ANDMEKAITSE INSPEKTSIOON

Lp Tiina Uudeberg
Justiitsministeerium
info@justdigi.ee

Teie 28.11.2025 nr 7-1/9632

Meie 19.12.2025 nr 2.3-4/25/3913-2

Arvamuse avaldamine ettepanekule

Täname, et saatsite Andmekaitse Inspektsioonile (AKI) arvamuse avaldamiseks Digital Omnibus (digitaalne omnibus) ja Digital Omnibus on AI (tehisintellekti omnibus) määruste ettepanekud.

Mitmed ettepanekus sisalduvad muudatused on suunatud eeskätt halduskoormuse vähendamisele ja andmekasutuse hõlbustamisele ettevõtjatele, mida AKI tervitab.

Kahjuks peame üldise märkusena nentima, et ettepanekutega ei kaasne sisulist hinnangut või mõjuanalüüsi, kuidas kavandatavad muudatused mõjutavad füüsiliste isikute olemasolevaid kaitsemeetmeid. Digitaalse omnibusi ettepanekus sisalduv mõjuanalüüs keskendub üksnes muudatuste mõjule ettevõtetele ja organisatsioonidele, käsitlemata, kuidas need mõjutavad üksikisiku põhiõigusi ja õiguste tegelikku kasutatavust. Euroopa Komisjon on väljendanud, et ettepanek ei vähenda isikuandmete kaitse taset. Samal ajal puudub analüüs üksikisiku õiguste vaatest, mistõttu ei ole sellist väidet võimalik objektiivselt kinnitada. Kuigi ettepanek rõhutab korduvalt selguse ja lihtsustamise eesmärki, ei analüüsita, kuidas neid eesmärke on tasakaalustatud võimalike tagajärgedega andmesubjektidele.

Lisaks ei ole hinnatud ka mõjusid andmekaitseasutustele. Olukorras, kus paljudes küsimustes alles hakkab kooruma välja selgus ning väikestes riikides nagu Eesti hakkab andmekaitseteadlikkus tekkima, toovad muudatused kaasa suure koormuse kasvu järelevalveasutustele. Tuleb arvestada, et käesolevate omnibussidega hakatakse muutma põhimõttelisi asju ning andmekaitse alustalasid. Ehkki EL õigusaktides on deklaratiivselt sätestatud, et liikmesriik peab tagama järelevalveasutustele piisava ressursi ja toimepidevuse, ei arvesta see liikmesriikide tegelike võimalusega ega ole ette nähtud ka mehhanisme või meetmeid, mis toetaks neid asutusi olukorras, kus liikmesriik vajalikke ressursse ei leia. Arvestades potentsiaalset muudatustega seotud selgitustaotluste esitamise mahtu tõlgendamisküsimustes, jääb järelevalveasutustel vähem ressurssi kaebusi menetleda ja panustada andmekaitse edendamisesse proaktiivselt.

Sisulise arvamuse tekst on peatükkide kaupa leitav allpoolt.

Arvamuse avaldamise hetkel ei ole Euroopa Komisjon avaldanud ametlikku digitaalse omnibussi tõlget. Sellest tulenevalt lähtub AKI arvamus ettepaneku mitteametlikus tõlkest. Juhul, kui teksti tõlge on ebakorrektne, täpsustab AKI hiljem vajadusel oma arvamust.

Arvamus on ülesehitatud õigusaktide järgi. Esmalt analüüsib AKI digitaalse omnibusi muudatusettepanekuid isikuandmete kaitse üldmäärusele ja andmemäärusele. Seejärel analüüsib AKI tehisintellekti omnibusi ettepanekuid tehisintellekti määruse muudatusteks. Pikematele analüüsidele eelneb kokkuvõte olulisemate tähelepanekutega.

Sisukord

ISIKUANDMETE KAITSE ÜLDMÄÄRUS

1. Isikuandmete mõiste

(IKÜM artikkel 4 lõige 1)

Kokkuvõte

Ettepanek muuta isikuandmete mõistet nihutab fookuse andmetöötleja subjektiivsele hinnangule, sidudes isikuandmete olemasolu konkreetse andmetöötleja tegelike või mõistlikult kasutatavate tuvastamisvahenditega, sõltumata kolmandate isikute võimalikust tuvastamisvõimest. AKI hinnangul ei suurenda see õiguskindlust, vaid vastupidi vähendab seda. Selline definitsioon kaldub kõrvale Euroopa Kohtu varasemast praktikast (sh C-582/14), kus kaudset tuvastatavust on hinnatud objektiivselt ja laiemalt, arvestades kolmandate isikute võimalusi. Pseudonüümimise kontekstis tehtud kohtuotsuse (C-413/23) laiendamine kõigile kaudse tuvastamise juhtumitele on AKI hinnangul põhjendamatu ning võib viia olukorrani, kus kaudselt tuvastatavad andmed langevad IKÜMi kohaldamisalast välja, nõrgestades andmesubjektide õigusi, tekitades ümberpööratud tõendamiskoormise, raskendades järelevalvet ja võimaldades regulatsiooni vältimist (sh III riikidesse andmeedastuste puhul). Selline lähenemine kahjustab õigusselgust ja ettenähtavust ning võib olla vastuolus Harta artiklitega 7 ja 8, kuna muudab isikuandmete kaitse ebamääraseks ja tingimuslikuks, raskendab andmesubjektide õiguste tegelikku kasutamist ning nõrgestab tõhusat haldus- ja kohtulikku õiguskaitset.

Euroopa Komisjon on teinud digitaalse Omnibusiga ettepaneku muuta IKÜM artikli 4 punktis 1 olevat isikuandmete mõistet. Ettepanekus sisalduv isikuandmete mõiste ei ole objektiivselt laiem kui hetkel kehtivas IKÜMis, kuid Komisjon on ettepanekus oluliselt laiendanud definitsiooni subjektiivset mõõdet. Ettepanekuga soovitakse lisada käesolevale mõistele juurde, et füüsilise isikuga seotud teave ei ole tingimata isikuandmed iga teise isiku või üksuse jaoks ainuüksi seetõttu, et teine üksus saab selle füüsilise isiku tuvastada. Teave ei ole antud üksuse jaoks isiklik, kui see üksus ei suuda tuvastada füüsilist isikut, kellega teave on seotud, võttes arvesse vahendeid, mida see üksus mõistlikult tõenäoliselt kasutab. Selline teave ei muutu selle üksuse jaoks isiklikuks ainuüksi seetõttu, et potentsiaalsel järgmisel saajal on vahendid, mida mõistlikult tõenäoliselt saab kasutada selle füüsilise isiku tuvastamiseks, kellega teave on seotud.

AKI on seisukohal, et ettepanek ei täida esitatud kujul eesmärki pakkuda suuremat õiguskindlust. Selge määratluse asemel peavad andmetöötlejad, sh VKE-d, igakordselt subjektiivselt hindama seda, millal andmed kujutavad endast konkreetse andmetöötleja jaoks isikuandmeid. VKE-del on selliste hinnangute tegemiseks vähem ressursse kui suurettevõtetel. Eriti problemaatiline on väljapakutud definitsiooni viimase lause tõlgendamine, mis vähendab õiguskindlust ning kahjustab õigust andmete kaitsele. Andmetöötlejad võivad hakata vältima isiku otsest tuvastamist eesmärgiga hoiduda IKÜMi kohaldumisest. See raskendab nii andmesubjekti õiguste teostamist kui ka tõhusat järelevalvet, kuivõrd keeruliseks võib osutuda tõendamine, millal vahendid andmetöötleja käsutusse tekkisid ja/või millal isik muutus andmetöötleja jaoks tuvastatavaks.

Euroopa Kohus on analüüsinud isikuandmete mõistet mitmetes lahendites. Lahendis C-582/14 selgitas kohus, et ka andmed, mis ei identifitseeri isikut otseselt (näiteks IP-aadress) võivad olla isikuandmed, kui vastutaval töötlejal on mõistlikult kasutatavad vahendid, et isik kolmanda osapoole kaudu (nt internetiteenuse pakkuja) tuvastada. Hilisemates lahendites on Euroopa Kohus seda lähenemist jätkanud. Kohtuotsustes C-319/22 ja C-479/22 rõhutas kohus, et isikuandmeteks

võivad kujuneda isegi tehnilised või näiliselt neutraalsed andmeüksused (nt sõiduki VIN-kood, rahvus, sugu), kui neid kombineerides saab isiku tuvastada isegi siis, kui mitte iga potentsiaalne andmesaaja ei suuda seda teha. Seega on Euroopa Kohus varasemalt pidanud oluliseks, kas isiku identiteet on mõnele isikule või isikute ringile objektiivselt tuvastatav.

Digitaalse Omnibusi ettepanekus olev isikuandmete definitsioon toetub aga Euroopa Kohtu otsusele C-413/23. Euroopa Kohus ütles antud lahendis, et pseudonüümitud andmed võivad olla isikuandmed ühe andmetöötleja jaoks (kellel on võimalik taasisikustada), ent mitte kolmanda osapoole jaoks, kellel sellised vahendid puuduvad ja kelle jaoks tuvastamine ei oleks mõistlikult teostatav. Euroopa Kohtu seisukoht piirdus olukorraga, kus kolmandal isikul puuduvad reaalsed või mõistlikult kasutatavad vahendid konkreetsete andmete taasisikustamiseks. Komisjoni töödokumendi punktis 1.2.2.1 on põhjendatud muudatuste tegemist asjaoluga, et huvigruppide arvates on kaudse tuvastamise ümber selgusetust. Edasi on selgitatud, et kuigi Euroopa Kohus on teinud lahendi pseudonüümimise kohta, mis on olemuselt kaudne tuvastamine, võtab Komisjon pseudonüümimise kohta tehtud kohtu lahendi arvesse kogu kaudse tuvastamise mõtestamise kontekstis.

AKI on seisukohal, et pseudonüümimise kontekstis tehtud lahendi laiendamine kõikidele kaudse tuvastamise juhtumitele on meelevaldne ning nõrgestab oluliselt isikuandmete kaitse taset. Komisjon laiendab seda loogikat juhtumitele, kus andmete saaja võib olla sellises ökosüsteemis, kus teistel osapooltel on tuvastamisvahendid olemas, kuid teave ei kvalifitseeru konkreetse üksuse jaoks isikuandmeteks. Lisaks ei arvesta Komisjon potentsiaalse järgmise saaja tuvastamisvõimet, ehkki Euroopa Kohtu varasemas praktikas (nt C-582/14) on tuvastatavust hinnatud laiemalt, võttes arvesse kõiki mõislikult kasutatavaid vahendeid ja viise, sealjuures on Euroopa Kohus viidatud lahendi punktis 46 sedastanud, et vahendi puudumise kriteerium on väga kõrge: identifitseerimise oht peab olema olematu või ebaoluline. Komisjon ei ole ettepanekus viidanud vahendi puudumise kriteeriumi hindamise kohustusele.

Näiteks harvikhaiguste kontekstis loetakse praeguse isikuandmete mõiste järgi üks diagnoos aastas isikuga seotud teabeks, kuna see võimaldab tuvastada konkreetse füüsilise isiku. Seega kvalifitseerub selline teave isikuandmeteks igale andmesubjekti identifitseerida püüdvale osapoolele. Uue mõiste kohaselt ei ole meie tänase arusaama kohaselt see info isikuandmed nende jaoks, kes ei saa konkreetset isikut mõistlikult tuvastada, võttes arvesse nende käsutuses olevad vahendid ja võimalused. See tähendab, et kuigi üksikdiagnoosi puhul võib olemasoleva teabe põhjal teoreetiliselt isiku tuvastada, ei muutu see automaatselt isikuandmeteks üksusele, kellel puuduvad realistlikud vahendid tuvastamiseks.

Teise näitena võib tuua isiku defineerimise teatud asjaolude kaudu, näiteks kui viidata isikule kui punase peaga poisile Ruhnust. Praeguse mõiste järgi kvalifitseerub selline kirjeldus isikuandmeteks, kuna see viitab tuvastatavale füüsilisele isikule. Uue mõiste kohaselt ei ole info siiski isikuandmed nende jaoks, kes ei suuda poissi mõistlikult tuvastada, näiteks kolmandate osapoolte jaoks, kellel puudub lisateave. Isikuandmeteks muutub teave ainult nende jaoks, kellel on praktiliselt kasutatavad vahendid ja võimalused konkreetse poisi tuvastamiseks.

Kaudse tuvastamise kontekstis toob uus definitsioon kaasa sisulise nihke. Kehtiva IKÜMi järgi tuleb hinnata, kas füüsiline isik on tuvastatav kolmandate isikute käsutuses olevate mõistlikult kasutatavate vahendite abil, mis tähendab, et kaudne tuvastamine toimib objektiivse standardi alusel. Komisjoni ettepanek muudab kriteeriumi subjektiivseks: kui konkreetse andmetöötleja käsutuses ei ole vahendeid tuvastamiseks, ei ole teave tema jaoks isikuandmed, isegi juhul, kui teised isikud suudaksid füüsilise isiku hõlpsasti tuvastada. Praktikas tähendab see, et kaudselt tuvastatavad andmed võivad langeda IKÜMi kohaldamisalast välja, mis vähendab

andmesubjektide kaitset ja killustab vastutust. See tekitab ühtlasi ümberpööratud tõendamiskoormise, kus AKI või andmesubjekt on kohustatud tõendama, kas andmetöötlejal olid vahendid isikute tuvastamiseks või kas tal oleks mõistlikult tõenäoliselt olnud võimalik selliseid vahendeid kasutada. AKI toob välja, et mõiste muutmisel võiks Komisjon võtta arvesse ka kolmandate isikute mõistliku võimaluse isikuid tuvastada. Täpsemalt tuleks isiku tuvastamise puhul arvesse võtta, kas mõnel mõistlikult ettenähtaval kolmandal isikul võivad olla vahendid isiku tuvastamiseks. Juhul, kui analüüsi tulemusel selgub, et sellised kolmandad isikud võivad olemas olla (näiteks internetti pilte või videoid üles laadides tuleb peaaegu alati seda võimalust möönda), on tegemist isikuandmetega.

Lisaks eelmainitud murekohtadele tekitab väljapakutud isikuandmete mõiste riske ka rahvusvaheliste andmeedastuste kontekstis. Nimelt võivad andmetöötlejad asuda seisukohale, et isikuandmete kolmandatesse riikidesse edastamisel ei ole vajalik IKÜM 5. peatükis toodud kaitsemeetmete kohaldamine, kuivõrd isikuandmete importijal ei pruugi olla vahendeid andmesubjektide tuvastamiseks. Alternatiivselt võivad andmetöötlejad asuda ka seisukohale, et IKÜM 5. peatükk ei ole üldse kohaldatav.

2.1. Põhiõiguste hartaga tagatud õiguste seos ettepanekuga

Isikuandmete mõiste kitsendamine ja abstraktsemaks muutumine ei puuduta ainult kaitseala kitsenemist, vaid õigusselguse ja ettenähtavuse nõrgenemist. Euroopa Liidu Põhiõiguste Harta (edaspidi Harta) artikkel 8 sätestab igaühe õiguse oma isikuandmete kaitsele. Harta artikkel 8 ei taga isikuandmete kaitset abstraktselt, vaid kui reaalselt kasutatavat õigust.

Liidetud kohtuasjades C-468/10 ja C-469/10 on selgitatud, et Harta artiklitega 7 ja 8 tunnustatud õigus eraelu austamisele isikuandmete töötlemisel puudutab igasugust teavet tuvastatud või tuvastatava füüsilise isiku kohta. Kui isikuandmete mõiste ja sellele lähenemine on abstraktne või ebamäärane, ei ole andmesubjektil enam võimalik mõistlikult ette näha, kas ja millisel alusel tema õigused rakenduvad. Selline lähenemine võib vähendada usaldust, mis ei pruugi hõlmata mitte ainult segadust andmete kasutamise osas, vaid nõrgestada andmesubjekti õiguste mahtu oma isikuandmete üle. Kirjeldatu aga omab otsest mõju andmesubjekti õiguste jõustamisele.

