

SELETUSKIRI
Vabariigi Valitsuse otsuse juurde
„Eesti seisukohad Euroopa Komisjoni digivaldkonna lihtsustamise koondpaketi kohta”

Euroopa Komisjon avaldas 19.11.2025 digivaldkonna lihtsustamise koondpaketi (nn digiomnibussi), mis sisaldab ettepanekuid nii Euroopa Liidu digivaldkonna õigusaktide muutmiseks kui ka tehisintellekti määruse muutmiseks. Samuti tehakse ettepanekud muuta isikuandmete kaitse üldmäärust, EL institutsioonide andmekaitsemäärust ning küberintsidentidest teavitamise raamistikku.

Digivaldkonna koondpakett keskendub ELi digi- ja andmereeglite lihtsustamisele, koondades ja ühtlustades mitmest eraldi õigusaktist tulenevaid kohustusi. Selle eesmärk on vähendada ettevõtjate halduskoormust, vältida kattuvaid nõudeid ning parandada õiguskindlust. Olulisemad muudatused hõlmavad eriliiki isikuandmete ning biomeetriliste andmete kasutamise tingimusi, aruandlus- ja teavitamiskohustuste lihtsustamist ning vastutavate töötlejate koormuse vähendamist madala riskiga andmetöötlusel.

Tehisaru pakett keskendub AI määruse rakendamise selgemaks ja innovatsioonisõbralikumaks muutmisele, lähtudes riskipõhisest lähenemisest. Ettepanekute eesmärk on vähendada madala riskiga AI-süsteemide regulatiivset koormust ning pakkuda rohkem paindlikkust väikeettevõtetele. AI koondpaketiga tehakse ettepanek kõrge riskiga AI-süsteemide pakkujatele kehtestatud nõuete edasilükkamiseks, et anda täiendav aeg standardite väljatöötamiseks. Samuti nähakse ette ELi tasandil AI testkeskkonna loomine.

Eesti peamised seisukohad digivaldkonna koondpaketi kohta sisaldavad järgmist:

- Eesti toetab digivaldkonna lihtsustamise koondpaketi raames Euroopa andmeõiguse reeglistiku lihtsustamist vähendamaks ebavajalikku ettevõtjate halduskoormust ja avaliku sektori töökoormust, muutes nii Euroopa andmeõiguse rakendamise tõhusamaks ning lihtsamaks.
- Eesti jaoks on oluline, et isikuandmete kaitse regulatsiooni muutmine ei tooks kaasa AI kasutusele võtmise ja treenimise senisest keerukamaks muutmist ega muudaks EL põhiõiguste hartas sätestatud põhiõiguste olemust. Näiteks peab ka avalik sektor saama vajadusel treenida tehisaru lahendusi. Õigusaktide muudatustele peavad eelnema põhjalikud mõjuanalüüsid.
- Eesti leiab, et digivaldkonna lihtsustamise koondpaketi menetlemisel tuleb arvestada, et käsitletavat teemasid on sisulised, erineva ajakriitilisuse ja mõjuga ning omavahel seotud. Seetõttu tuleb esmajärjekorras lahendada kõige ajakriitilisemad küsimused, millel on vahetu mõju õiguskindlusele ja regulatsiooni õigeaegsele rakendamisele, eelkõige suure riskiga tehisintellekti määruse rakendumistähtaja sätete kehtima hakkamise edasi lükkamine.

1. Sissejuhatus

Seisukohad on seotud järgnevate Euroopa digivaldkonna lihtsustamise koondpakettidega:

- Euroopa Parlamendi ja Nõukogu määrus, millega muudetakse määrusi (EL) 2016/679, (EL) 2018/1724, (EL) 2018/1725 ja (EL) 2023/2854 ning direktiive 2002/58/EÜ, (EL) 2022/2555 ja (EL) 2022/2557 seoses digivaldkonna õigusraamistiku lihtsustamisega ning tunnistatakse kehtetuks määrused (EL) 2018/1807, (EL) 2019/1150, (EL) 2022/868 ja direktiiv (EL) 2019/1024 (digivaldkonna koondpakett), (edaspidi ka üldine digikoondpakett)¹;

Sellega seotud muudatusettepanekute üldine eesmärk on Euroopa andmeõiguse lihtsustamine ja ettevõtete halduskoormuse vähendamine. Lisaks soovitakse andmeõiguse juhtimise ja tõhusa jõustamise parandamise kaudu vähendada nõuete keerukust, ettevõtete ja asutuste halduskulusid.

- Euroopa Parlamendi ja nõukogu määrus, millega muudetakse määruseid (EL) 2024/1689 ja (EL) 2018/1139 seoses tehisintellekti käsitlevate ühtlustatud õigusnormide (tehisintellekti käsitlev digivaldkonna koondpakett) rakendamise lihtsustamisega, (edaspidi ka tehisaru regulatsiooni koondpakett).²

Tehisaru regulatsiooniga seotud muudatusettepanekute üldine eesmärk on tugevdada tehisintellekti ameti teatud kategooriate tehisaru süsteemide seiret ja järelevalvet ning hõlbustada uuenduslike tehisaru süsteemide arendamist ja testimist ELi tasandil range regulatiivse järelevalve all enne nende süsteemide turule laskmist või muul viisil kasutuselevõttu. Lisaks soovitakse muudatustega tõhustada tehisintellekti määruse tehisaru süsteemidega seotud eeskirjade juhtimist ja tõhusat jõustamist. Muudatustega nähakse ette ELi tasandil katsekeskkonna loomine, mis võimaldaks piiriülest tegevust ja testimist.

Euroopa andmeõigus, sh tehisaru regulatsioon, on keerukas ja fragmenteeritud. Erinevad põhimõtted, reeglid, nõuded ja kohustused on erinevates õigusaktides, mis kasutavad muuhulgas kohati erinevaid termineid sarnastele asjadele. Haldus- ja töökoormus on erinevatele rakendajatele märkimisväärne. See kõik mõjutab ka Eestis Euroopa andmeõiguse rakendamist, mistõttu on probleem aktuaalne ka Eestis.

Esialgse hinnangu kohaselt toob algatus kaasa positiivseid mõjusid majandusele, infotehnoloogiale ja infoühiskonnale, inimeste õigustele ning riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele, kuludele ja tuludele. Samas võivad muudatused nõrgestada isikuandmete kaitset ja teha inimeste jaoks oma õiguste kasutamise keerulisemaks.

Tegemist on seadusandliku tavamenetlusega. Digivaldkonna lihtsustamise koondpakettide vastuvõtmiseks nõukogus on vaja kvalifitseeritud häälteenamust. Nende koondpakettide

¹ Proposal for a regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM (2025) 837. Kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex:52025PC0837>.

² Proposal for a regulation of the European Parliament and of the council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), COM/2025/836 final. Kättesaadav: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0836>.

menetluse ajakavad on veel kujunemisel, kuid esialgse info pinnalt soovitatsetehisaru regulatsiooni koondpaketi üldine lähenemine kokku leppida 2026. aasta suveks. Koondpakettide subsidiaarsustähtaeg on 16.03.2026.

Eelnõu on seotud mitmete Eesti EL poliitika 2025-2027 prioriteetidega (edaspidi *ELPOL*)³. Eelkõige on oluline, et ELi andmevaldkonnas suureneks õigusselgus ja –kindlus. Eelnõu ei ole otseses seoses eelnõu seletuskirja kirjutamise ajal menetluses oleva muu riigisisese eelnõuga.

2. Koostajad

Seisukohad ja seletuskirja koostasid Justiits- ja Digiministeeriumi (edaspidi *JDM*) üldosakonna kommunikatsiooni ja väliskoostöö talituse Euroopa Liidu asjade ja väliskoostöö juht Kristiina Krause (kristiina.krause@justdigi.ee), digiriigi osakonna digiriigi poliitika ja arenduse talituse juhataja Birgit Lüüs-Jakobs (birgit.luus-jakobs@justdigi.ee), sama talituse projektijuht Hendrik Roland Helm (hendrikroland.helm@justdigi.ee), sama talituse digiarengu valdkonna strateegiajuht Anna-Liisa Pärnalaas (anna-liisa.parnalaas@justdigi.ee), sama osakonna AI ja andmete talituse juhataja Ott Velsberg (ott.velsberg@justdigi.ee), sama talituse andmehalduse programmijuht Kuldar Aas (kuldar.aas@justdigi.ee), sama talituse bürokraati teenuste projektijuht Allar Laaneleht (allar.laaneleht@justdigi.ee), sama osakonna IT õiguse talituse nõunik Mait Heidelberg (mait.heidelberg@justdigi.ee), sama talituse juhataja Stina Avvo (stina.avvo@justdigi.ee), õiguspoliitika osakonna andmekaitseõiguse talituse juhataja Kristi Värk (kristi.vark@justdigi.ee), sama talituse nõunikud Kristel Niidas (kristel.niidas@justdigi.ee) ja Helen Uustalu (helen.uustalu@justdigi.ee), digitalistu ja küberturvalisuse osakonna riikliku küberturvalisuse talituse küberturvalisuse õigusnõunik Raavo Palu (raavo.palu@justdigi.ee) ning sama talituse rahvusvahelise küberturvalisuse koostööjuht Carmen Raal (carmen.raal@justdigi.ee).

Digiriigi valdkonna eest vastutab Justiits- ja Digiministeeriumi asekanstler Lauri Luht (lauri.luht@justdigi.ee), küberturvalisuse valdkonna eest asekanstler Tõnu Grünberg (tonu.grunberg@justdigi.ee) ja andmekaitse valdkonna eest asekanstler Heddi Lutterus (heddi.lutterus@justdigi.ee).

3. Sisu ja võrdlev analüüs

Eelnõu on seotud mitmete Eesti EL poliitika prioriteetidega. Eelkõige on oluline, et ELi andmete ja tehisintellekti valdkonnas suureneks õigusselgus ja -kindlus. Selleks tuleb komisjonil tagada tehisintellekti testkeskkondade ehk liivakastide loomine ELis, et anda ettevõtjatele ja avaliku sektori asutustele kindlus oma toote või teenuse ELi nõuetele vastavuse kohta (ELPOL p 69). Samuti on ELPOLi vaatest oluline ELi tasandil kehtestatud väärtuslike andmetike loetelu, mille suhtes tuleks olemasolevate riskide või ohuhinnangute tõttu kehtestada ühtsed avalikustamise piirangud (ELPOL p 67) ning ELis tuleb soodustada privaatsustehnoloogiate ja turvaliste andmetöötluskeskkondade kasutuselevõttu, et tagada andmete kasutamine ja väärindamine privaatsust tagaval viisil. Euroopa Komisjonil tuleb anda juhised ja luua selgus, millised

³ Riigikantselei. Eesti Euroopa Liidu poliitika prioriteetidid 2025 – 2027. Kättesaadav: <https://riigikantselei.ee/el-poliitika-julgeolek-ja-riigikaitse/eesti-euroopa-liidus/eesti-eli-poliitika> (05.01.2026).

privaatsustehnoloogiad on põhiõiguste kaitse seisukohalt ELis piisavad ja nõuetele vastavad (ELPOL p 70).

3.1. EL digivaldkonna lihtsustamise koondpakettide sisu muudatused õigusaktide kaupa

a. Üldise digikoondpaketi tehti andmeõiguse aktide muutmiseks järgnevad ettepanekud:

Andmeõiguse erinevate aktide liitmine andmemäärusega: mitteisikustatud andmete vaba liikumise määrus, andmehaldusmäärus, avaandmete direktiiv. Avaliku teabe kättesaadavust puudutavate nõuete kokku toomine andmehalduse määrusest ja avaandmete direktiivist, eesmärgiga katta piiratud ja piirangutega avaliku teabe avalikustamisele kohalduvad nõuded ühes õigusaktis (senise avaandmete direktiivi ja andmehalduse määruse eristatud käsitluse asemel). Liitmise eesmärk on vähendada õiguslikku keerukust – sealhulgas mõningaid kattuvusi, ebatäpseid mõisteid ning küsimusi selle kohta, kuidas erinevad õigusaktid omavahel koos toimivad. Oluline on tagada, et andmemäärus mitte ainult ei vähendaks koormust, vaid suurendaks ka õiguslikku selgust ja toetaks konkurentsivõimet.

Suurem osa üldise digikoondpaketi muudatusi on seotud kahe Euroopa andmeõiguse suunaga:

1. erasektori andmete jagamist ja taaskasutust puudutavate nõuete koondamine ühte õigusakti eesmärgiga anda ettevõtetele ühtne ülevaade andmetele ligipääsu ja andmevahenduse nõuetest, mis on integreeritud digikoondpaketi peatükki VIIa,
2. avaliku teabe kättesaadavust puudutavate nõuete kokku toomine eesmärgiga katta piiratud ja piirangutega avaliku teabe avalikustamisele kohalduvad nõuded ühes õigusaktis (senise avaandmete direktiivi ja andmehalduse määruse eristatud käsitluse asemel), mis on integreeritud koondpaketi peatükki VIIc.

Üldise digikoondpaketi olulisemad muudatused on:

- Andmemääruse muudatused (nt ettevõtja ja avaliku sektori vaheline andmevahetus);
- Andmehaldusmääruse muudatused (nt andmevahendusteenust osutavate organisatsioonide registreerimisnõude muutmine vabatahtlikuks ja neile organisatsioonidele kohalduvate nõuete leevendamine);
- Isikustamata andmete vaba liikumise määruse muudatused
- Avaandmete direktiiv muutub määruseks (ilmselt eeldab avaliku teabe seaduse muutmist). Määrus on vahetult kohaldatav ning täisharmoniseeriv. Muu hulgas tõstetakse avaandmete direktiivist andmemäärusesse avaliku sektori avaandmete eest tasu võtmise ja taaskasutamise standardlitsentside sätteid. Uue normi kohaselt võivad avaliku sektori asutused võtta väga suurtelt ettevõtetelt taaskasutamise eest suuremat tasu ning avaliku sektori asutused võivad näha väga suurtele ettevõtetele ette eritingimused litsentside osas. Sellised tasud ja tingimused peavad olema proportsionaalsed ja nende summa peab põhinema objektiivsetel kriteeriumidel. Väiksemate ettevõtete paremaks toetamiseks laiendatakse VKEdele mõeldud ELi andmeõiguse nõuete täitmist hõlbustavaid reegleid ka väikeste keskmise turukapitalisatsiooniga ettevõtjatele (VKTKEdele).
- Euroopa andmeinnovatsiooni nõukoja (EDIB) mandaadi laiendamine.

b. Üldise digikoondpaketi tehtud küberintsidentide ühtse teavitusakna (*Single-Entry Point* ehk SEP) ettepanekud

Mitmed õigusaktid (direktiiv (EL) 2022/2555 ehk NIS2 direktiiv, määrus (EL) 2016/679 ehk IKÜM, määrus (EL) 910/2014 ehk eIDAS määrus, direktiiv (EL) 2022/2557 ehk CER direktiiv, määrus (EL) 2022/2554 ehk DORA määrus, määrus (EL) 2024/1366 ehk piiriüleste elektrivoogude küberturvalisust käsitlevaid sektoripõhiseid norme sisaldav võrgueeskiri nimetusega NCCS määrus, lennunduse valdkonna määrused ehk komisjoni määrused (EL) 2023/203 ja 2022/1645, direktiiv (EL) 2002/58/EÜ ehk e-privatsuse direktiiv ja määrus (EL) 2024/2847 ehk CRA määrus) kohustavad intsidentidest/ juhtumitest teavitama asjakohast pädevat asutust. Tegemist on nende õigusaktide järgijatele dubleeriva kohustusega, kui samas juhtumist tuleb teavitada mitut asutust, kasutades erinevaid vorme.

Lahendusena nähakse ühtset teavitamise agent ehk SEPi, mis võimaldab rakendada põhimõtet “teavita üks kord ja jaga mitme osapoolega”. SEPi arendab välja ja haldab EL Küberturvalisuse Amet (ENISA) ning seda peaks saama ka integreerida liikmesriikide riiklike lahendustega. SEP tehniline lahendus võidakse arendada välja CRA määruse kohase teavitusplatvormi tehnoloogia peale. Siinsete seisukohtade koostamise hetke seisuga ei ole võimalik anda hinnangut, milliseid IT-arendusi ning millises rahalises ulatuses oleks vaja teha Eesti riiklikes infosüsteemides. Seda ka põhjusel, et ENISA on alles koostamas asjakohaseid meetmeid ja nõudeid, mis on seotud SEPIga. Ettepanekus on hinnatud, et liikmesriik vajaks 2-4 täiskohaga töötajat, et hallata liikmesriigis asuvat SEPi osa. Eelarvelisi kulusid menetletakse edaspidi riigieelarve strateegia ja riigieelarve koostamise käigus vastavalt riigi eelarvelistele võimalustele. Eesti eesmärk on saavutada eelnõu läbirääkimistel proportsionaalne lahendus, mis jätaaks liikmesriikide ühekordsed ja püsikulud võimalikult madalaks.

Ettepaneku kohaselt eri õigusaktides olevad teavitamise tähtajad õigusaktides ei muutu – kuid ettepaneku SEPi selgituses ei ole märgitud, et digiomnibussi hulgas on ka IKÜMi muudatus, mis muudab isikuandmetega seotud rikkumisest teavitamise tähtaega.

Ettepanekus on esitatud uuringu ülevaade, mille kohaselt 82% vastanud organisatsioonidest peavad teavitama küberintsidentidest rohkem kui ühele järelevalveasutusele, sealhulgas 21% kõikidest vastanutest on pidanud teavitama viite asutust. Siin tuleb arvestada ka asjaoluga, et kui tegemist on kontserniga või tegevusega, mis toimub mitmes liikmesriigis, siis tuleb teavitus esitada mitme liikmesriigi pädevatele asutustele. Ettepanekus leitakse, et ühe teavituskanali kaudu teavitamisel saaks vähemalt 50% organisatsioonidest vähendada teavitamisega seotud vaeva – kuna nad peaksid (vähemalt) kahe teavituse asemel tegema ühe teavituse; samal ajal kui ühele viiendikule organisatsioonidele väheneks vastav koormus 66-80%, kui nad saavad teha 3-5 teavituse asemel ühe teavituse. See tähendaks ELi üleselt säästu ca 41,5 miljonit EUR igal aastal. Tegemist on arvutusega, mis on seotud küberintsidentidest teavitamisega ning see ei võta arvesse võimalikku täiendavat säästu, mis on seotud isikuandmetega seotud rikkumistest teavitamisega ehk et kui ka need teavitused tulevad ühtsesse teavitusaknasse.

c. Üldise digikoondpaketi ja on isikuandmete kaitse üldmäärusega (IKÜM) seondult tehtud järgnevad ettepanekud:

- täpsustatakse isikuandmete mõistet – andmeid ei käsitata isikuandmetena, kui konkreetne andmeid omav osapool ei suuda nende põhjal isikut tuvastada. Isikuandmete staatus tekib üksnes siis, kui konkreetne vastuvõtja saab isiku mõistlikult tuvastada, ning ühe osapoole

tuvastamisvõime ei laiene automaatselt teistele. Teadusuuringu mõiste tuuakse põhjenduspunktidest määruse põhitekti;

- lisatakse mõisted: lõppseade, elektroonilise side võrk, veebibrauser, meediateenus, meediateenuse osutaja, internetipõhine kasutajaliides;
- täpsustatakse isikuandmete töötlemise lubatavust tehisaru arendamiseks ja kasutamiseks – kinnitatakse üle, et „õigustatud huvi“ võib olla tehisaru puhul õiguslikuks aluseks ning luuakse tingimused eriliiki isikuandmete töötlemiseks tehisaru arendamise ja kasutuse tarbeks;
- võimaldatakse eriliiki isikuandmete (biomeetriliste andmete) töötlemist, kui see on vajalik andmesubjekti isikusamasuse kontrollimiseks ning biomeetrilised andmed või kontrollimiseks vajalikud vahendid on andmesubjekti ainukontrolli all;
- muudetakse automaatotsuste ja profileerimise lubatavuse tingimusi;
- täpsustatakse andmesubjekti õigusi – andmesubjekt saab oma andmetele juurdepääsu üksnes andmekaitsealsetel eesmärkidel ja juurdepääsuõiguse kuritarvitamise korral võib keelduda taotlusele vastamast;
- laiendatakse andmesubjektile teabe andmise piiramise aluseid ja andmekaitse rikkumistest teavitamise viisi ja aega (ühtne teavituskanal ning teavitusaeg pikeneb 72 tunni pealt 96 tunnini);
- muudatusega antakse komisjonile õigus rakendusaktiga kehtestada Euroopa Andmekaitsealaste ettepaneku alusel isikuandmete töötlemise toimingute tüüpide loetelu, millele tuleb koostada andmekaitsealane mõjuhinnaang, mõjuhinnaangute vorm, meetodika. Komisjon saab rakendusaktiga sisustada määratlemata õigusmõisted (kõrge risk) ning määrata kindlaks millised pseudonüümimise viisid tagavad, et andmed ei oleks käsitatavad isikuandmetena;
- uuendatakse isikuandmete salvestamisega lõppseadmes (nn küpsiste) ja nõusolekutega seotud regulatsiooni – see koondatakse enam IKÜMi alla ja muudetakse e-privatsuse direktiivi.

