisese 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. Sellistest riigisisestest õigusnormidest tuleks komisjonile teatada 30 päeva jooksul pärast nende vastuvõtmist.

(38) Tehisintellektisüsteemide kasutamine avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil reaalajas toimuva füüsiliste isikute biomeetrilise kaugtuvastamise jaoks eeldab igal juhul biomeetriliste andmete töötlemist. Käesoleva määruse kohaseid õigusnorme, millega keelatakse selline kasutamine teatavate eranditega ja mis põhinevad ELi toimimise lepingu artiklil 16, tuleks kohaldada direktiivi (EL) 2016/680 artiklis 10 sätestatud biomeetriliste andmete töötlemist käsitlevate õigusnormide suhtes 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 (EL) 2016/680 artikli 8 alusel. Käesolevas määruses sätestatud 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 sellise muul otstarbel kui õiguskaitse eesmärgil kasutamise puhul nõudma käesoleva määruse kohast luba ega selle loa rakendamiseks sätestatud üksikasjalike riigisiseste õigusnormide kohaldamist.

(39) 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 andmesubjekti biomeetriliste andmete töötlemine keelatud, välja arvatud nendes artiklites sätestatud piiratud eranditega. Määruse (EL) 2016/679 artikli 9 lõike 1 kohaldamisel on riiklikud andmekaitseasutused juba teinud keelava otsuse biomeetrilise kaugtuvastamise kasutamise kohta muudel kui õiguskaitse eesmärkidel.

(40) 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 käesoleva määruse artikli 5 lõike 1 esimese lõigu punktis g sätestatud normid niivõrd, kuivõrd neid kohaldatakse biomeetrilise liigitamise süsteemide kasutamise suhtes politseikoostöö ja kriminaalasjades tehtava õigusalase koostöö valdkonna tegevustes, artikli 5 lõike 1 esimese lõigu punktis d sätestatud normid niivõrd, kuivõrd neid kohaldatakse selle sättega hõlmatud tehisintellektisüsteemide kasutamise suhtes, artikli 5 lõike 1 esimese lõigu punktis h ja lõigetes 2–6 ning artikli 26 lõikes 10 kehtestatud normid, mis võeti vastu ELi toimimise lepingu artikli 16 alusel, mis käsitlevad isikuandmete töötlemist liikmesriikide poolt ELi toimimise lepingu kolmanda osa V jaotise 4. või 5. peatüki kohaldamisalasse kuuluva tegevuse puhul, 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, Iirimaa suhtes siduvad.

(41) ELi lepingule ja ELi toimimise lepingule lisatud protokolli nr 22 (Taani seisukoha kohta) artiklite 2 ja 2a kohaselt ei ole käesoleva määruse artikli 5 lõike 1 esimese lõigu punktis g sätestatud normid niivõrd, kuivõrd neid kohaldatakse biomeetrilise liigitamise süsteemide kasutamise suhtes politseikoostöö ja kriminaalasjades tehtava õigusalase koostöö valdkonna tegevustes, artikli 5 lõike 1 esimese lõigu punktis d sätestatud normid niivõrd, kuivõrd neid kohaldatakse selle sättega hõlmatud tehisintellektisüsteemide kasutamise suhtes, artikli 5 lõike 1 esimese lõigu punktis h ja lõigetes 2–6 ning artikli 26 lõikes 10 kehtestatud normid, mis võeti vastu ELi toimimise lepingu artikli 16 alusel ja mis käsitlevad isikuandmete töötlemist liikmesriikide poolt ELi toimimise lepingu kolmanda osa V jaotise 4. või 5. peatüki kohaldamisalasse kuuluva tegevuse puhul, Taani suhtes siduvad ega kohaldatavad.

(42) Kooskõlas süütuse presumptsiooniga tuleks füüsilisi isikuid liidus alati hinnata nende tegeliku käitumise põhjal. Füüsilisi isikuid ei tohiks kunagi hinnata tehisintellekti prognoosil põhineva käitumise alusel, tuginedes üksnes nende profiilianalüüsile, isikuomadustele või erijoontele, nagu rahvus, sünnikoht, elukoht, laste arv, võlatase või automark, ilma et oleks olemas põhjendatud kahtlus, et see isik on seotud kuritegeliku tegevusega, mis tugineb objektiivsetele kontrollitavatele faktidele, ja ilma inimhinnanguta. Seetõttu tuleks keelata sellised füüsiliste isikutega seotud riskihindamised, mille eesmärk on hinnata nende rikkumise tõenäosust või prognoosida tegelikku või potentsiaalset kuriteo toimepanemist üksnes nende profiilianalüüsi või tema isikuomaduste ja erijoonte hindamise alusel. Ühelgi juhul ei taheta nimetatud keeluga osutada sellisele riskianalüüsile või puudutada sellist riskianalüüsi, mis ei põhine üksikisikute profiilianalüüsil või üksikisikute isikuomadustel ja erijoontel, näiteks tehisintellektisüsteemide puhul, mis kasutavad riskianalüüsi, et hinnata ettevõtjate finantspettuse tõenäosust kahtlaste tehingute või riskianalüüsivahendite alusel, et prognoosida uimastite või ebaseaduslike kaupade tõenäolist asukohta tolli poolt, näiteks teadaolevatel salakaubaveo marsruutidel.

(43) Keelata tuleks selliste tehisintellektisüsteemide turule laskmine, kasutusele võtmine või kasutamine, mis loovad või laiendavad näotuvastuse andmebaase internetist või videovalve salvestistest näokujutiste kindla suunitluseta ekstraheerimise kaudu, kuna see kasutusviis suurendab massilise jälgimise tunnet ja võib kaasa tuua põhiõiguste, sealhulgas eraelu puutumatuse õiguse ränga rikkumise.

(44) Tõsist muret tekitab selliste tehisintellektisüsteemide teaduslik alus, mille eesmärk on tuvastada või tuletada emotsioone, eelkõige seetõttu, et emotsioonide väljendamine on kultuuride ja olukordade lõikes ning isegi ühe inimese puhul väga erinev. Selliste süsteemide peamisteks puudusteks on piiratud usaldusväärsus, spetsiifilisuse puudumine ja piiratud üldistatavus. Seetõttu võivad tehisintellektisüsteemid, mis tuvastavad või tuletavad füüsiliste isikute emotsioone või kavatsusi nende biomeetriliste andmete põhjal, viia diskrimineerivate tulemusteni ning sekkuda asjaomaste isikute õigustesse ja vabadustesse. Võttes arvesse võimu ebavõrdsust töö või hariduse kontekstis koos nende süsteemide sekkuva olemusega, võivad sellised süsteemid kaasa tuua füüsiliste isikute või nende rühmade kahjustava või ebasoodsa kohtlemise. Seetõttu tuleks keelata selliste tehisintellektisüsteemide turule laskmine, kasutusele võtmine või kasutamine, mis on ette nähtud üksikisikute emotsionaalse seisundi tuvastamiseks töökoha ja haridusega seotud olukordades. See keeld ei tohiks hõlmata tehisintellektisüsteeme, mis lastakse turule üksnes meditsiinilistel või ohutusega seotud põhjustel, näiteks terapeutiliseks kasutuseks mõeldud süsteeme.

(45) Käesolev määrus ei tohiks mõjutada kasutusviise, mis on keelatud liidu õigusega, sealhulgas andmekaitseõiguse, diskrimineerimisvastase õiguse, tarbijakaitseõiguse ja konkurentsiõiguse alusel.

(46) Suure riskiga tehisintellektisüsteeme tohiks liidus turule lasta, kasutusele võtta või kasutada 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. Uue õigusraamistiku alusel, mida on täpsustatud komisjoni 2022. aasta sinises raamatus ELi toote-eeskirjade rakendamise kohta[20], on üldreegel, et ühe toote suhtes võib olla vaja kohaldada rohkem kui ühte liidu ühtlustamiõigusakti, näiteks Euroopa Parlamendi ja nõukogu määruseid (EL) 2017/745[21] ja (EL) 2017/746[22] või Euroopa Parlamendi ja nõukogu direktiivi 2006/42/EÜ[23], kuna kättesaadavaks tegemine või kasutusele võtmine saab toimuda ainult siis, kui toode vastab kõigile kohaldatavatele liidu ühtlustamisõigusaktidele. Järjepidevuse tagamiseks ja tarbetu halduskoormuse või kulu ärahoidmiseks peaks üht või mitut suure riskiga tehisintellektisüsteemi sisaldava toote pakkujatel, mille suhtes kohaldatakse käesoleva määruse ja käesoleva määruse lisas loetletud liidu ühtlustamisõigusaktide nõudeid, olema paindlikkus operatiivsete otsuste tegemisel selle kohta, kuidas tagada üht või mitut tehisintellektisüsteemi sisaldava toote vastavus kõigile liidu ühtlustamisõigusaktidega kohaldatavatele nõuetele optimaalseimal viisil. Suure riskiga tehisintellektisüsteemideks tuleks pidada üksnes selliseid tehisintellektisüsteeme, millel on liidus oluline kahjulik mõju inimeste tervisele, turvalisusele ja põhiõigustele, ning selline piirang minimeeriks kõik võimalikud rahvusvahelise kaubanduse piirangud.

---

20 ELT C 247, 29.6.2022, lk 1.

21 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).

22 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).

23 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).

(47) Tehisintellektisüsteemid võivad kahjustada inimeste tervist ja ohutust, eriti juhul, kui sellised süsteemid on toodete turvakomponendid. Kooskõlas liidu ühtlustamisõigusaktide eesmärkidega hõlbustada toodete vaba liikumist siseturul ja tagada, et siseturule saabuvad ainult ohutud ja muul viisil nõuetele vastavad tooted, on oluline igakülgselt ära hoida ja leevendada ohutusriske, mille toode kui tervik võib põhjustada oma digitaalsete komponentide, sealhulgas 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. Samamoodi peaksid usaldusväärsed ja täpsed olema üha keerulisemad diagnostikasüsteemid ja inimeste otsuseid toetavad süsteemid tervishoiusektoris, kus on tegemist elu ja tervise seisukohast eriti oluliste otsustega.

(48) 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, õigus mittediskrimineerimisele, õigus haridusele, tarbijakaitse, töötajate õigused, puuetega inimeste õigused, sooline võrdõiguslikkus, intellektuaalomandiõigus, õigus tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele, õigus kaitsele, süütuse presumptsioon ja õigus heale haldusele. Lisaks nimetatud õigustele on oluline rõhutada asjaolu, et lastel on eriõigusi, mis on sätestatud põhiõiguste 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 poliitikameetmetega rakendatud põhiõigust kõrgetasemelisele keskkonnakaitsele.

(49) 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[24], Euroopa Parlamendi ja nõukogu määruse (EL) nr 167/2013[25], Euroopa Parlamendi ja nõukogu määruse (EL) nr 168/2013[26], Euroopa Parlamendi ja nõukogu direktiivi 2014/90/EL[27], Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/797[28],

---

24 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).

25 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).

26 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).

27 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).

28 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).

Euroopa Parlamendi ja nõukogu määruse (EL) 2018/858[29], Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1139[30] ja Euroopa Parlamendi ja nõukogu määruse (EL) 2019/2144[31] kohaldamisalasse, siis on asjakohane muuta kõnealuseid õigusakte tagamaks, et kui komisjon võtab nimetatud õigusaktide alusel 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.

---

[29] 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).

[30] 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).

[31] 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).

(50) Tehisintellektisüsteemid, mis on toodete turvakomponendid või mis on ise tooted, mis kuuluvad teatavate käesoleva määruse lisas loetletud liidu ühtlustamisõigusaktide kohaldamisalasse, on asjakohane liigitada käesoleva määruse alusel suure riskiga tehisintellektisüsteemideks, kui asjaomane toode läbib vastavushindamismenetluse kolmandast isikust vastavushindamisasutuses vastavalt asjaomastele liidu ühtlustamisõigusaktidele. Sellised tooted on eeskätt masinad, mänguasjad, liftid, plahvatusohtlikus keskkonnas kasutatavad seadmed ja kaitsesüsteemid, raadioseadmed, surveseadmed, lõbusõidulaevade varustus, köisteed, küttegaasiseadmed, meditsiiniseadmed, *in vitro* diagnostika meditsiiniseadmed, lennundus ja autotööstus.

(51) 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 määruseid (EL) 2017/745 ja (EL) 2017/746, kui keskmise ja suure riskiga toodete puhul on ette nähtud kolmanda isiku tehtav vastavushindamine.

(52) Autonoomsed tehisintellektisüsteemid, nimelt suure riskiga tehisintellektisüsteemid, mis ei ole toodete turvakomponendid või mis on ise tooted, on asjakohane liigitada suure riskiga tehisintellektisüsteemideks, kui need põhjustavad oma sihtotstarbe tõttu suure riski inimeste tervisele ja ohutusele või põhiõigustele, võttes arvesse nii võimaliku kahju raskusastet kui ka selle tekkimise tõenäosust, ja kui neid kasutatakse käesolevas määruses eelnevalt täpselt kindlaks määratud valdkondades. Nende süsteemide kindlakstegemine põhineb samadel meetoditel ja kriteeriumidel, mida on kavas kohaldada suure riskiga tehisintellektisüsteemide loetelu tulevaste võimalike muudatuste suhtes, mida komisjonil peaks olema õigus delegeeritud õigusaktidega vastu võtta, et arvestada tehnoloogia kiire arengu ja võimalikke muutustega tehisintellektisüsteemide kasutamises.

(53) Samuti on oluline selgitada, et võib esineda konkreetseid juhtumeid, kus käesolevas määruses eelnevalt kindlaksmääratud valdkondades kasutatavad tehisintellektisüsteemid ei too kaasa olulist riski nendes valdkondades kaitstavatele õiguslikele huvidele, sest need ei mõjuta oluliselt otsuste tegemist ega kahjusta neid huve oluliselt. Käesoleva määruse kohaldamisel tuleks tehisintellektisüsteemi, mis ei mõjuta oluliselt otsuste tegemise tulemust, käsitada tehisintellektisüsteemina, mis ei mõjuta inim- ega automatiseeritud otsuste tegemise sisu ja seega ka tulemust. Tehisintellektisüsteem, mis ei mõjuta oluliselt otsuste tegemise tulemust, võib hõlmata olukordi, kus on täidetud üks või mitu järgmistest tingimustest. Esimene selline tingimus peaks olema see, et tehisintellektisüsteem on ette nähtud kitsa protseduurilise ülesande täitmiseks, näiteks selline tehisintellektisüsteem, mis muudab struktureerimata andmed struktureeritud andmeteks, tehisintellektisüsteem, mis liigitab sissetulevad dokumendid kategooriatesse, või tehisintellektisüsteem, mida kasutatakse duplikaatide avastamiseks paljude avalduste seas. Need ülesanded on nii kitsad ja piiratud iseloomuga, et nendega kaasnevad vaid piiratud riskid, mida ei suurenda tehisintellektisüsteemi kasutamine kontekstis, mis on loetletud käesoleva määruse lisas suure riskiga kasutusena. Teine tingimus peaks olema see, et tehisintellektisüsteemi täidetava ülesande eesmärk on parandada varem lõpule viidud inimtegevuse tulemusi, mis võivad olla käesoleva määruse lisas loetletud suure riskiga kasutuse seisukohalt asjakohased. Kui neid omadusi silmas pidada, siis lisab tehisintellektisüsteem inimtegevusele üksnes täiendava kihi, mistõttu on risk väiksem. Seda tingimust kohaldataks näiteks tehisintellektisüsteemide suhtes, mille eesmärk on parandada varem koostatud dokumentides kasutatavat keelt, näiteks seoses tooni ametlikkuse, akadeemilise keelestiiliga või teksti vastavusse viimisega teatava kaubamärgisõnumiga. Kolmas tingimus peaks olema see, et tehisintellektisüsteem on ette nähtud otsuste tegemise mustrite või varasematest otsustusmustritest kõrvalekallete tuvastamiseks.

Risk väheneks, sest tehisintellektisüsteemi kasutamine järgneb varem lõpule viidud inimhindamisele, mida ei kavatseta asendada ega mõjutada ilma nõuetekohase inimkontrollita. Sellise tehisintellektisüsteemi alla käib näiteks see, kui õpetaja teatavat hindamismustrit arvesse võttes saab tagantjärele kontrollida, kas õpetaja võis hindamismustrist kõrvale kalduda, et võimalikele vastuoludele või kõrvalekalletele tähelepanu juhtida. Neljas tingimus peaks olema, et tehisintellektisüsteem on ette nähtud täitma ülesannet, mis üksnes valmistab ette käesoleva määruse lisas loetletud tehisintellektisüsteemidega seotud hindamist, mistõttu on süsteemi väljundi võimalik mõju seoses järgneva hindamisega seotud riskiga väga madal. See tingimus hõlmab muu hulgas arukaid lahendusi dokumentide käitlemiseks, mille seas on mitmesugused funktsioonid alates indekseerimisest, otsingust, teksti- ja kõnetöötlusest või andmete sidumisest muude andmeallikatega, või tehisintellektisüsteeme, mida kasutatakse algdokumentide tõlkimiseks. Igal juhul tuleb silmas pidada, et risk, et käesoleva määruse lisas loetletud suure riskiga kasutusega tehisintellektisüsteemid põhjustavad tervisele, turvalisusele või põhiõigustele kahju, on oluline, kui tehisintellektisüsteem hõlmab profiilianalüüsi määruse (EL) 2016/679 artikli 4 punkti 4 või direktiivi (EL) 2016/680 artikli 3 punkti 4 või määruse (EL) 2018/1725 artikli 3 punkti 5 tähenduses. Jälgitavuse ja läbipaistvuse tagamiseks peaks pakkuja, kes leiab, et tehisintellektisüsteem ei ole eespool osutatud tingimuste alusel suure riskiga, koostama enne süsteemi turule laskmist või kasutusele võtmist hindamise dokumentatsiooni ning esitama kõnealuse nõudmise korral riikide pädevatele asutustele. Selline pakkuja peaks olema kohustatud registreerima tehisintellektisüsteemi käesoleva määruse alusel loodud ELi andmebaasis. Selleks et anda täiendavaid suuniseid selliste tingimuste praktiliseks rakendamiseks, mille alusel käesoleva määruse lisas loetletud suure riskiga tehisintellektisüsteemid ei ole erandjuhul suure riskiga, peaks komisjon pärast nõukojaga konsulteerimist esitama suunised, milles täpsustatakse, et praktilisele rakendamisele lisatakse nii suure riskiga tehisintellektisüsteemide kasutusjuhtumite praktiliste näidete põhjalik loetelu kui ka selliste tehisintellektisüsteemide, mis ei ole suure riskiga, kasutusjuhtumite praktiliste näidete põhjalik loetelu.

(54) Kuna biomeetrilised andmed on isikuandmete eriliik, on asjakohane liigitada mitmed biomeetriliste süsteemide kriitilised kasutusjuhtumid kõrge riskiga kategooriateks, kui nende kasutamine on asjaomase liidu ja riigisisese õigusega lubatud. Füüsiliste isikute biomeetrilise kaugtuvastamise jaoks mõeldud tehisintellektisüsteemide tehniline ebatäpsus võib kaasa tuua tulemuste kallutatuse ja põhjustada diskrimineerimist. Kallutatud tulemuste ja diskrimineeriva mõju risk on eriti arvestatav seoses vanuse, etnilise päritolu, rassi, soo või puuetega. Võttes arvesse riske, mida biomeetrilise kaugtuvastamise süsteemid põhjustavad, tuleks need sellest lähtuvalt liigitada suure riskiga süsteemideks. Selline klassifikatsioon ei hõlma tehisintellektisüsteeme, mis on ette nähtud biomeetriliseks kontrolliks, kaasa arvatud autentimiseks, mille ainus eesmärk on kinnitada, et konkreetne füüsiline isik on isik, kes ta väidab end olevat, ning kinnitada füüsilise isiku isikusamasust üksnes selleks, et saada juurdepääs teenusele, avada seade või saada juurdepääsuluba ruumidesse sisenemiseks. Lisaks tuleks suure riskiga tehisintellektisüsteemideks liigitada tehisintellektisüsteemid, mis on ette nähtud biomeetriliseks liigitamiseks määruse (EL) 2016/679 artikli 9 lõikega 1 kaitstud tundlike atribuutide või erijoonte alusel, mis põhinevad biomeetrilistel andmetel, kui need ei ole käesoleva määrusega keelatud, ja emotsioonituvastussüsteemid, mis ei ole käesoleva määrusega keelatud. Biomeetrilisi süsteeme, mis on ette nähtud üksnes küberturvalisuse ja isikuandmete kaitse meetmete võimaldamiseks, ei tohiks pidada suure riskiga tehisintellektisüsteemideks.

(55) Elutähtsa taristu juhtimise ja käitamise osas on otstarbekas liigitada suure riskiga tehisintellektisüsteemiks need tehisintellektisüsteemid, mis on mõeldud kasutamiseks direktiivi(EL) 2022/2557 lisa punktis 8 loetletud elutähtsa digitaristu, maanteeliikluse ning vee, gaasi, kütteenergia ja elektri tarnimise korraldamise ja käitamise turvakomponentidena, sest nende rike 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 või tulekahjuhäire juhtimissüsteemid pilvandmetöötluse keskustes.

(56) Tähtis on juurutada tehisintellektisüsteeme hariduses, et edendada kvaliteetset digiõpet ja -koolitust ning võimaldada kõigil õppijatel ja õpetajatel omandada ja jagada vajalikke digioskusi ja -pädevusi, sealhulgas meediapädevust ja kriitilist mõtlemist, et osaleda aktiivselt majanduses, ühiskonnas ja demokraatlikes protsessides. Kuid tehisintellektisüsteemid, mida kasutatakse hariduses või kutseõppes, eelkõige selleks, et otsustada juurdepääs või vastuvõtmine, isikute määramine haridus- ja kutseõppeasutustesse või -programmidesse kõikidel tasanditel, hinnata isikute õpitulemusi, hinnata üksikisiku asjakohast haridustaset ja oluliselt mõjutada haridus- ja koolitustaset, mida inimestele pakutakse või millele nad saavad juurde pääseda, või jälgida ja avastada õpilaste keelatud käitumist katsete ajal, tuleks liigitada suure riskiga tehisintellektisüsteemideks, sest need võivad otsustada inimese haridusliku ja kutsealase käekäigu ning mõjutada seega selle inimese toimetulekut. Kui sellised süsteemid ei ole korrektselt projekteeritud või kui neid ei kasutata korrektselt, võivad need olla eriti sekkuvad ja rikkuda õigust haridusele ja koolitusele, aga ka õigust mitte olla diskrimineeritud, ning põlistada aegade jooksul välja kujunenud diskrimineerimismustreid, näiteks naiste, teatavate vanuserühmade, puuetega inimeste või teatava rassilise või etnilise päritoluga või seksuaalse sättumusega inimeste vastu.

(57) Suure riskiga tehisintellektisüsteemideks tuleks liigitada ka tehisintellektisüsteemid, mida kasutatakse tööhõive, töötajate juhtimise ja iseenda tööandjana tegutsemise võimaluste valdkonnas, eeskätt inimeste töölevõtmiseks ja väljavalimiseks, tööalase suhte edendamise ja tööga seotud lepingulise suhte lõpetamise tingimusi mõjutavate otsuste tegemiseks, ülesannete jagamiseks isiku käitumise või isikuomaduste või erijoonte põhjal ning tööga seotud lepingulistes suhetes olevate isikute jälgimiseks või hindamiseks, sest need süsteemid võivad märkimisväärselt mõjutada nende isikute tulevasi karjääriväljavaateid, toimetulekut ja töötajate õigusi. Asjaomased tööga seotud lepingulised suhted peaksid sisuliselt käima ka selliste töötajate ja isikute kohta, kes osutavad teenuseid platvormide kaudu, nagu on nimetatud komisjoni 2021. aasta tööprogrammis. Töölevõtmisprotsessi käigus ning tööga seotud lepingulistes suhetes olevate isikute hindamisel, edutamisel või töösuhte jätkamisel 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 selliste isikute töötulemuste ja käitumise jälgimiseks, võivad kahjustada ka nende põhiõigusi andmekaitsele ja privaatsusele.

(58) Veel üks valdkond, milles tuleks tehisintellektisüsteemide kasutamisele erilist tähelepanu pöörata, on teatavate selliste oluliste era- ja avalike teenuste ja hüvede kättesaadavus ja kasutamine, mida inimesed vajavad, et ühiskonnas täielikult osaleda või oma elatustaset parandada. Eelkõige sõltuvad kõnealustest hüvitistest ja teenustest tavaliselt füüsilised isikud, kes taotlevad või saavad ametiasutustelt esmatähtsaid avalikke hüvesid ja teenuseid, nimelt tervishoiuteenuseid, sotsiaalkindlustushüvitisi, sotsiaalteenuseid, mis pakuvad kaitset raseduse ja sünnituse, haiguse, tööõnnetuste, vanaduse ja töökaotuse korral, ning sotsiaal- ja eluasemetoetust, ning kes on vastutavate asutuste suhtes kaitsetus olukorras. Kui tehisintellektisüsteeme kasutatakse selleks, et teha kindlaks, kas ametiasutus peaks sellist toetust andma või sellist teenust osutama, sellest 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 ning seetõttu tuleks need liigitada suure riskiga süsteemideks. Samas ei tohiks käesolev määrus takistada uuenduslike lähenemisviiside väljatöötamist ja kasutamist avalikus halduses, kus oleks nõuetekohaste ja ohutute tehisintellektisüsteemide laialdasemast kasutamisest kasu tingimusel, et need süsteemid ei põhjusta juriidilistele ja füüsilistele isikutele suuri riske.

Lisaks tuleks suure riskiga tehisintellektisüsteemideks liigitada tehisintellektisüsteemid, mida kasutatakse füüsilistele isikutele krediidihinnangu andmiseks või nende krediidivõimelisuse hindamiseks, sest need määravad kindlaks inimese võimaluse saada finantsvahendeid või elutähtsaid teenuseid, nagu eluaseme-, elektri- ja telekommunikatsiooniteenused. Sel otstarbel kasutatavad tehisintellektisüsteemid võivad põhjustada inimeste või rühmade vahelist diskrimineerimist ja võivad põlistada aegade jooksul välja kujunenud diskrimineerimismustreid, mille aluseks on näiteks rassiline või etniline päritolu, sugu, puue, vanus või seksuaalne sättumus, või võivad luua uut liiki diskrimineerivat mõju. Liidu õigusega ette nähtud tehisintellektisüsteeme, mille eesmärk on avastada pettusi finantsteenuste pakkumisel või mida kasutatakse usaldatavusnõuete täitmiseks, et arvutada krediidiasutuste ja kindlustusandjate kapitalinõudeid, ei tohiks käesoleva määruse alusel siiski pidada suure riskiga süsteemideks. Lisaks võivad tehisintellektisüsteemid, mis on ette nähtud kasutamiseks füüsiliste isikutega seotud riskihindamiseks ja hinnakujunduseks tervise- ja elukindlustuses, avaldada märkimisväärset mõju inimeste toimetulekule ning see võib, kui nende projekteerimine, arendamine ja kasutamine ei ole nõuetekohane, rikkuda inimeste põhiõigusi ning põhjustada tõsiseid tagajärgi nende elule ja tervisele, sealhulgas majanduslikku tõrjutust ja diskrimineerimist. Lisaks tuleks suure riskiga tehisintellektisüsteemideks liigitada ka tehisintellektisüsteemid, mida kasutatakse füüsiliste isikute hädaabikõnede hindamiseks ja liigitamiseks või kiirabi ja päästeteenistuse, sealhulgas politsei, tuletõrje ja arstiabi väljasaatmiseks ja väljakutsete prioriseerimiseks, ning erakorralise arstiabi patsientide triaažiks, sest sellised süsteemid teevad otsuseid olukordades, mis on inimeste elu, tervise ja vara seisukohast väga kriitilised.

(59) Võttes arvesse õiguskaitseasutuste rolli ja vastutust, iseloomustab nende toiminguid, millega kaasneb tehisintellektisüsteemide teatav kasutamine, võimu väga ebavõrdne jaotumine ja selle tulemuseks võib olla füüsilise isiku jälgimine, kinnipidamine või temalt 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 toimimine, täpsus või stabiilsus ei ole piisav 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, niivõrd, kuivõrd nende kasutamine on asjaomase liidu ja riigisisese õiguse kohaselt lubatud, 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 nende toimingute olemust ja nendega seotud riske, peaksid selliste suure riskiga tehisintellektisüsteemide hulka kuuluma eeskätt need tehisintellektisüsteemid, mis on ette nähtud kasutamiseks õiguskaitseasutuste või liidu institutsioonide, organite või asutuste poolt või nimel õiguskaitseasutuste toetamiseks, et hinnata füüsilise isiku kuriteo ohvriks langemise riski, valedetektorite ja sarnaste vahenditena tõendite usaldusväärsuse hindamiseks kuritegude uurimise või nende eest vastutusele võtmise käigus; ning kui see ei ole käesoleva määrusega keelatud, siis sellise rikkumise või korduva rikkumise riski hindamiseks, mis ei põhine üksnes füüsiliste isikute profiilianalüüsil ega füüsiliste isikute või rühmade isikuomaduste, erijoonte või varasema kuritegeliku käitumise hindamisel, kuritegude avastamise, uurimise või nende eest vastutusele võtmise käigus tehtaval profiilianalüüsil. Tehisintellektisüsteeme, mis on mõeldud kasutamiseks spetsiaalselt maksuametile ja tollile haldusmenetlustes ning rahapesu andmebüroodele, kes täidavad liidu rahapesuvastase õiguse kohaseid teabe analüüsimises seisnevaid haldusülesandeid, ei tuleks liigitada suure riskiga tehisintellektisüsteemideks, mida õiguskaitseasutused kasutavad kuritegude tõkestamise, avastamise, uurimise ja nende eest vastutusele võtmise eesmärgil. Tehisintellekti vahendite kasutamine õiguskaitseasutuste ja muude asjakohaste asutuste poolt ei tohiks muutuda ebavõrdsuse või tõrjutuse teguriks. Tehisintellekti vahendite kasutamise mõju kahtlusaluste kaitseõigustele ei tohiks eirata, eelkõige raskusi sisulise teabe saamisel nende süsteemide toimimise kohta ja sellest tulenevaid raskusi nende tulemuste vaidlustamisel kohtus, eriti uurimise all olevate füüsiliste isikute poolt.

(60) Rände- ja varjupaigavaldkonnas ning piirkontrollihalduses kasutatavad tehisintellektisüsteemid mõjutavad isikuid, kes on tihtipeale eriti kaitsetus olukorras ja sõltuvad pädevate ametiasutuste 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 ette nähtud kasutamiseks rände-, varjupaiga- ja piirikontrollihaldusega tegelevatele pädevatele asutustele või nende nimel, või liidu institutsioonidele, organitele või asutustele valedetektorite ja samalaadsete vahenditena, niivõrd, kuivõrd nende kasutamine on liidu ja liikmesriigi õiguse kohaselt lubatud, et hinnata teatavaid riske, mida kujutavad endast füüsilised isikud, kes sisenevad liikmesriigi territooriumile või taotlevad viisat või varjupaika; pädevate ametiasutuste abistamiseks varjupaiga-, viisa- ja elamisloataotluste ja nendega seotud kaebuste läbivaatamisel, sealhulgas tõendite usaldusväärsuse hindamisel seoses eesmärgiga teha kindlaks sellist staatust taotlevate füüsiliste isikute vastavus tingimustele; rände-, varjupaiga- ja piirikontrollihalduse kontekstis füüsiliste isikute avastamiseks, äratundmiseks või tuvastamiseks, välja arvatud reisidokumentide kontrollimine.

Rände- ja varjupaigavaldkonna ning piirikontrollihalduse valdkonna tehisintellektisüsteemid, mis kuluvad käesoleva määruse kohaldamisalasse, peaksid vastama Euroopa Parlamendi ja nõukogu määruses (EÜ) nr 810/2009,[32] Euroopa Parlamendi ja nõukogu direktiivis 2013/32/EL[33] ja muus liidu asjaomases õiguses sätestatud asjaomastele menetlusnõuetele. Liikmesriigid või liidu institutsioonid, organid ja asutused ei tohiks mingil juhul kasutada tehisintellektisüsteeme rände-, varjupaiga- ja piirikontrollihalduse valdkonnas selleks, et kõrvale hoida oma rahvusvahelistest kohustustest, mis nad on võtnud vastavalt 28. juulil 1951 Genfis alla kirjutatud ÜRO pagulasseisundi konventsioonile, mida on muudetud 31. jaanuari 1967. aasta protokolliga. Samuti ei tohi neid kasutada mingil viisil tagasi- ja väljasaatmise lubamatuse põhimõtte rikkumiseks ega liidu territooriumile sisenemise ohutute ja tõhusate seaduslike kanalite kasutamise, sealhulgas rahvusvahelise kaitse saamise õiguse keelamiseks.

---

32 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).

33 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).

(61) 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 tegelemiseks on asjakohane liigitada suure riskiga tehisintellektisüsteemideks need tehisintellektisüsteemid, mis on ette nähtud kasutamiseks õigusasutusele või selle nimel, et abistada õigusasutusi faktide ja seadustega tutvumisel ja nende tõlgendamisel ning õiguse kohaldamisel konkreetse faktide kogumi suhtes. Tehisintellektisüsteeme, mis on ette nähtud kasutamiseks vaidluste kohtuvälise lahendamise üksustele kõnealuse menetluse jaoks, tuleks samuti pidada suure riskiga süsteemideks, kui vaidluste kohtuvälise lahendamise menetluse tulemustel on pooltele õiguslikud tagajärjed. Tehisintellekti vahendite kasutamine võib kohtunike otsustusõigust või kohtute sõltumatust toetada, kuid ei tohiks neid asendada, sest lõppotsuste tegemine peab jääma inimestele. Tehisintellektisüsteemi liigitamist suure riskiga süsteemiks ei tohiks siiski laiendada tehisintellektisüsteemidele, mis on mõeldud puhtalt halduslikeks abitegevusteks, mis ei mõjuta tegelikku õigusemõistmist konkreetsetel juhtudel, nagu kohtuotsuste, dokumentide või andmete anonüümimine või pseudonüümimine, töötajatevaheline suhtlus või haldusülesanded.

(62) Ilma et see piiraks Euroopa Parlamendi ja nõukogu määruses (EL) 2024/…[34+] sätestatud õigusnormide kohaldamist ning selleks, et käsitleda riske, mis tulenevad põhjendamatust välisest sekkumisest põhiõiguste harta artiklis 39 sätestatud hääletamisõigusesse ning kahjulikust mõjust demokraatiale ja õigusriigile, tuleks tehisintellektisüsteemid, mis on mõeldud kasutamiseks selleks, et mõjutada valimiste või referendumite tulemusi või füüsiliste isikute hääletamiskäitumist nende hääletamisel valimistel või referendumitel, liigitada suure riskiga tehisintellektisüsteemideks, välja arvatud tehisintellektisüsteemid, mille väljundiga füüsilised isikud otseselt kokku ei puutu, näiteks vahendid, mida kasutatakse poliitiliste kampaaniate korraldamiseks, optimeerimiseks ja struktureerimiseks halduslikust ja logistilisest seisukohast.

(63) Asjaolu, et tehisintellektisüsteem on käesoleva määruse alusel liigitatud suure riskiga tehisintellektisüsteemiks, ei tohiks tõlgendada nii, et selle kasutamine on seaduslik muude liidu õigusaktide või liidu õigusega kooskõlas oleva riigisisese õiguse alusel, mis käsitlevad näiteks isikuandmete kaitset, valedetektorite või samalaadsete vahendite 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 riigisisesest õigusest. Käesolevat määrust ei tohiks käsitada isikuandmete, sealhulgas asjakohasel juhul isikuandmete eriliikide töötlemise õigusliku alusena, kui käesolevas määruses ei ole sõnaselgelt ette nähtud teisiti.

---

[34] Euroopa Parlamendi ja nõukogu ... määrus (EL) 2024/... poliitreklaami läbipaistvuse ja suunamise kohta (ELT L, ..., ELI: …).

[+] ELT: palun lisada teksti dokumendis PE 90/23 (2021/0381(COD)) sisalduv määruse number ja täiendada vastavat joonealust märkust.

(64) Et maandada riske, mida põhjustavad turule lastud või kasutusele võetud suure riskiga tehisintellektisüsteemid, ning tagada kõrge usaldusväärsus, tuleks suure riskiga tehisintellektisüsteemide suhtes kohaldada teatavaid kohustuslikke nõudeid, võttes arvesse tehisintellektisüsteemi sihtotstarvet ja kasutuskonteksti ning järgides pakkuja kehtestatud riskijuhtimissüsteemi. Meetmed, mida pakkujad võtavad käesoleva määruse kohustuslike nõuete täitmiseks, peaksid võtma arvesse tehisintellekti valdkonna tehnika üldtunnustatud taset ning olema käesoleva määruse eesmärkide saavutamiseks proportsionaalsed ja tõhusad. Uue õigusraamistiku alusel, mida on täpsustatud komisjoni 2022. aasta sinises raamatus ELi toote-eeskirjade rakendamise kohta, on üldreegel, et üks või mitu liidu ühtlustamisõigusakti võivad olla kohaldatavad ühele tootele, kuna kättesaadavaks tegemine või kasutusele võtmine saab toimuda ainult siis, kui toode vastab kõigile kohaldatavatele liidu ühtlustamisõigusaktidele. Käesoleva määruse nõuete kohaldamisalasse kuuluvate tehisintellektisüsteemide ohud on seotud kehtivatest liidu ühtlustamisõigusaktidest erinevate aspektidega ning seetõttu täiendavad käesoleva määruse nõuded olemasolevaid liidu ühtlustamisõigusakte. Näiteks võivad tehisintellektisüsteemi sisaldavad masinad või meditsiiniseadmed kujutada endast riske, mida asjakohastes liidu ühtlustamisõigusaktides sätestatud olulistes tervisekaitse- ja ohutusnõuetes ei käsitleta, kuna see valdkondlik õigus ei puuduta tehisintellektisüsteemidele omaseid riske.

Seega on korraga vaja kohaldada mitut ja üksteist täiendavat õigusakti. Järjepidevuse tagamiseks ning tarbetu halduskoormuse ja tarbetute kulude ärahoidmiseks peaks üht või mitut suure riskiga tehisintellektisüsteemi sisaldava toote pakkujatel, mille suhtes kohaldatakse käesoleva määruse ja uuel õigusraamistikul põhinevate ja käesoleva määruse lisas loetletud liidu ühtlustamisõigusaktide nõudeid, olema operatiivsete otsuste tegemisel paindlikkus selles osas, kuidas tagada üht või mitut tehisintellektisüsteemi sisaldava toote vastavus kõigile liidu ühtlustamisõigusaktide kohaldatavatele nõuetele optimaalseimal viisil. Selline paindlikkus võib tähendada näiteks pakkuja otsust integreerida osa käesoleva määruse kohaselt nõutavast testimis- ja aruandlusprotsessist, teabest ja dokumentatsioonist juba olemasolevatesse dokumentidesse ja menetlustesse, mida nõutakse käesoleva määruse lisas loetletud uuel õigusraamistikul põhinevate kehtivate liidu ühtlustamisõigusaktide alusel. See ei tohiks mingil viisil kahjustada pakkuja kohustust täita kõiki kohaldatavaid nõudeid.

(65) Riskijuhtimissüsteem peaks seisnema pidevalt korduvas protsessis, mida kavandatakse ja käitatakse suure riskiga tehisintellektisüsteemi kogu elutsükli jooksul. Kõnealuse protsessi eesmärk peaks olema teha kindlaks ja maandada tehisintellektisüsteemide asjakohaseid riske tervisele, turvalisusele ja põhiõigustele. Riskijuhtimissüsteem tuleks korrapäraselt läbi vaadata ja seda ajakohastada, et tagada selle jätkuv tõhusus, samuti käesoleva määruse alusel tehtud oluliste otsuste ja võetud meetmete põhjendused ja dokumentatsioon. See protsess peaks tagama, et pakkuja teeb kindlaks riskid või kahjuliku mõju ning rakendab maandamismeetmeid tehisintellektisüsteemide teadaolevate ja mõistlikult prognoositavate riskide suhtes tervisele, turvalisusele ja põhiõigustele, võttes arvesse nende sihtotstarvet ja mõistlikult prognoositavat väärkasutust, sealhulgas võimalikke riske, mis tulenevad tehisintellektisüsteemi ja selle töökeskkonna vastasmõjust. Riskijuhtimissüsteemis tuleks võtta tehisintellekti valdkonna tehnika taset silmas pidades kõige asjakohasemaid riskijuhtimismeetmeid. Kõige asjakohasemate riskijuhtimismeetmete kindlaksmääramisel peaks pakkuja tehtud valikud dokumenteerima ja neid selgitama ning vajaduse korral kaasama eksperte ja väliseid sidusrühmi. Suure riskiga tehisintellektisüsteemide mõistlikult prognoositava väärkasutamise kindlakstegemisel peaks pakkuja hõlmama tehisintellektisüsteemide kasutusviise, mis ei ole küll otseselt hõlmatud sihtotstarbega ega ette nähtud kasutusjuhendis, kuid mille puhul võib siiski põhjendatult eeldada, et see tuleneb kergesti prognoositavast inimkäitumisest konkreetse tehisintellektisüsteemi erijoonte ja kasutamise kontekstis. Kõik teadaolevad või prognoositavad asjaolud, mis on seotud suure riskiga tehisintellektisüsteemi kasutamisega vastavalt selle sihtotstarbele või mõistlikult prognoositava väärkasutamise tingimustes, mis võib seada ohtu tervise ja ohutuse või põhiõigused, peaksid olema lisatud kasutusjuhendisse, mille pakkuja koostab. Selle eesmärk on tagada, et juurutaja on suure riskiga tehisintellektisüsteemi kasutamisel neist teadlik ja võtab neid arvesse. Käesoleva määruse kohaste prognoositava väärkasutusega seotud riskimaandamismeetmete kindlakstegemine ja rakendamine ei tohiks nõuda pakkujalt spetsiaalseid täiendavaid suure riskiga tehisintellektisüsteemi jaoks mõeldud prognoositava väärkasutuse teemalisi treeninguid. Pakkujaid julgustatakse siiski kaaluma selliseid täiendavaid treenimismeetmeid mõistlikult prognoositava väärkasutamise leevendamiseks, kui see peaks olema vajalik ja asjakohane.

(66) Suure riskiga tehisintellektisüsteemide suhtes tuleks kohaldada riskijuhtimisega seotud nõudeid, mis puudutavad kasutatavate andmestike kvaliteeti ja asjakohasust, tehnilist dokumentatsiooni ja andmete säilitamist, läbipaistvust ja juurutajate teavitamist, inimjärelevalvet, töökindlust, täpsust ja küberturvalisust. Sellised nõuded on vajalikud, et tulemuslikult maandada riske tervisele, turvalisusele ja põhiõigustele. Kuna muud kaubandust vähem piiravad meetmed ei ole mõistlikult kättesaadavad, ei ole need piirangud põhjendamatud kaubanduspiirangud.

(67) Kvaliteetsed andmed ja juurdepääs kvaliteetsetele andmetele on struktuuri pakkumiseks ja paljude tehisintellektisüsteemide toimimise tagamiseks hädavajalik, 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. Kvaliteetsed treenimis-, valideerimis- ja testimisandmestikud eeldavad asjakohaste andmehaldus- ja juhtimistavade rakendamist. Treenimis-, valideerimis- ja testimisandmestikud, sealhulgas märgistus, peaksid olema asjakohased, piisavalt representatiivsed ning võimalikult suurel määral vigadeta ja täielikud, pidades silmas süsteemi sihtotstarvet. Selleks et hõlbustada liidu andmekaitseõiguse, näiteks määruse (EL) 2016/679 järgimist, peaksid andmehaldus- ja -juhtimistavad sisaldama isikuandmete puhul andmete kogumise algse eesmärgi läbipaistvust. Neil andmestikel peaksid olema asjakohased statistilised omadused, sealhulgas mis puudutab selliseid isikuid või isikute rühmi, kellega seoses kavatsetakse suure riskiga tehisintellektisüsteemi kasutada, pöörates erilist tähelepanu andmestike võimalike kallutatuste leevendamisele, kuna need võivad mõjutada inimeste tervist ja ohutust, avaldada negatiivset mõju põhiõigustele või põhjustada liidu õigusega keelatud diskrimineerimist, eriti kui andmeväljundid mõjutavad tulevaste toimingute sisendeid (tagasisideahelad). Kallutatus võib tuleneda näiteks aluseks olevatest andmestikest, eriti kui kasutatakse varasemaid andmeid, või see võib tekkida süsteemide rakendamisel tegelikus keskkonnas.

Tehisintellektisüsteemide abil saavutatud tulemusi võib mõjutada selline loomupärane kallutatus, mis kaldub järk-järgult suurenema ning sel viisil põlistama ja võimendama olemasolevat diskrimineerimist, eriti teatud kaitsetutesse rühmadesse, sealhulgas rassilistesse või etnilistesse rühmadesse kuuluvate isikute puhul. Nõue, et andmestikud peavad olema võimalikult suurel määral täielikud ja vigadeta, ei tohiks mõjutada eraelu puutumatuse säilitamise meetodite kasutamist tehisintellektisüsteemide arendamise ja testimise kontekstis. Eeskätt tuleks andmestikes sihtotstarbe jaoks nõutavas ulatuses võtta arvesse funktsioone, omadusi või elemente, mis iseloomustavad konkreetset geograafilist, kontekstuaalset, käitumuslikku või funktsionaalset keskkonda, kus kavatsetakse suure riskiga tehisintellektisüsteemi kasutada. Andmehaldusega seotud nõudeid saab täita, kasutades kolmandaid isikuid, kes pakuvad sertifitseeritud vastavusteenuseid, sealhulgas andmehalduse, andmestiku tervikluse ning andmete treenimise, valideerimise ja testimise tavade kontrollimist, kui on tagatud vastavus käesoleva määruse andmenõuetele.

(68) Suure riskiga tehisintellektisüsteemide arendamiseks ja hindamiseks peaks teatavatel osalejatel, näiteks pakkujatel, teada antud asutustel ja muudel asjaomastel üksustel, näiteks Euroopa 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 ühtsed Euroopa andmeruumid ning avaliku huvi nimel hõlpsam andmete jagamine ettevõtete vahel ja valitsusega on äärmiselt tähtis, et pakkuda tehisintellektisüsteemide treenimiseks, valideerimiseks ja testimiseks usaldusväärset, vastutustundlikku ja mittediskrimineerivat juurdepääsu kvaliteetsetele andmetele. Näiteks tervise valdkonnas hõlbustab Euroopa terviseandmeruum mittediskrimineerivat juurdepääsu terviseandmetele ja tehisintellekti algoritmide treenimist selliste andmestikega privaatsust tagaval, turvalisel, õigeaegsel, läbipaistval ja usaldusväärsel viisil ning asjakohase institutsioonilise juhtimise all. Asjaomased pädevad asutused, sealhulgas valdkondlikud asutused, kes pakuvad või toetavad juurdepääsu andmetele, võivad toetada ka kvaliteetsete andmete pakkumist tehisintellektisüsteemide treenimiseks, valideerimiseks ja testimiseks.

(69) Õigus eraelu puutumatusele ja isikuandmete kaitsele peab olema tagatud kogu tehisintellektisüsteemi elutsükli jooksul. Sellega seoses kohaldatakse isikuandmete töötlemisel võimalikult väheste andmete kogumise ning lõimitud ja vaikimisi andmekaitse põhimõtteid, mis on sätestatud liidu andmekaitseõiguses. Meetmed, mida pakkujad võtavad nende põhimõtete järgimise tagamiseks, võivad hõlmata mitte üksnes anonüümimist ja krüpteerimist, vaid ka sellise tehnoloogia kasutamist, mis võimaldab tuua andmetesse algoritme ja treenida tehisintellektisüsteeme ilma toor- või struktureeritud andmete pooltevahelise edastamise või kopeerimiseta, ilma et see piiraks käesolevas määruses sätestatud andmehalduse nõuete kohaldamist.

(70) Et kaitsta teiste õigust tehisintellektisüsteemide kallutatusest tuleneda võiva diskrimineerimise eest, peaksid pakkujad erandkorras ja ulatuses, mis on rangelt vajalik selleks, et tagada kallutatuse avastamine ja korrigeerimine seoses suure riskiga tehisintellektisüsteemidega, tingimusel et kohaldatakse asjakohaseid kaitsemeetmeid füüsiliste isikute põhiõiguste ja -vabaduste tagamiseks ning järgitakse kõiki käesolevas määruses sätestatud kohaldatavaid tingimusi lisaks määrustes (EL) 2016/679 ja (EL) 2018/1725 ning direktiivis (EL) 2016/680 sätestatud tingimustele, olema võimelised töötlema ka isikuandmete eriliike, mis pakuvad märkimisväärset avalikku huvi määruse (EL) 2016/679 artikli 9 lõike 2 punkti g ja määruse (EL) 2018/1725 artikli 10 lõike 2 punkti g tähenduses.

(71) Arusaadav teave selle kohta, kuidas suure riskiga tehisintellektisüsteemid on välja töötatud ja kuidas need kogu oma eluea jooksul töötavad, on äärmiselt oluline, et võimaldada nende süsteemide jälgitavust, kontrollida vastavust käesoleva määruse kohastele nõuetele ning jälgida nende toiminguid ja teha turustamisjärgset seiret. Selleks on vaja säilitada andmeid ja tagada sellise tehnilise dokumentatsiooni kättesaadavus, mis sisaldab teavet, mida on vaja, et hinnata, kas tehisintellektisüsteem vastab asjakohastele nõuetele, ja hõlbustada turustamisjärgset seiret. Sellise teabe hulka peaksid kuuluma süsteemi üldised omadused, võimed ja piirid, algoritmid, andmed, kasutatud treenimis-, testimis- ja valideerimisprotsessid ning dokumentatsioon asjaomase riskijuhtimissüsteemi kohta ning see peaks olema koostatud selgel ja ammendaval viisil. Tehniline dokumentatsioon peaks olema nõuetekohaselt ajakohane kogu tehisintellektisüsteemi eluea jooksul. Lisaks peaksid suure riskiga tehisintellektisüsteemid võimaldama tehniliselt sündmuste automaatset registreerimist, kasutades selleks logisid, süsteemi kogu eluea jooksul.

(72) Selleks et lahendada probleeme, mis on seotud teatavate tehisintellektisüsteemide läbipaistmatuse ja keerukusega, ning aidata juurutajatel täita käesolevast määrusest tulenevaid kohustusi, tuleks suure riskiga tehisintellektisüsteemide puhul enne nende turule laskmist või kasutusele võtmist nõuda nende läbipaistvust. Suure riskiga tehisintellektisüsteemid tuleks projekteerida viisil, mis võimaldab juurutajatel mõista, kuidas tehisintellektisüsteem toimib, hinnata selle funktsionaalsust ning mõista selle tugevaid külgi ja piire. Suure riskiga tehisintellektisüsteemidega peaks kaasnema asjakohane teave kasutusjuhendi kujul. Selline teave peaks hõlmama tehisintellektisüsteemi omadusi, võimeid ja toimimispiire. Need peaksid hõlmama teavet suure riskiga tehisintellektisüsteemi kasutamisega seotud võimalike teadaolevate ja prognoositavate asjaolude kohta, sealhulgas juurutaja tegevuse kohta, mis võib mõjutada süsteemi käitumist ja toimimist, mille puhul tehisintellektisüsteem võib põhjustada riske tervisele, turvalisusele ja põhiõigustele, muutuste kohta, mille pakkuja on eelnevalt kindlaks määranud ja mille vastavust hinnanud, ning asjakohaste inimjärelevalve meetmete kohta, sealhulgas meetmete kohta, millega hõlbustatakse tehisintellektisüsteemi väljundite tõlgendamist juurutajate poolt. Läbipaistvus, sealhulgas lisatud kasutusjuhendid, peaks aitama juurutajaid süsteemi kasutamisel ja toetama nende teadlike otsuste tegemist. Juurutajad peaksid muu hulgas olema paremas olukorras, et teha õige valik süsteemi osas, mida nad kavatsevad kasutada, võttes arvesse nende suhtes kohaldatavaid kohustusi, olema teadlikud kavandatud ja välistatud kasutusviisidest ning kasutama tehisintellektisüsteemi õigesti ja vastavalt vajadusele. Selleks et parandada kasutusjuhendis sisalduva teabe loetavust ja kättesaadavust, tuleks vajaduse korral lisada selgitavad näited, näiteks tehisintellektisüsteemi piiride ning kavandatud ja välistatud kasutusviiside kohta. Pakkujad peaksid tagama, et kogu dokumentatsioon, sealhulgas kasutusjuhendid, sisaldab sisukat, põhjalikku, kättesaadavat ja arusaadavat teavet, võttes arvesse sihtjuurutajate vajadusi ja prognoositavaid teadmisi. Kasutusjuhendid tuleks teha kättesaadavaks asjaomase liikmesriigi poolt kindlaks määratud keeles, mis on sihtjuurutajatele kergesti arusaadav.

(73) Suure riskiga tehisintellektisüsteeme tuleks projekteerida ja arendada nii, et füüsilised isikud saaksid jälgida nende toimimist, tagada, et neid kasutatakse ettenähtud viisil ja et nende mõju käsitletakse süsteemi elutsükli jooksul. 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 tegevuspiirangud, mida süsteem ise ei saa eirata, et süsteem reageerib inimoperaatori käskudele ning et järelevalvega tegelema määratud füüsilistel isiktel on selle ülesande täitmiseks vajalik pädevus, väljaõpe ja volitused. Samuti on hädavajalik tagada, kui see on asjakohane, et suure riskiga tehisintellektisüsteemid sisaldavad mehhanisme, mille abil suunata ja teavitada füüsilist isikut, kellele on määratud inimjärelevalve ülesanne, tegema teadlikke otsuseid, kas, millal ja kuidas sekkuda, et hoida ära negatiivseid tagajärgi või riske või süsteem peatada, kui see ei toimi ettenähtud viisil. Võttes arvesse märkimisväärseid tagajärgi isikutele, kui teatavad biomeetrilise tuvastamise süsteemid annavad valesid tulemusi, on asjakohane näha nende süsteemide puhul ette tõhusama inimjärelevalve nõue, et juurutaja 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. Võttes arvesse õiguskaitse, rände, piirikontrolli ja varjupaiga valdkonna eripära, ei tohiks seda nõuet kohaldada, kui liidu või liikmesriigi õiguses peetakse selle nõude kohaldamist ebaproportsionaalseks.

(74) Suure riskiga tehisintellektisüsteemid peaksid toimima kogu oma elutsükli jooksul järjepidevalt ning nende täpsus, stabiilsus ja küberturvalisus peaks nende sihtotstarvet arvesse võttes olema asjakohasel tasemel vastavalt tehnika üldtunnustatud tasemele. Komisjoni ning asjaomaseid organisatsioone ja sidusrühmi julgustatakse võtma nõuetekohaselt arvesse tehisintellektisüsteemi riskide maandamist ja nende negatiivset mõju. Toimimise parameetrite eeldatav tase tuleks deklareerida süsteemiga kaasas olevas kasutusjuhendis. Pakkujaid kutsutakse üles edastama see teave juurutajatele selgel ja kergesti arusadaval viisil, hoidudes vääritimõistmistest ja eksitavatest väidetest. Legaalmetroloogiat käsitleva liidu õiguse, sealhulgas Euroopa Parlamendi ja nõukogu direktiivide 2014/31/EL[35] ja 2014/32/EL[36] eesmärk on tagada mõõtmiste täpsus ning aidata kaasa äritehingute läbipaistvusele ja aususele. Sellega seoses peaks komisjon koostöös asjaomaste sidusrühmade ja organisatsioonidega, nagu metroloogia- ja võrdlusuuringuasutused, soodustama, kui see on asjakohane, tehisintellektisüsteemide võrdlusaluste ja mõõtmismeetodite väljatöötamist. Seda tehes peaks komisjon võtma teadmiseks rahvusvahelised partnerid, kes tegelevad metroloogia ja tehisintellektiga seotud asjakohaste mõõtmisnäitajatega, ja tegema nendega koostööd.

---

35 Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/31/EL mitteautomaatkaalude turul kättesaadavaks tegemist käsitlevate liikmesriikide õigusaktide ühtlustamise kohta (ELT L 96, 29.3.2014, lk 107).

36 Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/32/EL mõõtevahendite turul kättesaadavaks tegemist käsitlevate liikmesriikide õigusaktide ühtlustamise kohta (ELT L 096, 29.3.2014, lk 149).

(75) 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 (näiteks vead, rikked, ebakõlad, ootamatud olukorrad). Seepärast tuleks võtta tehnilisi ja korralduslikke meetmeid, et tagada suure riskiga tehisintellektisüsteemide stabiilsus, näiteks projekteerides ja arendades asjakohaseid tehnilisi lahendusi kahjuliku või muul viisil soovimatu käitumise ennetamiseks või minimeerimiseks. Nende tehniliste lahenduste seas võivad näiteks olla mehhanismid, mis võimaldavad süsteemil oma töö ohutult katkestada (tõrkekindluse plaanid) teatavate kõrvalekallete esinemisel või juhul, kui käitamine toimub väljaspool teatavaid eelnevalt kindlaks määratud piire. Nende riskide eest kaitsmata jätmine võib mõjutada ohutust või kahjustada põhiõigusi näiteks ekslike otsuste või tehisintellektisüsteemi loodud ekslike või kallutatud väljundite tõttu.

(76) Küberturvalisusel on oluline roll, et tagada tehisintellektisüsteemide vastupanuvõime pahatahtlike kolmandate isikute katsetele muuta süsteemi nõrku kohti ära kasutades süsteemi kasutust, käitumist või toimimist või kahjustada selle turvaomadusi. Tehisintellektisüsteemide vastu suunatud küberrünnetes võidakse ära kasutada tehisintellektispetsiifilisi ressursse, näiteks treeningandmestikke (näiteks andmemürgitus) või treenitud mudeleid (näiteks vastandründed (*adversarial attacks*) või liikmesuse järeldamine), või tehisintellektisüsteemi digivarade või IKT alustaristu nõrkusi. Seega peaksid suure riskiga tehisintellektisüsteemide pakkujad võtma riskidele vastava küberturvalisuse taseme tagamiseks sobivaid meetmeid, näiteks kehtestama turvakontrollid, võttes samuti asjakohasel juhul arvesse IKT alustaristut.

(77) Ilma et see piiraks käesolevas määruses sätestatud stabiilsuse ja täpsuse nõuete kohaldamist, võivad suure riskiga tehisintellektisüsteemid, mis kuuluvad Euroopa Parlamendi ja nõukogu määruse, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid kohaldamisalasse, tõendada kooskõlas kõnealuse määrusega vastavust käesoleva määruse küberturvalisuse nõuetele, täites kõnealuses määruses sätestatud olulisi küberturvalisuse nõudeid. Kui suure riskiga tehisintellektisüsteemid vastavad Euroopa Parlamendi ja nõukogu määruse, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid olulistele nõuetele, tuleks neid käsitada käesolevas määruses sätestatud küberturvalisuse nõuetele vastavana, kui nende nõuete täitmist tõendatakse kõnealuse määruse alusel väljastatud ELi vastavusdeklaratsioonis või selle osades. Sel eesmärgil tuleks küberturvalisuse riskide hindamisel, mis on seotud digielemente sisaldava tootega, mis on käesoleva määruse kohaselt liigitatud suure riskiga tehisintellektisüsteemiks, ja mis viiakse läbi Euroopa Parlamendi ja nõukogu määruse, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid alusel, võtta arvesse riske tehisintellektisüsteemi kübervastupidavusvõimele seoses volitamata kolmandate isikute katsetega muuta selle kasutust, käitumist või toimimist, sealhulgas tehisintellektile iseloomulikku nõrkusi, nagu andmemürgitus või vastandründed, ning kui see on asjakohane, riske põhiõigustele, nagu on käesolevas määruses nõutud.

(78) Käesolevas määruses sätestatud vastavushindamismenetlust tuleks kohaldada Euroopa Parlamendi ja nõukogu määruse, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid, kohaldamisalasse kuuluva ja käesoleva määruse alusel suure riskiga tehisintellektisüsteemiks liigitatud digielemente sisaldava toote oluliste küberturvalisuse nõuete suhtes. Sellise normi tagajärjel ei tohiks siiski väheneda Euroopa Parlamendi ja nõukogu määruse, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid, kohaldamisalasse kuuluvate digielemente sisaldavate kriitilise tähtsusega toodete usaldusväärsuse vajalik tase. Seepärast, erandina sellest normist, kohaldatakse suure riskiga tehisintellektisüsteemide suhtes, mis kuuluvad käesoleva määruse kohaldamisalasse ning mis on ühtlasi liigitatud Euroopa Parlamendi ja nõukogu määruse, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid, kohaselt olulisteks ja kriitilise tähtsusega digielemente sisaldavateks toodeteks ning mille suhtes kohaldatakse käesoleva määruse lisas sätestatud sisekontrollil põhinevat vastavushindamismenetlust, Euroopa Parlamendi ja nõukogu määruse, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid, vastavushindamist käsitlevaid sätteid niivõrd, kuivõrd see on seotud kõnealuse määruse oluliste küberturvalisuse nõuetega. Sellisel juhul tuleks kõigis muudes käesoleva määrusega hõlmatud aspektides kohaldada käesoleva määruse lisas sätestatud sisekontrollil põhineva vastavushindamismenetluse vastavaid sätteid. Tuginedes Euroopa Liidu Küberturvalisuse Ameti (ENISA) küberturvalisuse poliitikaga seotud teadmistele ja oskusteabele ning ENISA-le Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/881[37] antud ülesannetele, peaks komisjon tehisintellektisüsteemide küberturvalisusega seotud küsimustes ENISAga koostööd tegema.

---

[37] 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 15).

(79) On asjakohane, 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.

(80) ÜRO puuetega inimeste õiguste konventsiooni allkirjastajatena on liit ja liikmesriigid seadusega kohustatud kaitsma puuetega inimesi diskrimineerimise eest ja edendama nende võrdõiguslikkust, tagama puuetega inimestele teistega võrdsetel alustel juurdepääsu info- ja kommunikatsioonitehnoloogiale ja -süsteemidele ning tagama puuetega inimeste eraelu puutumatuse austamise. Arvestades tehisintellektisüsteemide kasvavat tähtsust ja kasutamist, peaks universaaldisaini põhimõtete kohaldamine kõigi uute tehnoloogiate ja teenuste suhtes tagama täieliku ja võrdse juurdepääsu kõigile, keda tehisintellekti tehnoloogiad potentsiaalselt mõjutavad või kes neid kasutavad, sealhulgas puuetega inimestele, võttes täielikult arvesse nende loomupärast väärikust ja mitmekesisust. Seepärast on oluline, et pakkujad järgiksid täielikult ligipääsetavusnõudeid, sealhulgas Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/2102[38] ja direktiivi (EL) 2019/882. Pakkujad peaksid tagama, et need nõuetelevastavuse kohustused on integreeritud. Seepärast tuleks vajalikud meetmed integreerida võimalikult suures ulatuses suure riskiga tehisintellektisüsteemi projekteerimisse.

