Kaasamistabel Vabariigi Valitsuse otsuse juurde „Eesti seisukohad Euroopa Komisjoni digivaldkonna lihtsustamise koondpaketi kohta"

Nr	Partner	Märkus, ettepanek või kommentaar	Arvestamine
1.	Majandus- ja Kommunikatsiooniministeerium	**Seisukoht: Peame oluliseks vähendada EL digiõiguse lihtsustamispaketiga halduskoormust nii ettevõtjatele kui avalikule sektorile.** Selgitus: EL õigusaktidest tuleneva koormuse vähendamine on olnud Eesti kauaaegne prioriteet. EL digiomnibussi eelnõuga soovitakse muuhulgas koondada andmeid puudutavad ELi õigusaktid ühtseks raamistikuks andmemääruses ning koondada ka küberintsidentidest teavitamise protsessi.	Arvestatud.
2.		Seisukoht: **Peame oluliseks lisada küberturvalisuse 2. direktiivi ehk NIS2 kohaldamisalasse kosmose valdkond ning sealjuures peab see hõlmama kõiki kosmosetaristu komponente.** Selgitus: Euroopa Komisjon esitas 25. juunil 2025. aastal Euroopa kosmosemääruse (EUSA). EUSA aruteludes nõukogu kosmosetöörühmas on keskendutud küberturvalisuse ja kerksusnõuetele, mis peavad arvestama valdkonna eripärasid, olema proportsionaalsed ning vältima dubleerimist ja liigset halduskoormust. Eesti peab vajalikuks küberturvalisuse valdkonnas horisontaalset lähenemist, seega tuleks eelistada mistahes erivajaduse esinemisel küberturvalisuse 2 direktiivi kohaldamist, sealhulgas erisätetega täiendamist. Sellega välditakse nõuete dubleerimist ja täiendava halduskoormuse teket ehk vajadust tõestada oma tegevuse kooskõla erinevate õigusaktidega. Kuna ettevõtjate tegevus ei piirdu sageli ühe tegevussektoriga ja pakutavad teenused on kasutatavad erinevates sektorites, võivad sektorite dubleerivad nõuded luua juurde bürokraatiat. Näiteks küberturvalisuse 2. direktiivi lisa 1 punkt 11 kohaselt on kriitilise tähtsusega sektor „kosmos" ja hõlmatud üksused on liikmesriikide või eraõiguslike isikute omandis olevad, hallatavad või käitatavad	Ei arvesta. Kuigi see on oluline ning selle sisuga on JDM nõus, siis see väljub digiomnibussi skoobist. Saab hinnata, kas samasisulise seisukoha saaks teha küberturvalisuse määruse (CSA) üle vaatamise käigus, mil võidakse NIS2 direktiivi täiendada. Vastav ettepanek avaldati 20.01.2026: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act.

		maapealsete taristute operaatorid, kes toetavad kosmosepõhiste teenuste osutamist. Kuigi komisjon on eelnõu koostamisel põhjendanud, et küberturvalisuse 2. direktiiv (direktiiv (EL) 2022/2555) ehk NIS2 ja elutähtsa teenuse osutajate toimepidevuse direktiiv (EL) 2022/2557 ehk CER direktiiv ei pruugi olla piisavad, kuna nende kohaldamisala ei hõlma kõiki kosmosetaristu komponente, eriti väiksemaid operaatoreid, siis Eesti ei nõustu sellega. Nimelt nii NIS2 kui ka CER direktiivi nõuded võivad laieneda väiksematele operaatoritele. Näiteks võib Eesti eripära arvestades elutähtsa teenuse osutajaks mikro- või väikeettevõtja. Komisjon on muuhulgas välja toonud, et kosmose valdkonnas tuleb luua riskijuhtimise raamistik, mis hõlmab küberturvalisust ja füüsilist turvalisust nii satelliitide kui ka maapealse taristu puhul. Seatakse kohustuslikud turvameetmed, intsidentide käsitlemise reeglid ja aruandlusmehhanismid. Kuid leiame, et seda on võimalik teha olemasolevat õigusraamistikku ära kasutades ja vajadusel täiendades. Kosmosega seotud küberturvalisuse osas tuleb ära kasutada olemasolevat ekspertiisi, sh EL asutuste kompetentsi. Euroopa Liidu Küberturvalisuse Amet (ENISA) peab jääma küberturvalisuse teemadel, sh kosmose küberturvalisus, valdkonna koordineerijaks ning liikmesriikide kontaktpunktiks. Näiteks peame vajalikuks et Riigi Infosüsteemi Ametile ei tekiks uut küberteemalist kontaktasutust. Mis tahes uus kontaktasutus võib tekitada info dubleerimist ja võib luua vajaduse täiendavaks töökohaks. Kübervaldkonnas on kasvamas uus turg Eesti küberturvalisuse ettevõtetele, luues võimalusi innovatsiooniks ja teenuste arendamiseks. Näiteks Euroopa komsosemääruse artiklis 88 ette nähtud kohustuslik ohuteabel põhinev läbistustestimine (Threat Led Penetration Testing, TLPT) võib pakkuda võimalusi kosmose	

		küberturbeharjutusväljaku (Space Cyber Range) sarnastele algatustele. Eesti soovib saada peamiseks küberturbeteenuste tarnijaks EL kosmoseprogrammile ning koostöös Eesti ettevõtlusega ja ESA-ga töötame selles suunas. EUSA rakendamine võib luua selgemad tingimused ja võimalused Eesti tööstusele.	
3.		Seisukoht: **Toetame andmete pseudonüümimise ja anonüümimise toimimise täpsustamist Euroopa Komisjoni poolt selgete kriteeriumide määratlemise teel** Selgitus: Tehnoloogia arenedes on ettevõtetele üha suuremaks väljakutseks kujunenud isikuandmete ja muude andmete vahel erisuse tegemine, kuna seni on puudunud selged tehnilised kriteeriumid. Seepärast toetame ettepanekut täiendada isikuandmete üldkaitse määrust (EL) 2016/679 uue artikliga 41a, mis annaks Euroopa Komisjonile volituse võtta vastu rakendusmääruseid täpsustamaks andmete pseudonüümimisega seotud meetmeid ja kriteeriume. Selline harmoniseerimine tagab suurema kindluse nii ettevõtetele kui ka pädevatele asutustele ning aitab maandada ebaõige klassifitseerimisega seotud riske.	Arvestatud osaliselt. Toetame liikmesriikide üleste juhiste koostamist, kuid ei toeta seda, et Euroopa Komisjon teeb seda rakendusmäärustega.
4.		Seisukoht: **Toetame Euroopa Parlamendi ja nõukogu määruse (EL) 2019/1150, mis käsitleb õigluse ja läbipaistvuse edendamist veebipõhiste vahendusteenuste ärikasutajate jaoks, kehtetuks muutmist. Õigusselguse tagamise eesmärgil saame toetada määruse valitud sätete kehtimist kuni neile viitavate EL õigusaktide muutmiseni, seda tähtajaga hiljemalt 31. detsember 2032.** Selgitus: Määrus (EL) 2019/1150 (lühidalt 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	Arvestatud.

		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 suhetes ärikasutajatega, kuid leiame, et nende nõuete lisandväärtus on kokkuvõttes pigem madal. Lisaks on P2B määruse kehtimise järgselt jõustunud Euroopa Parlamendi ja nõukogu määrus (EL) 2022/1925, mis käsitleb konkurentsile avatud ja õiglaseid turge digisektoris (lühidalt DMA), mille eesmärgiks on tagada digiturgude 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 suhetes, mistõttu toetame ettepanekut muuta määrus (EL) 2019/1150 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.	
5.		Seisukoht: **Toetame tehisintellekti määruse (EL) 2024/1689 muutmist eesmärgiga anda üldotstarbeliste tehisintellektimudelite ja väga suurtel digiplatvormidel või otsingumootorites rakendatavate tehisintellektisüsteemide järelevalve ülesanne Euroopa tehisintellektiametile.**	Arvestatud.

		Selgitus: Arvestades eelnimetatud tehisintellektisüsteemide laialdast kasutust ja mõju, saame toetada muudatusi, mis tsentraliseerivad selliste süsteemide järelevalve. Euroopa Parlamendi ja nõukogu määrus (EL) 2022/2065, mis käsitleb digiteenuste ühtset turgu (EL digiteenuste määrus, edaspidi 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 VLOPid ja VLOSEd rakendavad oma teenustes tehisintellektil põhinevaid süsteeme, mille puhul kehtivad riskimaandamiskohustused nii DSA kui ka tehisintellekti määruse alusel, leiame, et on asjakohane ühtlustada nende ettevõtete järelevalvet. Oleme arvamusel, et selline muudatus tagab tõhusama järelevalve ning vähendab nii liikmesriikide kui puudutatud ettevõtete halduskoormust.	
6.		Seisukoht: **Toetame tehisintellekti määruses (EL) 2024/1689 teatud väikese ja keskmise suurusega ettevõtetele (VKEdele) ettenähtud lihtsustusmeetmete laiendamist väikese ja keskmise turukapitulatsiooniga ettevõtetele (VKTKE – inglise keeles *small-mid caps*), et vähendada halduskoormust ja toetada nende konkurentsivõimet.** Selgitus: Eelnõuga tehakse ettepanek laiendada tehisintellekti määruses hetkel VKEdele ettenähtud lihtsustusmeetmeid, mis puudutab nt tehnilisele dokumentatsioonile ja kvaliteedihaldussüsteemi loomisele kehtivaid nõudeid, ka VKTKEdele. Seejuures viitab eelnõu komisjoni soovitusele (EL) 2025/1099, mille kohaselt loetakse VKTKEdeks ettevõtted, millel	Arvestatud.

		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 lihtsustuksid 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.	
7.		Seisukoht: T**oetame tehisintellekti määrusega (EL) 2024/1689 kõrge riskiga tehisintellektisüsteemide pakkujatele kehtestatud nõuete edasilükkamist, et anda täiendavat aega standardite ja juhiste väljatöötamiseks. Seejuures leiame, et prognoositavuse eesmärgil tuleks paindlike tähtaegade asemel kehtestada kindlad rakendustähtajad.** Selgitus: Harmoneeritud standardite, tehniliste kirjelduste ja juhiste olemasolu on tehisintellektisüsteeme pakkuvatele 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 tehisintellektisüsteemide pakkujatele seatud kohustuste kohaldumisaja edasilükkamist. Tehisintellekti omnibussi ettepanek näeb ette, et kohustused rakenduksid 6-12 kuu jooksul pärast Komisjoni otsust, mis kinnitab nõuete täitmist toetavate meetmete valmimist, kuid mitte	Arvestatud.

		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 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.	
8.	Siseministeerium	Siseministeerium toetab digiõiguse valdkonna lihtsustamise paketti. Samas soovime pöörata tähelepanu mõnele olulisele aspektile: Tehisintellekti määrusega seotud digiomnibusiga avatakse määrus (EL) 2024/1689 (tehisintellekti määrus, AIA), mis ei ole veel täies ulatuses jõustunud. Toetame, et muudetakse kõrge riskiga tehisintellektisüsteemide reeglite kohaldumisaega ja pooldame tähtaja sidumist standardite valmimisega. Tähtaegu on vajalik edasi lükata, et need oleksid kooskõlas vajalike standardite ja juhiste kättesaadavusega ning reegleid oleks võimalik korrektselt rakendada.	Arvestatud.
		Samuti toetame kõrge riskiga tehisintellektisüsteemide pakkujate kohustuste sätete muutmist ja halduskoormuse vähendamist. Mõistlik on ka ettepanek täiendavate juhendmaterjalide koostamiseks, mis pakuksid selgeid ja praktilisi juhiseid AI-määruse rakendamiseks koos teiste EL õigusaktidega. Lisaks toetame AI regulatiivse liivakasti ja selle reeglistiku täiendamisest. Hindame, et see aitaks AI teemasid paremini raamistada ja me	Arvestatud osaliseliselt. Arusaamatuks jääb ettepanek juhendmaterjalide koostamiseks, kuivõrd see on osa ka kehtivast AI määrusest. Sellekohased juhendid on ka juba osaliselt olemas. Juhendmaterjalide koostamiseks ei ole vaja õigusesse seda vajadust sätestada. AI liivakasti suunal

		saaksime kasutada nii EL AI liivakasti kui luua Eestis ka enda omasid.	saadeti aasta alguses konsultatsioonile rakendusakt.
9.		Samuti on Siseministeeriumi hinnangul vajalik intsidentidest teavitamise üks aken. Samas, ühtse teavituskanali loomisel tuleb tagada, et kriitiline ja ajakriitiline info jõuaks pädevate asutusteni viivitusteta ning et ei nõrgeneks riiklik võimekus intsidentidele kiiresti reageerida. Seetõttu on vajalik hinnata EL-i tasandi lahenduse koosmõju siseriiklike julgeoleku- ja kriisihaldusprotseduuridega. Hästi disainitud ühtne aken võimaldaks samal ajal vähendada halduskoormust, säilitades kõrge turvalisuse taseme. Samas toetame intsidentidest teavitamise ühe akna visiooni ja eesmärki, kuid siinkohal on ka Eestis tekkinud vastuolusid erinevate teemade osas, nt Küberkuritegevuse, RIA intsidentide teavitamise, TTJA teavitamise ja andmekaitse vaatest on erinevad vormid ja kohati ka erinevad tähtajad, mida täpselt soovitakse. Ideena tundub see sobiliku lahendusena, kuid siinkohal on vaja analüüsida protseduure ja koosmõju. Täpsemalt, mis on ootused direktiividelt siseriikliku seadusandlusesse ning milline on mõju protseduuridele. Ühtselt aknal oleks eeldatavasti vähem teavitamiskulusid.	Arvestatud. Selgitame, et Komisjoni ettepaneku selgitustes on märgitud, et ootus on ka ühtlustada vorme. Tähtaegade ühtlustamise osas on seisukoht koostatud.
10.		Andmehaldust ja seda toetavat tänast regulatsiooni arvestades toetame väga valdkonna konsolideerimise ettepanekut läbimõeldud, selgesse ja lihtsustatud formaati.	Arvestatud.

			Seisukohas rõhutakse süsteemsusele, mis tahab selget ja läbimõeldud regulatsiooni.
11.	Finantsinspektsioon	Finantsinspektsioonile teadaolevalt menetletakse Brüsselis ettepanekut (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025PC0837&qid=1764840573622), mille üheks osaks on ka DORA määruse muutmine. Meie vaatest tuleb kõige pealt märkida, et oleme oma tegevused ja arendused juba valmis teinud kehtivat DORA regulatsiooni järgides, st meil on juba tellitud vastavad tarkvaralahendused, loodud tehniline võimekus jne, mis kohe on käiku minemas. Eelnevast tulenevalt on oluline lisaks liikmesriikide poolt tõstatud turvalisuse ja tehnilistele teemadele välja selgitada ka SEP-i kulude pool. Aeg on näidanud, et üldjuhul on Euroopa kesksete lahenduste/süsteemide loomine väga kallis ettevõtmine ning need kulud peaks eelduslikult liikmesriigid (sh Finantsinspektsioon) ka ise kinni maksma. Arvestades, et meil on juba oma süsteem arendatud ja tellitud, siis oluline on teada, mis SEP loomine ja ülalpidamine võiks maksma minna, kes selle kinni maksab ning kuidas on planeeritud edaspidi SEP-i kasutamise kulude lahendus. Oma sisus on keskne lahendus mõistlik, kuid kui sellega kaasnevad väga suured kulud, siis ei pea SEP-i loomist vajalikuks.	Selgitame: ettepaneku selgitustes on teatava ülevaade võimalikest liikmesriigi kuludest välja toodud, kuid praktikas selgub selle sisu siis, kui on suurem selgus ühtse teavitusakna olemusest ning tehnilisest lahendusest.
12.	Cybernetica AS	Lähtekohad:	Teadmiseks võetud.

		1) Andmekaitses on IKÜM alguspäevadest vaieldud, mis on pseudonüümne ja kas miski saab olla anonüümne (nn “relatiivne” vs “absoluutne” andmekaitse). Hiljutised otsused, sh Judgment of the Court in Case C-413/23 P | EDPS v SRB (Concept of personal data) on seda sisustanud, aga üldine praktika on lahtine. Mitmed teadlased on pakkunud, et peaks lähenema riskianalüüsiga, mis on väga mõistlik mõte, aga pole praktikas olnud veel kuigi edukas. 2) See riskianalüüs siis hindaks mingi metoodikaga, kas mingis olukorras mingi tehnilise meetmega isikustatavate andmete töötlemine vastaks seaduse nõuetele või mitte. Lihtsate sõnadega - mis on see lävend, kus maalt me suudame taasidentifitseerimist vältida? 3) Omnibuss rõhutab sellise riskianalüüsi tähtsust tulevikus. Eesti kogemusest tehisintellekti, pilvteenuste, internetivalimiste jne riskianalüüsidega on näidanud, et üldised juhendid on toredad, aga neid ei osata rakendada, kui puudub vastav detailne teadmus. 4) Nt Eestis RITi tellitud pilvteenuste ja AI teenuste riskianalüüse peetakse edulugudeks, sest nad on konkreetsed. Teaduste akadeemia küberturvalisuse komisjoni riskianalüüsid valimiste tehnoloogia ja riigi kriitiliste teenuste jaoks on samuti konkreetsed, annavad selgeid nõuandeid, kuidas eluga edasi minna. Ettepanek: 1) Eesti teeb ettepaneku, et Eestisse loodaks kompetentsikeskus, mis toetab EDPB-d privaatsuskaitse tehnoloogiate riskianalüüsil.	