Samadest põhimõtetest lähtuvad ka EL institutsioonide andmekaitsemääruse muudatusettepanekud. Samas ei ole ettepanekus ette nähtud, et sarnaseid muudatusi tehakse direktiivis (EL) 2016/680 (nn õiguskaitseasutuste andmekaitse direktiiv, mis reguleerib isikuandmete töötlust süüteomenetluses ja kriminaalkaristuste täideviimisel).

d. Tehisaru regulatsiooni koondpaketi tehti tehisaru reguleerimise osas järgmised ettepanekud:

- muudetakse kõrge riskiga tehisintellektisüsteemide reeglite kohaldumisaega: rakendamise tähtaeg hakkab kulgema vastavate standardite valmimisest. Varasemalt pidid nimetatud nõuded hakkama kehtima 02.08.2026;
- täpsustatakse ning täiendatakse väikeste ja keskmise suurusega ettevõtetele (VKEdele) ning väikeste keskmise turukapitalisatsiooniga ettevõtjatele (VKTKEdele) kehtivaid regulatsioone;
- tehisintellektisüsteemide pakkujad ja juurutajad pidid varasemalt võimalikult suurel määral võtma meetmeid, et tõsta teadlikkust AI kasutamisest. Nüüd on see muutunud Komisjoni ja liikmesriikide ülesandeks, et selliseid ettevõtjaid julgustataks vastavate meetmete kaudu.
- muudetakse kõrge riskiga tehisintellektisüsteemide pakkujate kohustusi. Teatud juhtudele (nt olukorras, kus AI-d kasutatakse ainult kitsasteks menetluslikeks ülesanneteks) ei rakendu EL andmekogus registreerimise kohustus;

- muudetakse vastavushindamise asutuste AI määruses toodud sätteid;
- reguleeritakse võimalust eriliigilisi isikuandmeid töödelda tehisintellektisüsteemi kallutatuse avastamiseks ja parandamiseks, tingimusel et rakendatakse sobivaid kaitsemeetmeid;
- kaotatakse nõue ühtlustatud järelturu jälgimisplaani kasutamiseks;
- koondatakse Euroopa AI Ameti kätte üldotstarbelistel tehisintellekti mudelitel põhinevate süsteemide või väga suurtes veebiplatvormides ja otsingumootorites olevate tehisintellekti funktsioonide järelevalve;
- täiendatakse tehisintellekti regulatiivsete liivakastide (nn testkeskkondade) ja reaalses keskkonnas testimise reeglistikku, ning luuakse õiguslik alus ELi-ülese AI testkeskkonna loomiseks.

3.2. EL digivaldkonna lihtsustamise koondpakettide sisu vastavus kehtivale õigusele

a. Koondpakettide vastavus põhiseadusele

Üldises digikoondpaketi tehtud andmeõiguse (andmehaldusmääruse, andmemääruse, avaandmete direktiivi ja mitteisikustatud andmete vaba liikumise määruse) muudatuste ning ühe akna lahenduse (SEP) regulatsiooni puhul ei tuvastatud vastuolu Eesti Vabariigi põhiseadusega. Samas võivad edasised võimalikud muudatused, mis kätkevad endas isikuandmete mõiste muutmist, andmesubjekti päringu tegemise õigust üksnes andmekaitselistel eesmärkidel ja isikuandmete töötlemise lubatavus tehisaru rakendamisel, nõrgestada isikuandmete kaitset ja teha inimeste jaoks oma õiguste kasutamise keerulisemaks, mis ei pruugi olla proportsionaalne isikuandmete kaitse eesmärkidega. Teatud juhtudel võib võimalik ebaproportsionaalne riive minna vastuollu ka eraelu puutumatuse põhiõigusega (Eesti Vabariigi Põhiseadus § 26). Seetõttu ettepanekute menetluse käigus tuleb olla tähelepanelik, et eelnõusse selliseid vastuolusid ei jääks, muuhulgas olla tähelepanelik eraelu puutumatuse kaitse (EV Põhiseadus § 26) suhtes.

Muudatused toetavad ELPOLi ja VVTP eesmärgi vähendada halduskoormust, toetades samas teabe parema leitavuse ja taaskasutatavuse saavutamist.

b. Muu riigisisese õiguse muutmise vajadus

Üldises digikoondpaketi väljatoodud Euroopa andmeõiguse muudatused on otsekohalduvad, mistõttu enamik neist ei vaja riigisisest eraldi kehtestamist. Avaandmete direktiivi muutumisega Euroopa Liidu määruseks, tuleb üle vaadata avaandmetega seotud sätted avaliku teabe seaduses. Tulevase ühtse andmemäärusega dubleerivad sätted tuleb avaliku teabe seaduses kehtetuks tunnistada.

Tulevase tehisaru määruse rakendamise seadus peab **tehisaru regulatsiooni koondpaketi osa** muudatustega arvestama (eelkõige tehisaru liivakastide regulatsiooni muudatustega ning järelevalve muudatustega), kui seda menetlema hakatakse.

Üldises digikoondpaketi väljatoodud küberintsidentidest kui ka muudest juhtumitest teavitamise üks aken (SEP)

- Üldistatult võetuna on ühtse teavitusakna lahenduse (ingl k *single entry point*, SEP) loomine vastavuses VVTPs oleva eesmärgiga vähendada ettevõtjate halduskoormust.

- Digikoondpaketi ettepanekus on märgitud, et SEPiga seonduvalt muudetakse ainult IKÜMi, e-privatsuse direktiivi, NIS2 direktiivi ja CER direktiivi. Ülejäänud EL õigusaktide puhul on ette nähtud, et EL õiguse alusel kehtestatavates rakendusmäärustes või delegeeritud määrustes tagatakse ühtse teavituskasutusele võtmine. Samas ei ole ettepanekus märgitud, kas ning mil määral oleks vaja muuta ka direktiivi (EL) 2016/680 (reguleerib isikuandmete töötlust süüteomenetluses ja kriminaalkaristuste täideviimisel) või ka mõnda muud õigusakti, millel on sarnasusi siinse teemaga (nt kasvõi AI määrust).
- SEPi loomiseks on vaja muuta vähemalt küberturvalisuse seadust (eeldusel, et küberturvalisuse seaduse § 8 olemus ja sisu muutuks SEPiga seotud EL õiguslike muudatustega sellisel määral, et seaduse § 8 lõige 8¹ ei ole piisav õigusselguse tagamiseks ⁴), investeerimisfondide seaduse § 345¹, kindlustustegevuse seaduse § 105¹, krediitiasutuste seaduse § 92⁴, makseasutuste ja e-raha asutuste seaduse § 63⁶, väärtpaberite registri pidamise seaduse § 30², väärtpaberiturust seaduse § 82¹⁸ ja 125³ ning ilmselt teataval määral ka hädaolukorra seadust kui ka seda asendavat tsiviilkriisi ja riigikaitse seadust. Kui muudetakse ka õiguskaitseasutustega seotud andmekaitse direktiivi, siis tuleb muuta ka isikuandmete kaitse seaduse § 44 (õiguskaitseasutuste kohustus teavitada isikuandmetega seotud rikkumisest Andmekaitse Inspektsiooni). Lisaks eeltoodud seadustele tuleb muuta ka samade õigusaktidega seotud või nende alusel kehtestatud asjakohaseid määrusi.

4. EL asja vastavus pädevuse andmise, subsidiaarsuse ja proportsionaalsuse põhimõtetele

4.1. Õiguslik alus

Õiguslikuks aluseks on valitud ELi toimimise lepingu (edaspidi ka ELTL) artiklitel 114 ja 16, mis kajastavad muudetavate aktide õiguslikku alust. Asjakohane õiguslik alus määruse (EL) 2016/679 (isikuandmete kaitse üldmäärus ehk IKÜM) ja määruse (EL) 2018/1725 muutmise sätete jaoks on lepingu artikkel 16. Kuna kõik teised muudetavad aktid põhinevad lepingu artiklil 114, on sama õiguslik alus sobiv ka Euroopa digivaldkonna lihtsustamise koondpakettide vastavate muutmissetete jaoks.

4.2. Subsidiaarsus

EL lepingu artikli 5 lõikes 3 sätestatud subsidiaarsuse põhimõtte kohaselt tuleks ELi tasandil meetmeid võtta üksnes juhul, kui liikmesriigid üksi ei suuda kavandatud eesmärgi piisaval määral saavutada ning seetõttu on neid kavandatava meetme ulatuse või toime tõttu parem saavutada ELi tasandil.

Arvestades, et ettepanekutega muudetakse Euroopa Liidu õigusakte, saab neid muudatusi teha üksnes liidu tasandil. Esitatud ettepanekud säilitavad subsidiaarsuse loogika, millele muudetavad õigusaktid tuginevad.

Üldises digikoondpakettis välja toodud andmemääruse (EL) 2023/2854 muudatused tugevdavad määruse eesmärki kõrvaldada takistused ühtsel turul andmepõhise majanduse jaoks. Sihipäraste

⁴ Tolle lõike sõnastus: Kui Euroopa Komisjon võtab vastu Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 23 lõikes 11 nimetatud rakendusakti, milles täpsustatakse küberintsidendi, sealhulgas olulise mõjuga küberintsidendi kohta esitatava teate või raporti vorm ja selle esitamise kord, lähtutakse nimetatud rakendusaktis sätestatud nõuetest.

muudatuste eesmärk on lihtsustamine, selguse pakkumine ja halduskoormuse vähendamine nii erasektori kui ka riiklike asutuste jaoks. Esialgsel hinnangul muudatused ei sekku liikmesriikide ega ELi institutsioonide pädevusse. Läbirääkimistel tuleb olla tähelepanelik, et see nii ka jääks. Eelkõige võib see oht tekkida tehisintellekti ameti järelevalvesätete osas.

Sama kehtib ka üldises digikoondpaketis välja toodud avaandmete direktiivi (EL) 2019/1024 kehtetuks tunnistamise kohta, selle sisulised sätted viiakse üle andmemäärusesse ilma liikmesriikide ja ELi pädevuste vahetult kohaldatava rakendusmääruse (EL) 2023/138 (väärtuslike andmetike kohta) alla. Ühtsele andmemäärusele üleminek hõlbustab kavandatud muudatuste ühtset kohaldamist kõigis liikmesriikides. See toetab eelkõige avaliku sektori asutusi, kelle valduses on avaliku sektori andmed, aga ka nende andmete taaskasutajaid, ühtlustades menetlusi ning vähendades töökoormust. Vahetult kohaldatavate sätete jõustamine muutub tõenäoliselt liikmesriikide vahel ühtlasemaks. Digivaldkonna lihtsustamise koondpaketid jätavad liikmesriikidele piisavalt paindlikku võimaluse oma riiklike lahenduste loomiseks.

Üldises digikoondpaketis välja toodud isikuandmete kaitse üldmääruse (EL) 2016/679 ja määruse (EL) 2018/1725, samuti tehisaru regulatsiooni koondpaketis välja toodud tehisintellekti määruse (EL) 2024/1689 kavandatud muudatuste eesmärk on suurendada olemasolevate õigusnormide kohaldamise selgust ja etteaimatavust ning vähendada halduskoormust.

Üldises digikoondpaketis välja toodud ühtse teavitusakna kasutuselevõtuga (SEP) pakutakse välja üleeuroopaline lahendus, mille eesmärk on luua üks kanal mitme õigusliku kohustuse täitmiseks, mis on ettevõtjatele kehtestatud sisuliselt samast juhtumist raporteerimiseks. See lahendus ei muuda riiklike asutuste õigusi ega pädevust selliseid teateid vastu võtta. Vastupidi, ettepanek soodustab teavitamist, pakkudes lihtsasti kasutatava liidese kaudu ühtset teavitusakent, mis võimaldab esitada ühe teate, täites samal ajal mitu õiguslikku kohustust. Arvestades, et paljusid asjaomaseid teenuseid osutatakse piiriülesest ja teenusepakkujad tegutsevad mitmes liikmesriigis, on Euroopa-ülene lahendus vajalik.

4.3. Proportsionaalsus

EL lepingu artikli 5 lõikes 4 sätestatud proportsionaalsuse põhimõtte kohaselt peavad konkreetse meetme laad ja tugevus olema vastavuses tuvastatud probleemiga.

Euroopa digivaldkonna lihtsustamise koondpaketid sisaldavad muudatusi, mille eesmärk on vähendada ettevõtjate halduskoormust ja suurendada regulatiivset selgust, säilitades samal ajal muudetavate õigusaktide põhieesmärgid. Esialgse hinnangu kohaselt on tehtavad muudatused proportsionaalsed, kuna need toovad ettevõtjatele ja asutustele kaasa üksnes vähese kohanemiskulu ning võimaldavad samas märkimisväärset kulusäästu. Muudatustega vähendatakse ka ettevõtjate ja asutuste otseseid kulusid, lähtudes põhimõttest, et regulatiivseid eesmärke on võimalik saavutada väiksema koormusega.

Lihtsustamise eesmärki saavutatakse eelkõige õigusselguse suurendamise kaudu, täpsustades isikuandmete kaitse üldmääruse sätete kohaldamist ja kodifitseerides kehtivat tõlgenduspraktikat. See hõlmab muu hulgas selgitusi isikuandmeid sisaldavate tehisaru mudelite treenimise kohta, isikuandmete mõiste täpsustamist ning Euroopa Liidu Kohtu praktika, sealhulgas isikuandmete pseudonüümimisega seotud tõlgenduste, kodifitseerimist. Samas võivad muudatused, mis kätkevad endas isikuandmete mõiste muutmist, andmesubjekti päringu

tegemise õigust üksnes andmekaitselistel eesmärkidel ja isikuandmete töötlemise lubatavus tehisarukandmisel, nõrgestada isikuandmete kaitset ja teha inimeste jaoks oma õiguste kasutamise keerulisemaks, mis ei pruugi olla proportsionaalne isikuandmete kaitse eesmärkidega. Teatud juhtudel võib ebaproportsionaalne riive, minna vastuollu ka eraelu puutumatuse põhiõigusega (Eesti Vabariigi Põhiseadus § 26).

Lihtsustamise koondpakettis teatavate VKEdele kohaldatavate sätete laiendamine väikestele keskmise turukapitalisatsiooniga ettevõtjatele on sihipärane ning piirdub minimaalsete muudatustega.

Küberintsidentidest, isikuandmete rikkumistest ja muudest samalaadsetest juhtumitest teatamise ühtne teavitusaken vähendab kulusid, aitab lahendada alaraporteerimist ning suurendab teatamiskohustuste tõhusust. Veebipõhiste vahendusteenuste määrase (EL) 2019/1150 kehtetuks tunnistamine lõpetab ELi eeskirjade dubleerimise ja veebiplatvormidele kehtivad topeltkohustused. Need muudatused suurendavad õigusselgust ettevõtjate ja kodanike jaoks.

5. Esialgse mõjude analüüsi kokkuvõte

Esialgse hinnangu kohaselt toovad Euroopa digivaldkonna lihtsustamise koondpakettid kaasa mõju majandusele, infotehnoloogiale ja infoühiskonnale, inimeste õigustele ning riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele, kuludele ja tuludele.

Komisjon ei koostanud nimetatud koondpakettidele mõjuhinnangut, kuigi ettepanekuga tehtavad muudatused on olulised ja sisulised. Euroopa digivaldkonna lihtsustamise koondpakettidega tuli välja Komisjoni talituste töödokument (ing k *staff working document*).⁵

5.1. Mõju majandusele

Üldises digikoondpakettis väljatoodud andmeõiguse muudatused:

Mitme erineva andmevaldkonda reguleeriva õigusakti integreerimine ühte õigusakti võib parandada õigusselgust ja lihtsustada piiriülest tegutsemist andmete valdkonnas. Lisaks korrastab see andmeõigust - ettevõtjatel ja inimestel on tulevikus lihtsam leida erinevaid andmeõigusega seotud nõudeid, kohustusi, õigusi ja võimalusi. See võimaldab ühtlustada ka andmevaldkonna termineid, mis muudab ühtlustatud reeglid lihtsamini arusaadavaks ning toob erinevate andmeõiguse aktide seosed selgemalt välja. Samuti võimaldab seniste erinevate aktide integreerimine kaotada ebavajalikud ja liigsed nõuded. Avaandmete direktiivi liitmine andmemäärusega muudab avaandmete direktiivi määruseks, mis toob kaasa olukorra, kus avaandmetega seondud reeglistik muutub üle-euroopaliselt ühtsemaks. See võib soodustada ELi ülest avaliku teabe kättesaadavuse paranemist, mis muuhulgas annab ettevõtetele võimaluse luua avaliku teabe alusel uusi ja innovatiivseid piiriüleseid teenuseid.

⁵ Commission staff working document accompanying the documents: Proposal for a regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) and amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). Kättesaadav: <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>.

Mitmeid nõudeid leevendatakse ettevõtjate vaatest, mistõttu võib algatus vähendada ettevõtjate halduskoormust. See omakorda soodustab innovatsiooni ja konkurentsivõimet, kuna potentsiaalselt jääb rohkem ressursse tootearenduseks ja ettevõtluse võimalikuks kasvuks.

Samuti laiendatakse VKEde soodustingimusi VKEdelt väikestele keskmise turukapitalisatsiooniga ettevõtetele (VKTKEdele). See toob kaasa, et enamus (kui mitte kõik) Eesti ettevõtjad saavad tehtavatest leevendustest kasu ja sellega nende halduskoormus väheneb. See tähendab potentsiaalselt ka seda, et suurematele ettevõtetele kui VKEd ja VKTKEd võivad jääda kehtima rangemad reeglid. Kuna selliste suuremate ettevõtete arv on Eestis väike (või isegi olematu), siis selline mõju ei ole Eestis suur.