[38] Euroopa Parlamendi ja nõukogu 26. oktoobri 2016. aasta direktiiv (EL) 2016/2102, mis käsitleb avaliku sektori asutuste veebisaitide ja mobiilirakenduste juurdepääsetavust (ELT L 327, 2.12.2016, lk 1).

(81) Pakkuja peaks kehtestama usaldusväärse kvaliteedijuhtimissüsteemi, tagama nõutava vastavushindamismenetluse teostamise, koostama asjakohase dokumentatsiooni ja kehtestama stabiilse turustamisjärgse seire süsteemi. Suure riskiga tehisintellektisüsteemide pakkujatel, kelle suhtes kohaldatakse asjaomase valdkondliku liidu õiguse alusel kvaliteedijuhtimissüsteeme käsitlevaid kohustusi, peaks olema võimalus lisada käesoleva määrusega ette nähtud kvaliteedijuhtimissüsteemi elemendid juba kehtivasse kvaliteedijuhtimissüsteemi, mis oli ette nähtud kõnealuse muu valdkondliku liidu õigusega. Käesoleva määruse ja kehtiva liidu valdkondliku õiguse vastastikust täiendavust tuleks arvesse võtta ka tulevases standardimistegevuses või komisjoni vastuvõetavates suunistes. Ametiasutused, 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 ametiasutuse pädevust ja töökorraldust.

(82) Et võimaldada käesoleva määruse täitmine ja luua operaatoritele võrdsed tingimused, võttes sealjuures arvesse digitoodete kättesaadavaks tegemise eri vorme, on oluline tagada, et liidus asutatud isik saab igas olukorras esitada ametiasutustele kogu vajaliku teabe tehisintellektisüsteemi nõuetele vastavuse kohta. Seepärast peaks kolmandas riigis asutatud pakkuja enne oma süsteemide liidu turul kättesaadavaks tegemist määrama kirjaliku volitusega liidus asutatud volitatud esindaja. Pakkujate puhul, kes ei ole asutatud liidus, on sellel volitatud esindajal esmatähtis roll selliste pakkujate poolt liidus turule lastud või kasutusele võetud suure riskiga tehisintellektisüsteemide nõuetele vastavuse tagamisel ja nende liidus asutatud kontaktisikuna tegutsemisel.

(83) Võttes arvesse tehisintellektisüsteemide väärtusahela laadi ja keerukust ning kooskõlas uue õigusraamistikuga, on oluline tagada õiguskindlus ja hõlbustada käesoleva määruse järgimist. Seepärast on vaja selgitada asjaomaste ettevõtjate, näiteks importijate ja turustajate, kes võivad aidata kaasa tehisintellektisüsteemide arendamisele, rolli ja konkreetseid kohustusi kogu selles väärtusahelas. 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.

(84) Õiguskindluse tagamiseks on oluline selgitada, et teatavatel konkreetsetel tingimustel tuleks iga turustajat, importijat, juurutajat või muud kolmandat isikut käsitada suure riskiga tehisintellektisüsteemi pakkujana ning tal peaksid seega olema kõik asjaomased kohustused. See hõlmaks selliseid juhtumeid, kui nimetatud isik lisab oma nime või kaubamärgi juba turule lastud või kasutusele võetud suure riskiga tehisintellektisüsteemile, ilma et see piiraks selliste lepinguliste kokkulepete kohaldamist, milles sätestatakse, et kohustused jaotatakse muul viisil. See hõlmaks ka selliseid juhtumeid, kui see isik muudab oluliselt suure riskiga tehisintellektisüsteemi, mis on juba turule lastud või juba kasutusele võetud, ja nii, et see jääb suure riskiga tehisintellektisüsteemiks kooskõlas käesoleva määrusega, või kui ta muudab sellise tehisintellektisüsteemi, sealhulgas üldotstarbelise tehisintellektisüsteemi sihtotstarvet, mida ei ole liigitatud suure riskiga süsteemiks ja mis on juba turule lastud või kasutusele võetud, viisil, mis muudab selle tehisintellektisüsteemi käesoleva määruse kohaselt suure riskiga tehisintellektisüsteemiks. Neid sätteid tuleks kohaldada, ilma et see piiraks selliste konkreetsemate sätete kohaldamist, mis on kehtestatud teatavates uuel õigusraamistikul põhinevates liidu ühtlustamisõigusaktides, millega koos tuleks käesolevat määrust kohaldada. Näiteks määruse (EL) 2017/745 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.

(85) Üldotstarbelisi tehisintellektisüsteeme võib kasutada eraldi suure riskiga tehisintellektisüsteemidena või muude suure riskiga tehisintellektisüsteemide komponentidena. Seepärast peaksid selliste süsteemide pakkujad nende eripära tõttu ja selleks, et tagada vastutuse õiglane jagamine kogu tehisintellekti väärtusahelas, olenemata sellest, kas teised pakkujad võivad neid kasutada eraldi suure riskiga tehisintellektisüsteemidena või suure riskiga tehisintellektisüsteemide komponentidena, ning kui käesolevas määruses ei ole sätestatud teisiti, tegema asjakohasel juhul tihedat koostööd asjaomaste suure riskiga tehisintellektisüsteemide pakkujatega, et võimaldada neil täita käesolevast määrusest tulenevaid asjakohaseid kohustusi, ja käesoleva määruse alusel loodud pädevate asutustega.

(86) Kui pakkujat, kes tehisintellektisüsteemi algselt turule laskis või kasutusele võttis, ei tuleks käesolevas määruses sätestatud tingimustel enam käsitada pakkujana käesoleva määruse tähenduses ja kui see pakkuja ei ole sõnaselgelt välistanud tehisintellektisüsteemi muutmise suure riskiga tehisintellektisüsteemiks, peaks see endine pakkuja siiski tegema tihedat koostööd ja tegema kättesaadavaks vajaliku teabe ning pakkuma mõistlikult eeldatavat tehnilist juurdepääsu ja muud abi, mida on vaja käesolevas määruses sätestatud kohustuste täitmiseks, eelkõige seoses suure riskiga tehisintellektisüsteemide vastavushindamise järgimisega.

(87) Lisaks, kui suure riskiga tehisintellektisüsteemi, mis on toote turvakomponent, mis kuulub uuel õigusraamistikul põhinevate liidu ühtlustamisõigusaktide kohaldamisalasse, ei lasta turule ega võeta kasutusele tootest eraldi, peaks nendes õigusaktides määratletud toote valmistaja täitma käesolevas määruses pakkujale kehtestatud kohustusi ja eeskätt tagama selle, et lõpptootesse sisse ehitatud tehisintellektisüsteem vastab käesoleva määruse nõuetele.

(88) Tehisintellekti väärtusahelas pakuvad mitmed osalejad sageli tehisintellektisüsteeme, vahendeid ja teenuseid, aga ka komponente või protsesse, mille pakkuja inkorporeerib tehisintellektisüsteemi erinevatel eesmärkidel, sealhulgas mudelite treenimine ja ümbertreenimine, mudelite testimine ja hindamine, integreerimine tarkvarasse või muud mudeliarenduse aspektid. Nendel osalejatel on väärtusahelas oluline roll seoses pakkujaga, kes pakub suure riskiga tehisintellektisüsteemi, millesse nende tehisintellektisüsteemid, vahendid, teenused, komponendid või protsessid on integreeritud, ning nad peaksid kirjalikul kokkuleppel andma sellele pakkujale vajalikku teavet, võimeid, tehnilist juurdepääsu ja muud abi, tuginedes tehnika üldtunnustatud tasemele, et võimaldada pakkujal täielikult täita käesolevas määruses sätestatud kohustusi, ilma et see kahjustaks nende endi intellektuaalomandi õigusi või ärisaladusi.

(89) Kolmandaid isikuid, kes teevad üldsusele kättesaadavaks vahendeid, teenuseid, protsesse või tehisintellektikomponente, mis on muud kui üldotstarbelised tehisintellektimudelid, ei peaks kohustama täitma kogu tehisintellekti väärtusahelat katvate kohustustega seotud nõudeid, eelkõige neid kasutanud või need integreerinud pakkuja puhul, kui need vahendid, teenused, protsessid või tehisintellekti komponendid tehakse kättesaadavaks vaba ja avatud lähtekoodi litsentsi alusel. Vaba ja avatud lähtekoodiga vahendite, teenuste, protsesside või tehisintellekti komponentide, mis ei ole üldotstarbelised tehisintellektimudelid, arendajaid tuleks julgustada rakendama laialdaselt kasutatavaid dokumenteerimistavasid, nagu mudeli- ja andmelehed, et kiirendada teabe jagamist tehisintellekti väärtusahelas, võimaldades liidus edendada usaldusväärseid tehisintellektisüsteeme.

(90) Komisjon võiks välja töötada ja soovitada vabatahtlikke näidis-lepingutingimusi kasutamiseks suure riskiga tehisintellektisüsteemide pakkujate ja kolmandate isikute vahel, kes pakuvad suure riskiga tehisintellektisüsteemides kasutatavaid või integreeritud vahendeid, teenuseid, komponente või protsesse, et hõlbustada koostööd kogu väärtusahelas. Vabatahtlike näidis-lepingutingimuste väljatöötamisel peaks komisjon arvesse võtma konkreetsetes sektorites või ärimudelites kohaldatavaid võimalikke lepingulisi nõudeid.

(91) Arvestades tehisintellektisüsteemide olemust ning nende kasutamisega potentsiaalselt seotud riske ohutusele ja põhiõigustele, muu hulgas vajadust tagada reaalsetes oludes tehisintellektisüsteemi toimimise nõuetekohane seire, on otstarbekas näha juurutajatele ette konkreetsed kohustused. Esmajoones peaksid juurutajad võtma asjakohaseid tehnilisi ja organisatsioonilisi meetmeid tagamaks, et nad kasutavad suure riskiga tehisintellektisüsteeme kasutusjuhendi kohaselt, ning asjakohasel juhul tuleks kehtestada teatavad muud kohustused seoses tehisintellektisüsteemide töö seire ja andmete säilitamisega. Lisaks peaksid juurutajad tagama, et isikutel, kellele on antud ülesanne rakendada käesolevas määruses sätestatud kasutusjuhendeid ja inimjärelevalvet, on vajalik pädevus, eelkõige piisav tehisintellektipädevus, ning et neid on koolitatud ja neil on volitused nende ülesannete nõuetekohaseks täitmiseks. Nimetatud kohustused ei tohiks piirata juurutajate jaoks liidu või liikmesriikide õigusest tulenevaid muid suure riskiga tehisintellektisüsteemidega seotud kohustusi.

(92) Käesolev määrus ei piira tööandjate kohustusi, mis tulenevad liidu või liikmesriigi õigusest ja tavast, sealhulgas Euroopa Parlamendi ja nõukogu direktiivist 2002/14/EÜ[39], teavitada töötajaid või nende esindajaid tehisintellektisüsteemide kasutusele võtmise või kasutamise otsustest või neid teavitada ja ära kuulata. Endiselt on vaja tagada töötajate ja nende esindajate teavitamine suure riskiga tehisintellektisüsteemide kavandatavast kasutusele võtmisest töökohal, kui ei ole täidetud muude õigusaktidega ette nähtud teavitamis- või teavitamis- ja ärakuulamiskohustuste tingimused. Lisaks on selline teabe saamise õigus täiendav ja vajalik selleks, et saavutada käesoleva määruse aluseks olev põhiõiguste kaitse eesmärk. Seepärast tuleks käesolevas määruses sätestada sellekohane teabe esitamise nõue, ilma et see mõjutaks töötajate kehtivaid õigusi.

[39] Euroopa Parlamendi ja nõukogu 11. märtsi 2002. aasta direktiiv 2002/14/EÜ, millega kehtestatakse töötajate teavitamise ja nõustamise üldraamistik Euroopa Ühenduses – (EÜT L 80, 23.3.2002, lk 29).

(93) Kuigi tehisintellektisüsteemidega seotud riskid võivad tuleneda sellest, kuidas need süsteemid on projekteeritud, võivad riskid tuleneda ka sellest, kuidas selliseid tehisintellektisüsteeme kasutatakse. Suure riskiga tehisintellektisüsteemi juurutajatel on seega oluline roll põhiõiguste kaitse tagamisel, täiendades tehisintellektisüsteemi arendamisel pakkuja kohustusi. Juurutajad saavad kõige paremini aru, kuidas suure riskiga tehisintellektisüsteemi konkreetselt kasutatakse, ja suudavad seetõttu tuvastada võimalikke olulisi riske, mida ei olnud arendusetapis ette nähtud, tehes seda tänu täpsematele teadmistele kasutamise konteksti ning tõenäoliselt mõjutatud isikute või nende rühmade kohta, kelle hulka kuuluvad kaitsetud rühmad. Käesoleva määruse lisas loetletud suure riskiga tehisintellektisüsteemide juurutajatel on samuti oluline roll füüsiliste isikute teavitamisel ning nad peaksid, kui nad teevad füüsiliste isikutega seotud otsuseid või aitavad neid otsuseid teha, kohaldataval juhul teavitama füüsilisi isikuid sellest, et nende suhtes kasutatakse suure riskiga tehisintellektisüsteemi. See teave peaks sisaldama süsteemi sihtotstarvet ja selle tehtavate otsuste liiki. Juurutaja peaks teavitama ka füüsilisi isikuid nende käesoleva määrusega sätestatud õigusest saada selgitusi. Õiguskaitse eesmärkidel kasutatavate suure riskiga tehisintellektisüsteemide puhul tuleks seda kohustust rakendada kooskõlas direktiivi (EL) 2016/680 artikliga 13.

(94) Igasugune biomeetriliste andmete töötlemine, mis on seotud tehisintellektisüsteemide kasutamisega biomeetriliseks tuvastamiseks õiguskaitse eesmärgil, peab olema kooskõlas direktiivi (EL) 2016/680 artikliga 10, mis võimaldab sellist töötlemist üksnes siis, kui see on rangelt vajalik, kui andmesubjekti õiguste ja vabaduste kaitsmiseks võetakse asjakohaseid kaitsemeetmeid, ning kui see on lubatud liidu või liikmesriigi õigusega. Sellisel kasutamisel, kui see on lubatud, tuleb järgida ka direktiivi (EL) 2016/680 artikli 4 lõikes 1 sätestatud põhimõtteid, sealhulgas seaduslikkust, õiglust ja läbipaistvust, eesmärgi piiritlemist, täpsust ja säilitamise piiranguid.

(95) Võttes arvesse tagantjärele toimuva biomeetrilise kaugtuvastamise süsteemide sekkuvat iseloomu, siis ilma et see piiraks kohaldatava liidu õiguse, eelkõige määruse (EL) 2016/679 ja direktiivi (EL) 2016/680 kohaldamist, tuleks tagantjärele toimuva biomeetrilise kaugtuvastamise süsteemide kasutamise suhtes kohaldada kaitsemeetmeid. Tagantjärele toimuva biomeetrilise tuvastamise süsteeme tuleks alati kasutada viisil, mis on proportsionaalne, õiguspärane ja rangelt vajalik ning seega sihipärane tuvastatavate isikute, asukoha ja ajalise ulatuse poolest ning põhinema seaduslikult omandatud videosalvestistest koosneval suletud andmestikul. Ühelgi juhul ei tohiks tagantjärele toimuvat biomeetrilise kaugtuvastamise süsteemi kasutada õiguskaitse raames, mis toob kaasa valimatu jälgimise. Tingimused tagantjärele toimuva biomeetrilise kaugtuvastamise läbiviimiseks ei tohiks mingil juhul olla põhjus hoiduda kõrvale reaalajas toimuva biomeetrilise kaugtuvastamise keelamise ja rangete eranditega seotud tingimustest.

(96) Selleks et tõhusalt tagada põhiõiguste kaitse, peaksid suure riskiga tehisintellektisüsteemide juurutajad, kes on avalik-õiguslikud asutused, või avalikke teenuseid osutavad eraõiguslikud üksused ja teatavaid käesoleva määruse lisas loetletud suure riskiga tehisintellektisüsteemide juurutajad, nagu pangandus- või kindlustusüksused, viima enne nende süsteemide kasutusele võtmist läbi põhiõigustele avalduva mõju hindamise. Üksikisikutele olulisi avalikke teenuseid võivad osutada ka eraõiguslikud üksused. Selliseid avalikke teenuseid osutavad eraõiguslikud üksused on seotud avalikku huvi pakkuvate ülesannetega sellistes valdkondades nagu haridus, tervishoid, sotsiaalteenused, eluase, õigusemõistmine. Põhiõigustele avalduva mõju hindamise eesmärk on, et juurutaja teeks kindlaks konkreetsed riskid nende isikute või isikute rühmade õigustele, keda need tõenäoliselt mõjutavad, ning teeb kindlaks meetmed, mida tuleb võtta nende riskide realiseerumise korral. Mõju hindamine tuleks läbi viia enne suure riskiga tehisintellektisüsteemi juurutamist ja seda tuleks ajakohastada, kui juurutaja leiab, et mõni asjakohastest teguritest on muutunud. Mõju hindamisel tuleks kindlaks teha juurutaja asjakohased protsessid, milles suure riskiga tehisintellektisüsteemi kooskõlas selle sihtotstarbega kasutatakse, ning selles tuleks kirjeldada ajavahemikku ja sagedust, mil süsteemi kavatsetakse kasutada, ning selliste füüsiliste isikute ja rühmade konkreetseid kategooriaid, keda konkreetne kasutusolukord tõenäoliselt mõjutab.

Hindamise käigus tuleks kindlaks teha ka konkreetsed nende isikute või rühmade põhiõigusi mõjutada võiva kahju riskid. Selle hindamise käigus peaks juurutaja mõju nõuetekohaseks hindamiseks võtma arvesse vajalikku teavet, sealhulgas, kuid mitte ainult, suure riskiga tehisintellektisüsteemi pakkuja kasutusjuhendis esitatud teavet. Kindlakstehtud riske silmas pidades peaksid juurutajad määrama kindlaks meetmed, mida tuleb võtta nende riskide realiseerumise korral, sealhulgas näiteks juhtimiskorra selles konkreetses kasutuskontekstis, nagu inimjärelevalve kord vastavalt kasutusjuhendile või kaebuste käsitlemise ja kahju hüvitamise menetlused, kuna need võivad konkreetsetel kasutusjuhtudel olla olulised põhiõigustega seotud riskide maandamisel. Pärast selle mõju hindamist peaks juurutaja teavitama asjaomast turujärelevalveasutust. Selleks et koguda mõju hindamiseks vajalikku asjakohast teavet, võivad suure riskiga tehisintellektisüsteemi juurutajad, eelkõige juhul, kui tehisintellektisüsteeme kasutatakse avalikus sektoris, kaasata asjaomaseid sidusrühmi, sealhulgas tehisintellektisüsteemist tõenäoliselt mõjutatud isikute rühmade esindajaid, sõltumatuid eksperte ja kodanikuühiskonna organisatsioone selliste mõju hindamiste läbiviimisesse ja riskide realiseerumise korral võetavate meetmete kavandamisse. Euroopa tehisintellektiamet (edaspidi „tehisintellektiamet“) peaks välja töötama küsimustiku vormi, et hõlbustada nõuetele vastavust ja vähendada juurutajate halduskoormust.

(97) Õiguskindluse tagamiseks tuleks üldotstarbeliste tehisintellektimudelite mõiste selgelt määratleda ja eristada tehisintellektisüsteemide mõistest. See määratlus peaks põhinema üldotstarbelise tehisintellektimudeli peamistel funktsionaalsetel omadustel, eelkõige üldisusel ja võimel täita pädevalt mitmesuguseid eri ülesandeid. Neid mudeleid treenitakse tavaliselt suurte andmehulkadega mitmesuguste meetodite abil, näiteks enesejärelevalve all toimuv õpe, juhendamata õpe ja stiimulõpe. Üldotstarbelisi tehisintellektimudeleid võib turule lasta mitmel viisil, sealhulgas raamatukogude, rakendusliideste (API), otse allalaadimise kaudu või füüsilise koopiana. Neid mudeleid võib omakorda muuta või peenhäälestada uuteks mudeliteks. Kuigi tehisintellektimudelid on tehisintellektisüsteemide olulised komponendid, ei ole need eraldiseisvad tehisintellektisüsteemid. Tehisintellektisüsteemideks saamiseks on tehisintellektimudelitele vaja lisada täiendavaid komponente, näiteks kasutajaliides. Tehisintellektimudelid on tavaliselt integreeritud tehisintellektisüsteemidesse ja moodustavad osa tehisintellektisüsteemist. Käesolevas määruses sätestatakse erinormid üldotstarbeliste tehisintellektimudelite ja süsteemseid riske kujutavate üldotstarbeliste tehisintellektimudelite kohta, mida tuleks kohaldada ka siis, kui need mudelid on integreeritud tehisintellektisüsteemi või moodustavad osa tehisintellektisüsteemist. Seda tuleks mõista nii, et üldotstarbeliste tehisintellektimudelite pakkujate kohustusi tuleks kohaldada siis, kui üldotstarbelised tehisintellektimudelid on turule lastud.

Kui üldotstarbelise tehisintellektimudeli pakkuja integreerib oma mudeli oma tehisintellektisüsteemi, mis on turul kättesaadavaks tehtud või kasutusele võetud, tuleks seda mudelit käsitada turule lastuna ja seetõttu tuleks lisaks tehisintellektisüsteemidega seotud kohustustele kohaldada jätkuvalt käesolevas määruses mudelite suhtes sätestatud kohustusi. Mudelitele kehtestatud kohustusi ei peaks olema vaja kohaldada juhul, kui oma mudelit kasutatakse üksnes siseprotsessides, mis ei ole olulised toote või teenuse pakkumiseks kolmandatele isikutele, ja kui see ei mõjuta füüsiliste isikute õigusi. Võttes arvesse süsteemse riskiga üldotstarbeliste tehisintellektimudelite võimalikku märkimisväärset negatiivset mõju, tuleks nende suhtes alati kohaldada käesolevast määrusest tulenevaid asjakohaseid kohustusi. Määratlus ei tohiks hõlmata tehisintellektimudeleid, mida kasutatakse enne nende turule laskmist üksnes teadus-, arendus- ja prototüüpide loomise eesmärgil. See ei piira käesoleva määruse järgimise kohustust, kui mudel pärast sellist tegevust turule lastakse.

(98) Kui mudeli üldisust võiks muu hulgas kindlaks määrata ka parameetrite arvu alusel, siis mudeleid, millel on vähemalt miljard parameetrit ja mida on treenitud suure hulga andmetega, kasutades mastaapset enesejärelevalvet, tuleks pidada märkimisväärselt üldiseks ja pädevaks täitma mitmesuguseid erilisi ülesandeid.

(99) Suured generatiivsed tehisintellektimudelid on tüüpiline näide üldotstarbelisest tehisintellektimudelist, kuna need võimaldavad paindlikult genereerida sisu, näiteks teksti, audio, piltide või video kujul, mis suudab hõlpsasti täita mitmesuguseid eristatavaid ülesandeid.

(100) Kui üldotstarbeline tehisintellektimudel on integreeritud tehisintellektisüsteemi või on selle osa, tuleks seda süsteemi käsitada üldotstarbelise tehisintellektisüsteemina, kui see süsteem suudab tänu sellele integreerimisele täita mitmesuguseid eesmärke. Üldotstarbelist tehisintellektisüsteemi saab kasutada olemasoleval kujul või integreerida teistesse tehisintellektisüsteemidesse.

(101) Üldotstarbeliste tehisintellektimudelite pakkujatel on tehisintellekti väärtusahelas eriline roll ja vastutus, kuna nende pakutavad mudelid võivad olla aluseks mitmesugustele järgmise etapi süsteemidele, mida sageli pakuvad tootmisahela järgmise etapi pakkujad, kes vajavad mudelite ja nende võimete head mõistmist, et võimaldada selliste mudelite integreerimist oma toodetesse ning täita oma käesolevast või muudest määrustest tulenevaid kohustusi. Seepärast tuleks kehtestada proportsionaalsed läbipaistvusmeetmed, sealhulgas dokumentatsiooni koostamine ja ajakohastamine ning teabe esitamine üldotstarbelise tehisintellektimudeli kohta selle kasutamiseks järgmise etapi pakkujate poolt. Üldotstarbelise tehisintellektimudeli pakkuja peaks koostama tehnilise dokumentatsiooni ja seda ajakohastama, et teha see taotluse korral kättesaadavaks tehisintellektiametile ja riikide pädevatele asutustele. Nimetatud dokumentatsiooni lisatavad miinimumelemendid tuleks sätestada käesoleva määruse konkreetsetes lisades. Komisjonil peaks tehnoloogia arengut arvesse võttes olema õigus kõnealuseid lisasid delegeeritud õigusaktidega muuta.

(102) Tarkvara ja andmed, sealhulgas mudelid, mis on tarbimisse lubatud vaba ja avatud lähtekoodiga litsentsi alusel, mis võimaldab neid avalikult jagada ning mille puhul kasutajad saavad neile või nende muudetud versioonidele vabalt juurde pääseda, neid kasutada, muuta ja ümber jagada, võivad aidata kaasa teadusuuringutele ja innovatsioonile turul ning pakkuda liidu majandusele märkimisväärseid kasvuvõimalusi. Vaba ja avatud lähtekoodiga litsentside alusel tarbimisse lubatud üldotstarbeliste tehisintellektimudelite puhul tuleks läbipaistvuse ja avatuse kõrge tase lugeda tagatuks, kui nende parameetrid, sealhulgas kaalud, teave mudeliarhitektuuri kohta ja teave mudelite kasutamise kohta, tehakse üldsusele kättesaadavaks. Litsentsi tuleks käsitada vaba ja avatud lähtekoodiga litsentsina ka siis, kui see võimaldab kasutajatel kasutada, kopeerida, levitada, uurida, muuta ja täiustada tarkvara ja andmeid, sealhulgas mudeleid, tingimusel et mudeli algne pakkuja on nimetatud ning järgitakse identseid või võrreldavaid levitamistingimusi.

(103) Vaba ja avatud lähtekoodiga tehisintellekti komponendid hõlmavad tehisintellektisüsteemi tarkvara ja andmeid, sealhulgas mudeleid ja üldotstarbelisi tehisintellektimudeleid, vahendeid, teenuseid ja protsesse. Vaba ja avatud lähtekoodiga tehisintellekti komponente saab pakkuda eri kanalite kaudu, sealhulgas arendades neid avatud hoidlates. Käesoleva määruse kohaldamisel ei tohiks tehisintellekti komponentide suhtes, mida pakutakse tasu eest või millega teenitakse muul viisil raha, sealhulgas tehisintellekti komponendiga seotud tehnilise toe või muude teenuste pakkumise, sealhulgas tarkvaraplatvormi kaudu, või isikuandmete kasutamise kaudu muudel põhjustel kui üksnes tarkvara turvalisuse, ühilduvuse või koostalitlusvõime parandamiseks, välja arvatud mikroettevõtjate vahelised tehingud, kohaldada vaba ja avatud lähtekoodiga tehisintellekti komponentidele ette nähtud erandeid. Tehisintellekti komponentide kättesaadavaks tegemine avatud hoidlate kaudu ei tohiks iseenesest kujutada endast raha teenimist.

(104) Selliste üldotstarbeliste tehisintellektimudelite pakkujate suhtes, mis lubatakse tarbimisse vaba ja avatud lähtekoodiga litsentsi alusel ja mille parameetrid, sealhulgas kaalud, teave mudeliarhitektuuri kohta ja teave mudeli kasutamise kohta, tehakse üldsusele kättesaadavaks, tuleks kohaldada erandeid seoses läbipaistvusega seotud nõuetega, mis on kehtestatud üldotstarbelistele tehisintellektimudelitele, välja arvatud juhul, kui neid võib pidada süsteemseks riskiks, millisel juhul ei tohiks asjaolu, et mudel on läbipaistev ja sellega kaasneb avatud lähtekoodiga litsents, pidada piisavaks põhjuseks, et välistada käesolevast määrusest tulenevate kohustuste täitmine. Võttes arvesse, et üldotstarbeliste tehisintellektimudelite tarbimisse lubamine vaba ja avatud lähtekoodiga litsentsi alusel ei pruugi ilmtingimata avaldada olulist teavet mudeli treenimiseks või peenhäälestamiseks kasutatud andmestiku ega selle kohta, kuidas seeläbi tagati autoriõiguse normide järgimine, ei tohiks üldotstarbeliste tehisintellektimudelite suhtes ette nähtud erand läbipaistvusega seotud nõuete täitmisest mingil juhul puudutada kohustust koostada kokkuvõte mudeli treenimises kasutatud sisu kohta ega kohustust kehtestada liidu autoriõiguse normide järgimise põhimõtted, eelkõige selleks, et teha kindlaks Euroopa Parlamendi ja nõukogu direktiivi (EL) 2019/790[40] artikli 4 lõike 3 kohane õiguste piiramine ja seda järgida.

[40] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta direktiiv (EL) 2019/790, mis käsitleb autoriõigust ja autoriõigusega kaasnevaid õigusi digitaalsel ühtsel turul ning millega muudetakse direktiive 96/9/EÜ ja 2001/29/EÜ (ELT L 130, 17.5.2019, lk 92).

(105) Üldotstarbelised tehisintellektimudelid, eelkõige suured generatiivsed tehisintellektimudelid, mis on võimelised looma teksti, pilte ja muud sisu, pakuvad ainulaadseid innovatsioonivõimalusi, aga ka väljakutseid kunstnikele, autoritele ja teistele loovisikutele ning seoses sellega, kuidas nende loomingulist sisu luuakse, levitatakse, kasutatakse ja tarbitakse. Selliste mudelite arendamine ja treenimine nõuab juurdepääsu suurele hulgale tekstidele, piltidele, videotele ja muudele andmetele. Selles kontekstis võib sellise sisu otsimiseks ja analüüsimiseks, mis võib olla kaitstud autoriõiguse ja sellega kaasnevate õigustega, kasutada laialdaselt teksti- ja andmekaevemeetodeid. Autoriõigusega kaitstud sisu kasutamiseks on vaja asjaomase õiguste omaja luba, välja arvatud juhul, kui kohaldatakse autoriõigusega seotud erandeid ja piiranguid. Direktiiviga (EL) 2019/790 kehtestati erandid ja piirangud, millega lubatakse teatavatel tingimustel teha teksti- ja andmekaeve eesmärgil teoste või muu materjali reproduktsioone ja väljavõtteid. Nende õigusnormide kohaselt võivad õiguste omajad piirata õigusi oma teostele või muule materjalile, et hoida ära teksti- ja andmekaevet, välja arvatud juhul, kui seda tehakse teadusuuringute eesmärgil. Kui õigus loobuda on sõnaselgelt ja asjakohasel viisil väljendatud, peavad üldotstarbeliste tehisintellekti mudelite pakkujad hankima õiguste omajatelt loa, kui nad soovivad selliste teoste puhul teksti- ja andmekaevet teostada.

(106) Pakkujad, kes lasevad liidu turule üldotstarbelisi tehisintellektimudeleid, peaksid tagama käesolevas määruses sätestatud asjakohaste kohustuste täitmise. Selleks peaksid üldotstarbeliste tehisintellektimudelite pakkujad kehtestama põhimõtted autoriõigust ja sellega kaasnevaid õigusi käsitleva liidu õiguse järgimiseks, eelkõige õiguste omajate poolt direktiivi (EL) 2019/790 artikli 4 lõike 3 kohaselt sõnaselgelt väljendatud õiguste piiramise kindlakstegemiseks ja järgimiseks. Iga pakkuja, kes laseb üldotstarbelise tehisintellektimudeli liidu turule, peaks seda kohustust täitma, olenemata jurisdiktsioonist, kus nende üldotstarbeliste tehisintellektimudelite treenimise aluseks olevad autoriõigusega seotud toimingud aset leiavad. See on vajalik, et tagada üldotstarbeliste tehisintellektimudelite pakkujatele võrdsed tingimused, mille puhul ükski pakkuja ei tohiks saada liidu turul konkurentsieelist, kohaldades liidus sätestatud standarditest madalamaid autoriõiguse standardeid.

(107) Selleks et suurendada üldotstarbeliste tehisintellektimudelite, sealhulgas autoriõigusega kaitstud teksti ja andmete eeltreenimisel ja treenimisel kasutatavate andmete läbipaistvust, on asjakohane, et selliste mudelite pakkujad koostavad ja teevad üldsusele kättesaadavaks piisavalt üksikasjaliku kokkuvõtte üldotstarbelise tehisintellekti mudeli treenimiseks kasutatud sisust. Võttes nõuetekohaselt arvesse vajadust kaitsta ärisaladusi ja konfidentsiaalset äriteavet, peaks see kokkuvõte olema oma ulatuselt üldiselt terviklik, mitte tehniliselt üksikasjalik, et hõlbustada õigustatud huvidega isikutel, sealhulgas autoriõiguse omajatel, kasutada ja jõustada oma liidu õigusest tulenevaid õigusi, näiteks loetledes peamised mudelit treeninud andmekogud või andmestikud, nagu suured era- või avalikud andmebaasid või andmearhiivid, ning esitades kirjeldava selgituse muude kasutatud andmeallikate kohta. On asjakohane, et tehisintellektiamet koostaks kokkuvõtte vormi, mis peaks olema lihtne, tõhus ja võimaldama pakkujal esitada nõutava kokkuvõtte kirjeldaval kujul.

(108) Seoses üldotstarbeliste tehisintellekti mudelite pakkujatele pandud kohustusega kehtestada liidu autoriõiguse normide järgimise põhimõtted ja teha avalikult kättesaadavaks treenimiseks kasutatud sisu kokkuvõte, peaks tehisintellektiamet jälgima, kas pakkuja on need kohustused täitnud, ilma et ta kontrolliks või jätkaks treeningandmete tööpõhist hindamist seoses autoriõigusele vastavusega. Käesolev määrus ei mõjuta liidu õiguses sätestatud autoriõiguse normide täitmise tagamist.

(109) Üldotstarbeliste tehisintellekti mudelite pakkujate suhtes kohaldatavate kohustuste täitmine peaks olema vastav ja proportsionaalne mudeli pakkuja liigiga, välistades nõuete täitmise vajaduse isikute puhul, kes arendavad või kasutavad mudeleid mitteprofessionaalsel või teaduslikul eesmärgil, kuid keda tuleks siiski julgustada neid nõudeid vabatahtlikult täitma. Ilma et see piiraks liidu autoriõiguse normide kohaldamist, tuleks nimetatud kohustuste täitmisel võtta nõuetekohaselt arvesse pakkuja suurust ja võimaldada VKEdel, sealhulgas idufirmadel nõuete täitmiseks lihtsustatud viise, mis ei tohiks põhjustada ülemääraseid kulusid ega pärssida selliste mudelite kasutamist. Mudeli muutmise või peenhäälestamise korral peaksid üldotstarbeliste tehisintellektimudelite pakkuja kohustused piirduma selle muutmise või peenhäälestamisega, näiteks täiendades juba olemasolevat tehnilist dokumentatsiooni teabega muudatuste kohta, sealhulgas uute treenimisandmete allikatega, et täita käesolevas määruses sätestatud väärtusahelaga seotud kohustusi.

(110) Üldotstarbeliste tehisintellektimudelitega võivad kaasneda süsteemsed riskid, mis hõlmavad muu hulgas mis tahes tegelikku või mõistlikult prognoositavat negatiivset mõju seoses suurõnnetuste, elutähtsate sektorite häirete ning tõsiste tagajärgedega rahvatervisele ja ohutusele. mis tahes tegelikku või mõistlikult prognoositavat negatiivset mõju demokraatlikele protsessidele, avalikule ja majanduslikule julgeolekule ning ebaseadusliku, vale või diskrimineeriva sisu levitamist. Süsteemseid riske tuleks mõista nii, et need suurenevad mudeli võimete ja ulatusega, võivad tekkida mudeli kogu elutsükli jooksul ning neid mõjutavad väärkasutuse tingimused, mudeli usaldusväärsus, mudeli õiglus ja turvalisus, mudeli autonoomsuse tase, selle juurdepääs vahenditele, uudsed või kombineeritud modaalsused, tarbimisse lubamise ja levitamise strateegiad, kaitsemeetmete eemaldamise potentsiaal ja muud tegurid. Eelkõige on rahvusvahelised lähenemisviisid seni tuvastanud vajaduse pöörata tähelepanu järgmistele riskidele: riskid, mis tulenevad võimalikust tahtlikust väärkasutamisest või tahtmatutest kontrolliprobleemidest, mis tulenevad inimese tahte järgmisest; keemilised, bioloogilised, radioloogilised ja tuumaohud, näiteks viisid, kuidas vähendada sisenemise tõkkeid, sealhulgas relvade väljatöötamiseks, projekteerimiseks või kasutamiseks; küberründe võime, näiteks viisid, kuidas võimaldada haavatavuse avastamist, ärakasutamist või operatiivset kasutamist; koostoime ja vahendite kasutamise mõju, sealhulgas näiteks võime juhtida füüsilisi süsteeme ja häirida elutähtsat taristut; riskid, mis tulenevad sellest, et mudelid teevad endast koopiaid või on „isepaljunevad“ või treenivad teisi mudeleid; viisid, kuidas mudelid võivad põhjustada kahjuliku mõjuga kallutatust ja diskrimineerimist, mis võib ohustada üksikisikuid, kogukondi või ühiskonda; desinformatsiooni leviku soodustamine või eraelu puutumatuse kahjustamine, mis ohustab demokraatlikke väärtusi ja inimõigusi; risk, et konkreetne sündmus võib kaasa tuua ahelreaktsiooni, millel on märkimisväärne negatiivne mõju, mis võib mõjutada kogu linna, kogu valdkonna tegevust või tervet kogukonda.

(111) On asjakohane kehtestada metoodika üldotstarbeliste tehisintellektimudelite liigitamiseks süsteemse riskiga üldotstarbeliseks tehisintellektimudeliks. Kuna süsteemseid riske põhjustavad eriti suured võimed, tuleks üldotstarbelist tehisintellektimudelit käsitada süsteemset riski kujutavana, kui sellel on suure mõjuga võimed, mida hinnatakse asjakohaste tehniliste vahendite ja meetodite abil, või kui sellel on märkimisväärne mõju siseturule oma ulatuse tõttu. Üldotstarbelise tehisintellektimudeli suure mõjuga võimed on võimed, mis vastavad kõige arenenumates üldotstarbelistes tehisintellektimudelites registreeritud võimetele või ületavad neid. Mudeli kõiki võimeid saaks paremini mõista pärast selle turule laskmist või siis, kui juurutajad mudeliga kokku puutuvad. Vastavalt käesoleva määruse jõustumise ajal olemasolevale tehnika tasemele on üldotstarbelise tehisintellektimudeli treenimiseks kasutatud andmetöötluse kohtumaht, mida mõõdetakse ujukomatehtega, üks oluline mudeli võimete lähisväärtus. Treenimiseks kasutatud andmetöötluse kogumaht hõlmab andmetöötlust selliste tegevuste ja meetodite lõikes, mille eesmärk on mudeli võimete suurendamine enne juurutamist, näiteks eeltreenimine, sünteesitud andmete genereerimine ja peenhäälestamine. Seepärast tuleks kehtestada ujukomatehete esialgne künnis, mis juhul, kui üldotstarbeline tehisintellektimudel selle saavutab, annab alust eeldada, et mudel on süsteemse riskiga üldotstarbeline tehisintellektimudel. Seda künnist tuleks aja jooksul kohandada, et kajastada tehnoloogia ja tööstuse muutusi, nagu algoritmide paranemine või tõhusam riistvara, ning seda tuleks täiendada mudelite võimete võrdlusaluste ja näitajatega.

Sellise teabe saamiseks peaks tehisintellektiamet tegema koostööd teadusringkondade, tööstuse, kodanikuühiskonna ja muude ekspertidega. Künnised ning suure mõjuga võimete hindamise vahendid ja võrdlusalused peaksid olema üldotstarbelise tehisintellektimudeli üldisuse, selle võimete ja sellega seotud süsteemse riski kindlad prognoosijad ning need võiks võtta arvesse mudeli turule laskmise viisi või kasutajate arvu, keda see süsteem võib mõjutada. Selle süsteemi täiendamiseks peaks komisjonil olema võimalus teha üksikotsuseid, millega liigitatakse üldotstarbeline tehisintellektimudel süsteemse riskiga üldotstarbeliseks tehisintellektimudeliks, kui leitakse, et selle mudeli võimed või mõju on samaväärne sellega, mis on kehtestatud künnisega. Kõnealune otsus tuleks teha käesoleva määruse lisas sätestatud süsteemse riskiga üldotstarbeliste tehisintellektimudeli liigitamise kriteeriumide üldise hindamise alusel, milleks on näiteks treenimisandmestiku kvaliteet või maht, äri- ja lõppkasutajate arv, nende sisend- ja väljundmodaalsused, autonoomia tase ja mastabeeritavus või vahendid, millele tal on juurdepääs. Pakkuja, kelle mudel on liigitatud süsteemse riskiga üldotstarbeliseks tehisintellektimudeliks, põhjendatud taotluse korral peaks komisjon taotlust arvesse võtma ja võib otsustada uuesti hinnata, kas seda üldotstarbelist tehisintellektimudelit saab siiski pidada süsteemseid riske kujutavaks mudeliks.

(112) Samuti on vaja selgitada süsteemsete riskidega üldotstarbelise tehisintellektimudeli liigitamise menetlust. Üldotstarbelist tehisintellektimudelit, mis vastab suure mõjuga võimete suhtes kohaldatavale künnisele, tuleks käsitada süsteemse riskiga üldotstarbelise tehisintellektimudelina. Pakkuja peaks teavitama tehisintellektiametit hiljemalt kaks nädalat pärast nõuete täitmist või siis, kui on teada saadud, et üldotstarbeline tehisintellektimudel vastab eelduste aluseks olevatele nõuetele. See on eriti oluline seoses ujukomatehte künnisega, sest üldotstarbeliste tehisintellektimudelite treenimine nõuab märkimisväärset planeerimist, mis hõlmab arvutusressursside eelnevat jaotamist, ning seetõttu teavad üldotstarbeliste tehisintellektimudelite pakkujad juba enne treeningu lõppemist, kas nende mudel vastab künnisele. Seoses nimetatud teavitamisega peaks pakkuja suutma tõendada, et üldotstarbeline tehisintellektimudel ei kujuta erandkorras oma erijoonte tõttu süsteemseid riske ning seega ei tuleks seda liigitada süsteemsete riskidega üldotstarbeliseks tehisintellektimudeliks. See teave on tehisintellektiameti jaoks väärtuslik, et prognoosida süsteemsete riskidega üldotstarbeliste tehisintellektimudelite turule laskmist, ning pakkujad saavad juba varakult alustada tehisintellektiametiga suhtlemist. Kõnealune teave on eriti oluline seoses üldotstarbeliste tehisintellektimudelitega, mida kavatsetakse tarbimisse lubada avatud lähtekoodiga, arvestades et pärast avatud lähtekoodiga mudeli tarbimisse lubamist võib olla keerulisem rakendada vajalikke meetmeid, et tagada käesolevast määrusest tulenevate kohustuste täitmine.

(113) Kui komisjon saab teada, et üldotstarbeline tehisintellektimudel vastab nõuetele liigitada see süsteemse riskiga üldotstarbeliseks tehisintellektimudeliks, mida varem sellisena ei tuntud või millest asjaomane pakkuja ei olnud komisjoni teavitanud, peaks komisjonil olema õigus see nii liigitada. Kvalifitseeritud hoiatusteadete süsteem peaks tagama, et tehisintellektiamet saab lisaks oma järelevalvetegevusele ka teaduskomisjonilt teavet selliste üldotstarbeliste tehisintellektimudelite kohta, mis tuleks potentsiaalselt liigitada süsteemse riskiga üldotstarbeliseks tehisintellektimudeliks.

(114) Süsteemseid riske kujutavate üldotstarbeliste tehisintellektimudelite pakkujate suhtes tuleks lisaks üldotstarbeliste tehisintellektimudelite pakkujatele kehtestatud kohustustele kohaldada kohustusi, mille eesmärk on need riskid kindlaks teha ja neid maandada ning tagada piisav küberturvalisuse kaitse tase, olenemata sellest, kas seda mudelit pakutakse autonoomse mudelina või integreerituna tehisintellektisüsteemi või tootesse. Nende eesmärkide saavutamiseks tuleks käesoleva määrusega nõuda, et pakkujad viiksid läbi vajalikud mudelite hindamised, eelkõige enne selle esmakordset turule laskmist, sealhulgas mudelite vastandtestide läbiviimine ja nende dokumenteerimine, vajaduse korral ka sisemiste või sõltumatute välistestide abil. Lisaks peaksid süsteemse riskiga üldotstarbeliste tehisintellektimudelite pakkujad süsteemseid riske pidevalt hindama ja maandama, sealhulgas kehtestades näiteks riskijuhtimispõhimõtted, nagu vastutus- ja juhtimisprotsessid, rakendades turustamisjärgset seiret, võttes asjakohaseid meetmeid kogu mudeli elutsükli jooksul ja tehes koostööd tehisintellekti väärtusahela asjaomaste osalejatega.

(115) Süsteemse riskiga üldotstarbeliste tehisintellektimudelite pakkujad peaksid võimalikke süsteemseid riske hindama ja maandama. Kui hoolimata jõupingutustest teha kindlaks ja ennetada sellise üldotstarbelise tehisintellektimudeliga seotud riske, mis võib kujutada süsteemseid riske, põhjustab mudeli arendamine või kasutamine tõsise intsidendi, peaks üldotstarbelise tehisintellektimudeli pakkuja põhjendamatu viivituseta end intsidendiga kurssi viima ning edastama komisjonile ja riikide pädevatele asutustele kogu asjakohase teabe ja võimalikud parandusmeetmed. Lisaks peaksid pakkujad tagama mudeli ja selle füüsilise taristu piisava küberturvalisuse kaitse, kui see on asjakohane, kogu mudeli elutsükli jooksul. Pahatahtliku kasutamise või rünnetega seotud süsteemsete riskidega seotud küberturvalisuse kaitse puhul tuleks igakülgselt arvesse võtta mudeli juhuslikku leket, loata tarbimisse lubamist, turvameetmetest kõrvalehoidmist ning kaitset küberrünnete, loata juurdepääsu või mudelivarguste vastu. Seda kaitset saaks hõlbustada mudeli kaalude, algoritmide, serverite ja andmestike turvalisuse tagamisega, näiteks infoturbe talitluskindluse meetmete, konkreetsete küberturvalisuse põhimõtete, piisavate tehniliste ja väljakujunenud lahenduste ning küber- ja füüsilise juurdepääsu kontrolli kaudu, mis vastavad asjakohastele asjaoludele ja kaasnevatele riskidele.

(116) Tehisintellektiamet peaks julgustama ja hõlbustama tegevusjuhendite koostamist, läbivaatamist ja kohandamist, võttes arvesse rahvusvahelisi lähenemisviise. Osalema võiks kutsuda kõiki üldotstarbeliste tehisintellektimudelite pakkujaid. Tagamaks, et tegevusjuhendid kajastavad tehnika taset ja võtavad igakülgselt arvesse erinevaid vaatenurki, peaks tehisintellektiamet selliste juhendite koostamisel tegema koostööd asjaomaste riigi pädevate asutustega ning ta võiks vajaduse korral konsulteerida kodanikuühiskonna organisatsioonide ning muude asjaomaste sidusrühmade ja ekspertidega, sealhulgas teaduskomisjoniga. Tegevusjuhendid peaksid hõlmama üldotstarbeliste tehisintellektimudelite ja süsteemseid riske kujutavate üldotstarbeliste tehisintellektimudelite pakkujate kohustusi. Lisaks peaksid tegevusjuhendid süsteemsete riskide puhul aitama liidu tasandil kehtestada süsteemsete riskide liigi ja olemuse järgi riskitaksonoomia, mis hõlmab ka riskide allikaid. Tegevusjuhendites tuleks keskenduda ka konkreetsetele riskihindamis- ja maandamismeetmetele.

(117) Tegevusjuhendid peaksid olema keskne vahend, mis aitavad üldotstarbeliste tehisintellektimudelite pakkujatel nõuetekohaselt täita käesolevas määruses sätestatud kohustusi. Pakkujatel peaks olema võimalik tugineda tegevusjuhendile, et tõendada kohustuste täitmist. Komisjon võib rakendusaktidega otsustada kiita tegevusjuhendi heaks ja anda sellele üldise kehtivuse kogu liidus või kehtestada ühised õigusnormid asjaomaste kohustuste täitmiseks, kui käesoleva määruse kohaldamise ajaks ei saa tegevusjuhendit lõplikult vormistada või tehisintellektiamet ei pea seda piisavaks. Kui harmoneeritud standard on avaldatud ja see on hinnatud tehisintellektiameti kehtestatud asjakohaste kohustuste täitmiseks sobivaks, peaks Euroopa harmoneeritud standardi järgimine andma eelduse, et pakkujad vastavad nõuetele. Üldotstarbeliste tehisintellektimudelite pakkujad peaksid lisaks suutma tõendada nõuetele vastavust alternatiivsete asjakohaste vahendite alusel, kui tegevusjuhendid või harmoneeritud standardid ei ole kättesaadavad või kui nad otsustavad neile mitte tugineda.

(118) Käesoleva määrusega reguleeritakse tehisintellektisüsteeme ja -mudeleid, kehtestades teatavad nõuded ja kohustused asjaomastele turuosalistele, kes lasevad neid süsteeme või mudeleid liidus turule, võtavad kasutusele või kasutavad, täiendades seeläbi selliste vahendusteenuste osutajate kohustusi, kes integreerivad sellised süsteemid või mudelid oma teenustesse, mida reguleeritakse määrusega (EL) 2022/2065. Kui sellised süsteemid või mudelid on integreeritud väga suurtesse digiplatvormidesse või väga suurtesse internetipõhistesse otsingumootoritesse, kohaldatakse nende suhtes määruses (EL) 2022/2065 sätestatud riskijuhtimisraamistikku. Sellest tulenevalt tuleks eeldada, et käesoleva määruse vastavad kohustused on täidetud, välja arvatud juhul, kui tekivad märkimisväärsed süsteemsed riskid, mis ei ole hõlmatud määrusega (EL) 2022/2065, ja kui need on sellistes mudelites kindlaks tehtud. Selles raamistikus on väga suurte digiplatvormide ja väga suurte internetipõhiste otsingumootorite pakkujad kohustatud hindama võimalikke süsteemseid riske, mis tulenevad nende teenuste disainimisest, toimimisest ja kasutamisest, sealhulgas seda, kuidas teenuses kasutatavate algoritmiliste süsteemide kavandamine võib selliseid riske suurendada, samuti süsteemseid riske, mis tulenevad võimalikust väärkasutamisest. Need pakkujad on samuti kohustatud võtma asjakohaseid maandamismeetmeid, järgides põhiõigusi.

(119) Võttes arvesse liidu õiguse eri õigusaktide kohaldamisalasse jäävate digiteenuste innovatsiooni kiiret tempot ja tehnoloogilist arengut, pidades eelkõige silmas nende kasutamist ja tajumist kasutajate poolt, võib käesoleva määruse kohaldamisalasse kuuluvaid tehisintellektisüsteeme pakkuda vahendusteenustena või nende teenuste osadena määruse (EL) 2022/2065 tähenduses, mida tuleks tõlgendada tehnoloogianeutraalsel viisil. Näiteks võib tehisintellektisüsteeme kasutada internetipõhiste otsingumootorite pakkumiseks, eelkõige niivõrd, kuivõrd selline tehisintellektisüsteem nagu internetipõhine juturobot teeb otsinguid põhimõtteliselt kõigil veebisaitidel, lisab seejärel tulemused oma olemasolevatesse teadmistesse ja kasutab ajakohastatud teadmisi, et luua ühtne väljund, mis ühendab erinevaid teabeallikaid.

(120) Lisaks on määruse (EL) 2022/2065 tõhusa rakendamise hõlbustamiseks eriti asjakohased kohustused, mis on käesoleva määrusega kehtestatud teatavate tehisintellektisüsteemide pakkujatele ja juurutajatele, et võimaldada avastada ja avalikustada seda, et nende süsteemide väljundid on kunstlikult loodud või neid on manipuleeritud. See kehtib eelkõige seoses väga suurte digiplatvormide või väga suurte internetipõhiste otsingumootorite pakkujate kohustusega teha kindlaks ja maandada süsteemseid riske, mis võivad tuleneda kunstlikult loodud või manipuleeritud sisu levitamisest, eelkõige risk, et see põhjustab tegelikku või prognoositavat negatiivset mõju demokraatlikele protsessidele, ühiskondlikule arutelule ja valimisprotsessidele, sealhulgas desinformatsiooni kaudu.

(121) Oluline roll peaks olema standardimisel, et anda pakkujatele tehnilised lahendused, millega tagatakse käesoleva määruse järgimine kooskõlas tehnika tasemega, et edendada innovatsiooni ning konkurentsivõimet ja majanduskasvu ühtsel turul. Euroopa Parlamendi ja nõukogu määruse (EL) nr 1025/2012[41] artikli 2 punkti 1 alapunktis c määratletud harmoneeritud standardite – mis üldiselt peaksid kajastama tehnika taset – järgimine peaks olema pakkujate jaoks vahend, millega tõendada käesoleva määruse nõuete täitmist. Seepärast tuleks soodustada huvide tasakaalustatud esindatust, kaasates standardite väljatöötamisse kõik asjaomased sidusrühmad, eelkõige VKEd, tarbijaorganisatsioonid ning keskkonna- ja sotsiaalvaldkonna sidusrühmad, kooskõlas määruse (EL) nr 1025/2012 artiklitega 5 ja 6. Nõuete täitmise hõlbustamiseks peaks komisjon esitama standardimistaotlused põhjendamatu viivituseta. Standardimistaotluse koostamisel peaks komisjon konsulteerima nõuandva kogu ja nõukojaga, et koguda asjaomast oskusteavet. Kui aga asjakohased viited harmoneeritud standarditele puuduvad, peaks komisjonil olema võimalik rakendusaktidega ja pärast nõuandva koguga konsulteerimist kehtestada teatavate käesoleva määruse kohaste nõuete ühtsed kirjeldused.

---

[41] 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).

Ühtne kirjeldus peaks olema erakorraline varulahendus, mis hõlbustab pakkujal täita käesoleva määruse nõudeid, kui ükski Euroopa standardiorganisatsioon ei ole standardimistaotlust heaks kiitnud või kui asjakohastes harmoneeritud standardites ei ole piisavalt käsitletud põhiõigustega seotud probleeme või kui harmoneeritud standardid ei vasta taotlusele või kui asjakohase harmoneeritud standardi vastuvõtmisel esineb viivitusi. Kui harmoneeritud standardi vastuvõtmine viibib standardi tehnilise keerukuse tõttu, peaks komisjon seda enne ühtsete kirjelduste kehtestamist arvesse võtma. Ühtsete kirjelduste väljatöötamisel julgustatakse komisjoni tegema koostööd rahvusvaheliste partnerite ja rahvusvaheliste standardiorganisatsioonidega.

(122) Ilma et see piiraks harmoneeritud standardite ja ühtsete kirjelduste kasutamist, tuleks eeldada, et pakkujad, kes pakuvad suure riskiga tehisintellektisüsteemi, mida on treenitud ja testitud andmetega, mis kajastavad konkreetset geograafilist, käitumuslikku, kontekstipõhist või funktsionaalset keskkonda, milles tehisintellektisüsteemi kavatsetakse kasutada, järgivad asjakohaseid meetmeid, mis on ette nähtud käesolevas määruses sätestatud andmehalduse nõude raames. Ilma et see piiraks käesolevas määruses sätestatud stabiilsuse ja täpsuse nõuete kohaldamist, tuleks kooskõlas määruse (EL) 2019/881 artikli 54 lõikega 3 eeldada, et suure riskiga tehisintellektisüsteemid, mis on sertifitseeritud või mille kohta on välja antud vastavusdeklaratsioon kõnealuse määruse kohase küberturvalisuse sertifitseerimise kava alusel ja mille viited on avaldatud *Euroopa Liidu Teatajas*, vastavad käesoleva määruse küberturvalisuse nõudele, kui küberturvalisuse sertifikaat või vastavusdeklaratsioon või nende osad hõlmavad käesoleva määruse küberturvalisuse nõuet. See ei piira kõnealuse küberturvalisuse sertifitseerimise kava vabatahtlikku laadi.

(123) Selleks et tagada suure riskiga tehisintellektisüsteemide kõrge usaldusväärsus, peaksid need süsteemid enne nende turule laskmist või kasutuselevõtmist läbima vastavushindamise.

(124) Operaatorite koormuse vähendamiseks ja võimaliku dubleerimise vältimiseks on asjakohane hinnata uue õigusraamistiku alusel olemasolevate liidu ühtlustamisõigusaktide kohaldamisalasse kuuluvate toodetega seotud suure riskiga tehisintellektisüsteemide vastavust käesoleva määruse nõuetele osana kõnealuse õigusega juba ette nähtud vastavushindamisest. Seega ei tohiks käesoleva määruse nõuete kohaldatavus mõjutada uue liidu ühtlustamisõigusaktide kohaselt tehtava vastavushindamise eriomast loogikat, metoodikat või üldist ülesehitust.

(125) Arvestades suure riskiga tehisintellektisüsteemide keerukust ja nendega seotud riske, on oluline töötada suure riskiga tehisintellektisüsteemide jaoks välja asjakohane vastavushindamismenetlus, mis hõlmab teada antud asutusi, nn kolmanda isiku tehtavat vastavushindamist. Kuid võttes arvesse kutseliste turustamiseelsete sertifitseerijate praeguseid kogemusi tooteohutuse valdkonnas ja kaasnevate riskide erinevat olemust, on asjakohane 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 läbi viima pakkuja omal vastutusel, välja arvatud biomeetria jaoks ette nähtud tehisintellektisüsteemide puhul.

(126) Selleks et vajaduse korral viidaks läbi kolmanda isiku tehtavad vastavushindamised, peaksid riikide pädevad asutused käesoleva määruse alusel teavitama teada antud asutusi, tingimusel et need vastavad teatavatele nõuetele eeskätt sõltumatuse, pädevuse, huvide konflikti puudumise ja küberturvalisuse asjakohaste nõuete vallas. Riikide pädevad asutused peaksid saatma teavituse kõnealuste asutuste kohta komisjonile ja teistele liikmesriikidele komisjoni poolt otsuse nr 768/2008/EÜ I lisa artikli R23 alusel väljaarendatud ja hallatava elektroonilise teavitamise vahendi kaudu.

(127) Kooskõlas Maailma Kaubandusorganisatsiooni tehniliste kaubandustõkete lepingust tulenevate liidu kohustustega on asjakohane hõlbustada selliste vastavushindamistulemuste vastastikust tunnustamist, mille on saanud pädevad vastavushindamisasutused sõltumata territooriumist, kus nad on asutatud, tingimusel et kolmanda riigi õiguse alusel asutatud vastavushindamisasutused vastavad käesoleva määruse kohaldatavatele nõuetele ja liit on sõlminud sellekohase lepingu. Sellega seoses peaks komisjon aktiivselt uurima võimalike rahvusvaheliste õigusaktide koostamist sel eesmärgil ja eelkõige püüdma sõlmida vastastikuse tunnustamise lepinguid kolmandate riikidega.

(128) Liidu ühtlustamisõigusaktidega reguleeritud toodete olulise muudatuse laialdaselt juurdunud mõiste kohaselt on asjakohane, et kui tehakse muudatus, mis võib mõjutada suure riskiga tehisintellektisüsteemi vastavust käesolevale määrusele (näiteks 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, nimelt kohandavad automaatselt funktsioonide täitmise viisi, olema tegemist olulise muudatusega, tingimusel et pakkuja on kõnealused muudatused eelnevalt kindlaks määranud ja neid on vastavushindamise ajal hinnatud.

(129) Suure riskiga tehisintellektisüsteemidel peaks olema CE-märgis, mis näitab nende vastavust käesolevale määrusele, et nad saaksid siseturul vabalt liikuda. Tootesse sisseehitatud suure riskiga tehisintellektisüsteemide puhul tuleks kinnitada füüsiline CE-märgis ja seda võib täiendada digitaalse CE-märgisega. Suure riskiga tehisintellektisüsteemide puhul, mida pakutakse ainult digitaalselt, tuleks kasutada digitaalset CE-märgist. Liikmesriigid ei tohiks luua põhjendamatuid tõkkeid käesolevas määruses sätestatud nõuetele vastavate ja CE-märgisega suure riskiga tehisintellektisüsteemide turule laskmisele või kasutusele võtmisele.

(130) Teatavatel tingimustel võib uuenduslike tehnoloogiate kiire kättesaadavus olla inimeste tervise ja turvalisuse, keskkonnakaitse ja kliimamuutuste ning ühiskonna kui terviku jaoks olla äärmiselt tähtis. Seepärast on asjakohane, et teatavatel erandlikel põhjustel, mis on seotud avaliku julgeoleku või füüsiliste isikute elu ja tervise kaitse, keskkonnakaitse ning oluliste tööstus- ja taristuvarade kaitsega, võiksid turujärelevalveasutused lubada selliste tehisintellektisüsteemide turule laskmist või kasutusele võtmist, millele ei ole vastavushindamist tehtud. Käesolevas määruses sätestatud põhjendatud olukordades võivad õiguskaitseasutused või elanikkonnakaitseasutused võtta konkreetse suure riskiga tehisintellektisüsteemi kasutusele ilma turujärelevalveasutuse loata, tingimusel et sellist luba taotletakse põhjendamatu viivituseta kasutamise ajal või pärast seda.

(131) Et hõlbustada tööd, mida komisjon ja liikmesriigid tehisintellekti vallas teevad, ning suurendada avalikkuse jaoks läbipaistvust, peaksid muude kui asjaomaste olemasolevate liidu ühtlustamisõigusaktide kohaldamisalasse kuuluvate toodetega seotud suure riskiga tehisintellektisüsteemide pakkujad, samuti pakkujad, kes leiavad, et käesoleva määruse lisas suure riski kasutusena loetletud tehisintellektisüsteem ei ole kohaldatava erandi alusel suure riskiga, olema kohustatud registreerima iseenda ja teabe oma tehisintellektisüsteemi kohta ELi andmebaasis, mille loob ja mida haldab komisjon. Enne käesoleva määruse lisas suure riski kasutusena loetletud tehisintellektisüsteemi kasutamist peaksid suure riskiga tehisintellektisüsteemide juurutajad, kes on avaliku sektori asutused, ametid või organid, end selles ELi andmebaasis registreerima ja valima välja süsteemi, mida nad kavatsevad kasutada.