IKÜM-ga tagatud õigused nagu isikuandmetele juurdepääs, nende parandamine, kustutamine ja töötlemisele vastuväidete esitamine võivad muutuda juhuslikuks, sest andmesubjektil võib puududa kindel veendumus, kas tema isikuandmetele konkreetses olukorras IKÜM kohaldub. Kui puudub arusaam kaitsemehhanismide kohaldatavusest, on andmesubjektidel omakorda keeruline rakendada oma õigusi.

Harta artikliga 8 on lähedalt põimunud Harta artikkel 7, mis sätestab eraelu puutumatuse kaitse. Isikuandmete mõiste muutmisega kaasneb eraelu piiride hägustumine, kuivõrd ettenägematu ja ebaselge andmete töötlemisega võib kaasneda eraellu sekkumine. Harta artikkel 7 eeldab, et sekkumine eraellu oleks selgelt määratletud, ettenähtav ja piiratud. Olukorras, kus teabe isikuandmeteks kvalifitseerumise otsustab teabe valdaja, võib esineda oluline risk eraelu riiveks. Riive võib olla ulatuslik, sest isikuandmete töötlemine on osa eraelust ning isikuandmete määratlus on ettepaneku kohaselt abstraktne, mistõttu võivad subjektiivse hinnangu pinnalt leida aset pidevad eraelulised sekkumised, sest isikuandmete määratlus eraelu osana on kitsas ja vaieldav.

Järelevalveasutus peab kindlaks tegema, millised andmed kvalifitseeruvad isikuandmeteks ja kas neid töödeldi õiguspäraselt või mitte. Ebamäärane subjektiivne hinnang isikuandmetele ei taga tõhusat ja efektiivset menetlust, sest järelevalveasutusel tuleb selgitada ebamääraseid puutepunkte, mistõttu võib õiguste jõustamine viibida. Harta artikkel 41 sätestab õiguse heale haldusele ja

eeldab tõhusat õigeaegset ja läbipaistvat haldust. Kui isikuandmetele lähenemine on sisuliselt ebaselge, kannatab õiguste tegelik kaitse. Küsimus vaidluse eseme üle, mida võib kutsuda esile isikuandmete ebaselge määratlus võib omada mõju Harta artiklile 47, mis tagab õiguse efektiivsele õiguskaitsele. Kõigi eelduste järgi kutsub isikuandmete ebaselge määratlus esile vaidlused andmete kvalifitseerimise üle, kuivõrd esmalt tuleb välja selgitada, kas vaidluse esemeks on isikuandmed või mitte.

Kuigi eesmärk võib olla legitiimne, kaasneb abstraktse, subjektiivsel hinnangul põhineva isikuandmete mõistega õiguste nõrgenemine ning õigusselguse kadu, mida on Euroopa Kohus pidanud korduvalt oma lahendites põhiõiguste tõhusa kaitse eelduseks. Selle tagajärjel võivad andmesubjektide õigused muutuda formaalseks ja raskendatuks nii haldus-, kui kohtumenetluses.

2. Teadusuuringud

Kokkuvõte

Kuigi teadusuuringu mõiste määratlemine on tervitatav, on ettepanekus pakutud definitsioon äärmiselt lai ja osaliselt vastuoluline, hõlmates mistahes uurimistöö, ilma et oleks selgelt nõutav teaduslik metoodika või uue üldistatava teadmise loomine. Samuti jäävad ebaselgeks viited eetikanormidele, mis vähendab praktilist selgust ning võib viia selleni, et väga erinevad, sh puhtalt rakenduslikud või ärilised tegevused kvalifitseeritakse teadusuuringutena.

Ettepanekus on selgitatud, et teadusuuringu eesmärgil andmete töötlemisel võib õiguslikuks aluseks olla õigustatud huvi. Selline sõnastus võib tekitada riski, et eesmärgi olemasolu hakatakse võrdsustama õigusliku aluse olemasoluga. Kui seadusandja soov on tõlgendada põhjendust selliselt, et eesmärgi kooskõla tähendab ka õigusliku aluse olemasolu, tuleks AKI hinnangul muuta IKÜM artikli 5 lõike 1 punkti a.

Ettepanek pakub välja täiendava erandi andmesubjekti teavitamiskohustusest, mis koos laia teadusuuringu definitsiooniga võimaldab ulatuslikku teisesel eesmärgil töötlemist andmesubjekti teadmiseta. Selline lähenemine nõrgestab läbipaistvuse, eesmärgipärasuse ja minimaalsuse põhimõtteid, raskendab andmesubjekti õiguste, sh vastuväidete esitamise õiguse tegelikku kasutamist ning tekitab kahtlusi ettepanekute kooskõlas Hartaga, eriti proportsionaalsuse, ettenähtavuse ja tõhusa õiguskaitse nõuetega, nihutades tasakaalu andmesubjekti õiguste kahjuks.

Teadusuuringutega seoses on Euroopa Komisjon oma ettepanekus pakkunud välja mitmeid täiendusi. Käesolevaga esitab Andmekaitse Inspektsioon oma arvamuse väljapakutud muudatuste kaupa.

Teadusuuringu mõiste

(IKÜM artikkel 4 punkt 38)

Euroopa Komisjon on ettepanekus defineerinud teadusuuringu kui igasuguse uurimistöö, mis võib toetada ka innovatsiooni. Need tegevused peavad panustama olemasolevatesse teaduslikesse teadmistesse või rakendama olemasolevaid teadmisi uudsel viisil, neid tuleb läbi viia eesmärgiga aidata kaasa ühiskonna üldise teadmise ja heaolu kasvule ning need peavad järgima asjakohase uurimisvaldkonna eetikanorme. See ei välista, et uurimistöö eesmärk võib olla ka ärihuvide

edendamine.

AKI väljendab oma poolehoidu teadusuuringu defineerimiseks, arvestades et IKÜM mainib teadusuuringuid erinevates kontekstides ka ise, mistõttu suurem õigusselgus teadusuuringute mõiste ümber on vajalik. IKÜMi põhjenduspunktides 33 (nõusoleku kontekstis) ja 159 (õigusliku aluse kontekstis) on selgitatud teadusuuringuga seotud õigusi ja kohustusi. Ettepanekuga soovitakse lisada täiendavad põhjenduspunktid, milledes viidatud metodoloogiline lähenemine, teadustöö kvaliteet, eetikanormide järgimine ja avaliku huvi või statistika eesmärgil täiendav töötlemine on reguleeritud juba kehtivas IKÜMis, mistõttu nende lisamine määrusesse ei anna selgust ega täpsusta teadusuuringute määratlust. Tegelik mõju võimalikele ettepaneku eesmärkidele (andmesubjektide kaitse või teadusvabaduse tagamise) jääb seega piiratuks ning lisatavad põhjenduspunktid ei suurenda õiguslikku selgust.

Ettepanekus esitatud kujul mõiste on sisustatud vastuoluliselt. Esmalt ütleb termin, et teaduslikuks uuringuks on mistahes uurimistöö. AKI on seisukohal, et mistahes uurimistöö defineerimine teadustööks devalveerib teaduse ning teadusuuringute väärtust. Selline lähenemine ei arvesta asjaoluga, et teadusuuring eeldab enamat kui pelgalt uurimusliku tegevuse läbiviimist. Teaduslik uurimistöö peab tuginema teaduslikule metoodikale, olema teooriapõhine ning suunatud uue, üldistatava teadmise loomisele. Kui teadusliku uuringu mõiste alla hõlmatakse ka kirjeldavad, rakenduslikud või halduslikud analüüsid, ähmastub piir teadusliku ja muu uurimistöö vahel. Selle tulemusel kaob teadusuuringu eriline staatus kui süstemaatilise ja kontrollitava teadmise loomise viis. Seetõttu on AKI hinnangul põhjendatud lähenemine, mille kohaselt ei saa iga uurimistööd käsitada teadusliku uuringuna, vaid teadusuuringuks kvalifitseerumine eeldab kindlate sisuliste ja metodoloogiliste kriteeriumide täitmist.

Järgmiseks lisab ettepanek kriteeriumi „võib toetada ka innovatsiooni“, sh käib selle mõiste alla ka tehnoloogiaarendus ja demonstratsioon. See tähendab, et tootearendus, prototüüpimine ja muud rakenduslikud tegevused, mis tavaliselt ei kvalifitseeru akadeemiliseks teaduslikuks uurimiseks, võivad nüüd formaalselt olla teadusuuringud. Senine praktika piirdub pigem teadusliku uurimistööga, mis järgib akadeemilist või teaduslikku metoodikat ning mille eesmärk on genereerida üldist teaduslikku teadmistepagasit.

Ettepanekus toodud määratluse kohaselt võib pidada teadusuuringu eesmärgiks ka ärihuvide edendamist, mis erineb akadeemilisest tavapärasest teadusuuringu käsitlusest.

Kokkuvõttes on tegemist laia, kuid samas osaliselt vastuolulise määratlusega, mis suurendab ettevõtetele võimalust vormistada väga erinevaid tegevusi teadusuuringutena, kuid ei taga täielikku õigusselgust ega kooskõla teadusvabaduse põhimõtetega.

Teisalt, teadusliku uurimistöö mõiste kitsalt piiritlemine isikuandmete kontekstis võib olla vastuolus võimaliku teadusuuringute regulatsiooniga muudes valdkondades. Üldiselt ongi teadusuuringute mõiste üldjuhul konkreetselt defineerimata eelkõige teadusliku ja akadeemilise vabaduse tagamiseks.

Teadusuuringu enda eesmärk ja uuringu läbiviimine peab olema kooskõlas eetikanõuetega. Seejuures ei selgitata põhjenduspunktides ega sättes “vastava uurimisvaldkonna eetiliste standardite” tähendust. Teadustööde puhul on normiks üldjuhul teadustöö valdkonnast, uuringu metoodikast ning heast teadustavast tulenevate põhimõtete järgimise kohustus. Ka IKÜM võiks sarnast lähenemist kasutada ning konkreetse mõiste sõnastamise asemel rõhutada, et lisaks isikuandmete kõrgetasemelise kaitse tagamisele tuleb isikuandmetega tehtavates teadusuuringutes järgida head teadustava (näiteks Euroopa teaduse eetikakoodeks).

Eesmärgipiirangu muutmine teadusuuringute kontekstis

(IKÜM artikkel 5 lõige 1 punkt b)

Seoses eesmärgipärasusega on digitaalses omnibusis ettepanek muuta IKÜM artikli 5 lõike 1 punkti b selliselt, et andmed kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda edasi viisil, mis on nende eesmärkidega vastuolus; edasist töötlemist avalikes huvides arhiveerimise eesmärgil, teadus- või ajaloouuringute eesmärgil või statistilisel eesmärgil loetakse vastavalt artikli 89 lõikele 1 esialgsete eesmärkidega kooskõlas olevaks, olenemata käesoleva määruse artikli 6 lõike 4 tingimustest.

Esmapilgult võib tunduda, nagu väljapakutud täiendus looks uue ja laiemalt kohaldatava aluse andmete edasiseks töötlemiseks. Siiski ei ole see tõlgendus ainuvõimalik, kuivõrd kehtivat sätet lugedes on ka praegu võimalik samale järeldusele jõuda. Praktikas on kujunenud erinevad lähenemised, kus osa andmetöötlejaid ja järelevalveasutusi peavad vajalikuks rakendada täiendavalt artikli 6 lõike 4 analüüsi, seega saab väljapakutud muudatust mõista seadusandja algset soovi selgitava ja täpsustavana, mis ei loo uut erandit, vaid kõrvaldab senise tõlgendusliku ebakindluse.

Kombineerituna ettepanekus toodud äärmiselt laia teadusuuringu määratlusega, võib aga antud säte õõnestada IKÜMiga tagatavat kaitsetaset. Mistahes eesmärgil kogutud isikuandmeid oleks antud sätetele tuginedes hiljem võimalik kasutada näiteks mõne tehisintellektil põhineva keelemudeli arendamiseks, pidades silmas, et innovatsiooni toetamise kriteerium on valikuline ning ka uute teadmiste loomine ei ole nõutav, kuivõrd piisab ka olemasolevate teadmiste uudsel viisil rakendamisest. Eriti probleemne on võimalus sätet tõlgendada viisil, mis lubab järeldada, et edasise töötlemise korral teadusuuringu eesmärgil ei ole vajalik õigusliku aluse sobivuse hindamine, st ka õiguslikule alusele laieneks kooskõla eeldus. AKI märgib, et sellise tõlgendusega nõustuda ei saaks, sest muudatused räägivad endiselt eesmärkide, mitte õiguslike aluste kooskõla eeldusest ning nagu nähtub IKÜM artiklist 5 lg 1 p-dest a ja b on need eraldiseisvad põhimõtted.

Teadusuuringute läbi viimise õiguslik alus

(Ettepaneku põhjenduspunkt 32)

Ettepaneku selgituses ja põhjenduses 32 on öeldud, et kui liidu ega liikmesriigi õigusega ei ole vastuolus, siis on teadusuuringu eesmärgil isikuandmete töötlemise õiguslikuks aluseks õigustatud huvi (IKÜM artikkel 6 lõige 1 punkt f). Põhjendus 32 nendib küll, et vastutava töötleja kohustus tagada punkti f tingimuste täitmine ei ole piiratud. Siiski tekib küsimus, et kas juhul kui isikuandmete töötlemine vastab määruses toodud teadusuuringu definitsioonile ja töötlemine on juba eelduslikult eesmärgiga kooskõlas ilma, et seda peaks eraldi hindama, siis on ka õigustatud huvi olemasolu juba põhimõtteliselt eeldatav. Muudatuse tulemusel võib õigustatud huvi hindamine muutuda tarbetuks formaalsuseks.

Kui seadusandja soov on tõlgendada põhjendust selliselt, et eesmärgi kooskõla tähendab ka õigusliku aluse olemasolu, tuleks AKI hinnangul muuta IKÜM artikli 5 lõike 1 punkti a. Vastasel juhul oleks selline tõlgendus IKÜMi (ja mõnel juhul teaduseetikaga) vastuolus.

Andmesubjekti õigused teadusuuringute läbiviimisel

(IKÜM artikkel 13 lõige 5)

Lisaks IKÜMi artiklite 5 ja 6 muudatusele puudutab isikuandmete kaitset teadusuuringute kontekstis ka artikli 13 lõike 5 lisamine IKÜMi. Nimetatud lõike kohaselt kui töötlemine toimub teadusuuringute eesmärgil ning /.../ teabe esitamine osutub võimatuks või nõuaks ebaproportsionaalselt suuri pingutusi /.../ või kui käesoleva artikli lõikes 1 osutatud kohustus

tõenäoliselt muudaks töötlemise eesmärkide saavutamise võimatuks või kahjustaks seda oluliselt, ei pea vastutav töötleja esitama lõigetes 1, 2 ja 3 osutatud teavet. Sellistel juhtudel võtab vastutav töötleja andmesubjekti õiguste, vabaduste ja õigustatud huvide kaitsmiseks asjakohaseid meetmeid, sealhulgas teeb teabe avalikult kättesaadavaks. Lisaks on ettepaneku põhjenduspunktis 37 selgitatud, et teabe esitamine nõuaks ebaproportsionaalselt suuri pingutusi eelkõige juhul, kui vastutav töötleja isikuandmete kogumise ajal ei teadnud ega näinud ette, et ta töötleb isikuandmeid hiljem teadusliku uurimistöö eesmärgil.

Pakutud artikli 13 lõike 5 lisamine koos ettepanekus toodud teadusuuringu väga laia määratlusega loob praktikas ulatusliku võimaluse töödelda isikuandmeid teisesel eesmärgil andmesubjekti teavitamiseta. Teadusuuringu definitsioon annab võimaluse teha teadusuuringuid ka sellistel andmetöötlejatel, kes koguvad isikuandmeid otse andmesubjektilt näiteks teenuse osutamisel. Kui sellised andmetöötlejad soovivad isikuandmeid teisesel eesmärgil kasutada teadusuuringu läbiviimiseks, ei ole nad kohustatud isikut sellest teavitama. Seega puuduks andmesubjektil sisuliselt ülevaade, kas ja kuidas andmetöötleja tema andmeid kasutab. See nõrgestab läbipaistvuse põhimõtet ning muudab andmesubjekti õiguste kasutamise suurel määral teoreetiliseks.