Üldises digikoondpakettis väljatoodud IKÜM muudatused:

Tehtavad ettepanekud vähendavad ettevõtjate halduskoormust, kuid toovad samal ajal kaasa uut ebakindlust. Ettevõtjate jaoks lihtsustuvad dokumenteerimis- ja teavituskohustused ning andmekaitsealaste mõjuhinnangute koostamine, mis teeb reeglite järgimise eriti VKEdele kergemaks. Ka andmerikkumistest teavitamise piiramine vaid suure riskiga juhtumitele ja pikem teavitamise tähtaeg vähendab ettevõtjate halduskoormust ning lubab keskenduda tõsistele ohtudele. Samas tekitab kavandatav, kontekstipõhine isikuandmete määratlus õiguskindlusetust, sest ettevõtjad peaksid iga andmeedastuse puhul eraldi hindama, kas andmete saaja suudab isikut tuvastada. Positiivne mõju on nn küpsisenõuete lihtsustamisel, mis aitab vähendada nn nõusoleku-väsimust.

Üldises digikoondpakettis väljatoodud ühtse teavitusakna ettepanek:

Ettepaneku selgituse kohaselt on hetkeseisuga teavitavate üksuste (muuhulgas ettevõtjate) ligikaudne kulu ELi üleselt €83,1 miljonit aastas. See kulu hõlmab nii teavitaja organisatsiooni personali tööaega, selle personali kaasamisega seotud kulusid kui ka muid asjakohaseid kaasnevaid kulusid. Ühtse teavitusakna loomine vähendaks neid kulusid ca 50% ulatuses ehk eeldatavalt hoitaks ELis kokku aastas € 41,5 miljonit. Tegemist on arvutusega, mis on seotud küberintsidentidest teavitamisega ning see ei võta arvesse võimalikku täiendavat säästu, mis on seotud isikuandmetega seotud rikkumistest teavitamisega ehk kui ka need teavitused tulevad ühtsesse teavitusaknasse. Seega võimaldab ühtne teavitusaken paremini planeerida ressursse, et küberintsidenti või muud juhtumit lahendada – selle asemel, et tegeleda ühest juhtumist teavitamisega mitmele pädevale asutusele, kasutades erinevaid teavituskanaleid.

Tehisareregulatsiooni koondpakett:

Kavandatud AI määruse lihtsustamismeetmed peaksid vähendama AI määrusest tulenevate nõuete täitmise kulusid ja lihtsustama rakendamist ettevõtetele (eriti VKEdele ja väikeste keskmise turukapitalisatsiooniga ettevõtetele ehk VKTKEdele). AI määrusest tuleneva suure riskiga süsteemide nõuete tähtaja ja komisjoni esitatavate juhiste, standardite jms ajakavade ühtlustamine ja üleminekuperioodi kehtestamine võimaldab ettevõtjatel tõhusamalt AI määruse nõudeid täita, vältides ka vajadust kulukate tagasiulatuvate kohanduste järele, kui ettevõtete tehtavad arendused ei peaks osutuma komisjoni loodavatele suunistele vastavaks. See potentsiaalselt vähendab ettevõtjate halduskoormust. Samuti on sarnane mõju AI määrusest tulenevate VKEde leevenduste laiendamisel VKTKEdele, dokumentatsiooni lihtsustamisel ja ametiasutuste juhiste andmisel. AI määruse ja teiste ELi õigusaktide koostoime parandamine vähendab dubleerimist ja muudab ettevõtjatele kehtivad nõuded selgemaks.

Innovatsiooni toetamine tehisintellekti regulatiivsete testkeskkondade ja reaalse testimise kaudu aitab ettevõtetel tehisintellekti ohutult arendada ja testida ning hõlbustab nende nõuete täitmise jõupingutusi. Sellel on potentsiaali muuta Euroopa, sh Eesti, atraktiivsemaks AI-arenduskeskkonnaks ning kiirendada AI kasutuselevõttu majanduses.

Komisjoni hinnangul võib digikoondpakett tuua üle-euroopaliselt ettevõtetele kaasa kuni 1 335 634 500 euro suuruse halduskulude kokkuhoiu aastas ja lisaks 1 043 943 500 euro suuruse hinnangulise ühekordse kokkuhoiu. Eeldusel, et ettepanek jõustub 2027. aasta alguseks, ulatuks see komisjoni ametiaja lõpuks 2029. aastal vähemalt 5 miljardi euron. Lisaks säästetakse komisjoni hinnangul avaliku sektori asutustele 2029. aastaks veel 1 miljard eurot.⁶

5.2. Mõju infotehnoloogiale ja infoühiskonnale.

Üldises digikoondpaketis väljatoodud andmeõiguse muudatused:

Andmeõiguse aktide koondamine ühtsesse EL määрусesse võib parandada õigusselgust ja lihtsustada ettevõtjate piiriülest tegutsemist. Ettepanekud on suunatud ühtsema digitaalse turu arengu ja innovatsiooni soodustamisele. Ühtsemad ja konsolideeritud andmeõiguse reeglid tagavad selgema arusaama nõuetest, kohustustest ja võimalustest. Samuti tagavad need selgema ja ühtsema andmekorralduse täna mitmes erinevas õigusaktis olevate nõuete vaatest. See omakorda vähendab killustatust andmete valdkonnas, mis võimaldab inimesel ja ettevõtjal paremini mõista reegleid, suurendades läbipaistvust ja usaldust e-riigi vastu. Lisaks võimaldavad selgemad ja lihtsamad reeglid ettevõtjatel potentsiaalselt tuua turule kasutajasõbralikumaid e-teenuseid ning tooted.

Praeguse parima teadmise pinnalt ei vaja andmeõiguse nõuete ühtlustamine ja ühendamise ühe määрусse alla infosüsteemide arendusi.

Üldises digikoondpaketis väljatoodud IKÜM muudatused:

Ettepanekud on suunatud digitaalse ühtse turu arengu ja innovatsiooni toetamisele, eriti tehisaru ja andmete vaba liikumise vallas. Õigustatud huvi selgem tunnustamine tehisaru arendamisel ning laiendatud teadusuuringu mõiste peaksid soodustama innovatsiooni ja andmete kasutamist. Samas kaotab tehisaruspetsiifiliste sätete lisamine IKÜM-i tehnoloogianeutraalsuse.

Üldises digikoondpaketis väljatoodud ühtse teavitusakna ettepanek:

Ettepanek võib tekitada vajaduse teha arendusi ühtse teavitusaknaga seotud pädevate asutuste (ennekõike Riigi Infosüsteemi Amet, kuid sisuliselt ka Andmekaitse Inspeksioon, Finantsinspeksioon, Politsei- ja Piirivalveamet, Tarbijakaitse ja Tehnilise Järelevalve Amet ning Transpordiamet) infosüsteemides, võimaldamaks teavitusakna vahendusel asjakohaseid teateid kätte saada ja vahetada. Siinsete seisukohtade koostamise hetke seisuga ei ole võimalik anda hinnangut, milliseid IT-arendusi ning millises rahalises ulatuses oleks vaja teha Eesti riiklikes infosüsteemides. Seda ka põhjusel, et ENISA on alles koostamas asjakohaseid meetmeid ja

⁶ Commission staff working document accompanying the documents: Proposal for a regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) and amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). Kättesaadav: <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>. Vt eelkõige lk 88. Kõigi hinnanguliste kokkuvõtte ülevaade on esitatud II lisas.

nõudeid, mis on seotud ühtse teavituskannaga. Ettepanekus on hinnatud, et liikmesriik vajaks 2-4 täiskohaga töötajat, et hallata liikmesriigis asuva ühtse teavituskanna osa. Eelarvelisi kulusid menetletakse edaspidi riigieelarve strateegia ja riigieelarve koostamise käigus vastavalt riigi eelarvelistele võimalustele. Eesti eesmärk on saavutada eelnõu läbirääkimistel proportsionaalne lahendus, mis jätab liikmesriikide ühekordsed ja püsikulud võimalikult madalaks.

Tehisareregulatsiooni koondpakett:

Ettepanek soodustab digitaalse ühtse turu arengut ja innovatsiooni nagu ka andmeõiguse ning andmekaitseõiguse muudatused. Ühtsemad ja lihtsustatud AI nõuded tagavad selgema arusaama nõuetest, kohustustest ja võimalustest ning nende kohaldumisest. Rakendusaja edasilükkamine võimaldab ettevõtjatel tehniliselt paremini ette valmistada AI nõuete täitmiseks. See võimaldab potentsiaalselt tuua turule kasutajasõbralikumaid e-teenuseid ning tooted, millel on AI komponent. Samas AI treenimiseks õiguslike aluste kitsendamine (õigustatud huvi, andmesubjekti nõusolek) pärsib avalikul sektoril AI-d treenida, sest nimetatud alused ei saa olla avalikus sektoris andmetöötluse aluseks AI treenimisel, kuna õigustatud huvi saab avalik sektori õiguslikul alusena kasutada üksnes oma põhiülesannete väliselt (nt vara kaitseks), nõusoleku alusel andmete töötlemisel peab nõusolek mh vastama tingimusele, et see on antud vabatahtlikult. Arvestades, et vastutav töötleja on avaliku sektori asutus, on asutuse ja andmesubjekti jõuvahekord ebavõrdne ning ei vasta vabatahtlikkuse tingimusele.

Praeguse parima teadmise pinnalt ei vaja AI määruse muudatused kohustuslikke Eesti poolseid infotehnoloogilisi arendusi.

5.3. Mõju inimeste õigustele

Üldises digikoondpaketi väljatoodud andmeõiguse muudatused:

Olulisi ja otseseid mõjusid andmesubjektidele esialgses Komisjoni ettepanekus ei täheldatud. Praegune üldise digikoondpaketi ettepanek tõstab kokku erinevate andmeõiguse aktide norme ning lihtsustab ettevõtjate regulatsiooni.

Üldises digikoondpaketi väljatoodud IKÜMi muudatused:

Muudatused võivad nõrgendada isikuandmete kaitset ja teha inimeste jaoks oma õiguste kasutamise keerulisemaks. Kui isikuandmete mõiste muutub ebaselgemaks, võib sama info olla mõne töötleja jaoks „mitte-isikuandmed“, kuigi teised suudavad inimese tuvastada, mis vähendab kaitset ja tekitab õiguslikku segadust. Teadusuuringute erandid võivad lubada andmete töötlemist inimese teadmata, mis vähendab läbipaistvust. Automatiseeritud otsuste kergem lubamine võimaldab andmesubjektil otsustusprotsessi hiljem sekkuda, võimaldades tal alles tehtud otsust vaidlustada. Kui andmekaitsealastest rikkumistest tuleb teavitada vaid suure ohu korral, ei pruugi inimesed paljudest andmeleketest teada saada ega saa ise samme astuda kahju vähendamiseks. Eesti kavatseb ka edaspidi nõuda andmekaitsealastest rikkumistest teavitamist ka väiksemate rikkumiste korral. Niinimetatud küpsistega seotud ettepanekud vähendavad andmesubjektile tema isikuandmete töötlemise läbipaistvust, kuid aitavad leevendada nõusoleku väsimust.

Üldises digikoondpaketi ühtse teavituskanna ettepanek:

Ettepanekus toodud lahendus hõlbustab küberintsidentidest, isikuandmetega seotud rikkumistest kui ka muudest samalaadsetest juhtumitest teavituse esitamist pädevatele asutustele. See omakorda võimaldab pädeval asutusel talle kohalduva õigusakti alusel hinnata, kas ja millisel määral on vaja teavitusele reageerida. Reageerimise viis võib olla näiteks kas teavitaja või

avalikkuse suunas – viimase puhul näiteks avalikkuse, sh inimeste teavitamise kaudu. See omakorda suurendab teadlikkust ja selgust, miks midagi juhtus ning mil määral inimene saab enda kaitseks mingi abimeetme kasutusele võtta.

Tehisaru regulatsiooni koondpakett:

AI kirjaoskuse edendamise säte on leebemaks kirjutatud ning pole enam otseselt ettevõtja kohustus, vaid liikmesriigid peavad ergutama ettevõtjad vastavat oskust jagama. See võib mõjutada inimeste teadlikkust AI kasutamisevõimalustest. Koondpaketi lisatakse AI määrusesse uus artikkel 4a, mis puudutab eriliigiliste isikuandmete töötlemist eelarvamuste tuvastamiseks ja leevendamiseks ning näeb ette selliseks töötamiseks erikaitsemeetmeid isikuandmete kaitseks. Sellised kaitsemeetmed lisanduvad andmekaitseõiguse reeglitele, mistõttu tagatakse nendega isikute põhiõiguste tõhusam kaitse.

5.5 Mõju riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele, kuludele ja tuludele

Üldises digikoondpaketi väljatoodud andmeõiguse muudatused:

Kui andmevahendusteenusel kaotatakse nõue teavitamiseks, siis teatud määral pädeva asutuse ülesanded muutuvad ja see peaks kaasa tooma nende töökoormuse vähenemist. Hädaolukordades andmete kättesaadavuse regulatsiooni muutmine toob kaasa muutuse riigiasutuste õiguses erasektorilt andmeid saada. Võimalused on koondpaketi alusel konkreetsemad ja kitsamad. Digikoondpakett puudutab küll otseselt avaliku sektori andmete kättesaadavaks tegemise kohustust (senised avaandmete direktiiv ja andmehalduse määruse II peatükk), kuid kuivõrd digikoondpaketi ei seata uusi ega leevendata kehtivaid nõudeid, siis puudub ka mõju teabevaldajate korraldusele, kuludele ja tuludele.

Üldises digikoondpaketi väljatoodud IKÜMi muudatused:

Ettepanekud toovad riigiasutustele ja järelevalvele kaasa suurema töökoormuse ning uusi õiguslikke ja praktilisi raskusi. Kuna paljud uued reeglid põhinevad ebamäärastel mõistetel ja tehniliselt keerukatel hinnangutel, muutub ühtne ja järjepidev järelevalve keerulisemaks ning võib kasvada vaidluste ja selgitustaotluste hulk. Ühtse teavitusakna loomine rikkumiste jaoks võiks vähendada dubleerimist ja lihtsustada piiriüleste juhtumite käsitlemist, kuid samas ei pruugi oluline info õigete asutusteni piisavalt kiiresti jõuda ning tsentraliseeritud andmebaas võib kujuneda turvariskiks. Kui rikkumistest tuleb teatada vaid suure ohu korral, kaotavad järelevalveasutused ülevaate keskmise ohuga juhtumitest, mis on oluline turvasuundumuste jälgimiseks ja varajaseks sekkumiseks. Kui IKÜMiga muudetakse isikuandmete mõistet, aga samasugust muudatust ei tehta nn õiguskaitseasutuste andmekaitse direktiivis, peavad viimased hakkama eri menetlustes käsitlema isikuandmeid erinevatest mõistetest lähtuvalt. Muuhulgas võib isikuandmete mõiste kontekstipõhiseks muutmise tõttu suureneda Andmekaitse Inspektsiooni töökoormus.

Üldises digikoondpaketi ühtse teavitusakna ettepanek:

Ettepanek võib tekitada vajaduse teha arendusi ühtse teavitusaknaga seotud pädevate asutuste infosüsteemides, võimaldamaks teavitusakna vahendusel asjakohaseid teateid kätte saada ja vahetada. Siinsete seisukohtade koostamise hetke seisuga ei ole võimalik anda hinnangut, milliseid IT-arendusi ning millises rahalises ulatuses oleks vaja teha Eesti riiklikes infosüsteemides. Ettepanekus on hinnatud, et liikmesriik vajaks 2-4 täistööajaga töötajat, et hallata liikmesriigis asuvat ühtse teavitusakna osa. Nende töötajatega seotud töökulude suurus

selguvad siis, kui on selgus, milliseid ülesandeid need töötajad peavad täitma (nt IT-tehnilise rolli täitmine või teenuse omaniku rolli täitmine) - see selgub siis, kui komisjon on andnud parema ülevaate, milline ühtse teavituskna kui ELi ülene terviksüsteem välja näeb. Eelarvelisi kulusid menetletakse edaspidi riigieelarve strateegia ja riigieelarve koostamise käigus vastavalt riigi eelarvelistele võimalustele. Eesti eesmärk on saavutada eelnõu läbirääkimistel proportsionaalne lahendus, mis jätkaks liikmesriikide ühekordsed ja püsikulud võimalikult madalaks.

Tehisaru regulatsiooni koondpakett:

AI kirjaoskuse edendamise kohustus pannakse uue muudatusega liikmesriikidele, mis tõstab avaliku sektori töökoormust ja toob kaasa kulusid meetmete pakkumisel, millega seda kirjaoskust ettevõtete töötajatel edendada. Varasemalt oli see ettevõtja kohustus. Selles osas ettevõtja halduskoormus väheneb avaliku sektori töökoormuse kasvu tõttu. Samuti soovib Euroopa Komisjon hakata teostama suurte platvormide ja üldotstarbeliste tehisintellekti mudelite üle järelevalvet, selle võrra on riigiasutustel väiksem järelevalvekoormus. Ettepanekus tugevdatakse tehisintellektiameti pädevust üldotstarbelisel tehisintellektimudelil põhinevate tehisintellektisüsteemide järelevalves ja jõustamises, kui mudelit ja süsteemi pakub sama pakkuja. Samal ajal selgitatakse kõnealuses sättes, et see järelevalve ei hõlma tehisintellektisüsteeme, mis on seotud AI määruse I lisaga hõlmatud toodetega. Väga suurtesse digiplatvormidesse või väga suurtesse internetipõhistesse otsingumootoritesse integreeritud tehisintellektisüsteemide nõuetele vastavuse järelevalve ja jõustamine peaks kuuluma tehisintellektiameti pädevusse. Kuna sellised suured süsteemid toimivad üldjuhul piiriüleselt, siis AI ameti mõju nende järelevalvele on potentsiaalselt tõhusam kui ühe liikmesriigi piires saab olla.

6. Eesti seisukohad

Eesti seisukohad on jaotatud erinevatesse alapeatükkidesse järgmiselt:

- Euroopa digivaldkonna lihtsustamise koondpakettide üldised põhimõtted ehk seisukohad, mis kohalduvad üldisele digikoondpaketile (s.o. COM(2025) 837) kui ka tehisaru regulatsiooni koondpaketile (s.o. COM(2025) 836); järgnevad alapeatükid on konkreetsete temaatikatega seotud seisukohad;
- Üldises digikoondpakettis väljatoodud andmeõiguse muudatused – seisukohad, mis on seotud andmeõiguse erinevate aktide (mitteisikustatud andmete vaba liikumise määrus, andmehaldusmäärus, avaandmete direktiiv) lihtsustamise ning liitmisega andmemäärusega;
- Üldises digikoondpakettis väljatoodud ühtse teavitusakna ettepaneku ja muude kübervaldkonnaga seotud seisukohad – seisukohad, mis on seotud küberintsidentide, isikuandmetega seotud rikkumiste kui ka muude samalaadsete juhtumite raporteerimiseks ühtse teavitusaknaga; siinses osas on seisukohad küberintsidentide taksonoomia kui ka Euroopa Parlamendi ja nõukogu määruse (EL) 2022/2554 lihtsustamise kohta seoses Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2022/2555;
- Üldises digikoondpakettis väljatoodud isikuandmete kaitse seisukohad – seisukohad, mis on seotud isikuandmete kaitse üldmääruse muudatustega;
- Tehisaru regulatsiooni koondpaketi seisukohad – seisukohad, mis on seotud EL tehisintellekti määruse muutmisega.

6.1. Euroopa digivaldkonna lihtsustamise koondpakettide üldised põhimõtted

6.1.1. Eesti toetab Euroopa digivaldkonna lihtsustamise koondpakettide raames ELi andmeõiguse reeglistiku lihtsustamist, et vähendada ettevõtjate ebavajalikku halduskoormust ja avaliku sektori töökoormust ning võimaldada andmeid turvaliselt jagada.