Teistel juurutajatel peaks olema õigus teha seda vabatahtlikult. See ELi andmebaasi osa peaks olema avalik ja tasuta kättesaadav, teave peaks olema kergesti kasutatav, arusaadav ja masinloetav. ELi andmebaas peaks olema ka kasutajasõbralik, näiteks pakkudes otsingufunktsioone, sealhulgas märksõnade kaudu, võimaldades üldsusel leida asjakohast teavet, mis peab olema edastatud kõrge riskitasemega tehisintellektisüsteemide registreerimisel, ja teavet selliste kõrge riskiga tehisintellektisüsteemide kasutusmalli kohta, mis on suure riskiga tehisintellektisüsteemid vastavalt käesoleva määruse lisas sätestatule. ELi andmebaasis tuleks registreerida ka kõik suure riskiga tehisintellektisüsteemide olulised muudatused. Õiguskaitse, rände, varjupaiga ja piirikontrollihalduse valdkonna suure riskiga tehisintellektisüsteemide puhul tuleks registreerimiskohustusi täita ELi andmebaasi turvalises mitteavalikus osas. Turvalisele mitteavalikule osale peaks juurdepääs olema rangelt üksnes komisjonil ja turujärelevalveasutustel nende andmebaasi riikliku osa piires. Elutähtsa taristu valdkonna suure riskiga tehisintellektisüsteeme tuleks registreerida üksnes riiklikul tasandil. Kooskõlas määrusega (EL) 2018/1725 peaks ELi andmebaasi vastutav töötleja olema komisjon. Et ELi andmebaas oleks kasutuselevõtmisel täielikult toimiv, peaks andmebaasi loomise menetlus hõlmama funktsionaalsete kirjelduste väljatöötamist komisjoni poolt ja sõltumatut auditiaruannet. Komisjon peaks ELi andmebaasi vastutava töötlejana oma ülesannete täitmisel võtma arvesse küberturvalisuse riske. Et maksimeerida ELi andmebaasi kättesaadavust ja kasutamist avalikkuse poolt, peaks ELi andmebaas, sealhulgas selle kaudu kättesaadavaks tehtud teave, vastama direktiivi (EL) 2019/882 nõuetele.

(132) Teatavad tehisintellektisüsteemid, mis on mõeldud suhtlema füüsiliste isikutega või sisu looma, võivad põhjustada spetsiifilisi kellegi teisena esinemise või pettuse 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 ning sihipäraste erandite kohaldamist, et võtta arvesse õiguskaitse erivajadusi. 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. Kõnealuse kohustuse rakendamisel tuleks arvesse võtta nende füüsiliste isikute omadusi, kes kuuluvad oma vanuse või puude tõttu kaitsetutesse rühmadesse, niivõrd kui tehisintellektisüsteem on mõeldud ka nende rühmadega suhtlemiseks. Peale selle tuleks füüsilisi isikuid teavitada, kui nad puutuvad kokku tehisintellektisüsteemidega, 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. Selline teave ja teavitused tuleks edastada puuetega inimestele juurdepääsetavas vormingus.

(133) Mitmesugused tehisintellektisüsteemid võivad luua suures koguses sünteesitud sisu, mida inimestel on üha raskem eristada inimeste loodud ja ehtsast sisust. Nende süsteemide laialdasel kättesaadavusel ja üha paranevatel võimetel on märkimisväärne mõju teabe ökosüsteemi terviklusele ja usaldusväärsusele, põhjustades uusi mastaapse väärinformatsiooni ja manipuleerimise, pettuse, kellegi teisena esinemise ja tarbijate eksitamise riske. Seda mõju, tehnoloogia arengu kiiret tempot ning vajadust uute meetodite ja tehnikate järele teabe päritolu jälgimiseks arvesse võttes on asjakohane nõuda, et nende süsteemide pakkujad integreeriksid süsteemi tehnilised lahendused, mis võimaldavad masinloetavas vormingus märgistada ja tuvastada selle, et väljundi on loonud või seda on manipuleerinud tehisintellektisüsteem, mitte inimene. Sellised tehnikad ja meetodid peaksid olema nii usaldusväärsed, koostalitlusvõimelised, tõhusad ja töökindlad, kui see on olemasolevaid tehnikaid või nende kombinatsioone arvesse võttes tehniliselt võimalik, ning nendeks on näiteks vesimärgid, metaandmete identifitseerimine, krüptograafilised meetodid sisu päritolu ja autentsuse tõendamiseks, logimismeetodid, sõrmejäljed või muud asjakohased meetodid. Selle kohustuse rakendamisel peaksid pakkujad võtma arvesse ka eri liiki sisu eripärasid ja piire ning valdkonna asjakohaseid tehnoloogilisi ja turusuundumusi, nagu on kajastatud tehnika üldtunnustatud tasemes. Selliseid tehnikaid ja meetodeid saab rakendada tehisintellektisüsteemi või tehisintellektimudeli tasandil, sealhulgas sisu loovate üldotstarbeliste tehisintellektimudelite tasandil, hõlbustades seeläbi tehisintellektisüsteemi järgmise etapi pakkujal selle kohustuse täitmist. Proportsionaalsuse säilitamiseks on asjakohane ette näha, et see märgistamiskohustus ei peaks hõlmama tehisintellektisüsteeme, mis täidavad peamiselt standardse redigeerimise abifunktsiooni, ega tehisintellektisüsteeme, mis ei muuda oluliselt juurutaja esitatud sisendandmeid või nende semantikat.

(134) Lisaks tehisintellektisüsteemi pakkujate kasutatavatele tehnilistele lahendustele peaksid juurutajad, kes kasutavad tehisintellektisüsteemi, et luua või manipuleerida pildi-, audio- või videosisu, mis sarnaneb märgatavalt olemasolevate isikute, objektide, kohtade, üksuste või sündmustega ja võib inimesele ekslikult ehtne ja tõene näida (süvavõltsingud), ka selgel ja eristataval viisil avalikustama, et see sisu on kunstlikult loodud või seda on manipuleeritud, märgistades tehisintellekti väljundi vastavalt ja avalikustades selle tehisliku päritolu. Seda läbipaistvusnõude järgmist ei tohiks tõlgendada nii, et tehisintellektisüsteemi või selle väljundi kasutamine takistab põhiõiguste hartaga tagatud väljendusvabaduse ning kunsti ja teaduse vabaduse õiguse teostamist, eelkõige kui sisu moodustab osa ilmselgelt loomingulisest, satiirilisest, kunstilisest, väljamõeldud või samalaadsest teosest või programmist, tingimusel et kolmandate isikute õiguste ja vabaduste kaitseks kohaldatakse asjakohaseid kaitsemeetmeid. Sellistel juhtudel piirdub käesolevas määruses sätestatud süvavõltsingute läbipaistvuskohustus sellise loodud või manipuleeritud sisu olemasolu avalikustamisega asjakohasel viisil, mis ei takista teose kuvamist või vaatamist, sealhulgas selle tavapärast tarbimist ja kasutamist, säilitades samal ajal teose kasutatavuse ja kvaliteedi. Lisaks on asjakohane näha ette sarnane avalikustamiskohustus ka tehisintellekti loodud või manipuleeritud teksti puhul, kui see on avaldatud eesmärgiga teavitada avalikkust avalikku huvi pakkuvatest küsimustest, välja arvatud juhul, kui tehisintellekti loodud sisu on läbinud inimkontrolli või toimetusliku kontrolli ning füüsiline või juriidiline isik kannab sisu avaldamise eest toimetuslikku vastutust.

(135) Ilma et see piiraks läbipaistvuskohustuste kohustuslikkust ja täielikku kohaldatavust, võib komisjon samuti julgustada ja hõlbustada tegevusjuhendite koostamist liidu tasandil, et hõlbustada kunstlikult loodud või manipuleeritud sisu avastamise ja märgistamisega seotud kohustuste tõhusat rakendamist, sealhulgas toetada praktilist korda, mille abil teha vajaduse korral avastamismehhanismid juurdepääsetavaks ja hõlbustada koostööd teiste väärtusahelas osalejatega, levitada sisu või kontrollida selle ehtsust ja päritolu, et võimaldada üldsusel tehisintellekti loodud sisu tõhusalt eristada.

(136) Määruse (EL) 2022/2065 tõhusa rakendamise hõlbustamiseks on eriti asjakohased kohustused, mis on käesoleva määrusega kehtestatud teatavate tehisintellektisüsteemide pakkujatele ja juurutajatele, et võimaldada avastada ja avalikustada seda, et nende süsteemide väljundid on kunstlikult loodud või manipuleeritud. See kehtib eelkõige seoses väga suurte digiplatvormide või väga suurte internetipõhiste otsingumootorite pakkujate kohustusega teha kindlaks ja maandada süsteemseid riske, mis võivad tuleneda kunstlikult loodud või manipuleeritud sisu levitamisest, eelkõige oht, et see avaldab tegelikku või prognoositavat negatiivset mõju demokraatlikele protsessidele, ühiskondlikule arutelule ja valimisprotsessidele, sealhulgas desinformatsiooni kaudu. Käesoleva määruse kohane nõue märgistada tehisintellektisüsteemide loodud sisu ei piira määruse (EL) 2022/2065 artikli 16 lõikes 6 sätestatud teabe talletamise teenuse pakkujate kohustust töödelda kõnealuse määruse artikli 16 lõike 1 kohaselt saadud teateid ebaseadusliku sisu kohta ning see ei tohiks mõjutada konkreetse sisu hindamist ja selle ebaseaduslikkust käsitlevat otsust. Hindamisel tuleks lähtuda üksnes sisu õiguspärasust reguleerivatest õigusnormidest.

(137) Käesoleva määrusega hõlmatud tehisintellektisüsteemide läbipaistvuskohustuste täitmist ei tohiks tõlgendada nii, et tehisintellektisüsteemi või selle väljundi kasutamine on seaduslik käesoleva määruse või liidu ja liikmesriikide muu õiguse alusel, ning see ei tohiks piirata tehisintellektisüsteemide juurutajate muid läbipaistvuskohustusi, mis on sätestatud liidu või riigisiseses õiguses.

(138) Tehisintellekt on kiirelt arenev tehnoloogiaharu, mis eeldab regulatiivset järelevalvet ning turvalist ja kontrollitud eksperimenteerimisruumi, aga ka seda, et tagatud oleks vastutustundlik innovatsioon ning asjakohaste kaitsemeetmete ja riskimaandamismeetmete integreerimine. Et tagada õigusraamistik, mis edendab innovatsiooni, on tulevikukindel ja häirete suhtes vastupanuvõimeline, peaksid liikmesriigid tagama, et nende pädevad asutused loovad riiklikul tasandil vähemalt ühe tehisintellekti regulatiivliivakasti, mis hõlbustaks innovatiivsete tehisintellektisüsteemide arendamist ja testimist range regulatiivse järelevalve all, enne kui need süsteemid turule lastakse või muul moel kasutusele võetakse. Liikmesriigid võiksid seda kohustust täita, osaledes juba olemasolevates regulatiivliivakastides või luues regulatiivliivakasti koos ühe või mitme liikmesriigi pädeva asutusega, kui selline osalemine tagab osalevatele liikmesriikidele samaväärse riikliku katvuse. Tehisintellekti regulatiivliivakaste võiks luua füüsilisel, digitaalsel või hübriidkujul ning need võivad hõlmata nii füüsilisi kui ka digitaalseid tooteid. Samuti peaksid tehisintellekti regulatiivliivakastide loomise eest vastutavad asutused tagama, et regulatiivliivakastidel on nende toimimiseks piisavad vahendid, sealhulgas rahalised ja inimressursid.

(139) Tehisintellekti regulatiivliivakastide eesmärk peaks olema edendada tehisintellekti innovatsiooni, luues arendus- ja turustamiseelses etapis kontrollitud eksperimenteerimis- ja testimiskeskkonna, et tagada innovatiivsete tehisintellektisüsteemide vastavus käesolevale määrusele ning muule asjakohasele liidu ja liikmesriigi õigusele. Lisaks peaks tehisintellekti regulatiivliivakastide eesmärk olema suurendada innovaatorite õiguskindlust ning pädevate asutuste järelevalvet ja arusaamist tehisintellekti kasutamise võimalustest, tekkivatest riskidest ja mõjust, hõlbustada asutuste ja ettevõtjate regulatiivset õppimist, sealhulgas pidades silmas õigusraamistiku tulevast kohandamist, toetada koostööd ja parimate tavade jagamist tehisintellekti regulatiivliivakasti kaasatud asutustega ning kiirendada juurdepääsu turgudele, sealhulgas kõrvaldades tõkked VKEde, sealhulgas idufirmade jaoks. Tehisintellekti regulatiivliivakastid peaksid olema laialdaselt kättesaadavad kogu liidus ning erilist tähelepanu tuleks pöörata nende kättesaadavusele VKEde, sealhulgas idufirmade jaoks. Tehisintellekti regulatiivliivakastis osalemisel tuleks keskenduda küsimustele, mis tekitavad pakkujatele ja võimalikele pakkujatele õiguskindlusetust seoses innovatsiooni, liidus tehisintellektiga eksperimenteerimise ja tõenduspõhisele regulatiivsele õppimisele kaasaaitamisega. Tehisintellektisüsteemide järelevalve tehisintellekti regulatiivliivakastis peaks seega hõlmama süsteemide arendamist, treenimist, testimist ja valideerimist enne nende turule laskmist või kasutusele võtmist, samuti sellise olulise muudatuse määratlust ja tegemist, mis võib nõuda uut vastavushindamismenetlust. Kui selliste tehisintellektisüsteemide arendamise ja testimise käigus tuvastatakse oluline risk, tuleb selle põhjal võtta piisavaid maandamismeetmeid ja kui see ei ole võimalik, tuleb arendamine ja testimine peatada.

Kui see on asjakohane, peaksid tehisintellekti regulatiivliivakaste 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, teada antud asutused, testimis- ja eksperimenteerimisrajatised, teadus- ja eksperimenteerimislaborid, Euroopa digitaalse innovatsiooni keskused ning asjaomased sidusrühmad ja kodanikuühiskonna organisatsioonid. Selleks, et tagada ühetaoline rakendamine kogu liidus ja mastaabisääst, on asjakohane kehtestada tehisintellekti regulatiivliivakastide rakendamise ühised õigusnormid ja regulatiivliivakastide järelevalvega tegelevate asjaomaste ametiasutusete vahelise koostöö raamistik. Käesoleva määruse alusel loodud tehisintellekti regulatiivliivakastid ei tohiks piirata sellise muu õiguse kohaldamist, mis võimaldab luua muid regulatiivliivakaste, mille eesmärk on tagada kooskõla muu õigusega kui käesolev määrus. Kui see on asjakohane, peaksid nende muude regulatiivliivakastide eest vastutavad asjaomased pädevad asutused kaaluma, millised eelised on sellel, kui neid regulatiivliivakaste kasutatakse ka eesmärgiga tagada tehisintellektisüsteemide vastavus käesolevale määrusele. Riikide pädevate asutuste ja tehisintellekti regulatiivliivakastides osalejate vahelisel kokkuleppel võib tehisintellekti regulatiivliivakastide raames korraldada ja kontrollida ka testimist tegelikes tingimustes.

(140) Käesoleva määrusega tuleks tehisintellekti regulatiivliivakastis tegutsevatele pakkujatele ja võimalikele pakkujatele ette näha õiguslik alus muul otstarbel kogutud isikuandmete kasutamiseks, et arendada tehisintellekti regulatiivliivakastis avalikes huvides teatavaid tehisintellektisüsteeme, ainult konkreetsetel tingimustel kooskõlas määruse (EL) 2016/679 artikli 6 lõikega 4 ja artikli 9 lõike 2 punktiga g ning määruse (EL) 2018/1725 artiklitega 5, 6 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 määrustest (EL) 2016/679 ja (EL) 2018/1725 ning 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. Tehisintellekti regulatiivliivakastis tegutsevad pakkujad ja võimalikud pakkujad peaksid tagama asjakohased kaitsemeetmed ja tegema koostööd pädevate asutustega, järgides muu hulgas nende juhendeid ning tegutsedes viivitusteta ja heas usus, et vajalikul määral maandada turvalisust, tervist ja põhiõigusi ähvardavaid tuvastatud olulisi riske, mis võivad selles regulatiivliivakastis arendustegevuse, testimise ja eksperimenteerimise käigus tekkida.

(141) Selleks et kiirendada käesoleva määruse 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 regulatiivliivakastis. Sellistel juhtudel, võttes arvesse sellise testimise võimalikke tagajärgi üksikisikutele, tuleks siiski tagada, et käesoleva 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, kus teadva nõusoleku taotlemine takistaks tehisintellektisüsteemi testimist. Subjektide nõusolek sellises käesoleva määruse alusel toimuvas testimises osalemiseks erineb andmesubjektide nõusolekust oma isikuandmete töötlemiseks asjakohase andmekaitseõiguse alusel ega piira kõnealuse õiguse kohaldamist.

Samuti on oluline minimeerida riske ja võimaldada pädevatel asutustel teostada järelevalvet ning nõuda seetõttu, et võimalikud pakkujad esitaksid pädevale turujärelevalveasutusele tegelikes tingimustes testimise kava, registreeriksid testimise ELi andmebaasi vastavates osades, välja arvatud mõned piiratud erandid, kehtestada piirangud ajavahemikule, mille jooksul testimine saab toimuda, ning nõuda täiendavaid kaitsemeetmeid kaitsetusse rühma kuuluvatele isikutele, ning kirjalikku kokkulepet, milles määratakse kindlaks võimalike pakkujate ja juurutajate ülesanded ja kohustused ning tegelikes tingimustes testimises osalevate pädevate töötajate tõhus järelevalve. Lisaks on asjakohane näha ette täiendavad kaitsemeetmed tagamaks, et tehisintellektisüsteemi prognoose, soovitusi ja otsuseid saab tulemuslikult tagasi võtta ja jätta need tähelepanuta ning et isikuandmed on kaitstud ja kustutatakse, kui uuringus osalejad on oma nõusoleku testimises osalemiseks tagasi võtnud, ilma et see piiraks nende kui andmesubjektide õigusi, mis tulenevad liidu andmekaitseõigusest. Seoses andmete edastamisega on samuti asjakohane näha ette, et tegelikes tingimustes testimiseks kogutud ja töödeldud andmeid tuleks kolmandatele riikidele edastada üksnes siis, kui rakendatakse liidu õiguse kohaseid asjakohaseid ja kohaldatavaid kaitsemeetmeid, eelkõige kooskõlas liidu andmekaitseõiguse kohaste isikuandmete edastamise alustega, samas kui isikustamata andmete puhul kehtestatakse asjakohased kaitsemeetmed kooskõlas liidu õigusega, näiteks Euroopa Parlamendi ja nõukogu määrustega (EL) 2022/868[42] ja (EL) 2023/2854[43].

---

[42] Euroopa Parlamendi ja nõukogu 30. mai 2022. aasta määrus (EL) 2022/868 Euroopa andmehalduse kohta ning millega muudetakse määrust (EL) 2018/1724 (andmehalduse määrus) (ELT L 152, 3.6.2022, lk 1).

[43] Euroopa Parlamendi ja nõukogu 13. detsembri 2023. aasta määrus (EL) 2023/2854 ühtlustatud õigusnormide kohta, millega reguleeritakse õiglast juurdepääsu andmetele ja andmete kasutamist, millega muudetakse määrust (EL) 2017/2394 ja direktiivi (EL) 2020/1828 (andmemäärus) (ELT L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

(142) Tagamaks, et tehisintellekt toob ühiskonna ja keskkonna jaoks kaasa soodsad tulemused, julgustatakse liikmesriike toetama ja edendama tehisintellektilahenduste teadus- ja arendustegevust, et toetada ühiskonna ja keskkonna jaoks soodsate tulemuste saavutamist, näiteks tehisintellektipõhiseid lahendusi, et suurendada puuetega inimeste juurdepääsu, vähendada sotsiaal-majanduslikku ebavõrdsust või täita keskkonnaalaseid eesmärke, eraldades piisavalt vahendeid, sealhulgas avaliku sektori ja liidu rahalisi vahendeid, ning kui see on asjakohane ja tingimusel, et rahastamiskõlblikkuse ja valikukriteeriumid on täidetud, võttes eelkõige arvesse selliseid eesmärke taotlevaid projekte. Sellised projektid peaksid põhinema valdkondadevahelise koostöö põhimõttel tehisintellekti arendajate, ebavõrdsuse ja mittediskrimineerimise, juurdepääsetavuse, tarbija-, keskkonna- ja digitaalõiguste valdkonna ekspertide ning akadeemilise ringkonna vahel.

(143) Innovatsiooni edendamiseks ja kaitsmiseks on oluline pöörata erilist tähelepanu VKEde, sealhulgas idufirmade, mis on tehisintellektisüsteemide pakkujad või juurutajad, huvidele. Liikmesriigid peaksid seda silmas pidades välja töötama nimetatud operaatoritele suunatud algatusi, muu hulgas teadlikkuse suurendamise ja teabe edastamise teemal. Liikmesriigid peaksid andma VKEdele, sealhulgas idufirmadele, kelle registrijärgne asukoht või filiaal on liidus, eelisjuurdepääsu tehisintellekti regulatiivliivakastidele, tingimusel et nad vastavad kõlblikkustingimustele ja valikukriteeriumidele, ilma et see välistaks teiste pakkujate ja võimalike pakkujate juurdepääsu regulatiivliivakastidele eeldusel, et nad on täitnud samad tingimused ja kriteeriumid. Liikmesriigid peaksid kasutama olemasolevaid kanaleid, ja kui see on asjakohane, siis looma uusi spetsiaalseid kanaleid suhtlemiseks VKEde, sealhulgas idufirmade, juurutajate, muude innovaatorite ja vajaduse korral kohalike ametiasutustega, et toetada VKEsid kogu nende arendustegevuse jooksul, et anda juhiseid ja vastata päringutele käesoleva määruse rakendamise kohta. Kui see on asjakohane, peaksid need kanalid tegema koostööd, et luua sünergiat ja tagada ühtsus VKEdele, sealhulgas idufirmadele, ja juurutajatele antavates suunistes. Lisaks peaksid liikmesriigid lihtsustama VKEde ja muude asjaomaste sidusrühmade osalemist standardimise arendamise protsessis. Ühtlasi tuleks pakkujatest VKEde, sealhulgas idufirmade, konkreetsete huvide ja vajadustega arvestada siis, kui teada antud asutused määravad kindlaks vastavushindamise tasud. Komisjon peaks korrapäraselt hindama VKEde, sealhulgas idufirmade sertifitseerimis- ja nõuete täitmisega seotud kulusid, kasutades selleks läbipaistvaid konsultatsioone, ning peaks tegema liikmesriikidega koostööd selliste kulude vähendamiseks.

Näiteks 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 juurutajatele. VKEde, sealhulgas idufirmade erivajadustega arvestamiseks peaks komisjon esitama nõukoja taotlusel standardvormid käesoleva määrusega hõlmatud valdkondade jaoks. Lisaks peaks komisjon täiendama liikmesriikide jõupingutusi, luues kõigile pakkujatele ja juurutajatele ühtse teabeplatvormi, mis sisaldab käesoleva määrusega seotud hõlpsasti kasutatavat teavet, korraldades asjakohaseid teavituskampaaniaid, et suurendada teadlikkust käesolevast määrusest tulenevatest kohustustest, ning hinnates ja edendades tehisintellektisüsteemidega seotud riigihankemenetluste parimate tavade lähendamist. Keskmise suurusega ettevõtjatel, kes kvalifitseerusid hiljuti väikeettevõtjateks komisjoni soovituse 2003/361/EÜ[44] lisa tähenduses, peaks olema kõnealustele toetusmeetmetele juurdepääs, kuna neil uutel keskmise suurusega ettevõtjatel võivad mõnikord puududa vajalikud õiguslikud vahendid ja koolitus, et tagada käesoleva määruse nõuetekohane mõistmine ja järgimine.

[44] Komisjoni 6. mai 2003. aasta soovitus mikroettevõtjate ning väikeste ja keskmise suurusega ettevõtjate määratlemise kohta (ELT L 124, 20.5.2003, lk 36).

(144) Innovatsiooni edendamiseks ja kaitsmiseks peaksid tehisintellekti nõudeteenuste platvorm, kõik asjakohased liidu rahastamisprogrammid ja -projektid, nagu programm „Digitaalne Euroopa“ ja programm „Euroopa horisont“, mida rakendavad komisjon ja liikmesriigid vastavalt kas liidu või riiklikul tasandil, aitama kaasa käesoleva määruse eesmärkide saavutamisele.

(145) Et minimeerida rakendamisega seotud riske, mis tulenevad teadmiste ja oskusteabe puudumisest turul, ja muuta käesolevast määrusest tulenevate kohustuste täitmine pakkujate, eelkõige VKEde, sealhulgas idufirmade, ja teada antud asutuste jaoks hõlpsamaks, peaksid tehisintellekti nõudeteenuste platvorm, Euroopa digitaalse innovatsiooni keskused ning komisjoni ja liikmesriikide poolt liidu või riigi tasandil loodud testimis- ja eksperimenteerimisrajatised võimaluse korral aitama kaasa käesoleva määruse rakendamisele. Oma ülesannete ja pädevusvaldkondade piires on tehisintellekti nõudeteenuste platvorm, Euroopa digitaalse innovatsiooni keskused ning testimis- ja eksperimenteerimisrajatised võimelised andma pakkujatele ja teada antud asutustele eelkõige tehnilist ja teaduslikku tuge.

(146) Võttes arvesse mõne operaatori väga väikest suurust ja et tagada proportsionaalsus seoses innovatsioonikuludega, on asjakohane võimaldada mikroettevõtjatel täita ühte kõige kulukamat kohustust, näiteks kohustust kehtestada kvaliteedijuhtimise süsteem, lihtsustatud viisil, kuna see vähendaks nende ettevõtjate halduskoormust ja kulusid, ilma et see mõjutaks kaitse taset ja vajadust täita suure riskiga tehisintellektisüsteemidele kehtestatud nõudeid. Komisjon peaks välja töötama suunised, et täpsustada neid kvaliteedijuhtimise süsteemi elemente, mida mikroettevõtjad saavad lihtsustatud viisil täita.

(147) On asjakohane, 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 määrustele (EL) 2017/745 ja (EL) 2017/746.

(148) Käesoleva määrusega tuleks kehtestada juhtimisraamistik, mis võimaldab koordineerida ja toetada käesoleva määruse kohaldamist riiklikul tasandil ning suurendada suutlikkust liidu tasandil ja lõimida tehisintellekti valdkonna sidusrühmi. Käesoleva määruse tõhusaks rakendamiseks ja jõustamiseks on vaja juhtimisraamistikku, mis võimaldab liidu tasandil keskset oskusteavet koordineerida ja koguda. Tehisintellektiamet loodi komisjoni otsusega[45] ja selle ülesanne on arendada liidus oskusteavet ja suutlikkust tehisintellekti valdkonnas ning aidata kaasa tehisintellekti käsitleva liidu õiguse rakendamisele. Liikmesriigid peaksid hõlbustama tehisintellektiameti ülesannete täitmist, et toetada liidu oskusteabe ja liidu tasandil suutlikkuse arendamist ning tugevdada digitaalse ühtse turu toimimist. Lisaks tuleks luua liikmesriikide esindajatest koosnev nõukoda, teaduskomisjon teadusringkondade integreerimiseks ja nõuandev kogu, et saada sidusrühmadelt panus käesoleva määruse rakendamisse liidu ja riiklikul tasandil. Liidu oskusteabe ja suutlikkuse arendamine peaks hõlmama ka olemasolevate ressursside ja oskusteabe kasutamist, eelkõige koostoime kaudu struktuuridega, mis on loodud liidu tasandil muu õiguse täitmise tagamise kontekstis, ning koostoime kaudu seotud algatustega liidu tasandil, nagu Euroopa kõrgjõudlusega andmetöötluse ühisettevõte ning programmi „Digitaalne Euroopa“ tehisintellekti testimis- ja eksperimenteerimisrajatistega.

[45] Komisjoni 24. jaanuari 2024. aasta otsus, millega asutatakse Euroopa tehisintellekti amet C(2024) 390.

(149) Et hõlbustada käesoleva määruse sujuvat, tulemuslikku ja ühtset rakendamist, tuleks luua nõukoda. Nõukoda peaks kajastama tehisintellekti ökosüsteemi erinevaid huve ja koosnema liikmesriikide esindajatest. Nõukoda peaks vastutama mitmesuguste nõustamisalaste ülesannete eest, sealhulgas arvamuste, soovituste ja nõuannete andmine 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 pädevatele asutustele nõu andmine konkreetsetes tehisintellektiga seotud küsimustes. Selleks et anda liikmesriikidele teatav paindlikkus oma esindajate nimetamisel 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 teada antud asutustega seotud küsimustes. Turujärelevalve alaline allrühm peaks tegutsema käesoleva määruse kohaldamisel halduskoostöörühmana määruse (EL) 2019/1020 artikli 30 tähenduses. Vastavalt kõnealuse määruse 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 asjakohase liidu õiguse kontekstis tegutsevate asjaomaste liidu asutuste, eksperdirühmade ja võrgustikega, sealhulgas eelkõige nendega, kes tegutsevad andmeid, digitooteid ja -teenuseid käsitleva asjakohase liidu õiguse alusel.

(150) Selleks et tagada sidusrühmade kaasamine käesoleva määruse rakendamisse ja kohaldamisse, tuleks luua nõuandev kogu, et nõustada nõukoda ja komisjoni ning anda neile tehnilist oskusteavet. Selleks et sidusrühmade puhul oleks tagatud mitmekülgne ja tasakaalustatud esindatus ärihuvide ja mitteäriliste huvide vahel ning ärihuvide kategoorias VKEde ja muude ettevõtjate vahel, peaks nõuandev kogu muu hulgas hõlmama tööstust, idufirmasid, VKEsid, akadeemilisi ringkondi, kodanikuühiskonda, sealhulgas sotsiaalpartnereid, samuti Euroopa Liidu Põhiõiguste Ametit, ENISAt, Euroopa Standardikomiteed (CEN), Euroopa Elektrotehnika Standardikomiteed (CENELEC) ja Euroopa Telekommunikatsioonistandardite Instituuti (ETSI).

(151) Selleks et toetada käesoleva määruse rakendamist ja jõustamist, eelkõige tehisintellektiameti järelevalvetegevust seoses üldotstarbeliste tehisintellektimudelitega, tuleks luua sõltumatutest ekspertidest koosnev teaduskomisjon. Teaduskomisjoni kuuluvad sõltumatud eksperdid tuleks valida tehisintellekti valdkonna ajakohase teadusliku või tehnilise oskusteabe põhjal ning nad peaksid täitma oma ülesandeid erapooletult ja objektiivselt ning tagama oma ülesannete ja tegevuse käigus saadud teabe ja andmete konfidentsiaalsuse. Selleks et suurendada käesoleva määruse tõhusaks jõustamiseks vajalikku riiklikku suutlikkust, peaks liikmesriikidel olema võimalik taotleda oma jõustamistegevuseks toetust teaduskomisjoni ekspertide reservist.

(152) Selleks et toetada tehisintellektisüsteemidega seotud nõuetekohast jõustamist ja tugevdada liikmesriikide suutlikkust, tuleks luua liidu tehisintellekti testimise toetusstruktuurid ja teha need liikmesriikidele kättesaadavaks.

(153) Käesoleva määruse kohaldamisel ja täitmise tagamisel on keskne roll liikmesriikidel. Seoses sellega peaks iga liikmesriik määrama vähemalt ühe teavitava asutuse ja vähemalt ühe turujärelevalveasutuse riigi pädevateks asutusteks, eesmärgiga teha järelevalvet käesoleva määruse kohaldamise ja rakendamise üle. Liikmesriigid võivad otsustada määrata vastavalt oma riiklikele organisatsioonilistele iseärasustele ja vajadustele mis tahes avalik-õigusliku üksuse täitma käesoleva määruse tähenduses riigi pädeva asutuse ülesandeid. Selleks et suurendada liikmesriikide töökorralduse tõhusust ja luua ühtne kontaktpunkt suhtlemiseks üldsuse ja muude vastaspooltega liikmesriigi ja liidu tasandil, peaks iga liikmesriik määrama turujärelevalveasutuse, mis toimiks ühtse kontaktpunktina.

(154) Riigi pädevad asutused peaksid kasutama oma volitusi sõltumatult, erapooletult ja eelarvamusteta, et järgida oma tegevuse ja ülesannete täitmisel objektiivsuse ja erapooletuse põhimõtteid ning tagada käesoleva määruse kohaldamine ja rakendamine. Nende asutuste liikmed peaksid hoiduma igasugusest tegevusest, mis on vastuolus nende kohustustega, ning nende suhtes tuleks kohaldada käesoleva määruse kohaseid konfidentsiaalsusnõudeid.

(155) 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. Asjakohasel juhul peaks turustamisjärgne seire hõlmama analüüsi koostoime kohta muude tehisintellektisüsteemidega, sealhulgas muude seadmete ja tarkvaraga. Turustamisjärgne seire ei peaks hõlmama õiguskaitseasutustest juurutajate tundlikke operatiivandmeid. Selline süsteem on oluline ka selleks, et tõhusamalt ja õigeaegsemalt tegeleda riskidega, mis tulenevad suure riskiga 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, mille abil teatada asjaomastele asutustele kõikidest tõsistest intsidentidest, mis tulenevad nende tehisintellektisüsteemide kasutamisest, st intsidentidest või tõrgetest, mis põhjustavad surma või tõsist tervisekahju, elutähtsa taristu haldamise ja käitamise tõsiseid ja pöördumatuid häireid, põhiõiguste kaitseks ette nähtud liidu õigusest tulenevate kohustuste rikkumist või tõsist kahju varale või keskkonnale.

(156) 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 riigi pädevate asutuste nimetamist liikmesriikide poolt. Turujärelevalvetoimingud ei tohiks mõjutada järelevalve alla kuuluvate üksuste võimet täita oma ülesandeid sõltumatult, kui selline sõltumatus on nõutav liidu õiguses.

(157) 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 igasugusele käesoleva määruse alusel koostatud dokumentatsioonile. Tuleks kehtestada konkreetne kaitsemenetlus, et tagada piisav ja õigeaegne täitmise tagamine tehisintellektisüsteemide osas, mis kujutavad endast ohtu tervisele, turvalisusele ja põhiõigustele. Selliste endast riski kujutavate tehisintellektisüsteemide jaoks kehtestatud menetlust tuleks kohaldada suure riskiga tehisintellektisüsteemide suhtes, mis kujutavad endast riski, keelatud süsteemide suhtes, mis on turule lastud, kasutusele võetud või mida kasutatakse, rikkudes käesoleva määruse sätteid keelatud kasutusviiside kohta, ning tehisintellektisüsteemide suhtes, mis on tehtud kättesaadavaks käesolevas määruses sätestatud läbipaistvusnõudeid rikkudes ja kujutavad endast riski.

(158) Finantsteenuseid käsitlev liidu õigus sisaldab sisemise juhtimissüsteemi ja riskihalduse kohta käivaid õigusnorme ja nõudeid, mida kohaldatakse reguleeritud finantsasutuste suhtes nende teenuste pakkumise käigus, kaasa arvatud siis, kui nad kasutavad tehisintellektisüsteeme. Käesolevast määrusest tulenevate kohustuste ja finantsteenuseid käsitlevate liidu õigusaktide asjaomaste õigusnormide ja nõuete järjepideva kohaldamise ja täitmise tagamiseks tuleks nende õigusaktide järelevalve ja täitmise tagamise eest vastutavad pädevad asutused, eelkõige pädevad asutused, mis on määratletud Euroopa Parlamendi ja nõukogu määruses (EL) nr 575/2013[46] ning Euroopa Parlamendi ja nõukogu direktiivides 2008/48/EÜ,[47] 2009/138/EÜ[48], 2013/36/EL,[49] 2014/17/EL[50] ja (EL) 2016/97[51], määrata nende vastava pädevuse piires 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.

---

46 Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta määrus (EL) nr 575/2013 krediidiasutuste ja investeerimisühingute suhtes kohaldatavate usaldatavusnõuete kohta ja määruse (EL) nr 648/2012 muutmise kohta (ELT L 176, 27.6.2013, lk 1).

47 Euroopa Parlamendi ja nõukogu 23. aprilli 2008. aasta direktiiv 2008/48/EÜ, mis käsitleb tarbijakrediidilepinguid ja millega tunnistatakse kehtetuks nõukogu direktiiv 87/102/EMÜ (ELT L 133, 22.5.2008, lk 66).

48 Euroopa Parlamendi ja nõukogu 25. novembri 2009. aasta direktiiviga 2009/138/EÜ kindlustus- ja edasikindlustustegevuse alustamise ja jätkamise kohta (Solventsus II) (ELT L 335, 17.12.2009, lk 1).

49 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).

50 Euroopa Parlamendi ja nõukogu 4. veebruari 2014. aasta direktiiv 2014/17/EL elamukinnisvaraga seotud tarbijakrediidilepingute kohta ning millega muudetakse direktiive 2008/48/EÜ ja 2013/36/EL ja määrust (EL) nr 1093/2010 (ELT L 60, 28.2.2014, lk 34).

51 Euroopa Parlamendi ja nõukogu 20. jaanuari 2016. aasta direktiiv (EL) 2016/97, mis käsitleb kindlustustoodete turustamist (ELT L 26, 2.2.2016, lk 19).

Kõnealustel pädevatel asutustel peaksid olema kõik käesolevast määrusest ja määrusest (EL) 2019/1020 tulenevad volitused tagada käesoleva määruse nõuete ja kohustuste täitmine, sealhulgas õigus viia läbi tagantjärele tehtavaid turujärelevalvetoiminguid, mida saab asjakohasel juhul integreerida nende olemasolevatesse, asjaomasest finantsteenuseid käsitlevast liidu õigusest tulenevasse 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[52] 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 ja direktiivi 2013/36/EL 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 kohastesse olemasolevatesse kohustustesse ja menetlustesse. Kattuvuse vältimiseks tuleks ette näha ka piiratud erandid seoses pakkujate kvaliteedijuhtimissüsteemidega ja seirekohustusega, mis on pandud suure riskiga tehisintellektisüsteemide juurutajate, niivõrd, kuivõrd neid kohaldatakse direktiiviga 2013/36/EL reguleeritud krediidiasutuste suhtes. Sama korda tuleks kohaldada direktiivi 2009/138/EÜ kohaste kindlustus- ja edasikindlustusandjate ning kindlustusvaldusettevõtjate ning direktiivi (EL) 2016/97 kohaste kindlustusvahendajate suhtes ning muud liiki finantsasutuste suhtes, kes peavad täitma liidu finantsteenuseid käsitleva asjakohase õiguse kohaselt kehtestatud sisemise juhtimissüsteemi, korra või protsessidega seotud nõudeid, et tagada järjepidevus ja võrdne kohtlemine finantssektoris.

---

[52] Nõukogu 15. oktoobri 2013. aasta määrus (EL) nr 1024/2013, millega antakse Euroopa Keskpangale eriülesanded seoses krediidiasutuste usaldatavusnõuete täitmise järelevalve poliitikaga (ELT L 287, 29.10.2013, lk 63).

(159) Igal käesoleva määruse lisas loetletud biomeetriliste andmete valdkonnaga seotud suure riskiga tehisintellektisüsteemide turujärelevalveasutusel, kui neid süsteeme kasutatakse õiguskaitseks, rände-, varjupaiga- ja piirikontrollihalduseks või õigusemõistmiseks ja demokraatlikeks protsessideks, peaksid olema tõhusad uurimis- ja parandusvolitused, sealhulgas vähemalt õigus saada juurdepääs kõigile töödeldavatele isikuandmetele ja kogu teabele, mis on vajalik tema ülesannete täitmiseks. Turujärelevalveasutustel peaks olema võimalik kasutada oma volitusi täiesti sõltumatult. Käesoleva määrusega kehtestatud tundlikele operatiivandmetele juurdepääsu piirangud ei tohiks piirata neile asutustele direktiiviga (EL) 2016/680 antud volitusi. Ükski käesoleva määruse kohane erand, mis puudutab andmete avaldamist riiklikele andmekaitseasutustele, ei tohiks mõjutada nende asutuste praeguseid või tulevasi volitusi väljaspool käesoleva määruse kohaldamisala.

(160) Turujärelevalveasutused ja komisjon peaksid saama teha ettepanekuid ühismeetmete, sealhulgas ühiste uurimiste kohta, mida viivad läbi turujärelevalveasutused või turujärelevalveasutused koos komisjoniga ja mille eesmärk on edendada nõuetele vastavust, teha kindlaks mittevastavus, suurendada teadlikkust ja anda suuniseid käesoleva määruse kohta seoses selliste suure riskiga tehisintellektisüsteemide konkreetsete kategooriatega, mille puhul on leitud, et need kujutavad endast tõsist riski kahes või enamas liikmesriigis. Nõuete täitmise edendamiseks tuleks võtta ühismeetmeid kooskõlas määruse (EL) 2019/1020 artikliga 9. Ühisuurimiste koordineerimistoe peaks tagama tehisintellektiamet.

(161) On vaja selgitada liidu ja liikmesriikide tasandi kohustusi ja pädevusi seoses üldotstarbelistel tehisintellektimudelitel põhinevate tehisintellektisüsteemidega. Pädevuste kattumise vältimiseks peaks juhul, kui tehisintellektisüsteem põhineb üldotstarbelisel tehisintellektimudelil ning mudelit ja süsteemi pakub sama pakkuja, toimuma järelevalve liidu tasandil tehisintellektiameti kaudu, kellel peaks selleks olema turujärelevalveasutuse volitused määruse (EL) 2019/1020 tähenduses. Kõigil muudel juhtudel vastutavad tehisintellektisüsteemide järelevalve eest riiklikud turujärelevalveasutused. Selliste üldotstarbeliste tehisintellektisüsteemide puhul, mida juurutajad saavad kasutada otse vähemalt ühel eesmärgil, mis on liigitatud suure riskiga eesmärgiks, peaksid turujärelevalveasutused tegema tehisintellektiametiga koostööd, et hinnata nõuetele vastavust ning teavitada sellest nõukoda ja teisi turujärelevalveasutusi. Lisaks peaks turujärelevalveasutustel olema võimalik taotleda tehisintellektiametilt abi, kui turujärelevalveasutusel ei ole võimalik suure riskiga tehisintellektisüsteemi uurimist lõpule viia, kuna sellel puudub juurdepääs teatavale teabele, mis on seotud üldotstarbelise tehisintellektimudeliga, millel suure riskiga tehisintellektisüsteem põhineb. Sellistel juhtudel tuleks kohaldada määruse (EL) 2019/1020 VI peatükis sätestatud menetlust, mis käsitleb piiriülest vastastikust abi, *mutatis mutandis*.

(162) Selleks et liidu keskset oskusteavet ja koostoimet liidu tasandil parimal viisil ära kasutada, peaksid üldotstarbeliste tehisintellektimudelite pakkujate kohustuste järelevalve ja täitmise tagamise volitused kuuluma komisjoni pädevusse. Tehisintellektiametil peaks olema võimalik võtta kõik vajalikud meetmed, et jälgida käesoleva määruse tõhusat rakendamist seoses üldotstarbeliste tehisintellektimudelitega. Ametil peaks olema võimalik uurida üldotstarbeliste tehisintellektimudelite pakkujaid käsitlevate õigusnormide võimalikke rikkumisi nii omal algatusel, järelevalvetegevuse tulemuste põhjal kui ka turujärelevalveasutuste taotlusel kooskõlas käesolevas määruses sätestatud tingimustega. Selleks et toetada tehisintellektiameti tõhusat järelevalvet, peaks see nägema ette võimaluse, et järgmise etapi pakkujad saavad esitada kaebusi üldotstarbeliste tehisintellektimudelite ja -süsteemide pakkujaid käsitlevate õigusnormide võimaliku rikkumise kohta.

(163) Üldotstarbeliste tehisintellektimudelite juhtimissüsteemide täiendamiseks peaks teaduskomisjon toetama tehisintellektiameti seiretegevust ja võib teatavatel juhtudel edastada tehisintellektiametile kvalifitseeritud hoiatusteateid, mille põhjal alustatakse järelkontrolle, näiteks uurimisi. See peaks olema nii juhul, kui teaduskomisjonil on põhjust kahtlustada, et üldotstarbeline tehisintellektimudel kujutab endast konkreetset ja tuvastatavat riski liidu tasandil. Lisaks peaks see nii olema juhul, kui teaduskomisjonil on põhjust kahtlustada, et üldotstarbeline tehisintellektimudel vastab kriteeriumidele, mis annaksid alust liigitada see süsteemse riskiga üldotstarbeliseks tehisintellektimudeliks. Selleks et anda teaduskomisjonile teavet, mis on vajalik nende ülesannete täitmiseks, tuleks ette näha mehhanism, mille abil teaduskomisjon saab taotleda, et komisjon nõuaks pakkujalt dokumentatsiooni või teavet.

(164) Tehisintellektiametil peaks olema võimalik võtta vajalikke meetmeid, et jälgida käesolevas määruses sätestatud üldotstarbeliste tehisintellektimudelite pakkujate kohustuste tõhusat rakendamist ja täitmist. Tehisintellektiametil peaks olema võimalik uurida võimalikke rikkumisi kooskõlas käesolevas määruses sätestatud volitustega, sealhulgas nõudes dokumentatsiooni ja teavet, viies läbi hindamisi ning nõudes üldotstarbeliste tehisintellektimudelite pakkujatelt meetmete võtmist. Selleks et kasutada sõltumatut oskusteavet, peaks tehisintellektiametil olema võimalik kaasata hindamise käigus sõltumatuid eksperte, kes hindamisi ameti nimel läbi viivad. Kohustuste täitmine peaks olema tagatud, muu hulgas nõudes asjakohaste meetmete võtmist, sealhulgas riskimaandusmeetmeid tuvastatud süsteemsete riskide korral, ning piirates mudeli turul kättesaadavaks tegemist, võttes selle turult tagasi või nõudes tagasi. Kui see on lisaks käesolevas määruses sätestatud menetlusõigustele vajalik, peaksid üldotstarbeliste tehisintellektimudelite pakkujatel olema kaitsemeetmena määruse (EL) 2019/1020 artiklis 18 sätestatud menetlusõigused, mida tuleks kohaldada *mutatis mutandis*, ilma et see piiraks käesolevas määruses sätestatud konkreetsemaid menetlusõigusi.

(165) Muude tehisintellektisüsteemide kui suure riskiga tehisintellektisüsteemide arendamine kooskõlas käesoleva määruse nõuetega võib aidata kaasa eetilise ja usaldusväärse tehisintellekti laialdasemale levikule liidus. Muude kui suure riskiga tehisintellektisüsteemide pakkujaid tuleks julgustada koostama käitumisjuhendeid, sealhulgas nendega seotud juhtimismehhanisme, mille eesmärk on edendada suure riskiga tehisintellektisüsteemide suhtes kohaldatavate mõne või kõigi kohustuslike nõuete vabatahtlikku kohaldamist, mida on kohandatud vastavalt süsteemide sihtotstarbele ja väiksemale kaasnevale riskile ning võttes arvesse kättesaadavaid tehnilisi lahendusi ja tööstuse parimaid tavasid, nagu mudeli- ja andmekaardid. Kõigi tehisintellektisüsteemide, olgu need siis suure riskiga või mitte, ja tehisintellektimudelite pakkujaid ja vajaduse korral juurutajaid tuleks samuti julgustada vabatahtlikult kohaldama täiendavaid nõudeid, mis on seotud näiteks liidu usaldusväärse tehisintellekti eetikasuunistes sätestatud elementidega, keskkonnakestlikkusega, tehisintellektipädevuse meetmetega, tehisintellektisüsteemide kaasava ja mitmekesise projekteerimise ja arendamisega, sealhulgas tähelepanu pööramisega vähekaitstud isikutele ja juurdepääsetavusega puuetega inimeste jaoks, sidusrühmade osalemisega, kaasates vajaduse korral asjaomaseid sidusrühmi, nagu äri- ja kodanikuühiskonna organisatsioonid, akadeemilised ringkonnad, teadusorganisatsioonid, ametiühingud ja tarbijakaitseorganisatsioonid tehisintellektisüsteemide projekteerimisse ja arendamisse, ning arendusmeeskondade mitmekesisusega, sealhulgas soolise tasakaaluga. Vabatahtlike tegevusjuhendite tõhususe tagamiseks peaksid need põhinema selgetel eesmärkidel ja peamistel tulemusnäitajatel, et mõõta nende eesmärkide saavutamist. Samuti tuleks neid vajaduse korral töötada välja kaasaval viisil, kaasates asjaomaseid sidusrühmi, nagu äri- ja kodanikuühiskonna organisatsioonid, akadeemilised ringkonnad, teadusorganisatsioonid, ametiühingud ja tarbijakaitseorganisatsioonid. Komisjon võib töötada välja algatusi, sealhulgas 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.

(166) On oluline, et tehisintellektisüsteemid, mis on seotud toodetega, mis ei ole käesoleva määruse alusel suure riskiga ja mis seega ei pea vastama suure riskiga tehisintellektisüsteemide suhtes sätestatud nõuetele, oleksid siiski ohutud, kui need turule lastakse või kasutusele võetakse. Selle eesmärgi saavutamiseks kohaldatakse turvaabinõuna Euroopa Parlamendi ja nõukogu määrust (EL) 2023/988[53].

(167) 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 riigisisese õigusega. Nad peaksid täitma oma ülesandeid ja tegutsema viisil, mis kaitseb eelkõige intellektuaalomandi õigusi, konfidentsiaalset äriteavet ja ärisaladusi, käesoleva määruse tõhusat rakendamist, avaliku ja riigi julgeolekuga seotud huve, kriminaal- ja haldusmenetluste terviklust ning salastatud teabe terviklust.

---

[53] Euroopa Parlamendi ja nõukogu 10. mai 2023. aasta määrus (EL) 2023/988, milles käsitletakse üldist tooteohutust ja millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 1025/2012 ja Euroopa Parlamendi ja nõukogu direktiivi (EL) 2020/1828 ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2001/95/EÜ ja nõukogu direktiiv 87/357/EMÜ (ELT L 135, 23.5.2023, lk 1).

(168) Käesoleva määruse järgimine peaks olema tagatud karistuste määramise ja muude täitemeetmete abil. Liikmesriigid peaksid võtma kõik vajalikud meetmed, et tagada käesoleva määruse sätete rakendamine, sealhulgas kehtestades mõjusad, proportsionaalsed ja hoiatavad karistused nende rikkumise eest, ning järgides *ne bis in idem* põhimõtet. Käesoleva määruse rikkumise eest määratavate halduskaristuste tugevdamiseks ja ühtlustamiseks tuleks kehtestada teatavate konkreetsete rikkumiste eest määratavate haldustrahvide ülemmäärad. Trahvisummade hindamisel peaksid liikmesriigid võtma igal üksikjuhul arvesse kõiki konkreetse olukorra asjakohaseid asjaolusid, võttes nõuetekohaselt arvesse eelkõige rikkumise laadi, raskusastet ja kestust ning selle tagajärgi ja pakkuja suurust, eelkõige juhul, kui pakkuja on VKE, sealhulgas idufirma. Euroopa Andmekaitseinspektoril peaks olema õigus määrata trahve käesoleva määruse kohaldamisalasse kuuluvatele liidu institutsioonidele, asutustele ja organitele.

(169) Käesoleva määrusega kehtestatud üldotstarbeliste tehisintellektimudelite pakkujate kohustuste täitmine peaks olema tagatud muu hulgas trahvide abil. Selleks tuleks ette näha ka asjakohased trahvimäärad nende kohustuste rikkumise eest, sealhulgas komisjoni poolt käesoleva määruse kohaselt nõutud meetmete täitmata jätmise eest, kohaldades kooskõlas proportsionaalsuse põhimõttega asjakohaseid aegumistähtaegu. Kõik komisjoni poolt käesoleva määruse alusel tehtud otsused vaatab ELi toimimise lepingu kohaselt läbi Euroopa Liidu Kohus, sealhulgas seoses Euroopa Liidu Kohtu täieliku pädevusega karistuse määramisel ELi toimimise lepingu artikli 261 kohaselt.

(170) Liidu ja liikmesriigi õiguses on juba ette nähtud tõhusad õiguskaitsevahendid füüsilistele ja juriidilistele isikutele, kelle õigusi ja vabadusi tehisintellektisüsteemide kasutamine kahjustab. Ilma et see piiraks nimetatud õiguskaitsevahendite kohaldamist, peaks igal füüsilisel või juriidilisel isikul, kellel on alust arvata, et käesolevat määrust on rikutud, olema õigus asjaomasele turujärelevalveasutusele kaebus esitada.

(171) Mõjutatud isikutel peaks olema õigus selgitusele, kui juurutaja otsus põhineb peamiselt teatavate käesoleva määruse kohaldamisalasse kuuluvate suure riskiga tehisintellektisüsteemide väljundil ja kui see otsus tekitab õiguslikke tagajärgi või mõjutab neid isikuid sarnaselt märkimisväärselt viisil, mis nende arvates avaldab kahjulikku mõju nende tervisele, turvalisusele või põhiõigustele. See selgitus peaks olema selge ja sisukas ning andma aluse, mille põhjal saavad mõjutatud isikud oma õigusi kasutada. Õigust saada selgitust ei tohiks kohaldada selliste tehisintellektisüsteemide kasutamise suhtes, mille suhtes kehtivad liidu või liikmesriigi õigusest tulenevad erandid või piirangud, ning seda õigust tuleks kohaldada ainult siis, kui see ei ole liidu õiguses juba ette nähtud.

(172) Isikuid, kes tegutsevad käesoleva määruse rikkumisest teatajatena, tuleks liidu õiguse alusel kaitsta. Seega tuleks käesoleva määruse rikkumisest teatamise ja sellistest rikkumisest teatajate kaitse suhtes kohaldada Euroopa Parlamendi ja nõukogu direktiivi (EL) 2019/1937[54].

[54] Euroopa Parlamendi ja nõukogu 23. oktoobri 2019. aasta direktiiv (EL) 2019/1937 liidu õiguse rikkumisest teavitavate isikute kaitse kohta (ELT L 305, 26.11.2019, lk 17).

(173) Tagamaks, et õigusraamistikku saab vajaduse korral kohandada, peaks komisjonil olema õigus võtta kooskõlas ELi toimimise lepingu artikliga 290 vastu delegeeritud õigusakte, et muuta tingimusi, mille alusel tehisintellektisüsteemi ei käsitata suure riskiga tehisintellektisüsteemina; suure riskiga tehisintellektisüsteemide loetelu; tehnilist dokumentatsiooni käsitlevaid sätteid; ELi vastavusdeklaratsiooni sisu; vastavushindamismenetlusi käsitlevaid sätteid; sätteid, millega määratakse kindlaks need suure riskiga tehisintellektisüsteemid, mille suhtes tuleks kohaldada kvaliteedijuhtimissüsteemi ja tehnilise dokumentatsiooni hindamisel põhinevat vastavushindamist; künnist, võrdlusaluseid ja näitajaid süsteemse riskiga üldotstarbeliste tehisintellektimudelite liigitamise õigusnormides, sealhulgas neid võrdlusaluseid ja näitajaid täiendades; kriteeriume süsteemse riskiga üldotstarbeliste tehisintellektimudelite liigitamiseks; üldotstarbeliste tehisintellektimudelite pakkujate tehnilist dokumentatsiooni ja üldotstarbeliste tehisintellektimudelite pakkujatele esitatavat läbipaistvusteavet.. 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[55] 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.

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

(174) Võttes arvesse tehnoloogia kiiret arengut ja käesoleva määruse tõhusaks kohaldamiseks vajalikku tehnilist oskusteavet, peaks komisjon käesolevat määrust hindama ja vaatama selle läbi hiljemalt … [viis aastat pärast käesoleva määruse jõustumise kuupäeva] ja seejärel iga nelja aasta järel ning esitama Euroopa Parlamendile ja nõukogule aruande. Võttes arvesse mõju käesoleva määruse kohaldamisalale, peaks komisjon lisaks kord aastas hindama vajadust muuta suure riskiga tehisintellektisüsteemide loetelu ja keelatud kasutusviiside loetelu. Lisaks peaks komisjon hiljemalt … [neli aastat pärast käesoleva määruse jõustumise kuupäeva] ja seejärel iga nelja aasta järel hindama vajadust muuta käesoleva määruse lisas esitatud suure riskiga valdkondade rubriikide loetelu, läbipaistvuskohustuste kohaldamisalasse kuuluvaid tehisintellektisüsteeme, järelevalve- ja juhtimissüsteemi tõhusust ning üldotstarbeliste tehisintellektimudelite energiatõhusat arendamist käsitlevate standardimisdokumentide väljatöötamisel tehtud edusamme, sealhulgas vajadust täiendavate meetmete või tegevuste järele, ning esitama Euroopa Parlamendile ja nõukogule selle kohta aruande. Samuti peaks komisjon hiljemalt … [neli aastat pärast käesoleva määruse jõustumise kuupäeva] ja pärast seda iga kolme aasta järel hindama, kui mõjusalt ja tulemuslikult on vabatahtlikkusel põhinevad käitumisjuhendid edendanud suure riskiga tehisintellektisüsteemidele kehtestatud nõuete kohaldamist tehisintellektisüsteemide puhul, mis ei ole suure riskiga tehisintellektisüsteemid, ja võimalik, et ka muude täiendavate nõuete kohaldamist selliste tehisintellektisüsteemide puhul.

(175) 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[56].

(176) Kuna käesoleva määruse eesmärki, nimelt parandada siseturu toimimist ning edendada inimkeskse ja usaldusväärse tehisintellekti laialdast kasutuselevõttu, tagades samal ajal tervise, turvalisuse ja põhiõiguste hartas sätestatud põhiõiguste, sealhulgas demokraatia, õigusriigi põhimõtte, kõrgel tasemel kaitse ja keskkonnakaitse tehisintellektisüsteemide kahjuliku mõju vastu liidus ning toetades innovatsiooni, ei suuda liikmesriigid piisavalt saavutada, küll aga saab seda meetme ulatuse või 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.

---

[56] 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).

(177) 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 käesoleva määruse kohaste suure riskiga tehisintellektisüsteemide puhul. Erandkorras ja avaliku sektori vastutust silmas pidades peaksid käesoleva määruse lisas loetletud õigusaktidega loodud suuremahuliste IT-süsteemide komponentideks olevate tehisintellektisüsteemide operaatorid ja avaliku sektori asutustele kasutamiseks mõeldud suure riskiga tehisintellektisüsteemide operaatorid võtma vajalikud meetmed, et täita käesoleva määruse nõuded 2030. aasta lõpuks ja hiljemalt … [kuus aastat pärast käesoleva määruse jõustumise kuupäeva].

(178) Suure riskiga tehisintellektisüsteemide pakkujaid julgustatakse hakkama vabatahtlikult täitma käesoleva määruse asjakohaseid kohustusi juba üleminekuperioodi jooksul.

(179) Käesolevat määrust tuleks kohaldada alates … [kaks aastat pärast käesoleva määruse jõustumise kuupäeva]. Võttes aga arvesse vastuvõetamatut riski, mis on seotud tehisintellekti teatavate kasutusviisidega, tuleks keelde ja käesoleva määruse üldsätteid kohaldada juba alates … [kuus kuud pärast käesoleva määruse jõustumise kuupäeva]. Kuigi nende keeldude täielik mõju saavutatakse käesoleva määruse kohase juhtimise kehtestamise ja määruse jõustamisega, on oluline hakata keeldusid kohaldama juba varem, et võtta arvesse vastuvõetamatuid riske ja mõjutada muid menetlusi, näiteks tsiviilõiguses. Veelgi enam, juhtimise ja vastavushindamissüsteemiga seotud taristu tuleks tööle rakendada juba enne … [kaks aastat pärast käesoleva määruse jõustumise kuupäeva] ning seepärast tuleks teada antud asutusi ja juhtimisstruktuuri käsitlevaid sätteid kohaldada alates … [12 *kuud* pärast käesoleva määruse jõustumise kuupäeva]. Arvestades tehnoloogia kiiret arengut ja üldotstarbeliste tehisintellektimudelite kasutuselevõttu, tuleks üldotstarbeliste tehisintellektimudelite pakkujate kohustusi kohaldada alates …[12 kuud pärast käesoleva määruse jõustumise kuupäeva]. Tegevusjuhendid peaksid olema valmis hiljemalt … [9 kuud pärast käesoleva määruse jõustumise kuupäeva], et võimaldada pakkujatel nõuetele vastavust õigeaegselt tõendada. Tehisintellektiamet peaks tagama, et liigitamise reeglid ja menetlused on tehnoloogia arengut silmas pidades ajakohased. 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 … [12 kuud pärast käesoleva määruse jõustumise kuupäeva].

(180) Euroopa Andmekaitseinspektori ja Euroopa Andmekaitsenõukoguga konsulteeriti kooskõlas määruse (EL) 2018/1725 artikli 42 lõigetega 1 ja 2 ning nad esitasid oma ühisarvamuse 18. juunil 2021,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I peatükk
Üldsätted

Artikkel 1

Reguleerimisese

1. Käesoleva määruse eesmärk on parandada siseturu toimimist ning edendada inimkeskse ja usaldusväärse tehisintellekti kasutuselevõttu, tagades samal ajal tervise, ohutuse ja põhiõiguste hartas sätestatud põhiõiguste, sealhulgas demokraatia, õigusriigi põhimõtte ja keskkonnakaitse kõrgetasemelise kaitse tehisintellektisüsteemide kahjuliku mõju vastu liidus, ning toetada innovatsiooni.

2. Käesolevas määruses nähakse ette:

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

   b) teatavate tehisintellekti kasutusviiside keelustamine;

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

   d) ühtlustatud läbipaistvusnormid teatavate tehisintellektisüsteemide jaoks;

   e) üldotstarbeliste tehisintellektimudelite turule laskmise ühtlustatud õigusnormid;

f) turuseire, turujärelevalve juhtimise ja täitmise normid;

g) innovatsiooni toetavad meetmed, mis keskenduvad eelkõige VKEdele, sealhulgas idufirmadele.