		2) Kompetentsikeskus toetaks omnibussi vajadusi järgmisel moel: 2.1) EL andmekaitse ja omnibussi tuumküsimuste (uued teenused, AI rakendamine, põhiõiguste kaitse) lahendamisega, et meil oleks Euroopas moodsad e-teenused, mis vastavad meie väärtusruumile. 2.2) Privaatsuskaitse tehnoloogiate standardimine, sertifitseerimine ja tehnoloogiadiplomaatia. 2.3) Intsidentide töötlemise ja riskianalüüsi tugiüksus EDPB-le 2.4) Privaatsuskaitse tehnoloogiate ja riskianalüüsi võimekuse arendamine keskus (tehnilised riskianalüüsid ja nõuanded, praktilised tehnoloogia teekaardid, koolitusmaterjalid, e-riigi teenuste mustandid) koostöö Euroopa ja Eesti akadeemiliste partnerite ja tööstusega. 2.5) Kriitiliste EL võimekuste loomise nõustamine andmekaitse tehnoloogiate vaatepunktist. 2.6) Pilootprojektide koordineerimine Euroopa tasandil ja võimalusel liitlastega, et tugevdada ka kontinentide vahelist andmete ühist kasutamist. Põhjendused: 1) Eesti e-riik on küps nii teenuste, digitaalse identiteedi, andmete kasutuselevõtu kui ka digisuveräänse infotehnoloogia rakendamises. Meie kogemused on suurepärased, kuid nende kandmine Euroopasse on seni olnud keeruline. 2) Kompetentsikeskuse töö kaudu saaksime Euroopasse suunata Eesti e-riigi õppetunde, et ei juhtuks selliseid asju nagu COVID-19 pandeemia ajal, kui kehtisid Adolf Hitleri ja Miki Hiire	

		vaktsineerimistõendid, sest ei suudetud ehitada kehtivuskinnituse teenust, mis vastaks EL andmekaitsenõuetele. Meil oleks see võimekus olemas olnud, Eestis on sellised teenused olnud ID-kaardi algusajast, aga meil puudus võimekus seda Euroopasse üle kanda. 3) Eesti on privaatsuskaitse tehnoloogiate varane rakendaja. Eestil on olemas riiklik kontseptsioon ja teekaart ning ka vajadus neid rakendada. 4) Rahvusvaheliselt on Eesti seni osalenud OECD privaatsuskaitsetehnoloogiate arenduse töörühmades. Eesti saaks kompetentsikeskuse arendusest ise kasu ning saaks seda teadmust ka eksportida.	
13.	Riigikogu Kantselei	Riigikogu Kantselei tervitab Euroopa Komisjoni püüdlusi muuta kehtiv digiregulatsioon selgemaks, riskipõhisemaks ja praktilisemaks. Digiomnibussi üldine eesmärk – vähendada ebavajalikku halduskoormust, ühtlustada liikmesriikide praktikaid ning parandada regulatsioonide omavahelist koostoimet – on igati tervitatav. Positiivsena näeme eelkõige kavandatavaid muudatusi, mis puudutavad andmetöötluste dokumenteerimise lihtsustamist, andmesubjektide taotluste (DSAR) mõistlikumat käsitlemist, andmekaitsealaste mõjuhinnangute (DPIA) ühtlustamist ning isikuandmete rikkumistest teavitamise riskipõhisemat lähenemist.	Teadmiseks võetud.
14.		Samuti võib toetada kavatsust täpsustada pseudonüümiseeritud andmete käsitlust ning selgemat eristust isikuandmete ja mitteisikuliste andmete vahel, mis looks paremad eeldused andmeanalüütika ja tehisintellekti arendamiseks, säilitades samal ajal andmesubjektide põhiõiguste kaitse. Oluline on ka järelevalveasutuste koostöö tugevdamine ning seoste loomine	Teadmiseks võetud.

		teiste ELi digiregulatsioonidega, nagu tehisintellekti määrus, andmete määrus ja kübervastupidavuse raamistik.	
15.		Samas peab Riigikogu Kantselei vajalikuks juhtida tähelepanu, et eelnõu mitmetähenduslik sõnastus tekitab küsimusi identifitseeritavuse, pseudonüümiseeritud andmete käsitluse ning andmesubjekti õiguste ulatuse kohta. Ebapiisav selgus nendes küsimustes võib praktikas viia ebaühtlase tõlgendamiseni ning õigusselguse vähenemiseni, eriti olukordades, kus isikuandmete staatus sõltub tehnilistest ja tõenäosuspõhistest hinnangutest.	Arvestatud.
16.		Kokkuvõttes toetab Riigikogu Kantselei digiomnibussi üldist suunda ning selle eesmärki muuta andmekaitse- ja digiregulatsioon praktilisemaks ja riskipõhisemaks. Samas peame oluliseks, et edasises menetluses arvestataks õigusselguse tagamise vajadust.	Teadmiseks võetud.
17.	[12]	IKÜMja e-privaatsus ● Isikuandmete mõiste täpsustamine: Omnibusi ettepanek seob õigustatult „isikuandmed" sellega, mida vastutav töötleja saab mõistlikult teha tegelikult kättesaadavate vahenditega. Samas on vaja täiendavat selgitust, et kajastada täiel määral Euroopa Liidu Kohtu (CJEU) praktikat ja GDPRi põhjendust 26 ning vältida killustatud ja ülemäära laiu tõlgendusi. Me kutsume üles: säilitada Omnibusi muudatus lõpptekstis, täpsustades samal ajal, et tuvastatavust tuleb hinnata asjaomase	Arvestatud osaliselt. Nõustume, et isikuandmete mõiste sisustamisel tuleb arvestada kohtupraktikat ning teeme ettepanekut jätta mõiste täiendamine artiklis lisamata, kuid täiendada IKÜM põhjenduspunkti selgitusega, et mõiste sisustamisel tuleb lähtuda ka kohtupraktikast.

[2] Meta esitas ka artikli põhised kommentaarid, mida kõike siin tabelis ei ole – need on kättesaadavad https://adr.rik.ee/jm/dokument/18258217.

		üksuse vaatenurgast, võttes arvesse ka objektiivseid tegureid, nagu kulud, tehnoloogilised ressursid, tuvastamiseks vajalik aeg ning töötlemisel rakendatavad kaitsemeetmed.	
18.		● Automatiseeritud otsuste tegemise täpsustamine, et vältida ülereguleerimist: Omnibusi selgitus, et automatiseeritud otsused on artikli 22 alusel lubatud juhul, kui selle tingimused on täidetud – isegi siis, kui inimlik otsustamine oleks võimalik – on oluline samm õiges suunas. Me kutsume üles: säilitada Omnibussi muudatus lõpptekstis, täpsustades samal ajal, et GDPRi artikkel 22 kohaldub ainult automatiseeritud otsustele, mis määravad isiku õigusliku staatuse, lepingulised õigused või millel on võrreldavalt oluline ja püsiv mõju.	Arvestatud osaliselt. Pooldame automatiseeritud otsuste võimaldamist. Täpsustamist ei palu.
19.		● Tehisintellekti ja andmekaitse ühtlustamine: artikkel 88c on keskse tähtsusega, kuna see tunnustab selgesõnaliselt õigustatud huvi tehisintellekti arendamise ja kasutamise õigusliku alusena ning viib GDPRi kooskõlla tehisintellekti määruse (AI Act) mõistetega. See kehtestab kogu ELi hõlmava selge standardi tehisintellekti treenimiseks, vähendab õiguslikku killustatust ning ajakohastab tõhusalt GDPRi tehisintellekti ajastuks. 2. detsember 2025 Me kutsume üles: säilitada Omnibussi muudatus, kuid seda samal ajal lihtsustada, et eemaldada ebaselgused ja kattuvused.	Arvestatud osaliselt. Ei toeta õiguslike aluste kinnikirjutamist õigustatud huvile ja nõusolekule. Kõik IKÜM õiguslikud alused võivad olla isikuandmete töötlemisel aluseks.
20.		● Kaasvastutava töötleja mõiste korrigeerimine: kaasvastutavad töötlejad, mis oli algselt mõeldud erandliku korrana tegeliku kaasmääramise (co-determination) puhuks, on laialdaste	Mitte arvestatud.-

		tõlgenduste tõttu kujunenud sisuliselt üldiseks vastutusraamistikuks. Seda kohaldatakse nüüd laialdaselt, mis tekitab õiguslikku ebakindlust ja ebaproportsionaalseid vastavuskohustusi. Me kutsume üles: tegema artiklisse 26 sihipärase muudatuse, millega täpsustatakse, et vastutavaid töötlejaid käsitatakse kaasvastutavate töötlejatena üksnes siis, kui nad osalevad aktiivselt ning tegelikult mõjutavad töötlemise eesmärke ja vahendeid käsitlevaid otsuseid.	Selline ettepanek oleks vastuolus hiljutise kohtupraktikaga.
21.		Küpsised, e-privaatsus ja nõusolek ● Reeglite koondamine ja nõusolekuväsimuse algpõhjustega tegelemine: GDPRi ja e-privaatsuse regulatsiooni lahus hoidmine (GDPR artikkel 88a vs e-privaatsuse direktiivi artikkel 5 lõige 3) säilitab keerukuse, õigusliku killustatuse ja nõusolekuväsimuse. Pelgalt mõnede küpsiste ja jälgimisreeglite viimine GDPRi alla piiratud eranditega ei lahenda alusprobleeme. Me kutsume üles: tühistama e-privaatsuse direktiivi artikli 5 lõike 3 ja viima artikli 88a täielikult kooskõlla GDPRi õiguslike alustega ning allutama liiklusandmed ja otseturunduse (st tühistama e-privaatsuse direktiivi artiklid 6, 9 ja 13) täielikult GDPRile, säilitamata olemasolevaid e-privaatsuse sätteid.	Mitte arvestatud. Ühest küljest oleme nõus, et tuleb vältida dubleerimist, samas e-privaatsuse direktiivi sätted täiendavad GDPRi (mis kehtib ainult füüsiliste isikute andmete kaitsele). Nende sätetega nähakse ette ka juriidiliste isikute andmete kaitse .
22.		● Kohustuslike masinloetavate nõusolekusignaalide kaotamine (artikkel 88b): artikkel 88b lisaks olemasolevatele GDPRi reeglitele uue kohustusliku nõusolekusignaalide kihi, suurendades veelgi õiguslikku ja tehnilist keerukust. Varasemad katsed selliste signaalidega on ebaõnnestunud ning kohustuslik skeem oleks kulukas ja segadust tekitav, eriti VKEde jaoks, samal ajal kui	Mitte arvestatud.

		erandid (nt meedia jaoks) õõnestaksid veelgi sidusust ja kasutajate usaldust. Me kutsume üles: eemaldama artikli 88b lõpptekstist tervikuna.	
23.	Goo[34]	GDPRi kohta ○ AI ja õigustatud huvi: Ettepanek loob AI jaoks piirava „kahe režiimi“ süsteemi, mille tingimused on määratlemata ja mis kalduvad kõrvale GDPRi tavapärastest reeglitest. Õiguskindluse tagamiseks ja ühtse turu killustumise vältimiseks tuleb artikkel 88c viia kooskõlla väljakujunenud kohtupraktikaga, eemaldades need täiendavad tingimused ning sätte, mis võimaldab kehtestada riiklikke nõusolekunõudeid. ○ Eriliigilised andmed ja AI: Nõue rangelt „vältida“ tundlike andmete kogumist avalikust veebist ei ole tehniliselt teostatav ning eeldab paradoksaalsel kombel hoopis pealetükkivat seiret. See kohustus tuleks asendada praktilise „riskide maandamise“ standardiga, mis põhineb tehnilistel ja organisatsioonilistel meetmetel, ning eemaldada kohustuslikud väljundfiltrid, mis kahjustavad AI-vahendite funktsionaalset kasutatavust.	Arvestatud osaliselt. Eesti ei toeta AI arendamiseks ja opereerimiseks töötlemise õiguslike aluste kinni kirjutamist (GDPR art 88c ettepanek). Seisukohtades on privaatsuskaitse tehnoloogiate toetamise punkt. See aitab ka eriliigiliste andmete puhuks.
24.		ePrivaatsuse direktiivi kohta ○ Nõusolek brauseri tasandil: Artikkel 88b tuleb kustutada, kuna tsentraliseeritud brauserisignaalide kohustuslik kasutamine ei	Eesti toetab e-Privaatsuse direktiivi ajakohastamist ja isikuandmete töötlemise IKÜMi alla viimist.

[4] Google esitas ebapaberi, mis sisaldas nende põhisõnumieid ja pikemaid selgitusi, mis põhisõnumeid tutvustavad. Siia tabelisse lisati ennekõike põhisõnumid. Kogu sisend on leitav: https://adr.rik.ee/jm/dokument/18295967.

		lahenda praktikas kasutajate väsimust nõusolekute andmisest, vaid tekitab hoopis „nõusolekusegadust“ ning õõnestab funktsionaalselt reklaamipõhist veebi, sealhulgas privaatsust hoidvaid kontekstipõhise reklaami mudeleid. ○ GDPRi ühtne jõustamine: Tegeliku lihtsustamise saavutamiseks ja jõustamiskaose vältimiseks tuleb lahendada isiku- ja mitteisikuandmete vaheline „killustatud režiim“, viies kõik lõppseadmete kasutamist reguleerivad normid GDPRi alla ühe ühtse ja järjepideva mehhanismi kaudu. ○ Kontekstipõhise reklaami soodustamine: Privaatsuspõhise disaini (privacy-by-design) edendamiseks tuleb artiklit 88a laiendada nii, et see vabastaks selgesõnaliselt madala riskiga ja profileerimiseta tegevused — eelkõige kontekstipõhise reklaami ning selle toimimiseks vajalikud turvaelemendid — nõusolekunõuetest.	
25.		Küberturvalisuse kohta ○ Ambitsiooni tõstmine: standardiseerides teatamistähtajad 72-tunnise teavitamiskohustuse ümber, ühtlustades nende tähtaegade käivitumise alguspunkti, viies kooskõlla teatamiskohustusega intsidentide künnised ning ühtlustades aruandlusvormid. ○ Ühe kontaktpunkti edasiarendamine: kuigi ühtne sisenemispunkt on hea esimene samm, tuleks see integreerida CRA aruandlusplatvormiga. Teavitusi esitavaid üksusi tuleks kaasata tööriista disaini ja funktsionaalsuse kujundamisse ning neile peaks olema tagatud ametlik tagasisidemehhanism võimalike probleemide esiletoomiseks.	Selgitame: Eesti ootus on ühtlustada teavitamiste tähtaegu ei õigusaktides, kuid veel ei ole Eesti kokku pannud seisukohta, mis see tähtaeg või tähtajad võiksid olla. Ühe akna lahenduse tehnilised detailid on alles selgumisel, mille järel selguvad ka selle funktsionaalsused.

		○ Täiendav lihtsustamine: lihtsustamispingutusi tuleb laiendada ka väljapoole intsidentidest teatamist, hõlmates muu hulgas NIS2 ja CRA nõuete täitmise lihtsustamist.	
26.		**AI määruse kohta** ○ **Läbipaistvusnõuete tähtaegade pikendamine (art 50):** pikendada vastavusse viimise perioodi ühe aastani kõigi süsteemide (nii uute kui ka olemasolevate) puhul, hõlmates nii artikli 50 lõikeid 2 kui ka 4, et viia need kooskõlla tegevusjuhendiga (Code of Practice). ○ **Kõrge riskiga süsteemide kindlad kohaldamiskuupäevad:** määrata tähtajad kindlalt — lisa III puhul detsember 2027 ja lisa I puhul august 2028 — ning kõrvaldada sõltuvus haldusotsustest. ○ **Vastavushindajate valikuvabadus:** võimaldada teenuseosutajatel valida vastavushindaja ELi tasandi ja liikmesriikide asutuste vahel, et vältida kitsaskohti ja ära hoida lukustumist Komisjoni määratud üksusesse.	Arvestatud osaliselt. Eesti toetab suure riskiga süsteemide jõustumistähtaja sidumist vajalike juhendite ja standarditega. Rakendustähtaeg peab olema konkreetne. Muude tähtaegade edasilükkamine ei ole digiomnibussi skoobis ega mõistlik. Vastavushindamise osas, praeguse ettepaneku pinnalt ei tundu kitsaskohti sellega ka olevat.
27.	Tartu Ülikool	**Üldised kommentaarid** Standardite valmimise ja digital omnibusi planeeritud muudatuste jõustumise ebaselge tähtaeg tekitab suurt ebakindlust ja teadmatust tulevaste projektide osas.	Teadmiseks võetud.
28.		**Isikuandmete mõiste** • Identifitseerimise kriteeriumide ebaselgus Mõistlikult tuvastada ("*means reasonably likely to be used to identify the natural person*") jääb subjektiivseks mõisteks. Kuigi eesmärk on luua õigusselgust, tekib küsimus:	Arvestatud.