Selgitus: EL õigusaktidest tuleneva koormuse vähendamine on olnud Eesti kauaaegne prioriteet. Sellest johtuvalt toetame eesmärki ühtlustada ja lihtsustada kehtivaid andmereegleid, et luua selge ja tõhus õigusraamistik, mis võimaldab ettevõtetel ja avaliku sektori asutustel andmeid turvaliselt ning ulatuslikult jagada. ELi andmetöötlust reguleeriv õigusraamistik tuleb muuta selgemaks ja rakendamist tõhusamaks, vältides liigset regulatiivset koormust ja keerukust. Andmealaste õigusaktide ülevaatamisel on oluline päriselt keskenduda jõustamisele ning ennetada täiendava regulatsiooni tekkimist. Ebavajaliku halduskoormuse muutmisel tuleb arvestada nii ettevõtja vastavuskulusid kui aruandluskohustusi. Kaotada või vähendada tuleb ebavajalikku koormust, millel ei ole lisandväärtust.

6.1.2. Eesti peab oluliseks, et isikuandmete kaitse regulatsiooni muudatused ei too kaasa tehisaru kasutusele võtmise ja treenimise senisest keerukamaks muutmist (näiteks peab ka avalik sektor saama vajadusel tehisaru lahendusi treenida) ega muuda EL põhiõiguste hartas sätestatud põhiõiguste olemust. Õigusaktide muudatustega peavad komisjonilt kaasnema põhjalikud mõjuanalüüsid.

Selgitus: Eesti õigusriigina seisab selle eest, et õiguse muudatused ei ohustaks isikute põhiõigusi. Samas ei tohiks muudatused kaasa tuua innovatsiooni takistamist või selle elluviimise raskendamist. AI tehnoloogiana on samasugune nagu teised tehnoloogiad, mistõttu IKÜM andmetöötluse osas peaks rakenduma kehtivatel IKÜMi nõuetel. IKÜMi nõuete kitsendamine

või piiramine tehisaru kasutuselevõtu ning treenimise õigusliku aluse puhul ei ole põhjendatud. Näiteks ei ole põhjendatud tehisaru treenimist lubada vaid õigustatud huvi või nõusoleku alusel, mis saavad olla erasektoril õiguslikuks aluseks. Tuleb arvestada ka võimalusega, et avalik sektor soovib tehisaru treenida, kuid avalikul sektoril on sisuliselt võimatu või keelatud kasutada õigusliku alusena nõusolekut ja õigustatud huvi. Õiguslik alus andmete töötlemiseks tuleb valida igal AI tehnoloogiat kasutava toote ja teenuse puhul vastavalt sellest konkreetsest andmetöötlustest, mida tehakse.

Euroopa digivaldkonna lihtsustamise koondpakettides käsitletavate õigusaktide muutmisel tuleb leida kohane tasakaal erinevate põhiõiguste vahel. Eesti Euroopa Liidu poliitika aluspõhimõtete kohaselt peavad õigusaktide muudatustele eelnema põhjalikud mõjuanalüüsid. Antud juhul neid teostatud ei ole ja see raskendab ka muudatustega kaasnevate mõjude hindamist liikmesriigi tasandil. Muudatustega kaasnevate mõjude hinnang Euroopa Komisjoni poolt ei tohi käsitleda põhiõigusi valikuliselt, jättes mõju mõnele põhiõigusele (õigus isikuandmete kaitsele) sisuliselt hindamata. Mõjuhinnangu puudumise probleemi toome eelnõu läbirääkimisel riskikohana välja, ning soovime tulevikus näha põhjalikke mõjuanalüüse.

6.1.3. Eesti leiab, et Euroopa digivaldkonna lihtsustamise koondpakettide menetlemisel tuleb arvestada, et käsitletavad teemad on sisulised, erineva ajakriitilisuse ja mõjuga ning omavahel seotud. Seetõttu tuleb esmajärjekorras lahendada kõige ajakriitilisemad küsimused, millel on vahetu mõju õiguskindlusele ja regulatsiooni õigeaegsele rakendamisele, eelkõige suure riskiga tehisintellekti määruse rakendumistähtaja sätete kehtima hakkamise edasi lükkamine.

Selgitus: Ajakriitilisusel põhinev prioriseerimine aitab vältida rakendusprobleeme, vähendada regulatiivset killustumist ning tagada, et digiregulatsiooni muudatused on nii õigeaegsed kui ka sisuliselt kvaliteetsed. Selline lähenemine on vajalik õiguskindluse ja regulatsiooni rakendatavuse tagamiseks.

Euroopa digivaldkonna lihtsustamise koondpakettid koondavad mitmeid omavahel seotud teemasid, mis on erineva küpsusastme ja mõjuga. Nende üheaegne käsitlemine ilma ajakriitilisust arvestamata suurendab riski, et kõiki mõjusid ei hinnata piisavalt, eriti arvestades, et algatusega ei kaasnenud Komisjoni poolset mõjuhinnangut. See võib viia olukorrani, kus kiireloomulised küsimused lahendatakse liiga hilja või kiirustades, arvestamata kõiki vajalikke asjaolusid.

Ebaselgus ajaliselt kriitilistes küsimustes, nagu rakendamistähtajad, tekitab ebakindlust nii ettevõtjatele kui ka järelevalveasutustele. See raskendab investeringute ja vastavusmeetmete planeerimist ning võib kaasa tuua ebaühtlase kohaldamise liikmesriikides, kahjustades ühtse turu toimimist ja regulatsiooni usaldusväärsust. Näiteks on kehtiva AI määruse järgi suure riskiga tehisintellekti süsteemide kohaldamistähtaeg 2. august 2026, kuid on selge, et selleks ajaks ei ole valmis vajalikud juhised ja standardid. Seetõttu ei ole ettevõtjatel võimalik nõudeid täita ning järelevalvel nõuete täitmist kontrollida. Seega tuleks see küsimus lahendada esmajärjekorras.

Samas vajavad vähem ajakriitilised, kuid sisuliselt keerukad teemad rohkem aega läbimõeldud aruteluks. Kiirustades tehtud otsused võivad tekitada vastuolusid ja õiguslikke lünki ning

suurendada vajadust edasisteks parandusteks. Etapiviisiline käsitus aitab hoida fookuse esmavajadustel, säilitades samal ajal regulatsiooni kvaliteedi ja süsteemse kooskõla.

6.1.4. Eesti peab oluliseks, et kõigi Euroopa digivaldkonna lihtsustamise koondpakettide raames tehtavate muudatuste puhul läbivalt arvestatakse küberturvalisuse nõuetega ning need muudatused ei vähendaks küberturvalisuse taset.

Selgitus: Digivaldkonna lihtsustamise koondpakettide raames tehtavad muudatused lihtsustavad küberturvalisuse valdkonna toimimist (vt seisukoht 6.3.1. jj), kuid nende muudatuste käigus ei tohi tekkida olukord, kus edaspidiselt sobivaid ajakohaseid küberturvalisuse nõudeid ei järgita. Seetõttu on oluline, et koondpakettide raames tehtavad muudatused ei vähendaks küberturvalisuse taset, vaid need muudatused peavad aitama kaasa Euroopa Liidus soovitud ehk ühtlase taseme saavutamisele.

6.2. Üldises digikoondpaketi välja toodud andmeõiguse muudatused

6.2.1. Eesti toetab ühtse ELi andmemääruse loomist, mis koondab süsteemselt ja terminoloogiat ühtlustades avaandmete direktiivi, andmehaldusmääruse ning mitteisikustatud andmete vaba liikumise normid.

Selgitus: Andmehaldusmääruse, mitteisikustatud andmete vaba liikumise määruse, andmemääruse ja avaandmete direktiivi ühendamisel Euroopa andmeõiguse tähtsamaks üldnõuete regulatsiooniks luuakse ühtne andmemäärus, mis võimaldab erinevate andmeteemade vahel sünergiate ja seoste leidmist. Eesti peab oluliseks, et sellised seosed luuakse süsteemselt. Ülevaade seostest nii digikoondpaketi siseselt kui ka tehisintellekti määruse, AI rakendamise strateegia ning tulevase AI ja pilvetehnoloogia arendamise õigusaktiga aitab paremini tagada poliitikate omavahelist sidusust ja vältida dubleerimist. Põhjalikud mõjuanalüüsid ja seoste selgitused aitaksid kaasa ka algatuse suuremale läbipaistvusele.

Euroopa Komisjoni esitatud üldises digikoondpaketi ei ole andmehaldusmääruse, avaandmete direktiivi ja andmemääruse mõistete ühtlustamist veel piisavas mahus teostatud. Olulisim tuvastatud sõnavara ühtlustamise probleem koondpaketi on seotud dokumendi mõiste muutmisega. Kui kehtivas avaandmete direktiivis hõlmab dokumendi mõiste andmeid mistahes andmekandjal, (NB! Selline mõiste kattub ametlikele dokumentidele juurdepääsu Euroopa Nõukogu konventsioonis sätestatuga), siis üldine digikoondpaketi ettepanek eristab andmeid (digiandmekandjal) ja dokumente (mitte-digiandmekandjal). Samas on selles digikoondpaketi avaliku teabe kirjeldamist ja avalikustamist nõudvates punktides läbivalt jätkatud varasema avaandmete direktiivi ja andmehaldusmääruse sõnastuse “andmed või dokumendid” kasutamist. Seega nõuab andmemäärus uue definitsiooni alusel otseselt ka kõigi paberdokumentide kirjeldamist ja avalikustamist, kas avaandmete või piiratud andmete režiimi alusel (vastavalt senise avaandmete direktiivi või andmehalduse määruse mõistes), mis ei ole mõistlik, vajalik ega mõõdukas.

Näiteks ettepaneku artikli 32v lõige 1 näeb ette, et väärtuslikud andmestikud (mis on sama lõike alusel “andmed või dokumendid”) tehakse korduskasutamiseks kättesaadavaks masinloetavas vormingus sobivate API-de kaudu ning asjakohasel juhul ka hulgi allalaaditavana. Mitte-

digiaandmekandjal oleva dokumendi masinloetavas vormingus API-de kaudu avalikustamine ei ole loomulikult sisuliselt võimalik. Teise näitena on üldisesse digikoondpaketti kopeeritud a) seni avaandmete direktiivis olnud nõue avaliku sektori avaandmete avalikustamiseks riikide teabevärvates (digikoondpaketi artikkel 32s) ja b) andmehalduse määruse nõue avaliku sektori poolt hoitud piiratud teabe kirjeldamiseks ja nende kirjelduste avalikustamiseks riikide teabevärvates (digikoondpaketi artikkel 32aa). Seega on üldise koondpaketi erinevates osades kaks erinevas stiilis artiklit, mis sisuliselt nõuavad avaliku sektori asutustelt enamuse oma andmete kirjeldamist ja nende kirjelduste avalikustamist riiklikus teabevärvavas. Mõistlik oleks praeguse asemel esitada ühtne nõue peatükk VIIc üldosas, ehk sektsioon 1 järgmises ulatuses: avalik teave peab olema läbivalt kaardistatud ja kirjeldatud; teabe kirjeldused (ehk metaandmed) ja avaandmed peavad olema avalikustatud riiklikes teabevärvates (arvestades samas võimalike riigikaitseliste jm oluliste piirangutega, sh intellektuaalse omandi valdkonna regulatsioonist tulenevate nõuetega).

6.2.2. Eesti peab vajalikuks Euroopa Liidu tasemel väärtuslike andmetike kategooriate laiendamist, samas leiab Eesti, et avalikustada ei tohi andmetikke, mis seavad ohtu riigi sise- ja välisjulgeoleku. Täiendavate väärtuslike andmetike kategooria kehtestamisel tuleb arvestada mõjuga väiksematele liikmesriikidele.

Selgitus: Avaandmete direktiivi liitmisel andmemäärusega muutub see õigusakt määruseks ehk vahetult kohalduvaks ning täisharmoniseerivaks. Põhimõtteliselt Eesti toetab sellist õigusaktide liitmist (vt punkti 6.2.1), kuid seejuures peab hindama, milline on väärtuslike andmetike kättesaadavaks tegemisega seotud riskid ning nende mõju. Arvestada tuleb ka sellega, et Euroopa Liidus on erineva võimekusega liikmesriigid, kellel võivad olla erinevad mured. Avaandmete õiguse muutmisel peavad aluseks olema selged ja põhjendatud mõjude analüüsid. Eesti peab oluliseks Euroopa Liidu üleselt uute väärtuslike andmetike kategooriate kehtestamist. Samas uute väärtuslike andmetike kategooriate kehtestamisel ja täiendavate nõuete seadmisel peab analüüsima ja arvestama lisaks sotsiaalsele- ja majanduslikule kasule ka andmete kättesaadavaks tegemisest tingitud riske ning negatiivset mõju kõigi liikmesriikide julgeolekule, isikute põhiõigustele ning ettevõtete konkurentsivõimele.

6.2.3. Eesti leiab, et üldise digikoondpaketi ettepaneku tulemusena peab olema uues andmemääruses selgelt reguleeritud, millistel tingimustel võivad isikuandmed olla avaandmeteks. Isikuandmete avaldamine võib avaandmetena olla lubatud, kui andmesubjekt on selleks andnud oma nõusoleku või õigusega on ette nähtud andmete avalikustamine.

Selgitus: Toetame üldise digikoondpaketi eesmärki parendada avaliku teabe leitavust ja taaskasutatavust, sealhulgas avaliku teabe kasutuse parendamist privaatsustehnoloogiaid kasutades – see võimaldab teha teavet rohkem kättesaadavaks. Praegune olukord on loonud olulist õigusselgusetust: nt pole üheselt mõistetav, kuidas tuleks käsitleda isikuandmeid avaandmete kontekstis ning millised täpsed kohustused see seab nii teabevaldajale kui ka andmete kasutajatele. See ebamäärasus mitte üksnes ei raskenda avaandmete regulatsiooni rakendamist, vaid ohustab ka usaldust laiemasse andmeökosüsteemi.

Üldise digikoondpaketi artikkel 1 näeb ette, et avaandmete osa kohaldub nii isiku- kui isikustamata andmete suhtes. Samas ei ole selge, kuidas suhestuvad omavahel avaandmed ja

isikuandmed, sh millal võib isikuandmeid käsitleda avaandmetena. Kas isikuandmed on avaandmed üksnes siis, kui liidu või liikmesriigi õigusega on ette nähtud, et isikuandmete tagatakse ligipääs, ilma et selleks peaks teabenõuet esitama, või võivad olla avaandmed ka need isikuandmed, millele juurdepääsu pole liidu või liikmesriigi õigusega piiratud, kuid mille suhtes ka aktiivset avalikustamiskohustust õigusega pole ette nähtud.

Eesti leiab, et üldine reegel võiks olla see, et isikuandmete avaldamine võib avaandmetena olla lubatud, kui andmesubjekt on selleks andnud oma nõusoleku või seadusega on ette nähtud andmete avalikustamine. Kuivõrd isikuandmete avalikustamise kaudu kättesaadavaks tegemine määramata isikute ringile on oluline eraelu riive, siis tuleb seadusega sellise riive ette nägemisel eelnevalt anda hinnang riive lubatavusele, sh proportsionaalsusele.

6.2.4. Eesti toetab privaatsustehnoloogiate laialdasemat kasutamist erinevate andmete kaitseks, sealhulgas tuleb anda Komisjoni juhised selliste tehnoloogiate kasutamise võimaluste ja kriteeriumite kohta. Eesti ei näe vajadust privaatsustehnoloogiate kasutusvõimaluste juhised anda EL õigusaktiga.

Selgitus: Näiteks tehisaru regulatsiooni koondpakett näeb ette, et eriliigiliste isikuandmete töötlemisel kallutatuse avastamiseks ja leevendamiseks tuleb kohaldada tiptasemel turva- ja privaatsuse säilitamise meetmed, sealhulgas pseudonüümist (uus lisatav AI määruse artikkel 4a lg 1 punkt b). Samuti on kohustus kaitsemeetmeid kasutada tehisintellekti arendamiseks ja käitamiseks vajalikul andmetöötlusel (uus lisatav IKÜM art 88c). Need sätete näited on oma olemuselt privaatsuskaitsetehnoloogiad.

Tehnoloogia arenedes on ettevõtetele üha suuremaks väljakutseks kujunenud isikuandmete ja muude andmete vahel erisuse tegemine, kuna seni on puudunud selged tehnilised kriteeriumid. Seepärast toetame privaatsustehnoloogiate laiemat kasutamist. Toetame ettepanekut, et liikmesriikide üleselt täpsustatakse andmete pseudonüümimisega seotud meetmeid ja kriteeriume. Selline harmoneerimine tagab suurema kindluse ja vähendaks õiguslikku ebakindlust nii ettevõtetele kui ka pädevatele asutustele ning aitab maandada ebaõige klassifitseerimisega seotud riske. Teisalt aitavad privaatsustehnoloogiate laiem rakendamine ja õigusselguse loomine tagada andmesubjektide kaitset ning järelevalveasutuste praktikat antud teemas ühtlustada. Samas liikmesriikide ülesed juhised ei peaks olema piiritletud vaid andmete pseudonüümimisega, vaid võimalus peaks ka olema teiste privaatsustehnoloogiatega seotud meetmete ja kriteeriumite täpsustamist.

6.2.5. Eesti toetab ettepanekut kaotada nõue andmevahendusteenuste teavitamiseks ning leevendada andmevahendusteenusele kohalduvaid nõudeid täiendavate lisateenuste osutamise lubamisega.

Selgitus: Kehtivas andmehaldusmääruses on andmevahendusteenuse osutajal kohustus esitada teatis siseriiklikule pädevale asutusele (vt andmehaldusmääruse art 11). Üldises digikoondpaketi soovitakse andmevahendusteenused muuta vabatahtlikuks registreerimiseks. See tähendab seda, et teatist ei oleks vaja esitada (vt üldise digikoondpaketi muudatust artiklis 32e lg 1). Kehtivas määruses on ka jäigalt piiritletud lisateenused, mida andmevahendusteenusega seoses võib osutada (vt andmehaldusmääruse art 12 punkt e). Üldises

digikoondpaketi jäetakse osutatavate lisateenuste valik lahtiseks (vt üldise digikoondpaketi muudatust artiklis 32c punktid c ja d).

Eesti on varasemalt toetanud lähenemist, mille kohaselt oleks andmevahendusteenuse osutamine tegevusala, millele kohaldub vabatahtlik registreerimisvõimalus, kuid kehtiva määruse järgi tuleb esitada majandustegevuse teatis. Samuti on eelnõus leevendatud andmevahendusteenust osutavatele ettevõtetele kohalduvaid nõudeid seoses täiendavate lisateenuste osutamise lubatavusega (näiteks: võimalus osutada lisaks andmevahendusele ka andmete rikastamise ja analüüsi teenuseid). Eesti toetab seda lähenemist, kuivõrd selline nõuete leevendamine tõstab eeldatavalt ka Eesti ettevõtete huvi kohalikul ja liidu turul andmevahendusteenuseid pakkuda.

6.2.6. Eesti toetab ettepanekut muuta ELi andmemäärust nii, et avalikul sektoril on õigus saada erasektorilt hädaolukorras andmeid, kuid peab oluliseks, et selle sätte rakendamisel arvestatakse inimeste põhiõigustega ning liikmesriikides kohaldatakse seda ühtsetel alustel. Andmete edastamisel tuleb eelistada isikustamata andmete edastamist või kui see pole võimalik, siis tuleb kaaluda sobivate privaatsuskaitsetehnoloogiate kasutamist.