Artikkel 2

Kohaldamisala

1. Käesolevat määrust kohaldatakse järgmise suhtes:

a) pakkujad, kes tegelevad liidus tehisintellektisüsteemide turule laskmise või kasutusele võtmisega või üldotstarbeliste tehisintellektimudelite turule laskmisega, olenemata sellest, kas pakkuja on asutatud või asub liidus või kolmandas riigis;

b) liidus asutatud või asuvad tehisintellektisüsteemide juurutajad;

c) kolmandates riikides asutatud või asuvad tehisintellektisüsteemide pakkujad ja juurutajad, kui tehisintellektisüsteemi väljundit kasutatakse liidus;

d) tehisintellektisüsteemide importijad ja turustajad;

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

f) pakkujate volitatud esindajad, kes ei ole asutatud liidus;

g) liidus asuvad mõjutatud isikud.

2. Artikli 6 lõike 1 kohaselt suure riskiga tehisintellektisüsteemideks liigitatud süsteemide puhul, mis on seotud I lisa B jaos loetletud liidu ühtlustamisõigusaktidega hõlmatud toodetega, kohaldatakse üksnes artiklit 6, artikleid 102-109 ja artiklit 112. Artiklit 57 kohaldatakse üksnes niivõrd, kuivõrd käesoleva määruse kohased suure riskiga tehisintellektisüsteemidele esitatavad nõuded on nendesse liidu ühtlustamisõigusaktidesse integreeritud.

3. Käesolevat määrust ei kohaldata valdkondade suhtes, mis ei kuulu liidu õiguse kohaldamisalasse, ning see ei mõjuta ühelgi juhul liikmesriikide pädevust seoses riikliku julgeolekuga, olenemata üksuse liigist, kellele liikmesriigid on usaldanud nende pädevustega seotud ülesannete täitmise.

Käesolevat määrust ei kohaldata tehisintellektisüsteemide suhtes üksnes siis ja niivõrd, kuivõrd need lastakse turule, võetakse kasutusele või neid kasutatakse muudatustega või ilma muudatusteta üksnes sõjalisel, kaitse- või riikliku julgeoleku eesmärgil, olenemata seda tegevust teostava üksuse liigist.

Käesolevat määrust ei kohaldata tehisintellektisüsteemide suhtes, mida ei lasta turule ega võeta kasutusele liidus, kui väljundit kasutatakse liidus üksnes sõjalise, kaitse- või riikliku julgeoleku eesmärgil, 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 sõlmitud rahvusvahelise koostöö või õiguskaitse ja õigusalase koostöö alaste lepingute raames, tingimusel et selline kolmas riik või rahvusvaheline organisatsioon pakub piisavaid kaitsemeetmeid üksikisikute põhiõiguste ja -vabaduste kaitseks.

5. Käesolev määrus ei mõjuta määruse (EL) 2022/2065 II peatükis sätestatud vahendusteenuste osutajate vastutust käsitlevate sätete kohaldamist.

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

7. Käesolevas määruses sätestatud õiguste ja kohustustega seoses töödeldavate isikuandmete suhtes kohaldatakse isikuandmete kaitset, eraelu puutumatust ja side konfidentsiaalsust käsitlevat liidu õigust. Käesolev määrus ei mõjuta määrusi (EL) 2016/679 ja (EL) 2018/1725 ega direktiive 2002/58/EÜ ja (EL) 2016/680, ilma et see piiraks käesoleva määruse artikli 10 lõike 5 ja artikli 59 kohaldamist.

8. Käesolevat määrust ei kohaldata tehisintellektisüsteemide või tehisintellektimudelitega seotud teadus-, testimis- või arendustegevuse suhtes enne nende turule laskmist või kasutusele võtmist. Selline tegevus toimub kooskõlas kohaldatava liidu õigusega. See väljajätmine ei hõlma tegelikes tingimustes testimist.

9. Käesolev määrus ei piira muudes tarbijakaitset ja tooteohutust käsitlevates liidu õigusaktides sätestatud õigusnormide kohaldamist.

10. Käesolevat määrust ei kohaldata isikliku, mitte kutsetegevuse käigus tehisintellektisüsteeme kasutavate füüsilistest isikutest juurutajate kohustuste suhtes.

11. Käesolev määrus ei takista liidul või liikmesriikidel säilitamast või kehtestamast õigus- ja haldusnorme, mis on töötajatele soodsamad, et kaitsta nende õigusi seoses tehisintellektisüsteemide kasutamisega tööandjate poolt, või soodustamast või lubamast töötajate jaoks soodsamate kollektiivlepingute kohaldamist.

12. Käesolevat määrust ei kohaldata tehisintellektisüsteemide suhtes, mis on tarbimisse lubatud vaba ja avatud lähtekoodiga litsentside alusel, välja arvatud juhul, kui need lastakse turule või võetakse kasutusele suure riskiga tehisintellektisüsteemidena või artikli 5 või 50 kohaldamisalasse kuuluva tehisintellektisüsteemina.

Artikkel 3

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) „tehisintellektisüsteem“ – masinpõhine süsteem, mis on projekteeritud töötama erineval autonoomsuse tasemel ning mis võib pärast juurutamist olla kohanemisvõimeline ja mis saadud sisendist otseste või kaudsete eesmärkide saavutamiseks järeldab, kuidas genereerida väljundeid, näiteks prognoose, sisu, soovitusi või otsuseid, mis võivad mõjutada füüsilist või virtuaalset keskkonda;

2) „risk“ – kahju tekkimise tõenäosuse ja kahju tõsiduse astme kombinatsioon;

3) „pakkuja“ – füüsiline või juriidiline isik, ametiasutus, ametkond või muu organ, kes arendab tehisintellektisüsteemi või üldotstarbelist tehisintellektimudelit või kellel on väljatöötatud tehisintellektisüsteem või üldotstarbeline tehisintellektimudel ja kes laseb selle turule või võtab tehisintellektisüsteemi kasutusele oma nime või kaubamärgi all kas tasu eest või tasuta;

4) „juurutaja“ – füüsiline või juriidiline isik, ametiasutus, ametkond või muu organ, kes kasutab tehisintellektisüsteemi oma volituste alusel, välja arvatud juhul, kui tehisintellektisüsteemi kasutatakse isikliku, mitte kutselise tegevuse jaoks;

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

6) „importija“ – füüsiline või juriidiline isik, kes asub või on asutatud liidus ja kes laseb turule sellise füüsilise või juriidilise isiku nime või kaubamärki kandva tehisintellektisüsteemi, kes asub või on asutatud kolmandas riigis;

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

8) „operaator“ – pakkuja, toote valmistaja, juurutaja, volitatud esindaja, importija või levitaja;

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

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

11) „kasutusele võtmine“ – tehisintellektisüsteemi tarnimine esmakordseks kasutamiseks otse juurutajale 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 mõistlikult prognoositavast inimkäitumisest või interaktsioonist muude süsteemidega, sealhulgas muude tehisintellektisüsteemidega;

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

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

16) „tehisintellektisüsteemi tagasinõudmine“ – mis tahes meede, mille eesmärk on saavutada juurutajatele 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) „teavitav asutus“ – riigi ametiasutus, kes vastutab vastavushindamisasutuste hindamise, määramise ja neist teavitamise ning nende seire jaoks vajalike menetluste väljatöötamise ja läbiviimise eest;

20) „vastavushindamine“ – protsess, mille käigus tõendatakse, kas suure riskiga tehisintellektisüsteemi kohta III peatüki 2. jaos sätestatud nõuded on täidetud;

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

22) „teada antud asutus“ – vastavushindamisasutus, millest on teada antud käesoleva määruse ja liidu muude asjaomaste ühtlustamisõigusaktide kohaselt;

23) „oluline muudatus“ – tehisintellektisüsteemis pärast selle turule laskmist või kasutusele võtmist tehtud muudatus, mida pakkuja ei ole algses läbi viidud vastavushindamises ette näinud ega kavandanud ning mis mõjutab tehisintellektisüsteemi vastavust II peatüki 2. jaos sätestatud nõuetele või mille tulemusena muutub kasutusotstarve, mida silmas pidades on tehisintellektisüsteemi hinnatud;

24) „CE-märgis“ – märgis, millega pakkuja kinnitab, et tehisintellektisüsteem vastab III peatüki 2. jaos sätestatud nõuetele ja muudele kohaldatavatele liidu ühtlustamisõigusaktidele, millega nähakse ette märgise paigaldamine;

25) „turustamisjärgse seire süsteem“ – kõik toimingud, mida tehisintellektisüsteemi pakkuja teeb, 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 harmoneeritud standard;

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

29) „treenimisandmed“ – andmed, mida kasutatakse tehisintellektisüsteemi treenimiseks selle õpitavate parameetrite sobitamise abil;

30) „valideerimisandmed“ – andmed, mida kasutatakse treenitud tehisintellektisüsteemi hindamiseks ning selle mitteõpitavate parameetrite ja õppimisprotsessi reguleerimiseks, et muu hulgas hoiduda ala- või ülesobitamisest;

31) „valideerimisandmestik“ – eraldi andmestik või treenimisandmestiku osa kindlaksmääratud või muutuva jaotuse alusel;

32) „testimisandmed“ – andmed, mida kasutatakse sõltumatu hinnangu andmiseks tehisintellektisüsteemile, et kinnitada selle süsteemi eeldustekohast toimimist, enne kui süsteem lastakse turule või võetakse kasutusele;

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

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

35) „biomeetriline tuvastamine“ – inimese füüsiliste, füsioloogiliste, käitumuslike või psühholoogiliste omaduste automaatne tuvastamine füüsilise isiku isikusamasuse kindlakstegemiseks, võrreldes isiku biomeetrilisi andmeid andmebaasis säilitatavate isikute biomeetriliste andmetega;

36) „biomeetriline kontroll“ – füüsiliste isikute isikusamasuse automaatne, üks-ühele kontrollimine, sealhulgas autentimine, võrreldes nende biomeetrilisi andmeid varem esitatud biomeetriliste andmetega;

37) „isikuandmete eriliigid“ – 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 liigid;

38) „tundlikud operatiivandmed“ – operatiivandmed, mis on seotud kuritegude tõkestamise, avastamise, uurimise või nende eest vastutusele võtmisega ning mille avalikustamine võib ohustada kriminaalmenetluse terviklikkust;

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

40) „biomeetrilise liigitamise süsteem“ – tehisintellektisüsteem, mille eesmärk on jagada füüsilisi isikuid nende biomeetriliste andmete põhjal konkreetsetesse kategooriatesse, välja arvatud juhul, kui see on teise äriteenuse lisateenus ja rangelt vajalik objektiivsetel tehnilistel põhjustel;

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

42) „reaalajas toimuva biomeetrilise kaugtuvastamise süsteem“ – biomeetrilise kaugtuvastamise süsteem, milles biomeetriliste andmete hõive, võrdlemine ja tuvastamine toimub ilma märkimisväärse viivituseta, hõlmates lisaks viivitamatule tuvastamisele ka piiratud lühikesi viivitusi, et vältida kõrvalehoidmist;

43) „tagantjärele toimuva biomeetrilise kaugtuvastamise süsteem“ – biomeetrilise kaugtuvastamise süsteem, mis ei ole reaalajas toimuva biomeetrilise kaugtuvastamise süsteem;

44) „avalikult juurdepääsetav ruum“ – avalikus või eraomandis füüsiline koht, millele on juurdepääs määramatul arvul füüsilistel isikutel, olenemata sellest, kas kohaldatakse teatavaid juurdepääsutingimusi, ja olenemata võimalikest mahutavuspiirangutest;

45) „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, kellele liikmesriigi õiguse kohaselt on antud ülesanne teostada 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;

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

47) „tehisintellektiamet“ – komisjoni ülesanne aidata kaasa tehisintellektisüsteemide ning üldotstarbeliste tehisintellektimudelite rakendamisele, seirele ja järelevalvele ning tehisintellekti juhtimisele vastavalt komisjoni 24. jaanuari 2024. aasta otsusele; käesolevas määruses sisalduvaid viiteid tehisintellektiametile käsitatakse viidetena komisjonile;

48) „riigi pädev asutus“ – teavitav asutus või turujärelevalveasutus; ELi institutsioonide, ametite, asutuste, ja organite poolt kasutusele võetud või kasutatavate tehisintellektisüsteemide puhul käsitatakse käesolevas määruses toodud viiteid riikide pädevatele asutustele või turujärelevalveasutustele viidetena Euroopa Andmekaitseinspektorile;

49) „tõsine intsident“ – juhtum või tehisintellektisüsteemi talitlushäire, mis otseselt või kaudselt põhjustab ühe järgmistest tagajärgedest:

a) inimese surm või tõsine kahju inimese tervisele;

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

c) põhiõiguste kaitsmiseks mõeldud liidu õigusest tulenevate kohustuste rikkumine;

d) tõsine kahju varale või keskkonnale;

50) „isikuandmed“ – isikuandmed, nagu need on määratletud määruse (EL) 2016/679 artikli 4 punktis 1;

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

52) „profiilianalüüs“ – profiilianalüüs, nagu on määratletud määruse (EL) 2016/679 artikli 4 punktis 4;

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

54) „regulatiivliivakasti kava“ – osaleva pakkuja ja pädeva asutuse vahel kokku lepitud dokument, milles kirjeldatakse regulatiivliivakastis toimuva tegevuse eesmärke, tingimusi, ajakava, metoodikat ja nõudeid;

55) „tehisintellekti regulatiivliivakast“ – pädeva asutuse loodud kontrollitud raamistik, mis pakub tehisintellektisüsteemide pakkujatele või võimalikele pakkujatele võimalust arendada, treenida, valideerida ja testida innovatiivset tehisintellektisüsteemi asjakohastel juhtudel tegelikes tingimustes ning regulatiivliivakasti kava kohaselt piiratud aja jooksul regulatiivse järelevalve all;

56) „tehisintellektipädevus“ – oskused, teadmised ja arusaamine, mis võimaldavad pakkujatel, juurutajatel ja mõjutatud isikutel, võttes arvesse nende käesolevas määruses sätestatud õigusi ja kohustusi, tehisintellektisüsteeme teadlikult juurutada ja suurendada teadlikkust tehisintellekti võimalustest ja riskidest ning võimalikust kahjust, mida see võib põhjustada;

57) „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, ning see ei kvalifitseeru tehisintellektisüsteemi turule laskmiseks või kasutusele võtmiseks käesoleva määruse tähenduses, eeldusel et täidetud on kõik artiklite 57 või 60 kohased tingimused;

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

59) „teadev nõusolek“ – subjekti vaba, konkreetne, ühemõtteline 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;

60) „süvavõltsing“ – loodud või manipuleeritud kujutis või audio- või videosisu, mis sarnaneb tegelike isikute, esemete, kohtade, üksuste või sündmustega ning mis näib kasutajale petlikult ehtne või tõene;

61) „ulatuslik rikkumine“ – üksikisikute huve kaitsva liidu õigusega vastuolus olev tegevus või tegevusetus, mis:

a) on kahjustanud või võib tõenäoliselt kahjustada nende üksikisikute kollektiivseid huve, kes elavad vähemalt kahes muus liikmesriigis kui see, kus

i) tegevus või tegevusetus alguse sai või toimus,

ii) asjaomase pakkuja või, kui see on kohaldatav, tema volitatud esindaja asub või on asutatud, või

iii) juurutaja on asutatud, kui rikkumise on toime pannud juurutaja;

b) on kahjustanud, kahjustab või võib tõenäoliselt kahjustada üksikisikute kollektiivseid huve ja millel on ühiseid tunnuseid, sealhulgas sama ebaseaduslik tava, sama huvi rikkumine ja toimepanemine sama operaatori poolt samaaegselt vähemalt kolmes liikmesriigis;

62) „elutähtis taristu“ – määruse (EL) 2022/2557 artikli 2 punktis 4 määratletud elutähtis taristu;

63) „üldotstarbeline tehisintellektimudel“ – tehisintellektimudel, sealhulgas juhul, kui sellist tehisintellektimudelit treenitakse suure hulga andmetega, kasutades mastaapset enesejärelevalvet, millele on omane märkimisväärne üldisus ja suudab pädevalt täita mitmesuguseid eri ülesandeid, olenemata mudeli turule laskmise viisist, ning mida saab integreerida mitmesugustesse järgmise etapi süsteemidesse või rakendustesse, välja arvatud tehisintellektimudelid, mida kasutatakse teadus- ja arendustegevuses või prototüüpide loomiseks enne nende turule laskmist;

64) „suure mõjuga võimed“ – võimed, mis vastavad kõige arenenumates üldotstarbelistes tehisintellektimudelites tuvastatud võimetele või ületavad neid;

65) „süsteemne risk“ – risk, mis on spetsiifiline üldotstarbeliste tehisintellektimudelite suure mõjuga võimetele ja millel on märkimisväärne mõju liidu turule nende ulatuse või tegeliku või mõistlikult prognoositava negatiivse mõju tõttu rahvatervisele, ohutusele, avalikule julgeolekule, põhiõigustele või ühiskonnale tervikuna ning mida saab laialdaselt levitada kogu väärtusahela ulatuses;

66) „üldotstarbeline tehisintellektisüsteem“ – tehisintellektisüsteem, mis põhineb üldotstarbelisel tehisintellektimudelil ja mis suudab teenida mitmesuguseid eesmärke ja mis on mõeldud nii otseseks kasutamiseks kui ka integreerimiseks teistesse tehisintellektisüsteemidesse;

67) „ujukomatehe“ – mis tahes matemaatiline tehe või väärtuse omistamine, mis hõlmab ujukoma-arve (alamhulk reaalarvudest, mida arvutites esitatakse tavaliselt fikseeritud täpsusega täisarvudena, mille fikseeritud alus on astendatud täisarvulise astmega);

68) „järgmise etapi pakkuja“ – tehisintellektisüsteemi, sealhulgas üldotstarbelise tehisintellektisüsteemi pakkuja, mis integreerib tehisintellektimudeli, olenemata sellest, kas ta pakub tehisintellektimudelit ise ja see on vertikaalselt integreeritud või pakub seda lepinguliste suhete alusel mõni muu üksus.

Artikkel 4

Tehisintellektipädevus

Tehisintellektisüsteemide pakkujad ja juurutajad võtavad võimalikult suurel määral meetmeid, et tagada oma töötajate ja kõigi teiste nende nimel tehisintellektisüsteemide käitamise ja kasutamisega tegelevate isikute piisav tehisintellektipädevus, võttes arvesse nende tehnilisi teadmisi, kogemusi, haridust ja koolitust ning konteksti, milles tehisintellektisüsteeme tuleb kasutada, ning arvestades isikuid või isikute rühmi, kelle puhul tehisintellektisüsteeme kasutatakse.

II peatükk
Tehisintellekti keelatud kasutusviisid

Artikkel 5

Tehisintellekti keelatud kasutusviisid

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 või sihilikult manipuleerivaid või petlikke võtteid, mille eesmärk või tagajärg on isiku või isikute rühma käitumise oluline moonutamine, kahjustades oluliselt nende võimet teha teadlik otsus ja pannes nad seeläbi tegema otsuse, mida nad ei oleks muul juhul teinud, viisil, mis põhjustab või mõistliku tõenäosusega põhjustab sellele isikule, teisele isikule või isikute rühmale olulist kahju;

b) selliste tehisintellektisüsteemide turule laskmine, kasutusele võtmine või kasutamine, mis kasutavad ära füüsilise isiku või 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 selle isiku või sellesse rühma kuuluva isiku käitumist viisil, mis põhjustab või mõistliku tõenäosusega põhjustab sellele või mõnele teisele isikule olulist kahju;

c) selliste tehisintellektisüsteemide turule laskmine, kasutusele võtmine või kasutamine, millega hinnatakse või liigitatakse füüsilisi isikuid või isikute rühmi teatava aja jooksul, tuginedes nende sotsiaalsele käitumisele või teadaolevatele, tuletatud või prognoositud isiku- või iseloomuomadustele, kusjuures sotsiaalpunktide tulemuseks on üks või mõlemad järgmisest:

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

d) tehisintellektisüsteemide turule laskmine või kasutusele võtmine sellel konkreetsel eesmärgil või nende kasutamine füüsiliste isikute riskihindamiste tegemiseks, et hinnata või prognoosida riski, et füüsiline isik paneb toime kuriteo, tuginedes üksnes füüsilise isiku profiilianalüüsile või tema isikuomaduste ja erijoonte hindamisele; seda keeldu ei kohaldata tehisintellektisüsteemide suhtes, mida kasutatakse selleks, et toetada inimhinnangut isiku kuritegelikus tegevuses osalemise kohta, mis juba tugineb kuritegeliku tegevusega otseselt seotud objektiivsetele ja kontrollitavatele faktidele;

e) selliste tehisintellektisüsteemide turule laskmine või kasutusele võtmine sellel konkreetsel eesmärgil või nende kasutamine, mis loovad või laiendavad näotuvastuse andmebaase internetist või videovalve salvestistest näokujutiste kindla suunitluseta ekstraheerimise kaudu;

f) tehisintellektisüsteemide turule laskmine või kasutusele võtmine sellel konkreetsel eesmärgil või nende kasutamine füüsilise isiku emotsioonide tuletamiseks töökoha ja haridusasutustega seoses, välja arvatud juhul, kui tehisintellektisüsteemi kavatsetakse kasutusele võtta või turule viia meditsiinilistel või ohutusega seotud põhjustel;

g) selliste biomeetrilise liigitamise süsteemide turule laskmine või kasutuselevõtmine sellel konkreetsel eesmärgil või nende kasutamine, mis liigitavad füüsilisi isikuid individuaalselt nende biomeetriliste andmete alusel, et tuletada või järeldada nende rassi, poliitilisi vaateid, ametiühingusse kuulumist, usulisi või filosoofilisi veendumusi, seksuaalelu või seksuaalset sättumust; see keeld ei hõlma seaduslikult saadud biomeetriliste andmete, näiteks biomeetrilistel andmetel põhinevate piltide märgistamist või filtreerimist või biomeetriliste andmete kategoriseerimist õiguskaitse valdkonnas;

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

   i) konkreetsete inimröövi, inimkaubanduse või seksuaalse ärakasutamise ohvrite sihipärane otsimine ning kadunud isikute otsimine;

   ii) füüsiliste isikute elu või füüsilist turvalisust ähvardava konkreetse, suure ja vahetu ohu või tegeliku ja olemasoleva või tegeliku ja prognoositava terrorirünnaku ohu ärahoidmine;

iii) kuriteo toimepanemises kahtlustatava isiku asukoha kindlaks tegemine või tuvastamine kriminaaluurimise või süüdistuse esitamise või kriminaalkaristuse täitmisele pööramise eesmärgil II lisas osutatud kuritegude eest, mis on asjaomases liikmesriigis karistatavad vabadusekaotuse või vabadust piirava julgeolekumeetmega, mille maksimaalne pikkus on vähemalt neli aastat.

Esimese lõigu punkt h ei piira määruse (EL) 2016/679 artikli 9 kohaldamist biomeetriliste andmete töötlemise suhtes muudel kui õiguskaitse eesmärkidel.

2. Kui kasutatakse reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi avalikult juurdepääsetavas ruumis õiguskaitse jaoks ükskõik millisel lõike 1 esimese lõigu punktis h osutatud eesmärgil, toimub kasutus selles punktis sätestatud eesmärkidel üksnes selleks, et kinnitada konkreetselt sihtmärgiks oleva isiku isikusamasust, ning selle puhul 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 kasutataks;

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 käesoleva artikli lõike 1 esimese lõigu punktis h osutatud eesmärgil olema vastavuses kasutamise suhtes kehtivate vajalike ja proportsionaalsete kaitsemeetmete ja tingimustega kooskõlas selle kasutamist lubava siseriikliku õigusega ning seda eeskätt ajaliste, geograafiliste ja isikutega seotud piirangute osas. Reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine avalikult juurdepääsetavas ruumis on lubatud üksnes juhul, kui õiguskaitseasutus on viinud lõpule põhiõigustele avalduva mõju hindamise, nagu on sätestatud artiklis 27 ja on registreerinud süsteemi ELi andmebaasis vastavalt artiklile 49. Põhjendatud kiireloomulistel juhtudel võib selliseid süsteeme siiski hakata kasutama ilma neid ELi andmebaasis registreerimata, eeldusel et sellist luba taotletakse põhjendamatu viivituseta.

3. Lõike 1 esimese lõigu punkti h ja lõike 2 kohaldamisel on reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi igaks kasutamiseks avalikult juurdepääsetavas ruumis vaja eelnevat luba, mille annab selle liikmesriigi, kus kasutamine hakkab toimuma, õigusasutus või sõltumatu haldusasutus, kelle otsus on siduv, ja mis antakse põhjendatud taotluse põhjal kooskõlas lõikes 5 osutatud üksikasjalike siseriiklike õigusnormidega. Põhjendatud kiireloomulistel juhtudel võib siiski hakata sellist süsteemi kasutama ilma loata, tingimusel et sellist luba taotletakse põhjendamatu viivituseta ja hiljemalt 24 tunni jooksul. Kui selline luba lükatakse tagasi, lõpetatakse kasutamine viivitamata ning kõik andmed ning selle kasutamise tulemused ja väljundid jäetakse viivitamata kõrvale ja kustutatakse.

Pädev õigusasutus või sõltumatu haldusasutus, kelle otsus on siduv, annab loa üksnes juhul, kui on talle esitatud objektiivsete tõendite või selgete asjaolude põhjal veendunud, et kõnealuse reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine on vajalik ja proportsionaalne mõne lõike 1 esimese lõigu punktis h täpsustatud ja taotluses nimetatud eesmärgi saavutamiseks, ning et eelkõige piirdub süsteemi kasutamine sellega, mis on rangelt vajalik seoses ajavahemiku ning geograafilise ja isikulise kohaldamisalaga. Kõnealune asutus võtab taotluse kohta otsuse tegemisel arvesse lõikes 2 osutatud elemente. Ühtki isiku suhtes kahjulikke õiguslikke tagajärgi põhjustavat otsust ei tohi teha üksnes reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi tulemuste põhjal.

4. Ilma et see piiraks lõike 3 kohaldamist, teavitatakse asjaomast turujärelevalveasutust ja riiklikku andmekaitseasutust igast reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamisest avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil kooskõlas lõikes 5 osutatud siseriiklike õigusnormidega. Teates esitatakse vähemalt lõikes 6 täpsustatud teave ning teade ei sisalda tundlikke operatiivandmeid.

5. Liikmesriik võib otsustada näha ette võimaluse täielikult või osaliselt lubada reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamist avalikult juurdepääsetavas ruumis õiguskaitse jaoks lõike 1 esimese lõigu punktis h ning lõigetes 2 ja 3 loetletud piirides ja tingimustel. Asjaomased liikmesriigid kehtestavad 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 esimese lõigu punktis h loetletud eesmärkide, sealhulgas milliste punkti h alapunktis iii osutatud kuritegude puhul võib anda pädevatele asutustele loa kasutada neid süsteeme õiguskaitse jaoks. Liikmesriigid teatavad nendest õigusnormidest komisjonile hiljemalt 30 päeva jooksul pärast nende vastuvõtmist. Liikmesriigid võivad kooskõlas liidu õigusega kehtestada biomeetrilise kaugtuvastamise süsteemide kasutamise kohta piiravamaid õigusakte.

6. Riiklikud turujärelevalveasutused ja liikmesriikide riiklikud andmekaitseasutused, keda on lõike 4 kohaselt teavitatud reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamisest avalikult juurdepääsetavas ruumis õiguskaitse eesmärkidel, esitavad komisjonile sellise kasutamise kohta aastaaruanded. Selleks esitab komisjon liikmesriikidele ning riiklikele turujärelevalve- ja andmekaitseasutustele vormi, mis sisaldab teavet pädevate õigusasutuste või sõltumatu haldusasutuse poolt, kelle otsus on siduv, lõike 3 kohaste loataotluste suhtes tehtud otsuste arvu ja nende tulemuste kohta.

7. Komisjon avaldab lõikes 6 osutatud aastaaruannete põhjal aastaaruanded reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamise kohta avalikult juurdepääsetavates ruumides õiguskaitse eesmärgil, tuginedes liikmesriikide koondandmetele. Nimetatud aastaaruanded ei sisalda asjaomase õiguskaitsealase tegevuse tundlikke operatiivandmeid.

8. Käesolev artikkel ei mõjuta keelde, mida kohaldatakse juhul, kui tehisintellektiga seotud tegevus rikub muud liidu õigust.

III peatükk
Suure riskiga tehisintellektisüsteemid

1. JAGU
TEHISINTELLEKTISÜSTEEMIDE LIIGITAMINE SUURE RISKIGA TEHISINTELLEKTISÜSTEEMIDEKS

Artikkel 6

Suure riskiga tehisintellektisüsteemide liigitamise reeglid

1. Olenemata sellest, kas tehisintellektisüsteem lastakse turule või võetakse kasutusse punktides a ja b osutatud toodetest sõltumatult, peetakse seda tehisintellektisüsteemi suure riskiga süsteemiks, kui täidetud on mõlemad järgmised tingimused:

   a) tehisintellektisüsteem on mõeldud kasutamiseks toote turvakomponendina või tehisintellektisüsteem on ise toode, mis on hõlmatud I lisas loetletud liidu ühtlustamisõigusaktidega;

b) toode, mille turvakomponent tehisintellektisüsteem vastavalt punktile a on, või tehisintellektisüsteem ise kui toode peab läbima kolmanda isiku tehtava vastavushindamise, et selle saaks turule lasta või kasutusele võtta vastavalt I lisas loetletud liidu ühtlustamisõigusaktidele.

2. Lisaks lõikes 1 osutatud suure riskiga tehisintellektisüsteemidele peetakse suure riskiga süsteemideks ka III lisas osutatud tehisintellektisüsteeme.

3. Erandina lõikest 2 ei peeta III lisas osutatud tehisintellektisüsteemi suure riskiga süsteemiks, kui see ei ohusta oluliselt füüsiliste isikute tervist, ohutust või põhiõigusi, sealhulgas ei mõjuta oluliselt otsuste tegemise tulemust.

Esimest lõiget kohaldatakse siis, kui on täidetud ükskõik milline järgmistest tingimustest:

a) tehisintellektisüsteem on ette nähtud täitma kitsast menetlusülesannet;

b) tehisintellektisüsteem on ette nähtud parandama varem lõpetatud inimtegevuse tulemusi;

c) tehisintellektisüsteem on ette nähtud tuvastama otsustuste tegemise mustreid või kõrvalekaldeid varasematest otsustusmustritest ning see ei ole mõeldud varem lõpetatud inimhinnangu asendamiseks või mõjutamiseks ilma nõuetekohase inimkontrollita, või

d) tehisintellektisüsteem on ette nähtud III lisas loetletud kasutusjuhtumite puhul asjakohase hindamise ettevalmistava ülesande täitmiseks.

Olenemata esimesest lõigust käsitatakse III lisas osutatud tehisintellektisüsteemi alati suure riskiga tehisintellektisüsteemina, kui tehisintellektisüsteem teeb füüsiliste isikute profiilianalüüsi.

4. Pakkuja, kes leiab, et III lisas osutatud tehisintellektisüsteem ei ole suure riskiga, dokumenteerib oma hinnangu enne selle süsteemi turule laskmist või kasutusele võtmist. Sellise pakkuja suhtes kohaldatakse artikli 49 lõikes 2 sätestatud registreerimiskohustust. Riigi pädevate asutuste taotluse korral esitab pakkuja hindamise dokumendid.

5. Komisjon esitab pärast konsulteerimist Euroopa tehisintellekti nõukojaga (edaspidi „nõukoda“) ja hiljemalt … [18 kuud pärast käesoleva määruse jõustumise kuupäeva] suunised, milles täpsustatakse käesoleva artikli praktilist rakendamist kooskõlas artikliga 96, koos põhjaliku loeteluga nii suure riskiga kui ka muude tehisintellektisüsteemide kasutusjuhtumite praktiliste näidete kohta.

6. Komisjonil on õigus võtta kooskõlas artikliga 97 vastu delegeeritud õigusakte, et muuta käesoleva artikli lõike 3 teist lõiku, lisades selles sätestatud tingimustele uusi tingimusi või neid muuta, kui on konkreetseid ja usaldusväärseid tõendeid selliste tehisintellektisüsteemide olemasolu kohta, mis kuuluvad III lisa kohaldamisalasse, kuid ei kujuta endast märkimisväärset ohtu füüsiliste isikute tervisele, ohutusele või põhiõigustele.

7. Komisjon võtab kooskõlas artikliga 97 vastu delegeeritud õigusaktid, et muuta käesoleva artikli lõike 3 teist lõiku, jättes välja kõik selles sätestatud tingimused, kui on olemas konkreetsed ja usaldusväärsed tõendid selle kohta, et see on vajalik käesolevas määruses sätestatud tervise, ohutuse ja põhiõiguste kaitse taseme säilitamiseks.

8. Ükski lõike 3 teises lõigus sätestatud tingimuste muudatus, mis on vastu võetud käesoleva artikli lõigete 6 ja 7 kohaselt, ei tohi vähendada käesolevas määruses sätestatud tervise, ohutuse ja põhiõiguste kaitse üldist taset ning peab tagama järjepidevuse kooskõlas artikli 7 lõike 1 kohaselt vastu võetud delegeeritud õigusaktidega ning võtma arvesse turu ja tehnoloogia arengut.

Artikkel 7

III lisa muutmine

1. Komisjonil on õigus võtta kooskõlas artikliga 97 vastu delegeeritud õigusakte, et muuta III lisa, lisades sellesse suure riskiga tehisintellektisüsteeme või muutes nende kasutusjuhtumeid, kui täidetud on mõlemad järgmised tingimused:

   a) tehisintellektisüsteemid on mõeldud kasutamiseks III lisas loetletud valdkondades;

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

2. Lõike 1 punkti b kohase tingimuse hindamisel võtab komisjon arvesse järgmisi kriteeriume:

a) mis on tehisintellektisüsteemi sihtotstarve;

b) millises ulatuses on tehisintellektisüsteemi kasutatud või tõenäoliselt kasutatakse;

c) tehisintellektisüsteemis töödeldavate ja kasutatavate andmete laad ja hulk, eelkõige see, kas töödeldakse isikuandmete eriliike;

d) mil määral toimib tehisintellektisüsteem autonoomselt ja milline on inimese võimalus eirata otsust või soovitusi, mis võivad põhjustada võimalikku kahju;

e) millises ulatuses on tehisintellektisüsteemi kasutamine juba teinud kahju tervisele ja ohutusele või avaldanud negatiivset mõju põhiõigustele või tekitanud tõsist muret seoses sellise kahju või negatiivse mõju tekkimise võimalusega, nagu on näidanud näiteks riikide pädevatele asutustele esitatud aruanded või dokumenteeritud väited või muud aruanded, kui see on asjakohane;

f) milline oleks sellise kahju või negatiivse mõju võimalik ulatus, eeskätt intensiivsus ja võime mõjutada paljusid isikuid või ebaproportsionaalselt mõjutada üht kindlat isikute rühma;

g) 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;

h) mil määral esineb võimu ebavõrdsus, või on potentsiaalselt kahjustatud või negatiivselt mõjutatud isikud tehisintellektisüsteemi juurutaja suhtes kaitsetus olukorras, eelkõige staatuse, autoriteedi, teadmiste, majanduslike või sotsiaalsete olude või vanuse tõttu;

i) millises ulatuses on tehisintellektisüsteemi kaasamisel saavutatud tulemus kergesti parandatav või tagasipööratav, võttes arvesse selle parandamiseks või tagasipööramiseks kättesaadavaid tehnilisi lahendusi, kusjuures tulemust, millel on negatiivne mõju tervisele, ohutusele või põhiõigustele ei peeta kergesti parandatavaks või tagasipööratavaks;

j) tehisintellektisüsteemi juurutamisest üksikisikutele, rühmadele või ühiskonnale laiemalt tuleneva kasu suurus ja tõenäosus, sealhulgas võimalik tooteohutuse parendamine;

k) millises ulatuses on kehtiva liidu õigusega ette nähtud:

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

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

3. Komisjonil on õigus võtta kooskõlas artikliga 97 vastu delegeeritud õigusakte, et muuta III lisas esitatud loetelu, jättes sellest välja suure riskiga tehisintellektisüsteeme, kui täidetud on mõlemad järgmised tingimused:

a) asjaomane suure riskiga tehisintellektisüsteem ei tekita enam olulisi 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. JAGU

SUURE RISKIGA TEHISINTELLEKTISÜSTEEMIDELE ESITATAVAD NÕUDED

Artikkel 8

Nõuetele vastavus

1. Suure riskiga tehisintellektisüsteemid peavad vastama käesolevas jaos sätestatud nõuetele, võttes arvesse nende sihtotstarvet ning tehisintellekti ja tehisintellektiga seotud tehnoloogiate üldtunnustatud tehnika taset. Nendele nõuetele vastavuse tagamisel võetakse arvesse artiklis 9 osutatud riskijuhtimissüsteemi.

2. Kui toode sisaldab tehisintellektisüsteemi, mille suhtes kohaldatakse nii käesoleva määruse nõudeid kui ka I lisa A jaos loetletud liidu ühtlustamisõigusaktide nõudeid, vastutavad pakkujad selle eest, et nende toode vastab täielikult kõigile kohaldatavate liidu ühtlustamisõigusaktide kohastele kohaldatavatele nõuetele. Selleks et tagada lõikes 1 osutatud suure riskiga tehisintellektisüsteemide vastavus käesolevas jaos sätestatud nõuetele ning et tagada järjepidevus, vältida dubleerimist ja minimeerida lisakoormust, peab pakkujatel olema võimalus asjakohasel juhul integreerida oma toote kohta esitatavad vajalikud testimis- ja aruandlusprotsessid, teave ja dokumentatsioon I lisa A jaos loetletud liidu ühtlustamisõigusaktide kohaselt nõutavatesse juba olemasolevatesse dokumentidesse ja menetlustesse.

Artikkel 9

Riskijuhtimissüsteem

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

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

   a) selliste teadaolevate ja mõistlikult prognoositavate riskide kindlakstegemine ja analüüs, mida suure riskiga tehisintellektisüsteem võib kujutada tervisele, ohutusele või põhiõigustele, kui suure riskiga tehisintellektisüsteemi kasutatakse kooskõlas selle sihtotstarbega;

b) selliste riskide prognoosimine ja hindamine, mis võivad tekkida, kui suure riskiga tehisintellektisüsteemi kasutatakse vastavalt selle sihtotstarbele, aga ka mõistlikult prognoositava väärkasutamise tingimustes;

c) muude tekkida võivate riskide hindamine artiklis 72 osutatud turustamisjärgse seire süsteemist saadud andmete analüüsi põhjal;

d) asjakohaste ja sihipäraste riskijuhtimismeetmete vastuvõtmine punkti a kohaselt kindlaks tehtud riskide käsitlemiseks.

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

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

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

Kõige asjakohasemate riskijuhtimismeetmete kindlaksmääramisel tuleb tagada järgmine:

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

b) asjakohasel juhul sobivate riskimaandamis- ja kontrollimeetmete rakendamine, et käsitleda selliseid riske, mida ei saa kõrvaldada;

c) artikli 13 kohaselt nõutava teabe andmine ning asjakohasel juhul juurutajate koolitamine.

Suure riskiga tehisintellektisüsteemi kasutamisega seotud riskide kõrvaldamisel või vähendamisel võetakse nõuetekohaselt arvesse juurutajalt eeldatavaid tehnilisi teadmisi, kogemusi, haridust ja koolitust, ning eeldatavat kasutuskonteksti, milles kasutamiseks on süsteem mõeldud.

6. Suure riskiga tehisintellektisüsteeme testitakse, et teha kindlaks kõige asjakohasemad ja sihipäraseid riskijuhtimismeetmed. Testimisega tagatakse, et suure riskiga tehisintellektisüsteemid töötavad oma sihtotstarbe seisukohast järjepidevalt ning vastavad käesolevas jaos sätestatud nõuetele.

7. Testimismenetlused võivad hõlmata tegelikes tingimustes testimist kooskõlas artikliga 60.

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

9. Lõigetes 1–7 sätestatud riskijuhtimissüsteemi rakendamisel pööravad pakkujad tähelepanu sellele, kas suure riskiga tehisintellektisüsteem võib oma sihtotstarvet silmas pidades avaldada kahjulikku mõju alla 18-aastastele isikutele, ja kui see on asjakohane, muudele kaitsetutele rühmadele.

10. Suure riskiga tehisintellektisüsteemide pakkujate jaoks, kes peavad täitma liidu muu asjaomase õiguse alusel sisemisi riskijuhtimisprotsesse käsitlevaid nõudeid, võivad lõigetes 1–9 kirjeldatud aspektid olla kõnealuse õiguse kohaselt loodud riskijuhtimismenetluste osa või nendega kombineeritud.

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, kui selliseid andmestikke kasutatakse.

2. Treenimis-, valideerimis- ja testimisandmestike suhtes kohaldatakse suure riskiga tehisintellektisüsteemi sihtotstarbe seisukohast asjakohaseid andmehaldus- ja juhtimistavasid. Need tavad puudutavad eeskätt järgmist:

a) asjakohased projekteerimise käigus tehtavad valikud;

b) andmete kogumise protsessid ja andmete päritolu ning isikuandmete puhul andmete kogumise algne eesmärk;

c) andmevalmenduseks tehtavad asjakohased töötlemistoimingud, näiteks kommenteerimine, märgendamine, puhastamine, ajakohastamine, rikastamine ja koondamine;

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

e) vajalike andmestike kättesaadavuse, koguste ja sobivuse hindamine;

f) läbi vaatamine, pidades silmas võimalikku kallutatust, mis tõenäoliselt mõjutab inimeste tervist ja ohutust, mõjutab negatiivselt põhiõigusi või põhjustab diskrimineerimist, mis on liidu õigusega keelatud, eriti kui andmeväljundid mõjutavad sisendeid tulevaste toimingute jaoks;

g) asjakohased meetmed punkti f kohaselt kindlaks tehtud võimaliku kallutatuse avastamiseks, ennetamiseks ja leevendamiseks;

h) käesoleva määruse järgimist takistavate asjakohaste andmelünkade või puuduste kindlakstegemine ja võimalused nende lünkade ja puuduste kõrvaldamiseks.

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

4. Andmestikes tuleb sihtotstarbe jaoks vajalikus ulatuses võtta arvesse omadusi või elemente, mis iseloomustavad konkreetset geograafilist, kontekstuaalset, käitumuslikku või funktsionaalset keskkonda, kus kavatsetakse suure riskiga tehisintellektisüsteemi kasutada.

5. Niivõrd kui see on rangelt vajalik selleks, et tagada kallutatuse avastamine ja korrigeerimine suure riskiga tehisintellektisüsteemide puhul kooskõlas käesoleva artikli lõike 2 punktidega f ja g, võivad selliste süsteemide pakkujad erandkorras töödelda isikuandmete eriliike, kohaldades asjakohaseid kaitsemeetmeid füüsiliste isikute põhiõiguste ja -vabaduste kaitseks. Lisaks määruste (EL) 2016/679 ja (EL) 2018/1725 ning direktiivi (EL) 2016/680 sätetele peab selline töötlemine vastama kõigile järgmistele tingimustele:

   a) kallutatuse tuvastamist ja parandamist ei ole võimalik tulemuslikult saavutada muude andmete, sealhulgas tehisandmete või anonüümitud andmete töötlemisega;

b) isikuandmete eriliikide suhtes kehtivad isikuandmete taaskasutamise tehnilised piirangud ning tipptasemel turva- ja privaatsuse säilitamise meetmed, sealhulgas pseudonüümimine;

c) isikuandmete eriliikide suhtes kohaldatakse meetmeid, millega tagatakse töödeldavate isikuandmete turvalisus, kaitse ja asjakohased kaitsemeetmed, sealhulgas juurdepääsu range kontroll ja dokumenteerimine, et vältida väärkasutamist ja tagada, et ainult volitatud isikutel, kellel on asjakohased konfidentsiaalsuskohustused, on juurdepääs kõnealustele isikuandmetele;

d) isikuandmete eriliike ei tohi edastada ega üle anda ning need ei tohi olla teistele isikutele muul moel kättesaadavad;

e) isikuandmete eriliigid kustutatakse, kui kallutatus on parandatud või kui isikuandmete säilitamisperiood saab läbi, olenevalt sellest, kumb saabub varem;

f) määruste (EL) 2016/679 ja (EL) 2018/1725 ning direktiivi (EL) 2016/680 kohane isikuandmete töötlemise toimingute registreerimine hõlmab põhjuseid, miks isikuandmete eriliikide töötlemine oli rangelt vajalik kallutatuse avastamiseks ja parandamiseks ning miks seda eesmärki ei olnud võimalik saavutada muude andmete töötlemisega.

6. Nende suure riskiga tehisintellektisüsteemide arendamisel, mille puhul ei kasutata tehisintellektimudelite 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 jaos sätestatud nõuetele ja annaks riikide pädevatele asutustele ja teada antud asutustele selgel ja terviklikul kujul teabe, mis on vajalik, et hinnata tehisintellektisüsteemi vastavust neile nõuetele. Dokumentatsioon peab sisaldama vähemalt IV lisas loetletud elemente. VKEd, sealhulgas idufirmad, võivad esitada IV lisas täpsustatud tehnilise dokumentatsiooni elemente lihtsustatud viisil. Selleks kehtestab komisjon väikeste ja mikroettevõtjate vajadustele vastava lihtsustatud tehnilise dokumentatsiooni vormi. Kui VKE, sealhulgas idufirma, otsustab esitada IV lisas nõutud teabe lihtsustatud korras, kasutab ta käesolevas lõikes osutatud vormi. Teada antud asutused peavad seda vormi vastavushindamise tegemisel arvestama.

2. Kui turule lastakse või kasutusele võetakse suure riskiga tehisintellektisüsteem, mis on seotud tootega, mille suhtes kohaldatakse I lisa A osas loetletud liidu ühtlustamisõigusakte, koostatakse ühtne tehniline dokumentatsioon, mis sisaldab nii kogu lõikes 1 esitatud teavet kui ka nimetatud õigusaktide kohaselt nõutavat teavet.

3. Komisjon võtab kooskõlas artikliga 97 vastu delegeeritud õigusakte, et muuta IV lisa, kui see on vajalik selle tagamiseks, et tehniline dokumentatsioon sisaldab tehnika arengut arvestades kogu vajalikku teavet, et hinnata süsteemi vastavust käesolevas jaos sätestatud nõuetele.

Artikkel 12

Andmete säilitamine

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

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

   a) selliste olukordade tuvastamiseks, mille tulemusel võib suure riskiga tehisintellektisüsteem kujutada riski artikli 79 lõike 1 tähenduses või tuua kaasa olulise muudatuse;

   b) artiklis 72 osutatud turustamisjärgse seire hõlbustamiseks ning

   c) artikli 26 lõikes 5 osutatud suure riskiga tehisintellektisüsteemide toimimise seireks.

3. 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 otsingu tegemisel on saadud otsingutulemus;

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

Artikkel 13

Läbipaistvus ja juurutajate teavitamine

1. Suure riskiga tehisintellektisüsteeme tuleb projekteerida ja arendada selliselt, et oleks tagatud nende toimimise piisav läbipaistvus selleks, et juurutajad saaksid tõlgendada süsteemi väljundit ja seda asjakohaselt kasutada. Tagada tuleb käesolevas 3. jaos sätestatud pakkuja ja juurutaja asjaomaste kohustuste täitmiseks asjakohast liiki ja asjakohasel tasemel läbipaistvus.

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

3. Kasutusjuhend peab sisaldama vähemalt järgmist teavet:

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

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

i) süsteemi sihtotstarve;

ii) artiklis 15 osutatud täpsuse, sealhulgas süsteemi parameetrite, stabiilsuse ja küberturvalisuse tase, millest lähtudes on suure riskiga tehisintellektisüsteemi testitud ja see on valideeritud ning mida võib eeldada, samuti 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 või mõistlikult prognoositava väärkasutamise tingimustes, mis võib seada ohtu artikli 9 lõikes 2 osutatud tervise ja ohutuse või põhiõigused;

iv) kui see on kohaldatav, suure riskiga tehisintellektisüsteemi tehniline võimekus ja omadused, et anda teavet, mis on oluline selle väljundi selgitamiseks;

v) kui see on asjakohane, siis süsteemi toimimine seoses konkreetsete isikute või isikute rühmadega, kelle peal kavatsetakse süsteemi kasutada;

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

vii) kohaldataval juhul teave, mis võimaldab juurutajatel suure riskiga tehisintellektisüsteemi väljundit tõlgendada ja seda asjakohaselt kasutada;

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

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

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

f) kui see on asjakohane, selliste suure riskiga tehisintellektisüsteemi kuuluvate mehhanismide kirjeldus, mis võimaldavad juurutajatel logisid nõuetekohaselt koguda, salvestada ja tõlgendada vastavalt artikli 12 lõikele 1.

Artikkel 14

Inimjärelevalve

1. Suure riskiga tehisintellektisüsteeme projekteeritakse ja arendatakse selliselt, et füüsilised isikud saaksid teha süsteemide kasutamise ajal nende üle reaalset järelevalvet, muu hulgas asjakohaste inimene-masin kasutajaliideste abil.

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 jaos sätestatud nõudeid.

3. Järelevalvemeetmed peavad vastama suure riskiga tehisintellektisüsteemi riskidele, autonoomsuse tasemele ja kasutuskontekstile ning need tagatakse kas ühe järgmist liiki meetme või kõigi järgmist liiki meetmetega:

   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 juurutaja saaks neid rakendada.

4. Lõigete 1, 2 ja 3 rakendamiseks antakse suure riskiga tehisintellektisüsteem juurutajale sellisel viisil, et füüsilistel isikutel, kellele on antud ülesanne teha inimjärelevalvet, oleks võimalik, kui see on olenevalt asjaoludest asjakohane ja proportsionaalne:

   a) mõista nõuetekohaselt suure riskiga tehisintellektisüsteemi asjakohaseid võimeid ja piire ning teha igakülgset seiret selle toimimise üle, sealhulgas selleks, et avastada kõrvalekaldeid, väärtalitlusi ja ootamatut toimimist ning nendega tegeleda;

b) olla pidevalt teadlik võimalusest, et tekib kalduvus hakata automaatselt tuginema või liigselt tuginema suure riskiga tehisintellektisüsteemi toodetud väljundile (nn kalduvus eelistada automatiseerimist), seda eriti siis, kui tegemist on suure riskiga tehisintellektisüsteemidega, mida kasutatakse, et saada teavet või soovitusi füüsiliste isikute tehtavate otsuste jaoks;

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 toimimisse või katkestada süsteemi töö stopp-nupu või muu sarnase protseduuriga, mis võimaldab süsteemil ohutus olekus peatuda.

5. III lisa punkti 1 alapunktis a osutatud suure riskiga tehisintellektisüsteemide puhul tagatakse käesoleva artikli lõikes 3 osutatud meetmetega, et lisaks sellele ei tee ega otsusta juurutaja süsteemist saadud tuvastamise põhjal midagi, kui seda tuvastamist ei ole eraldi kontrollinud ja kinnitanud vähemalt kaks füüsilist isikut, kellel on vajalik pädevus, väljaõpe ja volitused.

Nõuet, et vähemalt kaks füüsilist isikut peavad eraldi kontrollima neid suure riskiga tehisintellektisüsteeme, mida kasutatakse õiguskaitse, rände, piirikontrolli või varjupaigaga seotud eesmärgil, ei kohaldata, kui liidu või riigi õiguse kohaselt peetakse selle nõude kohaldamist ebaproportsionaalseks.

Artikkel 15

Täpsus, stabiilsus ja küberturvalisus

1. Suure riskiga tehisintellektisüsteeme projekteeritakse ja arendatakse selliselt, et need saavutaksid asjakohase täpsuse, stabiilsuse ja küberturvalisuse taseme ning et nad toimiksid nendes aspektides järjekindlalt oma kogu elutsükli jooksul.

2. Selleks et käsitleda lõikes 1 sätestatud asjakohase täpsuse ja stabiilsuse taseme mõõtmise ning muude asjakohaste tulemusnäitajate tehnilisi aspekte, julgustab komisjon koostöös asjaomaste sidusrühmade ja organisatsioonidega, nagu metroloogia- ja võrdlusuuringuasutused, vajaduse korral võrdlusaluste ja mõõtmismeetodite väljatöötamist.

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

4. Suure riskiga tehisintellektisüsteemid peavad olema süsteemis või süsteemi töökeskkonnas tekkida võivate vigade, rikete või ebakõlade suhtes võimalikult vastupidavad, eriti juhul, kui põhjuseks on süsteemi interaktsioon füüsiliste isikute või muude süsteemidega. Selleks võetakse tehnilisi ja korralduslikke meetmeid.

   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, arendatakse selliselt, et kõrvaldada või vähendada niipalju kui võimalik potentsiaalselt kallutatud väljundite riski, mis võivad mõjutada edasiste toimingute sisendit (edaspidi „tagasisideahelad“) ning tagada, et selliseid tagasisideahelaid käsitletakse igakülgselt asjakohaste leevendusmeetmete kaudu.

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

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

Tehisintellektile iseloomulike nõrkuste käsitlemiseks kasutatavad tehnilised lahendused hõlmavad olenevalt asjaoludest meetmeid, millega hoida ära, avastada, tõrjuda, lahendada ja kontrollida ründeid, millega püütakse manipuleerida treenimisandmestikku („andmemürgitus“) või treenimisel kasutatavaid eeltreenitud komponente („mudelimürgitus“), sisendeid, mille eesmärk on panna tehisintellektimudel viga tegema („vastandnäited“ või „mudelist kõrvalehoidumine“), konfidentsiaalsusründeid või mudelivigu.

3. JAGU

SUURE RISKIGA TEHISINTELLEKTISÜSTEEMIDE PAKKUJATE JA JUURUTAJATE NING MUUDE OSALISTE KOHUSTUSED

Artikkel 16

Suure riskiga tehisintellektisüsteemide pakkujate kohustused

Suure riskiga tehisintellektisüsteemide pakkujad:

a) tagavad, et nende suure riskiga tehisintellektisüsteemid vastavad 2. jaos sätestatud nõuetele;

b) märgivad suure riskiga tehisintellektisüsteemile, või kui see ei ole võimalik, selle pakendile või kaasasolevatesse dokumentidesse vastavalt kas oma nime, registreeritud kaubanime või registreeritud kaubamärgi ning aadressi, millel saab nendega ühendust võtta;

c) võtavad kasutusele kvaliteedijuhtimissüsteemi, mis vastab artikli 17 nõuetele;

d) säilitavad dokumentatsiooni, millele on osutatud artiklis 18;

e) säilitavad oma suure riskiga tehisintellektisüsteemide automaatselt loodud logisid, kui need on nende kontrolli all, nagu on osutatud artiklis 19;

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

g) koostavad ELi vastavusdeklaratsiooni vastavalt artiklile 47;

h) kinnitavad suure riskiga tehisintellektisüsteemile CE-märgise, või kui see ei ole võimalik, siis selle pakendile või kaasasolevatele dokumentidele, et tõendada vastavust käesolevale määrusele kooskõlas artikliga 48;

i) täidavad artikli 49 lõikes 1 osutatud registreerimiskohustusi;

j) võtavad vajalikke parandusmeetmeid ja esitavad artiklis 20 nõutud teavet;

k) tõendavad riigi pädeva asutuse põhjendatud taotluse korral suure riskiga tehisintellektisüsteemi vastavust 2. jaos sätestatud nõuetele;

l) tagavad, et suure riskiga tehisintellektisüsteem vastab direktiivide (EL) 2016/2102 ja (EL) 2019/882 kohastele ligipääsetavusnõuetele.

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, menetlused ja süstemaatilised meetmed, mida kasutatakse suure riskiga tehisintellektisüsteemi projekteerimiseks, projekteerimise järelevalveks ja projektide kontrollimiseks;

c) meetodid, menetlused 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 valideerimismenetlused ning nende teostamise sagedus;

e) kohaldatavad tehnilised kirjeldused, sh standardid, ja juhul, kui asjaomaseid harmoneeritud standardeid ei kohaldata täies mahus või need ei hõlma kõiki 2. jaos sätestatud asjakohaseid nõudeid, siis ka vahendid, mida kasutatakse, et tagada suure riskiga tehisintellektisüsteemi vastavus kõnealustele nõuetele;

f) andmehalduse süsteemid ja menetlused, sealhulgas andmete hankimine, 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 72;

i) menetlused, mis on seotud tõsisest intsidendist teatamisega vastavalt artiklile 73;

j) suhtlemine riikide pädevate asutustega, teiste asjaomaste asutustega, sealhulgas nendega, kes pakuvad või toetavad juurdepääsu andmetele, teada antud asutustega, teiste operaatoritega, klientidega või muude huvitatud isikutega;

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

l) ressursside haldamine, sealhulgas 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. Pakkujad austavad igal juhul sellist rangusastet ja kaitsetaset, mis on vajalik, et tagada oma suure riskiga tehisintellektisüsteemide vastavus käesolevale määrusele.

3. Suure riskiga tehisintellektisüsteemide pakkujate jaoks, kes peavad täitma asjaomase valdkondliku liidu õiguse alusel kvaliteedijuhtimissüsteeme või samaväärset funktsiooni käsitlevaid kohustusi, võivad lõikes 1 loetletud aspektid olla osa kõnealuse õiguse kohastest kvaliteedijuhtimissüsteemidest.

4. Finantsasutustest pakkujate puhul, kes peavad täitma finantsteenuseid käsitleva liidu õiguse kohaseid nõudeid seoses nende sisemise juhtimissüsteemi, korra või protsessidega, loetakse kvaliteedijuhtimissüsteemi loomise kohustus, välja arvatud käesoleva artikli lõike 1 punktide g, h ja i osas, täidetuks, kui järgitakse nõudeid seoses sisemise juhtimissüsteemi, korra või protsessidega vastavalt finantsteenuseid käsitlevatele asjaomasele liidu õigusele. Seda silmas pidades võetakse arvesse artiklis 40 osutatud harmoneeritud standardeid.

Artikkel 18

Dokumentatsiooni säilitamine

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

a) artiklis 11 osutatud tehniline dokumentatsioon;

b) artiklis 17 osutatud kvaliteedijuhtimissüsteemi käsitlev dokumentatsioon;

c) kui see on kohaldatav, siis dokumendid muudatuste kohta, mille teada antud asutused on heaks kiitnud;

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

e) artiklis 47 osutatud ELi vastavusdeklaratsioon.

2. 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, mille tegevuskoht on riigi territooriumil, läheb pankrotti või lõpetab oma tegevuse enne selle ajavahemiku lõppu.

3. Finantsasutustest pakkujad, kes peavad täitma finantsteenuseid käsitleva liidu õiguse kohaseid nõudeid seoses nende sisemise juhtimissüsteemi, korra või protsessidega, säilitavad tehnilise dokumentatsiooni osana dokumentatsioonist, mida tuleb säilitada vastavalt asjaomasele finantsteenuseid käsitlevale liidu õigusele.

Artikkel 19

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. Ilma et see piiraks kohaldatava liidu või liikmesriigi õiguse kohaldamist, säilitatakse logisid suure riskiga tehisintellektisüsteemi sihtotstarbele vastava ajavahemiku jooksul, mis on vähemalt kuus kuud, välja arvatud juhul, kui kohaldatavas liidu või siseriiklikus õiguses, eelkõige isikuandmete kaitset käsitlevas liidu õiguses, on sätestatud teisiti.

2. Finantsasutustest pakkujad, kes peavad täitma finantsteenuseid käsitlevate liidu õiguse kohaseid nõudeid seoses nende sisemise juhtimissüsteemi, korra või protsessidega, säilitavad suure riskiga tehisintellektisüsteemide automaatselt genereeritud logisid osana dokumentatsioonist, mida tuleb säilitada vastavalt asjaomasele finantsteenuseid käsitlevale õigusele.

Artikkel 20

Parandusmeetmed ja teavitamiskohustus

1. 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, võtavad viivitamatult vajalikud parandusmeetmed, et viia süsteem vastavusse, võtta see turult tagasi, desaktiveerida või nõuda tagasi, nagu on asjakohane. Nad teavitavad sellest asjaomase suure riskiga tehisintellektisüsteemi turustajaid ning kohaldataval juhul juurutajaid, volitatud esindajat ja importijaid.

2. Kui suure riskiga tehisintellektisüsteem kujutab endast riski artikli 79 lõike 1 tähenduses ja pakkuja saab sellest riskist teada, peab ta viivitamata uurima selle põhjuseid koostöös aruandva juurutajaga, kui see on kohaldatav, ning teavitama turujärelevalveasutusi, kes on asjaomase suure riskiga süsteemi osas pädevad, ning kui see on kohaldatav, teada antud asutust, kes andis selle suure riskiga tehisintellektisüsteemi jaoks välja artikli 44 kohase sertifikaadi, esitades eelkõige teabe mittevastavuse laadi ja võetud asjakohaste parandusmeetmete kohta.

Artikkel 21

Koostöö pädevate asutustega

1. Suure riskiga tehisintellektisüsteemide pakkujad peavad pädeva asutuse põhjendatud taotluse korral esitama sellele asutusele kogu teabe ja dokumentatsiooni, mis on vajalik, et tõendada suure riskiga tehisintellektisüsteemi vastavust 2. jaos sätestatud nõuetele, tehes seda keeles, millest asutus saab kergesti aru ning mis on asjaomase liikmesriigi poolt osutatud üks liidu institutsioonide ametlikest keeltest.

2. Pädeva asutuse põhjendatud taotluse korral annavad pakkujad taotluse esitanud pädevale asutusele asjakohasel juhul ka juurdepääsu artikli 12 lõikes 1 osutatud suure riskiga tehisintellektisüsteemi automaatselt genereeritud logidele, kui sellised logid on nende kontrolli all.

3. Pädeva asutuse poolt käesoleva artikli kohaselt saadud teavet ja dokumentatsiooni käsitletakse kooskõlas artiklis 78 sätestatud konfidentsiaalsuskohustustega.

Artikkel 22

Suure riskiga tehisintellektisüsteemide pakkujate volitatud esindajad

1. Kolmandates riikides asutatud pakkujad peavad enne oma suure riskiga tehisintellektisüsteemide liidu turul kättesaadavaks tegemist määrama kirjaliku volitusega liidus asutatud volitatud esindaja.