		• kes määrab, mis on “mõistlikult tuvastatav”? Kelle jaoks mõistlikult? Milline on see “mõistlik” kompetents või mille alusel seda hinnata? • kas täna “mittemõistlik” vahend võib homme muutuda “mõistlikuks” ja tavapäraseks? • Vastutuse hajumine Muudatus loob olukorra, kus sama info võib olla ühe osapoole jaoks isikuandmed, teise jaoks mitte. Probleemid: • kui andmeid jagatakse mitme vahendaja kaudu, võib tekkida vastutuse "hall tsoon"; • andmesubjekti õiguste (juurdepääs, kustutamine) rakendamine muutub keeruliseks; • rikkumiste korral on raske määrata, kes kannab vastutust. • Kontrollimise ja vastutava töötleja paradoks Dokument ütleb, et organisatsioonid peavad kontrollima, kas jagatud andmed on isikuandmed või mitte (andmete saajale), kuid: • kuidas saab andmeedastaja teada, millised vahendid on andmete vastuvõtjal? • kas andmete edastaja peab uurima vastuvõtja tehnilisi võimekusi? • tekib vastuolu: organisatsioon ei ole vastutav töötleja, aga peab kontrollima. • Muud kommentaarid • Kuigi eesmärk on õiguskindluse suurendamine, võib tegelikult tekkida rohkem kohtuvaidlusi termini "mõistlik" tõlgendamise üle. • Isikul on raskem jälgida, kes nende andmeid töötleb (näiteks kui osapool ei pea end	

		isikuandmete töötlejaks) ja sellest lähtuvalt on isik ka nõrgemas positsioonis oma õiguste maksma panemisel. • Praeguses sõnastuses näeme ohtu, et kohustustest kõrvale hiilimiseks hakatakse liiga lõdvalt tõlgendama taasidendifitseerimise võimalust. Kuidas reguleeritakse sh, millised kohustused ja õigused on andmete töötlejal, kes "mõistlikul viisil" ei suuda andmed taasidentifitseerida? Milline on tema roll GDPR mõistes? Kui andmed edastatakse kolmandale töötlejale, kes suudab andmed identifitseerida, mis on tema roll? Kuidas tagada, et andmete töölemine põhineb õiguslikul alusel ja kes vastutab, kui peaks toimuma rikkumine? • <u>Näited</u> • **Näide 1.** Kuidas tõlgendatakse antud muudatuste valguses IP-aadressi. Nt vastutav töötleja kogub ankeedi kaudu andmeid, edastab need analüüsiks volitatud töötlejale, kellel ei ole võimalik ligi pääseda informatsioonile, mille abil andmesubjekte identifitseerida ja IP-aadressi abil tuvastad. Kui andmestikus ei ole ka muid andmeid, mis lubaks andmesubjekti tuvastada, kas siis on vajalik Data Prosessing Agreement (DPA), kui tegu ei ole enam isikuandmetega? Kas DPA-s sätestab vastutav töötleja tingimused, et volitatud töötleja tohib/ei tohi andmeid muul eesmärgil kasutada/edastada? Millistel juhtudel on DPA vajalik? Või kuna volitatud töötleja ei töötle isikuandmeid võib ta andmeid edasi töödelda ja edastada tingimusel, et veendub, et vastuvõtja ei suuda sammuti IP-	

		aadresite järgi isikuid tuvastada ja tema roll muutub sel juhul kelleks (GDPR mõistes)? • **Näide 2.** Terviseandmete liikumine: avaliku sektori raviasutus väljastab pseudonüümitud andmed teadusuuringu läbiviimiseks. Oletame, et teadusuuringu meeskond ja vastutav uurija hindab, et ei suuda "mõistlikult" andmesubjekte identifitseerida, kas teadusuuringu meeskond töötleb isikuandmeid? • Kui näidetes 1 ja 2 nimetatud volitatud töötleja edastab andmed uuele osapoolele või toimub rikkumine, kus andmed satuvad kolmandate osapoolte valdusesse, kes suudavad taasisikustada andmesubjekte, siis kuidas jaotuvad rollid? Kes on vastutav töötleja, kes on volitatud töötleja ja millised kohutused rakenduvad volitatud töötlejale?	
29.		**AI ja eriliiki andmed** • "*Appropriate measures*" ebaselgus o Puuduvad konkreetsed kriteeriumid, mis on "asjakohased organisatsioonilised ja tehnilised meetmed". o Probleemiks saavad erinevad tõlgendused eri organisatsioonides ja järelevalveasutustes. o Väiksematel ettevõtetel puudub suutlikkus hinnata meetmete piisavust. • "*Disproportionate effort*" lävend o Ei ole määratletud, millal eemaldamine nõuab "ebaproportsionaalset pingutust". o Suurettevõtted võivad kasutada seda väljapääsuna ja tegelikult andmeid mitte eemaldada.	Arvestatud.

		○ Majandusliku kasu vs andmesubjekti õiguste tasakaal on ebaselge. • "*Without undue delay*" ajaraamistiku puudumine. Ei täpsustata, mis on „alusetu viivitus“. See võib vastavalt kontekstile tähendada erinevaid aegu ja puudub selge järelevalve või vastutus viivituste eest. • Eeldatav nõusolek puudub Punkt (k) võimaldab eriliiki andmete töötlemist AI kontekstis ilma selge nõusolekuta, mis on vastuolus GDPRi põhimõtetega, kus eriliiki andmed nõuavad selgesõnalist nõusolekut. Andmesubjekt ei pruugi teada, et tema andmeid kasutatakse AI arenduses.	
30.		**Automatiseeritud otsused, sh profileerimine** • "*Necessity*" kriteeriumi nõrgendamine Uue tõlgenduse järgi peab automatiseeritud otsuse tegemine olema "vajalik", isegi kui on alternatiive ja see loob olukorra, kus organisatsioonid saavad õigustada peaaegu iga automatiseeritud otsust. Organisatsioonid võivad väita, et automatiseeritud otsused on vajalikud efektiivsuse/kulude kokkuhoiu jaoks ja eksisteerib risk, et igasugune äriline eesmärk tõlgendatakse “vajalikkuseks". Ei eristata madala ja kõrge riskiga otsuseid - sama lähenemine kehtib nii töölevõtmisel kui ka kontosaldo kontrollimisel.	Teadmiseks võetud.
31.		**Mõjuhinnang (DPIA)** • Hetkel saavad liikmesriigid kohandada DPIA nõudeid vastavalt kohalikele oludele ja ühtne EL-i nimekiri võib ignoreerida riigispetsiifilisi riske ja vajadusi.	Arvestatud.

		• On oht, et nimekiri võib olla liiga üldine (ei anna praktilist juhist, jääb kasutuks) või liiga spetsiifiline (ei sobi kõikide harude/sektorite jaoks). • EL'i otsustusprotsess on aeglane, kuid uued tehnoloogiad arenevad väga kiiresti. Eksisteerib risk, et loodav nimekiri on alati "aegunud". • Eestis on AKI andnud suunised ja hinnangud, millal on tegu suure riskiga töötlemisega ja millistel puhkudel on andmekaitsealane mõjuhinnang kindlasti vajalik aga komisjoni poolt antavad selged juhised ja template avaldaks kindlasti positiivset mõju mõjuhinnangute ühtlasemale kvaliteedile ja annaks andmesubjektidele ja töötlejatele suurema kindluse, et mõjuhinnang on läbi viidud piisava põhjalikkusega.	
32.		**Andmesubjekti päring** Juba praegu olemas GDPR-is, täiendus ei ole tingimata vajalik. Praegune GDPRi sõnastus on asjakohane ja täidab eesmärki.	Arvestatud.
33.		**Teavitamine** • Probleem - läbipaistvus väheneb. Andmesubjektid jäävad teadmatuks paljudest rikkumistest, mis neid mõjutavad ja kaob võimalus ise kasutusele võtta meetmeid (nt parooli vahetamine). • Lisandunud 24 tundi on abiks ründajatele - andmete edasimüük pimeturul, identiteedivargused jne. • "*Likely to result in high risk*" on subjektiivne hindamine. Organisatsioon ise otsustab, kas risk on "kõrge" ja sellest tekib potentsiaalne konflikt, kuna ettevõtted ei taha halba mainet ning risk alandatakse näiteks "see küll ei ole nii kõrge risk". "High risk" tähendus võib ja kindlasti ka varieerub liikmesriigiti, mis lisab kindlasti täiendavat segadust.	Arvestatud. Eesti ei poolda rikkumisest teavitamise lävendi tõstmist. SEPi osas on Euroopa Komisjon andnud selgitusi, et see ei ole mõeldud ainult piiriüleste juhtumite korral, vaid ka siis, kui tegemist on riigisisese intsidendiga. Tagasisides esitatud kommentaarid teavituste erinevate lävendite ja teavitamistähtaegade osas on asjakohased näited, millede kohta

		• "*Single-entry point (SEP)*" on mõeldud piiriüleste töötluste jaoks ning kui rikkumine mõjutab ainult üht riiki, on SEP kaudu teavitamine ebatõhus, kuna lisandub täiendav bürokraatia (suunamine). SEP võib osutuda ka kõige nõrgemaks lüliks, kui ta on üle koormatud või mingil põhjusel ei tööta. • NIS2 direktiiv nõuab samuti rikkumiste teatamist (erineva läve ja tähtajaga), DORA (finantssektoris) on omad nõuded jne. Ettevõtted peavad navigeerima mitme paralleelse süsteemi vahel. • Suure riskiga intsidentide teavitamiskohustuse erinevad tähtajad loodavas SEP-s. Kas intsidendist teavitaja peab eelnevalt ise klassifitseerima, millise intsidendiga on tegu (NIS2 24h vs GDPR 72->96h). Kuidas liiguvad esmalt andmekaitsealase intsidendina teavitatud rikkumise andmed õigete osapoolteni, kui selgub, et tegu oli siiski ka küberturvalisuse intsidendiga, millel on palju lühem teavitamise tähtaeg? Kas sellisel juhul on teavitaja eksinud ja vastutab, et pole teavitamiskohustusest kinni pidanud? Siseriiklikul tasandil on AKI loonud teavitajale vormi ja lihtsa viisi teavitamiseks, vajadus tuleneb mõne teise riigi järelvalve asutuse tegematusest pigem. • Mis juhtub olukorras, kui esmane rikkumine tundub "madala riskiga", kuid hiljem selgub, et tegemist on osaga suuremast rünnakust? Kuna hakkab 96 tundi jooksma? Kas alates esmasest rünnakust või hetkest, kui selgub täiendav informatsioon?	soovime eelnõu valmimise selgust ja konkreetsust saada.
34.		**Teadusuuringute mõiste** Teadusuuringu mõiste lisamine GDPR-i on igati tervitatav, seni oleme lähtunud siseriiklikust definitsioonist (TAKS) ja mõiste defineerimine looks suurem selguse, eriti EU sisese piiriülese	Teadmiseks võetud.

		andmetöötluse osas, kuid leiame, et praeguse sõnastuse juures on suur oht seda liiga vabalt tõlgendada. Praegune sõnastus defineerib pigem erasektori tegevust.	
35.	Andmekaitse Liit	**Kas toetate eelnõudes toodud eesmärke ja pakutud lahendusi? Palun tooge välja, milliseid toetate ja miks? Milliseid ettepanekuid Teie ei toeta ja miks?** Osaliselt toetame art 12(5) (andmesubjekti päringutele vastamine), art 13(4) (privaatsusteabe esitamise piirangud), art 35 (andmekaitsealase mõjuhinnangu nõuded) muudatusi, kuna nendega lihtsustakse eelkõige väike ja keskmistel ettevõtetel IKÜMi mõistlikku rakendamist. Samas ei toeta me Art 12(5) muudatuse ettepaneku seda osa, mis näeb ette, et andmesubjektid võivad oma isikuandmete kohta teabe saamiseks esitada päringu vaid isikuandmete kaitselistel eesmärkidel ehk „andmesubjekt kuritarvitab antud õigusi muul eesmärgil kui oma andmete kaitsmine“, sest on küsitav kas pakutud piirang on proportsionaalne. Täiesti sisustamata on mõiste “oma andmete kaitsmise eesmärk” ning kui see õigus jätta vastutavatele töötlejatele, siis läheb see otsesse vastuollu IKÜMi läbipaistvuse ja vastutuse põhimõttega. Näiteks võib isikuandmete vastutav töötleja isegi keelduda päringule vastamast, kui tema hinnangul ei ole selline päring esitatud andmekaitselisel eesmärgil. Sellisel juhul on andmesubjektil võimalik ilmselt pöörduda järelevalveasutuse poole, kelle ülesandeks tundub saavat ka päringu eesmärgi hindamine ning hindamine, kas vastutav töötleja peab päringule vastama või ei. On ilmselge, et vastutavate töötlejate huvides on võimalikult palju sellistele päringutele mittevastamine, mistõttu näeme, et pakutud lahendus võib tekitada täiendavat koormust järelevalveasutusele ning ei taga andmesubjektide õigust teada kuidas nende isikuandmetega ümber käiakse. Toetame ka art 33 muutmise ettepanekut, millega	Arvestatud osaliselt. Tähtaegade osas toome välja, et on problemaatiline, et sama platvormi kaudu on teavitamistel erinevad tähtajad. Toetame suure riskiga AI tähtaegade edasi lükkamist kuni valmivad Komisjoni poolt vajalikud standardid ja juhised. Eesti ei toeta AI arendamise ja opereerimise õiguslike aluste kinni kirjutamist. Kõik IKÜMi õiguslikus alused andmetöötluseks on võimalikud, olenevalt olukorrast. Juhime tähelepanu, et AI määrus ei loo eraldi õiguslikku alust AI süsteemide andmetöötluseks.

		ühtlustatakse andmesubjekti ja järelevalveasutuse isikuandmete alase rikkumise teavitamise nõue mõlemat tuleb teavitada ainult kõrge riskiga rikkumiste puhul. See vähendaks nii vastutavate töötlejate kui järelevalveasutuste töökoormust ning aitaks keskenduda kõrge riskiga juhtumite menetlemisele ja kahjulike tagajärgede maandamisele. Usume, et see on olnud ka täna Eesti järelevalveasutuste ootus. Toetame ka teavitamise tähtajapikendamist 96-le tunnile. See leevendaks eelkõige olukordi kus tähtaja arvestuse sisse jääb nädalavahetus. Tervitame AI omnibusi loogikat, et kohustuste täitmine lükatakse edasi seniks, kuni on töötatud välja tööriistad (standardid ja juhised) vastavate kohustuste rakendamiseks. Samuti toetame pisemaid muudatusi nagu nt kitsaste protseduuriliste toimingute puhul kõrge riskiga tehisintellekti kohustuste vähendamine (st kui high risk AI puhul on ainult AI element tegemas narrow procedural task'i, ei pea seda high risk AI-na registreerima). Toetame ka eriliigiliste isikuandmete töötlemiseks selge õigusliku aluse loomist AI mudelite kallutatuse vältimiseks. Toetame AI omnibusi võimalikult kiiret läbi menetlemist, eriti Tehisaru määruse kõrge riski kohustuste edasilükkamise vaatest, et vältida olukorda, kus kohustused hakkavad kehtima enne, kui neid edasi lükatakse. Praegune olukord tekitab ettevõtetele ebakindlust ja võimalikke ebamõistlikke kulusid.	
36.		**Kas toetate avaandmete direktiivi muutumist määruseks? Kas näete, et oleks vajalik muuta väärtuslike andmestike nimekirju. Kui jah, siis kuidas ja miks?** EAKL-I arvates on hetkel seadustes mida digital omnibus ümber kujundab, nii Andmehalduse kui Andmemäärus, täpselt defineerimata mis on "avaandmed" ja mis on "avalikud andmed". Parima praktika tava järgi on avaandmed need, mida creative commons litsentsiga saab	Arvestatud osaliselt. Lisatud on seisukoht ühendamise süsteemsusest. Samuti on seisukoht selles osas, mis on avaandmete ja isikuandmete vahekord. Avaandmete

		iga soovija ükskõik mispidi analüüsida ja kasutada (ja avaandmeteks ei tohiks olla isikuandmed) ning avalikud andmed on need, mida kodanikud (ja ettevõtted ning asutused) on riigile kohustatud seaduse alusel esitama ja riik on kohustatud kodanikele avalikustama. Ilmselgelt on riigi käes olevad andmed väärtuslikud ning nende põhjal lisaväärtuse loomine oleks hüve mitte ainult riigile, vaid ka kodanikele, eriti kui lisaväärtus kodanike elu paremaks teeb, kuid see ei peaks tulema riigi kodanike privaatsusõiguste arvelt. Uus planeeritav Avaandmete määrus, mis ühendab siis Andmehalduse ja Andmemääruse peaks sisaldama konkreetset definitsiooni mille järgi avaliku sektori asutused saaksid aru, mis on siis avaandmed ja mis avalikud andmed. Uue Avaandmete määruse ning Andmemääruses olevad nõuded andmete avaldamise (disclosure) võiksid sisaldada ka täpsemaid suuniseid – andmete kvaliteedi ja hulga kohta ja avaldamise sageduse kohta, kuna andmete avaldamine ei ole tasuta avaldajale ning piisava kvaliteedi puudumine ei võimalda andmetest lisandväärtust toota. **Millised aspektid ja ettepanekud vajaksid täpsustamist või lisaselgitusi, et oleksid praktikas rakendatavad?** Pooldame ühtset teavituskanalit, et sama rikkumise pinnalt ei tuleks mitmes kohas ning mitu korda teavitada. Samas teeb ühtse teavituse keeruliseks erinevates aktides toodud erinevad teavitustähtajad ning tekib küsimus, et kui küberturbe intsident on samal ajal kui andmekaitse intsident, siis kas peab jätkuvalt esitama mitu teavitust (24h möödumisel NIS2 esmane teavitus, 72h möödumisel NIS2 teisene teavitus ja 96h möödumisel GDPR teavitus?). Seetõttu teeksime ettepaneku ühtlustada ka ühtse teavituskanali kaudu edastatavate teavituste tähtaegasid.	mõistet on avatud avaandmete direktiivi põhjenduspunktis 16 ja AvTS § 3^1 lg 1. Arvestatud ja selgitame: tagasisides esitatud kommentaarid teavituste erinevate lävendite ja teavitamistähtaegade osas on asjakohased näited, millede kohta soovime eelnõu valmimise selgust ja konkreetsust saada.