Lisaks on teabe esitamata jätmise eelduste hindamine jäetud suures osas vastutava töötleja enda otsustada, kuna mõisted nagu „võimatus“ ja „ebaproportsionaalselt suured pingutused“ ei ole selgelt piiritletud. See suurendab õiguskindlusetust ja loob riski, et erandit hakatakse kasutama laialdaselt ka olukordades, kus individuaalne teavitamine oleks tegelikult võimalik. Ettepanekus viidatud võimalus piirduda teabe avalikult kättesaadavaks tegemisega eeldab, et andmesubjekt ise aktiivselt otsib infot tema andmete töötlemise kohta.

Väljapakutud muudatuste koosmõju kahjustab ka eesmärgipärasuse ja andmete minimaalsuse põhimõtteid, kuna teadusuuringu eesmärgile viitamine võib muutuda üldiseks õigustuseks ulatuslikule teisesel eesmärgil töötlemisele. See vähendab survet hinnata, kas konkreetsete isikuandmete töötlemine on teadusuuringu eesmärgi saavutamiseks tegelikult vajalik, ning suurendab riski, et teadusuuringu eesmärk sõnastatakse tagantjärele juba kogutud andmete õigustamiseks.

Lisaks eelnevale tekib küsimus, kuidas saab andmesubjekt kasutada õigust esitada vastuväiteid IKÜM artikkel 21 lõike 6 alusel (kui isikuandmeid töödeldakse teadus- või ajaloouuringute või statistilisel eesmärgil), kui tal puudub teave, kas tema andmeid teadusuuringu raames töödeldakse.

Ettepanek nihutab tasakaalu andmesubjekti õiguste kahjuks ning võib pikemas perspektiivis kahjustada usaldust nii andmetöötlejate kui ka teadusuuringute vastu. Arvestades, et IKÜMi muudatuste eesmärk on regulatiivne lihtsustamine ja VKE-de koormuse vähendamine, ei ole selge, kas läbipaistvuse oluline nõrgenemine ja õiguskindluse vähenemine on selle eesmärgi saavutamiseks põhjendatud.

2.1. Põhiõiguste hartaga tagatud õiguste seos ettepanekuga

Ettepanek laiendab teadusuuringute mõistet viisil, mis tekitab kahtlusi selle kooskõlas Hartas sätestatud proportsionaalsuse ja eesmärgipõhisuse põhimõtetega. Liialt avar teadusuuringute mõiste võib võimaldada selliste tegevuste kvalifitseerimist teadusuuringutena, mis ei ole sisuliselt seotud ei avaliku huvi, teadusliku metoodika ega uue teadmise loomisega, ning seeläbi piirata andmesubjekti õigusi ulatuslikumalt, kui see on vajalik.

Põhiõiguste harta artikli 52 lõike 1 kohaselt on põhiõiguste piiramine lubatav üksnes juhul, kui piirang on selgelt määratletud, teenib legitiimset eesmärki ning on proportsionaalne. Kui teadusuuringute mõiste on ebamäärane, muutub keerukaks hinnata nii piirangu vajalikkust kui ka

seda, kas eesmärgi saavutamiseks oleks võimalik kasutada vähem piiravaid meetmeid. Samuti kannatab läbipaistvus, kuna andmesubjektil võib puududa piisav ülevaade tema andmete tegelikest kasutusviisidest.

Kuigi põhiõiguste harta artikkel 13 tagab teadusuuringute ja akadeemilise vabaduse kaitse, ei saa seda tõlgendada üldise õigustusena isikuandmete kasutamiseks väljaspool selgelt piiritletud teaduslikku konteksti. Akadeemilise vabaduse austamine eeldab, et tegemist on tegeliku teadustegevusega, millel on selge metodoloogiline raamistik ja teadmiste loomise eesmärk. Seetõttu on teadusuuringute mõiste täpsem normatiivne määratlemine vajalik selleks, et tagada tasakaal teadusuuringute vabaduse ning andmesubjekti põhiõiguste tõhusa kaitse vahel.

3. Isikuandmete eriliikide töötlemine tehisintellekti arendamisel ja toimimisel (IKÜM artikkel 9 lõige 2 punkt k; IKÜM artikkel 9 lõige 5)

Kokkuvõte

Ettepaneku eesmärk vältida tehisintellekti arendamise ebaproportsionaalset takistamist on mõistetav. Küll aga on kavandatav erand korraga liiga lai ja samas põhjendamatult kitsas. Erand võib hõlmata sisuliselt igasugust tehisintellekti arendamist ja kasutamist sõltumata eesmärgist, seades ohtu eriliiki isikuandmete kaitse, kuid samal ajal seob nn kogemata isikuandmete töötlemise kontseptsiooni üksnes tehisintellekti ja eriliiki isikuandmetega, jättes välja muud tehnoloogiad ja tavalised isikuandmed. Lisaks nihutab ettepanek rõhu töötlemise tegelikult toimumiselt vastutava töötleja kavatsusele, mis ei ole kooskõlas IKÜMi artikli 9 ega andmete minimaalse kogumise põhimõttega ning tekitab paradoksaalse olukorra, kus eriliiki isikuandmed võivad olla nõrgemalt kaitstud kui muud isikuandmed.

Kavandatav artikli 9 lõige 5 tugineb ebarealistlikele tehnoloogilistele eeldustele, eelkõige seoses eriliiki isikuandmete eemaldamise võimalikkusega juba treenitud tehisintellekti mudelitest. Selline lähenemine normaliseerib eriliiki isikuandmete olemasolu tehisintellekti süsteemides ja on vastuolus IKÜMi artikli 9 lõike 2 erandliku iseloomuga.

AKI rõhutab, et erandi olemasolu ei vabasta andmetöötlejat IKÜMi artikli 6 kohase õigusliku aluse nõudest ning konkreetne tehnoloogia ei saa asendada eesmärgipõhist ja proportsionaalset andmetöötluse analüüsi.

Arvestades ka põhiõiguste hartast tulenevaid eraelu, isikuandmete kaitse, inimväärikuse ja tõhusa õiguskaitse nõudeid, peab AKI põhjendatumaks käsitleda tehisintellekti arendamisega seotud erandeid ja kohustusi tehisintellekti määruse raames, kus laiemad õigused oleksid tasakaalustatud selgemate ja rangemate kohustuste ning nende täitmise järelevalvega.

Digitaalne omnibus sisaldab ettepanekud täiendada eriliigiliste isikuandmete töötlemise erandeid IKÜM artikli 9 punktiga k, mille kohaselt on andmetöötlejal õigus töödelda eriliiki isikuandmeid, kui andmetöötleja tegeleb tehisintellekti süsteemi või mudeli arendamise või toimimisega. Ettepanek täpsustab hiljem IKÜM artikli 9 uues lõikes 5, et isikuandmete eriliikide kogumise ja muul viisil töötlemise vältimiseks rakendatakse asjakohaseid korralduslikke ja tehnilisi meetmeid. Kui vastutav töötleja tuvastab vaatamata selliste meetmete rakendamisele treenimiseks, testimiseks või valideerimiseks kasutatavates andmekogumites või tehisintellekti süsteemis või mudelis isikuandmete eriliikidesse kuuluvaid andmeid, eemaldab vastutav töötleja need andmed.

Kui nende andmete eemaldamine nõuab ebaproportsionaalselt suuri pingutusi, kaitseb vastutav töötleja neid andmeid igal juhul tõhusalt ja põhjendamatu viivituseta väljundite tootmiseks kasutamise, avalikustamise või muul viisil kolmandatele isikutele kättesaadavaks tegemise eest.

Selle täiendava erandi eesmärk on vältida tehisintellekti arendamise ja kasutamise ebaproportsionaalset takistamist, võttes arvesse töötleja võimekust tuvastada ja eemaldada tundlikke isikuandmeid, nagu on selgitatud ettepaneku põhjenduspunktis 33. Erand kehtib olukordades, kus töötleja ei kavatse teadlikult töödelda eriliiki isikuandmeid, kuid sellised andmed on juhuslikult süsteemi sattunud. Andmetöötleja peab rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid, et vältida eriliiki isikuandmete töötlemist kogu tehisintellekti süsteemi või mudeli elutsükli jooksul. Komisjoni hinnangul selgitab ettepanek olukordi, kus varem on olnud ebaselge, kas selline töötlemine on kooskõlas IKÜMi artikli 9 lõike 2 nõuetega, ning aitab seeläbi otseselt toetada innovatsiooni ja tehisintellekti arendamist, mis on usaldusväärne, diskrimineerimisvaba ja säilitab kõrge andmekaitsetaseme.

AKI on seisukohal, et uus erand on väga lai ja näib potentsiaalselt hõlmavat mis tahes tehisintellektimudeli või -süsteemi arendamist ja toimimist, sealhulgas mis tahes eesmärgil. Sellega kaasneb märkimisväärne oht eriliiki ehk kõige suuremat kaitset vajavatele isikuandmetele. Teisalt on uus erand kitsas, kuivõrd hõlmab kõikvõimalike tehnoloogiliste võimaluste seast vaid tehisintellekti arendamist ja toimimist, arvestamata näiteks klassikalisi algoritme ja muid automatiseeritud süsteeme. AKI toob lisaks välja, et erand hõlmab vaid eriliiki isikuandmete töötlemist, samas muude isikuandmete puhul selline erand puudub, mis justkui tekitab olukorra, kus eriliiki isikuandmed on vähem kaitstud kui tavalised isikuandmed.

Ettepaneku artikli 9 lõike 2 punktis k sätestatud uus erand koos uue lõikega 5 viitavad sellele, et erand hõlmab eriliiki isikuandmete töötlemist vaid juhul, kui vastutav töötleja ei kavatsenud selliseid andmeid töödelda. Seega fakt, kas konkreetne isikuandmete töötlemine kuulub punktis k sätestatud erandi alla, näib tuginevat hinnangule, kas vastutav töötleja kavatseb töödelda eriliiki isikuandmeid, samas kui artikli 9 lõikes 1 sätestatud keelud sõltuvad sellest, kas eriliiki isikuandmeid tegelikult töödeldakse või mitte. Eeltoodu on vastuolus ka andmete minimaalse kogumise põhimõttega, mis on kirjas IKÜM artikli 5 lõike 1 punktis b.

Tuleb rõhutada, et selline kogemata isikuandmete töötlemise kontseptsioon ei saa olemuslikult olla seotud üksnes tehisintellektiga ega eriliiki isikuandmetega. Kui sellist lähenemist peetakse vajalikuks, peaks see kehtima horisontaalselt kõikides sektorites ja kõigi isikuandmete puhul, mitte looma erandi üksnes konkreetsele tehnoloogiale. Vastasel juhul tekib põhjendamatu ebavõrdsus erinevate töötlemisviiside ning majandussektorite vahel ning risk, et tehnoloogia ise muutub isikuandmete kaitse nõrgendamise aluseks.

Probleemseks saab pidada ka lisatava artikli 9 lõike 5 sõnastust, et juhul kui tehisintellektisüsteemis tuvastatakse isikuandmete eriliigid, siis vastutav töötleja need eemaldab välja arvatud juhul, kui nende eemaldamine osutub ebaproportsionaalselt suureks jõupingutuseks. Tegelikkuses on levinud seisukoht, et tehisintellektist isikuandmete eemaldamine on võimalik küll teoorias, kuid mitte praktikas. Võimalik on kasutada isikuandmete maskeerimise või blokeerimise meetmeid, et mudel enam nendega ei arvestaks, kuid täielik eemaldamine pole võimalik.

Kui tehisintellekti mudelid on juba treenitud, on praeguse tehnoloogilise taseme juures (täna on ebaselge, mis ajaraamis nt masinõppe tehnoloogia areneb, mis võimaldaks andmeid päriselt kustutada) peaaegu võimatu sellest mudelist teatud meelde jäetud isikuandmeid eemaldada, välja arvatud juhul, kui seda mudelit teadlikult selliselt ümber treenitakse. Nii rajaneb kavandatav säte juba valedele eeldustele. On selge, et eriliiki isikuandmete eemaldamine tehisintellekti süsteemist või mudelist osutub ebaproportsionaalselt suureks jõupingutuseks, mis juba vaikimisi loob

eelduse, et need võivad seal olla. Samas IKÜM artikli 9 lõike 2 järgi peaks eriliiki andmete töötlemine olema erand ja eriliiki isikuandmed peaksid olema erilise kaitse all, mis tähendab, et vaikimisi lubatud andmetöötlus artikli 9 lõikes 5 ei ole lõikega 2 kooskõlas.

Eriliiki isikuandmete töötlemise erandi olemasolu ei tähenda, et IKÜMi artikli 6 kohane õiguslik alus muutub eeldatavaks. Ka tehisintellekti arendamise kontekstis peab isikuandmete töötlemisel alati eksisteerima selge ja sobiv õiguslik alus IKÜM artiklist 6 ning selle olemasolu ei saa asendada viitega tehnoloogilisele paratamatusele või juhuslikule andmete sattumisele süsteemi.

Oluline on märkida, et ettepanek keskendub eelkõige tehnoloogiale, mitte töötlemise eesmärkidele. IKÜMi loogika lähtub aga eesmärgipõhisest andmetöötlusest ning tehnoloogia on seejuures vahend, mitte iseseisev õigustav alus. Kui tehisintellekti arendajatele soovitakse anda laiemad õigused, peab sellega paratamatult kaasnema ka täpsem ja rangem kohustuste raamistik. Sellest tulenevalt oleks süsteemselt põhjendatum käsitleda selliseid erandeid ja kohustusi tehisintellekti määruses, kus on piiritletum kohaldumisala, määratud riskitasemed ning riskitasemetele vastavad teatud õigused ja kohustused ning on loodud reeglistik järelevalveks nende täitmise üle. Laiemad õigused tehisintellekti arendamisel peavad olema tasakaalustatud selgemate, konkreetsemate ja rangemate andmekaitseliste kohustustega, mitte üldise ja tehnoloogiapõhise erandiga IKÜMis.

3.1. Põhiõiguste hartaga tagatud õiguste seos ettepanekuga

Ettepanek võimaldab tehisintellekti süsteemide arendamisel ja kasutuselevõtul ulatuslikku isikuandmete, sealhulgas eriliiki isikuandmete töötlemist üksnes põhjendusel, et tehisintellektisüsteemid vajavad suuri andmemahtusid või keerukaid andmestikke. Selline lähenemine ei sisalda nõutavat vajaduse ega proportsionaalsuse analüüsi ning ei arvesta põhiõiguste hartas sätestatud põhimõttega, mille kohaselt peab eriliiki isikuandmete töötlemine olema erandlik, rangelt põhjendatud ja selgelt tasakaalus taotletava eesmärgi ning põhiõigustele avalduva mõjuga.

Harta artiklite 7 ja 8 valguses kujutab massiline andmekogumine, profileerimine ja andmete tuletuslik töötlemine endast sügavat sekkumist eraellu ja isikuandmete kaitse õigusesse. Tehisintellekti süsteemid ei piirdu üksnes olemasolevate andmete töötlemisega, vaid võimaldavad tuletada uusi andmeid, sealhulgas tervisliku seisundi, seksuaalse sättumuse või poliitiliste vaadete kohta. Arvestades, et eriliiki andmed on nii Harta artikli 8 kui ka IKÜM artikli 9 alusel erilise kaitse all, toob sellise töötlemise normaliseerimine kaasa olulise kaitsetaseme nõrgenemise.

Lisaks võib tehisintellekti põhine andmetöötlus riivata Harta artiklis 1 sätestatud inimväärikuse põhimõtet, kuivõrd isikuid käsitletakse pelgalt andmepunktide ja riskiprofiilidena, kaotades kontrolli oma identiteedi ja haavatavuste üle. Süsteemid, mis õpivad inimeste käitumisest ja „haavatavustest“, võivad sekkuda inimväärikuse olemusse viisil, mis ei ole kooskõlas põhiõiguste kaitse eesmärgiga.