Selgitus: Kehtiva andmemääruse artikli 14 kohaselt on andmevaldajatel kohustus teha avalikule sektorile andmed kättesaadavaks erakorralise vajaduse tõttu. Erakorralist vajadust ei ole määruuses 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 asjaomasel 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.

Üldise digikoondpaketi ettepaneku kohaselt lisatakse andmemäärusesse 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 sätte 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. Eesti leiab, et isikuandmete edastamisel tuleks alati kaaluda võimalike privaatsuskaitsetehnoloogiate, sh pseudonüümimise, kasutamist.

Kuigi üldise digikoondpaketi väljatoodud ettepanekuga eemaldatakse kehtivast andmemäärusest 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 (ing k *the 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 ühtsetel alustel. Nende osas võiks kõik liikmesriigid jälgida sarnast praktikat, vältimaks liikmesriigiti erinevaid tõlgendusi, mis hetkel tuleks hädaolukorra andmeid jagada ja millal mitte.

6.2.7. Eesti toetab ettepanekuid Euroopa Andmeinnovatsiooninõukogu mandaadi laiendamiseks, tugevdades nõukogu rolli andmepoliitika ja -korralduse, piiriülese andmevahetuse ja liiduülese tehnilise koostöö koordineerimisel.

Selgitus: Euroopa Andmeinnovatsiooninõukogu (ing. k European Data Innovation Board, EDIB) tänane mandaat on nõustada ja toetada Euroopa Komisjoni ELi andmehalduse ühtlustamisel. Nõukogu aitab kujundada ühiseid tavaid, juhiseid ja standardeid andmete taaskasutamiseks, andmevahendamiseks ja andmealtruismiks, edendab turvalist, koostalitlusvõimelist ja piiriülest andmete jagamist, toetab ühtsete Euroopa andmeruumide loomist ning aitab tagada andmete kaitse, küberturvalisuse, ausa konkurentsi ja siseturu toimimise nii ELis kui ka rahvusvahelises kontekstis. Detailsem tänane mandaat on andmehalduse määruse artiklis 30.

Üldises digikoondpaketi teeb Euroopa Komisjon ettepaneku andmeõiguse osas laiendada selle nõukogu mandaati, mh tugevdades tema rolli andmepoliitika, -korralduse, piiriülese andmevahetuse ja liiduülese tehnilise koostöö koordineerimisel. Eesti toetab Euroopa Andmeinnovatsiooninõukogu mandaadi laiendamist ettepanekus esitatud pädevuste piires. Samuti laiendatakse nõukogu liikmete hulka – lisaks hetkel andmehalduse määruuses ette nähtud andmevahetuse pädeva asutuse osalusele (Eestis: AKI), on nõukogus edaspidi võimalik osaleda ka liikmesriikide “andmeküsimustes pädevad osapooled” (Eestis: JDM, Statistikaamet, RIA).

Eesti toetab nimetatud muudatust, kuivõrd see võimaldab liikmesriikidel (sh Eestil) osaleda teemakohastes aruteludes vastavalt, kas tehnilise, strateegilise, poliitilise või õigusliku ekspertisiga (siiani on osalemine olnud piiratud andmekaitse vaatega) ja seeläbi tõsta nõukogu töö ja liiduülesete kokkulepete kvaliteeti.

6.2.8. Eesti toetab ettepanekut tunnistada kehtetuks veebipõhiste vahendusteenuste määrus (EL) 2019/1150. Õigusselguse tagamise eesmärgil toetame seda, et selle määruse teatud (digikoondpaketi väljatoodud) sätted kehtivad kuni neile viitavate EL õigusaktide muutmiseni, seda tähtajaga hiljemalt 31. detsember 2032.

Selgitus: Määrus (EL) 2019/1150, mis käsitleb õigluse ja läbipaistvuse edendamist veebipõhiste vahendusteenuste ärikasutajate jaoks (edaspidi P2B määrus) jõustus 2020. aastal. Euroopa komisjoni hilisem mõjuhindamine ja Eesti kogemus on näidanud määruse nõuete piiratud mõju, mida kinnitab muuhulgas veebipõhiste vahendusteenuste ärikasutajate madal kaebuste arv. Hilisem EL digiteenuste määrus (DSA) sisaldab nõudeid, mis kattuvad olulisel määral P2B põhisätetega. Mõlemad määrused seavad infoühiskonna vahendusteenuse osutajatele kohustused seoses teenusetingimuste läbipaistvuse; teenuse piiramise, peatamise ja lõpetamise tingimuste; sisu järjestuse läbipaistvuse ning ettevõtte sisese kaebuste menetlemise süsteemi loomise ja haldamisega. P2B määrus seab küll kohati täpsemad nõuded kohustuste kohaldumisele suhtes ärikasutajatega, kuid leiame, et nende nõuete lisandväärtus on kokkuvõttes pigem madal.

Lisaks on P2B määruse kehtimise järgselt jõustunud digiturgude määrus (DMA), mille eesmärgiks on tagada digiturgudel nn. pääsuvalitsejate teenuste ärikasutajatele võrdsemad konkurentsitingimused. Eelmainitud asjaolusid arvestades leiame, et DSA ja DMA tagavad piisava läbipaistvuse ja tasakaalustatuse veebipõhiste vahendusteenuste osutajate ja ärikasutajate vahelistes suhtes, mistõttu toetame ettepanekut muuta P2B määrus kehtetuks. Eraldi P2B määruse kaotamine vähendab ka võimalusi järelevalvealasteks konfliktideks tulenevalt P2B ja DSA määruste kohati erinevatest järelevalvemudelitest ning toetab eesmärki muuta EL õigusraamistik ühtlasemaks ja selgemaks. Õigusselguse eesmärgil saame toetada määruse valitud sätete pikemat kehtimist kuni nendele viitavate EL õigusaktide muutmiseni, seda lõpptähtajaga 31. detsember 2032.

6.3. Üldises digikoondpaketi väljatoodud ühtse teavitusakna ettepaneku ja muud kübervaldkonna seisukohad

6.3.1. Eesti toetab ettepanekut luua küberintsidentide, isikuandmetega seotud rikkumiste kui ka muude samalaadsete juhtumite raporteerimiseks ühtne teavitusaken. Ühtse teavitusakna loomisel on oluline tagada, et intsidentidest raporteerimine on turvaline, juurdepääsetav vaid vajalikele osapooltele, ei tõsta liikmesriikide kulusid ja kasutab ära olemasolevaid liikmesriikide lahendusi ning praktikaid. Ühtse akna loomine peab vähendama ka ettevõtjate halduskoormust ja kulu Euroopa Liidu eelarvele. Ennekoike tuleb lisaks teavituste sisu ühtlustamisele digikoondpaketi raames ühtlustada ka erinevates õigusaktides olevate teavituste esitamise tähtaegu.

Selgitus: Eesti toetab küberintsidentide raporteerimiseks ühtse teavitusakna ehk SEPi loomist. Mitmed õigusaktid (NIS2 direktiiv, IKÜM, eIDAS määrus, CER direktiiv, DORA määrus, piiriüleste elektrivoogude küberturvalisust käsitlevaid sektoripõhiseid norme sisaldav võrgueeskiri nimetusega NCCS määrus, lennunduse valdkonna määrused ehk komisjoni määrused (EL) 2023/203 ja 2022/1645, e-privatsuse direktiiv ja CRA määrus) kohustavad intsidentidest/ juhtumitest teavitama asjakohast pädevat asutust. Tegemist on nende õigusaktide järgijatele (avalikust ja erasektorist) dubleeriva kohustusega, kui samast juhtumist tuleb teavitada mitut asutust, kasutades erinevaid vorme. Lahendusena nähakse ühtset teavitamise akent ehk SEPi, mis võimaldab rakendada põhimõtet “teavita üks kord ja jaga mitme osapoolega”. Ettepaneku kohaselt SEPi arendab välja ja haldab EL Küberturvalisuse Amet (ENISA).

Üldises digikoonpaketi ettepanekus on märgitud, et SEPiga seonduvalt muudetakse ainult IKÜMi, e-privatsuse direktiivi, NIS2 direktiivi ja CER direktiivi. Ülejäänud EL õigusaktide puhul on ette nähtud, et EL õiguse alusel kehtestatavates rakendustähtaegades või delegeeritud

määrustes tagatakse ühtse teavituse vormi kasutusele võtmine. Samas ei ole ettepanekus märgitud, kas ning mil määral oleks vaja muuta ka direktiivi (EL) 2016/680 (reguleerib isikuandmete töötlust õiguskaitsealises eesmärgil) või ka mõnda muud õigusakti, millel on sarnasusi sinise teemaga (nt AI määrus).

Eesti jaoks on oluline, et loodav SEP on turvaline, sh et sellele saavad juurdepääsu vaid vajalikud osapooled. Näiteks peab olema selge, kas ning mil määral peaks ENISA saama SEPi kaudu edastatavale infole juurdepääsu - seda ka olukorras, kus SEPi arendajaks on ENISA. Juurdepääs SEPi kaudu edastatavale infole peab lähtuma teadmiskajaduse põhimõttest. Eesti seisukohtade koostamise hetkel ei ole veel selge, millised saavad olema SEPi tehnilised tingimused ja nõuded. Seetõttu ei ole teada, kas näiteks SEPi loomisega tekib ENISA juurde justkui keskne andmebaas või andmehoidla, mis sisaldab kõiki SEPi kaudu edastatud teavitusi. Kui selline andmebaas tekib (kuna praktikas on ilmselt vaja päringud vastu võtta, valideerida, talletada intsidentide info, et seda edasi saata/töödelda), on tegemist äärmiselt tundlikku infot sisaldava andmebaasiga. See omakorda loob võimaliku keskse sihtmärgi tekkeks, mille kompromiteerimine võib avaldada äärmiselt laiaulatuslikku mõju kogu EL siseturvalisusele. Vajalik on luua usaldus, et loodud süsteem on turvaline, ettevõtte ja kodanikud teavad, kuidas nende andmeid kasutatakse ja millised meetmed on kasutusele võetud, et turvalisus oleks tagatud. Vastasel juhul võib tekkida situatsioon, kus intsidentide raporteid ei esitata põhjusel, et süsteemi kui tervikut ei usaldata. SEPi loomisel tuleb ära kasutada võimalikul määral olemasolevaid Euroopa lahendusi ja praktikaid. Eelkirjeldatud selgituse tõttu tuleks SEPi loomisel kasutada ennekõike hajutatud arhitektuurilist lahendust, mis vähendaks tsentraalse andmebaasi või andmehoidla tekkimisega seotud riske. SEPi tekitamisel tuleb ka tagada, et see ei tekitaks liikmesriikidele liigset kulu.

Esitatud ettepanekus on selgitatud, et SEPi loomise raames tegeletakse mh ka sellega, et kui ühest juhtumist teavitada mitme õigusakti alusel, siis eri õigusaktide alusel küsitav info ja andmed oleksid ühesugused, kuid ettepanekus ei ole märgitud, kuivõrd tuleks ühtlustada eri EL õigusaktides ette nähtud tähtaegu. Küberintsidentide teavitamisele kehtivad nõuded, et esmane teavituse intsidentidele tuleb teha üldreeglina 24 tunni jooksul ja intsidentide teade tuleb teha hiljemalt 72 tunni jooksul. Isikuandmete kaitse valdkonnas toimuva isikuandmete nõuete rikkumisest tuleb teavitada 72 tunni jooksul ning pärast digiõnnetuse ettepanekus tehtavat muudatust tuleb see teha 96 tunni jooksul. Tolle muudatusega kaotatakse ära oluline varajase sekkumise mehhanism. Kõrge riskiga intsidentide puhul tähtsaja pikendamine 96 tunnini võib suure riskiga intsidentide korral olla iga lisapäev kahju piiramisel kriitilise tähtsusega. Samuti tuleb arvestada ka asjaoluga, et kui mingi juhtum on näiteks isikuandmetega seotud küberintsident, siis tuleb samast juhtumist teavitada pädevaid asutusi mitmel erineval ajahetkel. See kõik tekitab omakorda segadust – seda isegi ka siis, kui ettepanekus kirjeldatud SEP luuakse.

Komisjoni 24. juuni 2013. aasta määruse (EL) nr 611/2013 meetmete kohta, mida kohaldatakse eraelu puutumatust ja elektroonilist sidet käsitleva Euroopa Parlamendi ja nõukogu direktiivi 2002/58/EÜ kohaselt isikuandmetega seotud rikkumiste teatamise suhtes, kohaselt on üldkasutatava elektroonilise sideteenuse osutajal kohustus teatada isikuandmetega seotud rikkumistest. Nimetatud määruse kohaselt tuleb rikkumisest teavitada andmekaitse järelevalveasutust hiljemalt 24 tunni jooksul pärast rikkumise tuvastamist. Kindlasti tuleb selgitada, kuidas nimetatud määrus edaspidi ettepaneku muudatustega kooskõlas oleks.

Samuti märgime, et lahendus, kus ühtne teavitusekanal luuakse ENISA juurde ning ENISA saadab kogu vajamineva info edasi liikmesriikide pädevatele asutustele, ei pruugi olla jätkusuutlik. See võib pikendada ajakriitilises olukorras intsidentide käsitlemise aega. Kuna ENISA alles paneb paika konkreetseid meetmeid ja nõuded ühtsele teavitusekanale, siis ei ole seletuskirja koostamise

hetkel võimalik pakkuda välja alternatiivi, kuidas tagada jätkusuutlikkus. See selgub, kui ENISA on vastavad meetmed ja nõuded koostanud.

Kuigi üldise digikoondpaketi raames on võetud eesmärgiks ühtlustada nende teavituste sisu, siis tuleks muuhulgas ühtlustada ka teavituste saatmise tähtaegasid, mis on erinevates õigusaktides erinevalt sätestatud. Eesti seisukohtade ettevalmistamise käigus ei olnud võimalik analüüsida, mis oleks kõige sobivaim tähtaeg. Tolle ühtlustatud tähtaja puhul tuleb arvestada mitmete aspektidega, st nii teavituste esitajate (nii erasektorist kui avalikust sektorist) ja mõjutatud osapoolte (nt küberintsidendist mõjutatud partnerettevõtte või andmelekkega seotud andmesubjekti) huvidega kui ka konkreetset juhtumit lahendavate pädevate asutuste vajadustega.

6.3.2. Eesti teeb ettepaneku, et ühtse teavitusaknaga seondult ühtlustatakse küberintsidentide taksonoomiat, lisades vastava ülesande ELi ameti ENISA põhiülesannete hulka. Eesti leiab, et ENISA koostatud küberintsidentide taksonoomia kasutamine peab olema kohustuslik liidu-üleselt.

Selgitus: Esitatud seisukoht ei ole Euroopa digivaldkonna lihtsustamise koondpakettides endas kirjeldatud teemadest, vaid tegemist on praktikast tõusetunud vajadusega, mille puhul on vaja selgus saada. Kuna SEP on tehniline lahendus, mis peaks ka vahetama teavet riiklike teavituskanalitega, tekib suurendatud vajadus ühtse taksonoomia järele. Arvestades, et teavitatavad teemad erinevad riigiti ning teavitused edastatakse kohalikes keeltes, on ühtse ja läbimõeldud taksonoomia loomine eriti oluline. ELi küberintsidentide taksonoomia on Euroopa Liidus kasutatav ühine raamistik küberintsidentide kirjeldamiseks ja liigitamiseks. Selle eesmärk on tagada, et erinevad osapooled (EL asutused ja institutsioonid, liikmesriigid kui ka riikides asuvad isikud või üksused) lähtuksid küberintsidentide määramisel ja käsitlemisel samast käsitlusest. Eesti teeb ettepaneku, et vastava taksonoomia ülesande saab ENISA, kes on samalaadseid taksonoomiaid ka varem koostanud.

Ühtlustatud küberintsidentide taksonoomia kasutamine ELi üleselt ei juhtu niisama - mistõttu on vaja tekitada ka EL õigusesse nõue, et selle taksonoomia kasutamine on kohustuslik ELi üleselt. Selleks tuleks digiomnibussi muudatuste hulgas teha vastav muudatus ka näiteks NIS2 direktiivis või mõnes muus asjakohases EL õigusaktis.

6.3.3. Eesti toetab seda, et küberintsidentidest teavitamise ühtse teavitusakna loomine, arendamine ja haldamine muutub ELi ameti ENISA üheks põhiülesandeks. Eesti teeb ettepaneku majutada ühtne teavitusaken ELi ameti eu-LISA juures Eesti peakontori infrastruktuuris, lisades vastava ülesande eu-LISA põhiülesannete hulka.

Selgitus: Seisukoht on seotud SEPi tehnilisema rakendamisega. Eesti huvi ei ole suunatud SEPi sisulisele muutmisele, vaid selle tehnilise lahenduse kujundamisele ja võimalikule paiknemisele. Ettepanekus on märgitud, et SEPi loomine, arendamine ja haldamine saab olema ENISA ülesanne. See on Eesti hinnangul sobiv, kuid puudub selgus, kus taolist tehnilist lahendust majutatakse. Eestile teadaolevalt ei ole ENISAl hetkel endal taolist võimekust, et SEPi majutada. Lisaks ENISALE on loodud eraldi EL asutusena Vabadusel, Turvalisusel ja Õigusel Rajaneva Ala Suuremahuliste IT-süsteemide Operatiivjuhtimise Euroopa Liidu Amet ehk eu-LISA, mille ülesandeks on ELi justiits- ja siseasjade valdkonna suurte infosüsteemide ja sidetaristu arendamine ja haldamine. Eesti leiab, et ühe võimalusena võiks kaaluda SEPi tehnilise lahenduse majutamist Eestis eu-LISA peakontori infrastruktuuris, mistõttu teeb Eesti ettepaneku, et SEPi majutamine võiks toimuda eu-LISAs eeldusel, et see takistaks eu-LISA olemasolevate ülesannete täitmist. Selleks tuleb täiendada eu-LISA mandaati ja ülesandeid, kuna eu-LISA praegused ülesanded (vt Euroopa Parlamendi ja nõukogu määrust (EL) 2018/1726) on seotud sise- ja

justiitsvaldkonnaga ehk tema ülesanded ei hõlma siseturuga seotud ülesandeid. Eesti soovib, et SEPi majutamine toimuks sellisel juhul eu-LISA Eesti peakontori infrastruktuuris. See valik tugevdaks Eesti rolli Euroopa digitaalse ja küberjulgeoleku arhitektuuris ning looks pikaajalist strateegilist väärtust. See tähendab nii digikompetentsi kasvu, tugevamat rolli EL operatiivses võrgustikus kui ka laiemat julgeoleku- ja majanduslikku mõju, sh EL asutuste ja töötajate suuremat kohalolu Eestis. SEPi tehnilise lahenduse majutamise võimekuse loomine eu-LISAsse looks eeldused majutada ka teisi sarnaseid ELile strateegiliselt olulisi andmebaase ja IT lahendusi eu-LISA juures. Samuti toetaks ENISA ja eu-LISA koostöös lahendus EL agentuuride vahelist sünergiat, võimaldades kasutada ära mõlema ameti tugevusi ja kogemusi siseturvalisuse tagamisel..

Euroopa Komisjon avaldas 26.01.2026. a eu-LISA välise hindamise teatise⁷, milles leiti, et agentuuri volituste ja põhiülesannete muutmata jätmine käesolevas etapis võiks praegu paremini aidata eu-LISA-l täita tulemuslikult ja tõhusalt oma pooleliolevaid ülesandeid. Teatise kohaselt peaks eu-LISA seadma prioriteediks korraldusliku stabiilsuse ja strateegilised talitluslikud täiustused. Seega, kui Eesti seisukoht ei leia toetust siinsete ettepanekute arutelu käigus, võib seda ettepanekut esitada tulevaste õiguslike muudatuste aruteludes.