		Art 4 (1) “Isikuandmed” (Personal data) - mõiste muudatused on tekitanud väga elavad diskussiooni erialases ringkonnas. Mõistame Komisjoni soovi juurutada Ühtse Kriisilahendusnõukogu (SRB) lahendist tulenevat praktikat, kui omnibuses toodud mõiste SRB lahendiga võrreldes laiendatud. Pooldame seda, et selgitatakse ja defineeritakse täpsemalt konteksti, millistel juhtudel ei ole isikuandmed enam isikuandmed nign milliseid andmekaitse nõudeid ei peaks täitma olukorras, kus päriselt andmete saajal ei ole mõistlikult võimalik isikut enam antud andmete pinnalt tuvastada. Leiame, et seda oleks võimalik reguleerida ka selliselt, et sisustada täpsemalt pseudonüümimise mõiste ja siduda see kohustusega viia läbi regulaarset hindamist, et hinnata kas pseudonüümimine on piisavalt tugev. Isikuandmete mõiste praeguse sõnastuse laiendamine tekitab küsimusi selles osas, kuidas praktikas rakendada. Täpsemalt, milliseid andmekaitse nõudeid peab täitma juhul, kui saaja jaoks ei ole andmed enam isikuandmed. Näiteks kas on vajalik andmetöötluslepingu sõlmimine, kui vastutava töötleja vaatest on tegemist isikuandmetega, kuid saaja vaatest ei ole saadavad andmed isikustatud andmed. Sarnased küsimused võivad tekkida ka muude vastutava töötleja kohustuste täitmisel (nt andmelekkest teavitamine, Transfer Impact Assessment (TIA), volitatud töötlejate avaldamine andmesubjektile jms). Teeme ettepaneku selgelt IKÜM-is sätestada, et juhul, kui saaja jaoks ei ole tegemist isikuandmetega, ei ole kohustust sõlmida ka andmetöötluslepingut. AI treenimise/arendamise õiguslikud alused. Aastaid nähti vaeva, et hoida IKÜM tehnoloogianeutraalne, kuid nüüd on sisse kirjutatud konkreetse tehnoloogiaga seotud sätted. Kuigi tervitame, et on selgelt välja toodud, et eriliigilisi isikuandmeid võib kasutada AI kallutatuse vähendamiseks,	Arvestatud osaliselt treenimise ja arendamise õiguslike aluste seisukohta. Õiguslikke aluseid pole vaja kinni kirjutada. Kõik IKÜMis väljatoodud õiguslikud alused isikuandmete töötlemiseks võivad olla kohased. Lisaks avalikul sektoril pole võimalik AI-d treenida õigustatud huvi ega üldjuhul ka nõusoleku alusel. Tehnoloogianeutraalsuse seisukoht on lisatud.

		tundub AI treenimise üldise õigusliku aluse lisamine IKÜM-isse liigne ja ebavajalik. Ka muude tehnoloogiate puhul käib arendustegevus sisuliselt õigustatud huvi või isiku nõusoleku alusel. Seetõttu leiame, et ka täna kehtiv regulatsioon võimaldab AI treenimist viia läbi õigustatud huvi ja nõusoleku alusel. Antud sätete lisamine võib tekitada küsimusi, et kas muude tehnoloogiate arendamise puhul ei saa enam kasutada õigusliku alusena õigustatud huvi. Tervitame küpsiste klausli täpsustamist ja selle isikuandmeid puudutava osa toomist IKÜMisse, kuid see täpsustus ei ole siiski piisavalt kaugeleulatuva mõjuga, et anda andmesubjektile tegelik ülevaade veebis toimuva jälitamistegevuse (tracking) kohta. ePrivaatsuse direktiivilt IKÜM-le üleminek reguleerimaks isikuandmete töötlemist lõppkasutaja seadmes uue IKÜM artikli 88a kaudu tuues üle ePrivaatsuse art 5 lõige 3 “lõppkasutaja seadmesse salvestatule on vaja lõppkasutaja nõusolekut”, mõningate täiendustega, näiteks on piiratud nimekiri madala riskiga ja vajalikest eesmärkidest, mis ei vaja õiguspäraseks toimimiseks nõusolekut (nt edastamine; selgesõnaliselt taotletud teenus; sihtrühma mõõtmine vastutava töötleja enda tarbeks; turvalisuse tagamine). Kuid ikka räägitakse ainult küpsistest ja nõusolekutest küpsistele, jättes tähelepanuta jälitamise (tracking) muud tehnoloogiad ning jälitamise vajalikkuse või õiguspärasuse. EAKL ei ole kindel, et väljapakutud muudatused toovad kaasa selguse teiste jälgivate tehnoloogiate puhul (pixel, eTag etc), mille puhul võib vaielda, et lõppkasutaja seadmesse siiski midagi ei salvestata. Ehk oleks võinud Euroopa Komisjon siin julgem olla ning defineerinud tehnoloogia mittespetsiifilise veebis jälgimise vastuvõetavad tingimused? Küsitav on ka, et kas lihtsalt küpsiseid reguleerides on võimalik lahendada niinimetatud „nõusoleku väsimus“? Küpsiste puhul, kui veebilehitsejate standardid on	Teadmiseks võetud. Nõus selles osas, et e-Privaatsuse direktiiv vajab ajakohastamist ning ei tohiks enam keskenduda ainult teabe salvestamisele lõppseadmesse, vaid tuua kaasa selguse jälitamise tehnoloogiate kasutamises.

		praktilised ja kasutajakogemus selge, on võimalik nõusoleku väsimuse vähendamine, ilma nõusoleku tugevust õigusliku alusena kahjustamata. Samas on positiivne, et koos IKÜM artikliga 88b saab komisjon mandaadi brauseri/ rakenduse vahendatud nõusolekute andmise standardiseerimiseks; kui standardid on kehtestatud, peavad vastutavad töötlejad pärast lühikest ajapikendust austama masinloetavaid kasutajavalikuid, kusjuures nende puhul, kes neid järgivad, eeldatakse vastavust.	
37.		**Kas on Eesti jaoks spetsiifilisi aspekte, mis mõjutavad valdkonna seniseid praktikaid. Palun tooge konkreetseid näiteid, viidake võimalusel analüüsidele, raportitele.** ROPA (isikuandmete töötlemise register) kohustuse kehtestamine 750 või enama töötajaga ettevõtetele – Eesti kontekstis tundub, et selline muudatus võib tekitada praktikas probleeme. ROPA on andmekaitsekohustuste keskpunkt, mille olemasolu tagab ja aitab ka teiste andmekaitse kohustuste täitmist praktikas teostada. Kui seda pole, siis on praktiliselt ettevõtetel keerukas ka koostada nt privaatsusteadet ajakohasena, vastata andmesubjekti päringutele, kiirelt reageerida andmeleketele jms. Lisaks sellele võib jääda mulje, et kui on 750 või vähem töötajat, siis pole eriti vaja andmekaitse vaatest pingutada ning see ei aita tõsta teadlikkust andmekaitse teemade olulisusest laiemalt (vajalik ka nt tõhusa andmehalduse ja AI rakendamiseks). Lisaks on ülevaade ettevõtte või asutuse andmetöötlemise toimingutest ja kasutatavatest rakendustest vajalik selleks, et andmetest lisaväärtust saada. Lisaks on Eestis väga palju isikuandmete vastutavaid töötlejaid, kus töötab vähem kui 750 inimest. Seega Eesti suhtes tähendaks selline piirang seda, et väga paljud ettevõtted vabaneksid väga olulisest kohustusest. Võibolla tuleks tekitada võimalus liikmesriigil seda piirangut ise muuta, et iga liikmesriik saaks	Teadmiseks võetud.

		omale sobiva mugavduse teha ja näiteks lähtuda isikuandmete kogusest, mida töödeldakse.	
38.		**Palun tooge välja muud teemad, mis on nimetatud aktide puhul Teile murekohaks.** Andmete töötlemise dokumenteerimise kohustust ei peaks muutma. See on IKÜM halduskoormusest kõige suurema väärtusega osa ettevõtte või asutuse jaoks. Teades mis andmeid ettevõte töötleb võimaldab rohkemat kui IKÜM-ga vastavus, võimaldab ka andmete abil teha paremaid juhtimis- ja äriotsuseid	Teadmiseks võetud.
39.	Transpordiamet	**<u>Isikuandmete töötlemine</u>** Isik peab teadma, kuidas ja miks tema andmeid kasutatakse Eelnõu lihtsustab mitmete digiteenuste reegleid ja loob võimalusi andmete kiiremaks liikumiseks. Samas tuleb tagada, et: • isikuandmeid ei jagataks automaatselt ilma selge teavituseta; • isik teab alati, milleks tema andmeid kasutatakse ja kui kauaks; • andmete jagamist peab olema võimalik igal hetkel peatada. Andmete kogumine peab jääma minimaalseks Andmekaitse seisukohalt on oluline, et: • kogutakse ainult neid andmeid, mis on konkreetselt vajalikud, • vältida tuleb “igaks juhuks” kogumist,	Teadmiseks võetud.

		• infosüsteemi arhitektuur ei tohi soosida ülemäärast andmete töötlemist. Teenusepakkujate rollid ja vastutused tuleb täpselt lahti kirjutada Eelnõu peab selgelt määratlema: • kes vastutab andmete turvalisuse eest, • kus andmeid hoitakse, • millised turvanõuded on kohustuslikud, • kuidas järelevalve tegelikult toimub. Vastasel juhul võib vastutus muutuda hajusaks, mis on risk nii kasutajale kui ka asutustele. Andmete kasutamine peab olema jälgitav – kõik andmetega tehtavad toimingud (vaatamine, kasutamine, edastamine) peavad olema logitud ja kontrollitavad. Ilma jälgitavuseta ei ole võimalik hiljem tuvastada rikkumisi ega tagada andmete turvalisust.	
40.		**<u>Infoturve</u>** Pooldame *Single-Entry Point* tekitamist, kuid tähtajad vajavad täpsustamist (eri õigusaktides eri tähtajad – vajab ühtlustamist).	Arvestatud – vastav seisukoht on koostatud.
41.		**<u>Andmehaldus</u>** Toetame andmeõiguse erinevate aktide liitmist andmemäärusega, sest seeläbi muutuvad kohalduvad õigusaktid arusaadavamaks ja paremini leitavaks. Hetkel on õigusaktid liiga killustunud.	Arvestatud.

		Avaandmete direktiivi muutmine määruseks – loodav määrus peaks jätma teatud paindlikkuse, et oleks võimalik arvestada riigi erisustega.	
42.	Kaubandus- ja Tööstuskoda	**Õigusraamistiku ühtlustamine** Kaubanduskoda toetab algatuse eesmärki lihtsustada, ühtlustada ja muuta selgemaks kehtivaid mahukaid digivaldkonna õigusakte. Toetame suunda koondada asjakohane regulatsioon otsekohalduvatesse määrustesse, mis aitab vähendada õigusruumi killustatust liikmesriikide vahel. On oluline, et lihtsustamisprotsess vähendaks reaalset halduskoormust, eelkõige väike- ja keskmise suurusega ettevõtjate jaoks.	Teadmiseks võetud.
43.		**Isikuandmete kaitse üldmääruse (GDPR) ja küpsiste reeglite ajakohastamine** Peame positiivseks püüdlust lihtsustada isikuandmete kaitse üldmääruse (IKÜM/GDPR) ja küpsiste kasutamisega seotud nõudeid. Kaubanduskoja liikmed on välja toonud, et küpsiste ja isikuandmete kaitse üldmääruse rakendamist puudutavad punktid on ettevõtjate vaatest muutumas lihtsamaks ja selgemaks. Peame äärmiselt positiivseks püüdlust leevendada nn nõusoleku-väsimust läbi küpsiste klausli täpsustamise ning isikuandmeid puudutava osa integreerimise IKÜM-i raamistikku. Toetame kavandatavaid muudatusi, millega lihtsustatakse väikeettevõtjate jaoks töötlemistoimingute registri pidamist, privaatsusteabe esitamist ja andmekaitse mõjuhinnangute koostamist, kuna see tagab regulatsiooni mõistlikuma ja jõukohasema rakendamise.	Arvestatud osaliselt. Toome välja, et ohu lävendi tõstmine ei võimalda järelevalveasutustel oma kohustuste täitmist.

		Samuti toetame järelevalveasutuse teavitamise kohustuse piiramist vaid kõrge riskiga rikkumiste puhul ning teavitamise tähtaja pikendamist 96 tunnini, mis vähendab nii vastutavate töötlejate kui ka järelevalveasutuste töökoormust ja võimaldab keskenduda reaalselt ohtlike intsidentide menetlemisele.	
44.	Politsei- ja Piirivalveamet	1. Isikuandmete mõiste muutmine (isikuandmed on kontekstipõhised) Isikuandmete mõiste muutumine selliselt, et andmete kvalifitseerumine isikuandmeteks sõltub kontekstist ja mõistlikult kasutatavatest vahenditest, võib PPA hinnangul tuua kaasa mõiste tõlgendamise erinevused nii erinevate sektorite kui EL liikmesriikide vahel ning riski mõiste pahatahtlikuks ärakasutamiseks, mis võib õõnestada õiguskindlust ja isikuandmete ühtset kaitsetaset. Juhul, kui isikuandmete mõiste soovitakse siiski kontekstipõhiseks muuta, tuleb PPA hinnangul sätestada selged kriteeriumid ja siduvad juhised, et vältida subjektiivseid tõlgendamisi.	Arvestatud. Eesti ei toeta mõiste muutmist, kuid teeb ettepaneku täiendada IKÜM põhjenduspunkti selgitusega, et mõiste sisutamisel tuleb arvestada kohtupraktikaga.
45.		2. Andmekaitserikkumistest teavitamise tähtaja muutmine 72 tunnilt 96 tunnini PPA hinnangul tagab kehtiv 72-tunnine tähtaeg andmekaitserikkumistest teavitamiseks kiire reageerimise kõrge riskiga intsidentidele ning selle pikendamise korral 96 tunnini võib suure riskiga intsidendi korral olla iga lisapäev kahju piiramisel kriitilise tähtsusega. Ühtlasi, kuna täiendava info edastamine on võimalik ka pärast esmase teavituse tegemist, ei ole	Arvestatud. SEP osas on koostatud seisukoht, et eri õigusaktide alusel tehtavate

		esialgse teavitusega viivitamine põhjendatud ega tähtaja pikendamine vajalik. Lisaks eelnevale ning seoses intsidentidest teavitamise ühe akna (Single-Entry Point ehk SEP) loomisega, tekib ka küsimus, kuidas suhestub planeeritav muudatus muud liiki intsidentidest teavitamise tähtajaga (72h), mis ei muutu – eelkõige tekitab küsimusi asjaolu, et andmekaitsealane intsident võib samal ajal olla ka küberintsident. Eelnevast tulenevalt on PPA ettepanek säilitada senine 72-tunnine tähtaeg igat liiki intsidentidest teavitamiseks.	intsidentide esitamise tähtaega tuleks ühtlustada.
46.		3. Eriliiki isikuandmete kasutamine tehisintellekti arendamiseks ja toimimiseks Kuigi muudatusettepaneku eesmärk on soodustada innovatsiooni, tekitab see siiski mitmeid tõsiseid küsimusi, nt kuidas maandada turvariske ning kuidas on tagatud põhiõiguste kaitse (kui eriliiki isikuandmed satuvad tehisintellekti mudelitesse). Muuhulgas kaasneb muudatusega ka vajadus väga selgete juhiste osas, kuidas ja milliseid tehnilisi ja organisatsioonilisi meetmeid tuleb järgida, kuidas viia läbi riskihindamist ja seda dokumenteerida, millised on täpsed piirangud ja reeglid jms.	Arvestatud osaliselt. Eesti on seisukohal, et eristada tuleb selgelt arendamise ja toimimise etappe ja neid nii ka reguleerida. Eesti ei toeta isikuandmete töötlemisaluste kinni kirjutamist tehisintellekti arendamisel/treenimisel.
47.		4. Täiendavad ettepanekud tehisintellekti määruse muutmiseks 4.1. Õiguskaitseasutuste (law enforcement authority) ulatus ja kohustused PPA hinnangul ei hõlma õiguskaitseasutuse definitsioon ühisarenduste olukordi, kus osalevad nii avalikud kui eraõiguslikud partnerid. Seega tekib küsimus, kuidas määratleda	Mitte arvestada. Isikuandmete töötlemise vaatest on rollid endiselt vastutav ja volitatud töötleja. IKÜMi ja LED reeglid on selleks piisvad. AI määrus ei pea ega tohikski neid üle kirjutada. Õiguskaitseasustus on defineeritud

		teenusepakkuja (provider) ja vastutused, kui tehisintellektisüsteemid arendatakse ühiselt. PPA ettepanek on määratleda selgelt õiguskaitseasutuse definitsioon, mis kajastaks nende tegevuste ulatust, eriti koostööprojektides teiste asutuste, ettevõtete ja teadusasutustega. See aitab vältida ebaselgust ning tagab ühtse rakendamise. Täiendavalt juhib PPA tähelepanu, et kui tehisintellektisüsteeme arendatakse ühiselt ja kasutatakse ühiseid andmeid, tekib olukord, mis sarnaneb GDPR artikli 26 ja LED artikli 21 joint controllership mudelile. Sellest tulenevalt on PPA ettepanek rakendada tehisintellektimääruses sama mudelit ja määratleda mitme teenusepakkuja vastutus (joint providers). See looks nii läbipaistvuse, stabiilsuse kui ka vastavuse tehisintellektimääruse nõuetega.	AI määruse artiklis 3 punkti 45. Koostöö projektides rollid on samad, mis AI määruse art 3 defineeritud.
48.		4.2. Tehisintellektisüsteemide pakkujate ja kasutajate vaheline läbipaistvus PPA hinnangul on peamine probleem, et õiguskaitseasutused, kes kasutavad kõrge riskiga tehisintellektisüsteeme, ei saa alati täielikku tehnilist juurdepääsu kommertspakkujate loodud süsteemidele, kuna need on kaitstud ärisaladuste ja intellektuaalomandi seadustega. See omakorda raskendab tehisintellektimääruse nõuete täitmist, eriti vastutuse ja dokumentatsiooni osas. PPA hinnangul on vaja selgeid ja praktilisi juhiseid tehisintellektisüsteemide pakkujate ja kasutajate (deployers) rollide, vastutuse ja andmete jagamise kohustuse osas. Eelkõige on vaja täpsustada järgmist:	Mitte arvestada. Kehtivas AI määruses on juba rollid ja neile kohalduvad reeglid.