2. Pakkuja võimaldab oma volitatud esindajal täita pakkujalt saadud volituses kindlaksmääratud ülesandeid.

3. Volitatud esindaja täidab pakkujalt saadud volituses kindlaksmääratud ülesandeid. Volitatud esindaja esitab turujärelevalveasutuste nõudmisel neile volituse koopia pädeva asutuse poolt osutatud liidu institutsioonide ühes ametlikus keeles. Käesoleva määruse kohaldamisel annab volitus volitatud esindajale õiguse täita järgmisi ülesandeid:

   a) kontrollida, et koostatud on artiklis 47 osutatud ELi vastavusdeklaratsioon ja artiklis 11 osutatud tehniline dokumentatsioon ning et pakkuja on teostanud asjakohase vastavushindamismenetluse;

   b) säilitada pädevate asutuste ja artikli 74 lõikes 10 osutatud riiklike asutuste või organite jaoks kättesaadavana kümne aasta jooksul pärast suure riskiga tehisintellektisüsteemi turule laskmist või kasutusele võtmist pakkuja kontaktandmed, mida kasutades on volitatud esindaja nimetatud, artiklis 47 osutatud ELi vastavusdeklaratsiooni koopia, tehnilise dokumentatsiooni, ning kui see on asjakohane, teada antud asutuse väljastatud sertifikaadi;

   c) esitada pädevale asutusele põhjendatud taotluse korral kogu teave ja dokumentatsioon, sealhulgas käesoleva lõigu punktis b osutatud teave ja dokumentatsioon, mis on vajalik, et tõendada suure riskiga tehisintellektisüsteemi vastavust 2. jaos sätestatud nõuetele, sealhulgas pakkuda juurdepääsu suure riskiga tehisintellektisüsteemi automaatselt genereeritud logidele, nagu on osutatud artikli 12 lõikes 1, niivõrd, kuivõrd sellised logid on pakkuja kontrolli all;

d) teha pädevate asutustega põhjendatud taotluse korral koostööd kõigis toimingutes, mida pädev asutus seoses suure riskiga tehisintellektisüsteemiga ette võtab; eelkõige selleks, et vähendada ja maandada suure riskiga tehisintellektisüsteemist tulenevaid riske;

e) täita kohaldataval juhul artikli 49 lõikes 1 osutatud registreerimiskohustusi, või kui registreerimise teeb pakkuja ise, tagada VIII lisa A. jao punktis 3 osutatud teabe õigsus.

Volitusega antakse volitatud esindajale õigus, et tema poole võivad pöörduda lisaks pakkujale või selle asemel, pädevad asutused kõigis küsimustes, mis on seotud käesoleva määruse järgimise tagamisega.

4. Volitatud esindaja peatab volituse, kui ta arvab või tal on põhjust arvata, et pakkuja tegevus on vastuolus tema käesolevast määrusest tulenevate kohustustega. Sellisel juhul teatab ta volituse lõpetamisest ja selle põhjustest viivitamata asjakohasele turujärelevalveasutusele ning kui see on kohaldatav, asjaomasele teada antud asutusele.

Artikkel 23

Importijate kohustused

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

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

b) pakkuja on koostanud tehnilise dokumentatsiooni kooskõlas artikliga 11 ja IV lisaga;

c) süsteemil on nõutav CE-märgis ning sellega on kaasas artiklis 47 osutatud ELi vastavusdeklaratsioon ja kasutusjuhendid;

d) pakkuja on määranud volitatud esindaja kooskõlas artikli 22 lõikega 1.

2. Kui importijal on piisavalt põhjust arvata, et suure riskiga tehisintellektisüsteem ei ole käesoleva määrusega vastavuses või on võltsitud või sellega on kaasas võltsitud dokumentatsioon, ei vii ta süsteemi turule enne, kui see on viidud määrusega vastavusse. Kui suure riskiga tehisintellektisüsteem kujutab endast riski artikli 79 lõike 1 tähenduses, teavitab importija sellest süsteemi pakkujat, volitatud esindajaid ja turujärelevalveasutusi.

3. Importijad märgivad oma nime, registreeritud kaubanime või registreeritud kaubamärgi ja aadressi, millel nendega saab suure riskiga tehisintellektisüsteemi teemal ühendust võtta, selle pakendile või kaasasolevatesse dokumentidesse, kui see on kohaldatav.

4. Importijad tagavad vastavalt asjaoludele, et sel ajal, kui suure riskiga tehisintellektisüsteem on nende vastutuse all, ei ohusta ladustamise ega transpordi tingimused kohaldataval juhul selle vastavust 2. jaos sätestatud nõuetele.

5. Importijad säilitavad kümne aasta jooksul pärast suure riskiga tehisintellektisüsteemi turule laskmist või kasutusele võtmist koopia teada antud asutuse väljastatud sertifikaadist, kui see on kohaldatav, kasutusjuhendist ning artiklis 47 osutatud ELi vastavusdeklaratsioonist.

6. Importijad esitavad asjakohasele pädevale asutusele põhjendatud taotluse korral neile kergesti arusaadavas keeles kogu teabe ja dokumentatsiooni, sealhulgas lõikes 5 osutatud teabe ja dokumentatsiooni, mis on vajalik, et tõendada suure riskiga tehisintellektisüsteemi vastavust 2. jaos sätestatud nõuetele. Seda silmas pidades tagavad nad ka selle, et nendele asutustele saab kättesaadavaks teha tehnilise dokumentatsiooni.

7. Importijad teevad asjakohaste pädevate asutustega koostööd kõigis toimingutes, mida need asutused võtavad ette seoses suure riskiga tehisintellektisüsteemiga, mille importijad on turule lasknud, eelkõige selleks, et vähendada ja maandada sellest tulenevaid riske.

Artikkel 24

Turustajate kohustused

1. Enne suure riskiga tehisintellektisüsteemi turul kättesaadavaks tegemist kontrollivad turustajad, et see kannab nõutavat CE-märgist, et sellega on kaasas koopia artiklis 47 osutatud ELi vastavusdeklaratsioonist ja kasutusjuhend ning et olenevalt asjaoludest on kas selle süsteemi pakkuja või importija täitnud oma vastavad kohustused, mis on sätestatud artikli 16 punktides b ja c ning artikli 23 lõikes 3.

2. Kui turustaja arvab või tal on põhjust tema käsutuses oleva teabe põhjal arvata, et suure riskiga tehisintellektisüsteem ei ole vastavuses 2. jaos 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 79 lõike 1 tähenduses, teavitab turustaja sellest süsteemi pakkujat või importijat, nagu on asjakohane.

3. Turustaja tagab, et sel ajal, kui suure riskiga tehisintellektisüsteem on tema vastutuse all, ei ohusta ladustamise ega transpordi tingimused kohaldataval juhul süsteemi vastavust 2. jaos sätestatud nõuetele.

4. Turustaja, kes arvab või kellel on põhjust tema käsutuses oleva teabe põhjal arvata, et suure riskiga tehisintellektisüsteem, mille ta on turul kättesaadavaks teinud, ei vasta 2. jaos sätestatud nõuetele, võtab parandusmeetmeid, mis on vajalikud, et viia süsteem nende nõuetega vastavusse, võtta see turult tagasi või nõuda tagasi, või tagab, et olenevalt asjaoludest kas pakkuja, importija või mõni asjaomane operaator võtab sellised parandusmeetmed. Kui suure riskiga tehisintellektisüsteem kujutab endast riski artikli 79 lõike 1 tähenduses, teavitab turustaja sellest viivitamata süsteemi pakkujat või importijat ja asjaomase suure riskiga tehisintellektisüsteemi osas pädevaid asutusi, esitades eelkõige üksikasjad mittevastavuse ja võimalike võetud parandusmeetmete kohta.

5. Asjakohase pädeva asutuse põhjendatud taotluse korral esitavad suure riskiga tehisintellektisüsteemi turustajad sellele asutusele kogu teabe ja dokumentatsiooni lõigete 1–4 kohaselt võetud meetmete kohta, mis on vajalik, et tõendada kõnealuse süsteemi vastavust 2. jaos sätestatud nõuetele.

6. Turustajad teevad asjakohaste pädevate asutustega koostööd kõigis toimingutes, mida need asutused võtavad ette seoses suure riskiga tehisintellektisüsteemiga, mille turustajad on turul kättesaadavaks teinud, eelkõige selleks, et vähendada või maandada sellest tulenevat riski.

Artikkel 25

Vastutus tehisintellekti väärtusahelas

1. Turustajat, importijat, juurutajat või muud kolmandat isikut käsitatakse käesoleva määruse kohaldamisel suure riskiga tehisintellektisüsteemi pakkujana ning tema suhtes kohaldatakse artiklist 16 tulenevaid pakkuja kohustusi mis 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 muul viisil jaotatud;

   b) nad teevad suure riskiga tehisintellektisüsteemi, mis on juba turule lastud või kasutusele võetud, olulise muudatuse viisil, et see jääb suure riskiga tehisintellektisüsteemiks vastavalt artiklile 6;

c) nad muudavad tehisintellektisüsteemi, sealhulgas üldotstarbelisse tehisintellektisüsteemi, mida ei ole liigitatud suure riskiga tehisintellektisüsteemiks ja mis on juba turule lastud või kasutusele võetud, sihtotstarvet, nii et asjaomasest tehisintellektisüsteemist saab suure riskiga tehisintellektisüsteem vastavalt artiklile 6.

2. Lõikes 1 osutatud asjaolude ilmnemise korral ei käsitata tehisintellektisüsteemi algselt turule lasknud või kasutusele võtnud pakkujat enam käesoleva määruse kohaldamisel selle konkreetse tehisintellektisüsteemi pakkujana. Kõnealune algne pakkuja teeb tihedat koostööd uute pakkujatega ning teeb kättesaadavaks vajaliku teabe ja annab mõistlikult eeldatava tehnilise juurdepääsu ja osutab muud abi, mida on vaja käesolevas määruses sätestatud kohustuste täitmiseks, eelkõige seoses suure riskiga tehisintellektisüsteemide vastavushindamise järgimisega. Käesolevat lõiget ei kohaldata juhul, kui algne pakkuja on selgelt täpsustanud, et tema tehisintellektisüsteemi ei tohi muuta suure riskiga tehisintellektisüsteemiks, ja seetõttu ei kohaldata tema suhtes dokumentide üleandmise kohustust.

3. Suure riskiga tehisintellektisüsteemide puhul, mis on selliste toodete turvakomponendid, mille suhtes kohaldatakse I lisa A jaos loetletud liidu ühtlustamisõigusakte, käsitatakse nende toodete valmistajat suure riskiga tehisintellektisüsteemi pakkujana ja ta peab täitma artikli 16 kohaseid kohustusi ühel järgmistest juhtudest:

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

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

4. Suure riskiga tehisintellektisüsteemi pakkuja ja kolmas isik, kes tarnib tehisintellektisüsteemi, vahendeid, teenuseid, komponente või protsesse, mida kasutatakse suure riskiga tehisintellektisüsteemis või mis on sellesse integreeritud, määravad tehnika üldtunnustatud tasemele tuginedes kirjaliku kokkuleppega kindlaks vajaliku teabe, võimekuse, tehnilise juurdepääsu ja või muu abi, et võimaldada suure riskiga tehisintellektisüsteemi pakkujal täielikult täita käesolevast määrusest tulenevaid kohustusi. Käesolevat lõiget ei kohaldata kolmandate isikute suhtes, kes teevad vaba ja avatud lähtekoodi litsentsi alusel avalikele vahenditele, teenustele, protsessidele või komponentidele kättesaadavaks muud kui üldotstarbelised tehisintellektimudelid.

Tehisintellektiamet võib välja töötada ja soovitada vabatahtlikke näidis-lepingutingimusi kasutamiseks suure riskiga tehisintellektisüsteemide pakkujate ja kolmandate isikute vahel, kes pakuvad suure riskiga tehisintellektisüsteemides kasutatavaid või integreeritud vahendeid, teenuseid, komponente või protsesse. Vabatahtlike näidistingimuste väljatöötamisel peaks tehisintellektiamet arvesse võtma konkreetsetes sektorites või ärimudelites kohaldatavaid võimalikke lepingulisi nõudeid. Vabatahtlikud näidistingimused avaldatakse ja tehakse tasuta kättesaadavaks kergesti kasutatavas elektroonilises vormingus.

5. Lõiked 2 ja 3 ei piira vajadust järgida ja kaitsta intellektuaalomandi õigusi, konfidentsiaalset äriteavet ja ärisaladusi kooskõlas liidu ja siseriikliku õigusega.

Artikkel 26

Suure riskiga tehisintellektisüsteemide juurutajate kohustused

1. Suure riskiga tehisintellektisüsteemide juurutajad võtavad asjakohaseid tehnilisi ja organisatsioonilisi meetmeid eesmärgiga tagada, et nad kasutavad selliseid süsteeme vastavalt süsteemiga kaasas olevale kasutusjuhendile kooskõlas lõigetega 3 ja 6.

2. Juurutajad annavad inimjärelevalve ülesande sellistele füüsilistele isikutele, kellel on vajalik pädevus, väljaõpe ja vastavad volitused ning vajalikud tugistruktuurid.

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

4. Niivõrd, kuivõrd juurutajal on kontroll sisendandmete üle, tagab see juurutaja, et sisendandmed on suure riskiga tehisintellektisüsteemi sihtotstarbe seisukohast asjakohased ja piisavalt esinduslikud, ilma et see piiraks lõigete 1 ja 2 kohaldamist.

5. Juurutajad tegelevad suure riskiga tehisintellektisüsteemi toimimise seirega kasutusjuhendi alusel ja asjakohasel juhul teavitavad pakkujaid vastavalt artiklile 72. Kui juurutajatel on põhjust arvata, et kasutusjuhendi kohase kasutamise tulemusena võib suure riskiga tehisintellektisüsteem kujutada endast riski artikli 79 lõike 1 tähenduses, teavitavad nad põhjendamatu viivituseta pakkujat või turustajat ja asjaomast turujärelevalveasutust ning peatavad selle süsteemi kasutamise. Kui juurutajad on tuvastanud tõsise intsidendi, teavitavad nad sellest intsidendist viivitamata ka kõigepealt pakkujat ning seejärel importijat või turustajat ja asjaomaseid turujärelevalveasutusi. Kui juurutaja ei saa pakkujaga ühendust, kohaldatakse artiklit 73 *mutatis mutandis*. See kohustus ei hõlma õiguskaitseasutustest tehisintellektisüsteemide juurutajate tundlikke operatiivandmeid.

Finantsasutustest juurutajate puhul, kes peavad täitma finantsteenuseid käsitleva liidu õiguse kohaseid nõudeid seoses nende sisemise juhtimissüsteemi, korra või protsessidega, loetakse esimeses lõigus sätestatud seirekohustus täidetuks, kui vastavalt finantsteenuseid käsitlevale asjaomasele õigusele on täidetud sisemise juhtimissüsteemi, protsesside ja mehhanismide alased nõuded.

6. Suure riskiga tehisintellektisüsteemide juurutajad säilitavad selle suure riskiga tehisintellektisüsteemi poolt automaatselt genereeritud logisid niivõrd, kuivõrd sellised logid on nende kontrolli all, ajavahemiku jooksul, mis vastab suure riskiga tehisintellektisüsteemi sihtotstarbele ning vähemalt kuue kuu jooksul, välja arvatud juhul, kui kohaldatavas liidu või siseriiklikus õiguses, eelkõige isikuandmete kaitset käsitlevas liidu õiguses on sätestatud teisiti.

Finantsasutustest juurutajad, kes peavad täitma finantsteenuseid käsitleva liidu õiguse kohaseid nõudeid seoses nende sisemise juhtimissüsteemi, korra või protsessidega, säilitavad logisid osana dokumentatsioonist, mida tuleb säilitada vastavalt finantsteenuseid käsitlevale asjaomasele liidu õigusele.

7. Enne suure riskiga tehisintellektisüsteemi kasutusele võtmist või kasutamist töökohal teavitavad tööandjatest juurutajad töötajate esindajaid ja mõjutatud töötajaid sellest, et nende suhtes hakatakse kasutama suure riskiga tehisintellektisüsteemi. See teave esitatakse kohaldataval juhul kooskõlas töötajate ja nende esindajate teavitamist käsitlevates liidu ja siseriiklikes õigusaktides ja tavades sätestatud õigusnormide ja menetlustega.

8. Suure riskiga tehisintellektisüsteemide juurutajad, kes on avaliku sektori asutused või liidu institutsioonid, organid või asutused, täidavad artiklis 49 osutatud registreerimiskohustusi. Kui sellised juurutajad leiavad, et suure riskiga tehisintellektisüsteem, mida nad kavatsevad kasutada, ei ole registreeritud ELi andmebaasis, millele on osutatud artiklis 71, siis nad seda süsteemi ei kasuta ning teavitavad pakkujat või turustajat.

9. Suure riskiga tehisintellektisüsteemide juurutajad kasutavad käesoleva määruse 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.

10. Ilma et see piiraks direktiivi (EL) 2016/680 kohaldamist, taotleb tagantjärele toimuvaks biomeetriliseks kaugtuvastamiseks mõeldud suure riskiga tehisintellektisüsteemi juurutaja kuriteo toimepanemises kahtlustatava või süüdi mõistetud isiku sihipärase otsingu raames selle süsteemi kasutamiseks eelnevalt või põhjendamatu viivituseta, kuid mitte hiljem kui 48 tunni jooksul luba õigusasutuselt või haldusasutuselt, kelle otsus on siduv ja mille suhtes kohaldatakse kohtulikku kontrolli, välja arvatud juhul, kui seda kasutatakse võimaliku kahtlustatava esmaseks tuvastamiseks kuriteoga otseselt seotud objektiivsete ja kontrollitavate faktide põhjal. Iga kasutamine piirdub sellega, mis on rangelt vajalik konkreetse kuriteo uurimiseks.

    Kui esimese lõigu kohane loataotlus lükatakse tagasi, peatatakse viivitamata taotletud loaga seotud tagantjärele toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine ja selle suure riskiga tehisintellektisüsteemi kasutamisega seotud isikuandmed, mille jaoks luba taotleti, kustutatakse.

Ühelgi juhul ei tohi sellist suure riskiga tehisintellektisüsteemi tagantjärele toimuvaks biomeetriliseks kaugtuvastamiseks kasutada õiguskaitse eesmärkidel kindla suunitluseta, ilma et see oleks mingil viisil seotud kuriteo, kriminaalmenetluse, kuriteo tegeliku ja olemasoleva või tegeliku ja prognoositava ohuga või konkreetse teadmata kadunud isiku otsimisega. Ühtki isiku suhtes kahjulikke õiguslikke tagajärgi põhjustavat otsust ei tohi teha üksnes tagantjärele toimuva biomeetrilise kaugtuvastamise süsteemi tulemuste põhjal.

Käesolev lõige ei piira määruse (EL) 2016/679 artikli 9 ja direktiivi (EL) 2016/680 artikli 10 kohaldamist biomeetriliste andmete töötlemisel.

Olenemata eesmärgist või juurutajast, dokumenteeritakse selliste suure riskiga tehisintellektisüsteemide iga kasutamine asjaomases politseitoimikus ning tehakse taotluse korral kättesaadavaks asjaomasele turujärelevalveasutusele ja riiklikule andmekaitseasutusele, välistades õiguskaitsega seotud tundlike operatiivandmete avalikustamise. Käesolev lõik ei piira direktiiviga (EL) 2016/680 järelevalveasutustele antud volitusi.

Juurutajad esitavad asjaomastele turujärelevalve- ja riiklikele andmekaitseasutustele aastaaruanded tagantjärele toimuva biomeetrilise tuvastamise süsteemide kasutamise kohta, välistades õiguskaitsega seotud tundlike operatiivandmete avalikustamise. Aruanded võib koondada nii, et need hõlmaksid rohkem kui ühte kasutamist.

Liikmesriigid võivad kooskõlas liidu õigusega kehtestada tagantjärele toimuva biomeetrilise kaugtuvastamise süsteemide kasutamise kohta piiravamaid õigusakte.

11. Ilma et see mõjutaks käesoleva määruse artikli 50 kohaldamist, teavitavad selliste III lisas osutatud suure riskiga tehisintellektisüsteemide juurutajad, mis teevad füüsiliste isikutega seotud otsuseid või aitavad neid otsuseid teha, füüsilisi isikuid sellest, et nende suhtes kasutakse suure riskiga tehisintellektisüsteemi. Õiguskaitse eesmärgil kasutatavate suure riskiga tehisintellektisüsteemide suhtes kohaldatakse direktiivi (EL) 2016/680 artiklit 13.

12. Juurutajad teevad asjakohaste pädevate asutustega koostööd kõigis toimingutes, mida kõnealused asutused võtavad ette seoses suure riskiga tehisintellektisüsteemiga käesoleva määruse rakendamiseks.

Artikkel 27

Põhiõigustele avaldatava mõju hindamine suure riskiga tehisintellektisüsteemide puhul

1. Enne artikli 6 lõikes 2 osutatud suure riskiga tehisintellektisüsteemi juurutamist, välja arvatud suure riskiga tehisintellektisüsteemide puhul, mis on ette nähtud kasutamiseks III lisa punktis 2 loetletud valdkonnas, hindavad juurutajad, kes on avalik-õiguslikud asutused või avalikke teenuseid osutavad eraõiguslikud üksused, ning III lisa punkti 5 alapunktides b ja c osutatud suure riskiga tehisintellektisüsteemide juurutajad põhiõigustele avalduvat mõju, mida sellise süsteemi kasutamine võib avaldada. Selleks viivad juurutajad läbi hindamise, mis hõlmab järgmist:

   a) juurutaja kirjeldus protsessidest, milles suure riskiga tehisintellektisüsteemi kasutatakse kooskõlas selle sihtotstarbega;

   b) viide ajavahemikule, mille jooksul iga suure riskiga tehisintellektisüsteemi kavatsetakse kasutada, ja kasutamise sagedus;

c) füüsiliste isikute ja rühmade kategooriad, keda süsteemi kasutamine konkreetses kontekstis tõenäoliselt mõjutab;

d) konkreetsed käesoleva lõike punkti c kohaselt kindlaks tehtud füüsiliste isikute või isikute rühmade kategooriaid mõjutada võiva kahju riskid, võttes arvesse pakkuja poolt artikli 13 kohaselt esitatud teavet;

e) inimjärelevalve meetmete rakendamise kirjeldus vastavalt kasutusjuhendile;

f) nende riskide realiseerumise korral võetavad meetmed, sealhulgas sisejuhtimise kord ja kaebuste esitamise mehhanismid.

2. Lõikes 1 sätestatud kohustus kehtib suure riskiga tehisintellektisüsteemi esimese kasutamise korral. Sarnastel juhtudel võib juurutaja tugineda varem läbi viidud põhiõiguste mõjuhinnangutele või olemasolevatele pakkuja tehtud mõjuhinnangutele. Kui juurutaja leiab suure riskiga tehisintellektisüsteemi kasutamise ajal, et mõni lõikes 1 loetletud elementidest on muutunud või ei ole enam ajakohane, võtab juurutaja vajalikud meetmed teabe ajakohastamiseks.

3. Kui käesoleva artikli lõikes 1 osutatud hindamine on tehtud, teavitab juurutaja turujärelevalveasutust selle tulemustest, esitades täidetuna käesoleva artikli lõikes 5 osutatud vormi teavituse osana. Artikli 46 lõikes 1 osutatud juhul võib juurutajad nimetatud teavitamiskohustusest vabastada.

4. Kui mõni käesolevas artiklis sätestatud kohustustest on määruse (EL) 2016/679 artikli 35 või direktiivi (EL) 2016/680 artikli 27 kohaselt tehtud andmekaitsealase mõjuhinnangu tulemusel juba täidetud, täiendab käesoleva artikli lõikes 1 osutatud põhiõiguste mõjuhinnang kõnealust andmekaitsealast mõjuhinnangut.

5. Tehisintellektiamet töötab välja küsimustiku vormi, sealhulgas automaatse vahendi abil, et hõlbustada juurutajatel täita käesolevast artiklist tulenevaid kohustusi lihtsustatud viisil.

4. JAGU

TEAVITAVAD ASUTUSED JA TEADA ANTUD ASUTUSED

Artikkel 28

Teavitavad asutused

1. Iga liikmesriik määrab või loob vähemalt ühe teavitava asutuse, kes vastutab vastavushindamisasutuste hindamise, määramise ja neist teavitamise ning nende järelevalve jaoks vajalike menetluste väljatöötamise ja läbiviimise eest. Nimetatud menetlused töötatakse välja kõigi liikmesriikide teavitavate asutuste koostöös.

2. Liikmesriigid võivad otsustada, et lõikes 1 osutatud hindamist ja järelevalvet teostab 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 78.

7. Teavitavatel asutustel on oma ülesannete nõuetekohaseks täitmiseks piisavalt pädevaid töötajaid. Pädevatel töötajatel on kohaldataval juhul oma ülesannete täitmiseks vajalikud eksperditeadmised infotehnoloogia, tehisintellekti ja õiguse, sealhulgas põhiõiguste järelevalve valdkonnas.

Artikkel 29

Vastavushindamisasutuse teavitamistaotlus

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

2. Teavitamistaotlusega koos esitatakse dokument, kus kirjeldatakse vastavushindamistoiminguid, vastavushindamismoodulit või -mooduleid ja tehisintellektisüsteemide liike, millega tegelemiseks väidab see vastavushindamisasutus end pädev olevat, ning riikliku akrediteerimisasutuse väljastatud akrediteerimistunnistus (kui see on olemas), mis tõendab, et vastavushindamisasutus vastab artiklis 31 sätestatud nõuetele.

   Lisatakse mis tahes kehtivad dokumendid, mis on seotud taotlust esitava teada antud asutuse olemasolevate määramistega mõne muu liidu ühtlustamisõigusakti alusel.

3. Kui vastavushindamisasutus ei saa akrediteerimistunnistust esitada, siis esitab ta teavitavale asutusele kõik dokumentaalsed tõendid, mis on vajalikud, et kontrollida, tunnistada ja korrapäraselt jälgida tema vastavust artiklis 31 sätestatud nõuetele.

4. Kui tegemist on teada antud 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. Teada antud asutus ajakohastab käesoleva artikli lõigetes 2 ja 3 osutatud dokumentatsiooni alati, kui tehakse asjakohaseid muudatusi, et teada antud asutuste eest vastutav asutus saaks jälgida ja kontrollida pidevat vastavust kõigile artiklis 31 sätestatud nõuetele.

Artikkel 30

Teavitamiskord

1. Teavitavad asutused võivad teavitada ainult neist vastavushindamisasutustest, mis vastavad artiklis 31 sätestatud nõuetele.

2. Teavitavad asutused kasutavad komisjoni ja teiste liikmesriikide teavitamiseks igast lõikes 1 osutatud vastavushindamisasutusest komisjoni välja töötatud ja hallatavat elektroonilist teavitamisvahendit.

3. Käesoleva artikli lõikes 2 nimetatud teavitus sisaldab kõiki üksikasju vastavushindamistoimingutest, vastavushindamismoodulist või -moodulitest ja asjaomastest tehisintellektisüsteemide liikidest ning asjakohast pädevuse kinnitust. Kui teavitus ei põhine artikli 29 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 31 sätestatud nõuetele.

4. Asjaomane vastavushindamisasutus võib teada antud asutuse toiminguid teha ainult juhul, kui komisjon või teised liikmesriigid ei esita vastuväiteid kahe nädala jooksul alates teavitava asutuse poolsest teavitamisest, kui teavitus sisaldab artikli 29 lõikes 2 osutatud akrediteerimistunnistust, või kahe kuu jooksul alates teavitava asutuse poolsest teavitamisest, kui teavitus sisaldab artikli 29 lõikes 3 osutatud dokumentaalseid tõendeid.

5. Kui esitatakse vastuväiteid, alustab komisjon viivitamata konsultatsioone asjaomaste liikmesriikide ja vastavushindamisasutusega. Komisjon otsustab neid konsultatsioone silmas pidades, kas luba on põhjendatud. Komisjon saadab oma otsuse asjaomasele liikmesriigile ja asjaomasele vastavushindamisasutusele.

Artikkel 31

Teada antud asutusi puudutavad nõuded

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

2. Teada antud asutused täidavad organisatsioonilisi, kvaliteedijuhtimise, ressursside ja protsessidega seotud nõudeid, mis on vajalikud nende ülesannete täitmiseks, ning vastavaid küberturvalisuse nõudeid.

3. Teada antud asutuste organisatsiooniline struktuur, vastutusalade jaotus, aruandlusahelad ja tegevus peavad tagama usalduse teada antud asutuste tegevuse ja nende teostatud vastavushindamistoimingute tulemuste suhtes.

4. Teada antud asutused peavad olema sõltumatud suure riskiga tehisintellektisüsteemi pakkujast, mille vastavushindamisega nad tegelevad. Samuti peavad teada antud asutused olema sõltumatud mis tahes muust operaatorist, kellel on majanduslik huvi hinnatava suure riskiga tehisintellektisüsteemi vastu, ja kõigist pakkuja konkurentidest. See ei välista vastavushindamisasutuse tegevuseks vajalike hinnatud suure riskiga tehisintellektisüsteemide kasutamist ega selliste suure riskiga tehisintellektisüsteemide kasutamist isiklikel eesmärkidel.

5. Vastavushindamisasutus, selle juhtkond ega selle vastavushindamisülesannete täitmise eest vastutavad töötajad ei tohi olla otseselt seotud suure riskiga tehisintellektisüsteemide projekteerimise, arendamise, turustamise või kasutamisega ega esindada ühtegi isikut, kes nimetatud tegevustega tegeleb. Nad ei tohi osaleda üheski tegevuses, mis võib olla vastuolus nende otsuste sõltumatuse ja vastavushindamistoimingute usaldusväärsusega, mille teostamiseks on neist teada antud. See kehtib eelkõige nõustamisteenuste puhul.

6. Teada antud asutuste töö korraldatakse ja neid juhitakse nii, et tagada nende tegevuse sõltumatus, objektiivsus ja erapooletus. Teada antud asutused dokumenteerivad ja rakendavad struktuuri ja menetlused, millega tagatakse erapooletus ning mille abil edendatakse ja kohaldatakse erapooletuse põhimõtteid kogu nende organisatsiooni, töötajate ja hindamistoimingute osas.

7. Teada antud asutustel peavad olema dokumenteeritud menetlused, millega tagatakse, et nende töötajad, komiteed, tütarettevõtjad, alltöövõtjad ja kõik nendega seotud asutused või väliste asutuste töötajad austavad kooskõlas artikliga 78 vastavushindamistoimingute teostamise käigus saadud teabe konfidentsiaalsust, välja arvatud juhul, kui avalikustamine on seadusega nõutud. Teada antud 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 teada antud asutus tegutseb.

8. Teada antud asutustel peavad olema menetlused selliste toimingute teostamiseks, milles võetakse asjakohaselt arvesse pakkuja suurust, tegutsemisvaldkonda, tema struktuuri ning asjaomase tehisintellektisüsteemi keerukuse astet.

9. Teada antud asutused peavad võtma endale asjakohase vastutuskindlustuse seoses oma vastavushindamistoimingutega, välja arvatud juhul, kui vastutust kannab liikmesriik, milles nad on asutatud, vastavalt selle liikmesriigi õigusele, või kui see liikmesriik vastutab ise otseselt vastavushindamise eest.

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

11. Teada antud asutustel peab olema piisav sisepädevus, et tulemuslikult hinnata väliste isikute poolt nende nimel täidetud ülesandeid. Teada antud asutusele peab olema alaliselt kättesaadav piisavalt haldus-, tehnilisi, õigus- ja teadustöötajaid, kellel on kogemused ja teadmised asjaomaste tehisintellektisüsteemide liikide, andmete ja andmetöötlusega ning seoses 2. jaos sätestatud nõuetega.

12. Teada antud asutused osalevad artiklis 38 osutatud koordineerimistegevuses. Samuti osalevad nad otseselt või esindajate kaudu Euroopa standardiorganisatsioonides või tagavad, et nad on asjakohastest standarditest teadlikud ja nende viimase arenguga kursis.

Artikkel 32

Eeldatav vastavus teada antud asutusi puudutavatele nõuetele

Kui vastavushindamisasutus tõendab, et ta vastab sellistes asjakohastes harmoneeritud standardites või nende osades sätestatud kriteeriumidele, mille viited on avaldatud *Euroopa Liidu Teatajas*, eeldatakse, et ta vastab artiklis 31 sätestatud nõuetele niivõrd, kuivõrd kohaldatavad harmoneeritud standardid hõlmavad kõnealuseid nõudeid.

Artikkel 33

Teada antud asutuste tütarettevõtjad ja alltöövõtt

1. Kui teada antud asutus kasutab vastavushindamisega seotud ülesannete täitmiseks alltöövõtjat või tütarettevõtjat, tagab ta, et alltöövõtja või tütarettevõtja vastab artiklis 31 sätestatud nõuetele, ning teatab sellest teavitavale asutusele.

2. Teada antud asutus vastutab täielikult kõigi alltöövõtjate või tütarettevõtjate poolt täidetud ülesannete eest.

3. Alltöövõtjat või tütarettevõtjat võib kasutada ainult pakkuja nõusolekul. Teada antud asutused teevad oma tütarettevõtjate loetelu üldsusele kättesaadavaks.

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 alltöövõtu lõpetamise kuupäevast.

Artikkel 34

Teada antud asutuste põhitegevusega seotud kohustused

1. Teada antud asutused kontrollivad suure riskiga tehisintellektisüsteemide vastavust artiklis 43 sätestatud vastavushindamismenetluse kohaselt.

2. Teada antud asutused väldivad oma ülesannete täitmisel pakkujate liigset koormamist ning võtavad nõuetekohaselt arvesse pakkuja suurust, tegutsemissektorit, struktuuri ja asjaomase suure riskiga tehisintellektisüsteemi keerukuse astet, pidades eelkõige silmas halduskoormuse ja nõuete täitmisega seotud kulude minimeerimist seoses mikro- ja väikeettevõtjate soovituse 2003/361/EÜ tähenduses. Teada antud asutus järgib siiski sellist rangust ja kaitse taset, mida on vaja, et tagada suure riskiga tehisintellektisüsteemi vastavus käesoleva määruse nõuetele.

3. Teada antud asutused teevad kättesaadavaks ja esitavad taotluse korral kogu asjakohase dokumentatsiooni, sealhulgas pakkuja dokumentatsiooni, artiklis 28 osutatud teavitavale asutusele, et sellel asutusel oleks võimalik teostada hindamis-, määramis-, teavitamis- ja järelevalvetoiminguid ning hõlbustada käesolevas jaos kirjeldatud hindamist.

Artikkel 35

Teada antud asutuste identifitseerimisnumbrid ja loetelud

1. Komisjon määrab igale teada antud asutusele ühe identifitseerimisnumbri, isegi kui asutusest on teada antud rohkem kui ühe liidu õigusakti alusel.

2. Komisjon teeb üldsusele kättesaadavaks asutuste loetelu, millest on käesoleva määruse alusel teada antud, mis sisaldab ka nende identifitseerimisnumbreid ja toiminguid, mille teostamiseks neist on teavitatud. Komisjon tagab, et see loetelu hoitakse ajakohasena.

Artikkel 36

Muudatused teavitustes

1. Teavitav asutus teavitab komisjoni ja teisi liikmesriike kõigist asjakohastest muudatustest teada antud asutuse teavituses artikli 30 lõikes 2 osutatud elektroonilise teavitamisvahendi kaudu.

2. Teavituse ulatuse laiendamise suhtes kohaldatakse artiklites 29 ja 30 sätestatud menetlusi.

   Muude kui teavituse ulatuse laiendamisega seotud muudatuste puhul kohaldatakse lõigetes 3–9 sätestatud menetlusi.

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

4. Kui teavitaval asutusel on piisavalt põhjust arvata, et teada antud asutus ei vasta enam artiklis 31 sätestatud nõuetele või et ta ei täida oma kohustusi, siis uurib teavitav asutus seda küsimust viivitamata ja äärmiselt hoolikalt. Seoses sellega teatab ta asjaomasele teada antud asutusele tekkinud vastuväidetest ja annab talle võimaluse esitada oma seisukohad. Kui teavitav asutus on jõudnud järeldusele, et teada antud asutus ei vasta enam artiklis 31 sätestatud nõuetele või et ta ei täida oma kohustusi, siis vastavalt vajadusele seab teavitav asutus määramisele piirangud või peatab või tühistab selle sõltuvalt nõuetele mittevastavuse või kohustuste mittetäitmise raskusastmest. Ta teatab sellest viivitamata komisjonile ja teistele liikmesriikidele.

5. Kui määramine on peatatud, piiratud või täielikult või osaliselt tühistatud, peab teada antud asutus asjaomaseid pakkujaid sellest teavitama kümne päeva jooksul.

6. Määramise piiramise, peatamise või tühistamise korral võtab teavitav asutus asjakohaseid meetmeid tagamaks, et asjaomase teada antud asutuse toimikud hoitakse alles ja tehakse teistes liikmesriikides asuvatele teavitavatele asutustele ja turujärelevalveasutustele nende taotluse alusel kättesaadavaks.

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

   a) hindab mõju teada antud asutuse väljastatud sertifikaatidele;

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

c) nõuab, et teada antud asutus peataks või tunnistaks riikliku asutuse määratud mõistliku aja jooksul kõik alusetult väljastatud sertifikaadid kehtetuks, et tagada turul olevate suure riskiga tehisintellektisüsteemide jätkuv nõuetele vastavus;

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

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

8. Välja arvatud alusetult väljastatud sertifikaatide puhul ning kui määramine on peatatud või piiratud, jäävad sertifikaadid kehtima ühel 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 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 teada antud asutus on suuteline järelevalvet jätkama ja jätkuvalt vastutama olemasolevate sertifikaatide eest, mis on välja antud peatamise või piirangu kehtivuse ajaks; juhul kui teavitatav asutus teeb kindlaks, et teada antud asutus ei ole suuteline olemasolevate väljastatud sertifikaatide eest vastutama, esitab sertifikaadiga hõlmatud süsteemi pakkuja oma registreeritud tegevuskoha liikmesriigi pädevatele asutustele kolme kuu jooksul alates peatamisest või piirangu kehtestamisest, et mõni teine kvalifitseeritud teada antud asutus võtab peatamise või piirangu kehtimise ajaks ajutiselt üle teada antud asutuse järelevalve ja sertifikaatide eest vastutamisega seotud ülesanded.

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

a) selle liikmesriigi pädev asutus, kus on sertifikaadiga hõlmatud kõrge riskiga tehisintellektisüsteemi pakkuja registreeritud tegevuskoht, on kinnitanud, et asjaomaste suure riskiga tehisintellektisüsteemidega ei kaasne riski tervisele, ohutusele ega põhiõigustele, ning

b) mõni teine teada antud asutus on kirjalikult kinnitanud, et ta võtab üle otsese vastutuse nende tehisintellektisüsteemide eest ning viib nende hindamise lõpule 12 kuu jooksul alates määramise kehtetuks tunnistamisest.

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

Riigi pädev asutus või teada antud asutus, kes täidab selle teada antud asutuse ülesandeid, keda määramise muutmine puudutab, teavitab sellest viivitamata komisjoni, teisi liikmesriike ja teisi teada antud asutusi.

Artikkel 37

Teada antud asutuste pädevuse vaidlustamine

1. Komisjon uurib vajaduse korral kõiki juhtumeid, mille puhul on põhjust kahelda teada antud asutuse pädevuses või artiklis 31 sätestatud nõuete ja kohaldatavate kohustuste jätkuvas täitmises teada antud asutuse poolt.

2. Teavitav asutus annab komisjonile taotluse alusel kogu teabe asjaomase teada antud asutuse teavitamise või pädevuse säilitamise kohta.

3. Komisjon tagab, et käesoleva artikli kohase uurimise käigus saadud tundlikku teavet käsitatakse konfidentsiaalsena kooskõlas artikliga 78.

4. Kui komisjon on veendunud, et teada antud asutus ei täida või enam ei täida teavitamise aluseks olevaid nõudeid, teatab ta sellest teavitavale liikmesriigile ning nõuab, et see võtaks vajalikke parandusmeetmeid, sealhulgas vajaduse korral peataks teavituse või võtaks selle tagasi. Kui liikmesriik ei võta vajalikke parandusmeetmeid, võib komisjon rakendusaktiga määramise peatada, kehtetuks tunnistada või seda piirata. Kõnealune rakendusakt võetakse vastu kooskõlas artikli 98 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 38

Teada antud asutuste koordineerimine

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

2. Iga teavitav asutus tagab oma teada antud asutuste osalemise lõikes 1 osutatud rühma töös otseselt või määratud esindajate vahendusel.

3. Komisjon tagab teadmiste ja parimate tavade vahetamise teavitavate asutuste vahel.

Artikkel 39

Kolmandate riikide vastavushindamisasutused

Sellise kolmanda riigi õiguse alusel asutatud vastavushindamisasutustel, kellega liit on sõlminud lepingu, võidakse lubada tegutseda teada antud asutusena käesoleva määruse alusel, tingimusel et nad täidavad artiklis 31 sätestatud nõudeid või et nad tagavad võrdväärse vastavuse taseme.

5. JAGU

STANDARDID, VASTAVUSHINDAMINE, SERTIFIKAADID, REGISTREERIMINE

Artikkel 40

Harmoneeritud standardid ja standardimisdokumendid

1. Eeldatakse, et suure riskiga tehisintellektisüsteemid või üldotstarbelised tehisintellektimudelid, mis vastavad harmoneeritud standarditele või nende osadele, mille viited on avaldatud *Euroopa Liidu Teatajas* kooskõlas määrusega (EL) nr 1025/2012, on vastavuses käesoleva peatüki 2. jaos sätestatud nõuetega, või kui see on asjakohane, käesoleva määruse V peatüki 2. ja 3. jaos sätestatud kohustustega niivõrd, kuivõrd nimetatud standardid hõlmavad neid nõudeid või kohustusi.

2. Komisjon esitab kooskõlas määruse (EL) nr 1025/2012 artikliga 10 põhjendamatu viivituseta standardimistaotlused, mis hõlmavad kõiki käesoleva peatüki 2. jaos sätestatud nõudeid ja vajaduse korral käesoleva määruse V peatüki 2. ja 3. jaos sätestatud kohustusi hõlmavaid standardimistaotlusi. Standardimistaotluses nõutakse ka aruandlus- ja dokumenteerimisprotsesside tulemusi, et parandada tehisintellektisüsteemide ressursinäitajaid, näiteks vähendada suure riskiga tehisintellektisüsteemi energia- ja muude ressursside tarbimist selle olelusringi jooksul, ning üldotstarbeliste tehisintellektimudelite energiatõhuse tulemusi. Standardimistaotluse koostamisel konsulteerib komisjon nõukoja ja asjaomaste sidusrühmadega, sealhulgas nõuandva koguga.

Euroopa standardiorganisatsioonidele standardimistaotluse esitamisel täpsustab komisjon, et standardid peavad olema selged ja sidusad, sealhulgas kooskõlas standarditega, mis on välja töötatud eri sektorites I lisas loetletud kehtivate liidu ühtlustamisõigusaktidega hõlmatud toodete jaoks, ning nende eesmärk on tagada, et liidus turule lastud või kasutusele võetud suure riskiga tehisintellektisüsteemid või üldotstarbelised tehisintellektimudelid vastavad käesolevas määruses sätestatud asjakohastele nõuetele või kohustustele.

Komisjon palub Euroopa standardiorganisatsioonidel esitada tõendid selle kohta, et nad on andnud endast parima käesoleva lõike esimeses ja teises lõigus osutatud eesmärkide saavutamiseks kooskõlas määruse (EL) nr 1025/2012 artikliga 2.

3. Standardimisprotsessis osalejad püüavad edendada tehisintellekti investeerimist ja innovatsiooni, sealhulgas õiguskindluse suurendamise kaudu, ning liidu turu konkurentsivõimet ja kasvu, aitavad tugevdada ülemaailmset standardimisalast koostööd ja võtta arvesse tehisintellekti valdkonnas kehtivaid rahvusvahelisi standardeid, mis on kooskõlas liidu väärtuste, põhiõiguste ja huvidega, ning tõhustavad mitmeid sidusrühmi hõlmavat juhtimist, tagades huvide tasakaalustatud esindatuse ja kõigi asjaomaste sidusrühmade tõhusa osalemise kooskõlas määruse (EL) nr 1025/2012 artiklitega 5, 6 ja 7.

Artikkel 41

Ühtsed kirjeldused

1. Komisjonil võib võtta vastu rakendusakte, millega kehtestatakse ühtsed kirjeldused käesoleva peatüki 2. jaos sätestatud nõuete või vajaduse korral V peatüki 2. ja 3. jaos sätestatud kohustuste kohta, kui on täidetud järgmised tingimused:

   a) komisjon on esitanud määruse (EL) nr 1025/2012 artikli 10 lõike 1 kohaselt taotluse ühele või mitmele Euroopa standardiorganisatsioonile koostada harmoneeritud standard käesoleva peatüki 2. jaos sätestatud nõuete kohta või kui see on asjakohane, siis V peatüki 2. ja 3. jaos sätestatud kohustuste kohta, ning;

      i) ükski Euroopa standardiorganisatsioon ei ole taotlust vastu võtnud või

ii) kõnealust taotlust käsitlevaid harmoneeritud standardeid ei esitatud määruse (EL) nr 1025/2012 artikli 10 lõikes 1 sätestatud tähtaja jooksul või

iii) asjakohastes harmoneeritud standardites ei käsitleta piisavalt põhiõigustega seotud probleeme või

iv) harmoneeritud standardid ei vasta taotlusele ning

b) *Euroopa Liidu Teatajas* ei ole avaldatud ühtegi määruse (EL) nr 1025/2012 kohast viidet harmoneeritud standarditele, mis hõlmaks käesoleva peatüki 2. jaos sätestatud olulisi nõudeid või kui see on asjakohane, siis V peatüki 2. ja 3. jaos sätestatud kohustusi, ning tõenäoliselt sellist viidet mõistliku aja jooksul ei avaldata.

Ühtsete kirjelduste koostamisel konsulteerib komisjon artiklis 67 osutatud nõuandva koguga.

Käesoleva lõike esimeses lõigus osutatud rakendusaktid võetakse vastu kooskõlas artikli 98 lõikes 2 osutatud kontrollimenetlusega.

2. Enne rakendusakti eelnõu koostamist teavitab komisjon määruse (EL) nr 1025/2012 artiklis 22 osutatud komiteed sellest, et tema hinnangul on käesoleva artikli lõikes 1 sätestatud tingimused täidetud.

3. Eeldatakse, et suure riskiga tehisintellektisüsteemid või üldotstarbelised tehisintellektimudelid, mis vastavad lõikes 1 osutatud ühtsetele kirjeldustele või osale nimetatud kirjeldustest, on vastavuses käesoleva peatüki 2. jaos sätestatud oluliste nõuete või kui see on asjakohane, siis V peatüki 2. ja 3. jaos sätestatud kohustustega niivõrd, kuivõrd nimetatud ühtsed kirjeldused hõlmavad neid nõudeid.

4. Kui Euroopa standardiorganisatsioon võtab vastu harmoneeritud standardi ning see on esitatud komisjonile standardi viite avaldamiseks *Euroopa Liidu Teatajas*, hindab komisjon seda standardit kooskõlas määrusega (EL) nr 1025/2012. Kui harmoneeritud standardi viide avaldatakse *Euroopa Liidu Teatajas*, tunnistab komisjon kehtetuks lõikes 1 osutatud rakendusaktid või nende osad, mis hõlmavad samu nõudeid, mis on sätestatud käesoleva peatüki 2. jaos või kui see on asjakohane, siis samu kohustusi, mis on sätestatud V peatüki 2. ja 3. jaos.

5. Kui suure riskiga tehisintellektisüsteemide või üldotstarbeliste tehisintellektimudelite pakkujad ei täida lõikes 1 osutatud ühtseid kirjeldusi, peavad nad põhjendama, et nad on võtnud kasutusele käesoleva peatüki 2. jaos osutatud nõuetele või kui see on asjakohane, siis V peatüki 2. ja 3. jaos sätestatud kohustustele vähemalt samaväärsel tasemel vastavad tehnilised lahendused.

6. Kui liikmesriik on seisukohal, et ühtne spetsifikatsioon ei vasta täielikult käesoleva peatüki 2. jaos sätestatud nõuetele või kui see on asjakohane, siis V peatüki 2. ja 3. jaos sätestatud kohustustele, teatab ta sellest komisjonile, esitades üksikasjaliku selgituse. Komisjon hindab seda teavet ja võib asjakohasel juhul muuta rakendusakti, millega asjaomane ühtne spetsifikatsioon kehtestatakse.

Artikkel 42

Eeldatav vastavus teatavatele nõetele

1. Eeldatakse, et kui suure riskiga tehisintellektisüsteeme on treenitud ja testitud andmetega, mis kajastavad konkreetset geograafilist, käitumuslikku, kontekstipõhist ja funktsionaalset keskkonda, milles kasutamiseks on need süsteemid mõeldud, vastavad need süsteemid artikli 10 lõikes 4 sätestatud vastavatele nõuetele.

2. Eeldatakse, et suure riskiga tehisintellektisüsteemid, mis on sertifitseeritud või mille kohta on välja antud vastavusdeklaratsioon määruse (EL) 2019/881 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 kohaldatav, artiklis 41 osutatud ühtset kirjeldust, et tõendada III lisa punktis 1 loetletud suure riskiga tehisintellektisüsteemide vastavust 2. jaos sätestatud nõuetele, järgib pakkuja üht järgmistest vastavushindamismenetlustest, mis põhineb:

   a) VI lisas osutatud sisekontrollil või

   b) VII lisas osutatud kvaliteedijuhtimissüsteemi hindamisel ja tehnilise dokumentatsiooni hindamisel ning milles osaleb teada antud asutus.

   Tõendades suure riskiga tehisintellektisüsteemi vastavust 2. jaos sätestatud nõuetele, järgib pakkuja VII lisas sätestatud vastavushindamist järgmistel juhtudel:

   a) artiklis 40 osutatud harmoneeritud standardeid ei ole olemas ja artiklis 41 osutatud ühtsed kirjeldused ei ole kättesaadavad;

   b) pakkuja ei ole harmoneeritud standardit kohaldanud või on seda kohaldanud ainult osaliselt;

   c) punktis a osutatud ühtsed kirjeldused on olemas, kuid pakkuja ei ole neid kohaldanud;

d) punktis a osutatud harmoneeritud standardid või mõni neist on avaldatud piiranguga ja üksnes standardi selles osas, mida piirang puudutab.

VII lisas osutatud vastavushindamise jaoks võib pakkuja valida mis tahes teada antud asutuse. Kui aga suure riskiga tehisintellektisüsteemi kavatsevad kasutusele võtta õiguskaitse-, rände- või varjupaigaasutused või liidu institutsioonid, organid või asutused, tegutseb teada antud asutusena artikli 74 lõikes 8 või kohaldataval juhul lõikes 9 osutatud turujärelevalveasutus.

2. III lisa punktides 2–8 osutatud suure riskiga tehisintellektisüsteemide puhul järgivad pakkujad VI lisas osutatud sisekontrollil põhinevat vastavushindamist, mille korral ei ole teada antud asutuse osalemist ette nähtud.

3. I lisa A jaos loetletud liidu ühtlustamisõigusaktidega hõlmatud suure riskiga tehisintellektisüsteemide puhul, järgib pakkuja nende õigusaktide kohaselt nõutavat asjaomast vastavushindamismenetlust. Selliste suure riskiga tehisintellektisüsteemide suhtes kohaldatakse käesoleva peatüki 2. jaos 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.

Teada antud asutustel, kellest on teavitatud nende õigusaktide alusel, on selliseks hindamiseks õigus kontrollida, kas suure riskiga tehisintellektisüsteemid vastavad 2. jaos sätestatud nõuetele, tingimusel et nende teada antud asutuste vastavust artikli 31 lõigetes 4, 10 ja 11 sätestatud nõuetele on hinnatud nende õigusaktide kohase teavitamismenetluse raames.

Kui I 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 kohaldatav, artiklis 41 osutatud ühtseid kirjeldusi, mis hõlmavad kõiki käesoleva peatüki 2. osas sätestatud nõudeid.

4. Suure riskiga tehisintellektisüsteemidele, mis on juba läbinud vastavushindamise, tuleb teha uus vastavushindamine alati, kui süsteeme oluliselt muudetakse, olenemata sellest, kas muudetud süsteemi kavatsetakse edasi turustada või jätkab selle kasutamist praegune juurutaja.

   Kui tegemist on suure riskiga tehisintellektisüsteemiga, mis õpib edasi ka pärast turule laskmist või kasutusele võtmist, ei käsitata oluliste muudatustena suure riskiga tehisintellektisüsteemi ja selle toimimise muudatusi, mille pakkuja on eelnevalt esialgse vastavushindamise ajal määratlenud ja mis on osa IV lisa punkti 2 alapunktis f osutatud tehnilises dokumentatsioonis sisalduvast teabest;

5. Komisjonil on õigus võtta kooskõlas artikliga 97 vastu delegeeritud õigusaktid, et muuta VI ja VII lisa ajakohastades neid tehnika arengut silmas pidades.

6. Komisjonil on õigus võtta kooskõlas artikliga 97 vastu delegeeritud õigusaktid käesoleva artikli lõigete 1 ja 2 muutmiseks, et kohaldada III lisa punktides 2–8 osutatud suure riskiga tehisintellektisüsteemide suhtes VII lisas osutatud vastavushindamist või selle osi. Komisjon arvestab selliseid 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 teada antud asutustes.

Artikkel 44

Sertifikaadid

1. Teada antud asutuste poolt VII lisa kohaselt välja antavad sertifikaadid koostatakse keeles, mis on teada antud asutuse asutamisliikmesriigi asjaomastele asutustele kergesti arusaadav.

2. Sertifikaadid kehtivad nende märgitud ajavahemiku jooksul, mis ei ületa I lisaga hõlmatud tehisintellektisüsteemide puhul viit aastat ja III lisaga hõlmatud tehisintellektisüsteemide puhul nelja aastat. Pakkuja taotlusel võib sertifikaadi kehtivust pikendada korraga mitte rohkem kui viie aasta kaupa I lisaga hõlmatud tehisintellektisüsteemide puhul ja nelja aasta kaupa III lisaga hõlmatud tehisintellektisüsteemide puhul, võttes aluseks kohaldatavate vastavushindamismenetluste kohaselt tehtava uue hindamise. Sertifikaadi mis tahes lisad on kehtivad eeldusel, et sertifikaat kehtib.

3. Kui teada antud asutus leiab, et tehisintellektisüsteem ei vasta enam 2. jaos sätestatud nõuetele, peatab ta väljastatud sertifikaadi, tunnistab selle kehtetuks või kehtestab selle suhtes piirangud, võttes seejuures arvesse proportsionaalsuse põhimõtet, välja arvatud juhul, kui nimetatud nõuete täitmine tagatakse sellega, et süsteemi pakkuja võtab teada antud asutuse määratud asjakohase tähtaja jooksul asjakohaseid parandusmeetmeid. Teada antud asutus põhjendab oma otsust.

Teada antud asutuse otsuste, sealhulgas välja antud vastavussertifikaate käsitlevate otsuste vaidlustamiseks nähakse ette edasikaebamise kord.

Artikkel 45

Teada antud asutuste teavitamiskohustused

1. Teada antud asutused informeerivad teavitavat asutust järgmisest:

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

b) VII lisa nõuete kohaselt välja antud liidu tehnilise dokumentatsiooni hindamise sertifikaadi või kvaliteedijuhtimissüsteemi kinnituse tagasilükkamine, piiramine, peatamine või kehtetuks tunnistamine;

c) teavitamise ulatust või tingimusi mõjutavad asjaolud;

d) turujärelevalveasutustelt saadud teabenõuded vastavushindamistoimingute kohta;

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

2. Iga teada antud asutus informeerib teisi teada antud asutusi järgmisest:

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

b) liidu 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 teada antud asutus esitab teistele samu tehisintellektisüsteemide liike puudutavate samalaadsete vastavushindamistoimingutega tegelevatele teada antud asutustele asjakohase teabe negatiivsete ja taotluse korral ka positiivsete vastavushindamistulemuste kohta.

4. Teada antud asutused tagavad saadud teabe konfidentsiaalsuse kooskõlas artikliga 78.

Artikkel 46

Erand vastavushindamismenetlusest

1. Erandina artiklist 43 ja 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 ajavahemikuks, kuni toimuvad vajalikud vastavushindamismenetlused, võttes arvesse erandi aluseks olevaid erandlikke põhjuseid. Need menetlused viiakse lõpule põhjendamatu viivituseta.

2. 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. Kui lõikes 1 osutatud luba lükatakse tagasi, peatatakse suure riskiga tehisintellektisüsteemi kasutamine viivitamatult ning kõik sellise kasutamise tulemused ja väljundid jäetakse viivitamata kõrvale.

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

4. Kui ükski liikmesriik ega komisjon ei ole esitanud vastuväiteid liikmesriigi turujärelevalveasutuse lõike 1 kohaselt välja antud loa kohta 15 kalendripäeva jooksul alates lõikes 3 osutatud teabe kättesaamisest, loetakse luba põhjendatuks.

5. Kui 15 kalendripäeva jooksul alates lõikes 3 osutatud teabe kättesaamisest esitab mõni liikmesriik vastuväiteid mõne teise liikmesriigi turujärelevalveasutuse välja antud loa kohta või kui komisjon leiab, et luba on vastuolus liidu õigusega või et lõikes 3 osutatud liikmesriikide järeldus süsteemi vastavuse kohta ei ole põhjendatud, alustab komisjon viivitamata konsultatsioone asjaomase liikmesriigiga. Konsulteeritakse asjaomaste operaatoritega ning neil on võimalus esitada oma seisukohad. Komisjon otsustab seda arvesse võttes, kas luba on põhjendatud. Komisjon adresseerib oma otsuse asjaomasele liikmesriigile ning asjaomastele operaatoritele.

6. Kui komisjon leiab, et luba on põhjendamata, tunnistab asjaomase liikmesriigi turujärelevalveasutus selle kehtetuks.

7. Suure riskiga tehisintellektisüsteemide suhtes, mis on seotud I lisa A jaos loetletud liidu ühtlustamisõigusaktidega hõlmatud toodetega, kohaldatakse üksnes kõnealustes liidu ühtlustamisõigusaktides sätestatud erandeid vastavushindamisest.

Artikkel 47

ELi vastavusdeklaratsioon

1. Pakkuja koostab iga suure riskiga tehisintellektisüsteemi kohta kirjaliku masinloetava, füüsiliselt või e-allkirjastatud ELi vastavusdeklaratsiooni ja säilitab seda riigi pädevate asutuste jaoks kättesaadavana vähemalt kümne aasta jooksul pärast suure riskiga tehisintellektisüsteemi turule laskmist või kasutusele võtmist. ELi vastavusdeklaratsioonis nimetatakse, millise suure riskiga 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 2. jaos sätestatud nõuetele. ELi vastavusdeklaratsioon sisaldab V lisas sätestatud teavet ning see tõlgitakse keelde, mis on kergesti arusaadav nende liikmesriikide pädevatele asutustele, kus suure riskiga tehisintellektisüsteem turule lastakse või 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 kohaldatava liidu õiguse jaoks üks ainus ELi vastavusdeklaratsioon. Vastavusdeklaratsioon sisaldab kogu teavet, mida on vaja deklaratsiooniga seotud liidu ühtlustamisõigusaktide kindlakstegemiseks.

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

5. Komisjonil on õigus võtta kooskõlas artikliga 97 vastu delegeeritud õigusaktid, et muuta V lisa, ajakohastades selles lisas esitatud ELi vastavusdeklaratsiooni sisu, et lisada sinna elemente, mis muutuvad vajalikuks tulenevalt tehnika arengust.

Artikkel 48

CE-märgis

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

2. Digitaalselt pakutavate suure riskiga tehisintellektisüsteemide puhul kasutatakse digitaalset CE-märgist üksnes juhul, kui sellele on lihtne juurde pääseda liidese abil, mille kaudu kõnealusele süsteemile juurde pääsetakse, või kergesti juurdepääsetava masinloetava koodi või muude elektrooniliste vahendite kaudu.

3. CE-märgis kinnitatakse suure riskiga tehisintellektisüsteemile 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.

4. Kui see on kohaldatav, järgneb CE-märgisele artiklis 43 sätestatud vastavushindamismenetluste eest vastutava teada antud asutuse identifitseerimisnumber. Teada antud asutuse identifitseerimisnumbri kinnitab kas asutus ise või tema juhiste järgi pakkuja või pakkuja volitatud esindaja. Identifitseerimisnumber esitatakse ka kõigis reklaammaterjalides, kus on öeldud, et suure riskiga tehisintellektisüsteem vastab CE-märgise nõuetele.

5. Kui suure riskiga tehisintellektisüsteemide suhtes kohaldatakse muud liidu õigust, mis näeb samuti ette CE-märgise kinnitamise, peab CE-märgis viitama sellele, et suure riskiga tehisintellektisüsteem vastab ka selle muu õiguse nõuetele.

Artikkel 49

Registreerimine

1. Enne III lisas loetletud suure riskiga tehisintellektisüsteemi, välja arvatud III lisa punktis 2 osutatud suure riskiga tehisintellektisüsteemid, turule laskmist või kasutusele võtmist registreerib pakkuja või vajaduse korral volitatud esindaja ennast ja oma süsteemi artiklis 71 osutatud ELi andmebaasis.

2. Enne sellise suure riskiga tehisintellektisüsteemi turule laskmist või kasutusele võtmist, mille kohta pakkuja on vastavalt artikli 6 lõikele 3 teinud otsuse, et tegemist ei ole suure riskiga süsteemiga, registreerib pakkuja või kohaldataval juhul volitatud esindaja selle süsteemi artiklis 71 osutatud ELi andmebaasis.

3. Enne III lisas loetletud suure riskiga tehisintellektisüsteemi kasutuselevõttu või kasutamist, välja arvatud III lisa punktis 2 loetletud suure riskiga tehisintellektisüsteemide puhul, registreerivad end juurutajad, kes on avaliku sektori asutused, liidu institutsioonid, organid, ametid või asutused või nende nimel tegutsevad isikud, valivad süsteemi ja registreerivad selle kasutamise artiklis 71 osutatud ELi andmebaasis.

4. III lisa punktides 1, 6 ja 7 osutatud suure riskiga tehisintellektisüsteemide puhul õiguskaitse, rände, varjupaiga ja piirikontrolli haldamise valdkonnas toimub käesoleva artikli lõigetes 1, 2 ja 3 osutatud registreerimine artiklis 71 osutatud ELi andmebaasi turvalises mitteavalikus osas ning sisaldab üksnes järgmist teavet, nagu on asjakohane:

   a) VIII lisa A jao punktid 1–10, välja arvatud punktid 6, 8 ja 9;

   b) VIII lisa C jao punktid 1–3;

   c) VIII lisa B jao punktid 1–5 ning punktid 8 ja 9;

   d) IX lisa punktid 1, 2, 3 ja 5.

Ainult komisjonil ja artikli 74 lõikes 8 osutatud riiklikel asutustel on juurdepääs vastavatele käesoleva lõike esimeses lõigus loetletud ELi andmebaasi piiratud juurdepääsuga osadele.