Harta artikli 47 seisukohalt on problemaatiline ka tehisintellekti otsuste piiratud läbipaistvus ja vaidlustatavus. Kui otsused põhinevad eriliiki andmete töötlemisel või nendest tuletatud järeldustel, ei pruugi isikul olla võimalik mõista, miks tema suhtes konkreetne tulemus kujunes, mis omakorda pärsib tõhusat õiguskaitset.

Kõnealune lähenemine tõstatab Harta artikli 52 lõike 1 valguses riski, et eriliiki andmete töötlemisest saab tehisintellekti arenduses tavapärane praktika ning põhiõiguste kaitse taandub formaalseks. Lisaks ei saa välistada võimalikke riiveid Harta artiklite 20 ja 21 (võrdne kohtlemine

ja diskrimineerimiskeeld) osas, samuti Harta artiklite 10 ja 11 osas, kuna maailmavaadete ja hoiakute kaardistamine võib kaasa tuua enesetsensuuri ning piirata mõtte- ja sõnavabaduse tegelikku kasutamist.

4. **Isikuandmete eriliikide töötlemine biomeetriliste andmete puhul**
   (IKÜM artikkel 9 lõige 2 punkt l)

Ettepanek sisaldab uut eriliiki isikuandmete töötlemise erandit artikli 9 lõike 2 punktis l. Punkti l kohaselt on eriliiki isikuandmete töötlemine lubatud, kui biomeetriliste andmete töötlemine on vajalik andmesubjekti isikusamasuse kinnitamiseks (kontrollimine), kusjuures biomeetrilised andmed või kontrollimiseks vajalikud vahendid on andmesubjekti ainukontrolli all.

Ettepaneku põhjenduspunktis 34 on selgitatud, et säilitades biomeetrilisi andmeid turvaliselt ainult andmesubjekti juures või vastutava töötleja juures tipptasemel krüpteeritud kujul ning krüpteerimisvõtit või samaväärset vahendit valdab ainult andmesubjekt, ei tekita selline töötlemine tõenäoliselt olulisi ohte tema põhiõigustele ja -vabadustele. Vastutav töötleja ei saa biomeetrilistest andmetest teada või saab neid teada ainult väga piiratud aja jooksul kontrolliprotsessi käigus.

AKI tervitab biomeetriliste andmete töötlemiste õiguslikku alust ning nõustub põhjenduspunktis toodud näitega. Täiendus, et isikusamasuse kinnitamine biomeetria abil on lubatud vaid juhul, kui kontrollimiseks vajalikud vahendid on andmesubjekti ainukontrolli all, on oluline tingimus isikuandmete kaitse kontekstis.

5. **Andmesubjekti juurdepääs andmetele**
   (IKÜM artikkel 12 lõige 5)

Digitaalse omnibusi ettepanekus on IKÜM artikkel 12 lõiget 5 täiendatud ning välja on pakutud, et artiklite 13 ja 14 kohaselt esitatav teave ning artiklite 15–22 ja 34 alusel tehtavad teated ja võetud meetmed esitatakse tasuta. Kui andmesubjekti taotlused on ilmselgelt alusetud või ülemäärased, eelkõige nende korduva iseloomu tõttu või ka artikli 15 alusel esitatud taotluste puhul seetõttu, et andmesubjekt kuritarvitab käesoleva määrusega antud õigusi muul eesmärgil kui oma andmete kaitse, võib vastutav töötleja kas:

(a) nõuda mõistlikku tasu, võttes arvesse teabe või teate edastamise või taotletud toimingu tegemise halduskulusid; või

(b) keelduda taotluse alusel tegutsemast.

Vastutav töötleja kannab kohustust tõendada, et taotlus on ilmselgelt alusetu või et on mõistlik alus arvata, et see on ülemäärane.

Seega, ettepanek lisab andmetöötlejale võimaluse keelduda andmete väljastamisest artikli 15 kohaste taotluste puhul, kui andmesubjekt kuritarvitab IKÜM-iga antud õigusi muul eesmärgil kui oma andmete kaitsmine. Juurdepääsu andmisest keeldumise võimalus on andmetöötlejatel IKÜM artikkel 12 lõikes 5 olemas juba praegu. Kavandatud muudatus pöörab sisuliselt tõendamiskoormise andmetöötlejatelt andmesubjektidele: kui käesoleval hetkel on andmetöötlejal kohustus oma keeldumist põhjendada, siis edaspidi on esmalt andmesubjektil vaja tõendada, et tal on andmetele juurdepääsu vaja andmete kaitsmiseks ning andmetöötlejal on madal lävend oma keeldumist põhjendada.

AKI möönab, et andmesubjektide taotlused oma andmetele juurdepääsuks võivad teinekord olla ülemäärased või pahatahtlikud, näiteks naabrikaamerate vaidlused võivad alata sellest, et naaber soovib kaamera paigaldanud naabrilt saada enda liikumist sisaldavat kaamerapilti eelneva kuu lõikes. Ehkki naaber kasutab sellises olukorras oma IKÜM artikkel 15 õigust, võib olla tema

tegelikuks eesmärgiks koormata kaamera paigaldanud naabrit tülika järelevalvemenetlusega. Sellest hoolimata on AKI arvamusel, et käesoleva ettepaneku sõnastus on mõneti ebaõnnestunud, kuivõrd jätab mulje, et andmetöötlejal on laiaulatuslikud õigused jätta taotlused lahendamata ülemäärasuse põhjendusel. Selged juhised, kuidas ülemäärasust või õiguse kuritarvitamist hinnata, puuduvad. Selliste juhiste puudumine tekitab tõenäoliselt vaidlusi hindamise õiguspärasuse üle nii järelevalveasutuste vaates kui ka kohtumenetluses. See tähendab, et andmesubjektid tõenäoliselt jätavad selle õiguse kasutamata, kui on oht, et andmetele juurdepääsule võib eelneda aastatepikkune järelevalve- ja kohtumenetlus.

Ettepanek piirab andmesubjektide õiguste kasutamist juhtudele, kui andmesubjekt soovib andmeid oma andmete kaitsmiseks. Tegemist on väga kitsa käsitlusega, millal andmesubjekt võib soovida oma andmetele ligipääsu. Andmesubjekt võib soovida andmeid mitmetel teistel eesmärkidel, näiteks töösuhete kontekstis võib andmesubjekt soovida värbamisprotsessis kogutud andmetele ligipääsu, et hinnata, kas otsus põhines ebaõigetel hinnangutel või kindlustusvaidluse ettevalmistamisel võib andmesubjekt taotleda kindlustusandjalt andmeid, mis on seotud kahjukäsitlusega. Sellistel eesmärkidel andmete väljastamine ettepaneku kohaselt kohustuslik ei ole, kuivõrd andmete taotlemise eesmärgiks ei ole andmete kaitsmine.

IKÜM artikli 12 lõike 5 sõnastuse viimase lause muutmine “on mõistlik alus arvata” paneb rõhu taaskord subjektiivsele hinnangule. Ettepanekus toodud sõnastuse kohaselt on andmetöötlejal õigus pärida põhjendust andmesubjekti andmete saamiseks. Vaid juhul, kui andmesubjekti eesmärk on oma andmete kaitsmine, on andmetöötleja kohustatud andmed väljastama. Ettepaneku põhjenduspunkt 35 täiendab, et andmetöötlejal on ülemäärasest taotlusest keeldumisel madal tõendamiskohustus ning täpsustab, et igal juhul peaks andmesubjekt IKÜM artikli 15 alusel juurdepääsu taotlemisel olema võimalikult täpne ehk liiga laiaulatuslikke ja eristamata taotlusi tuleks samuti pidada liigseks. Tuleb arvestada, et teinekord tuleb pidada põhjendatuks andmesubjekti taotlust küsida välja kõik andmed, mis andmetöötlejal tema kohta olemas on selleks, et hinnata, kas andmete töötlemine konkreetse andmetöötleja poolt on seaduslik ja õiguspärane. Ettepaneku kohaselt on iga selline taotlus edaspidi ülemäärane ning andmetöötleja ei pea põhjendama sellisest taotlusest keeldumist. Ettepaneku põhjenduspunktide kohaselt peaks andmesubjekt teadma, mis andmed andmetöötlejal tema kohta on, kuid praktikas tekitavad vaidlusi just need andmed, mida andmetöötlejal olla ei tohiks.

Ehkki ettepanek täpsustab, et ülemääraseks võib pidada taotlusi, mille eesmärk ei ole andmete kaitsmine, tuleb märkida, et andmesubjekt võib taotluses küll tuua põhjenduseks andmete kaitsmise, kuid andmetöötlejal on õigus hinnata andmesubjekti põhjendust subjektiivselt, kas taotluse eesmärk on tõesti see, mida andmesubjekt väidab. See tekitab tulevikus vaidluskohti, mida täna olnud ei ole, ning järelevalveasutuste halduskoormus võib kasvada.

Euroopa Kohtu otsus kohtuasjas FT, C-307/22 punktides 38 ja 43 on selgitatud, et andmesubjekt ei pea vastutavale töötlejale esitama andmetele juurdepääsu taotluse põhjuseid. Kohtu sõnul on vastutav töötleja kohustatud andma andmesubjektile tasuta tema töödeldavate isikuandmete esimese koopia, isegi kui taotluse põhjus ei ole töötlemise seaduslikkusest teadasaamine ja selle kontrollimine. Samal seisukohal on Kohus olnud ka mitmetes hilisemates lahendites. Antud muudatus paistab olevat kantud pooleliolevast Euroopa Kohtu menetlusest C-526/24, kuid üksnes üks menetlus ei peaks laskma mõjutada senist praktikat, eriti kui see menetlus pole jõudnud Euroopa Kohtu lõpliku lahendini.

Ettepanek toob kaasa õigusliku ebakindluse nii andmesubjektide kui ka vastutavate töötlejate jaoks, tuues kaasa keerulisi äärmuslikke juhtumeid ja ettenähtavaid edasi-tagasi suhtlusi. Vastutavate töötlejate jaoks võib muutuda juurdepääsutaotluste hindamine keeruliseks. Selleks, et

hinnata, kas andmesubjekt soovib juurdepääsu andmete kaitsmiseks, peab andmetöötleja tõenäoliselt edaspidi rohkem andmeid töötlema. Seetõttu on väga küsitav, kas see kavandatav muudatus tegelikult vähendaks vastutavate töötlejate administratiivset koormust.

Andmesubjekti vaatest tekitab olukord teadmatust, kuivõrd hindamine oleks ettepaneku kohaselt iga andmetöötleja subjektiivsetel alustel, mistõttu sama põhjendus erinevate andmetöötlejate juures võib viia erineva lahenduseni. Seega asjaolu, kas andmetöötleja saab oma õigust kasutada või mitte, sõltub andmetöötleja diskretsioonist ja heast tahtest.

5.1. Põhiõiguste hartaga tagatud seos ettepanekuga

Harta artikkel 8 lg 2 kätkeb endas õigust tutvuda enda kohta kogutud andmetega ja nõuda nende parandamist. Harta tasandil on tegemist fundamentaalse õigusega ja Harta ei täpsusta, et sellise õiguse rakendamine eeldab teatud tingimustele vastamist. See tähendab, et andmesubjekt, kelle andmeid on kogutud, võib tutvuda oma andmetega ilma igasuguse põhjenduseta, eesmärgiga tagada inimväärikus ja autonoomia, kuid ühtlasi praktiliselt omada kontrolli oma andmete üle. Sõltumine andmetöötleja õigusest küsida põhjendusi on vastuolus Harta artikkel 8 lõikega 2, kuivõrd seab andmesubjekti enda andmete üle kontrolli teostamise tingimuslikuks.

6. Erandi täpsustamine, kui andmed on saadud andmesubjektilt (IKÜM artikkel 13 lõige 4)

Ettepanekuga täpsustatakse IKÜM artikli 13 lõike 4 teksti. Ettepaneku eesmärk on muuta erandit, mis lubab andmetöötlejatel mitte anda andmesubjektidele teavet juhul, kui isikuandmeid kogutakse otse andmesubjektilt. Kuigi kehtiv määrus loob artikli 13 kohase läbipaistvuskohustuse erandi juhuks, kui andmesubjektil on kogu teave juba olemas, soovitab ettepanek teha teabe esitamisest erandi juhul, kui vastutav töötleja mõistlikult eeldab, et andmesubjektil on juba teatav teave olemas (näiteks vastutava töötleja identiteet ning töötlemise eesmärk ja õiguslik alus). See täiendav erand kehtiks teatud tingimustel: i) isikuandmed on kogutud andmesubjektide ja vastutava töötleja vahelise selge ja piiritletud suhte kontekstis ning ii) vastutav töötleja tegutseb viisil, mis ei ole andmemahukas.

IKÜM artikkel 13 lõige 4 erand kehtib vaid juhul, kui ei kohaldu ükski välistustest. Näiteks on üheks välistuseks, et andmeid ei tohi edastada teistele vastuvõtjatele, seega näiteks raamatupidamisteenuse osutajale, makseteenuse osutajale, veebiserveri teenusepakkujale, e-mailiteenuse pakkujale jms, kes on vastuvõtjateks IKÜM artikkel 4 punkti 9 alusel. Välistuseks on ka andmete edastamine kolmandasse riiki, kuid mitmeid veebiserveri teenusepakkujad on just selliselt üles ehitatud, mistõttu oleks juba mitu alust erandi mittekohaldamiseks.

Käesoleva sõnastusega muudab ettepanek IKÜM artikkel 13 lõiget 4 drastiliselt, kuivõrd hetkel on andmetöötlejal võimalik toetuda erandile, et andmesubjektil on teave juba olemas. Ettepaneku järgi muutuvad erandi kasutamise tingimused aga nii kitsaks, et enamik andmetöötlejatest ei saa seda enam rakendada. Põhimõtteliselt kohalduks muudatus vaid mõnele ühemeheettevõttele või käsitöö tegijale, kes sularaha eest oma kaupu kuskil laadal müüb. Arvestades, et kõikide IKÜMi muudatuste eesmärk on vähendada VKE-de kohustusi ja halduskoormust, võtab käesolev muudatus võimaluse toetuda kehtivas IKÜMis olevale teabe teatavaks tegemise erandile.

7. Automatiseeritud otsuste tegemine (IKÜM artikkel 22 lõige 1)

Digitaalse omnibussi ettepanekuga soovitakse muuta IKÜMi artikli 22 lõikeid 1 ja 2 selliselt, et olemasolev sõnastus eemaldatakse, pannakse kokku lõiked 1 ja 2 ning uue sõnastuse kohaselt otsus, millel on andmesubjektile õiguslikud tagajärjed või mis teda sarnasel viisil oluliselt mõjutab,

võib põhineda üksnes automatiseeritud töötlusel, sealhulgas profiilianalüüsil, ainult juhul, kui see otsus vastab lõike 1 tingimustele.

IKÜM artikli 22 lõike 1 punkti a (kehtiva sõnastus artikli 22 lõike 2 punktis a) lisatakse allajoonitud tekst: on vajalik andmesubjekti ja andmetöötleja vahelise lepingu sõlmimiseks või täitmiseks, olenemata sellest, kas otsuse saaks teha muul viisil kui üksnes automatiseeritud vahenditega.

Muudatuse kohta on ettepaneku põhjenduspunktis 38 selgitatud, et asjaolu, et otsuse võiks langetada ka inimene, ei takista vastutaval töötlejal langetamast otsust üksnes automatiseeritud töötlemise teel. Kui eksisteerib mitu võrdselt tõhusat automatiseeritud töötlemise lahendust, peaks vastutav töötleja kasutama vähem riivavat.