6.3.4. Eesti teeb ettepaneku finantssektori digitaalset tegevuskerksust sätestavat määrust ehk DORA määrust ja vajadusel ka NIS2 direktiivi lihtsustada nii, et DORA määruse kohaldamisalas olevad finantssektori ettevõtjad ei tohi nõuda DORA määruse turvalisuse nõuetele vastavust kolmandast isikust IKT-teenuste osutajatelt, kes vastavad NIS2 direktiivis ja selle alusel kehtestatud nõuetele.

Selgitus: Esitatud seisukoht ei ole koostatud ajendatuna Euroopa digivaldkonna lihtsustamise koondpakettides kirjeldatud teemadest, vaid tegemist on praktikast tõusetunud vajadusega, mille puhul on vaja selgus saada ning millele juhtis tähelepanu ka üks turuosalisi esindav liit.

DORA määruse (määrus (EL) 2022/2554) kohaldamisalas olevad üksused on vabastatud NIS2 direktiivi küberturvalisuse nõuetest. Samas on praktikas ka neid IKT-teenuste osutajaid, kes on NIS2 direktiivi kohaldamisalas, kuid samal ajal osutavad nad IKT-teenuseid finantssektori üksustele, kellele kohaldub DORA määrus. NIS2 direktiivis on nende üksuste kohta kasutatud sõnastusi “hallatud teenuse osutaja” ja “hallatud turbetaenus osutaja”, mis on küberturvalisuse seadusesse üle võetud terminitena vastavalt “haldusteenuse osutaja” ja “infoturbetaenus osutaja”. DORA määruses on nende üksuste kohta kasutatud sõnastust “kolmandast isikust IKT-teenuse osutaja”.

DORA määrus ei kehtesta kolmandast isikust IKT-teenuse osutajatele üldist ja otsest kohustust olla iseseisvalt vastavuses DORA määruse nõuetele samal viisil nagu finantssektori ettevõtjatele. Küll aga vastavalt DORA määrusele, kui kolmandast isikust IKT-teenuse osutaja osutab teenuseid DORA määruse kohuslasele (loetletud DORA määruse artikli 2 lõike 1 punktides a–t ehk finantssektori ettevõtjale), siis loetakse neid teenuseid osaks finantsasutuse ökosüsteemist ja/või finantsasutuste poolt pakutavate teenuste lahutamatuks osaks. Seetõttu eeldatakse kolmandast isikust IKT-teenuse osutajalt tegutsemist kooskõlas DORA määruse loogika ja nõuetega.

DORA artikkel 28 lg 5 esimene lause viitab, et "finantssektori ettevõtja võib sõlmida lepingu vaid sellise kolmandast isikust IKT teenuse osutajaga, kes vastab asjakohastele

⁷ [https://ec.europa.eu/transparency/documents-register/detail?ref=SWD\(2026\)980&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2026)980&lang=en)

infoturbestandarditele”. Tegemist on finantssektori ettevõtja hoolsuskohustusega enne kolmandast isikust IKT-teenuse osutajaga lepingulistesse suhetesse astumist.

Kohustused kolmandast isikust IKT-teenuse osutajatele tulenevad aga DORA määruse artiklist 30, mis sätestab minimaalsed kohustuslikud lepingulised elemendid, milles finantssektori ettevõtja ja kolmandast isikust IKT-teenuse osutaja peavad kokku leppima. DORA määruse artikli 30 eesmärk on võimaldada finantssektori ettevõtjatel täita oma regulatiivseid kohustusi, tagades lepinguliste mehhanismide kaudu kontroll IKT-riskide üle ka väliste teenusepakkujate puhul. Selle saavutamiseks nõuab DORA määruse artikkel 30 kolmandast isikust IKT-teenuse osutajatega sõlmitavatelt lepingutelt detailset reguleerimist teenuse sisule, turbenõuetele, intsidendihaldusele, auditi- ja järelevalveõigustele, allhankimisele ning teenuse lõpetamise ja asendamise mehhanismidele.

Samas on oluline rõhutada, et NIS2 direktiiv juba kohustab NIS2-kohuslasi rakendama terviklikku küberturbe ja riskijuhtimise raamistikku, sealhulgas tehnilisi ja organisatsioonilisi turvameetmeid, intsidendihaldust, tarneahela riskide juhtimist ning juhtkonna vastutust. Sellekohased täpsemad nõuded on sätestatud NIS2 direktiivi artikli 21 lõike 5 alusel antud komisjoni rakendusmääruses (EL) 2024/2690. NIS2 direktiivi kohaldamisalas olevad üksused alluvad lisaks riiklikule järelevalvele ja sanktsioonimehhanismidele, mis tagavad kõrge ja õiguslikult siduva kaitsetaseme. Seega on NIS2 direktiivi eesmärgid ja sisuline fookus kooskõlas DORA määruse artikli 30 aluseks oleva riskijuhtimise loogikaga.

Praktikas ei ole DORA määruse artikli 30 nõuded NIS2 direktiivi kohaldamisalas olevate üksuste jaoks suunatud uute riskide maandamisele, vaid eeldavad juba kehtivate NIS2 direktiivi raamistike dubleerimist ja ümberstruktureerimist vastavalt iga finantssektori ettevõtjate lepinguliste vajaduste järgi. See väljendub mitmekordses dokumenteerimises, kliendipõhistes auditites, erinevates raporteerimisnõuetes ning lepingulises keerukuses, mis ei suurenda küberturvalisuse ega teenuse vastupidavuse tegelikku taset, kuid kasvatab ebamõistlikult kolmandast isikust IKT-teenuse pakkuja halduskoormust ja kulusid.

Seega tekitab eelkirjeldatud topelt nõue DORA määruse kohastele kolmandast isikust IKT-teenuse osutajatele topelt nõudeid. Seetõttu tuleks ettevõtjate halduskoormuse vähendamiseks ja regulatsioonide lihtsustamiseks muuta DORA määrust ja vajadusel ka NIS2 direktiivi viisil, et DORA määruse kohaldamisalas olevad finantssektori ettevõtjad ei tohi nõuda DORA määruse turvalisuse nõuetele vastavust kolmandast isikust IKT-teenuste osutajatelt, kes vastavad NIS2 direktiivis ja selle alusel kehtestatud nõuetele.

Kui vastav Eesti seisukoht ei leia toetust siinsete ettepanekute arutelude käigus, siis võib seda ettepanekut esitada tulevaste küberturvalisuse või finantsvaldkonnas tehtavate õiguslike muudatuste käigus.

6.4. Üldises digikoondpaketi väljatoodud isikuandmete kaitse üldmääruse muutmise seisukohad

6.4.1. Eesti ei toeta ettepanekut reguleerida isikuandmete kaitse üldmääruses tehisaru kui ühte tehnoloogilist lahendust. Eesti on seisukohal, et säilima peab IKÜM-i tehnoloogianeutraalsuse põhimõte. Samas ei tohi digikoondpaketi muudatused kaasa tuua tehisaru kasutusele võtmise ja treenimise senisest keerukamaks muutmist. Tehnoloogiaarenduseks isikuandmete töötlemine peab olema võimalik kõigil IKÜM-i andmetöötamise õiguslikel alustel. Eesti toetab, et tehnoloogia arendamiseks, mis on hõlmatud teadusuuringu mõistega, peab asjakohaste kaitsemeetmete rakendamisel olema

lubatud töödelda ka eriliiki isikuandmeid. Eesti leiab, et õiguskindluse suurendamiseks tuleb IKÜM-is täpsustada laiemalt teadusuuringuga (sh tehnoloogiaarendusega) seonduvaid kaitsemeetmeid, mis omakorda ei tohi olla andmetöötlust liiga piiravad. Tehnoloogia arendamine ja käitamine on erinevad töötlemistoimingud ja vajavad Eesti hinnangul eraldiseisvat andmetöötluse õiguslikku alust.

Selgitus: Muudatusettepanekuga plaanitakse täiendada IKÜMi tehisaru puudutava regulatsiooniga (kavandatud IKÜM artikkel 88c, seotud seisukohapunktiga 6.5.5.). Silmas tuleb aga pidada, et tehisaru puhul on tegemist ühega väga paljudest tehnoloogilistest süsteemidest, seega ei oleks IKÜM enam tehnoloogia neutraalne. Eesti ei toeta üksiku tehnoloogilise lahenduse reguleerimist määruses. Tehisaru tehnoloogiana on samasugune nagu teised tehnoloogiad, mistõttu isikuandmete töötlemisele tehisarus peaks rakendama kas kehtivat IKÜM-i nõuetel või kehtestades IKÜM-iga täiendavaid kaitsemeetmeid mitte üksnes tehnoloogia arendamiseks ja kasutamiseks (mis on juba hõlmatud teadusuuringu mõistega) vaid ka laiemalt teadusuuringute kontekstis. IKÜM peaks ette nägema minimaalsed kaitsemeetmed teadusuuringus isikuandmete töötlemiseks (näiteks võiks olla kaitsemeetmeteks olla privaatsustehnoloogiate kasutamine). See aitaks lihtsustada ka teadlaste vahelist rahvusvahelist koostööd. Samuti tuleb jätta paindlikus täiendavate kaitsemeetmete sätestamiseks EL-i ja riigisisese õigusega (eelkõige võttes arvesse vajadust teatud juhtudel teadusuuringu tegemise tingimuseks ette näha ka eetikakomitee hinnangu saamine).

Samas ei tohiks muudatused kaasa tuua innovatsiooni takistamist või selle elluviimise raskendamist. IKÜMi nõuete kitsendamine või piiramine tehisaru arendamise ning käitamise õigusliku aluse puhul ei ole põhjendatud (ei järgita IKÜMis olevat tehnoloogia neutraalsuse põhimõtet). Nt ei ole põhjendatud tehisaru treenimist lubada vaid õigustatud huvi või nõusoleku alusel. Tuleb arvestada ka võimalusega, et avalik sektor soovib tehisaru treenida. Õiguslik alus andmete töötlemiseks tuleb valida iga tehisaru tehnoloogiat kasutava toote ja teenuse puhul vastavalt sellest konkreetsest andmetöötlusest, mida tehakse. Andmetöötlejatele ei tohi luua ka petlikku kujutlust justkui oleks liidu seadusandja ühe tehnoloogia arendamise ja toimimise puhul õigustatud huvi hinnangu juba ette ära määranud ning muud üldmääruses toodud andmetöötluse õiguslikud alused on tehisaru arendamiseks välistatud.

Muudatusega luuakse tehnoloogia arenduseks (ettepanekutes tehisaru) ja käitamiseks isikuandmete töötlemiseks õiguslik alus. Toetame ettepanekut, et rakendades asjakohaseid kaitsemeetmeid (nt privaatsustehnoloogiaid), peaks olema lubatud ka eriliiki isikuandmete töötlemine teadusuuringute eesmärgil, sh tehnoloogiaarenduseks. Silmas peab pidama, et kuna kaitsemeetmed on pidevalt ajas muutuvad, siis kindlaks määratud loetelu ei ole võimalik ette näha. Eesti on seisukohal, et eriliiki isikuandmete töötlemine peab olema lubatud ainult tehnoloogia arendamiseks, arendatud tehnoloogia rakendamiseks (nt teenuse pakkumiseks) peab andmetöötlusel olema omaette õiguslik alus. Eesmärgipiirangu põhimõte peab jääma kehtima - igaks uuel eesmärgil andmetöötluseks peab olema omaette õiguslik alus. Ei tohi tekkida olukord, kus tehnoloogia arendamise eesmärgil toimub pidev andmetöötlus ka tehnoloogia kasutamise käigus. Leiame, et ettepanekus tehisintellekti arendamise ja toimimise jaoks ette nähtud kaitsemeetmed ja tingimused peaks kohalduma ka teiste tehnoloogiliste lahenduste, mitte üksnes tehisintellekti puhul ning ka teadusuuringutes laiemalt. Õiguskindluse suurendamiseks tuleks IKÜM-is täpsustada tehnoloogiaarendusega seonduva andmetöötluse suhtes kohaldatavaid kaitsemeetmeid. Kaitsemeetmete rakendamine peab tagama IKÜM-is toodud andmetöötluse põhimõtete kohaldamise ning aitama vältida olukorda, kus eriliiki isikuandmete töötlemine

teadusuuringute, sh tehnoloogiaarenduse eesmärgil on lihtsam kui tavaliste isikuandmete töötlemine.

Eesti on seisukohal, et artiklis 88c ette nähtud kaitsemeede vastuväite esitamise õiguse näol ei või minna laiemaks, kui IKÜM-iga ette nähtud. Tuleb vältida olukordi, kus isikutel võimaldatakse juba etteulatuvalt keelata isikuandmete teadusuuringutes kasutamise, mis seaks üldiselt ohtu teadustegevuse ja innovatsiooni.

6.4.2. Eesti toetab teadusuuringute mõiste avamist IKÜM-is, kuna see suurendab õigusselgust. Teadusuuringute mõiste peab hõlmama ka tehnoloogia, sealhulgas tehisintellekti, arendamist. Isikuandmete mõiste sisustamine IKÜM-is peab olema kooskõlas Euroopa Kohtu antud tõlgendusega ja põhitekti täiendamisele tuleb eelistada määruse põhjenduspunktidesse selgituste lisamist. IKÜM-i muutmise käigus tuleb vältida uute määratlemata õigusmõistete kasutuselevõttu. Mõistete muutmisel IKÜM-s tuleb vastavad muudatused teha ka õiguskaitseasutuste andmekaitse direktiivis. Erinevate isikuandmete kaitset reguleerivate Euroopa Liidu õigusaktide muudatuste kohaldamisaeg peab olema ühtlustatud.

Selgitus: Eesti hinnangul on asjakohane uue mõistena IKÜM-is avada seni põhitektis määratlemata õigusmõiste „teadusuuring“. IKÜM käsitleb teadusuuringutega seonduvat juba täna, kuid mõistele legaalse definitsiooni ei ole antud. Eesti leiab, et teadusuuringu mõiste puhul tuleb hoida selle senist laia kohaldamisala, mis muu hulgas hõlmab ka tehnoloogia arendust ja innovatsiooni. Seetõttu peaks ka tehisaru arendus kuuluma teadusuuringu mõiste alla. Teadusuuringu mõiste piiritlemisel tuleb samuti säilitada tasakaal teadusvabaduse ja andmesubjekti õiguste vahel. Teadusuuringu mõiste sisustamisel tuleb silmas pidada, et siia alla kuuluvad ka muud kui tehnoloogia uuringud nt digihumanitaaria, mälu- ja keeleteadus.

Eesti leiab, et isikuandmete mõiste käsitlemist võib IKÜM-is täpsustada, kuid see peab olema kooskõlas seniste Euroopa Kohtu poolt antud tõlgendustega (vt nt C-413/23P EDPS v SRB, C-582/14 Breyer, C-434/16 Nowak, C-683/21 Nacionalinis visuomenės sveikatos centras, C-579/21 Pankki, C-604/22 IAB Europe, C-479/22 P OC). Isikuandmete mõistel on IKÜM-is keskne koht, sellest sõltub, kas määrust tuleb kohaldada või mitte. Oluline on, et muudatuste käigus ei suureneks õigusselgusetus ega kahaneks andmesubjektide usaldus andmetöötluse suhtes. Vastasel korral suureneb kuritarvituste ja vaidluste risk, vastutuse hajumine, halduskoormus ettevõtjatele ja järelevalveasutuste töökoormus. Eesti arvates on kohane isikuandmete mõistega seonduvat täpsustada määruse põhjenduspunktides, jättes määruse põhitekti muutmata.

IKÜM-i kohaldamist on seni raskendanud mitmete määratlemata õigusmõistete kasutamine. Üldmääruse muudatuste käigus tuleb Eesti hinnangul vältida täiendavate määratlemata õigusmõistete kasutuselevõttu. Vastasel korral suureneb nii halduskoormus andmetöötlejatele kui ka järelevalveasutuste ja kohtute töökoormus. Suurem õigusselgus annab kindlustunde kõigile andmetöötlusega seotud isikutele.

Ettepanekuga nähakse ette muudatused ka Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määruses (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (EL institutsioonide andmekaitsemäärus), kuid õiguskaitseasutuste direktiivi vastavasisulisi muudatusi ettepanekuga

kavandatud ei ole. Euroopa Komisjon on andnud teada, et vastavasisulised muudatused esitatakse hiljem. Õiguskaitseasutuste jaoks muutub olukord keeruliseks, kuna nad peavad erinevates olukordades juhinduma erinevatest sätetest (mis puudutab näiteks isikuandmete mõistet, ühtset teavituskäsku või rikkumisest teavitamise tähtaegu). IKÜM, institutsioonide andmekaitsemäärus ja õiguskaitseasutuste direktiiv peaksid sellistes põhiküsimustes olema süsteemselt kohaldatavad.

6.4.3. Eesti toetab ettepanekut kehtiva õiguse täpsustamiseks, mille kohaselt loetakse isikuandmete edasist töötlemist teadus- või ajaloouringute, statistilisel või avalikes huvides toimuva arhiveerimise eesmärgil kooskõlas olevaks töötluse algsete eesmärkidega. Andmetöötluse eesmärkide kooskõla ei loo Eesti hinnangul iseseisvat õiguslikku alust andmetöötluseks, sh ei anna õigust täiendavaks andmehõiveks ja seda tuleks vastavalt määruse muutmisel põhjenduspunktis käsitleda.

Selgitus: Isikuandmete töötlemise eesmärgipiirangu laiendamine on mõeldud täpsustamaks olemasolevat regulatsiooni – kehtiva õiguse kohaselt ei loeta edasist töötlemist teadus- või ajaloouringute, statistilisel või avalikes huvides toimuva arhiveerimise eesmärgil esialgsete töötlemise eesmärkidega vastuolus olevaks. Samas ei loo muudatus isikuandmete töötlemiseks uut õiguslikku alust, vaid selgitab juba olemasolevat regulatsiooni, ja vähendab tõlgenduslikku ebakindlust. Muudatusega täpsustatakse, et olukorras, kus andmed on kogutud nt konkreetse avaliku ülesande täitmise eesmärgil, võib vastutav töötleja neid töödelda ka teadus- või ajaloouringute, statistilisel või avalikes huvides toimuva arhiveerimise eesmärgil.

Praktikas võib muudatus suurendada isikuandmete edasise töötlemise võimalusi ja tuua kaasa riske andmesubjektide õiguste kaitsele. Seetõttu tuleb selguse huvides Eesti hinnangul määruse põhjenduspunktis täpsustada, et andmetöötluse eesmärkide kooskõla ei anna iseseisvat õiguslikku alust edasiseks andmetöötluseks. Eesti leiab, et isikuandmete töötlemise eesmärgipiirangu laiendamise kontekstis tuleb määruse põhjenduspunktis selgelt välja tuua, et andmetöötlus sellisel juhul on üksnes lubatud nende andmete ulatuses, mis on vastutaval töötlejal olemas, mitte ei ole omaette õiguslikuks aluseks täiendavate andmete kogumisel ja täiendavate kaitsemeetmeteta töötlemisel.

6.4.4. Eesti toetab biomeetriliste andmete kasutamise lubamist isikusamasuse kinnitamiseks. Samas on Eesti seisukohal, et ettepanekus toodud tingimus, et andmed või kontrollivahendid peavad olema ainult andmesubjekti kontrolli all, ei ole praktiliselt teostatav. Eesti leiab, et nõue tuleks sõnastada nii, et see oleks seotud isiku poolt protsessi algatamise või konkreetse teenuse taotlemisega.