5. III lisa punktis 2 osutatud suure riskiga tehisintellektisüsteemid registreeritakse riiklikul tasandil.

IV peatükk
Teatavate tehisintellektisüsteemide pakkujate ja juurutajate läbipaistvuskohustused

Artikkel 50

Teatavate tehisintellektisüsteemide pakkujate ja juurutajate läbipaistvuskohustused

1. Pakkujad tagavad, et füüsiliste isikutega vahetult suhtlema mõeldud tehisintellektisüsteeme projekteeritakse ja arendatakse selliselt, et asjaomastele füüsilistele isikutele antakse teada, et nad suhtlevad tehisintellektisüsteemiga, välja arvatud juhul, kui see on piisavalt 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 või 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. Tehisintellektisüsteemide, sealhulgas üldotstarbeliste tehisintellektisüsteemide pakkujad, kes loovad sünteetilist audio-, pildi-, video- või tekstisisu, tagavad, et tehisintellektisüsteemi väljundid on märgitud masinloetavas vormingus ja tuvastatavad kui kunstlikult loodud või manipuleeritud. Pakkujad tagavad, et nende tehnilised lahendused on tõhusad, koostalitlusvõimelised, töökindlad ja usaldusväärsed, niivõrd kui see on tehniliselt teostatav, võttes arvesse eri liiki sisu eripära ja piiranguid, rakendamise kulusid ja tehnika üldtunnustatud taset, mis võib olla kajastatud asjakohastes tehnilistes standardites. Seda kohustust ei kohaldata, kui tehisintellektisüsteemid täidavad standardse redigeerimise abifunktsiooni või ei muuda oluliselt juurutaja esitatud sisendandmeid või nende semantikat või kui see on seadusega lubatud kuritegude avastamiseks, tõkestamiseks, uurimiseks või nende eest vastutusele võtmiseks.

3. Emotsioonituvastussüsteemi või biomeetrilise liigitamise süsteemi juurutajad annavad süsteemi tööst teada füüsilistele isikutele, kes selle süsteemiga kokku puutuvad, ning töötlevad vajaduse korral isikuandmeid kooskõlas määrustega (EL) 2016/679 ja (EL) 2018/1725 ning direktiiviga (EL) 2016/680. Seda kohustust ei kohaldata biomeetriliseks liigitamiseks ja emotsioonide tuvastamiseks kasutatavate tehisintellektisüsteemide suhtes, mida on seadusega lubatud kasutada kuritegude avastamiseks, tõkestamiseks või uurimiseks, tingimusel et kolmandate isikute õiguste ja vabaduste kaitseks kohaldatakse asjakohaseid kaitsemeetmeid ja kooskõlas liidu õigusega.

4. Sellise tehisintellektisüsteemi juurutajad, mis loob või manipuleerib pildi-, audio- või videosisu, mis kujutab endast süvavõltsingut, avalikustavad, et sisu on kunstlikult loodud või manipuleeritud. Seda kohustust ei kohaldata, kui kasutamine on seadusega lubatud kuritegude avastamiseks, tõkestamiseks, uurimiseks või nende eest vastutusele võtmiseks. Kui sisu moodustab osa ilmselgelt kunstilisest, loomingulisest, satiirilisest, väljamõeldud või samalaadsest teosest või programmist, piirduvad käesolevas lõikes sätestatud läbipaistvuskohustused sellise loodud või manipuleeritud sisu olemasolu avalikustamisega asjakohasel viisil, mis ei takista teose kuvamist või kasutamist.

   Sellise tehisintellektisüsteemi juurutajad, mis loob või manipuleerib teksti, mis avaldatakse eesmärgiga teavitada üldsust avalikku huvi pakkuvatest küsimustest, avalikustavad, et tekst on kunstlikult loodud või manipuleeritud. Seda kohustust ei kohaldata, kui kasutamine on seadusega lubatud kuritegude avastamiseks, tõkestamiseks, uurimiseks või nende eest vastutusele võtmiseks või kui tehisintellekti loodud sisu on läbinud inimkontrolli või toimetuskontrolli ning kui sisu avaldamise eest kannab toimetuslikku vastutust füüsiline või juriidiline isik.

5. Lõigetes 1–4 osutatud teave esitatakse asjaomastele füüsilistele isikutele selgel ja eristataval viisil hiljemalt esimese suhtlemise või kokkupuute ajal. Teave peab vastama kohaldatavatele ligipääsetavusnõuetele.

6. Lõiked 1–4 ei mõjuta III peatükis sätestatud nõudeid ja kohustusi ega piira muude liidu või riigisiseses õiguses tehisintellektisüsteemide juurutajatele sätestatud läbipaistvuskohustuste kohaldamist.

7. Tehisintellektiamet julgustab ja hõlbustab tegevusjuhendite koostamist liidu tasandil, et lihtsustada kunstlikult loodud või manipuleeritud sisu avastamise ja märgistamisega seotud kohustuste tõhusat rakendamist. Komisjonil võib võtta vastu rakendusakte kõnealuste tegevusjuhendite heakskiitmiseks artikli 56 lõikes 6 sätestatud korras. Kui komisjon leiab, et juhend ei ole piisav, võib ta kooskõlas artikli 98 lõikes 2 sätestatud kontrollimenetlusega võtta vastu rakendusakti, milles määratakse kindlaks ühised õigusnormid kõnealuste kohustuste rakendamiseks.

V peatükk
Üldotstarbelised tehisintellektimudelid

1. JAGU
LIIGITAMISE REEGLID

Artikkel 51

Üldotstarbeliste tehisintellektimudelite liigitamine süsteemse riskiga üldotstarbeliseks tehisintellektimudeliks.

1. Üldotstarbeline tehisintellektimudel liigitatakse süsteemse riskiga üldotstarbeliseks tehisintellektimudeliks, kui see vastab ühele järgmistest tingimustest:

   a) sellel on suure mõjuga võimed, mida hinnatakse asjakohaste tehniliste vahendite ja meetodite, sealhulgas näitajate ja võrdlusaluste alusel;

b) komisjoni otsuse põhjal, *ex officio* või pärast teaduskomisjoni kvalifitseeritud hoiatusteadet, on tal XIII lisas sätestatud kriteeriume arvesse võttes võimed või mõju, mis on samaväärne punktis a sätestatuga.

2. Eeldatakse, et üldotstarbelisel tehisintellektimudelil on lõike 1 punkti a kohased suure mõjuga võimed, kui selle treenimiseks kasutatud arvutuste koondsumma, mida mõõdetakse ujukomatehetes, on suurem kui 10^{25}.

3. Komisjon võtab kooskõlas artikliga 97 vastu delegeeritud õigusaktid, et muuta käesoleva artikli lõigetes 1 ja 2 loetletud künniseid ning täiendada võrdlusaluseid ja näitajaid, võttes arvesse tehnoloogia arengut, näiteks algoritmide paranemist või tõhusamat riistvara, et need künnised kajastaksid tehnika taset.

Artikkel 52

Menetlus

1. Kui üldotstarbeline tehisintellektimudel vastab artikli 51 lõike 1 punktis a osutatud tingimusele, teavitab asjaomane pakkuja sellest komisjoni viivitamata ja igal juhul kahe nädala jooksul pärast selle nõude täitmist või teadasaamist, et nõue täidetakse. Kõnealune teade sisaldab teavet, mis on vajalik tõendamaks, et asjaomane nõue on täidetud. Kui komisjon saab teada üldotstarbelisest tehisintellektimudelist, millega kaasnevad süsteemsed riskid, millest teda ei ole teavitatud, võib ta otsustada liigitada selle süsteemse riskiga mudeliks.

2. Artikli 51 lõike 1 punktis a osutatud nõudele vastava üldotstarbelise tehisintellektimudeli pakkuja võib koos teatega esitada piisavalt põhjendatud väited tõendamaks, et kuigi üldotstarbeline tehisintellektimudel vastab sellele nõudele, ei kujuta see erandkorras oma erijoonte tõttu süsteemseid riske ja seetõttu ei tuleks see klassifitseerida süsteemse riskiga üldotstarbeliseks tehisintellektimudeliks.

3. Kui komisjon jõuab järeldusele, et lõike 2 kohaselt esitatud väited ei ole piisavalt põhjendatud ja asjaomane pakkuja ei suutnud tõendada, et üldotstarbeline tehisintellektimudel ei kujuta oma erijoonte tõttu süsteemseid riske, lükkab ta need väited tagasi ja üldotstarbelist tehisintellektimudelit käsitatakse süsteemse riskiga üldotstarbelise tehisintellektimudelina.

4. Komisjon võib liigitada üldotstarbelise tehisintellektimudeli süsteemseid riske kujutavaks mudeliks *ex officio* või pärast teaduskomisjonilt artikli 90 lõike 1 punkti a kohase kvalifitseeritud hoiatusteate saamist, põhinedes XIII lisas sätestatud kriteeriumidele.

   Komisjonil on õigus võtta kooskõlas artikliga 97 vastu delegeeritud õigusakte, et muuta XIII lisa, täpsustades ja ajakohastades selles lisas esitatud kriteeriume.

5. Pakkuja, kelle mudel on liigitatud artikli 4 kohaselt süsteemse riskiga üldotstarbeliseks tehisintellektimudeliks, põhjendatud taotluse korral võtab komisjon taotlust arvesse ja võib otsustada uuesti hinnata, kas seda üldotstarbelist tehisintellektimudelit saab siiski pidada süsteemseid riske kujutavaks mudeliks, põhinedes XIII lisas toodud kriteeriumidele. Selline taotlus peab sisaldama objektiivseid, üksikasjalikke ja uusi põhjuseid, mis on esile kerkinud pärast liigitamisotsust. Pakkujad võivad taotleda uut hindamist kõige varem kuus kuud pärast liigitamisotsuse tegemist. Kui komisjon otsustab pärast uuesti hindamist säilitada mudeli liigitamise süsteemse riskiga üldotstarbeliseks tehisintellektimudeliks, võivad pakkujad taotleda uuesti hindamist kõige varem kuus kuud pärast kõnealuse otsuse tegemist.

6. Komisjon tagab süsteemse riskiga üldotstarbeliste tehisintellektimudelite loetelu avaldamise ja ajakohastab seda, ilma et see piiraks vajadust järgida ja kaitsta intellektuaalomandi õigusi ja konfidentsiaalset äriteavet või ärisaladusi kooskõlas liidu ja riigisisese õigusega.

2. JAGU

ÜLDOTSTARBELISTE TEHISINTELLEKTIMUDELITE PAKKUJATE KOHUSTUSED

Artikkel 53

Üldotstarbeliste tehisintellektimudelite pakkujate kohustused

1. Üldotstarbeliste tehisintellektimudelite pakkujad:

a) koostavad mudeli tehnilise dokumentatsiooni, sealhulgas selle treenimis- ja testimisprotsessi ning hindamistulemuste kohta, mis sisaldab vähemalt XI lisas sätestatud teavet, et esitada see taotluse korral tehisintellektiametile ja riigi pädevatele asutustele, ning ajakohastavad seda;

b) koostavad teabe ja dokumentatsiooni ning teevad selle kättesaadavaks tehisintellektisüsteemide pakkujatele, kes kavatsevad integreerida üldotstarbelise tehisintellektimudeli oma tehisintellektisüsteemidesse, ning ajakohastavad seda. Ilma et see piiraks vajadust jälgida ja kaitsta intellektuaalomandi õigusi ja konfidentsiaalset äriteavet või ärisaladusi kooskõlas liidu ja riigisisese õigusega, peab teave ja dokumentatsioon:

i) võimaldama tehisintellektisüsteemide pakkujatel saada hea ülevaate üldotstarbelise tehisintellektimudeli võimetest ja piiridest ning täita oma käesolevast määrusest tulenevaid kohustusi, ning

ii) sisaldama vähemalt XII lisas loetletud elemente;

c) kehtestavad põhimõtted, et järgida autoriõiguse alast liidu õigust ja seotud õigusi ning eelkõige tuvastada ja järgida, sealhulgas tipptasemel tehnoloogia abil, direktiivi (EL) 2019/790 artikli 4 lõike 3 kohaselt väljendatud õiguste piiramist;

d) koostavad ja teevad üldsusele kättesaadavaks piisavalt üksikasjaliku kokkuvõtte üldotstarbelise tehisintellektimudeli treenimiseks kasutatud sisu kohta vastavalt tehisintellektiameti esitatud vormile.

2. Lõike 1 punktides a ja b sätestatud kohustusi ei kohaldata selliste tehisintellektimudelite pakkujate suhtes, mis lubatakse tarbimisse vaba ja avatud lähtekoodi litsentsi alusel, mis võimaldab mudelile juurdepääsu, selle kasutamist, muutmist ja turustamist, ning mille parameetrid, sealhulgas kaalud, teave mudeliarhitektuuri kohta ja teave mudeli kasutamise kohta, tehakse üldsusele kättesaadavaks. Seda erandit ei kohaldata süsteemse riskiga üldotstarbeliste tehisintellektimudelite suhtes.

3. Üldotstarbeliste tehisintellektimudelite pakkujad teevad käesolevast määrusest tulenevate pädevuste ja volituste kasutamisel vajaduse korral koostööd komisjoni ja riigi pädevate asutustega.

4. Üldotstarbeliste tehisintellektimudelite pakkujad võivad kuni harmoneeritud standardi avaldamiseni tugineda tegevusjuhenditele artikli 56 tähenduses, et tõendada käesoleva artikli lõikes 1 sätestatud kohustuste täitmist. Euroopa harmoneeritud standardi järgimine tagab pakkujatele kohustuste täidetuse eelduse niivõrd, kuivõrd need standardid hõlmavad neid kohustusi. Üldotstarbeliste tehisintellektimudelite pakkujad, kes ei järgi heakskiidetud tegevusjuhendit ega Euroopa harmoneeritud standardit, peavad tõendama nõuetele vastavust alternatiivsete asjakohaste meetodite abil, mida komisjon peab hindama.

5. XI lisa, eelkõige selle punkti 2 alapunktide d ja e järgimise hõlbustamiseks võib komisjon võtta kooskõlas artikliga 97 vastu delegeeritud õigusakte, et täpsustada mõõtmis- ja arvutusmeetodeid, pidades silmas võrreldava ja kontrollitava dokumentatsiooni võimaldamist.

6. Komisjon võib võtta kooskõlas artikli 97 lõikega 2 vastu delegeeritud õigusakte, et ajakohastada XI ja XIII lisa, arvestades tehnika arenguga.

7. Mis tahes käesoleva artikli kohaselt saadud teavet ja dokumentatsiooni, sealhulgas ärisaladusi, käsitletakse kooskõlas artiklis 78 sätestatud konfidentsiaalsuskohustustega.

Artikkel 54

Üldotstarbeliste tehisintellektimudelite pakkujate volitatud esindajad

1. Kolmandates riikides asutatud pakkujad peavad enne oma üldotstarbelise tehisintellektisüsteemi liidu turul kättesaadavaks tegemist määrama kirjaliku volitusega liidus asutatud volitatud esindaja.

2. Pakkuja võimaldab oma volitatud esindajal täita pakkujalt saadud volituses kindlaksmääratud ülesandeid.

3. Volitatud esindaja täidab pakkujalt saadud volituses kindlaksmääratud ülesandeid. Volitatud esindaja esitab tehisintellektiameti taotluse korral neile volituse koopia liidu institutsioonide ühes ametlikus keeles. Käesoleva määruse kohaldamisel annab volitus volitatud esindajale õiguse täita järgmisi ülesandeid:

   a) kontrollida, et pakkuja on koostanud XI lisas sätestatud tehnilise dokumentatsiooni ja täitnud kõik artiklis 53 ja kohaldataval juhul artiklis 55 osutatud kohustused;

   b) hoida XI lisas täpsustatud tehnilise dokumentatsiooni koopiat tehisintellektiameti ja riikide pädevate asutuste jaoks kättesaadavana kümne aasta jooksul pärast üldotstarbelise tehisintellektimudeli turule laskmist ning säilitada volitatud esindaja määranud pakkuja kontaktandmeid;

   c) esitada tehisintellektiametile põhjendatud taotluse korral kogu teave ja dokumentatsioon, sealhulgas punktis b osutatud teave ja dokumentatsioon, mida on vaja, et tõendada käesolevas peatükis sätestatud kohustuste täitmist;

   d) teha põhjendatud taotluse korral koostööd tehisintellektiameti ja pädevate asutustega kõigis meetmetes, mida nad võtavad seoses üldotstarbelise tehisintellektimudeliga, sealhulgas juhul, kui mudel on integreeritud liidus turule lastud või kasutusele võetud tehisintellektisüsteemidesse.

4. Volitusega antakse volitatud esindajale õigus, et tema poole võivad lisaks pakkujale või pakkuja asemel pöörduda tehisintellektiamet või pädevad asutused kõigis küsimustes, mis on seotud käesoleva määruse järgimise tagamisega.

5. Volitatud esindaja lõpetab volituse, kui ta arvab või tal on põhjust arvata, et pakkuja tegevus on vastuolus tema käesolevast määrusest tulenevate kohustustega. Sellisel juhul teavitab ta viivitamata ka tehisintellektiametit volituste lõppemisest ja selle põhjustest.

6. Käesolevas artiklis sätestatud kohustust ei kohaldata selliste üldotstarbeliste tehisintellektimudelite pakkujate suhtes, mis lubatakse tarbimisse vaba ja avatud lähtekoodiga litsentsi alusel, mis võimaldab mudelile juurdepääsu, selle kasutamist, muutmist ja levitamist ning mille parameetrid, sealhulgas kaalud, teave mudeliarhitektuuri kohta ja teave mudeli kasutamise kohta, tehakse üldsusele kättesaadavaks, välja arvatud juhul, kui üldotstarbeliste tehisintellektimudelitega kaasnevad süsteemsed riskid.

3. JAGU

SÜSTEEMSE RISKIGA ÜLDOTSTARBELISTE TEHISINTELLEKTIMUDELITE PAKKUJATE KOHUSTUSED

Artikkel 55

Süsteemse riskiga üldotstarbeliste tehisintellektimudelite pakkujate kohustused

1. Lisaks artiklis 53 ja 54 loetletud kohustustele on süsteemse riskiga üldotstarbeliste tehisintellektimudelite pakkujatel kohustus:

   a) hinnata mudelit vastavalt standarditud protokollidele ja vahenditele, mis kajastavad tehnika taset, sealhulgas mudeli vastandtestide läbiviimine ja dokumenteerimine, et teha kindlaks ja maandada süsteemseid riske;

   b) hinnata ja maandada liidu tasandil võimalikke süsteemseid riske, sealhulgas nende allikaid, mis võivad tuleneda süsteemse riskiga üldotstarbeliste tehisintellektimudelite arendamisest, turule laskmisest või kasutamisest;

   c) jälgida ja dokumenteerida asjakohast teavet tõsiste intsidentide ja nende kõrvaldamiseks võetavate võimalike parandusmeetmete kohta ning esitada see põhjendamatu viivituseta tehisintellektiametile ja vajaduse korral riikide pädevatele asutustele;

   d) tagada süsteemse riskiga üldotstarbelise tehisintellektimudeli ja mudeli füüsilise taristu piisav küberturvalisuse kaitse.

2. Süsteemse riskiga üldotstarbeliste tehisintellektimudelite pakkujad võivad kuni harmoneeritud standardi avaldamiseni tugineda tegevusjuhendile artikli 56 tähenduses, et tõendada käesoleva artikli lõikes 1 sätestatud kohustuste täitmist. Euroopa harmoneeritud standardi järgimine tagab pakkujatele kohustuste täidetuse eelduse niivõrd, kuivõrd need standardid hõlmavad neid kohustusi. Süsteemse riskiga üldotstarbeliste tehisintellektimudelite pakkujad, kes ei järgi heakskiidetud tegevusjuhendit ega Euroopa harmoneeritud standardit, peavad tõendama nõuetele vastavust alternatiivsete asjakohaste meetodite abil, mida komisjon peab hindama.

3. Käesoleva artikli kohaselt saadud teavet ja dokumentatsiooni, sealhulgas ärisaladusi, käsitletakse kooskõlas artiklis 78 sätestatud konfidentsiaalsuskohustustega.

4. JAGU

TEGEVUSJUHENDID

Artikkel 56

Tegevusjuhendid

1. Tehisintellektiamet julgustab ja hõlbustab tegevusjuhendite koostamist liidu tasandil, et aidata kaasa käesoleva määruse nõuetekohasele kohaldamisele, võttes arvesse rahvusvahelisi lähenemisviise.

2. Tehisintellektiameti ja nõukoja eesmärk on tagada, et tegevusjuhendid hõlmavad vähemalt artiklites 53 ja 55 sätestatud kohustusi, sealhulgas järgmisi küsimusi:

a) vahendid, millega tagatakse, et artikli 53 lõike 1 punktides a ja b osutatud teavet ajakohastatakse turu ja tehnoloogia arengut silmas pidades;

b) treenimisel kasutatava sisu kokkuvõtte piisav üksikasjalikkus;

c) süsteemsete riskide liigi ja olemuse, sealhulgas vajaduse korral nende allikate kindlaksmääramine liidu tasandil;

d) liidu tasandil süsteemsete riskide hindamise ja juhtimise meetmed, menetlused ja kord, sealhulgas nende dokumenteerimine, mis peab olema riskidega proportsionaalne, võtma arvesse nende tõsidust ja tõenäosust ning nende riskide käsitlemise konkreetseid probleeme, arvestades võimalikke viise, kuidas sellised riskid võivad tehisintellekti väärtusahelas tekkida ja realiseeruda.

3. Tehisintellektiamet võib kutsuda tegevusjuhendite koostamises osalema kõiki üldotstarbeliste tehisintellektimudelite pakkujaid ja asjaomaseid riikide pädevaid asutusi. Protsessi võivad toetada kodanikuühiskonna organisatsioonid, tööstus, akadeemilised ringkonnad ja muud asjaomased sidusrühmad, näiteks tootmisahela järgmise etapi pakkujad ja sõltumatud eksperdid.

4. Tehisintellektiameti ja nõukoja eesmärk on tagada, et tegevusjuhendites on selgelt esitatud nende erieesmärgid ja need sisaldavad kohustusi ja meetmeid, sealhulgas vajaduse korral peamisi tulemusnäitajaid, et tagada nende eesmärkide saavutamine, ning et neis võetakse nõuetekohaselt arvesse kõigi huvitatud isikute, sealhulgas mõjutatud isikute vajadusi ja huve liidu tasandil.

5. Tehisintellektiameti eesmärk on tagada, et tegevusjuhendites osalejad annaksid tehisintellektiametile korrapäraselt aru kohustuste täitmise, võetud meetmete ja nende tulemuste kohta, sealhulgas vajaduse korral mõõdetuna peamiste tulemusnäitajate alusel. Peamised tulemusnäitajad ja aruandluskohustused kajastavad eri osalejate suuruse ja suutlikkuse erinevusi.

6. Tehisintellektiamet ja nõukoda jälgivad ja hindavad korrapäraselt tegevusjuhendite eesmärkide saavutamist osalejate poolt ja nende panust käesoleva määruse nõuetekohasesse kohaldamisse. Tehisintellektiamet ja nõukoda hindavad, kas tegevusjuhendid hõlmavad artiklites 53 ja 55 sätestatud kohustusi ning jälgivad ja hindavad korrapäraselt oma eesmärkide saavutamist. Nad avaldavad oma hinnangu tegevusjuhendite piisavuse kohta.

   Komisjon võib rakendusaktiga tegevusjuhendi heaks kiita ja seda liidus üldiselt kohaldada. Kõnealune rakendusakt võetakse vastu kooskõlas artikli 98 lõikes 2 osutatud kontrollimenetlusega.

7. Tehisintellektiamet võib kutsuda kõiki üldotstarbeliste tehisintellektimudelite pakkujaid tegevusjuhendeid järgima. Selliste üldotstarbeliste tehisintellektimudelite pakkujate puhul, millega ei kaasne süsteemseid riske, võib järgimine piirduda artiklis 53 sätestatud kohustustega, välja arvatud juhul, kui nad väljendavad selgesõnaliselt oma huvi kogu tegevusjuhendi järgimise vastu.

8. Tehisintellektiamet julgustab ja hõlbustab vajaduse korral ka tegevusjuhendite läbivaatamist ja kohandamist, pidades eelkõige silmas uusi standardeid. Tehisintellektiamet aitab hinnata olemasolevaid standardeid.

9. Tegevusjuhendid peavad olema valmis hiljemalt … [9 kuud pärast käesoleva määruse jõustumise kuupäeva]. Tehisintellektiamet võtab vajalikud meetmed, sealhulgas kutsub pakkujaid vastavalt lõikele 7 üles.

   Kui … [12 kuud pärast jõustumise kuupäeva] ei saa tegevusjuhendit lõplikult vormistada või kui tehisintellektiamet leiab, et see ei ole käesoleva artikli lõike 6 kohase hindamise põhjal piisav, võib komisjon näha rakendusaktidega ette ühised õigusnormid artiklites 53 ja 55 sätestatud kohustuste, sealhulgas käesoleva artikli lõikes 2 sätestatud küsimuste rakendamiseks. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 98 lõikes 2 osutatud kontrollimenetlusega.

VI peatükk
Innovatsiooni toetavad meetmed

Artikkel 57

Tehisintellekti regulatiivliivakastid

1. Liikmesriigid tagavad, et nende pädevad asutused loovad riiklikul tasandil vähemalt ühe tehisintellekti regulatiivliivakasti, mis hakkab toimima hiljemalt … [24 kuud pärast käesoleva määruse jõustumise kuupäeva]. Nimetatud regulatiivliivakasti võib luua ka koos teise liikmesriigi pädevate asutustega. Komisjon võib pakkuda tehnilist tuge, nõu ja vahendeid tehisintellekti regulatiivliivakastide loomiseks ja käitamiseks.

   Esimese lõigu kohast kohustust võib täita ka olemasolevas regulatiivliivakastis osalemisega, kui see osalemine tagab osalevatele liikmesriikidele samaväärse riikliku katvuse.

2. Samuti võib luua täiendavaid tehisintellekti regulatiivliivakaste piirkondlikul või kohalikul tasandil või ühiselt koos teiste liikmesriikidega.

3. Euroopa Andmekaitseinspektor võib samuti luua tehisintellekti regulatiivliivakasti liidu institutsioonidele, organitele ja asutustele ning täita riikide pädevate asutuste rolle ja ülesandeid kooskõlas käesoleva peatükiga.

4. Liikmesriigid tagavad, et lõigetes 1 ja 2 osutatud pädevad asutused eraldavad piisavalt vahendeid käesoleva artikli tõhusaks ja õigeaegseks täitmiseks. Kui see on asjakohane, teevad riikide pädevad asutused koostööd teiste asjaomaste asutustega ja võivad võimaldada muude tehisintellekti ökosüsteemis osalejate kaasamist. Käesolev artikkel ei mõjuta muid liidu või riigisisese õiguse alusel loodud regulatiivliivakaste. Liikmesriigid tagavad asjakohasel tasemel koostöö nende muude regulatiivliivakastide üle järelevalvet teostavate asutuste ja riigi pädevate asutuste vahel.

5. Lõike 1 kohaselt loodud tehisintellekti regulatiivliivakastid tagavad kontrollitud keskkonna, mis soodustab innovatsiooni ja hõlbustab tehisintellektisüsteemide arendamist, treenimist, testimist ja valideerimist piiratud aja jooksul enne nende turule laskmist või kasutusele võtmist spetsiaalse regulatiivliivakasti kava kohaselt, milles on kokku leppinud pakkujad või võimalikud pakkujad ja pädev asutus. Sellised liivakastid võivad hõlmata tegelikes tingimustes testimist, mille üle teostatakse järelevalvet selles liivakastis.

6. Pädevad asutused pakuvad vajaduse korral tehisintellekti regulatiivliivakasti raames suuniseid, järelevalvet ja tuge, et teha kindlaks riskid, mis avalduvad eelkõige põhiõigustele, tervisele ja ohutusele, testimisele, leevendusmeetmetele ja nende tulemuslikkusele seoses käesoleva määruse kohustuste ja nõuetega ning vajaduse korral muu liivakastis jälgitava liidu ja liikmesriikide õigusega.

7. Pädevad asutused annavad tehisintellekti regulatiivliivakastis osalevatele pakkujatele ja võimalikele pakkujatele suuniseid regulatiivsete ootuste ning käesolevas määruses sätestatud nõuete ja kohustuste täitmise kohta.

Tehisintellektisüsteemi pakkuja või võimaliku pakkuja taotluse korral esitab pädev asutus kirjaliku tõendi regulatiivliivakastis edukalt läbi viidud tegevuste kohta. Riigi pädev asutus esitab ka väljumisaruande, milles kirjeldatakse üksikasjalikult regulatiivliivakastis toimunud tegevusi ning sellega seotud tulemusi ja õpitulemusi. Pakkujad võivad kasutada sellist dokumentatsiooni, et tõendada oma vastavust käesolevale määrusele vastavushindamisprotsessi või asjakohaste turujärelevalvetoimingute kaudu. Sellega seoses võtavad turujärelevalveasutused ja teada antud asutused positiivselt arvesse riigi pädeva asutuse esitatud väljumisaruandeid ja kirjalikke tõendeid, et vastavushindamismenetlusi mõistlikul määral kiirendada.

8. Vastavalt artikli 78 konfidentsiaalsussätetele ning pakkuja või võimaliku pakkuja nõusolekul on komisjonil ja nõukojal õigus saada juurdepääs väljumisaruannetele ning nad võtavad neid asjakohasel juhul arvesse oma käesolevast määrusest tulenevate ülesannete täitmisel. Kui nii pakkuja või võimalik pakkuja kui ka riigi pädev asutus on sellega sõnaselgelt nõus, võib väljumisaruande teha käesolevas artiklis osutatud ühtse teabeplatvormi kaudu üldsusele kättesaadavaks.

9. Tehisintellekti regulatiivliivakastide loomise eesmärk on aidata kaasa järgmiste eesmärkide saavutamisele:

   a) õiguskindluse parandamine, et saavutada käesolevale määruse või vajaduse korral muu kohaldatava liidu ja riigisisese õiguse järgimine;

   b) parimate tavade jagamise toetamine tehisintellekti regulatiivliivakastis osalevate ametiasutustega tehtava koostöö kaudu;

c) innovatsiooni ja konkurentsivõime edendamine ning tehisintellekti ökosüsteemi arendamise hõlbustamine;

d) tõenduspõhisele regulatiivsele õppimisele kaasaaitamine;

e) tehisintellektisüsteemide liidu turule juurdepääsu hõlbustamine ja kiirendamine, eelkõige siis, kui neid pakuvad VKEd, sealhulgas idufirmad;

10. Riikide pädevad asutused tagavad, et niivõrd, kuivõrd innovatiivsed tehisintellektisüsteemid on seotud isikuandmete töötlemisega või kuuluvad muul moel muude selliste riiklike asutuste või pädevate asutuste järelevalve alla, kes pakuvad või toetavad juurdepääsu andmetele, on riiklikud andmekaitseasutused ja kõnealused muud riiklikud või pädevad asutused seotud tehisintellekti regulatiivliivakasti toimimisega ning osalevad oma asjakohaste ülesannete ja volituste ulatuses nende aspektide järelevalves.

11. Tehisintellekti regulatiivliivakastid ei mõjuta regulatiivliivakastide järelevalvega tegelevate pädevate asutuste järelevalve- või parandusvolitusi, sealhulgas piirkondlikul ega kohalikul tasandil. Kui selliste tehisintellektisüsteemide arendamise ja testimise käigus tehakse kindlaks oluline risk tervisele, ohutusele ja põhiõigustele, tuleb selle põhjal võtta asjakohaseid leevendusmeetmeid. Riikide pädevatel asutustel on õigus testimisprotsess ajutiselt või alaliselt peatada või regulatiivliivakastis osalemine peatada, kui tõhus leevendamine ei ole võimalik, ning nad teavitavad sellisest otsusest tehisintellektiametit. Riikide pädevad asutused kasutavad oma järelevalvevolitusi asjakohase õigusega ettenähtud piirides, kasutades konkreetse tehisintellekti regulatiivliivakasti projekti suhtes õigusnormide rakendamisel oma kaalutlusõigust, et toetada tehisintellektialast innovatsiooni liidus.

12. Tehisintellekti regulatiivliivakastis osalevad pakkujad ja võimalikud pakkujad vastutavad kohaldatava liidu ja riigisisese vastutust käsitleva õiguse alusel igasuguse kahju eest, mida regulatiivliivakastis toimuvad eksperimendid võivad kolmandatele isikutele tekitada. Juhul kui võimalikud pakkujad järgivad konkreetset plaani ja osalemise tingimusi ning järgivad heauskselt riigi pädeva asutuse antud juhiseid, ei kohalda kõnealused asutused siiski käesoleva rikkumise korral haldustrahve. Juhul kui muud pädevad asutused, kes vastutavad muu liidu ja riigisisese õiguse eest, osalesid aktiivselt regulatiivliivakastis testitava tehisintellektisüsteemi järelevalves ja andsid suuniseid nõuete täitmiseks, ei määrata selle õigusega seoses haldustrahve.

13. Tehisintellekti regulatiivliivakastid projekteeritakse ja rakendatakse nii, et need hõlbustavad piiriülest koostööd riikide pädevate asutuste vahel, kui see on asjakohane.

14. Riikide pädevad asutused koordineerivad oma tegevust ja teevad koostööd nõukojas.

15. Riikide pädevad asutused teavitavad tehisintellektiametit ja nõukoda regulatiivliivakasti loomisest ning võivad paluda neilt tuge ja suuniseid. Tehisintellektiamet teeb kavandatavate ja olemasolevate regulatiivliivakastide loetelu üldsusele kättesaadavaks ning ajakohastab seda, et soodustada tehisintellekti regulatiivliivakastides tihedamat suhtlust ja piiriülest koostööd.

16. Riikide pädevad asutused esitavad tehisintellektiametile ja nõukojale aastaaruanded ühe aasta möödumisel tehisintellekti regulatiivliivakasti loomisest ja seejärel igal aastal kuni selle tegevuse lõpetamiseni, ja lõpparuande. Nimetatud aruannetes esitatakse teave nende regulatiivliivakastide rakendamise edusammude ja tulemuste kohta, sealhulgas heade tavade, intsidentide, saadud kogemuste ja soovituste kohta seoses nende ülesehituse ning asjakohasel juhul ka käesoleva määruse, sealhulgas selle delegeeritud õigusaktide ja rakendusaktide kohaldamise ja võimaliku muutmise kohta ning muu sellise liidu õiguse kohaldamise kohta, mille üle pädevad asutused teevad regulatiivliivakastis järelevalvet. Riikide pädevad asutused teevad need aastaaruanded või nende kokkuvõtted üldsusele internetis kättesaadavaks. Komisjon võtab vajaduse korral aastaaruandeid arvesse oma käesolevast määrusest tulenevate ülesannete täitmisel.

17. Komisjon töötab välja ühtse ja sihtotstarbelise liidese, mis sisaldab kogu asjakohast teavet tehisintellekti regulatiivliivakastide kohta, et võimaldada sidusrühmadel tehisintellekti regulatiivliivakastidega suhelda ja esitada pädevatele asutustele päringuid ning küsida mittesiduvaid suuniseid tehisintellektitehnoloogiaid sisaldavate uuenduslike toodete, teenuste ja ärimudelite nõuetele vastavuse kohta, kooskõlas artikli 62 lõik 1 punktiga c. Komisjon kooskõlastab proaktiivselt oma tegevust riikide pädevate asutustega, kui see on asjakohane.

Artikkel 58

Tehisintellekti regulatiivliivakastide üksikasjalik kord ja toimimine

1. Selleks et vältida killustatust liidus, võtab komisjon vastu rakendusaktid, milles määratakse kindlaks tehisintellekti regulatiivliivakastide loomise, arendamise, rakendamise, käitamise ja järelevalve üksikasjalik kord. Nimetatud rakendusaktid sisaldavad ühiseid põhimõtteid järgmistes küsimustes:

   a) kõlblikkus- ja valikukriteeriumid tehisintellekti regulatiivliivakastis osalemiseks;

   b) tehisintellekti regulatiivliivakasti taotlemise, selles osalemise, selle seire, sellest väljumise ja selle lõpetamise kord, sealhulgas regulatiivliivakasti kava ja väljumisaruanne;

   c) osalejate suhtes kohaldatavad tingimused.

   Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 98 lõikes 2 osutatud kontrollimenetlusega.

2. Lõike 1 punktis b osutatud rakendusaktidega tagatakse,

   a) et tehisintellekti regulatiivliivakastid on avatud kõigile taotlevatele tehisintellektisüsteemi pakkujatele või võimalikele taotlevatele tehisintellektisüsteemi pakkujatele, kes vastavad kõlblikkus- ja valikukriteeriumidele, mis on läbipaistvad ja õiglased ning riikide pädevad asutused teavitavad taotlejaid oma otsusest kolme kuu jooksul alates taotluse esitamisest;

b) et tehisintellekti regulatiivliivakastid võimaldavad laialdast ja võrdset juurdepääsu ning vastavad osaleda soovijate nõudlusele; pakkujad või võimalikud pakkujad võivad esitada taotlusi ka partnerluses kasutajate ja muude asjaomaste kolmandate isikutega;

c) et tehisintellekti regulatiivliivakastide üksikasjalik kord ja tingimused toetavad võimalikult suurel määral riikide pädevate asutuste paindlikkust oma tehisintellekti regulatiivliivakastide loomisel ja käitamisel;

d) et VKEdel, sealhulgas idufirmadel on tasuta juurdepääs tehisintellekti regulatiivliivakastidele, ilma et see piiraks riikide pädevate asutuste õigust võtta erakorraliste kulude eest õiglast ja proportsionaalset tasu;

e) et need aitavad pakkujatel või võimalikel pakkujatel täita tehisintellekti regulatiivliivakasti väljundite abil käesolevast määrusest tulenevaid vastavushindamiskohustusi ja kohaldada vabatahtlikult artiklis 95 osutatud käitumisjuhendeid;

f) et tehisintellekti regulatiivliivakastid hõlbustavad tehisintellekti ökosüsteemi teiste asjaomaste osalejate, näiteks teada antud asutuste ja standardiorganisatsioonide, VKEde, sealhulgas idufirmade, ettevõtete, novaatorite, testimis- ja eksperimenteerimisrajatiste, teadus- ja katselaborite ja Euroopa digitaalse innovatsiooni keskuste, tippkeskuste, üksikute teadlaste kaasamist, et võimaldada ja hõlbustada koostööd avaliku ja erasektoriga;

g) et tehisintellekti regulatiivliivakasti taotlemise, valimise, selles osalemise ja sealt väljumise menetlused, protsessid ja haldusnõuded on lihtsad, kergesti mõistetavad ja selgelt edastatud, et hõlbustada piiratud õigus- ja haldussuutlikkusega VKEde, sealhulgas idufirmade osalemist, ning need ühtlustatakse kogu liidus, et vältida killustatust ja tagada, et liikmesriigi või Euroopa Andmekaitseinspektori loodud tehisintellekti regulatiivliivakastis osalemist tunnustatakse vastastikku ja ühetaoliselt ning sellel on kogu liidus ühesugune õiguslik mõju;

h) et tehisintellekti regulatiivliivakastis osalemine piirdub ajavahemikuga, mis on projekti keerukuse ja ulatuse seisukohast asjakohane ning mida riigi pädev asutus võib pikendada;

i) et tehisintellekti regulatiivliivakastid hõlbustavad selliste vahendite ja taristu arendamist, mida kasutatakse regulatiivse õppimise seisukohast oluliste tehisintellektisüsteemide mõõtmete (nt täpsus, stabiilsus ja küberturvalisus) testimiseks, võrdlemiseks, hindamiseks ja selgitamiseks, samuti meetmete arendamist selleks, et minimeerida riske põhiõigustele ning ühiskonnale laiemalt.

3. Tehisintellekti regulatiivliivakastides osalevad võimalikud pakkujad, eelkõige VKEd ja idufirmad, suunatakse vajaduse korral kasutama juurutamiseelseid teenuseid, nagu suunised käesoleva määruse rakendamise kohta ning muud lisaväärtust andvad teenused, näiteks abi standardimisdokumentide koostamisel ja sertifitseerimisel, testimis- ja eksperimenteerimisrajatised, Euroopa digitaalse innovatsiooni keskused ja tippkeskused.

4. Kui riikide pädevad asutused kaaluvad tegelikes tingimustes testimise lubamist, mida jälgitakse käesoleva artikli alusel loodud tehisintellekti regulatiivliivakasti 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 59

Isikuandmete täiendav töötlemine tehisintellekti regulatiivliivakastis teatavate tehisintellektisüsteemide arendamiseks avalikes huvides

1. Muudel eesmärkidel seaduslikult kogutud isikuandmeid võib tehisintellekti regulatiivliivakastis töödelda üksnes teatavate tehisintellektisüsteemide arendamiseks, treenimiseks ja testimiseks liivakastis, kui on täidetud kõik järgmised tingimused:

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

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

      ii) keskkonna kõrgetasemeline kaitse ja kvaliteedi parandamine, elurikkuse kaitse, saastekaitse, rohepöörde meetmed, kliimamuutuste leevendamine ja kohanemismeetmed;

iii) energiasäästlikkus;

iv) transpordisüsteemide ja liikuvuse, elutähtsa taristu ja võrkude ohutus ja vastupidavus;

v) avaliku halduse ja avalike teenuste tõhusus ja kvaliteet;

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

c) olemas on mõjusad seiremehhanismid, et teha kindlaks, kas regulatiivliivakastis toimuvate eksperimentide ajal võib tekkida suuri riske andmesubjektide õigustele ja vabadustele, nagu on osutatud määruse (EL) 2016/679 artiklis 35 ja määruse (EL) 2018/1725 artiklis 39, ning reageerimismehhanismid, mis võimaldavad neid riske kiiresti maandada ja vajaduse korral andmete töötlemise peatada;

d) regulatiivliivakasti keskkonnas töödeldavad isikuandmed paiknevad funktsionaalselt eraldiseisvas, isoleeritud ja kaitstud andmetöötluskeskkonnas võimaliku pakkuja kontrolli all ning neile andmetele on juurdepääs ainult volitatud isikutel;

e) pakkujad võivad algselt kogutud teavet jagada ainult kooskõlas liidu andmekaitseõiguseega; regulatiivliivakastis kogutud mis tahes isikuandmeid väljaspool seda liivakasti jagada ei tohi;

f) isikuandmete töötlemine regulatiivliivakasti keskkonnas ei too kaasa andmesubjekte mõjutavaid meetmeid või otsuseid ega mõjuta nende isikuandmete kaitset käsitlevas liidu õiguses sätestatud õiguste kohaldamist;

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

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

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

j) regulatiivliivakasti keskkonnas arendatud tehisintellektiprojekti, selle eesmärkide ja oodatavate tulemuste lühiülevaade avaldatakse pädevate asutuste veebisaidil; see kohustus ei hõlma õiguskaitse-, piirikontrolli-, rände- või varjupaigaasutuste tegevusega seotud tundlikke operatiivandmeid.

2. 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 regulatiivliivakastides konkreetse liidu või liikmesriigi õiguse alusel ja samadel kumulatiivsetel tingimustel, millele on osutatud lõikes 1.

3. Lõige 1 ei piira liidu ega liikmesriigi sellise õiguse kohaldamist, mis välistab isikuandmete töötlemise muul otstarbel kui selles õiguses selgelt nimetatud eesmärkidel, samuti liidu või liikmesriigi sellise õiguse kohaldamist, millega kehtestatakse innovatiivsete tehisintellektisüsteemide arendamiseks, testimiseks või treenimiseks vajaliku isikuandmete töötlemise alus või mis tahes muu õiguslik alus, järgides isikuandmete kaitset käsitlevat liidu õigust.

Artikkel 60

Suure riskiga tehisintellektisüsteemide testimine tegelikes tingimustes väljaspool tehisintellekti regulatiivliivakaste

1. Suure riskiga tehisintellektisüsteemide testimist tegelikes tingimustes väljaspool tehisintellekti regulatiivliivakaste võivad teostada III lisas loetletud suure riskiga tehisintellektisüsteemide pakkujad või võimalikud pakkujad kooskõlas käesoleva artikliga ja vastavalt käesolevas artiklis osutatud tegelikes tingimustes testimise kavale, ilma et see piiraks artikli 5 kohaste keeldude kohaldamist.

   Komisjon määrab rakendusaktidega kindlaks tegelikes tingimustes testimise kava üksikasjalikud elemendid. Komisjon võtab need rakendusaktid vastu kooskõlas artikli 98 lõikes 2 osutatud kontrollimenetlusega.

Käesolev lõige ei piira nende liidu või riigisiseste õigusaktide kohaldamist, mis käsitlevad I lisas loetletud liidu ühtlustamisõigusaktidega hõlmatud toodetega seotud suure riskiga tehisintellektisüsteemide testimist tegelikes tingimustes.

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

3. Suure riskiga tehisintellektisüsteemide tegelikes tingimustes testimine käesoleva artikli alusel ei piira liidu või liikmesriigi õiguse kohaselt nõutava mis tahes eetilise kontrolli kohaldamist.

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 turujärelevalveasutusele, kus tegelikes tingimustes testimine läbi viiakse;

   b) selle liikmesriigi turujärelevalveasutus, kus tegelikes tingimustes testimine läbi viiakse, on tegelikes tingimustes testimise ja tegelikes tingimustes testimise kava heaks kiitnud; kui turujärelevalveasutus ei ole 30 päeva jooksul vastanud, loetakse tegelikes tingimustes testimise tingimused ja tegelikes tingimustes testimise kava heakskiidetuks; kui liikmesriigi õiguses ei ole vaikivat nõusolekut ette nähtud, on tegelikes tingimustes testimiseks jätkuvalt vaja luba;

c) pakkuja või võimalik pakkuja, välja arvatud III lisa punktides 1, 6 ja 7 osutatud õiguskaitse-, rände- ja varjupaigavaldkonna ning piirikontrollihalduse valdkonna suure riskiga tehisintellektisüsteemide ja III lisa punktis 2 osutatud suure riskiga tehisintellektisüsteemide pakkuja või võimalik pakkuja, on vastavalt artikli 71 lõikele 4 registreerinud tegelikes tingimustes testimise üleliidulise kordumatu ühtse identifitseerimisnumbriga ja IX lisas täpsustatud teabega; III lisa punktides 1, 6 ja 7 osutatud õiguskaitse-, rände- ja varjupaigavaldkonna ning piirikontrollihalduse valdkonna suure riskiga tehisintellektisüsteemide pakkuja või võimalik pakkuja on registreerinud tegelikes tingimustes testimise ELi andmebaasi turvalises mitteavalikus osas vastavalt artikli 49 lõike 4 punktile d üleliidulise kordumatu ühtse identifitseerimisnumbriga ja selles täpsustatud teabega; III lisa punktis 2 osutatud suure riskiga tehisintellektisüsteemide pakkuja või võimalik pakkuja on registreerinud tegelikes tingimustes testimise vastavalt artikli 49 lõikele 5;

d) tegelikes tingimustes testimist teostava pakkuja või võimaliku pakkuja on asutatud liidus või ta on määranud seadusliku esindaja, kes on asutatud liidus;

e) tegelikes tingimustes testimiseks kogutud ja töödeldud andmeid edastatakse kolmandatele riikidele üksnes siis, kui rakendatakse liidu õiguses ette nähtud asjakohaseid kaitsemeetmeid;

f) tegelikes tingimustes testimine ei kesta kauem, kui on vaja selle eesmärkide saavutamiseks, ja igal juhul mitte kauem kui kuus kuud, mida võib pikendada täiendava kuue kuu võrra tingimusel, et pakkuja või võimalik pakkuja teatab sellest eelnevalt turujärelevalveasutusele ja lisab selgituse sellise pikendamise vajalikkuse kohta;

g) tegelikes tingimustes testitavad subjektid, kes kuuluvad oma vanuse tõttu kaitsetusse gruppi, on asjakohaselt kaitstud;

h) kui pakkuja või võimalik pakkuja korraldab tegelikes tingimustes testimise koostöös ühe või mitme juurutaja või võimaliku juurutajaga, on neid juurutajaid teavitatud kõigist testimise aspektidest, mis on nende osalemisotsuse seisukohast olulised, ning neile on antud artiklis 13 osutatud asjakohased tehisintellektisüsteemi kasutusjuhendid; pakkuja või võimalik pakkuja ning juurutaja ja võimalik juurutaja sõlmivad lepingu, milles on täpsustatud nende rollid ja kohustused, et tagada vastavus käesoleva määruse ning muu kohaldatava liidu ja liikmesriikide õiguse sätetega, mis käsitlevad tegelikes tingimustes testimist;

i) tegelikes tingimustes testimise subjektid on andnud teadva nõusoleku vastavalt artiklile 61, või õiguskaitse puhul, kui teadva nõusoleku taotlemine takistaks tehisintellektisüsteemi testimist, ei avalda tegelikes tingimustes testimise ega selle tulemused testimise subjektidele negatiivset mõju ning pärast testi tegemist nende isikuandmed kustutatakse;

j) tegelikes tingimustes testimise üle teostavad reaalset järelevalvet pakkuja või võimalik pakkuja ning juurutajad või võimalikud juurutajad isikute abil, kellel on asjaomases valdkonnas sobiv kvalifikatsioon ning oma ülesannete täitmiseks vajalik suutlikkus ja väljaõpe ning vastavad volitused;

k) tehisintellektisüsteemi prognoose, soovitusi või otsuseid saab tulemuslikult tagasi võtta ja jätta tähelepanuta.

5. Kõik tegelikes tingimustes testimise subjektid või asjakohasel juhul nende seaduslikud esindajad võivad testimisest igal ajal, kahju kandmata ja selgitusi andmata lahkuda, võttes tagasi oma teadva nõusoleku, ja võivad nõuda oma isikuandmete kohest ja lõplikku kustutamist. Teadva nõusoleku tagasivõtmine ei mõjuta juba teostatud tegevusi.

6. Kooskõlas artikliga 75 annavad liikmesriigid oma turujärelevalveasutustele volitused nõuda pakkujatelt ja võimalikelt pakkujatelt teavet, teha etteteatamata kaug- või kohapealseid kontrolle ning kontrollida tegelikes tingimustes testimise läbiviimist ja sellega seotud suure riskiga tehisintellektisüsteeme. Turujärelevalveasutused kasutavad neid volitusi, et tagada tegelikes tingimustes testimise ohutu areng.

7. Igast tegelikes tingimustes testimise käigus tuvastatud tõsisest intsidendist teatatakse riiklikule turujärelevalveasutusele kooskõlas artikliga 73. Pakkuja või võimalik pakkuja võtab viivitamata leevendusmeetmeid, või kui see ei ole võimalik, siis peatab tegelikes tingimustes testimise kuni leevendamiseni, või vastasel korral lõpetab tegelikes tingimustes testimise. Pakkuja või võimalik pakkuja kehtestab sellise tegelikes tingimustes testimise lõpetamise puhuks menetluse tehisintellektisüsteemi viivitamatuks tagasinõudmiseks.

8. Pakkujad või võimalikud pakkujad teavitavad tegelikes tingimustes testimise peatamisest või lõpetamisest ja selle lõpptulemustest selle liikmesriigi turujärelevalveasutust, kus tegelikes tingimustes testimine läbi viiakse.

9. Pakkuja või võimalik pakkuja vastutab kohaldatava vastutust käsitleva liidu ja liikmesriigi õiguse alusel igasuguse tegelikes tingimustes testimise käigus tekitatud kahju eest.

Artikkel 61

Teadev nõusolek osalemiseks tegelikes tingimustes testimises väljaspool tehisintellekti regulatiivliivakaste

1. Artikli 60 kohaseks tegelikes tingimustes testimiseks võetakse testimise subjektidelt enne sellises testimises osalemist vabatahtlikult antud teadev nõusolek, mille nad annavad pärast seda, kui neile on igakülgselt antud täpset, selget, asjakohast ja arusaadavat teavet järgmise kohta:

   a) tegelikes tingimustes testimise olemus ja eesmärgid ning nende osalemisega seotud võimalikud ebamugavused;

   b) tingimused, mille alusel tegelikes tingimustes testimine läbi viiakse, sealhulgas testimise subjekti või subjektide osalemise eeldatav kestus;

   c) nende osalemisega seotud õigused ja tagatised, eelkõige õigus igal ajal keelduda tegelikes tingimustes testimisest ja õigus testimisest lahkuda, ilma et nad kannaks kahju või peaks andma selgitusi;

   d) tehisintellektisüsteemi prognooside, soovituste või otsuste tagasivõtmise või tähelepanuta jätmise kord;

   e) artikli 60 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 testimise subjektidele või nende seaduslikule esindajale.

Artikkel 62

Meetmed pakkujate ja juurutajate, eelkõige VKEde, sealhulgas idufirmade jaoks

1. Liikmesriigid teevad järgmist:

a) annavad VKEdele, sealhulgas idufirmadele, kellel on liidus registrijärgne asukoht või filiaal, eelisjuurdepääsu tehisintellekti regulatiivliivakastile, eeldusel et nad vastavad kõlblikkustingimustele ja valikukriteeriumidele; eelisjuurdepääs ei takista muudel VKEde, sealhulgas muude kui käesolevas lõikes osutatud idufirmade juurdepääsu tehisintellekti regulatiivliivakastile, tingimusel et nad vastavad ka kõlblikkustingimustele ja valikukriteeriumidele;

b) korraldavad VKEde, sealhulgas idufirmade, juurutajate ja asjakohasel juhul kohalike ametiasutuste vajadustest lähtuvaid konkreetseid teadlikkuse suurendamise üritusi ja koolitusi käesoleva määruse kohaldamise kohta;

c) kasutavad olemasolevaid spetsiaalseid kanaleid ja loovad asjakohasel juhul uusi kanaleid VKEde, sealhulgas idufirmade, juurutajate, muude innovaatorite ja asjakohasel juhul kohalike ametiasutustega suhtlemiseks, et anda nõu ja vastata päringutele käesoleva määruse rakendamise kohta, sealhulgas seoses osalemisega tehisintellekti regulatiivliivakastides;

d) lihtsustavad VKEde ja muude asjaomaste sidusrühmade osalemist standardimise arendamise protsessis.

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, turu suurusest ja muudest asjaomastest näitajatest.

3. Tehisintellektiamet teeb järgmist:

a) esitab standardvormid käesoleva määrusega hõlmatud valdkondade kohta, nagu nõukoda on oma taotluses täpsustanud;

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 63

Erandid konkreetsete operaatorite suhtes

1. Mikroettevõtjad soovituse 2003/361/EÜ tähenduses võivad täita käesoleva määruse artiklis 17 nõutud kvaliteedijuhtimissüsteemi teatavaid elemente lihtsustatud viisil, tingimusel et neil ei ole partnerettevõtjaid ega sidusettevõtjaid kõnealuse soovituse tähenduses. Selleks töötab komisjon välja suunised kvaliteedijuhtimissüsteemi elementide kohta, mida võib täita lihtsustatud viisil, võttes arvesse mikroettevõtjate vajadusi, ilma et see mõjutaks kaitsetaset ja suure riskiga tehisintellektisüsteemidele esitatavate nõuete täitmise vajadust.

2. Käesoleva artikli lõiget 1 ei tõlgendata nii, et see vabastaks need operaatorid muude käesolevas määruses sätestatud nõuete ja kohustuste täitmisest, sealhulgas artiklites 9, 10, 11, 12, 13, 14, 15, 72 ja 73 sätestatud nõuete ja kohustuste täitmisest.

VII peatükk
Juhtimine

1. JAGU
JUHTIMINE LIIDU TASANDIL

Artikkel 64

Tehisintellektiamet

1. Komisjon arendab liidu oskusteavet ja suutlikkust tehisintellekti valdkonnas tehisintellektiameti kaudu.

2. Liikmesriigid hõlbustavad tehisintellektiametile usaldatud ülesannete täitmist, nagu on kajastatud käesolevas määruses.

Artikkel 65

Euroopa tehisintellekti nõukoja loomine ja selle struktuur

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

2. Nõukojas on iga liikmesriigi kohta üks esindaja. Euroopa Andmekaitseinspektor osaleb vaatlejana. Tehisintellektiamet 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.

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

4. Liikmesriigid tagavad, et nende esindajad nõukojas:

   a) omavad oma liikmesriigis asjakohaseid pädevusi ja volitusi, et aidata aktiivselt kaasa nõukoja artiklis 66 osutatud ülesannete täitmisele;

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

   c) 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.

5. Liikmesriikide määratud esindajad võtavad kahekolmandikulise häälteenamusega vastu nõukoja kodukorra. Kodukorras sätestatakse eelkõige eesistuja valimise menetluse kord, tema volituste kestus ja tema ülesannete kirjeldus, üksikasjalik hääletuskord ning nõukoja ja selle allrühmade tegevuse korraldus.

6. Nõukoda moodustab kaks alalist allrühma, et luua platvorm turujärelevalveasutuste vaheliseks koostööks ja teavitada ametiasutusi turujärelevalve ja teada antud asutustega seotud küsimustes.

   Turujärelevalve alaline allrühm peaks käesoleva määruse kohaldamisel tegutsema halduskoostöörühmana (ADCO rühm) määruse (EL) 2019/1020 artikli 30 tähenduses.

   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 kutsuda vaatlejatena osalema artiklis 67 osutatud nõuandva kogu esindajaid.

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

8. Nõukoja eesistuja on üks liikmesriikide esindajatest. Tehisintellektiamet tagab nõukojale sekretariaaditeenused, kutsub eesistuja taotluse korral kokku koosolekud ja valmistab ette päevakorra vastavalt nõukoja käesolevast määrusest tulenevatele ülesannetele ja nõukoja kodukorrale.

Artikkel 66

Nõukoja ülesanded

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

a) aidata kaasa käesoleva määruse kohaldamise eest vastutavate pädevate riigiasutuste vahelisele koordineerimisele ning toetada koostöös asjaomaste turujärelevalveasutustega ja nende nõusolekul artikli 74 lõikes 11 osutatud turujärelevalveasutuste ühistegevust;

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

c) anda nõu käesoleva määruse rakendamisel, eelkõige seoses üldotstarbelisi tehisintellektimudeleid käsitlevate õigusnormide jõustamisega;

d) aidata kaasa haldustavade ühtlustamisele liikmesriikides, sealhulgas seoses artiklis 46 osutatud erandiga vastavushindamismenetlustest ning seoses artiklites 57, 59 ja 60 osutatud tehisintellekti regulatiivliivakastide toimimisega ja tegelikes tingimustes testimisega;

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

i) käitumisjuhendite ja tegevusjuhendite väljatöötamine ja kohaldamine vastavalt käesolevale määrusele ja komisjoni suunistele;

ii) käesoleva määruse hindamine ja läbivaatamine vastavalt artiklile 112, sealhulgas seoses artiklis 73 osutatud tõsistest intsidentidest teatamistega ja artiklis 71 osutatud ELi andmebaasi toimimisega, delegeeritud õigusaktide või rakendusaktide ettevalmistamisega seoses käesoleva määruse võimaliku vastavusse viimisega I lisas loetletud liidu ühtlustamisõigusaktidega;

iii) III peatüki 2. jaos sätestatud nõudeid käsitlevad tehnilised kirjeldused või olemasolevad standardid;

iv) artiklites 40 ja 41 osutatud harmoneeritud standardite või ühtsete kirjelduste kasutamine;

v) suundumused, nagu Euroopa ülemaailmne konkurentsivõime tehisintellekti valdkonnas, tehisintellekti levik liidus ja digioskuste arendamine;

vi) suundumused tehisintellekti väärtusahelate arenevas tüpoloogias, eelkõige seoses sellest tuleneva mõjuga vastutusele;

vii) võimalik vajadus muuta III lisa kooskõlas artikliga 7 ja võimalik vajadus artikli 5 võimalikuks läbivaatamiseks vastavalt artiklile 112, võttes arvesse asjakohaseid kättesaadavaid tõendeid ja tehnoloogia uusimaid arenguid;

f) toetada komisjoni, et edendada tehisintellektipädevust, üldsuse teadlikkust ja arusaamist tehisintellektisüsteemide kasutamisega seotud kasust, riskidest, kaitsemeetmetest ja õigustest ning kohustustest;

g) hõlbustada ühiste kriteeriumide väljatöötamist ning turuosaliste ja pädevate asutuste ühist arusaamist käesolevas määruses sätestatud asjakohastest mõistetest, sealhulgas aidates kaasa võrdlusaluste väljatöötamisele;

h) teha vajaduse korral koostööd teiste liidu institutsioonide, organite ja asutuste, samuti asjaomaste liidu eksperdirühmade ja võrgustikega, eelkõige tooteohutuse, küberturvalisuse, konkurentsi, digi- ja meediateenuste, finantsteenuste, tarbijakaitse, andmete ja põhiõiguste kaitse valdkonnas;

i) aidata kaasa tõhusale koostööle kolmandate riikide pädevate asutuste ja rahvusvaheliste organisatsioonidega;

j) abistada riikide pädevaid asutusi ja komisjoni käesoleva määruse rakendamiseks vajalike organisatsiooniliste ja tehniliste eksperditeadmiste väljatöötamisel, sealhulgas aidata hinnata käesoleva määruse rakendamises osalevate liikmesriikide töötajate koolitusvajadusi;

k) aidata tehisintellektiametil toetada riikide pädevaid asutusi tehisintellekti regulatiivliivakastide loomisel ja arendamisel ning hõlbustada koostööd ja teabevahetust tehisintellekti regulatiivliivakastide vahel;

l) teha kaastööd ja anda asjakohast nõu suunisdokumentide väljatöötamisel;

m) nõustada komisjoni tehisintellekti käsitlevates rahvusvahelistes küsimustes;

n) esitada komisjonile arvamusi üldotstarbelisi tehisintellektimudeleid käsitlevate kvalifitseeritud hoiatusteadete kohta;

o) saada liikmesriikidelt arvamusi üldotstarbeliste tehisintellektimudelitega seotud kvalifitseeritud hoiatusteadete ning tehisintellektisüsteemide seire ja jõustamise riiklike kogemuste ja tavade kohta, eelkõige üldotstarbelisi tehisintellektimudeleid integreerivate süsteemide puhul.

Artikkel 67

Nõuandev kogu

1. Luuakse nõuandev kogu, mis annab nõukojale ja komisjonile tehnilist oskusteavet ja nõustab neid, et aidata kaasa nende käesolevast määrusest tulenevate ülesannete täitmisele.