Uus sõnastus näib alandavat automatiseeritud otsuste kasutamise künnist ning kuigi otsuse võiks langetada ka inimene, ei takista see enam automatiseeritud otsuse tegemise võimalust. Kehtiva IKÜM-i kohaselt piirab vajalikkuse kriteerium automatiseerimist ainult juhtudele, kui teistmoodi ei ole võimalik lepingut täita. Ka olemasolev kohtupraktika tõlgendab vajalikkuse kriteeriumit selliselt, näiteks lahendites C-252/21 (Meta vs Bundeskartellamt), C-634/21 (SCHUFA Holding AG) ja C-817/19 (Ligue des droits humans/PNR).

Artikli ümbersõnastamine toob kaasa olulise õigusliku muudatuse, võttes fookuse üksikisiku õiguselt keelduda automatiseeritud otsusest ning pannes selle vastutava töötleja tegevusõiguse määramisele. Sealjuures tuleks panna tähele, et artikkel 22 on IKÜM II peatükis, mis on pealkirjastatud kui "Andmesubjekti õigused". IKÜM artikkel 12 lõige 2 viitab samuti, et vastutav töötleja aitab kaasa artiklite 15-22 kohaste andmesubjekti õiguste kasutamisele. IKÜM artikli 22 väljapakutud sõnastus ei tugevda andmesubjekti õigust mitte alluda üksnes automatiseeritud otsustele, vaid nihutab regulatiivse tasakaalu selgelt andmetöötleja huvide kasuks. Kui automatiseeritud otsuse lubatavus seotakse üksnes lepingulise vajalikkusega, sõltumata sellest, kas otsus oleks võimalik teha ka muul, vähem riivaval viisil, kaotab artikkel 22 oma kaitsefunktsiooni ning erand muutub sisuliselt reegliks. Selle tulemusel kaotab andmesubjekti õigus oma sisu ning artikli paiknemine IKÜMi andmesubjekti õigusi käsitlevas peatükis muutub normatiivses plaanis formaalseks, mitte tegelikku õiguskaitset tagavaks.

Komisjon on ettepaneku põhjenduspunktis 38 selgitanud, et suurema õiguskindluse tagamiseks tuleks selgitada, et otsuseid, mis põhinevad üksnes automatiseeritud töötlemisel, on lubatud teha siis, kui on täidetud eritingimused. AKI toob välja, et juba täna seisavad andmesubjektid sageli silmitsi läbipaistmatute (automatiseeritud) otsustega näiteks tööle kandideerimisel või krediidilimiitide kasutamisel. Kui automatiseeritud andmetöötlus muutub lepingute puhul vaikimisi põhivalikuks, muutuvad artikli 22 lõikes 3 sisalduvad kaitsemeetmed veelgi olulisemaks, kuid ettepanek ei tugevda kaitsemeetmeid. Vastupidiselt annab ettepanek võimaluse vähendada kontrolli, kas sellise automatiseeritud otsuse kasutamine oli tegelikult vajalik. Ehkki Komisjon on ettepanekuga soovinud tagada suuremat õiguskindlust, ei täida muudetud sõnastus eesmärki.

Andmekaitse Inspektsioon juhib tähelepanu ka tehnilisele sõnastusveale. Kuigi ettepanek ühendab lõiked 1 ja 2, ei kajastu ettepanekus lõigete 3 ja 4 ristviidete täpsustamine.

8. Rikkumisteated ja ühtne teavituspunkt
(IKÜM artikkel 33)

Kokkuvõte

Digitaalne omnibus muudab IKÜM artikli 33 rikkumisteadete reegleid, tõstes teavitamise

lävendi suure ohu realiseerimisele, sätestades teavitamise ühtse teavituspunkti kaudu ning pikendades järelevalveasutuse teavitamise tähtaega 72 tunnilt 96 tunnile. AKI hinnangul aitab lävendi tõstmine vähendada halduskoormust ja vähendab liigsete teavituste survet andmetöötlejatele, kuid samas kaob järelevalveasutuste võimalus jälgida nn keskmise ohuga rikkumisi ning kaotatakse oluline varajase sekkumise mehhanism.

Ühtne teavituspunkt võimaldab andmetöötlejatel edastada rikkumisteated korraga mitmele järelevalveasutusele, toetades haldusprotsesside koordineerimist. Samas tuleb arvestada, et erinevad õigusaktid sätestavad rikkumisest teavitamisele erinevad tähtajad ja künnised: ettepaneku kohaselt tuleb andmekaitsega seotud suure ohuga rikkumistest teavitada 96 tunni jooksul, samas kui NIS2 direktiiv ja Komisjoni määrus 611/2013 näevad ette lühemaid tähtaegu ja teisi lävendeid, mis võivad samale intsidendile kehtida. Kuna ettepanek ei täpsusta nende tähtaegade ja lävendite kooskõla, võib see tekitada õiguslikku ebaselgust rikkumisteadete esitamisel ning vajab täiendavat selgitamist ja koordineerimist.

Digitaalse omnibusi ettepanek lisab IKÜMi artiklile 33 lõike 6, mille kohaselt koostab ja edastab Euroopa Andmekaitsenõukogu (EAKN) Komisjonile ettepaneku ühtse vormi kohta, mille alusel teavitatakse lõikes 1 osutatud pädevat järelevalveasutust isikuandmetega seotud rikkumisest, ning loetelu asjaolude kohta, millal isikuandmetega seotud rikkumine võib tõenäoliselt kujutada endast suurt ohtu füüsilise isiku õigustele ja vabadustele. AKI toetab mõtet anda ühiste vormide väljatöötamise juhtimine EAKNile. Küll aga on AKI on seisukohal, et EAKN väljatöötatud vormide vastuvõtmise autonoomsus peab jääma EAKNile kui iseseisvale Euroopa institutsioonile. Andes vormide muutmise õiguse ja rakendusaktina vastuvõtmise õiguse Euroopa Komisjonile, on küsimuse all esmalt EAKNi kui organi sõltumatus ning teisalt ei ole kindel, kas rakendusaktiga vastu võetu väljendab EAKNi soovitusi ja praktikaid. Seetõttu tuleks teha artikli 33 lõikes 6 täpsustus, et EAKNi väljatöötatud vormid tuleb Euroopa Komisjonil rakendusaktina vastu võtta muutmata kujul.

Peamine muudatus seoses rikkumisteadetega sisaldub artikli 33 lõikes 1 (allajoonitud tekst), mille kohaselt teavitab vastutav töötleja isikuandmetega seotud rikkumise korral, mis tõenäoliselt kujutab endast suurt ohtu füüsiliste isikute õigustele ja vabadustele põhjendamatu viivituseta ja võimaluse korral hiljemalt 96 tunni jooksul pärast rikkumisest teadasaamist direktiivi (EL) 2022/2555 artikli 23a kohaselt loodud ühtse teavituspunkti *(single entry point)* kaudu artiklite 55 ja 56 kohaselt pädevat järelevalveasutust.

Allajoonitud tekst viitab kolmele muudatusele:

1) rikkumisteavitused tuleb teha vaid suure ohu tõenäolisel ilmnemisel (praeguse ohu ilmnemise asemel);

2) rikkumisteated tuleb esitada 96 tunni jooksul (varasema 72 tunni asemel) ning

3) rikkumisteade tuleb esitada ühtse teavituspunkti (*single entry point)* kaudu.

AKI esitab analüüsi iga muudatuse kohta eraldi.

Rikkumisteadete esitamine suure ohu tõenäolisel ilmnemisel

Kehtiv IKÜM sätestab kaheastmelise rikkumise hindamise loogika. Esmalt teavitavad vastutavad töötlejad IKÜM artikli 33 lõike 1 kohaselt andmekaitse järelevalveasutusi alati, kui rikkumine on seotud riskiga isikuandmete kaitsele ning teiseks teavitavad vastutavad töötlejad IKÜM artikli 34

kohaselt rikkumisega seotud andmesubjekte juhul, kui oht[1] on suur.

Selline kaheastmeline loogika võimaldab täna järelevalveasutustel säilitada ülevaade erinevatest rikkumistest ja annab võimaluse otsustada sekkumise vajaduse ning ulatuse või hinnata, kas on täiendavalt vaja teavitada andmesubjekte. Eeldus on, et juhul kui rikkumine on suur ning on vajalik teavitada andmesubjekte, peab sellele eelnema alati järelevalveasutuse teavitamine.

Ettepanekus tõstetakse IKÜM artikli 33 künnis kõrge ohutasemeni ja artiklite 33 ning 34 ohutasemed ühtlustuvad. Sellega kaotatakse justkui järelevalveasutuste vaatest vajalik esmane filter ja jäetakse alles ainult olulisematest kõrvalekalletest teavitamine. Sellest tulenevalt kaotavad järelevalveasutused teadmise enamikest intsidentidest, mis ei ole tavapäraselt suure ohuga, kuid annavad olulist teavet turvalisuse suundumuste ja vastutavate töötlejate nõuete täitmise kohta. AKI nõustub, et tänase praktika kohaselt on andmetöötlejatel suundumus pigem teatada ka väga väikestest rikkumistest ning halduskoormust arvestades on tervitatav, et praegust sõnastust soovitakse muuta. Küll aga tundub, et kuigi muudatus on kasulik andmetöötlejatele (puudub enamasti teavitamiskohustus), kaob järelevalveasutustel oluline võimalus seirata andmekaitsealaste nõuete täitmise kohustusi.

Praegu on IKÜM artikli 34 lõikega 4 antud andmekaitse järelevalveasutustele õigus vastutava töötleja hinnang riski kohta ümber hinnata. Kui vastutav töötleja väidab, et rikkumine ei ole suure riskiga, kuid järelevalveasutus ei nõustu, võivad järelevalveasutused siiski anda vastutavale töötlejale korralduse andmesubjekte teavitada.

Ettepaneku kohaselt ei pea vastutav töötleja vähem kui suure ohu puhul järelevalveasutust teavitama. Järelevalveasutus ei saa sellisel juhul vajalikku esialgset teavitust, mis on vajalik teisese hindamise (kas tegemist võiks olla suure riskiga juhtumiga) läbiviimiseks. See muudab artikli 34 lõike 4 sisuliselt kehtetuks, jättes ainsa kontrolliõiguse vastutavale töötlejale. Kuigi vastutaval töötlejal jääb alles rikkumise dokumenteerimise kohustus, peaks järelevalveasutus neid edaspidi eraldi igalt andmetöötlejalt hakkama välja küsima, mis loob halduskoormust juurde.

AKI teeb ettepaneku tõsta teavitamise lävend ohtudele, mida ei saa pidada väikeseks. Selliselt jääks alles kohustus teavitada ka nn keskmistest ohtudest, mille realiseerumise korral oleks järelevalveasutustel vajadusel võimalik kasutada oma IKÜM artikli 34 lõikes 4 ettenähtud õigust.

Tähtaja pikendamine 72 tunnilt 96 tunnile

Kehtiva õiguse kohaselt tuleb andmetöötlejal andmekaitse järelevalveasutust teavitada rikkumisest 72 tunni jooksul. Ettepanek pikendab teavitamiskohustust 96 tunnile. See annab vastutavatele töötlejatele piisavalt aega põhjalikuma uurimise tegemiseks, mis võib parandada esitatud teabe kvaliteeti. Teisalt jätab ettepanek alles andmetöötleja võimaluse hiljem rikkumisteadet täpsustada, mistõttu jääb ebaselgeks teavitamiskohustuse aja pikendamise vajadus ja kuidas see teenib lihtsustamise eesmärki.

Ühtse teavituspunkti kaudu pädevate järelevalveasutuste teavitamine

Ettepaneku kohaselt luuakse ühtne teavituspunkt direktiivi 2022/2555 (NIS2) artikli 23a alusel. Pärast teavituspunkti loomist on andmetöötlejatel kohustus järelevalveasutusi (sh andmekaitse kui ka küberturvalisuse) rikkumistest teavitada vaid ühtse teavituspunkti kaudu ühel korral. Täpsemalt on ettepanekus NIS2 artikli 23a lõike 3 punktis f kohta toodud, et üksuse poolt ühtse teavituspunkti kaudu esitatud teabe ühekordset teavitust saab kasutada aruandluskohustuste täitmiseks, mis on sätestatud mis tahes muus liidu õigusaktis, mis näeb ette intsidentide teatamise ühtse

[1] Andmekaitse Inspektsioon möönab, et inglise keeles kasutatakse sõna "risk", samas eesti keeles "oht". Käesoleva arvamuse kirjutamisel lähtub Andmekaitse Inspektsioon ametlikust eestikeelsest tõlkest.

teavituspunkti kaudu. AKI märgib, et intsidentidest teavitamise kohustus ühtse teavituspunkti kaudu on ettepanekus toodud välja IKÜM-i, direktiivi 2022/2557 (elutähtsa teenuse osutajate direktiiv), NIS2, määruse 910/2014 (EIDAS) ning määruse 2022/2554 (tegevuskerksuse määrus ehk DORA) puhul.

Eeltoodud õigusaktidest võib olla rikkumiste korral ühisosa näiteks IKÜMi ja NIS2 rikkumiste puhul. NIS2 rikkumistest teavitamise aeg on NIS2 artikli 23 kohaselt vastavalt kas 24 või 72 tundi. Kuigi rikkumistest teavitamine käib ettepaneku kohaselt ühtse teavituspunkti kaudu, on andmetöötlejal kaks erinevat tähtaega rikkumisest teavitamiseks. See võib tekitada õiguslikku ebaselgust, kuivõrd ettepaneku kohaselt on andmetöötlejal tarvis esitada rikkumise kohta teade ühtse teavituspunkti kaudu korraga kõikidele järelevalveasutustele vaid ühel korral.

Veelgi enam, NIS2 rikkumistel ei ole teavitamiskünnist kõrge ohutasemega rikkumistel, seega tuleb andmetöötlejal küberrikkumiste korral rikkumisteade teha isegi siis, kui seda teadet ei esitata IKÜMi järelevalveasutusele. Sellest tulenevalt ei ole AKI-le arusaadav seadusandja eesmärk lõdvendada rikkumisteadete esitamise kohustuse piire, kui seda tehakse vaid andmekaitsega seotud rikkumiste puhul.

Eeltoodust hoolimata pooldab AKI initsiatiivi luua ühtne teavituspunkt, mille kaudu on võimalik andmetöötlejal esitada rikkumisteateid korraga mitmetele järelevalveasutustele, mis omakorda toetab digitaalse omnibusi eesmärki vähendada andmetöötlejate halduskoormust. AKI märgib, et ühtse teavituspunkti ülesehituse tehniline ja organisatoorne pool vajab täpsustamist.

8.1. Isikuandmetega seotud rikkumistest teavitamine muude õigusaktide alusel

Ettepanek näeb ette, et direktiivi 2002/58/EÜ artikkel 4 tuleks kehtetuks tunnistada. Selle põhjenduseks tuuakse, et isikuandmete töötlemise turvalisuse osas, vastavalt e-privaatsuse direktiivi artikli 4 lõigetele 1 ja 1a, ning isikuandmete rikkumistest teatamise osas, vastavalt artikli 4 lõigetele 3–5, on IKÜM-is juba sätestatud põhjalikud ja ajakohased reeglid. Seetõttu peaksid need tingimused kehtima nii elektrooniliste sideteenuste osutajate kui ka sidevõrkude pakkujate suhtes, tagades ühtsed nõuded vastutavatele ja volitatud töötlejatele.

Ühtlustamise põhimõttega võib AKI põhimõtteliselt nõustuda, kuid samas märgib, et kehtib ka Komisjoni määrus 611/2013, mille kohaselt on üldkasutatava elektroonilise sideteenuse osutajal kohustus teatada isikuandmetega seotud rikkumistest. Määruse kohaselt tuleb rikkumisest teavitada andmekaitse järelevalveasutust hiljemalt 24 tunni jooksul pärast rikkumise tuvastamist. Ettepanekus ei ole selgitatud, kuidas Komisjoni määrus 611/2013 edaspidi ettepaneku muudatustega kooskõlas oleks, ühtlasi ei ole ettepanekus viidet selle määruse tühistamisele.