		• Kasutajad peavad saama täita oma juriidilisi kohustusi vastavalt tehisintellektimäärusele ning neil peab olema vajalik juurdepääs pakkujate dokumentidele, et täita oma hoolsuskohustust. • Pakkujad säilitavad vastutuse tagada, et tehisintellektisüsteem on kujundatud ja dokumenteeritud viisil, mis võimaldab kasutajal täita kehtivaid kohustusi, mis võib tähendada ka täieliku tehnilise info avaldamist kasutajatele. • Standardiseeritud lepingulised klauslid või mallid võiksid toetada ühtsust EL liikmesriikide vahel, tagades selle, et pakkujad jagavad piisavalt teavet, kaitstes samal ajal siiski ettevõtte ärisaladusi või intellektuaalomandit.	
49.		4.3. Andmete valideerimine ja tehisintellektisüsteemide treenimine PPA hinnangul on andmete valideerimisel ja tehisintellektisüsteemide treenimisel peamine probleem tehisintellektimääruse koostoime olemasolevate õigusaktidega, nagu GDPR ja LED. Samuti on oluline välja tuua, et: • tehisintellektisüsteemide kvaliteet ja usaldusväärsus sõltuvad kõrgekvaliteediliste treeningandmete kättesaadavusest. • suurte andmehulkade töötlemisel on õiguslikud takistused. • GDPR-i artikli 6 alusel andmete uuesti töötlemine ei ole realistlik, sest nõuded on killustatud ja keerulised. Eelnevast tulenevalt on PPA ettepanek täpsustada rakendusjuhistes võimalusi andmetele ligipääsuks ja nende taaskasutuseks, et vältida GDPR-i ja LED-iga seotud lahknevusi ja liikmesriikide erinevaid tõlgendusi. Samuti on PPA hinnangul vaja täpsustada GDPR-i artikleid 5 ja 6 ehk vaja on juhiseid	Mitte arvestada. Aktid on koostoimelised. IKÜM ja LED kohalduvad tehisarule nagu igale teisele isikuandmetöötlusele.

		proportsionaalsuse ja vajalikkuse testide rakendamiseks tehisintellektisüsteemide treenimisel.	
50.	Kodanik	1 Sissejuhatus 1.1 Omnibus 1.1.1 Euroopa Komisjon (EK) on teinud ettepaneku ulatusliku muudatuste paketi kohta ELi digitaalses õigusraamistikus. Nende ettepanekute, mida koondnimetusena nimetatakse digitaalseks Omnibusiks (Digital Omnibus), eesmärk on ajakohastada ja ühtlustada digiregulatsioone liikmesriikide vahel. Digitaalne Omnibus hõlmab olemasolevate õigusaktide muudatusi ning uusi raamistikke, et lahendada esilekerkivaid probleeme digikeskkonnas. Liikmesriigid kujundavad praegu oma seisukohti nende ettepanekute suhtes ning järgmine tagasiside on mõeldud sisendina nende aruteludeks. 1.2 Taust 1.2.1 Kuigi praegustes aruteludes domineerivad mured liigse andmekogumise ja eraelu puutumatuse vähenemise pärast, on oluline pöörduda tagasi eraelu puutumatuse õiguse alusprintsiipide juurde. See õigus loodi põhiprobleemi lahendamiseks: üksikisikute kaitsmiseks põhjendamatu sekkumise, jälgimise ja isikuandmete väärkasutuse eest – nii analoogses kui ka digitaalses kontekstis. 1.2.2 Digitaalse Omnibusi määruse ettepanek (november 2025): link 1.2.3 Euroopal on pikaajaline traditsioon tunnustada eraelu puutumatuse olulisust. Peaaegu pool sajandit tagasi, 1981. aastal, võttis Euroopa Nõukogu vastu konventsiooni 108 – esimese	Teadmiseks võetud.

		õiguslikult siduva rahvusvahelise lepingu, mis keskendus andmekaitsele. Konventsioon 108 käsitles riske, mis kaasnesid arvutustehnoloogia üha laialdasema kasutamisega profileerimise tõhustamiseks ning isikuandmete kuritarvitamise võimalusega. 1.2.4 Arvutusvõimsuse ja andmetöötlusvõimekuse arenguga on kasvanud ka profileerimise ja jälgimise keerukus. Eraelu puutumatuse õiguse algset eesmärki mõistes saab selgeks, et õigusaktid peavad arenema koos tehnoloogilise arenguga. Selles kontekstis mängis Euroopa Komisjoni konkurentsivolinik Margrethe Vestager keskset rolli digiregulatsioonide edendamisel, sealhulgas isikuandmete kaitse üldmääruse (GDPR) ja teiste algatuste puhul, mille eesmärk oli tugevdada tarbija- ja digiõigusi. 1.2.5 Lühikese aja jooksul saavutas EL selle, mida paljud pidasid turu- ja tarbijaõiguste reguleerimise kullastandardiks, eriti tehnoloogiasektoris. Hilisemad aruanded, nagu Draghi aruanne ja Letta aruanne, tõid aga esile uued väljakutsed ja võimalused edasiseks reformiks. Need aruanded kujundasid EK hiljutised ettepanekud, sh digitaalse Omnibussi. 1.2.6 Letta aruanne ühtse turu tuleviku kohta (aprill 2024): link 1.2.7 Draghi aruanne ELi konkurentsivõime kohta (september 2024): link 1.3 Probleem 1.3.1 Nii Letta aruanne kui ka Draghi aruanne toovad esile regulatiivse koormuse kui ühe teguri, mis pärsib innovatsiooni ja seeläbi ka ELi konkurentsivõimet. Siiski on oluline märkida, et kumbki aruanne ei käsitle digiõigusi – näiteks eraelu puutumatust – esmase probleemina. Digiõigusi käsitletakse pigem teiseste	

		kaalutlustena, keskendudes muudele süsteemsetele küsimustele, nagu turu killustatus, jõustamisraskused ja halduslik ebatõhusus. 1.3.2 Aruanded ei kutsu üles digiõiguste kaotamisele ega nõrgestamisele. Näiteks ei soovita kumbki aruanne viia ELi standardeid kooskõlla leebemate režiimidega eraelu puutumatuse või tarbijakaitse arvelt. Vastupidi, Letta aruanne tunnistab selgesõnaliselt ELi regulatiivse raamistiku mõju üleilmsetele standarditele nn Brüsseli efekti kaudu, rõhutades tugeva digiõiguste kaitse olulisust. 1.3.3 Mõlema aruande rõhuasetus on ELi poliitikate koordineerimisel, ühtlustamisel ja lihtsustamisel. Neid eesmärke käsitletakse viisidena tõhususe ja konkurentsivõime parandamiseks, mitte olemasolevate digiõiguste raamistike, nagu GDPR, õõnestamiseks. 1.4 Teisisõnu 1.4.1 Oluline on eristada aruannete järeldusi ja Euroopa Komisjoni pakutud lahendusi. Aruanded toovad esile probleemid ja võimalused, kuid EK pakutud lahendused – näiteks digitaalses Omnibussis – võivad neid väljakutseid tõlgendada või käsitleda erinevalt. Näiteks: 1.4.1.1 Regulatsioonide lihtsustamine ja koondamine ei tähenda iseenesest digiõiguste nõrgestamist. Selle eesmärk võib olla hoopis dubleerimise vähendamine ja selguse suurendamine. 1.4.1.2 Poliitikate jõustamise ebakõlade kõrvaldamine ei võrdu olemasolevate seaduste, nagu GDPR, eesmärkide hülgamisega. See võib tähendada üksnes tõhusamat rakendamist.	

		1.4.2 Digitaalse Omnibussi sihtmärgiks olevad õigusaktid loodi algselt konkreetsete probleemide lahendamiseks, näiteks üksikisikute kaitsmiseks põhjendamatu jälgimise ja andmete väärkasutuse eest. Enne nende seaduste muutmist on kriitiline küsida: kas algsed probleemid on lahendatud? Kui mitte, siis millised on kaitsemeetmete vähendamise või kaotamise riskid? 1.4.2.1 Millised on regulatiivsete prioriteetide nihutamise võimalikud tagajärjed? Näiteks kas konkurentsivõime kasv võib tulla usalduse või põhiõiguste arvelt?	
51.		2 Kavandatav lahendus 2.1 Enne kui alustame 2.1.1 Enne kui analüüsida, mida digitaalses Omnibussis koondatakse või muudetakse, on oluline esile tõsta see, mis deregulatiivse suuna raames on välja jäetud. Need väljajätmised on märgilised, sest need puudutavad ELi digivalitsemise raamistiku olulisi osi, mis olid mõeldud uute probleemide lahendamiseks, kuid on nüüd kas hüljatud või edasi lükatud. 2.1.2 ELi lähenemine tehisintellekti reguleerimisele oli algselt kavandatud kaheastmelise raamistikuna: 2.1.2.1 Tehisintellekti määrus (AI Act, AIA): keskendub tehisintellektisüsteemide klassifitseerimisele ja juhtimisele, sealhulgas riskipõhisele jaotusele ja vastavusnõuetele. 2.1.2.2 Tehisintellekti vastutuse direktiiv (AI Liability Directive, AILD): pidi kehtestama selged reeglid tehisintellekti põhjustatud kahjude eest vastutuse kohta, tagades vastutuse ja õiguskaitsevahendid mõjutatud isikutele.	Teadmiseks võetud.

		2.1.3 Euroopa Parlamenti kinnitati, et kui AIA vastu võetakse, järgneb sellele AILD, et raamistik oleks terviklik. AILD on aga vahepeal laiemate deregulatiivsete eesmärkide raames tühistatud. See jätab ELi kavandatud tehisintellekti valitsemisstruktuurist alles vaid poole ning tekitab vastutuse ja õiguskaitse osas regulatiivse lünga. 2.1.4 2002. aastal vastu võetud e-privaatsuse direktiiv oli ammu moderniseerimist vajanud. Euroopa Komisjon tegi ettepaneku asendada see e-privaatsuse määrusega, mis oleks: 2.1.4.1 kehtestanud otsekohalduva regulatsiooni (mitte direktiivi, mis vajab ülevõtmist), tugevdanud kasutajate nõusolekunõudeid elektroonilises suhtluses ning pakkunud tugevat kaitset metaandmetele ja digitaalsele kommunikatsioonile. 2.1.5 Selle väljajätmine jätab ELi digiõiguste raamistikku märkimisväärse lünga. 2.1.6 Märkus: digitaalse Omnibussi praegusel versioonil puuduvad põhjalikud mõjuhinnangud kavandatavate muudatuste kohta. Kavandatud lahendusi tuleks hinnata mõjuhinnangute kaudu, mis arvestavad nii majanduslikke kui ka põhiõigustega seotud mõjusid. See tagaks, et muudatused on kooskõlas ELi pikaajalise pühendumusega digiõigustele ning lahendavad samal ajal aruannetes tuvastatud praktilisi probleeme. 2.2 Mis koondatakse 2.2.1 Nagu varem märgitud, ei tähenda regulatsioonide lihtsustamine ja koondamine iseenesest digiõiguste nõrgestamist. Selle eesmärk võib olla dubleerimise vähendamine ja selguse suurendamine. Üldjoontes tundub see osa (mis koondatakse)	

		vähem problemaatiline kui järgmine (mis muudetakse), välja arvatud e-privaatsuse regulatsiooni tühistamine. 2.2.1.1 Avatud andmete direktiiv (ODD, 2019/1024): viidud andmemäärusesse (Data Act). 2.2.1.2 Andmehalduse määrus (DGA, 2022/868, II peatükk): andmevahenduse ja avaliku sektori andmete taaskasutuse reeglid viidud andmemäärusesse. 2.2.1.3 Platvormilt ettevõtjale määrus (P2B, 2019/1150): tunnistatud kehtetuks, kuna selle eesmärgid on nüüd suures osas kaetud digitaalturgude määruse ja digiteenuste määrusega. 2.2.1.4 Mitteisikuandmete vaba liikumise määrus (FFNDR, 2018/1807): tunnistatud kehtetuks, põhireeglid (nt põhjendamatu andmete lokaliseerimise keeld) viidud andmemäärusesse. 2.2.1.5 e-privaatsuse direktiiv (2002/58/EÜ): tunnistatud kehtetuks, osa selle sätteid (eriti küpsiste ja jälgimise kohta) integreeritakse GDPRi. 2.2.2 Ühtne intsidentide teavitamise punkt: uus digitaalne tööriist võimaldab ettevõtetel teatada küberturbeintsidentidest ja andmeleketest üks kord, täites korraga mitme õigusakti (nt NIS2, GDPR, DORA, eIDAS, CER) nõudeid. 2.3 Mis muudetakse 2.3.1 GDPR – isikuandmete määratlus 2.3.1.1 Praegune määratlus: objektiivne. Andmeid käsitatakse „isikuandmetena”, kui need on seotud tuvastatud või tuvastatava	

		isikuga, sõltumata sellest, kas vastutav töötleja saab isiku tegelikult tuvastada. Kavandatav määratlus: subjektiivne. Andmed on „isikuandmed" ainult siis, kui konkreetne töötleja suudab isikut realistlikult tuvastada. 2.3.1.2 Näide: kui „ettevõte A" omab pseudonüümitud andmeid, kuid tal puudub võti isikute taas-tuvastamiseks, ei oleks need tema jaoks enam „isikuandmed" – isegi kui „ettevõte B" suudaks need andmed tuvastada. Tagajärg: Euroopa Komisjon saaks määrata, millal pseudonüümitud andmed ei ole teatud üksuste jaoks enam isikuandmed. Riskid: subjektiivsed lüngad, jõustamisraskused, õiguslik ebakindlus ja võimalikud vastuolud ELi põhiõiguste hartaga. 2.3.1.3 Subjektiivsed lüngad: töötlejad võiksid ise deklareerida, et andmed ei ole isikuandmed, muutes järelevalve peaaegu võimatuks. Õiguslik ebakindlus: muudatused käivitaksid aastatepikkuse kohtuvaidluste laine. Vastuolu hartaga: ettepanek langetab kaitsetaset alla direktiivi 95/46 taseme, millele harta viitab miinimumstandardina. 2.3.2 GDPR – teadusuuringute erandid 2.3.2.1 Kavandatud muudatused: laiad erandid „igasugusele teadusuuringule", mis „võib toetada innovatsiooni" või hõlmab „olemasolevate teadmiste uuel viisil rakendamist" (nt	

		tehisintellekti treenimine). Nõue järgida „eetilisi standardeid", mis on sageli määratlemata või tööstuse kujundatud. 2.3.2.2 Riskid: äriettevõtted võiksid GDPRist mööda hiilida, nimetades tegevuse „teadusuuringuks". See õõnestab GDPRi põhimõtteid nagu eesmärgipärasus ja andmete minimeerimine ning ei täida harta artikli 8 nõutud vajalikkuse ja proportsionaalsuse kriteeriume. 2.3.3 Lisaks 2.3.3.1 Kavandatud muudatused: töötlejad võivad jätta andmetöötluse kohta teabe andmata, kui: – töötlemine toimub „teadusuuringute eesmärgil"; – teabe andmine on „võimatu" või nõuab „ebaproportsionaalset pingutust"; – avaldamine „tõsiselt kahjustaks" uurimise eesmärke. 2.3.3.2 Riskid: nõrgestab läbipaistvust, mis on GDPRi alustala. Andmesubjektid võivad kaotada võimaluse oma õigusi kasutada. „Teadusuuringu" lai määratlus võib hõlmata peaaegu iga teisest andmekasutust. 2.3.4 Tehisintellekt – õigustatud huvi 2.3.4.1 Kavandatav tekst: isikuandmete töötlemist tehisintellekti arendamiseks ja kasutamiseks võib pidada õigustatud huviks, kui see ei kaalu üles andmesubjekti õigusi ja vabadusi ning rakendatakse sobivaid kaitsemeetmeid. 2.3.4.2 Mõju: loob eelduse, et tehisintellektiga seotud töötlemine on õigustatud, nihutades tõendamiskoormuse andmesubjektidele ja luues tehnoloogiaspetsiifilise erandi.	

		2.3.5 Tehisintellekt – kaitsemeetmed 2.3.5.1 Kavandatud kaitsemeetmed: andmete minimeerimine, suurem läbipaistvus, tingimusteta õigus esitada vastuväide. 2.3.5.2 Probleemid: ebamäärane sõnastus, raskused järelevalves ja rakendamises. 2.3.6 Tehisintellekt – mured 2.3.6.1 Tehnoloogianeutraalsuse hülgamine, õiguslik ebakindlus, jõustamisraskused. 2.3.6.2 Avalike andmete kasutamine treenimiseks, biomeetriliste andmete töötlemine ja vastuväiteõiguse praktiline piiratus. 2.3.6.3 Artikkel 88c võib nõrgendada andmekaitset, suurendada ebakindlust ja soodustada suuri tehnoloogiaettevõtteid. 2.3.7 Märkus 2.3.7.1 AI Acti kõrge riskiga süsteemide nõuete jõustumine on edasi lükatud. 2.3.7.2 Harmoneeritud standardid ja juhised ei ole 2025. aasta lõpu seisuga valmis, mis suurendab ebakindlust eriti VKEde jaoks. 3 Kokkuvõte 3.1 Digitaalne Omnibus toob muudatusi, mis vähendavad küll koormust, kuid tekitavad märkimisväärset ebamäärasust ja riske. 3.1.1 Selgus vs ebakindlus: tekib oht, et keerukus hoopis suureneb, eriti VKEde jaoks.	