2. Nõuandva kogu liikmed esindavad tasakaalustatult valitud sidusrühmi, sealhulgas tööstussektorit, idufirmasid, VKEsid, kodanikuühiskonda ja akadeemilisi ringkondi. Nõuandva kogu liikmeskonna hulgas on tasakaalustatult esindatud ärihuvid ja ärivälised huvid ning ärihuvide kategoorias VKEde ja muude ettevõtjate huvid.

3. Komisjon nimetab nõuandva kogu liikmed kooskõlas lõikes 2 sätestatud kriteeriumidega sidusrühmade seast, kellel on tehisintellekti valdkonnas tunnustatud oskusteave.

4. Nõuandva kogu liikmete ametiaeg on kaks aastat, mida võib pikendada kuni neljaks aastaks.

5. Nõuandva kogu alalised liikmed on Euroopa Liidu Põhiõiguste Amet, ENISA, Euroopa Standardikomitee (CEN), Euroopa Elektrotehnika Standardikomitee (CENELEC) ja Euroopa Telekommunikatsioonistandardite Instituut (ETSI).

6. Nõuandev kogu kehtestab oma kodukorra. Nõuandev kogu valib oma liikmete hulgast vastavalt lõikes 2 sätestatud kriteeriumidele kaks kaasesimeest. Kaasesimeeste ametiaeg on kaks aastat ja seda võib pikendada ühe korra.

7. Nõuandev kogu peab koosolekuid vähemalt kaks korda aastas. Nõuandev kogu võib kutsuda oma koosolekutele eksperte ja muid sidusrühmi.

8. Nõuandev kogu võib nõukoja või komisjoni taotlusel koostada arvamusi, soovitusi ja kirjalikke seisukohti.

9. Nõuandev kogu võib vastavalt vajadusele moodustada alalisi või ajutisi allrühmi, mille eesmärk on uurida käesoleva määruse eesmärkidega seotud konkreetseid küsimusi.

10. Nõuandev kogu koostab oma tegevuse kohta aastaaruande. Aastaaruanne tehakse üldsusele kättesaadavaks.

Artikkel 68

Sõltumatutest ekspertidest koosnev teaduskomisjon

1. Komisjon kehtestab rakendusaktiga sätted, et luua sõltumatutest ekspertidest koosnev teaduskomisjon (edaspidi „teaduskomisjon“), mille eesmärk on toetada käesoleva määruse kohaseid täitmise tagamise toiminguid. Kõnealune rakendusakt võetakse vastu kooskõlas artikli 98 lõikes 2 osutatud kontrollimenetlusega.

2. Teaduskomisjon koosneb ekspertidest, kelle komisjon valib tehisintellekti valdkonnas ajakohaste teaduslike või tehniliste eksperditeadmiste alusel, mis on vajalikud lõikes 3 sätestatud ülesannete täitmiseks, ning ekspert peab tõendatult vastama kõikidele järgmistele tingimustele:

   a) omab tehisintellekti valdkonnas eriteadmisi ja pädevust ning teaduslikke või tehnilisi eksperditeadmisi;

   b) on sõltumatu tehisintellektisüsteemide või üldotstarbeliste tehisintellektimudelite pakkujatest;

   c) on võimeline tegutsema hoolsalt, täpselt ja objektiivselt.

   Komisjon määrab nõukojaga konsulteerides vastavalt nõutavatele vajadustele kindlaks komisjonis osalevate ekspertide arvu ning tagab õiglase soolise ja geograafilise esindatuse.

3. Teaduskomisjon nõustab ja toetab tehisintellektiametit, eelkõige seoses järgmiste ülesannetega:

a) toetab käesoleva määruse rakendamise ja täitmise tagamist seoses üldotstarbeliste tehisintellektimudelite ja -süsteemidega, eelkõige järgmiselt:

i) teavitades tehisintellektiametit üldotstarbeliste tehisintellektimudelite võimalikest süsteemsetest riskidest liidu tasandil kooskõlas artikliga 90;

ii) aidates kaasa üldotstarbeliste tehisintellektimudelite ja süsteemide võimete hindamise vahendite ja meetodite väljatöötamisele, sealhulgas võrdlusaluste kaudu;

iii) andes nõu süsteemse riskiga üldotstarbeliste tehisintellektimudelite klassifitseerimise kohta;

iv) andes nõu mitmesuguste üldotstarbeliste tehisintellektimudelite ja -süsteemide klassifitseerimise kohta;

v) aidates kaasa vahendite ja vormide väljatöötamisele;

b) toetab turujärelevalveasutuste tööd, kui nad seda taotlevad;

c) toetab artikli 74 lõikes 11 osutatud piiriüleseid turujärelevalvetegevusi, ilma et see piiraks turujärelevalveasutuste volitusi;

d) toetab tehisintellektiametit tema kohustuste täitmisel seoses artikli 81 kohase liidu kaitsemeetmete menetlusega.

4. Teaduskomisjoni eksperdid täidavad oma ülesandeid erapooletult ja objektiivselt ning tagavad oma ülesannete ja tegevuse käigus saadud teabe ja andmete konfidentsiaalsuse. Lõike 3 kohaste ülesannete täitmisel nad ei küsi ega võta vastu juhiseid mitte kelleltki. Iga ekspert koostab huvide deklaratsiooni, mis tehakse üldsusele kättesaadavaks. Tehisintellektiamet kehtestab süsteemid ja menetlused võimalike huvide konfliktide aktiivseks haldamiseks ja ennetamiseks.

5. Lõikes 1 osutatud rakendusakt sisaldab sätteid tingimuste, menetluste ja üksikasjaliku korra kohta, mille alusel teaduskomisjon ja selle liikmed peavad edastama hoiatusteateid ning taotlema teaduskomisjoni ülesannete täitmisel tehisintellektiameti abi.

Artikkel 69

Liikmesriikide juurdepääs ekspertide reservile

1. Liikmesriigid võivad kasutada teaduskomisjoni ekspertide abi, et toetada oma käesoleva määruse kohaseid täitmise tagamise toiminguid.

2. Liikmesriikidelt võidakse nõuda ekspertide pakutava nõustamise ja toe eest tasu. Tasu struktuur ja suurus ning hüvitatavate kulude ulatus ja struktuur kehtestatakse artikli 68 lõikes 1 osutatud rakendusaktiga, võttes arvesse käesoleva määruse asjakohase rakendamise eesmärke, kulutasuvust ja vajadust tagada kõikidele liikmesriikidele ekspertide kasutamise võimalus.

3. Komisjon hõlbustab vajaduse korral liikmesriikide jaoks võimalust kasutada õigeaegselt eksperte ning tagab, et liidu tehisintellekti testimise toe poolt artikli 84 kohaselt ja ekspertide poolt käesoleva artikli kohaselt läbiviidava toetustegevuse kombineerimine on tõhusalt korraldatud ja annab parima võimaliku lisaväärtuse.

2. JAGU

RIIGI PÄDEVAD ASUTUSED

Artikkel 70

Riigi pädevate asutuste ja ühtsete kontaktpunktide määramine

1. Iga liikmesriik loob või määrab käesoleva määruse kohaldamisel riigi pädevateks asutusteks vähemalt ühe teavitava asutuse ja vähemalt ühe turujärelevalveasutuse. Nimetatud riigi pädevad asutused peavad kasutama oma volitusi sõltumatult, erapooletult ja eelarvamusteta, et järgida oma tegevuses ja ülesannete täitmisel objektiivsuse ja erapooletuse põhimõtteid ning tagada käesoleva määruse kohaldamine ja rakendamine. Kõnealuste asutuste liikmed hoiduvad kõigest, mis on kokkusobimatu nende kohustustega. Tingimusel, et järgitakse nimetatud põhimõtteid, võivad selliseid tegevusi ja ülesandeid vastavalt liikmesriigi organisatsioonilistele vajadustele täita üks või mitu määratud asutust.

2. Liikmesriigid teatavad komisjonile oma teavitavate asutuste ja turujärelevalveasutuste nimed ja nende asutuste ülesanded, samuti edaspidistest nendega seotud muudatustest. Liikmesriigid teevad hiljemalt … [12 kuud pärast käesoleva määruse jõustumise kuupäeva] üldsusele kättesaadavaks teabe selle kohta, kuidas saab pädevate asutuste ja ühtsete kontaktpunktidega elektrooniliste sidevahendite kaudu ühendust võtta. Liikmesriigid määravad käesoleva määruse kohaldamisel turujärelevalveasutuse, kes tegutseb ühtse kontaktpunktina, ning teatavad komisjonile selle ühtse kontaktpunkti nime. Komisjon teeb ühtsete kontaktpunktide loetelu üldsusele kättesaadavaks.

3. Liikmesriigid tagavad, et nende riigi pädevatel asutustel on käesolevast määrusest tulenevate ülesannete tulemuslikuks täitmiseks piisavad tehnilised, rahalised ja inimressursid ning taristu. Eeskätt peab riigi pädevatele asutustele olema pidevalt kättesaadav piisaval arvul töötajaid, kelle pädevuste ja eksperditeadmiste hulka kuuluvad põhjalik arusaamine tehisintellekti tehnoloogiatest, andmetest ja andmetöötlusest, isikuandmete kaitsest, küberturvalisusest, põhiõigustest ja tervise ja ohutusega seotud riskidest ning teadmised kehtivatest standarditest ja õiguslikest nõuetest. Liikmesriigid hindavad ja vajaduse korral ajakohastavad igal aastal käesolevas lõikes osutatud pädevus- ja ressursinõudeid.

4. Riigi pädevad asutused võtavad piisaval tasemel küberturvalisuse tagamiseks asjakohaseid meetmeid.

5. Riigi pädevad asutused tegutsevad oma ülesannete täitmisel kooskõlas artiklis 78 sätestatud konfidentsiaalsuskohustustega.

6. Hiljemalt … [üks aasta pärast käesoleva määruse jõustumise kuupäeva] ja seejärel iga kahe aasta tagant teavitavad liikmesriigid komisjoni riigi pädevate asutuste rahaliste vahendite ja inimressursside olukorrast, hinnates sealjuures nende piisavust. Komisjon edastab selle teabe nõukojale arutamiseks ja võimalikeks soovitusteks.

7. Komisjon hõlbustab kogemuste vahetamist riigi pädevate asutuste vahel.

8. Riigi pädevad asutused võivad anda juhiseid ja nõu käesoleva määruse rakendamise kohta, eelkõige VKEdele, sealhulgas idufirmadele, võttes arvesse nõukoja ja komisjoni juhiseid ja nõuandeid, kui see on asjakohane. Kui riigi pädevad asutused kavatsevad anda juhiseid ja nõu tehisintellektisüsteemi kohta valdkondades, mille suhtes kehtib ka muu liidu õigus, konsulteeritakse vastavalt vajadusele selle liidu õiguse alusel riigi pädevate asutustega.

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

VIII peatükk

Suure riskiga tehisintellektisüsteemide ELi andmebaas

Artikkel 71

III lisas loetletud suure riskiga tehisintellektisüsteemide ELi andmebaas

1. Komisjon loob koostöös liikmesriikidega ELi andmebaasi, mis sisaldab käesoleva artikli lõigetes 2 ja 3 osutatud teavet artikli 6 lõikes 2 osutatud suure riskiga tehisintellektisüsteemide kohta, mis on registreeritud vastavalt artiklitele 49 ja 60 ning tehisintellektisüsteemide kohta, mida vastavalt artikli 6 lõikele 3 ei peeta suure riskiga süsteemiks ning mis on registreeritud vastavalt artikli 6 lõikele 4 ja artiklile 49, ning haldab seda. Sellise andmebaasi funktsionaalsete kirjelduste koostamisel konsulteerib komisjon asjaomaste ekspertidega ja sellise andmebaasi funktsionaalsete kirjelduste ajakohastamisel konsulteerib komisjon nõukojaga.

2. VIII lisa A ja B jaos loetletud andmed sisestab ELi andmebaasi pakkuja või kohaldataval juhul volitatud esindaja.

3. VIII lisa C jaos loetletud andmed sisestab kooskõlas artikli 49 lõigetega 3 ja 4 ELi andmebaasi juurutaja, kes on avaliku sektori asutus, amet või organ või tegutseb selle nimel.

4. Välja arvatud artikli 49 lõikes 4 ja artikli 60 lõike 4 punktis c osutatud osa, on ELi andmebaasis sisalduv artikli 49 kohaselt registreeritud teave juurdepääsetav ja üldsusele kättesaadav kasutajasõbralikul viisil. Teave peaks olema kergesti navigeeritav ja masinloetav. Artikli 60 kohaselt registreeritud teave on kättesaadav üksnes turujärelevalveasutustele ja komisjonile, välja arvatud juhul, kui võimalik pakkuja või pakkuja on andnud nõusoleku, et see teave tehakse kättesaadavaks ka üldsusele.

5. ELi andmebaas sisaldab isikuandmeid ainult niivõrd, kuivõrd see on vajalik käesoleva määruse kohaseks teabe kogumiseks ja töötlemiseks. See teave hõlmab nende füüsiliste isikute nimesid ja kontaktandmeid, kes vastutavad süsteemi registreerimise eest ja on volitatud esindama pakkujat või asjakohasel juhul juurutajat.

6. ELi andmebaasi vastutav töötleja on komisjon. Komisjon teeb pakkujatele, võimalikele pakkujatele ja juurutajatele kättesaadavaks piisava tehnilise ja haldustoe. ELi andmebaas peab vastama kohaldatavatele ligipääsetavusnõuetele.

IX peatükk
Turustamisjärgne seire, teabe jagamine ning turujärelevalve

1. JAGU
TURUSTAMISJÄRGNE SEIRE

Artikkel 72

Pakkujapoolne turustamisjärgne seire ja suure riskiga tehisintellektisüsteemide turustamisjärgse seire kava

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

2. Turustamisjärgse seire süsteem peab aktiivselt ja süstemaatiliselt koguma, dokumenteerima ja analüüsima juurutajate esitavaid või muudest allikatest kogutavaid asjakohaseid andmeid suure riskiga tehisintellektisüsteemide toimimise kohta kogu nende eluea jooksul ning võimaldama pakkujal hinnata, kas tehisintellektisüsteemid vastavad jätkuvalt III peatüki 2. jaos sätestatud nõuetele. Asjakohasel juhul hõlmab turustamisjärgne seire analüüsi koostoime kohta muude tehisintellektisüsteemidega. See kohustus ei hõlma õiguskaitseasutustest juurutajate tundlikke operatiivandmeid.

3. Turustamisjärgse seire süsteem peab põhinema turustamisjärgse seire kaval. Turustamisjärgse seire kava on IV lisas osutatud tehnilise dokumentatsiooni osa. Komisjon võtab … [18 kuud pärast käesoleva määruse jõustumist] vastu rakendusakti, millega nähakse ette üksikasjalikud sätted turustamisjärgse seire kava vormi ja kavas sisalduvate elementide loetelu kehtestamise kohta. Kõnealune rakendusakt võetakse vastu kooskõlas artikli 98 lõikes 2 osutatud kontrollimenetlusega.

4. I lisa A jaos loetletud liidu ühtlustamisõigusaktidega hõlmatud suure riskiga tehisintellektisüsteemide puhul, mille turustamisjärgse seire süsteem ja kava on juba kehtestatud nende õigusaktide alusel, siis on selleks, et tagada järjepidevus, vältida dubleerimist ja viia miinimumini lisakoormus, pakkujatel võimalus vajaduse korral integreerida lõigetes 1, 2 ja 3 kirjeldatud vajalikud elemendid, kasutades lõikes 3 osutatud vormi, nendes õigusaktide alusel juba olemas olevatesse süsteemidesse ja kavadesse, tingimusel et nii saavutatakse samaväärne kaitsetase.

   Käesoleva lõike esimest lõiku kohaldatakse ka III lisa punktis 5 osutatud suure riskiga tehisintellektisüsteemide suhtes, mille on turule lasknud või kasutusele võtnud finantsasutused, kes peavad täitma finantsteenuseid käsitleva liidu õiguse kohaseid nõudeid seoses nende sisemise juhtimissüsteemi, korra või protsessidega.

2. JAGU

TEABE JAGAMINE TÕSISTE INTSIDENTIDE KOHTA

Artikkel 73

Tõsistest intsidentidest teatamine

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

2. Lõikes 1 osutatud 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 või kohaldataval juhul juurutaja saab tõsisest intsidendist teadlikuks.

   Esimeses lõigus osutatud teatamise tähtaja puhul võetakse arvesse tõsise intsidendi raskusastet.

3. Olenemata käesoleva artikli lõikest 2 toimub ulatusliku rikkumise või artikli 3 punkti 49 alapunktis b määratletud tõsise intsidendi korral käesoleva artikli lõikes 1 osutatud teatamine viivitamata ja mitte hiljem kui kaks päeva pärast seda, kui pakkuja või kohaldataval juhul juurutaja saab tõsisest intsidendist teada.

4. Olenemata lõikest 2 toimub inimese surma korral teatamine viivitamata pärast seda, kui pakkuja või juurutaja on teinud kindlaks suure riskiga tehisintellektisüsteemi ja tõsise intsidendi vahelise põhjusliku seose, või kohe, kui ta kahtlustab sellise seose olemasolu, kuid mitte hiljem kui kümme päeva pärast päeva, mil pakkuja või kohaldataval juhul juurutaja saab tõsisest intsidendist teada.

5. Kui see on vajalik õigeaegse teatamise tagamiseks, võib pakkuja või kohaldataval juhul juurutaja esitada esialgse mittetäieliku aruande, millele järgneb täielik aruanne.

6. Pärast lõike 1 kohast tõsisest intsidendist teatamist korraldab pakkuja viivitamata tõsise intsidendi ja asjaomase tehisintellektisüsteemi vajaliku uurimise. See hõlmab intsidendi riskihindamist ja parandusmeetmeid.

   Pakkuja teeb esimeses lõigus osutatud uurimise käigus koostööd pädevate asutustega ja asjaomase teada antud asutusega, kui see on asjakohane, ning ei korralda ühtegi uurimist, mille käigus muudetakse asjaomast tehisintellektisüsteemi selliselt, et see võiks mõjutada intsidendi põhjuste järgnevat hindamist, enne kui ta on sellisest tegevusest teavitanud pädevat asutust.

7. Kui asjaomane turujärelevalveasutus saab teate artikli 3 punkti 49 alapunktis c osutatud tõsise intsidendi kohta, teatab ta sellest artikli 77 lõikes 1 osutatud riiklikele ametiasutustele või organitele. Komisjon koostab spetsiaalse juhendi, et hõlbustada käesoleva artikli lõikes 1 sätestatud kohustuste täitmist. Juhend antakse välja … [12 kuud pärast käesoleva määruse jõustumist] ja seda hinnatakse korrapäraselt.

8. Turujärelevalveasutus võtab määruse (EL) 2019/1020 artiklis 19 ette nähtud asjakohased meetmed seitsme päeva jooksul alates käesoleva artikli lõikes 1 osutatud teate saamise kuupäevast ning järgib kõnealuses määruses sätestatud teavitamiskorda.

9. III lisas osutatud suure riskiga tehisintellektisüsteemide puhul, mille lasevad turule või võtavad kasutusele pakkujad, kelle suhtes kohaldatakse liidu õigusakte, millega nähakse ette käesolevas määruses sätestatuga samaväärsed teatamiskohustused, piirdub tõsistest intsidentidest teatamine artikli 3 punkti 49 alapunktis c osutatud intsidentidega.

10. Suure riskiga tehisintellektisüsteemide puhul, mis on selliste seadmete turvakomponendid või mis on ise sellised seadmed, mille suhtes kohaldatakse määrusi (EL) 2017/745 ja (EL) 2017/746, teavitatakse ainult käesoleva määruse artikli 3 punkti 49 alapunktis c osutatud tõsistest intsidentidest ning nendest teatatakse riigi pädevale asutusele, kelle liikmesriik, kus intsident aset leidis, on selleks otstarbeks valinud.

11. Riigi pädevad asutused teatavad tõsisest intsidendist viivitamata komisjonile vastavalt määruse (EL) 2019/1020 artiklile 20, sõltumata sellest, kas nad on intsidendi suhtes meetmeid võtnud või mitte.

3. JAGU

TÄITMISE TAGAMINE

Artikkel 74

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 artikli 2 lõikes 1 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 ja asjaomastele riiklikele konkurentsiasutustele igal aastal kogu turujärelevalvetoimingute käigus kindlaks tehtud teabe, mis võib pakkuda huvi liidu konkurentsiõiguse kohaldamise seisukohast. Samuti esitavad nad komisjonile igal aastal aruande kõnealusel aastal esinenud keelatud tavade kasutamise ja võetud meetmete kohta.

3. Käesoleva määruse kohaldamisel on I lisa A jaos loetletud liidu ühtlustamisõigusaktidega hõlmatud toodetega seotud suure riskiga tehisintellektisüsteemide puhul turujärelevalveasutuseks nende õigusaktide alusel määratud ametiasutus, kes vastutab turujärelevalvetoimingute eest.

Erandina esimesest lõigust ja sobivate asjaolude korral võivad liikmesriigid määrata turujärelevalveülesandeid täitma mõne muu asutuse, tingimusel et nad tagavad koordineerimise asjaomaste valdkondlike turujärelevalveasutustega, kes vastutavad I lisas loetletud liidu ühtlustamisõigusaktide täitmise tagamise eest.

4. Käesoleva määruse artiklites 79–83 osutatud menetlusi ei kohaldata selliste tehisintellektisüsteemide suhtes, mis on seotud I lisa A jaos loetletud liidu ühtlustamisõigusaktidega hõlmatud toodetega, kui selliste õigusaktidega on juba ette nähtud menetlused, mis tagavad samaväärse kaitsetaseme ja millel on sama eesmärk. Sellistel juhtudel kohaldatakse selle asemel asjakohaseid valdkondlikke menetlusi.

5. Ilma et see piiraks turujärelevalveasutuste määruse (EL) 2019/1020 artikli 14 kohaseid volitusi, võivad turujärelevalveasutused käesoleva määruse tõhusa täitmise tagamiseks kasutada kõnealuse määruse artikli 14 lõike 4 punktides d ja j osutatud volitusi vastavalt vajadusele kaugühenduse teel.

6. Käesoleva määruse kohaldamisel on liidu finantsteenuste valdkonna õigusega 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.

7. Erandina lõikest 6 võib liikmesriik sobivate asjaolude korral 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 määrusega (EL) nr 1024/2013 loodud ühtses järelevalvemehhanismis, peaksid viivitamata esitama Euroopa Keskpangale turujärelevalvetoimingute käigus kindlaks tehtud teabe, mis võib pakkuda võimalikku huvi seoses kõnealuses määruses sätestatud Euroopa Keskpanga usaldatavusnõuete täitmise järelevalve ülesannetega.

8. Käesoleva määruse III lisa punktis 1 loetletud suure riskiga tehisintellektisüsteemide puhul, kui neid süsteeme kasutatakse õiguskaitse ja piirihalduse eesmärgil ning õigusemõistmiseks ja demokraatlikeks protsessideks, ning käesoleva määruse III lisa punktides 6, 7 ja 8 loetletud suure riskiga tehisintellektisüsteemide puhul, määravad liikmesriigid käesoleva määruse kohaldamisel turujärelevalveasutuseks kas määruse (EL) 2016/679 või direktiivi (EL) 2016/680 kohaselt pädeva andmekaitse järelevalveasutuse või mis tahes muu direktiivi (EL) 2016/680 artiklites 41–44 sätestatud samadel tingimustel määratud asutuse. Turujärelevalvetoimingud ei mõjuta mingil viisil õigusasutuste sõltumatust ega sekku muul viisil nende tegevusse, kui nad tegutsevad õigusemõistjana.

9. Kui liidu institutsioonid, organid ja asutused kuuluvad käesoleva määruse kohaldamisalasse, tegutseb nende järelevalve teostamisel pädeva asutusena Euroopa Andmekaitseinspektor, välja arvatud Euroopa Liidu Kohtu puhul, kui kohus täidab õigusemõistmise funktsiooni.

10. Liikmesriigid hõlbustavad koordineerimist käesoleva määruse alusel määratud turujärelevalveasutuste ja muude asjaomaste riiklike asutuste või organite vahel, kes teevad järelevalvet I lisas loetletud liidu ühtlustamisõigusaktide või muu III lisas osutatud liidu õiguse kohaldamise üle, mis võivad suure riskiga tehisintellektisüsteemide seisukohast olulised olla.

11. Turujärelevalveasutused ja komisjon saavad teha ettepanekuid ühismeetmete, sealhulgas ühisuurimiste kohta, mida viivad läbi kas turujärelevalveasutused või turujärelevalveasutused koos komisjoniga ja mille eesmärk on edendada nõuetele vastavust, teha kindlaks mittevastavus, suurendada teadlikkust ja anda suuniseid käesoleva määruse kohta seoses selliste suure riskiga tehisintellektisüsteemide konkreetsete kategooriatega, mille puhul on leitud, et need kujutavad endast kooskõlas määruse (EL) 2019/1020 artikliga 9 tõsist riski kahes või enamas liikmesriigis. Tehisintellektiamet tagab ühisuurimiste koordineerimistoe.

12. Ilma et see piiraks määrusega (EL) 2019/1020 antud volitusi ning kui see on asjakohane ja piirdub nende ülesannete täitmiseks vajalikuga, annavad pakkujad turujärelevalveasutustele täieliku juurdepääsu dokumentatsioonile ning suure riskiga tehisintellektisüsteemide 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.

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

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

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

14. Turujärelevalveasutuste poolt saadud teavet ja dokumentatsiooni käsitletakse kooskõlas artiklis 78 sätestatud konfidentsiaalsuskohustustega.

Artikkel 75

Vastastikune abi, turujärelevalve ja üldotstarbeliste tehisintellektisüsteemide kontroll

1. Kui tehisintellektisüsteem põhineb üldotstarbelisel tehisintellektimudelil ning mudeli ja süsteemi arendab sama pakkuja, on tehisintellektiametil volitused jälgida ja kontrollida selle tehisintellektisüsteemi vastavust käesolevast määrusest tulenevatele kohustustele. Oma seire- ja järelevalveülesannete täitmiseks on tehisintellektiametil kõik käesolevas jaos ja määruses (EL) 2019/1020 sätestatud turujärelevalveasutuse volitused.

2. Kui asjaomastel turujärelevalveasutustel on piisavalt põhjust arvata, et üldotstarbelised tehisintellektisüsteemid, mida juurutajad saavad otse kasutada vähemalt ühel eesmärgil, mis on käesoleva määruse kohaselt liigitatud suurt riski tekitavaks, ei vasta käesolevas määruses sätestatud nõuetele, teevad nad vastavushindamise läbiviimisel koostööd tehisintellektiametiga ning teavitavad sellest vastavalt nõukoda ja teisi turujärelevalveasutusi.

3. Kui turujärelevalveasutus ei suuda suure riskiga tehisintellektisüsteemi uurimist lõpule viia, kuna ta ei saa juurdepääsu teatavale üldotstarbelise tehisintellektimudeliga seotud teabele, kuigi ta on teinud selle teabe saamiseks kõik vajaliku, võib ta esitada põhjendatud taotluse tehisintellektiametile, kes tagab asjaomasele teabele juurdepääsu. Sel juhul esitab tehisintellektiamet taotluse esitanud asutusele viivitamata, kuid hiljemalt 30 päeva jooksul teabe, mida tehisintellektiamet peab vajalikuks, et teha kindlaks, kas suure riskiga tehisintellektisüsteem on nõuetele mittevastav. Turujärelevalveasutused tagavad saadud teabe konfidentsiaalsuse vastavalt käesoleva määruse artiklile 78. Määruse (EL) 2019/1020 VI peatükis sätestatud menetlust kohaldatakse *mutatis mutandis*.

Artikkel 76

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 58 kohaselt järelevalvet tehisintellekti regulatiivliivakastis, testitakse tegelikes tingimustes, kontrollivad turujärelevalveasutused vastavust artiklile 60 osana oma järelevalverollist tehisintellekti regulatiivliivakastis. Pakkujale või võimalikule pakkujale tegelikes tingimustes testimise lubamiseks võivad need asutused teha asjakohasel juhul erandi artikli 60 lõike 4 punktides f ja g sätestatud tingimustest.

3. Kui turujärelevalveasutus on saanud pakkujalt, võimalikult pakkujalt või tõsise intsidendiga seotud kolmandalt isikult teavet või kui tal on muud alust arvata, et artiklites 60 ja 61 sätestatud tingimused ei ole täidetud, võib ta vajaduse korral teha oma territooriumil ühe järgmistest otsustest:

   a) peatada või lõpetada tegelikes tingimustes testimine;

   b) nõuda pakkujalt või võimalikult pakkujalt ning juurutajalt ja võimalikult juurutajalt tegelikes tingimustes testimise mis tahes aspekti muutmist.

4. Kui turujärelevalveasutus on teinud käesoleva artikli lõikes 3 osutatud otsuse või esitanud vastuväite artikli 60 lõike 4 punkti b tähenduses, märgitakse otsuses või vastuväites selle põhjused ja see, kuidas pakkuja või võimalik pakkuja saab otsuse või vastuväite vaidlustada.

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

Artikkel 77

Põhiõigusi kaitsvate asutuste volitused

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

2. Hiljemalt … [kolm kuud pärast käesoleva määruse jõustumist] määrab iga liikmesriik lõikes 1 osutatud ametiasutused või organid ning teeb nende loetelu üldsusele kättesaadavaks. Liikmesriigid teavitavad loetelust komisjoni ja teisi liikmesriike ning hoiavad selle ajakohasena.

3. Kui lõikes 1 osutatud dokumentatsioon ei ole piisav, et teha kindlaks, kas põhiõigusi kaitsva liidu õiguse kohaseid kohustusi on rikutud, võib lõikes 1 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.

4. Käesoleva artikli lõikes 1 osutatud riiklike ametiasutuste või organite poolt käesoleva artikli sätete kohaselt saadud teavet või dokumentatsiooni käsitletakse kooskõlas artiklis 78 sätestatud konfidentsiaalsuskohustustega.

Artikkel 78

Konfidentsiaalsus

1. Komisjon, turujärelevalveasutused ja teada antud asutused, ning kõik muud füüsilised ja juriidilised isikud, kes osalevad käesoleva määruse kohaldamises, tagavad kooskõlas liidu või riigisisese õigusega oma ülesannete täitmisel ja tegevuse käigus saadud teabe ja andmete konfidentsiaalsuse, et kaitsta eeskätt järgmist:

   a) intellektuaalomandi õigused ning füüsilise või juriidilise isiku konfidentsiaalne äriteave või ärisaladus, kaasa arvatud lähtekoodid, välja arvatud juhtudel, millele on viidatud Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/943[57] artiklis 5;

   b) käesoleva määruse tulemuslik rakendamine, eelkõige inspekteerimise, uurimise ja auditite eesmärgil;

   c) avaliku ja riigi julgeolekuga seotud huvid;

   d) kriminaal- või haldusmenetluste usaldusväärsus;

[57] Euroopa Parlamendi ja nõukogu 8. juuni 2016. aasta direktiiv (EL) 2016/943, milles käsitletakse avalikustamata oskusteabe ja äriteabe (ärisaladuste) ebaseadusliku omandamise, kasutamise ja avalikustamise vastast kaitset (ELT L 157, 15.6.2016, lk 1).

e) liidu või riigisisese õiguse kohaselt salastatud teave.

2. Vastavalt lõikele 1 käesoleva määruse kohaldamises osalevad asutused küsivad ainult andmeid, mis on rangelt vajalikud tehisintellektisüsteemidest lähtuva ohu hindamiseks ja nende volituste täitmiseks kooskõlas käesoleva määrusega ja määrusega (EL) 2019/1020. Kooskõlas kohaldatava liidu või riigisisese õigusega kehtestavad nad piisavad ja tõhusad küberturvalisuse meetmed, et kaitsta saadud teabe ja andmete turvalisust ja konfidentsiaalsust, ning kustutavad kogutud andmed kohe, kui neid ei ole enam vaja eesmärgil, milleks need saadi.

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

Kui õiguskaitse-, rände- või varjupaigaasutused on III lisa punktis 1, 6 või 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 74 lõigetes 8 ja 9 osutatud turujärelevalveasutused taotluse alusel viivitamata tutvuda dokumentatsiooniga või saada selle koopia. Dokumentatsiooni või selle koopiaga on lubatud tutvuda ainult neil turujärelevalveasutuse töötajatel, kellel on asjakohasel tasemel salastatud teabele juurdepääsu luba.

4. Lõiked 1, 2 ja 3 ei mõjuta komisjoni, liikmesriikide ja nende asjaomaste ametiasutuste ning teada antud asutuste õigusi ja kohustusi vahetada teavet ja edastada hoiatusi, sealhulgas piiriülese koostöö kontekstis, ega mõjuta osaliste kohustusi anda teavet liikmesriikide kriminaalõiguse kohaselt.

5. Komisjon ja liikmesriigid võivad vajaduse korral ning kooskõlas rahvusvaheliste ja kaubanduslepingute asjaomaste sätetega vahetada konfidentsiaalset teavet nende kolmandate riikide reguleerivate asutustega, kellega nad on sõlminud kahe- või mitmepoolsed konfidentsiaalsuse kokkulepped, mis tagavad konfidentsiaalsuse piisava taseme.

Artikkel 79

Riski kujutavate tehisintellektisüsteemidega tegelemise riikliku tasandi menetlus

1. Riski kujutavat tehisintellektisüsteemi käsitatakse määruse (EL) 2019/1020 artikli 3 punktis 19 määratletud „ohtliku tootena“ niivõrd, kuivõrd tegemist on inimeste tervisele, ohutusele või põhiõigustele avalduvate riskidega.

2. Kui liikmesriigi turujärelevalveasutusel on piisavalt põhjust uskuda, et tehisintellektisüsteem kujutab endast käesoleva artikli lõikes 1 osutatud riski, korraldab ta asjaomase tehisintellektisüsteemi hindamise, et selgitada välja, kas süsteem vastab käesolevas määruses sätestatud nõuetele ja kohustustele. Erilist tähelepanu pööratakse sellistele tehisintellektisüsteemidele, mis kujutavad endast riski kaitsetutele rühmadele. Kui tuvastatakse põhiõigustega seotud riskid, teavitab turujärelevalveasutus sellest ka artikli 77 lõikes 1 osutatud asjaomaseid riiklikke ametiasutusi või organeid ja teeb nendega täielikku koostööd. Asjaomased operaatorid teevad vastavalt vajadusele koostööd turujärelevalveasutuse ja muude artikli 77 lõikes 1 osutatud riiklike ametiasutuste või organitega.

Kui turujärelevalveasutus või kohaldataval juhul turujärelevalveasutus koostöös artikli 77 lõikes 1 osutatud riikliku ametiasutusega, leiab nimetatud hindamise käigus, et tehisintellektisüsteem ei vasta käesolevas määruses sätestatud nõuetele ja kohustustele, nõuab ta põhjendamatu viivituseta, et asjaomane operaator võtaks vastavalt tema ettekirjutusele kõik vajalikud parandusmeetmed, et viia tehisintellektisüsteem nimetatud nõuetega vastavusse, turult kõrvaldada või tagasi nõuda ajavahemiku jooksul, mille turujärelevalveasutus võib ette näha, ja igal juhul hiljemalt 15 tööpäeva või asjaomases kohaldatavas liidu ühtlustamisõigusaktides ette nähtud tähtaja jooksul.

Turujärelevalveasutus teavitab sellest asjaomast teada antud asutust. Käesoleva lõike teises lõigus osutatud meetmete suhtes kohaldatakse määruse (EL) 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 tema poolt liidu turul kättesaadavaks tehtud asjaomaste 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 oma riigisisesel turul tehisintellektisüsteemi kättesaadavaks tegemine või kasutusele võtmine või seda piirata või toode või autonoomne tehisintellektisüsteem turult kõrvaldada või tagasi nõuda. See asutus teavitab nimetatud meetmetest põhjendamatu viivituseta komisjoni ja teisi liikmesriike.

6. Lõikes 5 osutatud teavitus sisaldab kõiki kättesaadavaid üksikasju, eelkõige nõuetele mittevastava tehisintellektisüsteemi tuvastamiseks vajalikke andmeid, teavet tehisintellektisüsteemi päritolu ja tarneahela, väidetava mittevastavuse ja riski olemus, võetud riiklike meetmete olemuse ja kestuse kohta 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;

   b) suure riskiga tehisintellektisüsteemi mittevastavus III peatüki 2. jaos sätestatud nõuetele;

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

d) artikli 50 rikkumine.

7. Muud 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 teada antud riigisisese meetmega nõus, siis ka oma vastuväidetest.

8. Kui kolme kuu jooksul alates käesoleva artikli lõikes 5 osutatud teavituse kättesaamisest ei ole liikmesriigi turujärelevalveasutus ega komisjon esitanud vastuväiteid teise liikmesriigi turujärelevalveasutuse võetud ajutise meetme suhtes, loetakse meede põhjendatuks. See ei piira asjaomase operaatori määruse (EL) 2019/1020 artikli 18 kohaseid menetlusõigusi. Käesolevas lõikes osutatud kolme kuu pikkust tähtaega lühendatakse 30 päevani, kui rikutud on käesoleva määruse artiklis 5 osutatud tehisintellekti kasutusviiside keeldu.

9. Turujärelevalveasutused tagavad, et asjaomase toote või tehisintellektisüsteemi suhtes võetakse põhjendamatu viivituseta asjakohased piiravad meetmed, näiteks kõrvaldatakse toode või tehisintellektisüsteem liikmesriigi põhjendamatu viivituseta nende turult.

Artikkel 80

III lisa kohaldamisel sellise tehisintellektisüsteemiga tegelemise menetlus, mida pakkuja ei ole liigitanud suure riskiga süsteemiks

1. Kui turujärelevalveasutusel on piisavalt põhjust arvata, et tehisintellektisüsteem, mille pakkuja on artikli 6 lõike 3 kohaselt liigitanud tehisintellektisüsteemiks, mida ei peeta suure riskiga süsteemiks, on tegelikult suure riskiga tehisintellektisüsteem, viib ta läbi asjaomase tehisintellektisüsteemi hindamise, et selgitada välja, kas tehisintellektisüsteem tuleks liigitada suure riskiga tehisintellektisüsteemiks vastavalt artikli 6 lõikes 3 sätestatud tingimustele ja komisjoni suunistele.

2. Kui turujärelevalveasutus leiab kõnealuse hindamise käigus, et asjaomane tehisintellektisüsteem on suure riskiga, nõuab ta asjaomaselt pakkujalt, et see viiks tehisintellektisüsteemi põhjendamatu viivituseta vastavusse käesolevas määruses sätestatud nõuete ja kohustustega ning võtaks asjakohased parandusmeetmed ajavahemiku jooksul, mille turujärelevalveasutus võib ette näha.

3. Kui turujärelevalveasutus on seisukohal, et asjaomase tehisintellektisüsteemi kasutamine ei piirdu üksnes tema liikmesriigi territooriumiga, teavitab ta põhjendamatu viivituseta komisjoni ja teisi liikmesriike hindamistulemustest ja meetmetest, mille võtmist ta on pakkujalt nõudnud.

4. Pakkuja tagab, et võetakse kõik vajalikud meetmed, et viia tehisintellektisüsteem vastavusse käesolevas määruses sätestatud nõuete ja kohustustega. Kui asjaomase tehisintellektisüsteemi pakkuja ei vii tehisintellektisüsteemi nende nõuete ja kohustustega vastavusse käesoleva artikli lõikes 2 osutatud ajavahemiku jooksul, määratakse pakkujale artikli 99 kohane trahv.

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

6. Kui asjaomase tehisintellektisüsteemi pakkuja ei võta käesoleva artikli lõikes 2 osutatud ajavahemiku jooksul piisavaid parandusmeetmeid, kohaldatakse artikli 79 lõikeid 5–9.

7. Kui turujärelevalveasutus teeb käesoleva artikli lõike 1 kohase hindamise käigus kindlaks, et pakkuja jättis tehisintellektisüsteemi suure riskiga tehisintellektisüsteemiks liigitamata seetõttu, et pääseda III peatüki 2. jao nõuete täitmisest, määratakse pakkujale artikli 99 kohane trahv.

8. Kasutades oma volitusi teha järelevalvet käesoleva artikli kohaldamise üle ning kooskõlas määruse (EL) 2019/1020 artikliga 11 võivad turujärelevalveasutused teha asjakohaseid kontrolle, võttes eelkõige arvesse käesoleva määruse artiklis 71 osutatud ELi andmebaasis säilitatavat teavet.

Artikkel 81

Liidu kaitsemeetmete menetlus

1. Kui kolme kuu jooksul alates artikli 79 lõikes 5 osutatud teavituse kättesaamisest või artiklis 5 osutatud tehisintellekti kasutusviiside keelu rikkumise korral 30 päeva jooksul esitab ühe liikmesriigi turujärelevalveasutus vastuväite teise turujärelevalveasutuse võetud meetme suhtes või kui komisjon leiab, et meede on liidu õigusega vastuolus, alustab komisjon ilma põhjendamatu viivituseta konsultatsioone asjaomase liikmesriigi turujärelevalveasutuse ja operaatori või operaatoritega ning hindab riiklikku meedet. Selle hindamise tulemuste põhjal otsustab komisjon kuue kuu jooksul või artiklis 5 osutatud tehisintellekti kasutusviiside keelu rikkumise korral 60 päeva jooksul alates artikli 79 lõikes 5 osutatud teavituse saamisest, kas riiklik meede on põhjendatud, ning teatab oma otsuse asjaomase liikmesriigi turujärelevalveasutusele. Komisjon teavitab oma otsusest ka teisi turujärelevalveasutusi.

2. Kui komisjon leiab, et asjaomase liikmesriigi võetud meede on põhjendatud, tagavad kõik liikmesriigid, et nad võtavad asjaomase tehisintellektisüsteemi suhtes asjakohaseid piiravaid meetmeid, näiteks nõuavad tehisintellektisüsteemi põhjendamatu viivituseta kõrvaldamist oma turult, ning teavitavad sellest vastavalt komisjoni. Kui komisjon peab riiklikku meedet põhjendamatuks, tühistab asjaomane liikmesriik 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 82

Riski kujutavad nõuetele vastavad tehisintellektisüsteemid

1. Kui liikmesriigi turujärelevalveasutus leiab pärast artikli 79 kohast hindamist ning pärast konsulteerimist artikli 77 lõikes 1 osutatud asjaomase riikliku ametiasutusega, et ehkki suure riskiga tehisintellektisüsteem vastab käesoleva määruse nõuetele, kujutab see riski inimeste tervisele või ohutusele, põhiõigustele või avalike huvide kaitse muude aspektidele, nõuab ta, et asjaomane operaator võtaks tema määratava aja jooksul põhjendamatu viivituseta kõik vajalikud meetmed tagamaks, et asjaomane tehisintellektisüsteem ei kujuta turule laskmise või kasutusele võtmise korral enam sellist riski.

2. Pakkuja või muu asjaomane operaator tagab, et parandusmeetmed võetakse kõigi asjaomaste tehisintellektisüsteemide suhtes, mille ta on liidu turul kättesaadavaks teinud, lõikes 1 osutatud liikmesriigi turujärelevalveasutuse ettekirjutuse kohase tähtaja jooksul.

3. Liikmesriigid teavitavad lõike 1 kohasest tähelepanekust viivitamata komisjoni ja teisi liikmesriike. Teave peab sisaldama kõiki teadaolevaid üksikasju, eelkõige asjaomase tehisintellektisüsteemi tuvastamiseks vajalikke andmeid, teavet tehisintellektisüsteemi päritolu ja tarneahela, kaasneva riski olemuse ning liikmesriigi võetud meetmete olemuse ja kestuse kohta.

4. Komisjon alustab põhjendamatu viivituseta konsulteerimist asjaomaste liikmesriikide ja asjaomaste operaatoritega ning hindab võetud riiklikke meetmeid. Nimetatud hindamise tulemuste põhjal otsustab komisjon, kas meede on põhjendatud, ning teeb vajaduse korral ettepaneku muude sobivate meetmete võtmiseks.

5. Komisjon edastab oma otsuse viivitamata asjaomastele liikmesriikidele ning asjaomastele operaatoritele. Ta teavitab sellest ka teisi liikmesriike.

Artikkel 83

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) CE-märgise kinnitamisel ei ole järgitud artikli 48 nõudeid;

   b) CE-märgist ei ole kinnitatud;

   c) artiklis 47 osutatud ELi vastavusdeklaratsiooni ei ole koostatud;

d) artiklis 47 osutatud ELi vastavusdeklaratsioon ei ole koostatud õigesti;

e) artiklis 47 osutatud ELi andmebaasi ei ole kannet tehtud;

f) ei ole määratud volitatud esindajat, kui see on kohaldatav;

g) tehniline dokumentatsioon ei ole kättesaadav.

2. Kui lõikes 1 osutatud mittevastavust ei kõrvaldata, võtab asjaomase liikmesriigi turujärelevalveasutus asjakohased ja proportsionaalsed meetmed tehisintellektisüsteemi turul kättesaadavaks tegemise piiramiseks või keelamiseks või tagab selle viivitamatu tagasinõudmise või kõrvaldamise turult.

Artikkel 84

Liidu tehisintellekti testimise toetusstruktuurid

1. Komisjon määrab tehisintellekti valdkonnas määruse (EL) 2019/1020 artikli 21 lõike 6 kohaselt ühe või mitu liidu tehisintellekti testimise toetusstruktuuri.

2. Ilma et see piiraks lõikes 1 osutatud ülesannete täitmist, annavad liidu tehisintellekti testimise toetusstruktuurid nõukoja, komisjoni või turujärelevalveasutuste taotlusel ka sõltumatut tehnilist või teaduslikku nõu.

4. JAGU

ÕIGUSKAITSEVAHENDID

Artikkel 85

Õigus esitada kaebus turujärelevalveasutusele

Ilma et see piiraks muude halduslike või kohtulike õiguskaitsevahendite kohaldamist, võib iga füüsiline või juriidiline isik, kellel on alust arvata, et käesoleva määruse sätteid on rikutud, esitada asjaomasele turujärelevalveasutusele kaebuse.

Kooskõlas määrusega (EL) 2019/1020 võetakse selliseid kaebusi arvesse turujärelevalvetoimingute tegemisel ja neid käsitletakse turujärelevalveasutuste poolt selleks kehtestatud erimenetluste kohaselt.

Artikkel 86

Õigus üksikotsuste tegemise selgitamisele

1. Igal mõjutatud isikul, kelle suhtes kohaldatakse otsust, mille on teinud juurutaja III lisas loetletud suure riskiga tehisintellektisüsteemi, välja arvatud III lisa punktis 2 loetletud süsteemid, väljundi põhjal ja millel on õiguslikud tagajärjed või mis mõjutab seda isikut sama märkimisväärselt viisil, mis tema arvates kahjustab tema tervist, ohutust või põhiõigusi, on õigus nõuda juurutajalt selget ja sisulist selgitust tehisintellektisüsteemi rolli kohta otsustusmenetluses ja tehtud otsuse peamiste elementide kohta.

2. Lõiget 1 ei kohaldata selliste tehisintellektisüsteemide kasutusjuhtude suhtes, mille puhul on liidu või riigisiseses õiguses kooskõlas liidu õigusega ette nähtud erandid selle lõike kohastest kohustust või nende täitmise piirangud.

3. Käesolevat artiklit kohaldatakse ainult niivõrd, kui lõikes 1 osutatud õigus ei ole muul viisil liidu õiguses sätestatud.

Artikkel 87

Rikkumistest teatamine ja rikkumisest teatajate kaitse

Käesoleva määruse rikkumistest teatamise ja sellistest rikkumistest teatajate kaitse suhtes kohaldatakse direktiivi (EL) 2019/1937.

5. JAGU

ÜLDOTSTARBELISTE TEHISINTELLEKTIMUDELITE PAKKUJATE SUHTES KOHALDATAV JÄRELEVALVE, UURIMINE, TÄITMISE TAGAMINE JA JÄLGIMINE

Artikkel 88

Üldotstarbeliste tehisintellektimudelite pakkujate kohustuste täitmise tagamine

1. Komisjonil on ainupädevus teostada järelevalvet V peatüki järgimise üle ja tagada selle täitmine, võttes arvesse artiklis 94 sätestatud menetluslikke tagatisi. Komisjon usaldab nende ülesannete täitmise tehisintellektiametile, ilma et see piiraks komisjoni korralduslikke volitusi ning liikmesriikide ja liidu vahelist pädevuste jaotust, mis põhineb aluslepingutel.

2. Ilma et see piiraks artikli 75 lõike 3 kohaldamist, võivad turujärelevalveasutused nõuda, et komisjon teostaks oma käesolevas jaos sätestatud volitusi, kui see on vajalik ja proportsionaalne, et abistada turujärelevalveasutusi nende käesolevast määrusest tulenevate ülesannete täitmisel.

Artikkel 89

Seiremeetmed

1. Tehisintellektiamet võib talle käesoleva jao alusel määratud ülesannete täitmiseks võtta vajalikke meetmeid, et jälgida, kas üldotstarbeliste tehisintellektimudelite pakkujad kohaldavad ja täidavad mõjusalt käesoleva määruse sätteid, sealhulgas nende heakskiidetud tegevusjuhendeid.

2. Järgmise etapi pakkujatel on õigus esitada kaebus käesoleva määruse väidetava rikkumise kohta. Kaebus peab olema igakülgselt põhjendatud ja selles tuleb märkida vähemalt järgmine teave:

   a) asjaomase üldotstarbelise tehisintellektimudeli pakkuja kontaktpunkt;

   b) asjakohaste faktide kirjeldus, käesoleva määruse asjaomased sätted ja põhjus, miks järgmise etapi pakkuja arvab, et üldotstarbelise tehisintellektimudeli pakkuja on rikkunud käesolevat määrust;

   c) mis tahes muu teave, mida taotluse saatnud järgmise etapi pakkuja peab asjakohaseks, sealhulgas vajaduse korral tema omal algatusel kogutud teave.

Artikkel 90

Teaduskomisjoni edastatud süsteemse riski hoiatusteated

1. Teaduskomisjon võib edastada tehisintellektiametile kvalifitseeritud hoiatusteate, kui tal on alust kahtlustada, et:

   a) üldotstarbeline tehisintellektimudel kujutab endast liidu tasandil konkreetset tuvastatavat riski või

   b) üldotstarbeline tehisintellektimudel vastab artiklis 51 osutatud tingimustele.

2. Sellise kvalifitseeritud hoiatusteate saamisel võib komisjon, tehisintellektiameti kaudu ja pärast nõukoja teavitamist teostada käesolevas jaos sätestatud volitusi kõnealuse küsimuse analüüsimiseks. Tehisintellektiamet teavitab nõukoda mis tahes meetmetest vastavalt artiklitele 91–94.

3. Kvalifitseeritud hoiatusteade peab olema igakülgselt põhjendatud ja selles tuleb märkida vähemalt järgmine teave:

   a) asjaomase süsteemse riskiga seotud üldotstarbelise tehisintellektimudeli pakkuja kontaktpunkt;

   b) asjakohaste faktide kirjeldus ja põhjus, miks teaduskomisjon hoiatusteate tegi;

   c) mis tahes muu teave, mida teaduskomisjon peab asjakohaseks, sealhulgas asjakohasel juhul tema omal algatusel kogutud teave.

Artikkel 91

Õigus taotleda dokumente ja teavet

1. Komisjon võib nõuda, et asjaomase üldotstarbelise tehisintellektimudeli pakkuja esitab artiklite 53 ja 55 kohaselt koostatud dokumendid või mis tahes lisateabe, mis on vajalik selleks, et hinnata kõnealuse pakkuja vastavust käesolevale määrusele.

2. Enne teabenõude saatmist võib tehisintellektiamet algatada üldotstarbelise tehisintellektimudeli pakkujaga struktureeritud dialoogi.

3. Teaduskomisjoni põhjendatud taotluse korral võib komisjon esitada üldotstarbelise tehisintellektimudeli pakkujale teabenõude, kui juurdepääs teabele on vajalik ja proportsionaalne teaduskomisjoni artikli 68 lõike 2 kohaste ülesannete täitmiseks.

4. Teabenõudes märgitakse nõude õiguslik alus ja eesmärk, täpsustatakse, millist teavet küsitakse, määratakse kindlaks ajavahemik, mille jooksul teave tuleb esitada, ning märgitakse, millised on artiklis 101 sätestatud trahvid ebaõige, mittetäieliku või eksitava teabe esitamise eest.

5. Asjaomase üldotstarbelise tehisintellektimudeli pakkuja või tema esindaja esitab nõutud teabe. Juriidilised isikud, äriühingud või ettevõtjad, või kui pakkuja ei ole juriidiline isik, siis isikud, kes on seaduse või põhikirja alusel volitatud neid esindama, esitavad nõutud teabe asjaomase üldotstarbelise tehisintellektimudeli pakkuja nimel. Volitatud juristid võivad esitada teavet oma klientide nimel. Kliendid jäävad siiski täielikult vastutavaks, kui esitatud teave on ebatäielik, ebaõige või eksitav.

Artikkel 92

Õigus korraldada hindamisi

1. Tehisintellektiamet võib pärast nõukojaga konsulteerimist korraldada asjaomase üldotstarbelise tehisintellektimudeli hindamisi:

   a) et hinnata, kas pakkuja täidab käesolevast määrusest tulenevaid kohustusi, kui artikli 91 kohaselt kogutud teave ei ole piisav, või

   b) et uurida süsteemse riskiga üldotstarbeliste tehisintellektimudelite süsteemseid riske liidu tasandil, eelkõige pärast teaduskomisjoni kvalifitseeritud hoiatusteadet kooskõlas artikli 90 lõike 1 punktiga a.

2. Komisjon võib otsustada määrata tema nimel hindamisi läbi viivad sõltumatud eksperdid, sealhulgas artikli 68 kohaselt loodud teaduskomisjonist. Selle ülesande täitmiseks määratud sõltumatud eksperdid peavad vastama artikli 68 lõikes 2 sätestatud kriteeriumidele.

3. Lõike 1 kohaldamisel võib komisjon taotleda juurdepääsu asjaomasele üldotstarbelisele tehisintellektimudelile rakendusliideste või muude asjakohaste tehniliste vahendite ja tööriistade, sealhulgas lähtekoodi kaudu.

4. Juurdepääsunõudes märgitakse nõude õiguslik alus, eesmärk ja põhjused ning määratakse kindlaks ajavahemik, mille jooksul juurdepääs tuleb võimaldada, ja märgitakse, millised on artiklis 101 sätestatud trahvid juurdepääsu andmisest keeldumise puhul.

5. Asjaomase üldotstarbelise tehisintellektimudeli pakkujad või selle esindajad esitavad nõutud teabe. Kui tegemist on juriidiliste isikutega, siis äriühingud või ettevõtjad, või kui pakkuja ei ole juriidiline isik, siis isikud, kes on seaduse või põhikirja alusel volitatud neid esindama, võimaldavad taotletud juurdepääsu asjaomase üldotstarbelise tehisintellektimudeli pakkuja nimel.

6. Komisjon võtab vastu rakendusaktid, milles sätestatakse hindamiste üksikasjalik kord ja tingimused, sealhulgas sõltumatute ekspertide kaasamise üksikasjalik kord, ning nende valimise kord. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 98 lõikes 2 osutatud kontrollimenetlusega.

7. Enne asjaomasele üldotstarbelisele tehisintellektimudelile juurdepääsu taotlemist võib tehisintellektiamet algatada üldotstarbelise tehisintellektimudeli pakkujaga struktureeritud dialoogi, et koguda rohkem teavet mudeli sisemise testimise, süsteemsete riskide vältimise sisemiste kaitsemeetmete ning muude sisemenetluste ja -meetmete kohta, mida pakkuja on selliste riskide maandamiseks võtnud.

Artikkel 93

Õigus nõuda meetmeid

1. Kui see on vajalik ja asjakohane, võib komisjon nõuda pakkujatelt, et nad:

   a) võtavad asjakohaseid meetmeid artiklites 53 ja 54 sätestatud kohustuste täitmiseks;

   b) rakendavad riskimaandamismeetmeid, kui artikli 92 kohaselt tehtud hindamine on tekitanud tõsiseid ja põhjendatud kahtlusi süsteemse riski kohta liidu tasandil;

   c) piiravad mudeli turul kättesaadavaks tegemist, turult kõrvaldamist või tagasivõtmist.

2. Enne meetme taotlemist võib tehisintellektiamet algatada üldotstarbelise tehisintellektimudeli pakkujaga struktureeritud dialoogi.

3. Kui lõikes 2 osutatud struktureeritud dialoogi käigus teeb süsteemse riskiga üldotstarbelise tehisintellektimudeli pakkuja ettepaneku rakendada riskimaandamismeetmeid süsteemse riski käsitlemiseks liidu tasandil, võib komisjon oma otsusega muuta need kohustused siduvaks ja teatada, et meetmete võtmiseks ei ole enam alust.

Artikkel 94

Üldotstarbelise tehisintellektimudeli ettevõtjatest operaatorite menetlusõigused

Määruse (EL) 2019/1020 artiklit 18 kohaldatakse *mutatis mutandis* üldotstarbelise tehisintellektimudeli pakkujate suhtes, ilma et see piiraks käesolevas määruses sätestatud konkreetsemaid menetlusõigusi.

X peatükk
Käitumisjuhendid ja suunised

Artikkel 95

Käitumisjuhendid erinõuete vabatahtlikuks kohaldamiseks

1. Tehisintellektiamet ja liikmesriigid julgustavad ja hõlbustavad käitumisjuhendite, sealhulgas nendega seotud juhtimismehhanismide koostamist, eesmärgiga edendada osa või kõigi III peatüki 2. jaos sätestatud nõuete vabatahtlikku kohaldamist muude kui suure riskiga tehisintellektisüsteemide suhtes, võttes arvesse kättesaadavaid tehnilisi lahendusi ja tööstusharu parimaid tavasid, mis võimaldavad selliseid nõudeid kohaldada.

2. Tehisintellektiamet ja liikmesriigid hõlbustavad selliste käitumisjuhendite koostamist, mis käsitlevad erinõuete vabatahtlikku kohaldamist kõigi tehisintellektisüsteemide suhtes, sealhulgas juurutajate poolt, võttes aluseks selged eesmärgid ja peamised tulemusnäitajad, et mõõta nende eesmärkide saavutamist, hõlmates muu hulgas järgmisi elemente:

a) liidu usaldusväärse tehisintellekti eetikasuunistes sätestatud kohaldatavad elemendid;

b) tehisintellektisüsteemide keskkonnakestlikkusele avalduva mõju hindamine ja minimeerimine, sealhulgas seoses energiatõhusa kavandamise ja tehisintellekti tõhusa projekteerimise, treenimise ja kasutamise meetoditega;

c) tehisintellektipädevuse edendamine, eelkõige tehisintellekti arendamise, toimimise ja kasutamisega tegelevate isikute puhul;

d) tehisintellektisüsteemide kaasava ja mitmekesise projekteerimise hõlbustamine, sealhulgas kaasavate ja mitmekesiste arendusmeeskondade loomise ning sidusrühmade selles protsessis osalemise edendamise kaudu;

e) tehisintellektisüsteemide poolt kaitsetutele isikutele või kaitsetute isikute rühmadele ning samuti soolisele võrdõiguslikkusele avalduva negatiivse mõju hindamine ja ennetamine, sealhulgas seoses puuetega inimeste juurdepääsuga.

3. Käitumisjuhendeid võivad koostada üksikud tehisintellektisüsteemide pakkujad või juurutajad või nende esindusorganisatsioonid või mõlemad, kaasates sellesse tegevusse huvitatud sidusrühmi ning nende esindusorganisatsioone, sealhulgas kodanikuühiskonna organisatsioone ja akadeemilisi ringkondi. Käitumisjuhendid võivad käia ühe või mitme tehisintellektisüsteemi kohta, võttes arvesse asjaomaste süsteemide sihtotstarbe sarnasusi.

4. Käitumisjuhendite koostamist edendades ja hõlbustades võtavad tehisintellektiamet ja liikmesriigid arvesse VKEde, sealhulgas idufirmade erihuve ja vajadusi.

Artikkel 96

Komisjoni suunised käesoleva määruse rakendamise kohta

1. Komisjon töötab välja suunised käesoleva määruse praktilise rakendamise kohta, eriti järgmise kohta:

   a) artiklites 8–15 ja artiklis 25 osutatud nõuete ja kohustuste kohaldamine;

   b) artiklis 5 osutatud keelatud kasutusviisid;

   c) oluliste muudatustega seotud sätete praktiline rakendamine;

   d) artiklis 50 sätestatud läbipaistvuskohustuste praktiline rakendamine;

e) üksikasjalik teave käesoleva määruse seose kohta I lisas loetletud liidu ühtlustamisõigusaktidega ja muu asjakohase liidu õigusega, sealhulgas nende täitmise tagamise järjepidevusega;

f) artikli 3 punktis 1 sätestatud tehisintellektisüsteemi määratluse kohaldamine.

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

Käesoleva lõike esimeses lõigus osutatud suunistes võetakse nõuetekohaselt arvesse tehisintellekti valdkonna tehnika üldtunnustatud taset ning artiklites 40 ja 41 osutatud asjakohaseid harmoneeritud standardeid ja ühtseid kirjeldusi või neid harmoneeritud standardeid või tehnilisi kirjeldusi, mis on sätestatud liidu ühtlustamisõiguse kohaselt.

2. Liikmesriikide või tehisintellektiameti taotlusel või omal algatusel ajakohastab komisjon varem vastu võetud suuniseid, kui seda peetakse vajalikuks.

XI peatükk
Volituste delegeerimine ja komiteemenetlus

Artikkel 97

Delegeeritud volituste rakendamine

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

2. Artikli 6 lõikes 6 ja artikli 7 lõikes 4, artikli 7 lõigetes 1 ja 3, artikli 11 lõikes 3, artikli 43 lõigetes 5 ja 6, artikli 47 lõikes 5, artikli 51 lõikes 3, artikli 52 lõikes 4 ja artikli 53 lõigetes 5 ja 6 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 6 lõigetes 6 ja 7, artikli 7 lõigetes 1 ja 3, artikli 11 lõikes 3, artikli 43 lõigetes 5 ja 6, artikli 47 lõikes 5, artikli 51 lõikes 3, artikli 52 lõikes 4 ja artikli 53 lõigetes 5 ja 6 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 otsuses nimetatud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.

4. Enne delegeeritud õigusakti vastuvõtmist konsulteerib komisjon kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes sätestatud põhimõtetega iga liikmesriigi määratud ekspertidega.