Selgitus: Eriliiki isikuandmete töötlemise lubatavuse kontekstis on vajalik täpsustada biomeetriliste andmete töötlemise aluseid. Eesti toetab ettepanekus toodud lahendust, mis lubab biomeetria kasutamist isikusamasuse kinnitamiseks ainult juhul, kui andmed või kontrollivahendid (näiteks biomeetriliste andmetega passi automaatkontrolli masin) on ainult andmesubjekti kontrolli all. Selline selgelt piiritletud ja andmesubjekti õigusi kaitsev lahendus võimaldab kaasas käia kaasaja vajadustega.

Ettepanekus toodud tingimus, mis ütleb, et selline andmetöötlus on lubatud ainult juhul, kui andmed või kontrollivahendid on ainult andmesubjekti kontrolli all, ei ole aga täidetav. Mõiste „sole control“ kontseptsioon on ebaselge, võimaldab väga laia tõlgendust ja sellega kaasnevat isikute põhiõiguste ulatusliku riivet. Eesti on seisukohal, et isikusamasuse kinnitamiseks tehtav

andmetöötlus peab olema seotud konkreetse teenusega, mida isik ise taotleb ning sellega kaasnevalt isikusamasuse kinnitamise protsess teadlikult algatab. Andmetöötlus peab olema isiku jaoks turvaline ja läbipaistev.

6.4.5. Eesti on seisukohal, et automatiseeritud töötlusel, sh profiilianalüüsil põhinevate otsuste regulatsioon IKÜM-is peab olema selgelt sõnastatud andmesubjekti õigusena. Automatiseeritud töötlusel põhinevaid, andmesubjektile õiguslikke tagajärgi kaasa toovaid või talle märkimisväärset mõju avaldavaid, otsuseid tohib teha üksnes piiritletud juhtudel ning vastutav töötleja peab sellise andmetöötluse suhtes rakendama täiendavaid kaitsemeetmeid, sh peab andmesubjektil säilima õigus isiklikule kontaktile, et väljendada oma seisukohta ja otsust vaidlustada.

Selgitus: Kehtiva regulatsiooni järgi on andmesubjektil üldjuhul õigus nõuda, et tema suhtes ei tehtaks otsust, mis põhineb üksnes automatiseeritud töötlusel (st et otsuse tegemisel puudub inimese mõtestatud sekkumine). Teatud juhtudel on seda õigust siiski piiratud. Ettepaneku kohaselt võib automatiseeritud töötlusel põhineva otsuse teha ka ilma, et andmesubjektil oleks enne otsuse tegemist võimalik sellest keelduda. Samas jääb kehtima põhimõte, et nn automaatotsused on lubatavad üksnes piiratud juhtudel ning nende rakendamisel tuleb kohaldada erinevaid kaitsemeetmeid, nn andmesubjektile konkreetse teabe andmine (nt otsuse tegemise meetodika ja kasutatud tehnoloogiate kohta) ja andmesubjekti õigus otsesele isiklikule kontaktile, õigus väljendada oma seisukohta, õigust saada selgitust otsuse kohta, mis tehti pärast sellist hindamist, ning õigust seda otsust vaidlustada. Eesti toetab eelviidatud põhimõtete kehtima jäämist, kuivõrd need kaitsevad andmesubjekti. Samal põhjusel peab Eesti arvates jääma eriliiki isikuandmete töötlemine nn automaatotsuste vastuvõtmiseks selgelt piiritletuks nii nagu see on kehtivas IKÜM-is. Muudatus loob võimalused kiiremaks ja andmesubjekti vähem koormavaks andmetöötluseks, säilitades siiski andmesubjektile tema õiguste kaitseks vajalikud meetmed.

Eesti seisukohal, et juhul kui muudetakse IKÜM artiklit 22 nii nagu on ettepanekus toodud, siis tuleb säte sõnastada andmesubjekti õigusena. Praegusel juhul see nii ei ole, aga õigusakti süsteemsuse seisukohalt oleks vaja vastavad muudatused teha. Juhul kui sõnastust ei muudeta, tuleks lubatavale andmetöötlusele leida regulatsioonis õigem koht.

6.4.6. Eesti ei toeta ettepanekut piirata andmesubjekti õigusi selliselt, et õigus oma andmetega tutvuda oleks andmesubjektil üksnes andmekaitselistel eesmärkidel. Andmetega tutvumise õigus peab olema andmesubjektil ka muul juhul kui üksnes andmekaitsega seondult.

Selgitus: Eesti on seisukohal, et andmesubjekt ei peaks vastutavale töötlejale avaldama, millisel eesmärgil ta oma isikuandmete kohta saadud teavet kavatseb edasi töödelda, veel enam puudub vastutavalt töötlejal igasugune võimalus seda ka kontrollida. Antud juhul on tegemist andmesubjekti õigusi tugevalt piirava regulatsiooniga, mida tegelikkuses ei ole ka võimalik tagada. Siinkohal on oluline ka EV põhiseaduse § 44 tulenev isiku õigus tutvuda tema kohta riigiasutustes ja kohalikes omavalitsustes ning riigi ja kohalike omavalitsuste hoitavate andmetega. Seda õigust võib põhiseaduse kohaselt piirata vaid väga selgelt määratletud juhtumitel.

Muudatus nihutab praktikas tõendamiskoormise andmesubjektile, andes vastutavale töötajale laia ja subjektiivse otsustusruumi päringutest keeldumiseks, mis võib vähendada andmesubjektide õiguste tegelikku kasutamist.

6.4.7. Eesti on seisukohal, et Euroopa Andmekaitsekoostöö tuleb anda täpsustavad juhised isikuandmete kaitse alastest rikkumistest teavitamise kohta, eelkõige mida peetakse alusetuks viivituseks ja kõrgeks ohuks. Eesti ei toeta rikkumistest teavitamise lävendi tõstmist kõrge ohuga intsidentideni, vaid soovib, et teavitamise lävend on seotud ohtudega, mida ei saa pidada väikeseks.

Selgitus: Eesti on seisukohal, et rikkumisest teavitamise korral peab olema ühtne arusaam, mida peetakse silmas alusetu viivituse ja kõrge riski all. Ei tohi tekkida olukorda, kus vastutavad töötajad jätaavad rikkumisest teavitamata, kuna nad ei oska riske piisavalt hästi hinnata. Seetõttu tuleb Euroopa Andmekaitsekoostöö tuleb anda nende mõistete sisustamise kohta selged juhised.

Ettepaneku tagajärjel kaob järelevalveasutuste võimalus jälgida nn keskmise ohuga rikkumisi. Eesti teeb ettepaneku tõsta teavitamise lävend ohtudele, mida ei saa pidada väikeseks. Teavitamise lävendi tõstmine ohtudele, mida ei saa pidada väikseks, jätab alles kohustuse teavitada ka nn keskmistest ohtudest, mille realiseerumise korral oleks järelevalveasutustel vajadusel võimalik kasutada oma IKÜM artikli 34 lõikes 4 ettenähtud õigust. Rikkumistest teavitamist käsitleb ka seletuskirja punkt 6.3.1.

6.4.8. Eesti leiab, et ettepanekuga tuleb säilitada Euroopa Andmekaitsekoostöö senised pädevused ja nende arvelt ei ole asjakohane suurendada Euroopa Komisjoni pädevusi. Eesti on seisukohal, et ka edaspidi peab Euroopa Andmekaitsekoostöö andma ühtseid juhiseid IKÜM-i tõlgendamise seotud küsimustes.

Selgitus: Ettepaneku kohaselt väheneb Euroopa Andmekaitsekoostöö (EAKN) pädevus seoses õigusega kehtestada isikuandmete töötlemise toimingute tüüpide loetelu, millele tuleb koostada andmekaitsealane mõjuhinnang ning loetelu, mille puhul see ei ole nõutav. Samuti väheneb pädevus mõjuhinnangute vormi ja meetoodika koostamises. Muudatusega jääb lõplik otsustusõigus komisjonile. Eesti leiab, et Euroopa Andmekaitsekoostöö iseseisvus peab selles osas säilima. Samasugune pädevus peab Eesti arvates olema EAKNile olema ka pseudonüümimise kriteeriumite määramise suhtes. Silmas tuleb pidada, et komisjon osaleb andmekaitsekoostöö töös üksnes vaatlejana, muudatuse tulemusel hakkab komisjon juhiseid andma aga rakendusaktiga.

Rakendusaktid võimaldavad määruse sisu täpsustada, mitte aga muuta. Ettepanek annab aga komisjonile rakendusaktide kaudu võimaluse muuta IKÜM-i kohaldamisala isikuandmete tõlgendamisele, mis võib omakorda tekitada õiguslikku ebakindlust. Õigusaktide tõlgendamise õigus peaks jääma järelevalveasutustele, Euroopa Kohtule ning EAKN-ile. Eesti ei toeta võimalust, et komisjon võiks läbi rakendusaktide sisuliselt muuta olulisi põhiõigustega seotud definitsioone.

EAKN-i antavad juhised ühtlustavad isikuandmete kaitse valdkonna õiguse rakendamise kvaliteeti. Seetõttu toetab Eesti ettepanekut töötada välja ühtsed nõuded, millal on mõjuhinnangu tegemine kohustuslik ning millal ei ole. Läbi ühtsete nõuete on võimalik vähendada siseturul tegutsevate ettevõtjate halduskoormust. Samuti toetab Eesti ettepaneku osa, et EAKN-ile antakse

ülesandeks välja töötada andmekaitsealase mõjuhinna koostamiseks ühtne vorm ja metoodika.

Järelevalveasutuste ja EAKN-i autonoomsuse säilitamiseks peab Eesti siiski vajalikuks jätta nõuete ja vormide koostamise volitused vaid EAKN-ile. Andes nõuete ja vormi koostamise muutmise õiguse ja rakendusaktina vastuvõtmise õiguse komisjonile, on küsimuse all esmalt EAKN-i kui organi sõltumatus ning teisalt ei ole kindel, kas rakendusaktiga vastu võetu väljendab EAKN-i soovitusi ja järelevalveasutuste tegelikke praktikaid. Sama kehtib ka loetelu IKÜM art 33 lg 6 nimetatud kõrge riskiga juhtumite loetelu kohta.

Lisaks sellele on EL-tasandi loetelu õigusaktina kehtestamisel ohuks ignoreerida riigispetsiifilisi riske ja vajadusi ning arvestades menetluse pikkusi EL-i tasandil, on loodav nimekiri alati aegunud.

6.4.9. Eesti toetab ettepanekut lihtsustada nõudeid seoses isikuandmete salvestamisega lõppseadmes (nn küpsised), kuna see leevendab nõusoleku väsimust. Eesti peab oluliseks, et küpsiste puhul oleks ajaline kehtivus määratud nii keeldumisele kui ka nõusoleku andmisele. Juhul kui isik on andnud nõusoleku lõppseadmes isikuandmete salvestamisele, peaks Eesti hinnangul ka sellisel juhul teatud ajaperioodi tagant temalt üle küsima, kas ta jätkuvalt on nõus tema poolt eelnevalt andmetöötluseks antud nõusolekuga.

Selgitus: Probleemkohana toob Eesti välja, et nn küpsiste regulatsioon jääb ettepaneku kohaselt siiski killustatuks, kuna isikustatud andmete nõusoleku regulatsioon sisaldub IKÜM-is, kuid isikustamata andmete regulatsioon jääb ka edaspidi e-privatsuse direktiivi. See toob omakorda kaasa praktilise probleemi, kuidas andmetöötaja saab kindlaks teha, kas lõppseade (nt mobiiltelefon või arvuti) kuulub füüsilisele isikule ning kas kogutud teave toob kaasa isikuandmete töötlemise.

Juhime ka tähelepanu, et kui seadmel on mitu kasutajat, siis tekib risk, et vähem teadlik kasutaja on andnud nõusoleku, et taustal kasutatakse küpsiseid, millele teadlikum kasutaja poleks nõusolekut andnud.

Eesti hinnangul vajab täpsustamist ka artikli 88a lõige 4, mis reguleerib nõusolekut. Tuleks veenduda, et nõusolekuga seotu oleks kooskõlas IKÜM artikli 7 lõikega 4. “Nõusolekutaotlusest keeldumise” (ing. k “*to refuse requests for consent*”) asemel peab olema kirjas, et nõusoleku andmine ning tagasi võtmine peab olema võimalik ühe klikiga.

6.4.10. Eesti teeb ettepaneku, et liikmesriigi andmekaitse järelevalveasutustel peab olema võimalus jätta kaebused läbi vaatamata, kui need ei ole andmekaitse normide täitmise tagamise seisukohalt prioriteetsed.

Selgitus: Eelnõuga tehakse ettepanekuid halduskoormuse vähendamiseks, kuid alates IKÜMi jõustumisest on olnud üha kasvas trendis ka isikuandmete kaitse järelevalveasutuste töökoormus. Eesti leiab, et järelevalveasutuste töökoormuse leevendamiseks on vaja võtta täiendavaid meetmeid. Kuivõrd andmekaitse järelevalveasutused on kohustatud kõik neile esitatud kaebused läbi vaatama, peaks Eesti hinnangul olema neil ka õigus sellised kaebused tagasi lükata, kui nad ei pea kaebust andmekaitse normide täitmise tagamise seisukohalt prioriteetseks. Selline lähenemine vähendaks riigisiseste järelevalveasutuste töökoormust. Järelevalvemenetluses prioriteetide seadmisel peab olema liikmesriikidel võimalus ette näha kriteeriumid, millest järelevalveasutus lähtub. Näiteks võiks kriteeriumidena arvesse võtta järelevalve eesmärgi, oma

ressursside tulemuslikku kasutamist, menetluse esemeks oleva rikkumise iseloomu, ulatust ja mõju ning avalikku huvi.

6.5. Tehisaru regulatsioon koondpaketis väljatoodud EL tehisintellekti määruse muutmise seisukohad

6.5.1. Eesti toetab tehisintellekti määruse muutmist eesmärgiga anda üldotstarbeliste tehisintellektimudelite ja väga suurte digiplatvormidel või otsingumootorites rakendatavate tehisintellekti süsteemide järelevalve ülesanne Euroopa tehisintellekti ametile, kuid selline AI ameti järelevalve peab olema piiriüleste ja süsteemsete riski aspektide osas, milles liikmesriigi pädevusest ja võimekusest üksi ei piisa. Tehisintellekti ameti järelevalve pädevus ei tohi dubleerida siseriiklikku järelevalve pädevust ega takistada siseriiklikku järelevalvet, kus riigil on suveräänsus, pädevus ja mõistlik võimalus järelevalvet ise teostada. Lisaks on oluline väga suurte digiplatvormide või otsingumootorite pakkujate järelevalve nõuete ühtlustamine erinevate Euroopa Liidu õigusaktide vahel, tagamaks neile ühtne Euroopa järelevalveraamistik.

Selgitus: Euroopa tehisintellektiamet on kogu ELis tehisintellektialaste eksperditeadmiste keskus, mis edendab ühiskonnale ja majandusele kasulike tehisintellektilahenduste väljatöötamist ja kasutuselevõttu. Selle ameti üksused, mandaat ja täpsemad ülesanded on AI määruse artiklites 64-69. Kehtiva regulatsiooni kohaselt ei ole tehisintellekti ametil järelevalve pädevust. See on liikmesriikide pädevatel asutustel.

AI amet peaks tegelema järelevalvega teemades, mis on piiriülesed ja kätkevad endas süsteemseid riske. Süsteemsete riskide all on mõeldud eelkõige selliseid riske, mis ulatuslikult võivad kahjustada ühiskondlikke huve või põhiõigusi. Seega need on riskid, millel on oluline ja laiaulatuslik mõju Euroopa siseturusele. Tavaliselt selliste riskidega tegelemiseks ei piisa ühest liikmesriigist, vaid vaja mitme riigi poolt tegutsemist. Samas teemades, kus liikmesriigil on pädevus ja võimalus järelevalvet teha siseriiklikult, ei tohiks AI ameti järelevalve seda takistada (näiteks Eesti turul pakutava tehisintellekti mudeli järelevalve suure riskiga tehisintellekti suhtes). Samuti ei tohi juhtuda, et sama juhtumi osas tehakse topelt järelevalvet - nii liikmesriigi kui ka AI ameti poolt.

Arvestades eelnimetatud tehisintellektisüsteemide laialdast kasutust ja mõju, saame toetada muudatusi, mis tsentraliseerivad selliste süsteemide järelevalvet. EL digiteenuste määrus (DSA) kehtestas väga suurte digiplatvormide (VLOP) või otsingumootorite (VLOSE) pakkujatele võrreldes teiste teenuseosutajatega rangemad kohustused, nõudes neilt muuhulgas oma teenustega kaasnevate süsteemsete riskide hindamist ja maandamist. DSA alusel on nende ettevõtete järelevalvajaks Euroopa Komisjon. Arvestades, et paljud VLOP-id ja VLOSE-d rakendavad oma teenustes tehisintellektil põhinevaid süsteeme, mille puhul kehtivad riskide maandamise kohustused nii DSA kui ka tehisintellekti määruse alusel, leiame, et on asjakohane ühtlustada nende ettevõtete järelevalvet DSA ja AI määruse vahel. Oleme arvamusel, et selline muudatus tagab tõhusama järelevalve ning vähendab nii liikmesriikide kui puudutatud ettevõtete halduskoormust.

6.5.2. Eesti toetab tehisintellekti määruses väikese ja keskmise suurusega ettevõtetele ettenähtud lihtsustusmeetmete laiendamist väikese ja keskmise turukapitalisatsiooniga ettevõtetele, et vähendada nende halduskoormust ja toetada konkurentsivõimet.

Selgitus: Tehisaru regulatsiooni koondpaketiga tehakse ettepanek laiendada tehisintellekti määruses hetkel VKEdele ettenähtud lihtsustusmeetmeid, mis puudutab nt tehnilisele

dokumentatsioonile ja kvaliteedihaldussüsteemi loomisele kehtivaid nõudeid, ka väikese, keskmise turukapitalisatsiooniga ettevõtetele ehk VKTKEdele. Seejuures viitab eelnõu komisjoni soovitusel (EL) 2025/1099, mille kohaselt loetakse VKTKEdeks ettevõtted, millel on kuni 750 töötajat ja mille aastakäive ei ületa 150 miljonit eurot või aastane bilansimaht ei ületa 129 miljonit eurot. Eestis on küll ligi 99,9% ettevõtjatest VKEd, kuid eelnõuga lihtsustaksid ka teatud tegevused nii-öelda kasvufaasis olevatele ettevõtetele (Eestis on suurettevõtteid, millel on üle 250 töötaja 2024. a andmetel 187, neist osa moodustavad VKTKEd, mis on kasvavad ja kasvupotentsiaaliga ettevõtted). Kuigi muudatused mõjutaksid vaid väikest arvu ettevõtteid Eestis, saame leevendusmeetmete laiendamist siiski toetada, kuna VKTKEde halduskoormuse kergendamine toetab nende konkurentsivõimet ning vähendab takistusi VKEde kasvamisel VKTKEdeks.

6.5.3. Eesti toetab tehisintellekti määrusega kõrge riskiga AI süsteemide pakkujatele kehtestatud nõuete edasilükkamist, et anda Euroopa Komisjonile täiendavat aega standardite ja juhiste väljatöötamiseks. Lisaks peab avalikule ja erasektorile jääma piisav aeg, et oma tegevused loodud standardite ja juhistega kooskõlla viia. Nõuete kohaldumise tähtaja prognoositavuse eesmärgil tuleb paindlike tähtaegade asemel kehtestada kindlad rakendustähtajad.