		3.1.2 Tasakaalu puudumine: vastutuse raamistik on puudulik, eriti AILD tühistamise tõttu. 3.1.3 Kooskõla põhiõiguste hartaga: oht õõnestada artiklit 8 ja GDPRi aluspõhimõtteid. 3.1.4 Kolmandate osapoolte eelis: suured tehnoloogiaettevõtted võivad ebaproportsionaalselt võita; VKEde olukord võib halveneda. 3.2 Seetõttu 3.2.1 Palume käsitleda kogu dokumendis esile toodud puudujääke. 3.2.2 Põhiküsimused: kuidas probleem määratleti, milliseid alternatiive kaaluti ja kas dereguleerimine on saanud sama põhjaliku analüüsi kui varasemad, põhiõigusi austavad lahendused.	
52.	Eesti Infotehnoloogia ja Telekommunikatsiooni Liit	1. ITL toetab algatuse eesmärki kehtivaid keerulisi ja mahukaid õigusakte lihtsustada. Mitmed paketis sisalduvad muudatused on Eesti ettevõtetele kasulikud, s.h need mis puuduvad just väiksemaid ettevõtteid. Seega leiame, et Eesti võiks lihtsustamispaketile toetust avaldada, kuna see on õige suund ning selles pakutakse välja lahendusi mitmele murele, mida turuosalised on praktikas tõstatanud. 2. Toetame muudatusi, mis lihtsustavad andmete kasutamist ning vähendavad osapoolte jaoks bürokraatiat. Näiteks kohustuslike aruannete vormide asendamist vabatahtlikega ja registreerimiskohustuste vähendamist.	Teadmiseks võetud

		3. Toetame seda, et erinevad andmealased õigusaktid liidetakse üheks õigusaktiks ehk kogu asjakohane regulatsioon koondatakse andmemäärusse. Varasemalt oleme leidnud, et esimese sammuna tuleks hetkel kehtivad ja peagi jõustuvad EL-i õigusaktid üle vaadata, eemaldada nende ülekatted ja kõrvaldada vastuolud ning regulatsiooni oluliselt lihtsustada ja alles siis mõelda konsolideerimise peale. Euroopa Komisjon pakub digiomnibussiga neid samme koos ning see tundub mõistlik, eriti kuna palju regulatsioone tunnistatakse ka kehtetuks. 4. Üldpõhimõttena toetame ka seni direktiivides sisalduva regulatsiooni viimist määrusesse kui otsekohalduvasse õigusakti. Peame selle all silmas andmealaseid õigusakte, kuna selles valdkonnas on juba palju otsekohalduvaid määruseid ning seetõttu võiks kogu asjakohane regulatsioon kehtida määrusena. 5. Peame oluliseks, et töö digivaldkonna õigusaktide lihtsustamise nimel jätkuks, kuna antud pakett on alles esimene samm. Seejuures on oluline arvestada suuremat eesmärki tagada õiguskindlusja selgus ehk anda osapooltele aega regulatsioone rakendada, teha nende mõjude ja tulemuste kohta järeldusi ning hoiduda pidevast muutmisest ja uute kohustuste kehtestamisest. Eesmärk lihtsustada ja halduskoormust vähendada on väga hea, kuid tähendab ka, et niipea digivaldkonnas veel õigusrahu oodata pole.	
53.		Andmemäärusega 1.1. Toetame ettepaneku artikkel 1 punkte 6 ja 7, millega kitsendatakse ettevõtetelt riigile andmete andmise kohustust ainult hädaolukorras andmete andmisele. Nõustume, et kehtivas andmemääruse on see kohustus liiga ulatuslik.	Arvestatud osaliselt. Hädaolukorras andmete küsimise seisukoht läks sisse. IaaS ja PaaS teema ei ole omnibussi Komisjoni poolt pakutud ja seega see ettepanek läheb skoobist välja. Nende teenuste

		1.2. Teeme ettepaneku kaaluda eelnõuga lisaks sõnaselgelt IaaS ja PaaS teenuste väljavõtmist andmemääruse teenuseosutaja vahetamise ja andmete ülekantavuse (switching portability) skoobist, kuivõrd nende teenuste olemusest tulenevalt ei ole see praktikas tehniliselt mõistlikult rakendatav. 1.3. Toetame ettepaneku artikkel 1 punkti 3, millega kehtestatakse täiendavad tingimused, mis võimaldava andmete omanikest ettevõtetel kaitsta oma ärisaladust. Leiame, et sellest meetmest on abi ettevõtetel, kes on kohustatud andmemääruse kohaselt teatud tingimustel oma klientide andmeid väljastama teistele ettevõtetele. Juhul, kui digiomnibussi edasise menetluse käigus tuleb arutlusele ka ettepanek erasektori andmete kohustusliku jagamise vabatahtlikuks muutmiseks andmemääruses, siis tuleb suhtuda sellesse ettevaatlikult ning kindlasti analüüsida hoolikalt selle kasusid ja kahjusid. Erasektori ja eelkõige väiksemate teenus- või tootmisettevõtete (näiteks põllumajanduse sektoris) poolt vaadatuna on andmemäärusega kehtestatud B2B andmejagamise kohustus siiski kasulik, kuna võimaldab saada suurtelt tööstusettevõtetelt vajalikke andmeid, mille peale saab ehitada uusi innovaatilisi teenuseid ja pakkuda tarbijatele suuremat valikut, näiteks valida seadmete hooldusteenuse pakkujaid.	väljavõtmist ei toetatud, kuivõrd siin ka tarbija huvid. Tehniliselt rakendamine võimalik, eeldab ühtseid aluseid (vt andmemääruse art 35). Põhiõigustega kooskõla seisukoht on lisatud. IKÜM kohaldub.
54.		2. Avaandmete direktiiviga 2.1. Digiomnibuss sisaldab ettepanekut tunnistada avaandmete direktiiv kehtetuks ja hõlmata selles sisalduv andmemäärusesse. See tähendaks, et seni direktiiviga reguleeritu tuleb Eesti avaliku teabe seaduses kehtetuks tunnistada, kuna kohalduma hakkab EL-i otsekohalduv regulatsioon. Selle ettepaneku osas seisukoha kujundamiseks on vaja analüüsida, mida selline muudatus praktikas Eestis kaasa tooks.	Arvestatud.

		Kuna avaliku sektori käes olevate andmete avamine on seni kulgenud üsna vaevaliselt, siis kui otsekohalduv määrus sätestaks selle selgema kohustusena ja andmete avamine kulgeks edukamalt, peame vajalikuks seda toetada. 2.2. Meil puuduvad hetkel ettepanekud väärtuslike andmete nimekirja muutmiseks. Toetame seda, et liikmesriikidele on jäetud otsustusvabadus ja see võimaldab Eestis siseriiklikult täiendavaid väärtuslikke andmestikke nimetada. 2.3. Märgime, et avaandmete direktiivist andmemäärusesse toodavate sätete osas (ettepaneku artikkel 1 punktiga 18 lisatav peatükk VIIc) tekitab küsimust andmete ja dokumentide eristamine. Kord nimetatakse neid koos ja teinekord eraldi. Seetõttu on raske aru saada, mida täpsemalt mõeldakse. Samuti, kuidas see seostub andmemääruses andmete definitsiooniga (andmemääruse art 2 punktiga 1: andmed on tegevuse, faktide või teabe ning sellise tegevuse, faktide või teabe kogumi digitaalne väljendus, muu hulgas heli-, visuaal- või audiovisuaalsalvestise kujul). 2.4. Avaliku sektori avaandmete (seda just toorandmete – raw data) kättesaadavaks tegemine peaks printsiibis olema tasuta. Vaid väärindatud andmete kättesaadavaks tegemine võib olla tasuline. Ettepaneku artikkel 1 lõikega 2 lisatakse andmemääruse artiklisse 2 punt 61, millega defineeritakse investeeringutasuvus. Andmemäärusesse lisatav artikkel 32q lubab investeerimistasuvust arvestada avaandmete eest nõutava tasu puhul. Oleme seisukohal, et avaandmete puhul ei tohiks investeeringutasu arvesse võtmine olla lubatud, kuna need investeeringud on tehtud maksumaksja raha eest ning see on juba olnud ühiskonna ühine panus.	

55.		3.1. Isikuandmete kaitse üldmääruse (IKÜM) muudatuste osas on seni olnud nii Euroopa kui ka Eesti ettevõtted pigem ettevaatlikud peljates selle avamist. Ka praegu on näha, et tegemist on kõige rohkem tähelepanu saava osaga digiomnibussist. Juba on tehtud ka ettepanekuid menetleda IKÜM-it puudutavaid ettepanekuid muust paketist eraldi, et need ei saaks takistuseks kiirel edasiliikumisel. Toome omalt poolt välja, et koos tehisintellekti määruse võimalike muudatustega menetlemise positiivne pool seisneb selles, et siis on reaalselt olemas selged kasutusjuhud tehisintellekti jaoks vajalike andmete/andmestike põhjal ehk koosmõju on kindlasti olemas ning vajab arvestamist. Lisame, et kuna IKÜM-I muudatusi on palju ning need on seotud kogu digiomnibussi eelnõu teiste sätetega, siis põhjalikku analüüsi saaks teha, kui oleks olemas eelnõu terviktekst. 3.2. Isikuandmete mõistet puudutavad muudatused: 3.2.1.IKÜM artikli 4 lg 1 ehk isikuandmete mõiste muudatused on tekitanud väga elavat diskussiooni erialases ringkonnas. Mõistame Euroopa Komisjoni soovi juurutada Euroopa Kohtu otsusest EDPS vs SRB (C-413/23) tulenevat praktikat, kui ettepanekus toodud mõistet on sellest tulenevalt oluliselt laiendatud. Pooldame seda, et mitte kõiki andmekaitse nõudeid ei peaks täitma olukorras, kus tegelikkuses andmete saajal ei ole mõistlikult võimalik isikut antud andmete pinnalt tuvastada. Samas oleks seda võimalik reguleerida ka selliselt, et sisustada täpsemalt pseudonüümimise mõiste ja siduda see kohustusega seda ajas hinnata. SRB lahendis on selgelt vastutava töötleja pingutuse element sisse kirjutatud, s.t ta peab midagi eraldi tegema selleks, et teine pool ei saaks isikuid enam tuvastada. ITL-ina tervitame seda lähenemist. Samuti saaks täpsemalt reguleerida, millal loetakse andmeid pseudonüümituks ning kohustada võtma arvesse	Arvestatud osaliselt. Isikuandmete mõiste osas ei toeta Eesti mõiste täiendamist ning palub täiendada IKÜM põhjenduspunkti selgitusega, et mõiste sisustamisel tuleb arvestada kohtupraktikaga. Eesti ei toeta ka ohu lävendi tõstmist teavitamisel, kuna see raskendab järelevalveasutusel oma kohustuste täitmist. Eesti toetab erinevates õigusaktides olevate teavituste tähtaegade ühtlustamist. Teadusuuringu mõiste osas võtame arvamus teadmiseks, selgitame, et IKÜM-i eesmärk ei ole kitsenda teadusuuringute tegemist üksnes teadusasutustega vaid innovatsiooni tegemise võimalus peab olema laiemalt. AI treenimise/arendamise õiguslike aluste kinni kirjutamist ei toeta. Selgitused eespool ning seisukohtades. Eriliigiliste andmete kasutamine kallutatavuse tuvastamisel ja sellekohased PETid on seisukohtades arvestatud.

		mis iganes tehnoloogilisi või keskkonnas toimunud arenguid, mille puhul peab uuesti hindama, kas võetud meetmed on olnud piisavad. 3.2.2.Isikuandmete mõiste praeguse sõnastuse laiendamine tekitab küsimusi selles osas, kuidas muudatust praktikas rakendada. Täpsemalt, milliseid andmekaitse nõudeid peab täitma juhul, kui saaja jaoks ei ole andmed enam isikuandmed. Näiteks kas on vajalik andmetöötluslepingu sõlmimine, kui vastutava töötleja vaatest on tegemist isikuandmetega, kuid saaja vaatest ei ole saadavad andmed isikustatud andmed. Sarnased küsimused võivad tekkida ka muude vastutava töötleja kohustuste täitmisel (nt andmelekkest teavitamine, andmeedastuse mõju hindamine, volitatud töötlejate avaldamine andmesubjektile jms). 3.2.3.Teeme ettepaneku selgelt IKÜM-is sätestada, et juhul, kui saaja jaoks ei ole tegemist isikuandmetega, ei ole kohustust sõlmida ka andmetöötluslepingut. 3.3. Toetame muudatusi millega IKÜM art 12 lg 5 (töötlemistoimingute registri piirangud), art 13 lg 4 (privaatsusteabe esitamise piirangud) ja art 35 (andmekaitse mõjuhinnangu nõuded) alusel lihtsustakse eelkõige väike- ja keskmistel ettevõtetel IKÜM mõistlikku rakendamist. 3.4. Töötlemistoimingute registri kohustuse kehtestamine 750 või enama töötajaga ettevõtetele võib aga Eesti kontekstis tekitada praktikas probleeme. Töötlemistoimingute register on andmekaitsekohustuste keskpunkt, mille olemasolu tagab ja aitab ka teiste andmekaitse kohustuste täitmist praktikas teostada. Kui seda pole, siis on praktiliselt ettevõtetel keerukas ka koostada näiteks privaatsusteadet ajakohasena, vastata andmesubjekti päringutele, kiirelt reageerida andmeleketele jms. Lisaks sellele	

		võib jääda mulje, et kui on 750 või vähem töötajat, siis pole eriti vaja andmekaitse vaatest pingutada ning see ei aita tõsta teadlikkust andmekaitse teemade olulisusest laiemalt. Näiteks on töötlemistoimingute register vajalik ka tõhusa andmehalduse ja tehisintellekti rakendamiseks. 3.5. Toetame IKÜM art 33 muutmise ettepanekut, mille kohaselt kehtiks järelevalveasutusele isikuandmete nõuete rikkumisest teavitamise kohustus ainult kõrge riskiga rikkumiste puhul. See vähendaks nii vastutavate töötlejate kui ka järelevalveasutuste töökoormust ning aitaks keskenduda kõrge riskiga juhtumite menetlemisele ja kahjulike tagajärgede maandamisele. Usume, et see on olnud ka täna järelevalveasutuste ootus. Toetame ka teavitamise tähtaja pikendamist 96-le tunnile. See leevendaks eelkõige olukordi kus tähtaja arvestuse sisse jääb nädalavahetus. 3.6. Seoses tehisintellekti treenimise ja arendamise õiguslikke aluseid puudutava muudatusega märgime, et tegemist on olulise muudatusega, kuna seni tehnoloogianeutraalsena hoitud IKÜM-isse soovitakse sisse kirjutada konkreetse tehnoloogiaga seotud sätted. Esiteks toetame muudatust, millega tuuakse selgelt välja, et eriliigilisi isikuandmeid võib kasutada tehisintellekti kallutatavuse vähendamiseks. Teiselt poolt vajab meie hinnangul täiendavat kaalumist ja arutelusid tehisintellekti treenimise üldise õigusliku aluse lisamine IKÜM-isse. Meie hinnangul võiks see alus sisalduda pigem tehisintellekti määruses, kuna IKÜM-it võiks hoida jätkuvalt tehnoloogianeutraalsena, et seda tuleviku arengutele mõeldes mitte kinni kirjutada. 3.7. Ettepanekuga artikkel 3 lõikega 1 soovitakse IKÜM-is defineerida teadusuuring ning lõikega 2 muuta avalikes huvides hilisem töötlemine arhiveerimise, teadus- või ajaloolise uurimistöö või statistilistel eesmärkidel esialgse töötlemise	

		eesmärgiga ühilduvaks. Analüüsimist vajab, mida see praktikas tähendaks ning kuidas mõjuks isikuandmete kaitsele, kuna need eesmärgid on väga laiad. Samuti tekitab teadusuuringu defineerimine IKÜM-is küsimuse, miks seda vaja on, kui teadusmaailm lähtub selleks Frascati käsiraamatust 2015 „Teadusuuringuid ja eksperimentaalarendust käsitlevate andmete kogumise ja esitamise suunised“.	
56.		4. ePrivaatsuse direktiiviga 4.1. Tervitame küpsiste klausli täpsustamist ja selle isikuandmeid puudutava osa toomist IKÜMisse. 4.2. Avaldame sektori poolt ootuse, et digiomnibussi ettepanekuga võiks pakkuda lahenduse ka ülejäänud ePrivaatsuse direktiivi osas. ITL on seisukohal, et ePrivaatsuse direktiiv vajab ülevaatamist tervikuna, jätkuvalt reguleerimist vajavate teemade reguleerimist muude õigusaktidega ning eraldiseisva õigusaktina kehtetuks tunnistamist.	Teadmiseks võetud. Selgitame, et Eesti toetab e-Privaatsuse direktiivi ajakohastamist ja isikuandmete töötlemise IKÜMi alla viimist. e-Privaatsuse direktiivi sätteid muudetakse ka DNA aktiga.
57.		5. Intsidentide raporteerimisega: 5.1. Küberturvalisus on sarnaselt andmevaldkonnale väga ulatuslikult reguleeritud. Antud juhul on Euroopa Komisjon otsustanud lahendada vaid väga väikse osa murest ehk pakub välja ainult ühise teavitamiskanali loomise et sama rikkumise pinnalt ei tuleks mitmes kohas ning mitu korda teavitada et sama rikkumise pinnalt ei tuleks mitmes kohas ning mitu korda teavitada. Selline üks teavitamiskanal on kindlasti tervitatav, eriti piiriüleselt tegutsevate ettevõtete jaoks, ning me toetame seda. Ühtse teavituskanali kasutamist võiks kaaluda ka veel täiendavate õigusaktide tarbeks, nt tehisintellekti määrus. Samas võiks lihtsustamise eesmärki silmas pidades olla ambitsioonikam ning	