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

6. Artikli 6 lõike 6 või 7, artikli 7 lõike 1 või 3, artikli 11 lõike 3, artikli 43 lõike 5 või 6, artikli 47 lõike 5, artikli 51 lõike 3, artikli 52 lõike 4 või artikli 53 lõike 5 või 6 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 98

Komiteemenetlus

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

2. Käesolevale lõikele viitamisel kohaldatakse määruse (EL) nr 182/2011 artiklit 5.

XII peatükk
Karistused

Artikkel 99

Karistused

1. Kooskõlas käesolevas määruses sätestatud tingimustega kehtestavad liikmesriigid õigusnormid karistuste ja muude täitemeetmete kohta, mis võivad hõlmata ka hoiatusi ja mitterahalisi meetmeid, mida kohaldatakse operaatorite poolt käesoleva määruse rikkumise korral, ning võtavad kõik vajalikud meetmed, et tagada nende nõuetekohane ja tõhus rakendamine, võttes sellega arvesse komisjoni poolt artikli 96 kohaselt välja antud suuniseid. Kehtestatud karistused peavad olema mõjusad, proportsionaalsed ja hoiatavad. Neis tuleb arvesse võtta VKEde, sealhulgas idufirmade huve ja nende majanduslikku elujõulisust.

2. Liikmesriigid teavitavad komisjoni viivitamata ja hiljemalt kohaldamise alguskuupäeval lõikes 1 osutatud karistusnormidest ja muudest täitemeetmetest ning teavitavad teda viivitamata nende hilisematest muudatustest.

3. Artiklis 5 osutatud tehisintellekti kasutusviiside keelu rikkumise korral kohaldatakse haldustrahvi kuni 35 000 000 eurot, või kui rikkuja on ettevõtja, kuni 7 % tema eelmise majandusaasta ülemaailmsest kogukäibest olenevalt sellest, kumb on suurem.

4. Mittevastavuse korral mõnele järgmisele operaatorite või teada antud asutustega seotud sättele, välja arvatud need, mis on sätestatud artiklis 5, kohaldatakse haldustrahvi kuni 15 000 000 eurot, või kui rikkuja on ettevõtja, kuni 3 % tema eelmise majandusaasta ülemaailmsest kogukäibest olenevalt sellest, kumb on suurem:

   a) pakkujate kohustused vastavalt artiklile 16;

   b) volitatud esindajate kohustused vastavalt artiklile 22;

   c) importijate kohustused vastavalt artiklile 23;

   d) turustajate kohustused vastavalt artiklile 24;

   e) juurutajate kohustused vastavalt artiklile 26;

   f) teada antud asutuste nõuded ja kohustused vastavalt artiklile 31, artikli 33 lõigetele 1, 3 ja 4 või artiklile 34;

   g) pakkujate ja juurutajate läbipaistvuskohustused vastavalt artiklile 50.

5. Kui teada antud asutustele või riigi pädevatele asutustele on taotluse peale esitatud vale, ebatäielikku või eksitavat teavet, kohaldatakse haldustrahve kuni 7 500 000 eurot, või kui rikkuja on ettevõtja, kuni 1 % tema eelmise majandusaasta ülemaailmsest kogukäibest olenevalt sellest, kumb on suurem.

6. VKEde, sealhulgas idufirmade puhul sõltub iga käesolevas artiklis osutatud trahv lõigetes 3, 4 ja 5 osutatud protsendimäärast või summast, olenevalt sellest, kumb on väiksem.

7. 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, võttes arvesse tehisintellektisüsteemi eesmärki ning asjakohasel juhul mõjutatud isikute arvu ja neile tekitatud kahju suurust;

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

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

d) rikkumise toime pannud operaatori suurus, aastakäive ja turuosa;

e) juhtumi asjaolude suhtes kohaldatavad igasugused muud raskendavad või kergendavad tegurid, näiteks rikkumisest otseselt või kaudselt saadud finantskasu või välditud kahju;

f) mil määral tehakse koostööd riigi pädevate asutustega rikkumise heastamiseks ja rikkumise võimaliku kahjuliku mõju leevendamiseks;

g) operaatori vastutuse ulatus, võttes arvesse tema rakendatud tehnilisi ja korralduslikke meetmeid;

h) mil viisil said riigi pädevad asutused rikkumisest teada, eelkõige kas operaator teatas rikkumisest ja millises ulatuses ta seda tegi;

i) kas rikkumine pandi toime tahtlikult või hooletusest;

j) operaatori võetud meetmed mõjutatud isikutele tekitatud kahju leevendamiseks.

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

9. 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.

10. Käesoleva artikli kohaste volituste kasutamise suhtes kohaldatakse kooskõlas liidu ja riigisisese õigusega asjakohaseid menetluslikke kaitsemeetmeid, sealhulgas tõhusaid õiguskaitsevahendeid ja nõuetekohast menetlust.

11. Liikmesriigid esitavad komisjonile igal aastal aruande käesoleva artikli kohaselt määratud haldustrahvide ning nendega seotud kohtuvaidluste või kohtumenetluste kohta.

Artikkel 100

Liidu institutsioonide, organite ja asutuste suhtes kohaldatavad haldustrahvid

1. Euroopa Andmekaitseinspektor võib määrata haldustrahve käesoleva määruse kohaldamisalasse kuuluvatele liidu institutsioonidele, organitele ja asutustele. 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; võetakse arvesse asjaomase tehisintellektisüsteemi eesmärki ning asjakohasel juhul mõjutatud isikute arvu ja neile tekitatud kahju suurust;

   b) liidu institutsiooni, organi või asutuse vastutuse suurus, võttes arvesse tema rakendatud tehnilisi ja korralduslikke meetmeid;

   c) liidu institutsiooni, organi või asutuse poolt võetud meetmed mõjutatud isikutele tekitatud kahju leevendamiseks;

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

e) liidu institutsiooni, organi või asutuse varasemad sarnased rikkumised;

f) millisel viisil sai Euroopa Andmekaitseinspektor rikkumisest teada, eelkõige kas liidu institutsioon, organ või asutus teatas rikkumisest ja millises ulatuses ta seda tegi;

g) liidu institutsiooni, organi või asutuse aastaeelarve.

2. Artiklis 5 osutatud tehisintellekti kasutusviiside keelu rikkumise korral kohaldatakse haldustrahve kuni 1 500 000 eurot.

3. Kui tehisintellektisüsteem ei vasta mõnele käesolevast määrusest tulenevale nõudele või kohustusele, välja arvatud need, mis on sätestatud artiklis 5, kohaldatakse haldustrahvi kuni 750 000 eurot.

4. Enne käesoleva artikli alusel otsuse tegemist annab Euroopa Andmekaitseinspektor liidu institutsioonile, organile või asutusele, 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 laekuvad liidu üldeelarvesse. Trahvid ei tohi mõjutada trahvi saanud liidu institutsiooni, organi või asutuse tõhusat toimimist.

7. Euroopa Andmekaitseinspektor teavitab igal aastal komisjoni käesoleva artikli kohaselt tema poolt määratud haldustrahvidest ja algatatud kohtuvaidlustest või kohtumenetlustest.

Artikkel 101

Üldotstarbeliste tehisintellektimudelite pakkujate trahvid

1. Komisjon võib üldotstarbeliste tehisintellektimudelite pakkujatele määrata trahve, mis ei ületa 3 % nende eelmise majandusaasta ülemaailmsest kogukäibest või 15 000 000 eurot, olenevalt sellest, kumb summa on suurem, kui komisjon leiab, et pakkuja tahtlikult või hooletusest:

   a) rikub käesoleva määruse asjakohaseid sätteid;

   b) ei ole täitnud artikli 91 kohast dokumendi- või teabenõuet või esitas ebaõiget, mittetäielikku või eksitavat teavet;

c) ei täitnud artikli 93 alusel nõutud meedet;

d) ei andnud komisjonile juurdepääsu üldotstarbelisele tehisintellektimudelile või süsteemse riskiga üldotstarbelisele tehisintellektimudelile, et viia läbi artikli 92 kohane hindamine.

Trahvi või sunniraha summa kindlaksmääramisel võetakse arvesse rikkumise olemust, raskusastet ja kestust, võttes nõuetekohaselt arvesse proportsionaalsuse ja asjakohasuse põhimõtteid. Komisjon võtab arvesse ka kohustusi, mis on võetud vastavalt artikli 93 lõikele 3 või esitatud asjakohastes tegevusjuhistes vastavalt artiklile 56.

2. Enne lõike 1 kohase otsuse vastuvõtmist edastab komisjon oma esialgsed järeldused üldotstarbelise tehisintellektimudeli pakkujale ja annab talle võimaluse esitada oma seisukohad.

3. Käesoleva artikli kohaselt määratud trahvid peavad olema mõjusad, proportsionaalsed ja hoiatavad.

4. Teave käesoleva artikli alusel määratud trahvide kohta edastatakse vajaduse korral ka nõukojale.

5. Euroopa Liidu Kohtul on täielik pädevus komisjoni poolt käesoleva artikli kohaselt tehtud trahvimääramise otsused läbi vaadata. Kohus võib määratud trahvi tühistada, seda vähendada või suurendada.

6. Komisjon võtab vastu rakendusaktid, mis sisaldavad käesoleva artikli lõike 1 kohaste otsuste võimaliku vastuvõtmisega seotud menetluste üksikasjalikku korda ja menetlustagatisi. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 98 lõikes 2 osutatud kontrollimenetlusega.

XIII peatükk
Lõppsätted

Artikkel 102

Määruse (EÜ) nr 300/2008 muutmine

Määruse (EÜ) nr 300/2008 artikli 4 lõikesse 3 lisatakse järgmine lõik:

„Võttes vastu üksikasjalikke meetmeid turvaseadmete tehniliste kirjelduste ning nende heakskiitmise ja kasutamise korra kohta, mis on seotud tehisintellektisüsteemidega Euroopa Parlamendi ja nõukogu määruse (EL) 2024/…[*+] tähenduses, võetakse arvesse nimetatud määruse III peatüki 2. jaos sätestatud nõudeid.

---

[*] Euroopa Parlamendi ja nõukogu … määrus (EL) 2024/…, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ja muudetakse määrusi (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ja direktiivid 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828 (tehisintellektimäärus) (ELT L, …, ELI: …).“

[+] ELT: palun sisestada teksti käesoleva määruse (2021/0106(COD)) number ja täiendada vastavat joonealust märkust.

Artikkel 103

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) 2024/…[*+] tähenduses, võetakse arvesse nimetatud määruse III peatüki 2. jaos sätestatud nõudeid.

---

[*] Euroopa Parlamendi ja nõukogu … määrus (EL) 2024/…, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ja muudetakse ja määrusi (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ja direktiivid 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828 (tehisintellektimäärus) (ELT L, …, ELI: …).“

[+] ELT: palun sisestada teksti käesoleva määruse (2021/0106(COD)) number ja täiendada vastavat joonealust märkust.

Artikkel 104

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) 2024/…[*+] tähenduses, võetakse arvesse nimetatud määruse III peatüki 2. jaos sätestatud nõudeid.

---

[*] Euroopa Parlamendi ja nõukogu … määrus (EL) 2024/…, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ja muudetakse määrusi (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ja direktiivid 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828 (tehisintellektimäärus) (ELT L, …, ELI: …).“

[+] ELT: palun sisestada teksti käesoleva määruse (2021/0106(COD)) number ja täiendada vastavat joonealust märkust.

Artikkel 105

Direktiivi 2014/90/EL muutmine

Direktiivi 2014/90/EL artiklisse 8 lisatakse järgmine lõige:

„5. 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) 2024/…[*+] tähenduses, võtab komisjon arvesse nimetatud määruse III peatüki 2. jaos sätestatud nõudeid.

---

[*] Euroopa Parlamendi ja nõukogu … määrus (EL) 2024/…, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ja muudetakse määrusi (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ja direktiivid 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828 (tehisintellektimäärus) (ELT L, …, ELI: …).“

[+] ELT: palun sisestada teksti käesoleva määruse (2021/0106(COD)) number ja täiendada vastavat joonealust märkust.

Artikkel 106

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) 2024/…[*+] tähenduses, võetakse arvesse nimetatud määruse III peatüki 2. jaos sätestatud nõudeid.

---

[*] Euroopa Parlamendi ja nõukogu … määrus (EL) 2024/…, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ja muudetakse määrusi (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ja direktiivid 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828 (tehisintellektimäärus) (ELT L, …, ELI: …).“

[+] ELT: palun sisestada teksti käesoleva määruse (2021/0106(COD)) number ja täiendada vastavat joonealust märkust.

Artikkel 107

Määruse (EL) 2018/858 muutmine

Määruse (EL) 2018/858 artiklisse 5 lisatakse järgmine lõige:

„4. Võttes vastu esimese lõigu kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) 2024/…[*+] tähenduses, võetakse arvesse nimetatud määruse III peatüki 2. jaos sätestatud nõudeid.

---

[*] Euroopa Parlamendi ja nõukogu … määrus (EL) 2024/…, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ja muudetakse määrusi (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ja direktiivid 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828 (tehisintellektimäärus) (ELT L, …, ELI: …).“

[+] ELT: palun sisestada teksti käesoleva määruse (2021/0106(COD)) number ja täiendada vastavat joonealust märkust.

Artikkel 108

Määruse (EL) 2018/1139 muutmine

Määrust (EL) 2018/1139 muudetakse järgmiselt.

1) Artiklisse 17 lisatakse järgmine lõige:

„3. Ilma et see piiraks lõike 2 kohaldamist, kui võetakse vastu lõike 1 kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) 2024/…[*+] tähenduses, võetakse arvesse nimetatud määruse III peatüki 2. jaos sätestatud nõudeid.

---

[*] Euroopa Parlamendi ja nõukogu … määrus (EL) 2024/…, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ja muudetakse määrusi (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ja direktiivid 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828 (tehisintellektimäärus) (ELT L, …, ELI: …).“

2) Artiklisse 19 lisatakse järgmine lõige:

„4. Võttes vastu lõigete 1 ja 2 kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid määruse (EL) 2024/…[++] tähenduses, võetakse arvesse nimetatud määruse III peatüki 2. jaossätestatud nõudeid.“

[+] ELT: palun sisestada teksti käesoleva määruse (2021/0106(COD)) number ja täiendada vastavat joonealust märkust.

[++] ELT: palun lisada käesoleva määruse (2021/0106(COD)) number.

3) Artiklisse 43 lisatakse järgmine lõige:

„4. Võttes vastu lõike 1 kohaseid rakendusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid määruse (EL) 2024/…[+] tähenduses, võetakse arvesse nimetatud määruse III peatüki 2. jaos 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) 2024/…[+] tähenduses, võetakse arvesse nimetatud määruse III peatüki 2. jaos sätestatud nõudeid.“

5) Artiklisse 57 lisatakse järgmine lõik:

„Võttes vastu kõnealuseid rakendusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid määruse (EL) 2024/…[+] tähenduses, võetakse arvesse nimetatud määruse III peatüki 2. jaos 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) 2024/…[+] tähenduses, võetakse arvesse nimetatud määruse III peatüki 2. jaos sätestatud nõudeid.“

[+] ELT: palun lisada käesoleva määruse (2021/0106(COD)) number.

Artikkel 109

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) 2024/…[*++] tähenduses, võetakse arvesse nimetatud määruse III peatüki 2. jaos sätestatud nõudeid.

---

[*] Euroopa Parlamendi ja nõukogu … määrus (EL) 2024/…, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ja muudetakse määrusi (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ja direktiivid 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828 (tehisintellektimäärus) (ELT L, …, ELI: …).“

[++] ELT: palun sisestada teksti käesoleva määruse (2021/0106(COD)) number ja täiendada vastavat joonealust märkust.

Artikkel 110

Direktiivi (EL) 2020/1828 muutmine

Euroopa Parlamendi ja nõukogu direktiivi (EL) 2020/1828[58] I lisasse lisatakse järgmine punkt:

„68) Euroopa Parlamendi ja nõukogu määrus (EL) 2024/…[+], millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ja muudetakse määrusi (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ja direktiivid 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828 (tehisintellektimäärus) (ELT L, …, ELI: …)“.

Artikkel 111

Juba turule lastud või kasutusele võetud tehisintellektisüsteemid ning juba turule lastud üldotstarbelised tehisintellektimudelid

1. Ilma et see piiraks artikli 5 kohaldamist, nagu on osutatud artikli 113 lõike 3 punktis a, viiakse tehisintellektisüsteemid, mis on X lisas loetletud õigusaktidega loodud suuremahuliste IT-süsteemide komponendid ja mis on turule lastud või kasutusele võetud enne … [36 kuud pärast käesoleva määruse jõustumise kuupäeva], käesoleva määrusega vastavusse 31. detsembriks 2030.

---

[58] Euroopa Parlamendi ja nõukogu 25. novembri 2020. aasta direktiiv (EL) 2020/1828, mis käsitleb tarbijate kollektiivsete huvide kaitsmise esindushagisid ja millega tunnistatakse kehtetuks direktiiv 2009/22/EÜ (ELT L 409, 4.12.2020, lk 1).

[+] ELT: Palun sisestada teksti käesoleva määruse kuupäev ja number (2021/0106(COD)).

Käesolevas määruses sätestatud nõudeid võetakse arvesse, kui hinnatakse X lisas loetletud õigusaktidega loodud suuremahulisi IT-süsteeme neis õigusaktides sätestatud korra kohaselt ning kui need õigusaktid asendatakse või neid muudetakse.

2. Ilma et see piiraks artikli 5 kohaldamist, nagu on osutatud artikli 113 lõike 3 punktis a, kohaldatakse käesolevat määrust selliste suure riskiga tehisintellektisüsteemide, välja arvatud käesoleva artikli lõikes 1 osutatud süsteemid, mis on turule lastud või kasutusele võetud enne … [24 kuud pärast käesoleva määruse jõustumise kuupäeva], operaatorite suhtes üksnes juhul, kui alates sellest kuupäevast on nende süsteemide projekti oluliselt muudetud. Igal juhul võtavad ametiasutustele kasutamiseks mõeldud suure riskiga tehisintellektisüsteemide pakkujad ja juurutajad käesoleva määruse nõuete täitmiseks vajalikud meetmed hiljemalt … [kuus aastat pärast käesoleva määruse jõustumise kuupäeva].

3. Selliste üldotstarbeliste tehisintellektimudelite pakkujad, mis on turule lastud enne … [12 kuud pärast käesoleva määruse jõustumise kuupäeva], võtavad vajalikud meetmed, et täita käesolevas määruses sätestatud kohustused hiljemalt … [36 kuud pärast käesoleva määruse jõustumise kuupäeva].

Artikkel 112

Hindamine ja läbivaatamine

1. Komisjon hindab pärast käesoleva määruse jõustumist kord aastas ning artiklis 97 sätestatud volituste delegeerimise tähtaja lõpuni seda, kas III lisas esitatud loetelu ja artiklis 5 sätestatud tehisintellekti keelatud kasutusviiside loetelu on vaja muuta. Komisjon esitab kõnealuse hindamise tulemused Euroopa Parlamendile ja nõukogule.

2. Hiljemalt … [neli aastat pärast käesoleva määruse jõustumise kuupäeva] ja seejärel iga nelja aasta järel hindab komisjon järgmist ja esitab selle kohta aruande Euroopa Parlamendile ja nõukogule:

   a) vajadus teha muudatusi, et laiendada III lisas olemasolevaid valdkondade rubriike või lisada uusi valdkondade rubriike;

   b) muudatused nende tehisintellektisüsteemide loetelus, mille puhul on vaja täiendavaid läbipaistvusmeetmeid vastavalt artiklile 50;

   c) muudatused, mis suurendavad järelevalve- ja juhtimissüsteemi tõhusust.

3. Komisjon esitab Euroopa Parlamendile ja nõukogule hiljemalt … [viis aastat pärast käesoleva määruse jõustumise kuupäeva] ning pärast seda iga nelja aasta järel aruande käesoleva määruse hindamise ja läbivaatamise kohta. Aruanne sisaldab hinnangut täitmise tagamise struktuuri kohta ja võimaliku vajaduse kohta, et liidu asutus kõrvaldaks tuvastatud puudused. Tähelepanekute põhjal lisatakse aruandele vajaduse korral ettepanek käesoleva määruse muutmiseks. Aruanded avalikustatakse.

4. Lõikes 2 osutatud aruannetes pööratakse erilist tähelepanu järgmisele:

   a) riigi pädevate asutuste rahaliste, tehniliste ja inimressursside olukord, et nad saaksid tulemuslikult täita neile käesoleva määruse alusel määratud ülesandeid;

   b) olukord seoses artikli 99 lõikes 1 osutatud karistuste, eelkõige haldustrahvidega, mida liikmesriigid kohaldavad käesoleva määruse rikkumise korral;

   c) vastuvõetud harmoneeritud standardid ja ühtsed kirjeldused, mis on välja töötatud käesoleva määruse toetamiseks;

   d) pärast käesoleva määruse jõustumist turule sisenevate ettevõtjate arv ja kui paljud neist on VKEd.

5. Hiljemalt … [neli aastat pärast käesoleva määruse jõustumise kuupäeva] hindab komisjon tehisintellektiameti toimimist, kas tehisintellektiametile on antud piisavad volitused ja pädevused oma ülesannete täitmiseks ning kas käesoleva määruse nõuetekohaseks rakendamiseks ja täitmise tagamiseks on asjakohane ja vajalik tõsta tehisintellektiameti staatust ning suurendada selle täitmise tagamise pädevust ja vahendeid. Komisjon esitab hindamisaruande Euroopa Parlamendile ja nõukogule.

6. Hiljemalt … [neli aastat pärast käesoleva määruse jõustumise kuupäeva] ja seejärel iga nelja aasta tagant esitab komisjon aruande üldotstarbeliste tehisintellektimudelite energiatõhusat arendamist käsitlevate standardimisdokumentide väljatöötamisel tehtud edusammude läbivaatamise kohta ning hindab vajadust täiendavate meetmete või tegevuste, sealhulgas siduvate meetmete või tegevuste järele. Nimetatud aruanne esitatakse Euroopa Parlamendile ja nõukogule ning see avalikustatakse.

7. Komisjon hindab hiljemalt … [neli aastat *pärast käesoleva määruse jõustumise kuupäeva*] ja pärast seda iga kolme aasta järel, kui mõjusalt ja tulemuslikult on vabatahtlikkusel põhinevad käitumisjuhendid edendanud III peatüki 2. jaos sätestatud muude kui suure riskiga tehisintellektisüsteemide ja võimaluse korral muude kui suure riskiga tehisintellektisüsteemide muude täiendavate nõuete kohaldamist, muu hulgas seoses keskkonnakestlikkusega.

8. Lõigete 1–7 kohaldamisel esitavad nõukoda, liikmesriigid ja riikide pädevad asutused komisjonile tema taotluse korral põhjendamatu viivituseta teavet.

9. Lõigetes 1–7 osutatud hindamiste ja läbivaatamiste käigus võtab komisjon arvesse nõukoja, Euroopa Parlamendi, nõukogu ning muude asjaomaste organite ja allikate seisukohti ja tähelepanekuid.

10. Komisjon esitab vajaduse korral asjakohased ettepanekud käesoleva määruse muutmiseks, eelkõige võttes arvesse tehnika arengut, tehisintellektisüsteemide mõju tervisele, ohutusele ja põhiõigustele, ning võttes arvesse infoühiskonna arengut.

11. Käesoleva artikli lõigetes 1–7 osutatud hindamiste ja läbivaatamiste hõlbustamiseks arendab tehisintellektiamet riskitasemete hindamiseks välja objektiivse ja osalusel põhineva metoodika, mis põhineb asjaomastes artiklites sätestatud kriteeriumidel ja uute süsteemide lisamisel järgmistesse loeteludesse:

    a) III lisas sätestatud loetelu, sealhulgas olemasolevate valdkondade rubriikide laiendamine või uute valdkondade rubriikide lisamine sellesse lisasse;

    b) artiklis 5 sätestatud keelatud kasutusviiside loetelu ning,

    c) nende tehisintellektisüsteemide loetelu, mille puhul on vaja täiendavaid läbipaistvusmeetmeid vastavalt artiklile 50.

12. Mis tahes lõike 10 kohases käesoleva määruse muudatuses või asjakohases delegeeritud õigusaktis või rakendusaktis, mis puudutab I lisa B jaos esitatud valdkondlikke liidu ühtlustamisõigusakte, võetakse arvesse iga sektori regulatiivseid eripärasid ning olemasolevaid juhtimis-, vastavushindamis- ja täitmise tagamise mehhanisme ning nendega loodud asutusi.

13. Hiljemalt … [seitse aastat pärast käesoleva määruse jõustumise kuupäeva] teeb komisjon käesoleva määruse jõustamise hindamise ja esitab selle kohta aruande Euroopa Parlamendile, nõukogule ning Euroopa Majandus- ja Sotsiaalkomiteele, võttes arvesse käesoleva määruse kohaldamise esimesi aastaid. Selle hindamise tulemuste põhjal ja kui see on asjakohane, lisatakse aruandele ettepanek käesoleva määruse muutmiseks seoses täitmise tagamise struktuuriga ja vajadusega luua liidu amet tuvastatud puuduste kõrvaldamiseks.

Artikkel 113

Jõustumine ja kohaldamine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas.*

Käesolevat määrust kohaldatakse alates … [24 kuud pärast käesoleva määruse jõustumise kuupäeva].

Kuid:

a) I ja II peatükki kohaldatakse alates … [kuus kuud pärast käesoleva määruse jõustumise kuupäeva];

b) III peatüki 4. jagu, V peatükki, VII peatükki, XII peatükki ja artiklit 78 kohaldatakse alates … [12 kuud pärast käesoleva määruse jõustumise kuupäeva], välja arvatud artikkel 101;

c) artikli 6 lõiget 1 ja käesolevas määruses sätestatud vastavaid kohustusi kohaldatakse alates … [36 kuud pärast käesoleva määruse jõustumise kuupäeva].

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

I LISA

Liidu ühtlustamisõigusaktide loetelu

A jagu. 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)

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 jagu. Muude liidu ühtlustamisõigusaktide loetelu

13. 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)

14. 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)

15. 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)

16. 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)

17. 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)

18. 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)

19. 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)

20. 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), niivõrd, 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 kaugjuhtimisseadmetega

II LISA

Artikli 5 lõike 1 esimese lõigu punkti h alapunktis iii osutatud kuritegude loetelu

Artikli 5 lõike 1 esimese lõigu punkti h alapunktis iii osutatud kuriteod:

– terrorism,

– inimkaubandus,

– laste seksuaalne ekspluateerimine ning lasteporno,

– ebaseaduslik kauplemine narkootiliste või psühhotroopsete ainetega,

– ebaseaduslik kauplemine relvade, laskemoona või lõhkeainetega,

– tahtlik tapmine, raskete kehavigastuste tekitamine,

– ebaseaduslik kauplemine inimorganite või -kudedega,

– ebaseaduslik kauplemine tuumamaterjalide või radioaktiivsete ainetega,

– inimröövi, ebaseaduslik vabadusevõtmine või pantvangi võtmine,

– Rahvusvahelise Kriminaalkohtu pädevusse kuuluvad kuriteod,

– õhusõiduki või laeva kaaperdamine,

– vägistamine,

– keskkonna vastu suunatud kuriteod,

– organiseeritud või relvastatud röövv,

– sabotaaž,

– osalemine kuritegelikus organisatsioonis, mis on seotud ühe või mitme eespool loetletud kuriteoga.

III LISA

Artikli 6 lõikes 2 osutatud suure riskiga tehisintellektisüsteemid

Artikli 6 lõike 2 kohaselt on suure riskiga tehisintellektisüsteemid järgmistes valdkondades loetletud tehisintellektisüsteemid.

1. Biomeetria, kui selliste süsteemide kasutamine on lubatud asjakohase liidu või riigisisese õigusega:

   a) biomeetrilise kaugtuvastamise süsteemid.

      See ei hõlma tehisintellektisüsteeme, mis on ette nähtud kasutamiseks biomeetriliseks kontrolliks ja mille ainus eesmärk on kinnitada, et konkreetne füüsiline isik on isik, kes ta väidab end olevat;

   b) tehisintellektisüsteemid, mis on ette nähtud biomeetriliseks liigitamiseks tundlike või kaitstud atribuutide või omaduste alusel, mis põhinevad nende atribuutide või omadustega seotud järeldustel;

   c) tehisintellektisüsteemid, mis on ette nähtud emotsioonituvastuseks.

2. Elutähtis taristu: tehisintellektisüsteemid, mis on ette nähtud kasutamiseks elutähtsa digitaristu, maanteeliikluse või vee, gaasi, kütteenergia või elektri tarnimise korraldamise ja käitamise turvakomponentidena.

3. Haridus ja kutseõpe:

a) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks selleks, et määrata kindlaks füüsiliste isikute juurdepääs haridus- ja kutseõppeasutustele või nende vastuvõtmine või määramine nendesse kõigil tasanditel;

b) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks õpiväljundite hindamiseks, muu hulgas juhul, kui neid väljundeid kasutatakse füüsiliste isikute õppeprotsessi suunamiseks haridus- ja kutseõppeasutustes kõigil tasanditel;

c) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks selleks, et hinnata sobivat haridustaset, mille isik saab või millele tal on juurdepääs kõigi tasandite haridus- ja kutseõppeasutustes;

d) tehisintellektisüsteemid, mis on ette nähtud õpilaste keelatud käitumise jälgimiseks ja avastamiseks kõigi tasandite haridus- ja kutseõppeasutustes tehtavate testide ajal.

4. Tööhõive, töötajate juhtimine ja iseenda tööandjana tegutsemise võimaldamine:

a) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks füüsiliste isikute töölevõtmiseks või valimiseks, eelkõige sihipäraste töökuulutuste avaldamiseks, tööle kandideerimise taotluste analüüsimiseks ja filtreerimiseks ning kandidaatide hindamiseks;

b) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks selleks, et teha otsuseid, mis mõjutavad tööga seotud suhteid, edutamist ja tööga seotud lepinguliste suhete lõpetamist, et jagada isiku käitumise või isikuomaduste või erijoonte põhjal tööülesandeid või tegeleda selliste suhete kontekstis inimeste töötulemuste ja käitumise seire ja hindamisega

5. Oluliste erateenuste ning oluliste avalike teenuste ja hüvede kättesaadavus ja kasutamine:

a) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks ametiasutustele või nende nimel, et hinnata füüsiliste isikute vastavust oluliste avalike hüvede ja teenuste, sealhulgas tervishoiuteenuste saamise tingimustele, samuti selleks, et selliseid hüvesid ja teenuseid anda, vähendada, tühistada või tagasi nõuda;

b) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks selleks, et hinnata füüsiliste isikute krediidikõlblikkust või anda neile krediidihinnang, välja arvatud tehisintellektisüsteemid, mida kasutatakse finantspettuste avastamiseks;

c) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks füüsiliste isikutega seotud riskihindamiseks ja hinnakujunduseks elu- ja tervisekindlustuse puhul;

d) tehisintellektisüsteemid, mis on ette nähtud füüsiliste isikute hädaabikõnede hindamiseks ja liigitamiseks või kasutamiseks kiirabi ja päästeteenistuse, sealhulgas politsei, tuletõrje ja arstiabi väljasaatmiseks ja väljasaatmisprioriteetide seadmiseks ning erakorralise arstiabi patsientide triaaži süsteemide tööks.

6. Õiguskaitse, kui selliste süsteemide kasutamine on lubatud asjakohase liidu või riigisisese õigusega:

a) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks õiguskaitseasutustele või nende nimel või liidu institutsioonidele, organitele või asutustele õiguskaitseasutuste toetamiseks või nende nimel, et hinnata füüsilise isiku riski langeda kuriteo ohvriks;

b) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks õiguskaitseasutustele või nende nimel või liidu institutsioonidele, organitele või asutustele õiguskaitseasutuste toetamiseks valedetektori või sarnase vahendina;

c) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks õiguskaitseasutustele või nende nimel või liidu institutsioonidele, organitele ja asutustele õiguskaitseasutuste toetamiseks, et hinnata tõendite usaldusväärsust kuritegude uurimise või nende eest vastutusele võtmise käigus;

d) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks õiguskaitseasutustele või nende nimel või liidu institutsioonidele, organitele ja asutustele õiguskaitseasutuste toetamiseks, et hinnata füüsilise isiku poolt õigusrikkumise või korduva õigusrikkumise toimepanemise riski mitte üksnes füüsiliste isikute profiilianalüüsi põhjal, nagu on osutatud direktiivi (EL) 2016/680 artikli 3 punktis 4, või hinnata füüsiliste isikute või rühmade isikuomadusi, erijooni või varasemat kuritegelikku käitumist;

e) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks õiguskaitseasutustele või nende nimel või liidu institutsioonidele, organitele ja asutustele õiguskaitseasutuste toetamiseks, et teha kuritegude avastamise, uurimise või nende eest vastutusele võtmise käigus füüsiliste isikute profiilianalüüsi, nagu on osutatud direktiivi (EL) 2016/680 artikli 3 lõikes 4.

7. Rände-, varjupaiga- ja piirikontrollihaldus, kui selliste süsteemide kasutamine on lubatud asjakohase liidu või riigisisese õigusega:

a) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks pädevatele asutustele või nende nimel või kasutamiseks liidu institutsioonidele, organitele või asutustele valedetektorite ja muude samalaadsete vahenditena;

b) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks pädevatele ametiasutustele või nende nimel või liidu institutsioonidele, asutustele ja organitele, et hinnata riske, sh julgeolekuriski, ebaseadusliku rände riski või terviseriski, mille põhjustab füüsiline isik, kes kavatseb siseneda või on sisenenud liikmesriigi territooriumile;

c) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks pädevatele ametiasutustele või nende nimel või liidu institutsioonidele, organitele või asutustele, et abistada pädevaid ametiasutusi varjupaiga-, viisa- ja elamisloataotluste ja nendega seotud kaebuste läbivaatamisel seoses sellist staatust taotlevate füüsiliste isikute vastavusega asjakohastele tingimustele, hõlmates sellega seotud tõendite usaldusväärsuse hindamine;

d) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks pädevatele ametiasutustele või nende nimel või liidu institutsioonidele, organitele või asutustele rände-, varjupaiga- või piirikontrollihalduse kontekstis, füüsiliste isikute avastamiseks, ära tundmiseks või tuvastamiseks, välja arvatud reisidokumentide kontrollimine.

8. Õigusemõistmine ja demokraatlikud protsessid:

a) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks õigusasutustele või nende nimel, et abistada õigusasutusi faktide ja seadustega tutvumisel ja nende tõlgendamisel ning õiguse rakendamisel konkreetse faktide kogumi suhtes, või mida kasutatakse sarnasel viisil vaidluste kohtuväliseks lahendamiseks;

b) tehisintellektisüsteemid, mis on ette nähtud kasutamiseks selleks, et mõjutada valimiste või rahvahääletuste tulemusi või füüsiliste isikute hääletamiskäitumist valimistel või rahvahääletustel. See ei hõlma tehisintellektisüsteeme, mille väljundiga füüsilised isikud otseselt kokku ei puutu, näiteks vahendid, mida kasutatakse poliitiliste kampaaniate korraldamiseks, optimeerimiseks või struktureerimiseks halduslikust või logistilisest seisukohast.

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, pakkuja nimi ja süsteemi versioon, mis kajastab selle seost varasemate versioonidega;

   b) kuidas tehisintellektisüsteem suhtleb või kuidas seda võidakse kasutada, et suhelda riistvara või tarkvaraga, sealhulgas muude tehisintellektisüsteemidega, mis ei ole tehisintellektisüsteemi enda osa, kui see on kohaldatav;

   c) asjaomase tarkvara või püsivara versioonid ja kõik versiooniuuendustega seotud nõuded;

   d) kõigi selliste vormide kirjeldus, milles võidakse tehisintellektisüsteem turule lasta või kasutusele võtta, näiteks riistvarasse integreeritud tarkvarapakett, allalaadimised või rakendusliidesed;

   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) juurutajale pakutava kasutajaliidese põhikirjeldus;

h) vajaduse korral juurutaja kasutusjuhendid ja juurutajale pakutava kasutajaliidese põhikirjeldus, kui see on kohaldatav.

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 neid kasutas, need integreeris või neid muutis;

b) süsteemi projekti kirjeldus, täpsemalt tehisintellektisüsteemi ja algoritmide üldine loogika; olulisemad konstruktsioonivalikud, sealhulgas põhjendused ja eeldused, sealhulgas nende isikute või isikute rühmade kohta, kelle suhtes kasutamiseks on see süsteem mõeldud; peamised liigitamisvalikud; mida on süsteem projekteeritud optimeerima ja milline on eri parameetrite olulisus; süsteemi eeldatava väljundi kirjeldus ja väljundi kvaliteet; otsused võimalike kompromisside kohta seoses kasutatud tehniliste lahendustega, et järgida III peatüki 2. jaos 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, sealhulgas nende andmestike üldine kirjeldus ning teave nende päritolu, ulatuse ja peamiste omaduste kohta; kuidas andmed on saadud ja valitud; märgistamismenetlused (näiteks juhendatud õppe korral), andmete puhastamise metoodikad (näiteks võõrväärtuste avastamine);

e) hinnang artikli 14 kohaselt vajalikele inimjärelevalve meetmetele, sealhulgas hinnang tehnilistele meetmetele, mida on vaja, et juurutajatel oleks lihtsam tehisintellektisüsteemi väljundit tõlgendada, vastavalt artikli 13 lõike 3 punktile d;

f) kui see on kohaldatav, 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 peatüki 2. jaos sätestatud asjaomastele nõuetele;

g) kasutatud valideerimis- ja testimismenetlused, sealhulgas teave kasutatud valideerimis- ja testimisandmete ja nende peamiste omaduste kohta; parameetrid, mida kasutatakse, et mõõta täpsust, stabiilsust ja vastavust muudele III peatüki 2. jaos sätestatud asjaomastele nõuetele ning võimalikku diskrimineerivat mõju; testilogid ja kõik testiaruanded, mis on varustatud kuupäeva ja vastutavate isikute allkirjadega, sealhulgas seoses punktis f osutatud ette kindlaks määratud muudatustega;

h) kehtestatud küberturvalisuse meetmed.

3. Üksikasjalik teave tehisintellektisüsteemi seire, toimimise ja kontrollimise kohta, eeskätt seoses järgmisega: süsteemi võimed ja piirid, sealhulgas täpsusaste konkreetsete isikute või isikute rühmade puhul, kelle peal süsteemi kavatsetakse kasutada, ning üldine eeldatav täpsusaste võrreldes süsteemi 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 juurutajatel oleks lihtsam tehisintellektisüsteemide väljundit tõlgendada; sisendandmete kirjeldused, kui see on asjakohane.

4. Konkreetse tehisintellektisüsteemi toimivusnäitajate asjakohasuse kirjeldus.

5. Riskijuhtimissüsteemi üksikasjalik kirjeldus vastavalt artiklile 9.

6. Süsteemi elutsükli jooksul pakkuja poolt tehtud asjassepuutuvate muudatuste kirjeldus.

7. Loetelu täielikult või osaliselt kohaldatavatest harmoneeritud standarditest, mille viited on avaldatud *Euroopa Liidu Teatajas*; kui selliseid harmoneeritud standardeid ei ole kohaldatud, siis III peatüki 2. jaos sätestatud nõuete täitmiseks kasutatud lahenduste üksikasjalik kirjeldus, sealhulgas muude asjaomaste kohaldatud standardite ja tehniliste kirjelduste loetelu.

8. Artiklis 47 osutatud ELi vastavusdeklaratsiooni koopia.

9. Turustamisjärgse seire etapis tehisintellektisüsteemi toimimise hindamiseks kasutusele võetud süsteemi üksikasjalik kirjeldus vastavalt artiklile 72, sealhulgas artikli 72 lõikes 3 osutatud turustamisjärgse seire kava.

V LISA

ELi vastavusdeklaratsioon

Artiklis 47 osutatud ELi vastavusdeklaratsioon peab sisaldama kogu järgmist teavet.

1. Tehisintellektisüsteemi nimi ja liik ning muud üheselt mõistetavad lisaviited, mis võimaldavad tehisintellektisüsteemi kindlaks teha ja seda jälgida.

2. Pakkuja või kohaldataval juhul tema volitatud esindaja nimi ja aadress.

3. Märge, et artiklis 47 osutatud ELi vastavusdeklaratsioon on väljastatud üksnes pakkuja vastutusel.

4. Kinnitus selle kohta, et tehisintellektisüsteem vastab käesolevale määrusele ja olenevalt asjaoludest muule liidu asjaomasele õigusele, millega on ette nähtud artiklis 47 osutatud ELi vastavusdeklaratsiooni väljastamine.

5. Kui tehisintellektisüsteem hõlmab isikuandmete töötlemist, avaldus selle kohta, et tehisintellektisüsteem vastab määrustele (EL) 2016/679 ja (EL) 2018/1725 ning direktiivile (EL) 2016/680.

6. Viited asjaomastele kasutatud harmoneeritud standarditele või muudele ühtsetele kirjeldustele, mille põhjal vastavust deklareeritakse.

7. Kui see on kohaldatav, siis teada antud asutuse nimetus ja tunnusnumber, vastavushindamismenetluse kirjeldus ja väljastatud sertifikaadi tunnusnumber.

8. Deklaratsiooni väljastamise koht ja kuupäev, allakirjutanu nimi ja amet, teave, kelle poolt või kelle nimel on nimetatud isik allkirja andnud, ning allkiri.

VI LISA

Sisekontrollil põhinev vastavushindamine

1. Sisekontrollil põhinev vastavushindamine on punktidel 2, 3 ja 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 peatüki 2. jaos sätestatud asjakohastele olulistele nõuetele.

4. Ühtlasi kontrollib pakkuja, kas tehisintellektisüsteemi projekteerimis- ja arendusprotsess ning artiklis 72 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 teada antud asutusele.

3.2. Kvaliteedijuhtimissüsteemi hindab teada antud 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 heakskiidetud kvaliteedijuhtimissüsteemi rakendamist ja haldamist, et see oleks jätkuvalt piisav ja tõhus.

3.4. Pakkuja informeerib teada antud asutust kõigist muudatustest, mis kavatsetakse teha heakskiidetud kvaliteedijuhtimissüsteemis või sellega hõlmatud tehisintellektisüsteemide loetelus.

Teada antud asutus vaatab kavandatud muudatused läbi ja otsustab, kas muudetud kvaliteedijuhtimissüsteem vastab jätkuvalt punktis 3.2 osutatud nõuetele või on vaja uut hindamist.

Teada antud 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 teada antud 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 teada antud asutusele;

c) IV lisas osutatud tehniline dokumentatsioon.

4.3. Teada antud asutus vaatab tehnilise dokumentatsiooni läbi. Kui see on asjakohane ja piirdub tema ülesannete täitmiseks vajalikuga, antakse teada antud asutusele täielik juurdepääs kasutatavatele treenimis-, valideerimis- ja testimisandmestikele, sealhulgas, kui see on asjakohane ja kui kohaldatakse kaitsemeetmeid, rakendusliideste (API) või muude asjakohaste kaugjuurdepääsu võimaldavate tehniliste vahendite ja tööriistade kaudu.

4.4. Tehnilise dokumentatsiooni läbivaatamise käigus võib teada antud asutus nõuda, et pakkuja esitaks täiendavaid tõendeid või teeks täiendavaid teste, et oleks võimalik nõuetekohaselt hinnata tehisintellektisüsteemi vastavust III peatüki 2. jaos sätestatud nõuetele. Kui teada antud asutus ei ole pakkuja tehtud testidega rahul, teeb teada antud asutus ise piisavad testid, nagu on asjakohane.

4.5. Kui see on vajalik, et hinnata suure riskiga tehisintellektisüsteemi vastavust III peatüki 2. jaos sätestatud nõuetele pärast seda, kui kõik muud mõistlikud viisid vastavuse kontrollimiseks on ammendunud ja osutunud ebapiisavaks, ja põhjendatud taotluse alusel antakse teada antud asutusele juurdepääs tehisintellektisüsteemi treenimis- ja treenitud mudelitele, sealhulgas selle asjaomastele parameetritele. Sellise juurdepääsu suhtes kohaldatakse intellektuaalomandi ja ärisaladuste kaitset käsitlevat kehtivat liidu õigust.

4.6. Teada antud asutuse otsusest teatatakse pakkujale või tema volitatud esindajale. Teade sisaldab tehnilise dokumentatsiooni hindamise järeldusi ning põhjendatud hindamisotsust.

Kui tehisintellektisüsteem vastab III peatüki 2. jaos sätestatud nõuetele, annab teada antud asutus välja liidu tehnilise dokumentatsiooni hindamise sertifikaadi. Sertifikaat sisaldab pakkuja nime ja aadressi, läbivaatamise põhjal tehtud järeldusi, võimalikke kehtivustingimusi ja tehisintellektisüsteemi identifitseerimiseks vajalikke andmeid.

Sertifikaat ja selle lisad sisaldavad kogu asjakohast teavet, et oleks võimalik hinnata tehisintellektisüsteemi vastavust nõuetele ja et tehisintellektisüsteemi saaks kasutamise ajal kontrollida, kui see on kohaldatav.

Kui tehisintellektisüsteem ei vasta III peatüki 2. jaos sätestatud nõuetele, keeldub teada antud asutus liidu tehnilise dokumentatsiooni hindamise sertifikaadi väljastamisest ja teatab sellest taotlejale, põhjendades keeldumist üksikasjalikult.

Kui tehisintellektisüsteem ei vasta nõuetele, mis puudutavad süsteemi treenimiseks kasutatud andmeid, tuleb tehisintellektisüsteemi enne uue vastavushindamise taotlemist uuesti treenida. Sellisel juhul peab liidu tehnilise dokumentatsiooni hindamise sertifikaadi väljastamisest keeldunud teada antud asutuse põhjendatud hindamisotsus sisaldama konkreetseid argumente tehisintellektisüsteemi treenimiseks kasutatud andmete kvaliteedi kohta, eelkõige mittevastavuse põhjuste kohta.

4.7. Teada antud asutus, kes väljastas liidu tehnilise dokumentatsiooni hindamise sertifikaadi, hindab kõiki tehisintellektisüsteemi muudatusi, mis võivad mõjutada tehisintellektisüsteemi vastavust nõuetele või süsteemi sihtotstarvet. Pakkuja informeerib sellist teada antud asutust, kui ta kavatseb teha eespool nimetatud muudatusi või kui ta saab muul moel sellistest muudatustest teada. Teada antud asutus hindab kavandatud muudatusi ja otsustab, kas kavandatud muudatused eeldavad uut vastavushindamist vastavalt artikli 43 lõikele 4 või piisab nende puhul liidu tehnilise dokumentatsiooni hindamise sertifikaadi lisast. Viimasel juhul hindab teada antud asutus muudatusi, teatab pakkujale oma otsuse ning, juhul kui muudatused heaks kiidetakse, väljastab pakkujale liidu tehnilise dokumentatsiooni hindamise sertifikaadi lisa.

5. Heakskiidetud kvaliteedijuhtimissüsteemide järelevalve

5.1. Punktis 3 osutatud teada antud asutuse teostatava järelevalve eesmärk on tagada, et pakkuja järgib igakülgselt heakskiidetud kvaliteedijuhtimissüsteemi tingimusi.

5.2. Pakkuja annab teada antud asutusele hindamise jaoks juurdepääsu ruumidele, kus toimub tehisintellektisüsteemi projekteerimine, arendamine ja testimine. Lisaks jagab pakkuja teada antud asutusega kogu vajalikku teavet.

5.3. Teada antud asutus teostab korrapäraselt auditeid tagamaks, et pakkuja säilitab ja rakendab kvaliteedijuhtimissüsteemi, ja esitab pakkujale selle kohta auditeerimisaruande. Seoses nende audititega võib teada antud asutus täiendavalt testida tehisintellektisüsteeme, mille kohta on väljastatud liidu tehnilise dokumentatsiooni hindamise sertifikaat.

VIII LISA

Teave, mis tuleb esitada
suure riskiga tehisintellektisüsteemi registreerimisel vastavalt artiklile 49

A jagu – teave, mille suure riskiga tehisintellektisüsteemide pakkujad peavad esitama kooskõlas artikli 49 lõikega 1

Suure riskiga tehisintellektisüsteemide kohta, mis tuleb registreerida vastavalt artikli 49 lõikele 1, tuleb esitada järgmine teave ning seda edaspidi ajakohastada.

1. Pakkuja nimi, aadress ja kontaktandmed.

2. Kui pakkuja nimel esitab teabe keegi teine, siis selle isiku nimi, aadress ja kontaktandmed.

3. Volitatud esindaja nimi, aadress ja kontaktandmed, kui see on kohaldatav.

4. Tehisintellektisüsteemi kaubanimi ning muud täiendavad üheselt mõistetavad viited, mis võimaldavad tehisintellektisüsteemi kindlaks teha ja seda jälgida.

5. Tehisintellektisüsteemi sihtotstarbe ning selle tehisintellektisüsteemi kaudu toetatavate komponentide ja funktsioonide kirjeldus.

6. Süsteemi kasutatava teabe (andmed, sisendid) ja selle toimimisloogika põhiline ja kokkuvõtlik kirjeldus.

7. Tehisintellektisüsteemi staatus (turul või kasutuses, ei ole enam turul/kasutuses, tagasi nõutud).

8. Teada antud asutuse väljastatud sertifikaadi liik, number ja kehtivusaeg ning teada antud asutuse nimetus või tunnusnumber, kui see on asjakohane.

9. Punktis 8 osutatud sertifikaadi skaneeritud koopia, kui see on asjakohane.

10. Kõik liikmesriigid, kus tehisintellektisüsteem on liidus turule lastud, kasutusele võetud või kättesaadavaks tehtud.

11. Artiklis 47 osutatud ELi vastavusdeklaratsiooni koopia.

12. Elektrooniline kasutusjuhend. Seda teavet ei esitata III lisa punktides 1, 6 ja 7 osutatud suure riskiga tehisintellektisüsteemide kohta sellistes valdkondades, nagu õiguskaitse või rände-, varjupaiga- ja piirikontrollihaldus.

13. Täiendava teabe URL, kui see on asjakohane.

B jagu – teave, mille suure riskiga tehisintellektisüsteemide pakkujad peavad esitama kooskõlas artikli 49 lõikega 2

Suure riskiga tehisintellektisüsteemide kohta, mis tuleb registreerida vastavalt artikli 49 lõikele 2, tuleb esitada järgmine teave ning seda edaspidi ajakohastada.

1. Pakkuja nimi, aadress ja kontaktandmed.

2. Kui pakkuja nimel esitab teabe keegi teine, siis selle isiku nimi, aadress ja kontaktandmed.

3. Volitatud esindaja nimi, aadress ja kontaktandmed, kui see on kohaldatav.

4. Tehisintellektisüsteemi kaubanimi ning muud täiendavad üheselt mõistetavad viited, mis võimaldavad tehisintellektisüsteemi kindlaks teha ja seda jälgida.

5. Tehisintellektisüsteemi sihtotstarbe kirjeldus.

6. Artikli 6 lõikes 3 sätestatud tingimus või tingimused, mille alusel tehisintellektisüsteemi ei peeta suure riskiga süsteemiks.

7. Lühikokkuvõte põhjustest, mille alusel tehisintellektisüsteemi ei peeta artikli 6 lõike 3 kohase menetluse kohaldamisel suure riskiga süsteemiks.

8. Tehisintellektisüsteemi staatus (turul või kasutuses, ei ole enam turul/kasutuses, tagasi nõutud).

9. Kõik liikmesriigid, kus tehisintellektisüsteem on liidus turule lastud, kasutusele võetud või kättesaadavaks tehtud.

C jagu – teave, mille suure riskiga tehisintellektisüsteemide juurutajad peavad esitama kooskõlas artikli 49 lõikega 3

Suure riskiga tehisintellektisüsteemide kohta, mis tuleb registreerida vastavalt artikli 49 lõikele 3, tuleb esitada järgmine teave ning seda edaspidi ajakohastada.

1. Juurutaja nimi, aadress ja kontaktandmed.

2. Juurutaja nimel teavet esitava isiku nimi, aadress ja kontaktandmed.

3. Tehisintellektisüsteemi pakkuja poolt ELi andmebaasi kandmise URL.

4. Artikli 27 kohaselt läbi viidud põhiõigustele avalduva mõju hinnangu tulemuste kokkuvõte.

5. Määruse (EL) 2016/679 artikli 35 või direktiivi (EL) 2016/680 artikli 27 kohaselt tehtud andmekaitsealase mõjuhinnangu kokkuvõte, nagu on täpsustatud käesoleva määruse artikli 26 lõikes 8, kui see on kohaldatav.

IX LISA

Teave, mis tuleb esitada III lisas loetletud suure riskiga tehisintellektisüsteemi registreerimisel seoses tegelikes tingimustes testimisega kooskõlas artikliga 60

Tegelikes tingimustes testimise kohta, mis tuleb registreerida vastavalt artiklile 60, 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 juurutajate 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.

X LISA

Liidu õigusaktid vabadusel, turvalisusel ja õigusel rajaneva 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 7. juuli 2021. aasta määrus (EL) 2021/1133, millega muudetakse määrusi (EL) nr 603/2013, (EL) 2016/794, (EL) 2018/1862, (EL) 2019/816 ja (EL) 2019/818 seoses tingimuste kehtestamisega juurdepääsu saamiseks muudele ELi infosüsteemidele viisainfosüsteemi kasutamise eesmärgil (ELT L 248, 13.7.2021, lk 1).

b) Euroopa Parlamendi ja nõukogu 7. juuli 2021. aasta määrus (EL) 2021/1134, millega muudetakse Euroopa Parlamendi ja nõukogu määrusi (EÜ) nr 767/2008, (EÜ) nr 810/2009, (EL) 2016/399, (EL) 2017/2226, (EL) 2018/1240, (EL) 2018/1860, (EL) 2018/1861, (EL) 2019/817 ja (EL) 2019/1896 ning tunnistatakse kehtetuks nõukogu otsused 2004/512/EÜ ja 2008/633/JSK, et reformida viisainfosüsteemi (ELT L 248, 13.7.2021, lk 11).

3. Eurodac-süsteem

Euroopa Parlamendi ja nõukogu … määrus (EL) 2024/…, millega luuakse biomeetriliste andmete võrdlemise Eurodac-süsteem, et kohaldada tulemuslikult Euroopa Parlamendi ja nõukogu määruseid (EL) 2024/… ja (EL) 2024/… ja nõukogu direktiivi 2001/55/EÜ ning tuvastada ebaseaduslikult riigis viibivad kolmandate riikide kodanikud ja kodakondsuseta isikud, ning mis käsitleb liikmesriikide õiguskaitseasutuste ja Europoli päringuid andmete võrdlemiseks Eurodac-süsteemi andmetega õiguskaitse eesmärgil ning millega muudetakse Euroopa Parlamendi ja nõukogu määruseid (EL) 2018/1240 ja (EL) 2019/818[+] ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrus (EL) nr 603/2013.

4. Riiki sisenemise ja riigist lahkumise süsteem

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).

[+] ELT: palun lisada teksti dokumendis PE-CONS 15/24 (2016/0132(COD)) sisalduva määruse number ja joonealusesse märkusesse kõnealuse määruse number, kuupäev, pealkiri ja ELT avaldamisviide.

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

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 ning muudetakse Euroopa Parlamendi ja nõukogu määrusi (EÜ) nr 767/2008, (EL) 2016/399, (EL) 2017/2226, (EL) 2018/1240, (EL) 2018/1726, (EL) 2018/1861 ning nõukogu otsuseid 2004/512/EÜ ja 2008/633/JSK (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 ning muudetakse määrusi (EL) 2018/1726, (EL) 2018/1862 ja (EL) 2019/816 (ELT L 135, 22.5.2019, lk 85).

XI LISA

Artikli 53 lõike 1 punktis a osutatud tehniline dokumentatsioon – üldotstarbeliste tehisintellektimudelite pakkujate tehniline dokumentatsioon

1. jagu

Teave, mille peavad esitama kõik üldotstarbeliste tehisintellektimudelite pakkujad

Artikli 53 lõike 1 punktis a osutatud tehniline dokumentatsioon peab sisaldama vähemalt järgmist teavet vastavalt mudeli suurusele ja riskiprofiilile.

1. Üldotstarbelise tehisintellektimudeli üldine kirjeldus, sealhulgas:

   a) ülesanded, mida mudel on ette nähtud täitma, ning selliste tehisintellektisüsteemide liik ja olemus, millesse seda saab integreerida;

   b) kohaldatavad vastuvõetavad kasutuspõhimõtted;

   c) tarbimisse lubamise kuupäev ja turustamismeetodid;

   d) arhitektuur ja parameetrite arv;

   e) sisendite ja väljundite modaalsus (nt tekst, kujutis) ja vorming;

   f) litsents.

2. Punktis 1 osutatud mudeli elementide üksikasjalik kirjeldus ja asjakohane teave arendusprotsessi kohta, sealhulgas järgmised elemendid:

a) tehnilised vahendid (nt kasutusjuhend, taristu, vahendid), mis on vajalikud üldotstarbelise tehisintellektimudeli integreerimiseks tehisintellektisüsteemidesse;

b) mudeli ja treenimisprotsessi spetsifikatsioonid, sealhulgas treenimismeetodid ja -tehnikad, peamised projekteerimisvalikud, sealhulgas põhjendused ja tehtud eeldused; mida on mudel projekteeritud optimeerima ja milline on eri parameetrite olulisus, kui see on asjakohane;

c) teave treenimisel, testimisel ja valideerimisel kasutatud andmete kohta, kui see on kohaldatav, sealhulgas andmete liik ja päritolu ning andmehooldusmeetodid (nt puhastamine, filtreerimine jne), andmepunktide arv, nende ulatus ja põhiomadused; kuidas andmed saadi ja valiti, samuti kõik muud meetmed andmeallikate ja kindlaks määratava kallutatuse tuvastamise meetodite sobimatuse avastamiseks, kui see on kohaldatav;

d) mudeli treenimiseks kasutatavad arvutusressursid (nt ujukomatehete arv), treenimise aeg ja muud treenimisega seotud asjakohased üksikasjad;

e) mudeli teadaolev või hinnanguline energiatarbimine.

Punkti e puhul, kui mudeli energiatarbimine ei ole teada, võib energiatarbimine põhineda kasutatud arvutusressursse käsitleval teabel.

2. jagu

Lisateave, mille peavad esitama

kõik süsteemse riskiga üldotstarbeliste tehisintellektimudelite pakkujad

1. Hindamisstrateegiate üksikasjalik kirjeldus, sealhulgas hindamistulemused, tuginedes kättesaadavatele avalikele hindamisprotokollidele ja -vahenditele või muudele hindamismeetoditele. Hindamisstrateegiad hõlmavad hindamiskriteeriume, parameetreid ja metoodikat piiride tuvastamiseks.

2. Kui see on kohaldatav, siis selliste meetmete üksikasjalik kirjeldus, mis on kehtestatud sisemiste ja/või väliste vastandtestimiste tegemiseks (nt punaste tiimide kasutamine), mudelite kohandamiseks, sealhulgas ühtlustamiseks ja peenhäälestamiseks.

3. Kui see on kohaldatav, siis süsteemi arhitektuuri üksikasjalik kirjeldus, milles selgitatakse, kuidas tarkvarakomponendid üksteisele toetuvad või üksteisele sisendit annavad ja üldise andmetöötlusega integreeruvad.

XII LISA

Artikli 53 lõike 1 punktis b osutatud teave läbipaistvuse kohta
– üldotstarbeliste tehisintellektimudelite pakkujate tehniline dokumentatsioon
järgmise etapi pakkujatele, kes integreerivad mudeli oma tehisintellektisüsteemi

Artikli 53 lõike 1 punktis b osutatud teave peab sisaldama vähemalt järgmist.

1. Üldotstarbelise tehisintellektimudeli üldine kirjeldus, sealhulgas:

   a) ülesanded, mida mudel on ette nähtud täitma, ning nende tehisintellektisüsteemide liik ja olemus, millesse seda saab integreerida;

   b) kohaldatavad vastuvõetavad kasutuspõhimõtted;

   c) tarbimisse lubamise kuupäev ja turustamismeetodid;

   d) kuidas mudel suhtleb või kuidas seda võidakse kasutada, et suhelda riistvara või tarkvaraga, mis ei ole ise tehisintellektisüsteemi osa, kui see on kohaldatav;

   e) üldotstarbelise tehisintellektimudeli kasutamisega seotud asjakohase tarkvara versioonid, kui see on kohaldatav;

   f) arhitektuur ja parameetrite arv;

   g) sisendite ja väljundite modaalsus (nt tekst, kujutis) ja vorming;

   h) mudeli litsents.

2. Mudeli komponentide ja selle arendamise protsessi kirjeldus:

a) tehnilised vahendid (nt kasutusjuhend, taristu, vahendid), mis on vajalikud üldotstarbelise tehisintellektimudeli integreerimiseks tehisintellektisüsteemidesse;

b) sisendite ja väljundite modaalsus (nt tekst, pilt jne) ja vorming ning nende maksimaalne suurus (nt kontekstiakna pikkus jne);

c) teave treenimisel, testimisel ja valideerimisel kasutatud andmete kohta, kui see on kohaldatav, sealhulgas andmete liik ja päritolu ning andmehooldusmetoodika.

XIII LISA

Kriteeriumid, mille alusel liigitatakse üldotstarbeline tehisintellektimudel artiklis 51 osutatud süsteemse riskiga mudeliks

Selleks et teha kindlaks, kas üldotstarbelisel tehisintellektimudelil on artikli 51 lõike 1 punktis a sätestatutega samaväärsed võimed või mõju, võtab komisjon arvesse järgmisi kriteeriume:

a) mudeli parameetrite arv;

b) andmestiku kvaliteet või suurus, näiteks mõõdetuna tokenite abil;

c) mudeli treenimisel kasutatud arvutuste hulk, mida mõõdetakse ujukomatehetes või näidatakse muude muutujate kombinatsiooniga, nagu treenimise hinnanguline maksumus, treenimiseks kuluv hinnanguline aeg või treenimise hinnanguline energiatarbimine;

d) mudeli sisendite ja väljundite modaalsus, nagu tekst-tekst (suured keelemudelid), tekst-pilt, multimodaalsus ja tehnika tasemel künnised suure mõjuga võimete kindlaksmääramiseks iga modaalsuse puhul ning sisendite ja väljundite konkreetne liik (nt bioloogilised järjestused);

e) mudeli võimete võrdlusalused ja hinnangud, sealhulgas ülesannete arv ilma lisatreenimiseta, kohanemisvõime uute, eristatavate ülesannete õppimiseks, selle autonoomsuse ja mastaabitavuse tase, vahendid, millele mudelil on juurdepääs;

f) kas mudelil on suur mõju siseturule tulenevalt levikuulatusest, mida eeldatakse juhul, kui see on tehtud kättesaadavaks vähemalt 10 000 liidus tegutsevale registreeritud ärikasutajale;

g) registreeritud lõppkasutajate arv.