Selgitus: AI määrusest tulenevate harmoniseeritud standardite, tehniliste kirjelduste ja juhiste olemasolu on tehisintellekti süsteemide pakkujatele ja kasutavatele ettevõtetele väga oluline, kuna see lihtsustab nõuete täitmist ja võimaldab seda teha kulutõhusal viisil, samuti aitavad standardid tagada süsteemide kvaliteedi ja usalduse nende vastu. Kuna antud määrusega seotud standardite jm tehniliste materjalide väljatöötamine on võtnud planeeritust kauem aega, toetame kõrge riskiga tehisintellekti süsteemide pakkujatele seatud kohustuste kohaldumisaja edasilükkamist. AI omnibussi ettepanek näeb ette, et kohustused rakenduksid 6-12 kuu jooksul pärast Komisjoni otsust, mis kinnitab nõuete täitmist toetavate meetmete valmimist, kuid mitte hiljem kui 02.12.2027 või 02.08.2028, vastavalt süsteemi määrusest tulenevale kuuluvusele.

Leiame, et prognoositavuse ja õigusselguse eesmärgil tuleks paindlike tähtaegade asemel kehtestada kindlad tähtajad, mis on piisavad, kohustuste rakendumisele. Hetkel ei ole täielikku selgust Komisjoni kinnitusprotsessi toimimise osas ning rakendustähtaegade prognoosimatus raskendab nõueteks valmistumist nii ettevõtetele kui ka pädevatele asutustele. Kindlate kuupäevaliste tähtaegade olemasolu lahendaks need probleemid.

6.5.4. Eesti on teatud tingimustel valmis toetama ettepanekut, mis võimaldaks isikuandmeid töödelda tehisaru kallutatuse avastamiseks ja kõrvaldamiseks. Sellisel töötlusel peavad olema rakendatud piisavad privaatsuskaitse meetmed, vajadus eriliigiliste andmete töötluseks peab olema põhjendatud ega tohi olla vaikumisi lubatud eelduseks. Taolist uut sätet AI määruses ei tohi lugeda eraldiseisvaks andmetöötluse õiguslikuks aluseks.

Selgitus: Tehisaru kallutatuse avastamise on olukordade tuvastamine, kus tehisaru süsteem kohtleb eri inimesi või grupe ebaõiglaselt või teeb süstemaatiliselt viltuseid otsuseid mingi tunnuse alusel. Tehisaru regulatsiooni koondpaketi ettepanekuga lisatakse AI määrusesse uus artikkel 4a, mis sätestab kõigile AI süsteemide ja -mudelite pakkujatele ja juurutajatele võimaluse töödelda eriliigilisi isikuandmeid selleks, et avastada ja kõrvaldata tehisaru kallutatust. Selle võimaluse kasutamise tingimuseks on asjakohaste kaitsemeetmete kasutamine. Siinkohal tuleb arvestada IKÜMi kehtiva artikliga 9 lõikega 2, mille kohaselt ei tohiks eriliiki isikuandmete töötlemist käsitleda kui vaikumisi lubatud tegevust. Vastupidiselt peab selline eriliigiliste

andmete töötlus olema rangelt piiratud, läbipaistvalt põhjendatud ja tehniliselt kontrollitud. Seda põhjusel, et vältida nii õiguslikke rikkumisi kui ka ühiskondlikku kahju.

Üldise digikoondpaketi ettepaneku kohaselt soovitakse IKÜMi lisada artikkel 88c (vt ka seisukoha punkti 6.4.1.), 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 koondpaketi 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 konkreetset 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 äriiline 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.

6.5.5. Eesti peab oluliseks tehisaru regulatiivsetes testkeskkondades ja reaalses tingimustes testimise võimalusi, kuid Euroopa Liidu tasandil ei tohi regulatsioone kinni kirjutada, takistada innovatsiooni ega ohtu seada põhiõiguste kaitset. Eesti toetab AI ameti juurde regulatiivse testkeskkonna loomist, kui see loob lisandväärtust siseriiklike testkeskkondade ees, näiteks toetab piiriüleste süsteemide testimist ja ei dubleeri riigisiseseid testkeskkondasid.

Selgitus: Kehtiv AI määrus näeb ette võimaluse enne AI toote turule laskmist toodet testida nn regulatiivses testkeskkonnas. Tehisintellekti testkeskkond on pädeva asutuse loodud kontrollitud raamistik, mis pakub AI süsteemide (võimalikele) pakkujatele võimalust arendada, treenida, valideerida ja testida innovatiivset tehisintellektisüsteemi asjakohastel juhtudel tegelikes tingimustes ning testkeskkonna kava kohaselt piiratud aja jooksul regulatiivse järelevalve all (vt AI määruse art 3 punkti 55). Sellised AI testimised on olulised selle eesmärgipäraseks ning AI määrusest tulenevaid nõudeid täitval viisil. Kuna AI süsteeme on mitmeid ja erinevatel otstarvetel, ei ole mõistlik testimise regulatsioone Euroopa Liidu tasandil kinni kirjutada. Liikmesriikidel peab jääma autonoomsus otsustamiseks testkeskkondades spetsiifilisi tingimusi, mis on vajalikud nende prioriteetsetes valdkondades. Iga liikmesriik peaks saama oma prioriteetseid valdkondi ise määrata.

Positiivseks saab pidada EL tasandi regulatiivse testkeskkonna loomist, kuid see ei tohi dubleerida siseriiklike testkeskkondi, seda enam, et juba täna on võimalik luua piiriüleseid testkeskkondi. Peab olema üheselt selge, millist lisandväärtust EL-i tasandi testkeskkond pakub siseriiklike ees. EL-i tasandil testkeskkonna loomine võiks aidata toetada innovatsiooni, eelkõige VKE-de ja start-upide kontekstis ning vältida „forum shoppingut“ ning killustunud lähenemist liikmesriikide lõikes.

Ettepanekus on mainitud, et tehisintellektiamet peaks EL-i AI regulatiivseid testkeskkondi rakendama koostöös pädevate riiklike asutustega, seejuures aga ei selgitata vastava koostöö tegemise kriteeriumeid ega erinevate asutuste rollide ja pädevuste jaotust. Eesti jaoks on oluline,

et EL-i AI ameti juurde loodavad tehisintellekti regulatiivsed testkeskkonnad ei dubleeriks siseriiklikke testkeskkondi ning pakuksid lisandväärtust näiteks piiriüleste süsteemide testimise võimaldamise näol. Liiduülese testkeskkonna loomisel on vajalik kindla järelevalveraamistiku kehtestamine seoses isikuandmete töötlemisega (näiteks juhul kui leiab aset isikuandmete töötlemisega seotud rikkumine).

6.5.6. Eesti toetab ettepanekut muuta tehisintellekti määruses põhiõigusi kaitsvate asutuste volitusi viisil, mis suunab põhiõigusi kaitsvaid asutusi ja turujärelevalveasutusi koostööle ning väldib järelevalvatavatel korduvat dokumentide esitamist, kuid ei piira põhiõigusi kaitsvate asutuste pädevust teha järelevalvetoiminguid.

Selgitus: Põhiõigusi kaitsvatel asutustel on kehtiva AI määruse artikli 77 alusel volitus dokumentatsiooni küsimiseks otse tehisintellektisüsteemide juurutajatelt ja pakkujatelt. Siinjuures on oluline märkida, et kehtiva määruse tekst lubab seda vaid kõrge riskiga tehisaru vaatest, kuid uus AI koondpaketi ettepanek sellist piirangut enam ei sea. Viimases lauses väljatoodud osas Eestil murekohtasid pole.

AI määruse artikli 77 kohaldumine tuleb teha üheselt mõistetavaks. Ettepaneku järgi peaksid saavad põhiõigusi kaitsvad asutused vastavat dokumentatsiooni hakkama taotlema turujärelevalveasutuste kaudu. Täna kehtivas määruses on kohustus turujärelevalveasutust teavitada, kuid mitte tema kaudu taotlusi teha. AI koondpaketi põhjenduspunkt 19 täiendab, et koostöö tugevdamiseks tuleks selgitada, et teabele ja dokumentidele juurdepääsu taotlused tuleks esitada pädevale turujärelevalveasutusele. AI koondpaketi muudatus suurendab tõenäoliselt asutuste töökoormust ning võib tekitada turujärelevalveasutuste juurde nn „pudelikaela“ kui neile lisandub kohustus lisaks olemasolevatele kohustustele igakordselt asuda põhiõigusi kaitsvatele asutustele dokumentatsiooni vahendava asutuse rolli. Järelevalve pädevused on turujärelevalve ja põhiõigusi kaitsvate asutuste vahel erinevad, mistõttu ei pruugi põhiõigusi kaitsvate asutuste ja turujärelevalve asutuste ülesannet täitmiseks vajaminev dokumentatsioon olla sama. See tähendaks, et turujärelevalveasutus peaks küsima kõiki dokumente, ka talle mitte vaja minevaid dokumente, juurutajatelt ja pakkujatelt. Selline olukord ei ole õiguslikult pädev, kuivõrd turujärelevalve asutus saab oma tegevuse piires vaid dokumente menetleda. Samuti ei aita artikli 77 muutmine täita ettepaneku lihtsustavat eesmärki. Selle asemel muutub protsess keerulisemaks, kuivõrd sama eesmärgi täitmiseks on vajalik läbida täiendavaid samme. Ühtlasi kitsendatakse selliselt põhiõigus kaitsvate asutuste, sh Andmekaitse Inspektsiooni, pädevusi. Loogiline lahendus oleks selline, kus andmed või dokumendid küsitakse turujärelevalve asutuselt olukorras, kus neil need olemas. Kui see pole nii, siis peaks jääma põhiõiguste kaitsvate asutustele võimalus otse järelevalvatavalt infot saada.

6.5.7. Eesti peab oluliseks digi- ja tehisaru oskuste arendamist, mis toetab nii innovatsiooni, konkurentsivõimet kui ka kaasavat osalemist tehisarupõhises digipöördes. Selliste oskuste arendamine peab toimuma erinevate osapoolte, sealhulgas tehisaru juurutajate ja pakkujate ning avaliku sektori koostöös.

Selgitus: Peame digi- ja tehisaru oskuste arendamist oluliseks poliitikaprioriteediks, mis toetab nii innovatsiooni, konkurentsivõimet kui ka kaasavat osalemist AI-põhises digipöördes. Kehtivas AI määruses on tehisaru süsteemide pakkujatel ja juurutajatel kohustus võtta võimalikult suurel määral kasutusele meetmeid, et tagada oma töötajate ja kõigi teiste nende nimel tehisintellektisüsteemide käitamise ja kasutamise tegelevate isikute piisav tehisintellektipädevus (AI kirjaoskus), võttes arvesse nende tehnilisi teadmisi, kogemusi, haridust ja koolitust ning konteksti, milles tehisintellektisüsteeme tuleb kasutada, ning arvestades isikuid või isikute rühmi, kelle puhul tehisintellektisüsteeme kasutatakse. Uue algatuse kohaselt

pakkujatel ja juurutajatel enam sellist kohustust pole, aga liikmesriikidel ja Komisjonile on pandud kohustus julgustada AI pakkujaid ja juurutajad selliseid samme võtma. Sättega ei täpsustada, mil moel julgustamine peaks toimuma, kuid tekstist saab välja lugeda, et tegemist on aktiivse tegevusega pakkujate ja juurutajate suunal. Eesti hinnangul vähendab see oluliselt võimalust inimeste tehisintellektipädevust suurendada, mis on AI ajastul väga oluline. Samuti suurendab selline sõnastus potentsiaalselt avaliku sektori kulusid, sest kuigi sätte sõnastus viitab julgustamisele, tuleb avalikul sektoril AI pakkujaid ja juurutajaid julgustada spetsiifiliste meetmetega, mis võivad hõlmata ka rahalist kulu.

Tervitame ELi ja liikmesriikide tasandil paremini koordineeritud, avalikule poliitikale tuginevat lähenemist AI-kirjaoskusele, kuid leiame, et vastutust ei tohiks nihutada üksnes riigile – oma roll on ka AI-lahenduste pakkujatel ja juurutajatel. AI-kirjaoskus on pikaajaline ja horisontaalne pädevus, mis peab olema lõimitud haridusse, avalikku haldusesse ja elukestvasse õppesse kuid ka olema loomulik osa AI pakkumise ja juurutamise protsessides.

AI-kirjaoskus tähendab eri sihtrühmade jaoks erinevat taset teadmisi ja oskusi – alates üldisest teadlikkusest kodanikele kuni süvateadmiseni ametnikele ja spetsialistidele. Seetõttu peaks igal juhul tulevane lähenemine jätma liikmesriikidele piisava paindlikkuse kohandada meetmeid oma riikliku konteksti järgi.

7. Arvamuse saamine ning seisukohtade kooskõlastamine

Justiits- ja Digiministeerium on seisukohtade ettevalmistamisel küsinud sisendit Majandus- ja Kommunikatsiooniministeeriumilt, Haridus- ja Teadusministeeriumilt, Kaitseministeeriumilt, Kliimaministeeriumilt, Välisministeeriumilt, Kultuuriministeeriumilt, Rahandusministeeriumilt, Siseministeeriumilt, Sotsiaalministeeriumilt, Regionaal- ja Põllumajandusministeeriumilt, Riigi Infosüsteemi Ametilt, Riigi Info- ja Kommunikatsioonitehnoloogia Keskuselt, Registre ja Infosüsteemide Keskuselt, Riigiside Sihtasutuselt, Rahandusministeeriumi Infotehnoloogiakeskuselt, Tervise ja Heaolu Infosüsteemide Keskuselt, Siseministeeriumi infotehnoloogia- ja arenduskeskuselt, Keskkonnaministeeriumi Infotehnoloogiakeskuselt, Põllumajanduse Registre ja Informatsiooni Ametilt, Regionaal- ja Põllumajandusministeeriumi Infotehnoloogia Keskuselt, Andmekaitse Inspeksioonilt, Tarbijakaitse ja Tehnilise Järelevalve Ametilt, Eesti Pangalt, Finantsinspeksioonilt, Statistikaametilt, Rahvusarhiivilt, Eesti Keele Instituudilt, Põllumajandus- ja Toiduametilt, Transpordiametilt, Ravimiametilt, Terviseametilt, Eesti Linnade ja Valdade Liidult, Eesti Väike- ja Keskmiste Ettevõtjate Assotsiatsioonilt, Politsei- ja Piirivalveametilt, Tööandjate Keskliidult, Taltech AIRE-lt, Konkurentsiametilt, Patendiametilt, Teenusmajanduse Kojalt, Eesti Advokatuuri IP/IKT komisjonilt, Eesti Kaubandus-Tööstuskojalt, Eesti Põllumajandus-Kaubanduskojalt, Toiduainetööstuse Liidult, Eesti Kaupmeeste Liidult, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidult Andmekaitse Liidult, Eesti Meediaettevõtete Liidult, Eesti Autorite Ühingult, Eesti Esitajate Liidult, Eesti Fonogrammitootjate Ühingult, MTÜ Filmi Esmasalvestuse Tootjate Ühingult, Eesti Audiovisuaalautorite Liidult, Balti Uudismeedia Väljaandjate Ühingult, Eesti Näitlejate Liidult, Eesti Kirjastuste Liidult, Eesti Ajakirjanike Liidult, Eesti Rahvusraamatukogult, Patendivolinike Kojalt, MTÜ-lt Maakondlikud Arenduskeskused, Eesti Akrediteerimise Keskuselt, Tallinna Tehnikaülikooli infotehnoloogia teaduskonnalt, Tartu Ülikoolilt, Eesti Pangaliidult, Haiglate Liidult, Perearstide Seltsilt, Eesti Vee-ettevõtete Liidult, Kiirabi Liidult, Apteekrite Liidult, Eesti Elektritööstuse Liidult, Eesti Jõujaamade ja Kaugkütte Ühingult, Eesti Gaasiliidult, Eesti Transpordikütuste Ühingult, Eesti Juristide Liidult, Riigiprokuratuurilt, Notarite Kojalt,

Kohtutäiturite ja Pankrotihaldurite Kojalt, Riigikohtult, Tallinna Ringkonnakohtult, Harju Maakohtu Tallinna kohtumajalt, Pärnu Maakohtu Haapsalu kohtumajalt, Tartu Maakohtu Tartu kohtumajalt, Tartu Ringkonnakohtult, Tallinna Ringkonnakohtult, Open Knowledge Estonia-lt, Eesti Isikuloo Keskuselt, Eesti Mälu Instituudilt, Inimõiguste Instituudilt, E-riigi akadeemialt, Eesti Koostöö Kogult, Tartu Ülikooli arvutiteaduste instituudilt, Tartu Ülikooli õigusteaduskonnalt, Riigikantseleilt, Riigikogu kantseleilt, Presidendi kantseleilt ja Õiguskantsleri kantseleilt. Kaasamiskiri leitav Justiits- ja Digiministeeriumi dokumendiregistris⁸.

Arvamuste kogumisest avaldati ka pressiteade.⁹ Infot kaasamisest ja algatustest jagati riikliku küberturvalisuse poliitika nõukojale (02.12.2025), sündmusteenuste listi (02.12.2025), teenuste koordinaatorite listi (02.12.2025), avaliku teenuste nõukojale (02.12.2025) ning andmete võrgustikku (02.12.2025). Euroopa digivaldkonna lihtsustamise koondpakettide temaatikat arutati ka andmekaitse nõukojas 02.12.2025 ja 5.01.2026.

09.12.2025 toimus avalik kaasamisseminar, kus tehti ülevaade senistest Eesti seisukohtadest digi-, küber- ja andmevaldkonna regulatsioonide kohta, tutvustati Euroopa digivaldkonna lihtsustamise koondpakettide sisusid ning arutleti Komisjoni ettepanekute üle.

Arvamuse saatsid Majandus- ja Kommunikatsiooniministeerium, Siseministeerium, Sotsiaalministeerium, Regionaal- ja Põllumajandusministeerium, Kultuuriministeerium, Riigikogu, Riigikantselei, Transpordiamet, Eesti Andmekaitse Liit, Finantsinspeksioon, Maa- ja Ruumiamet, Patendiamet, Statistikaamet, Eesti Vee-ettevõtete Liit, Eesti Keele Instituut, Eesti Linnade ja Valdade Liit, Riigi Infosüsteemi Amet, Eesti Interneti AS, Andmekaitse Inspeksioon, Põllumajandus ja Toiduamet, Eesti Rahvusraamatukogu, Tarbijakaitse ja Tehnilise Järelevalve Amet, Eesti Infotehnoloogia ja Telekommunikatsiooni Liit, Politsei- ja Piirivalveamet, Eesti Kaubandus- Tööstuskoda, Tartu Ülikool, Cybernetica AS, Meta, Google, Veriff OÜ.

Saabunud sisendid on esitatud kaasamistabelis (lisa 1) ning saabunud ettepanekutega on võimaluse korral arvestatud. Ministeeriumid on seisukohad kooskõlastanud EL koordineerimiskogus.

⁸ Digiomnibusside kaasamiskiri Justiits-ja Digiministeeriumi dokumendiregistris. Kättesaadav: <https://adr.rik.ee/jm/dokument/18178270>

⁹ Pressiteade: Justiits- ja digiministeerium kutsub andma tagasisidet EL Digiomnibussile. Kättesaadav: <https://www.justdigi.ee/uudised/justiits-ja-digiministeerium-kutsub-andma-tagasisidet-el-digiomnibussile>