		ühtlustada ka teavitamise aegasid, vorme jm EL-i küberturvalisuse õigusaktides. 5.2. Ühtse teavituskanali loomine tekitab kohe ka küsimuse sellest, et teavitamise tähtajad on õigusaktides väga erinevad. Näiteks NIS2 direktiivi kohaselt tuleb esmane teavitus küberintsidendist esitada 24h jooksul, isikuandmeid puudutavast intsidendist on samas digiomnibussi ettepaneku kohaselt aega teavitada 96h ehk see vahe on märkimisväärne. Selleks, et kohuslased saaksid ühtset teavituskanalit kasutada, peaksid nad justkui lähtuma iga teavituse puhul kõige lühemast tähtajast, mis ei arvestada asjaoludega, mida neid tähtaegu määrates silmas peeti ehk sellega, et teavituse koostamiseks on teatud juhtudel vaja rohkem aega. Teine variant oleks, et ikkagi tuleb esitada mitu teavitust: 24h möödumisel NIS2 esmane teavitus, 72h möödumisel NIS2 teine teavitus ja 96h möödumisel IKÜM teavitus. Just seetõttu on oluline lisada digiomnibussi ka ühtse teavituskanali kaudu edastatavate teavituste tähtaegade ühtlustamine. 5.3. Seoses NIS2 direktiivi ja DORA-ga tõstatame ka teema, mis vajab EL-i õigusaktide tasemel lahendamist ning on väga vajalik ettevõtete halduskoormuse vähendamiseks ja regulatsioonide lihtsustamiseks. Kehtivate õigusaktide kohaselt on DORA subjektid vabastatud NIS2 täitmisest, kuid NIS2 subjektid, kes osutavad teenuseid DORA subjektidele, peavad vastama ka DORA-le. See tekitab NIS2 subjektidest IKT teenuse osutajatele, kes soovivad oma teenuseid osutada ka finantssektori asutustele, väga suurt koormust. Seetõttu teeme ettepaneku lisada digi omnibussi NIS2 ja DORA muutmine selliselt, NIS2 direktiivi kohuslased, kes osutavad finantssektori asututele IKT teenuseid, ei pea tõendama eraldi DORA-le vastavust, vaid need	5.1. ja 5.2. Arvestatud 5.3. Arvestatud, vastav seisukoht on koostatud

		turvanõuded tunnistatakse samaväärseteks, kui nad vastavad NIS2 alusel kehtestatud nõuetele. Oleme seisukohal, et Eesti võiks olla selle olulise muudatuse eestkõneleja.	
58.	Riigi Infosüsteemi Amet	**Üldhinnangud eelnõudes toodud eesmärkidele ja pakutud lahendustele** 1. RIA vaatest on eelnõudes toodud üldised eesmärgid – reeglite ühtlustamine, killustatuse vähendamine ja parema õigusselguse loomine – põhimõtteliselt toetatavad. Eesti digiriigi toimimine eeldab, et andmete taaskasutuse, turvalisuse ja kättesaadavuse reeglid oleksid võimalikult selged ja üheselt mõistetavad. 2. Samas on RIA jaoks oluline, et pakutud lahendused ei tooks kaasa olukorda, kus tehniline vastutus ja õiguslik vastutus ei ole omavahel kooskõlas. Kui kohustused muutuvad vahetult kohaldatavaks ELi määruse kaudu, peab olema selge, millises ulatuses eeldatakse RIA-lt tehnilist hinnangut, nõustamist või järelevalvelist rolli ning millal on tegemist teiste asutuste pädevusega. Lahendusi, mis jätavad selle piiri ebaselgeks, ei saa pidada piisavalt praktiliseks. 3. Seoses isikuandmete töötlemise reeglitega AI arendamisel ja kasutamisel on RIA jaoks oluline tagada, et arvestatakse ka avaliku sektori vajadustega. Näiteks peaks lubatud isikuandmete töötlemise õiguslikud alused hõlmama riigi poolt isikuandmete töötlemiseks kasutatavaid aluseid.	Arvestatud.
59.		**Avaandmete direktiivi muutumine määruseks** 1. Avaandmete direktiivi muutumine määruseks on RIA vaates põhimõtteliselt toetatav, kuna see vähendab liikmesriikide vahelisi erinevusi ja loob ühtlasema õiguskeskkonna. Samas on oluline, et määruse tekst arvestaks selgelt küberturbe ja teenuste töökindluse aspektiga. RIA kogemus näitab, et masinloetavus ja API-põhine ligipääs ei ole pelgalt tehniline mugavus, vaid ka	Arvestatud osaliselt. Kõikide avaandmete osas piiranguid pole sätestatud ja see läheb ka omnibussi eesmärgist kaugele. Seisukohades välja toodud, et täiendavate väärtuslike andmestike kategooria kehtestamisel tuleb arvestada

		potentsiaalne riskivektor. Seetõttu peab määrus võimaldama proportsionaalseid kaitsemeetmeid, nagu ligipääsupiirangud, kasutusmahupiirid ja autentimine, ilma et neid käsitataks avaandmete põhimõtte rikkumisena. Väärtuslike andmestike nimekirjade osas on oluline, et nende laiendamine toimuks koos selge riskihinnangu loogikaga. Eesti kontekstis võib näiteks haldus- ja menetlusandmetel olla suur ühiskondlik väärtus, kuid nende avamine ilma piisavate turva- ja privaatsusmehhanismideta looks märkimisväärseid riske nii andmekaitse kui ka küberturbe vaates.	loodava ELi ühtse avaandmete määruseks mõjuga väiksematele liikmesriikidele ning liikmesriikidele peab jääma piisav otsustusvabadus väärtuslike andmestike kujundamisel. Autentimise nõue, ligipääsupiirangud lähevad kaitsemeetmetena tavapärasest avaandmete lähenemisest kaugemale ning piiraks Euroopa Liidu üleselt kui ka rahvusvaheliselt andmete taaskasutamist, ning ei saa toetada.
60.		**Praktiline rakendatavus** 2. Praktilise rakendatavuse seisukohalt vajab RIA hinnangul täpsustamist eelkõige rollijaotus. Tuleb selgelt määratleda, milline asutus vastutab tehnilise taristu, milline andmepoliitika ja milline järelevalve eest. Praegu on oht, et RIA-st kujuneb vaikimisi asutus, kellelt oodatakse nii tehnilist hinnangut, riskide maandamist kui ka sisulist tõlgendust, ilma et see roll oleks õiguslikult selgelt sätestatud. Samuti vajavad täpsustamist üleminekusätted: direktiivilt määrusele üleminek peab olema ajaliselt ja sisuliselt selge, et vältida olukorda, kus RIA peab samaaegselt lähtuma nii senisest riigisisesest regulatsioonist kui ka vahetult kohaldatavast ELi õigusest. 4. Eesti jaoks on spetsiifiline see, et suur osa andmete taaskasutusest toimub teenuste ja liideste kaudu, mitte staatiliste andmekogude avaldamisena. RIA kogemus näitab, et sama tehniline liides võib teenindada nii avalikku taaskasutust kui ka kriitilisi riigisiseseid protsesse. See tähendab, et avaandmete reeglid mõjutavad otseselt ka riigi infosüsteemide töökindlust ja küberturvet. Lisaks tuleb arvestada, et Eesti on	Mitte arvestatud. Ettepanek väljub omnibussi raamidest. Rollide mandaadid on andmeõiguses määratud. Avaandmete normide sisu ei muudeta. Need lihtsalt ühendatakse andmemäärusega. Kuna norme ei muudeta, siis kohanemiseks lisaaega ei ole vaja. Normid on täna juba kehtivad.

		kõrge digitaalse küpsusega riik, mistõttu suureneb ka rahvusvaheline huvi meie andmete ja liideste vastu. See omakorda tõstab kuritarvituse ja teenustõkestuse riski ning eeldab, et ELi õigusraamistik ei seaks RIA-le ebarealistlikke ootusi „avatuse“ osas ilma piisavate kaitsevahenditeta. 5. RIA jaoks on murekohaks eelkõige see, et lihtsustamise eesmärgi all ei tekiks uusi kaudseid kohustusi, mida tuleb täita ilma vastava ressursi, volituse või õigusliku selguseta. Samuti on oluline vältida olukorda, kus määrus loob formaalselt ühtsed reeglid, kuid praktikas suureneb vajadus iga üksikjuhtumi eraldi tõlgendamiseks. RIA rolli vaates on kriitiline, et tehnilised juhised ja põhimõtted ei muutuks vaikimisi siduvaks „pehmeks õiguseks“ ilma, et nende õiguslik kaal ja vastutus oleksid selgelt määratletud. 6. Seoses avaandmete direktiivi ja andmehalduse määruse ühildamisel oleks vajalik tekitada enne õigusmuudatuste jõustumist uued väärtused, kuidas eristada avaandmeid ja kaitstud andmeid lisaks kõrgväärtusega andmetele. RIA vajab aega, et viia muutused sisse nii standardisse kui rakendustesse ja seda kirjeldajatele kommunikeerida.	
61.		**Ühtse kontaktpunkti loomine** 7. Esiteks on ühtse kontaktpunkti (*single-entry point, SEP*) loomine positiivne samm erinevatele teenuse osutajatele, kes peavad intsidentide kohta raporteid esitama. Kindlasti toetame seda, et raporti esitamise kohuslased saaksid seda teha võimalikult efektiivselt ja vähese ajakuluga. 8. Siiski ei ole praegu selgelt ja üheselt aru saada, kuidas SEP praktikas toimib. SEP loomisel on vajalik ühtlustada erinevate liikmesriikide standardid, millega intsidendid kvalifitseeritakse ja kuidas neid käsitletakse. Samuti on vajalik ühtlustada	Selgitame. Hetkel teadaolev info on, et ENISA haldab SEP keskkonda, kuid ta ei saa juurdepääsu selle kaudu esitatud teavitustele. Tolle keskkonna kaudu toimub teavituse edastamine asjakohase riigi või riikide asjakohasele pädevale asutusele või pädevatele asutustele. Hetkel puudub info, kas tegemist on eraldiseisva

		erinevate regulatsioonide alusel esitatavad intsidendiraportid ning nendes sisalduv vajalik info (NIS2, GDPR, DORA). 9. Küsitav on, kas SEP keskkond luuakse viisil, kus esmase teavituse saavad liikmesriigid, kes edastavad vajadusel info ENISA-le või haldab kogu SEP keskkonda ENISA, kes suunab intsidendiga seotud info vastavatele pädevatele asutustele liikmesriikides. 10. **RIA hinnangul ei ole lahendus, kus SEP keskkond luuakse ENISA juurde ning ENISA saadab kogu vajamineva info edasi liikmesriikide pädevatele asutustele jätkusuutlik. See võib pikendada ajakriitilises olukorras intsidendi käsitlemise aega.** Loogilisem oleks ülesehitus, kus SEP raporteerimiskeskkond luuakse liikmesriikide juurde, kes edastavad võimaliku riikide ülese intsidendiohu korral info ENISA-le, mille kaudu saadetakse teave teiste riikide pädevatele asutustele. 11. **Näeme, et andmete koondamine ja keskse andmebaasi/andmehoidla loomine sisaldab endas võimalikku turvariski**. Suure tõenäosusega tuleb info koondamisel luua ENISA juurde andmebaas seoses SEP raportitega. Kui selline andmebaas tekib (ilmselt on vaja päringud vastu võtta, valideerida, talletada intsidendiinfo, et seda edasi saata/töödelda), on tegemist äärmiselt tundlikku infot sisaldava andmebaasiga. See omakorda loob võimaliku keskse sihtmärgi, mille kompromiteerimine võib avaldada äärmiselt laiaulatuslikku mõju kogu EL siseturvalisusele. Vajalik on luua usaldus, et loodud süsteem on turvaline, ettevõtted ja kodanikud teavad, kuidas nende andmeid kasutatakse ja millised meetmed on kasutusele võetud, et turvalisus oleks tagatud. Vastasel juhul võib tekkida situatsioon, kus intsidendiraporteid ei esitata põhjusel, et süsteemi kui tervikut ei usaldata.	andmete (tsentraalse) kogumiga/hoidlaga või kas tegemist on andmete edastuse kanal/vahend vms. Esitatud ettepaneku kohaselt valmistab ENISA SEPiga seotud nõudeid ja meetmeid alles ette. Seejärel on ka võimalik hinnata, kas ja milline on Eesti seisukoht SEPi arhitektuuri osas.

		RIA hinnangul ei pruugi olla mõistlik luua ühte keskset andmebaasi, vaid hajutada info, et kogu tundlik info ei oleks talletatud keskselt. Samuti soovitame selgelt määratleda krüpteerimisstandardid, muuhulgas peaks arvestama selged ja kindlad kriteeriumid juurdepääsu osas ja reeglid korrapärase auditeerimise jaoks.	
62.	Regionaal- ja Põllumajandusministeerium	**Üldine toetus regulatsioonide vähendamisele ja ühtlustamisele** Toetame digiomnibusiga seotud regulatsioonide vähendamist ja regulatsioonide ühtlustamist, et vähendada halduskoormust ning lihtsustada menetlusi.	Teadmiseks võetud.
63.		**SME/SMC erisused põllumajandusettevõtetele** Toetame SME/SMC (väike- ja keskmise suurusega ettevõtete ning väikese turukapitalisatsiooniga ettevõtete) erisusi ning peame oluliseks, et need laieneksid ka põllumajandusettevõtetele *Selgitus:* põllumajandusettevõtted vajavad sarnast paindlikkust ja halduskoormuse vähendamist nagu teised VKE-d, arvestades sektori eripärasid ja ELi ühise põllumajanduspoliitika nõudeid.	Arvestada osaliselt. Ettepanekud andmeõiguses on valdkonna neutraalsed. Eesti seisukohatades toetame tehisintellekti määruses väikese ja keskmise suurusega ettevõtetele ettenähtud lihtsustusmeetmete laiendamist väikese ja keskmise turukapitalisatsiooniga ettevõtetele, et vähendada nende halduskoormust ja toetada konkurentsivõimet. Need hüved laienevad kõikidele valdkondadele. Seal ei ole omnibussis erisusi ning ei pea vajalikuks seega eraldi põllumajandust välja tuua.
64.		**Kaubandussaladuse kaitse**	Teadmiseks võetud. Põhiõiguste kaitse seisukohad olemas.

		Toetame kaubandussaladuse kaitse tugevdamist ning peame oluliseks, et digiomnibusiga ei kaasneks liigseid kohustusi kolmandate riikide riskide hindamisel.	
65.		**Proportsionaalsus** Rõhutame proportsionaalsuse põhimõtet kontrollinõuete rakendamisel – nõuded peavad olema kooskõlas ettevõtete suuruse, tegevusvaldkonna ja tegeliku riskiga.	Teadmiseks võetud.
66.		**Tehisintellekti (AI) eelnõu seisukohad** **Standardite ja juhiste eelnev rakendamine** Toetame põhimõtet, et AI-ga seotud kohustuste rakendamise eelduseks on eelnevalt standardite ja juhiste valmissaamine ja need on tehtud ka kergelt ning kiirelt kättesaadavaks. Rakendamise tähtaeg peab olema sealjuures mõistliku ajaga määratud. See tagab, et ettevõtted saavad kohustusi täita selgete ja ühtsete reeglite alusel ning välditakse ebamõistlikku halduskoormust.	Arvestatud.
67.		**AI regulatiivsed liivakastid ja testimine** Toetame AI regulatiivsetes liivakastides (sandbox) ja reaalses keskkonnas testimise EL-üleste nõuete loomist. Soovime regionaal- ja põllumajandusministeeriumi vastutusvaldkonna AI lahenduste testimist AI regulatiivsetes liivakastides.	Arvestatud. Testkeskkondadele ei ole määratud AI määrusega valdkondlikke piiranguid.
68.	Maa- ja Ruumiamet	Üldiselt toetame antud lihtsustuspaketti, mis loob lihtsama arusaama euroopa õigusaktide maastikul. Osaliselt mitmest dokumendist saab üks ning võrreldes hetke seisuga, siis nende vahelised seosed saavad ühes dokumendis selgemaks. Samuti on igati tervitatav lihtsustused, kus liikmesriikide haldus- ja ressursikoormus vähenevad.	Arvestatud osaliselt. Põhiõiguste kaitse seisukohad on kaetud. AI juhiste andmist ei ole vaja reguleerida õigusaktiga. Sellekohased normid olemas ja suuresti need ka mitteregulatiivsed

		Mõned mõtted: Toetame, et andmed tuleb võimalusel algusest peale disainida kui avaandmed. Samas ei pea avaldama neid andmed, mis on ajaliselt aegunud või mahuliselt ebaproportsionaalselt suured, millega lisatakse asutustele liigne koormus. Kindlasti tuleb arvestada, et teatud andmete avalikustamise kohustus võib kahjustada nt isikute privaatsust. Samas nende andmete avalikustamise piiramine võib mõjutada nende majanduslikku ja sotsiaalset potentsiaali. Näitena võib tuua Maa- ja Ruumiameti poolt avalikustatavad orto- ja kaldaerofotod, mille hea eraldusvõime riivab inimeste privaatsust õiguskantsleri seisukoha alusel https://www.oiguskantsler.ee/sites/default/files/2025-11/Orto-%20ja%20kaldaerofotode%20avalikustamine.pdf. Samas on kõrge eraldusvõime innovatsiooni aluseks masinõppele või sisendiks 3D mudelitele, mida saab kasutada erasektor, teadusasutused ja ka avaliksektor ise. Juurdepääsu piiramine võib teatud määral sellist innovatsiooni pärssida. Väärtuslike andmestike puhul on tervitatav, et andmete avalikustamise reeglites on selgelt kirjas, et massallalaadimine on kohustuslik, kui see on mõistlik. Eelnevalt oli georuumiliste andmete ning maa seire ja keskkonna andmetel massallalaadimise loomine kohustuslik. Viimse puhul oli „mõistlikkuse“ märkus ainult ajaloolistel andmetel.	meetmed. Avaandmete direktiivi muutmine määruseks on seisukohaga toetatud. Komisjoni ettepanekud ei hõlma INSPIRE direktiivi ja seega seda lisanduvat teemat seisukohana me digiomnibussidesse ei pane. INSPIRE direktiivil oma lihtsustuspakett käimas, kus võimalik murekohad tõstatada.