9. Andmekaitsealane mõjuhinnang
(IKÜM artikkel 35)

Seoses andmekaitsealase mõjuhinnangu tegemise kohustusega muudab ja täiendab digitaalse omnibussi ettepanek IKÜM artikli 35 lõikeid 4-6. Viidatud lõigete kohaselt koostab ja edastab EAKN Komisjonile ettepaneku loetelu kohta töötlemistoimingute liikidest mille suhtes kohaldatakse või ei kohaldata andmekaitsealase mõjuhinnangu nõuet. Lisaks koostab ja edastab EAKN Komisjonile ettepaneku mõjuhinnangu tegemise ühise vormi ja metoodika kohta.

AKI toetab ettepanekut töötada välja ühtsed nõuded, millal on mõjuhinnangu tegemine kohustuslik ning millal ei ole, sest see teenib nende ettevõtjate, kes siseturul tegutsevad, halduskoormuse vähendamist. Samuti toetab AKI ettepaneku osa, et EAKNile antakse ülesandeks välja töötada andmekaitsealase mõjuhinnangu koostamiseks ühtne vorm ja metoodika.

Järelevalveasutuste ja EAKNi autonoomsuse säilitamiseks peab AKI siiski vajalikuks jätta nõuete ja vormide koostamise volitused vaid EAKNile. Andes nõuete ja vormi koostamise muutmise õiguse ja rakendusaktina vastuvõtmise õiguse Komisjonile, on küsimuse all esmalt EAKNi kui organi sõltumatus ning teisalt ei ole kindel, kas rakendusaktiga vastu võetu väljendab EAKNi soovitusi ja järelevalveasutuste tegelikke praktikaid. Seetõttu tuleks teha artiklis 35 täpsustus, et EAKNi väljatöötatud nõuded ja vormid tuleb Komisjonil rakendusaktina vastu võtta muutmata kujul.

10. Pseudonüümimine
(IKÜM artikkel 41a)

Ettepanek lisab IKÜMi uue artikli 41a, mille kohaselt võib Komisjon vastu võtta rakendusakte, et täpsustada vahendeid ja kriteeriume, mille alusel teha kindlaks, kas pseudonüümimise teel saadud andmed ei ole enam teatud üksuste jaoks isikuandmed.

Selline lähenemine annab Komisjonile rakendusaktide kaudu justkui võimaluse muuta IKÜMi kohaldamisala isikuandmete tõlgendamisele, mis võib omakorda tekitada õiguslikku ebakindlust. Õigusaktide tõlgendamise õigus peaks jääma järelevalveasutustele, Euroopa Kohtule ning EAKNile. AKI ei toeta võimalust, et Komisjon võiks läbi rakendusaktide sisuliselt muuta olulisi põhiõigustega seotud definitsioon.

11. Terminaliseadmed ja nõusolek
(IKÜM artikkel 88a)

AKI tervitab Komisjoni eesmärki lihtsustada andmesubjektide digitaalset kogemust ja lahendada laialt levinud „*cookie fatigue*", mis on tingitud e-privaatsuse direktiivi praegustest tõlgendustest. Erandite kehtestamine auditooriumi mõõtmiseks ja kohustusliku „ühe klõpsuga" nõusoleku kasutuselevõtt on positiivsed sammud kasutajasõbralikuma interneti suunas.

Ettepanek loob õigusliku lahknevuse. Seadmes olevaid isikuandmeid reguleerib edaspidi IKÜM artikkel 88a, kuid ettepaneku põhjenduspunkt 47 selgitab, et isikustamata andmeid reguleerib endiselt e-privaatsuse direktiivi artikkel 5 lõige 3. Praktikas tekitab see küsimuse, kuidas andmetöötleja, näiteks veebipood, saab kindlaks teha, kas lõppseade kuulub füüsilisele isikule ning kas kogutud teave toob kaasa isikuandmete töötlemise.

E-privaatsuse direktiivi artikkel 5 lõige 3 nõuab selget ja arusaadavat teavet andmete töötlemise eesmärgi kohta. IKÜM artikli 88a lõike 1 sõnastuse kohaselt on isikuandmete salvestamine füüsilise isiku lõppseadmesse või juba salvestatud isikuandmetele juurdepääsu saamine lubatud ainult juhul, kui see isik on andnud oma nõusoleku vastavalt käesolevale määrusele. Seega e-privaatsuse direktiivile sarnast teabe esitamise kohustust lisatav artikkel 88a otsesõnu ei näe ette. Tekib küsimus, kas eeldatakse, et kuna kohalduvad IKÜMi üldised nõusoleku reeglid, ei ole eraldi kohustust teavet selgelt esitada.

Ettepanekuga soovitakse lisada artikli 88a lõige 3, mille kohaselt on isikuandmete salvestamine füüsilise isiku lõppseadmesse või juba salvestatud isikuandmetele juurdepääsu saamine ilma nõusolekuta ja hilisem töötlemine seaduslik ulatuses, mis on vajalik punktide a-d eesmärkidel. AKI möönab, et punktid a-b on üle võetud e-privaatsuse direktiivist, punktide c-d puhul tutvustab Komisjon aga täiendavaid erandeid.

Nõusolek IKÜMi mõistes tähendab vabatahtlikku tahteavaldust. Lõike 3 tekst viitab olukordadele, kus nõusoleku andmine ei ole vajalik. Samas jääb selgusetuks, kas seadusandja on tahtnud selles lõikes kehtestada kohustusliku nõusoleku olukorra või hoopis viidata artikli 6 lõike 1 punkti c aluse tekkimisele. Need kaks õiguslikku alust kannavad erinevaid tagajärgi, näiteks nõusoleku

puhul peab andmesubjektil alati olema võimalus seda tagasi võtta. Kui seadusandja on tahtnud lõikest 3 teha artikli 6 lõike 1 punkt c kohase õigusliku aluse, tekitab viide nõusoleku puudumisele segadust. AKI rõhutab, et artikli 6 lõike 1 nimetatud õiguslikel alustel puudub hierarhia ning nõusolek ei ole teiste aluste seas ülim.

Artikli 88a lõike 3 rakendamisel on vajalik täpsustada, millistes olukordades punktid c ja d, kohalduvad. Näiteks punkt c lubab andmetöötlejal koondada teavet veebiteenuse kasutamise kohta ainult omaenda tarbeks. Põhimõtteliselt on tegemist statistikaga, mis näitab veebilehe pidajale, näiteks kui palju kliente, mis vanuses, mis soost ning mis riigist tema veebilehel käis. AKI nõustub, et praktikas ei saa veebilehe pidaja sellisele teabele ligi, mis võimaldaks isikuid tuvastada, mistõttu on erandi tegemine õigustatud.

Oluline on selgitada, et kõik tegevused, mis väljenduvad väljaspool „koondamise“ mõistet, peaksid toimuma vaid täiendava õigusliku aluse olemasolul. Samuti tuleb selgitada, kui kaugele võib töötlemine ulatuda eesmärkide saavutamiseks, ilma et see ületaks artiklis sätestatud lubatu piire.

AKI leiab, et ettepanekus IKÜM artikli 88a lõike 3 punktis d sisalduv ulatuslik turvalisuse erand õigustab pealetükkivaid skaneerimistehnikaid ilma vajalike proportsionaalsuse kontrollideta. See kaotab IKÜMist tuleneva tasakaalustamistesti ning muudab vastutava töötleja juurdepääsu terminaliseadmetele vaikimisi lubatavaks. Kehtiva õiguse kohaselt eeldab selline juurdepääs õigustatud huvi olemasolu ning huvide kaalumist andmesubjekti õigustega. Kavandatav sõnastus annab vastutavatele töötlejatele sisuliselt piiramatu tegevusruumi, ilma et sekkumise ulatust ja intensiivsust tuleks hinnata.

Ilma sõnaselge proportsionaalsuse ja rangelt vajaliku ulatuse nõudeta võib erand õigustada skaneerimise praktikaid, sealhulgas kogu kõvaketta skaneerimist, krüpteeritud sõnumite analüüsimist enne edastamist ning kohalike failide kaugotsingut, mis kujutavad endast sügavat sekkumist eraellu.

Täpsustamist vajab ka artikli 88a lõige 4, mis reguleerib nõusolekut. Selle asemel, et suunata fookus konkreetsete kasutajaliidese elementide sätestamisele, tuleks veenduda, et nõusolekuga seotu oleks kooskõlas artikli 7 lõikega 4. Sellest tulenevalt tuleb pidada ettepanekus välja pakutud teksti kohmakaks, sest “nõusolekutaotlusest keeldumise” (in k *to refuse requests for consent*) asemel võiks olla kirjas, et nõusoleku andmine ning tagasi võtmine peaks olema võimalik ühe klikiga.

AKI on arvamusel, et IKÜM artikli 88a lisamine on vajalik samm, et reguleerida isikuandmete töötlemist lõppseadmetes. Samas vajab artikli sõnastus täpsustamist, et tagada õigusselgus ja andmesubjekti õiguste tegelik kaitse.

13. Andmesubjekti automatiseeritud ja masinloetavad valikud seoses isikuandmete töötlemisega füüsilise isiku lõppseadmes
(IKÜM artikkel 88b)

Digitaalse omnibussi IKÜM artikkel 88b koosmõjus artikliga 88a loob raamistiku, mille kaudu andmesubjekt saab väljendada oma nõusolekut või keelduda sellest automatiseeritud ja masinloetava vahendi kaudu, näiteks brauseri tasandil. See tähendab, et andmetöötlejad peavad austama andmesubjekti antud valikuid ning Euroopa Komisjoni ülesanne on tagada standardite loomine masinloetavate signaalide tõlgendamiseks.

Küsimusi tekitab ka nõusoleku andmise viis, mis on sätestatud artikli 88b lõigetes 1 ja 2. Andes nõusolek brauseri tasandil on tegemist tulevikku vaatava nõusolekuga. Kui andmesubjekt annab

nõusoleku kõikide võimalike küpsiste paigaldamiseks, ei tea ta nõusoleku andmise hetkel, milliseid küpsiseid milline veebileht kasutada võib. Selliselt antud nõusolekut ei saa pidada teadlikuks. Teisalt tekitab küsimusi ka nõusoleku kehtimise aeg. Kui artikli 88a lõike 4 punkti c kohaselt on nõusoleku andmisest keeldutud, küsitakse nõusolekut kuue kuu pärast uuesti. Sarnast lähenemist võiks kasutada ka nõusoleku andmise korral, kus iga kuue kuu tagant on andmesubjektil võimalus oma küpsiste sätted üle vaadata ja vajadusel korrigeerida. Põhjenduseks ei saa olla asjaolu, et andmesubjektil on võimalus oma nõusolek igal ajal tagasi võtta, sest nõusolekut anda võib samuti igal ajal ka kuuekuulise teavituseta.

Meediateenusepakkujate erand artikli 88b lõikes 3 võib viia olukorrani, kus automatiseeritud nõusolek ei kehti kõigi veebiteenuste puhul, vähendades standardiseerimise ja kasutaja kontrolli tegelikku ulatust. Ühtlasi on seadusandja meediateenusepakkujate puhul ilmselt soovinud teha sarnast erandit nagu kehtivas IKÜMis on tehtud artikkel 85 lõikes 2 (andmetöötlus ajakirjanduslikel eesmärkidel). Kui seadusandja tahe selline oli, tuleks sõnastus kooskõlastada artikli 85 lõikega 2, kuivõrd meedia ja ajakirjandus ei ole sünonüümid.

12. Tehisintellekti arendamine ja juurutamine
(IKÜM artikkel 88c)

Digitaalse omnibussi ettepanek lisab IKÜMi artikli 88c. Artikli 88c kohaselt kui isikuandmete töötlemine on vajalik vastutava töötleja huvides tehisintellekti määruse artikli 3 punktis 1 määratletud tehisintellekti süsteemi või tehisintellekti mudeli arendamise ja käitamise kontekstis, võib sellist töötlemist teostada õigustatud huvi alusel IKÜM artikli 6 lõike 1 punkti f tähenduses, kui see on asjakohane, välja arvatud juhul, kui muud liidu või siseriiklikud õigusaktid nõuavad sõnaselgelt nõusolekut ja kui andmesubjekti huvid või põhiõigused ja -vabadused, mis nõuavad isikuandmete kaitset, on selliste huvide suhtes ülimuslikud, eelkõige juhul, kui andmesubjekt on laps. Sellise töötlemise suhtes kohaldatakse asjakohaseid korralduslikke, tehnilisi meetmeid ja kaitsemeetmeid andmesubjekti õiguste ja vabaduste jaoks, näiteks andmete minimeerimise põhimõtte järgimise tagamiseks allikate valiku etapis ning tehisintellekti või -süsteemi või -mudeli koolitamisel ja testimisel, et kaitsta tehisintellekti süsteemis või -mudelis säilitatud jääkandmete avalikustamata jätmise eest, et tagada andmesubjektidele suurem läbipaistvus ja anda andmesubjektidele tingimusteta õigus oma isikuandmete töötlemisele vastuväiteid esitada.

Euroopa Kohtu praegune kohtupraktika (nt C-131/12 Google Spain) sätestab, et pelgalt ärihuvi ei ole automaatselt põhiõigustest ülimuslik ning „vajalikkust“ tuleb tõlgendada kitsalt. Artikkel 88c püüab sellest mööda minna, kehtestades eelduse, et tehisintellekti arendamine on artikli 6 lõike 1 punkti f kohaselt õigustatud huvi alusel teostatav.

Ka olemasoleva regulatsiooni alusel ei ole välistatud, et tehisintellekti arendamiseks isikuandmete töötlemine õigustatud huvi alusel võib teatud juhtudel olla õiguspärane, võttes arvesse isikuandmete töötlemise põhimõtteid. Selline nn õigustatud huvi eriregulatsioon ühe tehnoloogialiigi jaoks jätab petliku mulje justkui lihtsustatud korras on õigustatud huvi juba ette õiguspärane ning välistab EAKNi poolt õigustatud huvi aluse puhul suunistes toodud kolmeastmelise huvi hindamise, sh andmetöötleja ja andmesubjekti huvide tasakaalustamise, mille nõue tuleneb IKÜM art 6 lg 1 p f enda sõnastusest. AKI pöörab tähelepanu ettepaneku sõnastusele, mis kasutab väljendeid „vajadusel” ja „võib taotleda”. Selliste väljendite kasutamine suure riskiga andmete töötlemiseks ei paku vajalikku õiguskindlust. Vastupidiselt jätab see seaduslikkuse kindlaksmääramise sisuliselt vastutava töötleja subjektiivse hinnangu hooleks, mida järelevalveasutustel on ilma selgete seadusjärgsete kriteeriumideta raske vaidlustada.

Tekst hõlmab lisaks tehisintellekti treenimisele ka tehisintellekti opereerimist. See viib

ebaloogilise tulemuseni: standardse SQL-andmebaasi kaudu andmeid töötlev vastutav töötleja peab oma õiguslikku alust rangelt põhjendama, samas kui vastutav töötleja, kes töötleb täpselt samu andmeid samal eesmärgil tehisintellekti süsteemi kaudu, saab viidata artikli 88c õigustatud huvi eeldusele.

Ettepanek keskendub treenimisele ja opereerimisele kuid ignoreerib tehisintellekti väljundit. Tehisintellekti mudelid tekitavad sageli „hallutsinatsioone“ ehk valeandmeid (nt isiku valesüüdistused kuriteos). Vastutavad töötlejad väidavad praegu parandamise või kustutamise taotluste esitamisel, et nende taotluste lahendamine on tehniliselt võimatu. Artikkel 88c tugevdab seda seisukohta, muutes andmesubjektide õiguskaitsevahendid praktiliselt olematuks. Parandamise ja kustutamise taotluse esitamine on aga vaid hüpoteetiline võimalus. Ettepaneku põhjenduspunktis 31 viidatakse andmesubjekti mõistlikele ootustele, läbipaistvusele ja vastuväite esitamise võimalusele. Praktikas ei saa andmesubjekt teadagi, et tema kraabitud isikuandmeid kasutatakse tehisintellekti treenimiseks ning läbipaistvuse tagamine on problemaatiline. Samuti on andmesubjektil võimatu esitada andmete töötlemisele vastuväidet, kuna ta isegi ei tea oma andmete töötlemisest.

13. Põhiõiguste hartaga tagatud õiguste seos järelevalveasutuste tööga

Ettepanek vähendab sellisel kujul liikmesriikide järelevalveasutuste tegelikku võimalust kohaldada isikuandmete kaitse üldmäärust, mis on vastuolus Euroopa Liidu põhiõiguste harta artiklis 47 sätestatud tõhusa õiguskaitse põhimõttega. Ettepanekus sisalduvad normid on võrreldes kehtiva IKÜMiga oluliselt subjektiivsemad ja tehniliselt keerukamad, muutes nende ühtse ja järjepideva jõustamise praktikas oluliselt raskemaks ning ressursimahukamaks olukorras, kus ressursse juurde leida, eriti väikestel riikidel, on keeruline.

Selline regulatiivne nihe suurendab riski, et andmesubjekti õiguste kaitse muutub ebajärjekindlaks ning järelevalvepraktika liikmesriikide vahel killustub. Selle tulemusel võib andmesubjektil rikkumise korral puududa reaalne ja tõhus võimalus oma õigusi maksma panna, isegi kui need on formaalselt õigusaktides sätestatud. Euroopa Kohtu praktika, sealhulgas kohtuasi C-333/22, rõhutab, et põhiõiguste kaitse peab olema praktiline ja tõhus, mitte üksnes teoreetiline või näiline.

Selline olukord on problemaatiline ka harta artikli 52 lõike 1 tähenduses, kuna õiguste sisuline nõrgenemine jõustamise tasandil kujutab endast kaudset, kuid tegelikku põhiõiguste piiramist. Kui normatiivne raamistik ei taga tõhusat järelevalvet ega reaalselt toimivat õiguskaitset, kahjustab see põhiõiguste olemust ning ei ole kooskõlas proportsionaalsuse ega õiguskindluse põhimõtetega.

14. Teiste õigusaktidega suhestumine

Digital Omnibusi ettepaneku põhjenduspunktis 44 on välja toodud, et määrus (EL) 2018/1725 (EUDPR) ja direktiiv (EL) 2016/680 (LED) tuleks viia kooskõlla käesoleva määrusega määrusesse (EL) 2016/679 tehtud muudatustega. Digital Omnibusi ettepanekute valguses tähendab LEDi ning sellele tuginevate siseriiklike õigusaktide kooskõlla viimine IKÜM-iga seda, et Eesti õiguses tuleb vajadusel täiendada või täpsustada juba kehtivaid LED-i rakendusakte, st isikuandmete kaitse seadust.

EUDPR muudatused on ettepanekusse sisse toodud (ettepaneku lk 85 jj), kuid LED direktiivi muudatusi ei ole. Õiguskaitseasutuste jaoks muutub olukord keeruliseks, kui nad peavad erinevates olukordades juhinduma erinevatest sätetest (mis puudutab näiteks isikuandmete mõistet või rikkumisest teavitamise tähtaegu).

ANDMEMÄÄRUS

15. Andmete väljastamisest keeldumine
(Andmemäärus artikkel 4 lõige 8)

Kehtiva andmemääruse artikkel 4 lõike 8 kohaselt on andmevaldajal, kes on ühtlasi ärisaladuse omaja, võimalik andmetele juurdepääsu taotlus rahuldamata jätta, kui on väga tõenäoline, et ärisaladuse avalikustamine põhjustab talle suurt majanduslikku kahju. Digitaalse omnibussi ettepaneku kohaselt lisatakse ärisaladuste kaitsmiseks juurde lisaalus andmete väljastamisest keeldumiseks. Nimelt on andmevaldajal võimalik andmete väljastamisest keelduda, kui ta tõendab, et on olemas suur risk, et ärisaladus võib jõuda kolmandate riikidega seotud üksusteni, kus ärisaladuse kaitse ei ole piisav.

Praktikas võib tekkida olukord, kus ärisaladust puudutavad andmed sisaldavad ka isikuandmeid. IKÜM artikli 15 alusel on andmesubjektil õigus isikuandmetega tutvuda. Andmesubjekti õigust andmetega tutvuda saab piirata mh IKÜM artikli 23 kohaselt liidu õiguses sätestatud seadusandliku meetmega. Kehtiva andmemääruse põhjenduspunkti 31 kohaselt ei tohiks määruses sätestatud erandid andmetele juurdepääsu õigusest mingil juhul piirata IKÜM-i kohast andmesubjektide juurdepääsuõigust.

Ettepanekus ja põhjenduspunktides ei ole eraldi välja toodud, kuidas ärisaladuse kaitsega seotud lisaalus andmete väljastamisest keeldumiseks IKÜM-st tuleneva andmesubjekti juurdepääsuõigusega suhestub. Kehtiva määruse põhjenduspunktidele tuginedes ei ole siiski tegemist eraldiseisva alusega, mis lubaks andmevaldajal isikuandmete väljastamisest keelduda. Seega ei peaks andmete väljastamisest keeldumiseks loodav lisaalus isikuandmete väljastamisest keeldumisele kohalduma ja andmevaldaja peab isikuandmete väljastamisest keeldumisel tuginema IKÜM-st tulenevale alusele nagu ka praegu kehtiv regulatsioon ette näeb.

16. Erasektorilt üldises hädaolukorras andmete taotlemine
(Andmemäärus artikkel 14)

Kehtiva andmemääruse artikli 14 kohaselt on andmevaldajatel kohustus teha avalikule sektorile andmed kättesaadavaks erakorralise vajaduse tõttu. Erakorralist vajadust ei ole määruses otseselt defineeritud, kuid artiklis 15 on täpsustatud, et erakorralise vajadusena tuleks käsitleda näiteks olukorda, kus andmed on vajalikud üldisele hädaolukorrale reageerimiseks. Üldine hädaolukord on defineeritud kehtiva andmemääruse artikli 2 punktis 29, mille kohaselt on üldine hädaolukord ajaliselt piiratud erakorraline olukord (nagu rahvatervise, loodusõnnetusest tingitud hädaolukord või inimtegevusest tingitud suurõnnetus, sh ulatuslik küberturvalisuse intsident), mis mõjutab negatiivselt liidu, liikmesriigi või selle osa elanikkonda ning millega kaasneb oht, et see võib tõsiselt ja püsivalt kahjustada elamistingimusi või majanduslikku või finantsstabiilsust või oluliselt ja vahetult halvendada majanduslikke varasid liidus või asjaomases liikmesriigis, ja mis tehakse kindlaks või kuulutatakse ametlikult välja vastavalt liidu või riigisisese õiguse kohastele asjakohastele menetlustele.

Kehtiva andmemääruse artikli 15 lõike 1 punkti b alusel ja põhjenduspunkti 72 kohaselt ei saa avalik sektor taotleda isikuandmete väljastamist, kui avaliku sektori taotlused põhinevad erakorralisel vajadusel, mis ei ole seotud üldise hädaolukorraga.

Digitaalse omnibusi ettepaneku kohaselt lisatakse määrusesse artikkel 15a, millega eemaldatakse andmevaldajate kohustus väljastada andmeid avalikule sektorile erakorralise vajaduse tõttu ja andmete väljastamise kohustus kehtib üksnes üldises hädaolukorras või vahetult pärast üldist hädaolukorda olukorra leevendamiseks või taastumise toetamiseks. Ettepaneku kohaselt on

avaliku sektori asutusel õigus esitada andmevaldajale taotlus eelkõige isikustamata andmete väljastamiseks. Andmemäärusele lisatava artikli 15a lõike 2 kohaselt peaks isikuandmete väljastamine toimuma olukorras, kus isikustamata andmed ei ole üldise hädaolukorraga tegelemiseks piisavad ja kus võimalik, pseudonüümitakse isikuandmed enne väljastamist.

Tegemist on kehtiva andmemääruse artikkel 17 lõike 2 punkti e (ettepaneku kohaselt eemaldatakse säte andmemäärusest) sarnase sättega, kuid märgata on olulist erinevust. Kehtiva sätte kohaselt võib isikuandmeid avalikule sektorile väljastada vaid pseudonüümitud kujul, kuid ettepanekus toodud artikkel 15a lõike 2 kohaselt on pseudonüümimine võimalus, mitte kohustus.

Kuigi ettepanekuga eemaldatakse määrusest erakorralise vajaduse tõttu andmete väljastamise alus, eristab ettepanek siiski üldist hädaolukorda ja olukorda, kui avaliku sektori asutus taotleb andmeid üldise hädaolukorra leevendamiseks või taastumise toetamiseks (in k t*he recovery from a public emergency*). Viimase korral on lubatud väljastada ainult isikustamata andmeid (ettepanekuga lisatav art 15a lõige 3). Oluline on, et hädaolukorraga seotud piiride tõmbamine oleks liidus ühtne ning jälgiks sama praktikat kõikides liikmesriikides.

17. Andmehalduse määruse lisamine andmemäärusesse
(Andmemäärus peatükk VIIa)

Kehtiva andmehalduse määruse artikkel 11 lõike 1 järgi pidid kõik andmevahendusteenuse osutajad, kes kavatsevad osutada artiklis 10 osutatud andmevahendusteenuseid, esitama teatise andmevahenduse pädevale asutusele.

Digitaalse omnibusi ettepanekuga andmemäärusesse lisatav peatükk VIIa jätab lisatavas artikli 32 lõikes 2 edaspidi andmevahendusteenuse osutajatele teatise esitamise vabatahtlikuks. Digitaalse omnibusi ettepaneku põhjenduspunktis 8 on selgitatud, et turu praeguses arenguetapis näib olevat piisav vabatahtlik kord, mis võimaldab neutraalsetel osalejatel teistest osalejatest eristada. Jätkusuutlike ärimudelite võimaldamiseks tuleks korda muuta vähem rangeks, kaotades andmevahendusteenuste ja muude lisaväärtusteenuste õigusliku eraldamise nõude, mida teenusel peaks olema lubatud pakkuda, asendades selle funktsioonipõhise eraldamisega, säilitades samal ajal teatavad kaitsemeetmed.

Kavandatavat VIIa peatükki soovitakse kohaldada isikuandmete ja isikustamata andmete suhtes. Järelevalveasutused on valmistunud, et olla valmis andmevahendusteenuse osutajate teatiste vastuvõtmiseks. Kehtiv raamistik oleks loonud järelevalveasutustele võimaluse olla sellistest teenuseosutajatest ja nende tegevusest teadlik. Andmevahendusteenuse osutajatele nende tegevusest teatamise vabatahtlikuks jätmine võib luua olukorra, kus teenuseosutajate üle puudub igasugune teadmine ja kontroll. Kui teatiste esitamine jääb vabatahtlikuks, tekib risk, et järelevalveasutustel puudub ülevaade teenuseosutajatest, kes vahendavad isikuandmeid. See omakorda vähendab võimalust hinnata, kas andmete töötlemine toimub kooskõlas IKÜMi nõuetega, näiteks seoses töötlemise õigusliku aluse, turvameetmete ja andmesubjektide õiguste tagamisega. Selline olukord võib suurendada ohtu, et andmeid vahendatakse piisava kontrollita, mis võib viia ebapiisava turvalisuse või andmesubjektide õiguste rikkumiseni.

Isikuandmete kaitse kõrge taseme tagamise küsitavustele viitab ettepaneku andmemääruse artikli 32c punkt c, mille kohaselt võivad andmevahendusteenuse osutajad pakkuda lisateenuseid, näiteks andmete säilitamine, hooldamine, teisendamine, krüpteerimine, anonüümimine ja pseudonüümimine. Punktis on nimetatud, et seda võib teha ainult andmevaldaja või andmesubjekti selgesõnalisel taotlusel või nõusolekul.

Võib eeldada, et planeeritavas muudatuses peetakse silmas, et lisateenuste osutamine on lubatav kas andmevaldaja selgesõnalisel taotlusel või andmesubjekti nõusolekul. Konkreetne sõnastus aga

võimaldab tõlgendada seda ka viisil, et sobivaks võib osutuda andmesubjekti selgesõnaline taotlus. Isikuandmete puhul on vaja töötlemiseks IKÜM artikkel 6 lõikest 1 tulenevat õiguslikku alust. Seega ei loo muudatus selgesõnalist ega ühtselt tõlgendatavat regulatsiooni. Andmemääruse artikli 32c punkti c tasuks võrrelda ettepanekus andmemääruse artikkel 32f lõikega 3, mille sõnastuses on andmesubjekti nõusolekut ja andmevaldaja luba selgelt eristatud.

18. Avaandmetega seotud põhimõtete muudatused

(Andmemäärus peatükk VIIc)

Andmemääruse muudatustega soovitakse ühildada avaandmete ning piiranguga avaliku sektori andmete taaskasutamise regulatsioonid. Käesoleval hetkel on avaandmete direktiiv ning andmehalduse määrus oma olemuselt erinevad osas, mis puudutab regulatsioonide piire, kuivõrd kui avaandmete direktiiv kohaldub nii andmetele kui ka dokumenditele, siis kehtiv andmemäärus piiranguga andmete puhul kohaldub vaid andmetele.

Andmemääruse ettepaneku kohaselt on andmemääruse eesmärk ühildada avaandmete direktiiv 2019/1024 ja andmehalduse määrus 2022/868. AKI nõustub, et ühtne õigusakt on positiivne suund ühtlustamaks andmete taaskasutamise reegleid ja definitsioone. Käesoleval hetkel on avaandmete direktiivi erinevalt ülevõtmine toonud kaasa piiranguta andmete taaskasutamise piiride erinevad tõlgendused.

Praktikas tekitab probleeme, kui avaldatud isikuandmeid taasavalikustatakse mujal, näiteks infoportaalides, ja neid kombineeritakse veel omakorda muude avalikest allikatest leitud isikuandmetega. Ettepaneku põhjenduspunkti 24 kohaselt ei tähenda isikuandmete sisaldus teabes seda, et neid ei tohi anda taaskasutamiseks, vaid nende kasutamist tuleb vajadusel piirata ja anda kasutamiseks kaitstud andmetena. Seega, kui isikuandmed on osa avalikust teabest, peab teabevaldaja enne nende taaskasutamiseks andmist hindama, kas avaldamine võib kahjustada andmesubjekti õigusi ja huve ning vajadusel anda see teave taaskasutamiseks kaitsemeetmetega. Ettepanekus on andmemääruse artikli 17 lõike 1 punktis g täpsustatud, et isikuandmete taaskasutamiseks andmisel peab enne andmete kasutamiseks andmist võtma kasutusele kaitsemeetmeid. Selline lähenemine näitab, et isikuandmeid ei tohi avaandmetena taaskasutamiseks kaitsemeetmeteta anda.

Ettepaneku põhjenduspunktis 7 on selgitatud, et andmemäärus ei loo õiguslikku alust isikuandmete töötlemiseks. Selline käsitlus näitab, et isikuandmete töötlemise puhul peab lähtuma IKÜM-st. See aitab tõsta teadlikkust, et isikuandmete taaskasutamine (ka juba avalikustatud isikuandmete) eeldab IKÜM artiklist 6 tuleneva õigusliku aluse olemasolu. Seda kinnitab ka ettepaneku kavandatav andmemääruse artikkel 32w lg 2 punkt c.

Ettepanekus andmemääruse artikli 32w lõiked 3 ja 4 sätestavad konkreetsed viisid, kuidas isikuandmeid saab taaskasutamiseks anda. Eelkõige näevad sätted ette võimaluse isikuandmete anonüümimiseks või muul viisil ettevalmistamiseks; samuti võib kehtestada kohustuse töödelda andmeid üksnes turvalises töötlemiskeskkonnas või füüsilises ruumis. Lisaks võib taaskasutajale määrata konfidentsiaalsuskohustuse. Oluline on, et teabevaldajal säilib õigus kontrollida taaskasutaja teostatud andmete või dokumentide töötlemise protsessi, vahendeid ja tulemusi, et tagada andmete või dokumentide kaitse terviklikkus. Ettepanekus andmemääruse artikli 32w lõige 5 sätestab selgelt, et juhul kui eelnevate tingimuste kohaselt ei ole võimalik isikuandmeid sisaldavaid andmeid avaandmeteks anda, on nende taaskasutamine lubatud üksnes andmesubjekti nõusolekul. AKI hinnangul on tegemist tasakaalustatud ja asjakohase, aga eelkõige selgust loova lahendusega.

Ettepanekus andmemääruse artikli 32x lõike 1 kohaselt on taaskasutaja kohustatud teavitama

avaliku sektori asutust kavatsusest edastada teatavat liiki kaitstud andmeid, mis ei ole isikuandmed, kolmandasse riiki, ning teavitama edastamise eesmärgist andmete taaskasutamise taotlemise ajal. Küsitav on, mida tuleb selles kontekstis edastamisena käsitada, näiteks kas see hõlmab ka andmete üleslaadimist teenustesse, kus andmed liiguvad, näiteks pilveteenused või analüütikakeskkonnad, mis paiknevad või mille alltöövõtjad paiknevad kolmandates riikides. Ettepanek eeldab teavitamist taotluse esitamise ajal, kuid praktikas puudub avaliku sektori asutustel ülevaade, kes avaandmete portaalist andmeid alla laadib või mida taaskasutajad teabenõude tulemusena saadud andmetega hiljem teevad. Seetõttu võib teavitamiskohustus tunduda taaskasutajate vaatest bürokraatlik ja raskesti rakendatav, teisalt puudub ka teavitamise üle järelevalvevõimalus.

AKI on arvamusel, et avaandmete regulatsioon ettepanekus on selgem kui kehtiv avaandmete direktiiv ning kaitsemeetmete rakendamise kohustus tagab nii isikustatud kui ka isikustamata andmete taaskasutamise turvalisuse ja usalduse. Avaandmete avaldamisel ja taaskasutamisel on oluline leida tasakaal avatud juurdepääsu ja isikuandmete kaitse vahel, seda eelkõige juhul, kui avaandmed võivad sisaldada isikuandmeid.

19. Isikuandmete eriliikide töötlemine kallutatuse tuvastamiseks ja leevendamiseks
(Tehisintellekti määruse artikkel 4a)

Tehisintellekti omnibusi ettepanekuga lisatakse tehisintellekti määrusesse artikli 4a kujul õiguslik alus isikuandmete eriliikide töötlemiseks kõigi tehisintellektisüsteemide ja -mudelite pakkujate ja juurutajate poolt, kui see on vajalik kallutatuse avastamiseks ja kõrvaldamiseks, tingimusel et kohaldatakse asjakohaseid kaitsemeetmeid. Tehisintellekti omnibusi põhjenduspunkti 6 kohaselt kehtestatakse see alus kooskõlas IKÜM artikli 9 lõike 2 punktiga g.

Kallutatuse tuvastamine ja selle korrigeerimine on selgelt iga tehisintellektimudeli või -süsteemi pakkuja ja juurutaja selge huvi. Seega võib arvata, tehisintellektimudelite ja -süsteemide pakkujad ja juurutajad peavad alati vajalikuks eriliiki isikuandmete töötlemist ja tegelikkuses ei teki ilmselt olukorda, kus vajalikkuse puudumist jaatada saaks. Nii luuakse ka tehisintellekti määruse artikliga 4a vaikimisi eeldus, et eriliiki isikuandmete töötlemine on alati aktsepteeritav. Samas arvestades IKÜM artikkel 9 lõiget 2 ei tohiks eriliiki isikuandmete töötlemist käsitleda kui vaikimisi lubatud tegevust. Vastupidiselt peab see olema rangelt piiratud, läbipaistvalt põhjendatud ja tehniliselt kontrollitud, et vältida nii õiguslikke rikkumisi kui ka ühiskondlikku kahju.

Küsitavusi tekitab selle sätte loomisel ka õiguslike alustega seonduv. Digitaalse omnibusi ettepaneku kohaselt soovitakse IKÜMi lisada artikkel 88c, kehtestades sellega eelduse, et tehisintellekti arendamine on artikli 6 lõike 1 punkti f kohaselt õigustatud huvi alusel teostatav. Teisalt, mis puudutab isikuandmete eriliikide töötlemist kallutatuse tuvastamiseks ja leevendamiseks, siis tehisintellekti omnibusi ettepanekus tehisintellekti määruse artikkel 4a soovitakse kehtestada IKÜM artikkel 9 lõike 2 punkti g alusel. Viimane neist ütleb, et eriliiki isikuandmete töötlemine on lubatud, kui see on vajalik olulise avaliku huviga seotud põhjustel liidu või liikmesriigi õiguse alusel ning on proportsionaalne saavutatava eesmärgiga, austab isikuandmete kaitse õiguse olemust ja tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks. Nii ei ole kallutatuse tuvastamine ja selle leevendamine enam tehisintellektimudeli või -süsteemi pakkuja või juurutaja huvi, vaid avalikkuse huvi. See viitab mõningasele ebakõlale, sest tegelikult on ka ilmselt tehisintellektimudeli või -süsteemi pakkujal või juurutajal äriline huvi, et loodud tehisintellekt oleks usaldusväärne, mis omakorda võimaldaks saada enam kasutajaid. Seejuures võib kallutatuse tuvastamine ja selle leevendamine toimuda juba arendamise etapis, mille puhul tõstatub küsimus, kas sellisel juhul töödeldakse eriliiki isikuandmeid korraga mitmele erinevale õiguslikule alusele tuginedes.

Kavandatava artikkel 4a lõige 1 punkt e näeb ette tingimuse, et isikuandmete eriliigid kustutatakse pärast erapoolikuse parandamist või isikuandmete säilitamisperioodi lõppu, olenevalt sellest, kumb saabub varem. Käesoleva arvamuse peatükis 4 on AKI juba tõstatanud küsimuse, kas isikuandmete kustutamine juba süsteemi sattunud andmete puhul on ikka võimalik.

20. Registreerimiskohustusest loobumine
(Tehisintellekti määruse artikkel 49 lõige 2)

Kehtiva tehisintellekti määruse artikkel 49 lõike 2 kohaselt registreerib pakkuja või kohaldataval juhul volitatud esindaja 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, selle süsteemi artiklis 71 osutatud ELi andmebaasis. See nõue kavatsetakse tehisintellekti omnibusi eelnõu punkti 14 kohaselt kaotada, seega edaspidi jääb tehisintellekti määruse artikkel 6 lõike 3 kohane hindamine ja dokumenteerimiskohustus pakkuja vastutada (nii nagu see seni on olnudki), kuid muudatuse kohaselt ei pea pakkuja enam sellisest

süsteemist teada andma. Kuigi tehisintellekti omnibusi põhjenduspunkti 9 järgi võivad riiklikud pädevad asutused nõuda pakkujatelt dokumendid välja, ei pruugi pädeval asutusel olla üldse teadmistki tehisintellekti pakkuja olemasolust. Dokumentide väljanõudmise eeldus on selliste dokumentide olemasolust teadmine. Nii võib turule sattuda ja seal mõnda aega tegutseda tehisintellektisüsteem, mille pakkuja on kvalifitseerinud tehisintellekti määruse artikkel 6 lõike 3 kohase süsteemina, kuid mille õigeaegse registreerimise korral oleks riiklikul pädeval asutusel tekkinud selle olemasolu kohta teadmine, et vajadusel järelevalvemeetmetega sekkuda.

21. Tehisintellekti regulatiivliivakastid
(Tehisintellekti määrus artikkel 57)

Kehtiv tehisintellekti määrus seab liikmesriikide pädevatele asutustele kohustuse luua riiklikul tasandil vähemalt üks tehisintellekti regulatiivliivakast. Ettepanekuga sätestatakse Euroopa tehisintellektiametile (tehisintellektiamet) võimalus luua selline regulatiivliivakast ka liidu tasandil. AKI on seisukohal, et EL-i tasandil regulatiivliivakasti loomine võiks aidata toetada innovatsiooni, eelkõige VKE-de ja start-upide kontekstis ning vältida „*forum shoppingut*“ ning killustunud lähenemist liikmesriikide lõikes. Samas tõstatuvad ettepanekuga ka potentsiaalsed ohukohad. Tegelikes tingimustes testimine ei tohiks viia kontrollimatu andmetöötluseni. Vajalik on kindlate protseduuride paika seadmine liivakastist väljumiseks ning andmete kustutamiseks kui testimine on lõppenud. Ettepanek tekitab küsimusi riiklike pädevate asutuste rolli kohta EL-i tasandi liivakastide disainimisel ja järelevalves. Nimelt mainitakse ettepanekus, et tehisintellektiamet peaks EL-i tehisintellekti regulatiivliivakaste rakendama koostöös pädevate riiklike asutustega, seejuures aga ei selgitata vastava koostöö tegemise kriteeriumeid ega erinevate asutuste rollide ja pädevuste jaotust. Kehtiva tehisintellekti määruse artikli 57 lõige 10 näeb riiklike tehisintellekti regulatiivliivakastide suhtes ette riikide pädevate asutuste kohustuse tagada, et niivõrd kui tehisintellektisüsteemid on seotud isikuandmete töötlemisega, 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.

AKI leiab, et liiduülese tehisintellekti regulatiivliivakasti loomisel on sarnaselt eeltoodud sättega vajalik kindla järelevalveraamistiku kehtestamine seoses isikuandmete töötlemisega (näiteks juhul kui leiab aset isikuandmete töötlemisega seotud rikkumine).

22. Üldotstarbelise tehisintellektisüsteemi järelevalve ja kontroll
(Tehisintellekti määruse artikkel 75)

Tehisintellekti omnibusi raames täpsustatakse tehisintellekti määruse artiklit 75, millega tugevdatakse tehisintellektiameti rolli üldotstarbeliste tehisintellektisüsteemide järelevalves ja koordineerimises. Artikli eesmärk on tagada üldotstarbeliste tehisintellektisüsteemide ühtne käsitlus liidu tasandil ning vältida killustunud järelevalvet, arvestades nende süsteemide laia kasutusulatust ja piiriülest mõju. Tehisintellektiametile antakse pädevus koguda ja hinnata teavet üldotstarbeliste tehisintellektisüsteemide kohta, toetada liikmesriikide järelevalveasutusi ning teha koostööd Euroopa tasandi struktuuridega, et tagada määruse järjepidev kohaldamine.

Tehisintellekti omnibusi ettepanekust jääb selgusetuks, kuidas jagunevad vastutus ja pädevus tehisintellektiameti ning riiklike andmekaitse järelevalveasutuste vahel olukordades, kus üldotstarbelisel tehisintellektisüsteemil põhinev lahendus toob kaasa IKÜMi rikkumise. Ilma selge rollijaotuseta võib tekkida regulatiivne lünk, kus tehniline järelevalve tehisintellekti alusel ja isikuandmete kaitse järelevalve IKÜMi alusel ei moodusta sidusat tervikut, vaid eksisteerivad

paralleelselt, vähendades isikuandmete kaitse tegelikku tõhusust.

23. Liikmesriigi järelevalveasutuste pädevuse piirid
(Tehisintellekti määruse artikkel 77)

AKI tõlgenduse kohaselt on põhiõigusi kaitsvatel asutustel kehtiva tehisintellekti määruse artikli 77 alusel volitus dokumentatsiooni küsimiseks otse tehisintellektisüsteemide juurutajatelt ja pakkujatelt. Ettepaneku järgi peaksid põhiõigusi kaitsvad asutused vastavat dokumentatsiooni hakkama taotlema turujärelevalveasutuste kaudu. Selline muudatus suurendab tõenäoliselt halduskoormust ja võib tekitada turujärelevalveasutuste juurde nn „pudelikaela" kui neile lisandub kohustus lisaks olemasolevatele kohustustele igakordselt asuda põhiõigusi kaitsvatele asutustele dokumentatsiooni vahendava asutuse rolli. AKI on seisukohal, et kehtiv tehisintellekti määruse artikkel 77 tuleks jätta muutmata, kuivõrd see ei aita täita ettepaneku lihtsustavat eesmärki. Selle asemel muutub protsess keerulisemaks, kuivõrd sama eesmärgi täitmiseks on vajalik läbida täiendavaid samme. Ühtlasi kitsendatakse selliselt põhiõigus kaitsvate asutuste pädevusi.

KÜSIMUSED EUROOPA KOMISJONILE

Käesolevaga esitab Andmekaitse Inspektsioon oma tekkinud küsimused.

1. Kuidas tuleks mõista isikuandmete mõiste juures „mõistlikult tõenäoliselt kasutatavad vahendeid" ning kuidas haakub sellega EK lahendi C-582/14 p 46 sätestatu, et vahendite kasutamisel peab identifitseerimise oht olema olematu või ebaoluline?
2. Miks ei ole Komisjon võtnud isikuandmete mõiste kontekstis arvesse kolmandate isikute mõistlikku võimalust isikuid tuvastada olukorras, kus teabevaldajal selline teave puudub?
3. Kas seadusandja soov on tõlgendada IKÜM artikkel 5 lõike 1 punkti b põhjendust selliselt, et eesmärgi kooskõla tähendab ka õigusliku aluse olemasolu?
4. Miks ei ole tehisintellektiga seonduvaid sätteid lisatud tehisintellekti määrusesse, vaid tehnoloogiliselt neutraalsesse IKÜMi?
5. Kuidas hinnata andmetöötleja kavatsust isikuandmete töötlemisel IKÜM artikkel 9 lõike 5 kohaselt?
6. IKÜM artikli 12 lõike 5 kohaselt võib pidada ülemääraseks neid andmesubjekti taotlusi, mille eesmärk ei ole andmete kaitsmine. Mida tähendab viidatud „andmete kaitsmine" ning milliste kriteeriumite alusel tuleks hinnata andmesubjekti eesmärki?
7. IKÜM artikli 13 lõike 4 välistusi arvesse võttes kellel on võimalik antud artiklis viidatud erandit kasutada?
8. Ühtse teavituspunkti loomisel jääb arusaamatuks ENISA roll andmete saamisel. Kas ENISA-l on andmete nägemise õigus? Kuidas hakkab andmete liikumine andmetöötlejalt järelevalveasutusele täpselt toimuma?
9. Kuidas suhestuvad omavahel ühtse teavituspunkti kaudu erinevatele järelevalveasutustele edastatavate teadete tähtajad? Kas mõistlik ei oleks kehtestada ühtne tähtaeg ning järelevalveasutuse teavitamise lävend?
10. Kas saame õigesti aru, et kui ühtse teavituspunkti kaudu esitatakse teavitus NIS2 alusel RIAle tähtajaga 24 tundi ja AKIle tähtajaga 96 tundi sama intsidendi osas, siis kas need teavitused tulevad AKIle RIAga samaaegselt ning sellisel juhul on teavitustähtaeg lühem?
11. Rikkumisteate esitamise künnise tõstmise kasuks räägib asjaolu, et järelevalveasutused saavad suurel hulgal rikkumisteateid. Kui eesmärgiks on vähendada väheoluliste

rikkumisteadete esitamist, kas künnis ei peaks olema madalam kui praegu väljapakutud „suur oht“?

12. Milline on ettepaneku suhe Komisjoni määrusega 611/2013?
13. Kas IKÜM artikli 88a lõike 4 nõusolekutaotlusest keeldumine ei ole vastuolus IKÜM artikli 7 lõikega 4?
14. Kas IKÜM artikli 88b raamistik on brauseripidajale vabatahtlik?
15. Milline on andmemääruses reguleeritud väärtuslike andmestike ja isikuandmete suhe?
16. Millised on Euroopa tehisintellektiameti ja riiklike pädevate asutuste koostöö tegemise kriteeriumid ning milline on vastavate asutuste rollide ning pädevuste jaotus EL-i tehisintellekti regulatiivliivakasti kontekstis?

Lugupidamisega
(allkirjastatud digitaalselt)
Pille Lehis
peadirektor

Kirsika Nigul
kirsika.nigul@aki.ee
6828712