		Tehisintellekti määrusega seotult oleks ettepanek, et avalikule sektorile võiks olla rohkem ühtseid juhendeid, kuidas praktikas üldse tohib rakendada AI-d? Sealhulgas millised riskid on isikuandmete töötlemisega seoses ja ühtlasi juriidilises mõttes küsimus, et kes vastutab? Näiteks kui AI erinevate rakenduste või muu sisendi vms alusel midagi valesti otsustatakse/kustutatakse/andmeid õigusvastaselt töödeldakse jne. Avaandmete direktiivi muutumine määruseks on kindlasti mõistlik, sest siis ei pea liikmesriigid enda seadustes muudatusi tegema. See muudab tegevuste otsustamise ja otsuste jõustumise kiiremaks. Väärtuslike andmestike nimekirja (HVD) muutmisel tuleks arvestada muutuva INSPIRE direktiiviga, mille lihtsustuspakett samuti hiljuti avalikustati https://environment.ec.europa.eu/publications/simplification-administrative-burdens-environmental-legislation_en. Täna veel ei saa anda sisendit, mida täpsemalt peaks arvestama, aga HVD sisaldab suurel hulgal INSPIRE direktiivi nõudeid ruumiandmeteenuste avalikustamisel, seega on kokkupuude tugev.	
69.	Eesti Rahvusraamatukogu	Eesti Rahvusraamatukogu tervitab Euroopa Komisjoni algatust lihtsustada Euroopa Liidu andme- ja tehisintellekti regulatiivset raamistikku ning vähendada killustatust ja kattuvusi. Ühtne ja selgem raamistik toetab nii avaliku sektori asutusi kui ka teadlasi, suurendades õigusselgust ja vähendades halduskoormust. Mäluasutuste ja teadusasutuste jaoks on eriti olulised kavandatavad täpsustused andmekaitseraamistikus, eelkõige seoses isikuandmete töötlemisega teadusuuringute eesmärgil, edasise töötlemise	Arvestatud osaliselt. Teadusuuringu mõiste tagasiside arvestatud. Tehisintellekti suure riskiga süsteemid on defineeritud juba kehtivas AI määruses. Euroopa digivaldkonna lihtsustamise koondpaketiga neid juurde ei lisata. Suure riskiga tehisaru süsteemid on määratud suure riskiga just põhiõiguste kaitse põhimõttel, seega

		eesmärkide ühilduvusega ning anonümiseerimise ja pseudonüümimise selgema reguleerimisega. Samuti on positiivne, et tehisintellekti määruses kavandatakse lihtsustusi, laiendatud toetusmeetmeid, regulatiivseid liivakaste ja täiendavat juhendmaterjali. Need võiksid soodustada vastutustundlikku innovatsiooni digiteerimises, uurimistöös ja kultuuripärandi kogudele juurdepääsu parandamisel. Samas soovime juhtida tähelepanu mitmele küsimusele, mis võivad mõjutada mälu- ja teadusasutuste suutlikkust täita oma avaliku huvi ülesannet. Avaliku sektori andmete raamistik ja kultuuripärandi asutuste eripära Avaliku sektori andmete taaskasutuse reeglite koondamine ühte andmemäärusesse võib vähendada tähelepanu raamatukogude ja teiste mäluasutuste eripäradele. Need asutused haldavad keerukaid andmekogumeid, mis sisaldavad kultuuripärandi materjale, autoriõigusega kaitstud teoseid ja isikuandmeid. Ühtne horisontaalne lähenemine võib seetõttu suurendada tõlgendus- ja halduskoormust asutustele, kelle põhifunktsioon on säilitamine, juurdepääsu tagamine ja teadustöö toetamine, mitte andmete majanduslik kasutamine. Seda eriti just kontekstis, kus andmemääruse fookus on ettevõtlusvajaduste ja andmepõhise konkurentsivõime toetamisel. Sellises raamistikus muutub avaliku sektori andmete taaskasutus vaid üheks osaks laiemas regulatsioonis, mitte eraldi poliitikavaldkonnaks. Seetõttu võib tekkida oht, et raamatukogusid käsitletakse eeskätt avaliku sektori andmevaldajate, mitte kultuuripärandi asutustena, kuigi nende ülesanded ja kogude olemus on oluliselt teistsugused. Seda tausta	selles osas on kooskõla olemas. Avaliku sektori asutusi ja VKEde meetmed ei ole võrreldavad, seega avaliku setori asutusele VKEde lihtsustamise võimalusi ei saa pakkuda. Digikoondpakett ei muuda sisuliselt avaliku sektori andmete kirjeldamise ja avalikustamise kohustust. Sh jääb kehtima põhimõte, et igal liikmesriigil on, nii praegu kehtiva avaandmete direktiivi ja andmehalduse määruse kui ka edaspidi digikoondpaketi alusel, võimalus seada täpsemaid tingimusi andmetele ligipääsu pakkumiseks. Samuti on avaliku sektori andmete avalikustamist puudutavatest osadest tulenev peamine nõue andmete leitavuse tagamine, mitte kohustus anda andmed taaskasutuseks olukorras, kus see ei ole mõistlik ja kohane.

		arvestades on oluline meenutada, et kehtiv avaandmete direktiiv tunnustab selgelt kultuuripärandi asutusi erijuhtudena ning möönab, et kõiki materjale ei saa ega tohiks vabalt taaskasutada. Ka andmemäärus peab tagama õigusselguse ja vältima kaitsemeetmete nõrgenemist, mis võimaldavad raamatukogudel tasakaalustada avatust vastutusega. Andmemäärus saab kultuuripärandi kaitsemeetmeid tagada ilma lihtsustamise eesmärki kahjustamata, kui põhimõtted sätestatakse selgelt õigusakti tasandil, mitte ei jäeta tõlgendamise või juhendmaterjalide tasandile. Kultuuripärandi asutuste valduses olevate andmete taaskasutamist teaduslikel, hariduslikel, kultuurilistel või demokraatlikel eesmärkidel tuleks selgelt tunnustada õiguspärase avaliku huvi eesmärgina, mis erineb ärilisest taaskasutusest. Samuti peaks asutustel olema võimalus taaskasutamisest keelduda, kui see kahjustaks säilitamist, moonutaks kultuurilist tõlgendust või koormaks ebaproportsionaalselt avalikke ressursse. See oleks proportsionaalsuse põhimõttega kooskõlas olev täpsustus, mitte uute õiguste loomine. Lisaks ei tohiks kultuuripärandi materjalide avalikku kättesaadavust tõlgendada automaatse loana automatiseeritud taaskasutuseks või tehisintellekti treenimiseks, arvestades kehtivaid autoriõiguse ja andmebaasiõiguse eristusi. Teadusuuringute mõiste ja kultuuripärandi uurimine Kuigi teadusuuringuid puudutavad täpsustused on tervitatavad, on oluline, et kultuuripärandi uurimist, digihumanitaariat ja mäluteadusi tunnustataks selgelt teadusuuringute mõiste osana. See	

		aitaks vältida ebakindlust ja ülemääraselt ettevaatlikke andmetöötluspraktikaid. Tehisintellekti regulatsioon ja mitteärilised kasutusviisid Näeme potentsiaalse ohuna, et tehisintellekti mitteärilised ja avalikku teenust pakkuvad kasutusviisid võivad tahtmatult sattuda kõrge riskiga süsteemide kategooriasse või neile rakendatakse ebaproportsionaalseid nõudeid. See võib pärssida innovatsiooni, mis toetab demokraatlikku juurdepääsu teadmistele ja kultuurilist mitmekesisust. Raamatukogude, arhiivide ning kultuuri- ja haridusasutuste poolt mitteärilisel eesmärgil kasutatavaid tehisintellekti süsteeme – näiteks otsingu- ja soovitussüsteeme, digiteerimistehnoloogiaid ning kogudele juurdepääsu hõlbustavaid tööriistu –, mis ei tekita isikutele õiguslikke ega samaväärselt olulisi tagajärgi, tuleks käsitada eelduslikult mitte-kõrge riskiga süsteemidena, välja arvatud juhul, kui need selgelt kuuluvad tehisintellekti määruse III lisas loetletud juhtude alla. See lähenemine oleks kooskõlas ka isikuandmete kaitse üldmääruses käsitletava profileerimise mõistega. Samuti võiks kaaluda teatud erisuste laiendamist avalikes huvides tegutsevatele avaliku sektori asutustele, sarnaselt väikese ja keskmise suurusega ettevõtetele. Kultuuripärandi digiteerimise ja juurdepääsulahenduste selgesõnaline hõlmamine regulatiivsete liivakastide alla toetaks vastutustundlikku innovatsiooni ilma regulatsiooni eesmärke kahjustamata. Kokkuvõte Eesti Rahvusraamatukogu toetab Komisjoni eesmärke lihtsustada	

		regulatiivset raamistikku ja soodustada innovatsiooni ning on valmis aruteludes aktiivselt kaasa töötama. Samas rõhutame vajadust arvestada raamatukogude ja teiste mäluasutuste eripärase rolliga, et lihtsustamismeetmed tugevdaksid – mitte ei piiraks – nende võimet teenida avalikke huve, säilitada kultuurimälu ja toetada teadustööd kogu Euroopa Liidus.	
70.	Põllumajandus- ja Toiduamet	PTA toetab eelnõudes toodud üldisi eesmärke ning pakutud lahendusi, mis on suunatud Euroopa Liidu digivaldkonna õigusraamistiku lihtsustamisele, selguse suurendamisele ja halduskoormuse vähendamisele.	Võetud teadmiseks.
71.		Seoses eelnõus kavandatava isikuandmete mõiste kitsendamisega tekivad põhjendatud õiguslikud küsimused. Euroopa Liidu Kohtu senise praktika kohaselt on isikuandmete mõistet tõlgendatud järjepidevalt laialt, hõlmates muu hulgas ka pseudonüümitud andmeid ning andmeid, mis võimaldavad isiku kaudset tuvastamist, eelkõige juhul, kui selline tuvastamine on mõistlikult tõenäoline. Isikuandmete mõiste kitsendamine võib tekitada olukorra, kus andmeid, mis tegelikkuses võimaldavad isiku tuvastamist — eriti erinevate andmekogumite ühendamisel või tehisintellekti kasutamisel — ei käsitata enam formaalselt isikuandmetena. Selline lähenemine võib kaasa tuua olukorra, kus andmekaitse tase sõltub mitte tegelikust riskist andmesubjekti õigustele ja vabadustele, vaid andmete formaalsest kvalifitseerimisest. Sellest tulenevalt on oluline, et võimaliku kitsendamise ulatus ja kriteeriumid oleksid selgelt määratletud ning kooskõlas Euroopa	Arvestatud.

		Liidu Kohtu väljakujunenud tõlgendustega, vältimaks isikuandmete kaitse tegeliku taseme põhjendamatut nõrgenemist.	
72.	Andmekaitse Inspektsioon	Mitmed ettepanekus sisalduvad muudatused on suunatud eeskätt halduskoormuse vähendamisele ja andmekasutuse hõlbustamisele ettevõtjatele, mida AKI tervitab. Kahjuks peame üldise märkusena nentima, et ettepanekutega ei kaasne sisulist hinnangut või mõjuanalüüsi, kuidas kavandatavad muudatused mõjutavad füüsiliste isikute olemasolevaid kaitsemeetmeid. Digitaalse omnibusi ettepanekus sisalduv mõjuanalüüs keskendub üksnes muudatuste mõjule ettevõtetele ja organisatsioonidele, käsitlemata, kuidas need mõjutavad üksikisiku põhiõigusi ja õiguste tegelikku kasutatavust. Euroopa Komisjon on väljendanud, et ettepanek ei vähenda isikuandmete kaitse taset. Samal ajal puudub analüüs üksikisiku õiguste vaatest, mistõttu ei ole sellist väidet võimalik objektiivselt kinnitada. Kuigi ettepanek rõhutab korduvalt selguse ja lihtsustamise eesmärki, ei analüüsita, kuidas neid eesmärke on tasakaalustatud võimalike tagajärgedega andmesubjektidele. Lisaks ei ole hinnatud ka mõjusid andmekaitseasutustele. Olukorras, kus paljudes küsimustes alles hakkab kooruma välja selgus ning väikestes riikides nagu Eesti hakkab andmekaitseteadlikkus tekkima, toovad muudatused kaasa suure koormuse kasvu järelevalveasutustele. Tuleb arvestada, et käesolevate omnibussidega hakatakse muutma põhimõttelisi asju ning andmekaitse alustalasid. Ehkki EL õigusaktides on deklaratiivselt sätestatud, et liikmesriik peab tagama	Arvestatud.

		järelevalveasutustele piisava ressursi ja toimepidevuse, ei arvesta see liikmesriikide tegelike võimalusega ega ole ette nähtud ka mehhanisme või meetmeid, mis toetaks neid asutusi olukorras, kus liikmesriik vajalikke ressursse ei leia. Arvestades potentsiaalset muudatustega seotud selgitustaotluste esitamise mahtu tõlgendamisküsimustes, jääb järelevalveasutustel vähem ressurssi kaebusi menetleda ja panustada andmekaitse edendamisesse proaktiivselt. Sisulise arvamuse tekst on peatükkide kaupa leitav allpoolt.	
73.		**Isikuandmete kaitse üldmäärus** **1. Isikuandmete mõiste (IKÜM artikkel 4 lõige 1)** **Kokkuvõte**: *Ettepanek muuta isikuandmete mõistet nihutab fookuse andmetöötleja subjektiivsele hinnangule, sidudes isikuandmete olemasolu konkreetse andmetöötleja tegelike või mõistlikult kasutatavate tuvastamisvahenditega, sõltumata kolmandate isikute võimalikust tuvastamisvõimest. AKI hinnangul ei suurenda see õiguskindlust, vaid vastupidi vähendab seda. Selline definitsioon kaldub kõrvale Euroopa Kohtu varasemast praktikast (sh C-582/14), kus kaudset tuvastatavust on hinnatud objektiivselt ja laiemalt, arvestades kolmandate isikute võimalusi. Pseudonüümimise kontekstis tehtud kohtuotsuse (C-413/23) laiendamine kõigile kaudse tuvastamise juhtumitele on AKI hinnangul põhjendamatu ning võib viia olukorrani, kus kaudselt tuvastatavad andmed langevad IKÜMi kohaldamisalast välja,*	Arvestatud.

		nõrgestades andmesubjektide õigusi, tekitades ümberpööratud tõendamiskoormise, raskendades järelevalvet ja võimaldades regulatsiooni vältimist (sh III riikidesse andmeedastuste puhul). Selline lähenemine kahjustab õigusselgust ja ettenähtavust ning võib olla vastuolus Harta artiklitega 7 ja 8, kuna muudab isikuandmete kaitse ebamääraseks ja tingimuslikuks, raskendab andmesubjektide õiguste tegelikku kasutamist ning nõrgestab tõhusat haldus- ja kohtulikku õiguskaitset. Euroopa Komisjon on teinud digitaalse Omnibusiga ettepaneku muuta IKÜM artikli 4 punktis 1 olevat isikuandmete mõistet. Ettepanekus sisalduv isikuandmete mõiste ei ole objektiivselt laiem kui hetkel kehtivas IKÜMis, kuid Komisjon on ettepanekus oluliselt laiendanud definitsiooni subjektiivset mõõdet. Ettepanekuga soovitakse lisada käesolevale mõistele juurde, et füüsilise isikuga seotud teave ei ole tingimata isikuandmed iga teise isiku või üksuse jaoks ainuüksi seetõttu, et teine üksus saab selle füüsilise isiku tuvastada. Teave ei ole antud üksuse jaoks isiklik, kui see üksus ei suuda tuvastada füüsilist isikut, kellega teave on seotud, võttes arvesse vahendeid, mida see üksus mõistlikult tõenäoliselt kasutab. Selline teave ei muutu selle üksuse jaoks isiklikuks ainuüksi seetõttu, et potentsiaalsel järgmisel saajal on vahendid, mida mõistlikult tõenäoliselt saab kasutada selle füüsilise isiku tuvastamiseks, kellega teave on seotud. AKI on seisukohal, et ettepanek ei täida esitatud kujul eesmärki pakkuda suuremat õiguskindlust. Selge määratluse asemel peavad andmetöötlejad, sh VKE-d, igakordselt subjektiivselt hindama	

		seda, millal andmed kujutavad endast konkreetse andmetöötleja jaoks isikuandmeid. VKE-del on selliste hinnangute tegemiseks vähem ressursse kui suurettevõtetel. Eriti problemaatiline on väljapakutud definitsiooni viimase lause tõlgendamine, mis vähendab õiguskindlust ning kahjustab õigust andmete kaitsele. Andmetöötlejad võivad hakata vältima isiku otsest tuvastamist eesmärgiga hoiduda IKÜMi kohaldumisest. See raskendab nii andmesubjekti õiguste teostamist kui ka tõhusat järelevalvet, kuivõrd keeruliseks võib osutuda tõendamine, millal vahendid andmetöötleja käsutusse tekkisid ja/või millal isik muutus andmetöötleja jaoks tuvastatavaks. Euroopa Kohus on analüüsinud isikuandmete mõistet mitmetes lahendites. Lahendis C-582/14 selgitas kohus, et ka andmed, mis ei identifitseeri isikut otseselt (näiteks IP-aadress) võivad olla isikuandmed, kui vastutaval töötlejal on mõistlikult kasutatavad vahendid, et isik kolmanda osapoole kaudu (nt internetiteenuse pakkuja) tuvastada. Hilisemates lahendites on Euroopa Kohus seda lähenemist jätkanud. Kohtuotsustes C-319/22 ja C-479/22 rõhutas kohus, et isikuandmeteks võivad kujuneda isegi tehnilised või näiliselt neutraalsed andmeüksused (nt sõiduki VIN-kood, rahvus, sugu), kui neid kombineerides saab isiku tuvastada isegi siis, kui mitte iga potentsiaalne andmesaaja ei suuda seda teha. Seega on Euroopa Kohus varasemalt pidanud oluliseks, kas isiku identiteet on mõnele isikule või isikute ringile objektiivselt tuvastatav. Digitaalse Omnibusi ettepanekus olev isikuandmete definitsioon toetub aga Euroopa Kohtu otsusele C-413/23. Euroopa Kohus ütles	

		antud lahendis, et pseudonüümitud andmed võivad olla isikuandmed ühe andmetöötleja jaoks (kellel on võimalik taasisikustada), ent mitte kolmanda osapoole jaoks, kellel sellised vahendid puuduvad ja kelle jaoks tuvastamine ei oleks mõistlikult teostatav. Euroopa Kohtu seisukoht piirdus olukorraga, kus kolmandal isikul puuduvad reaalsed või mõistlikult kasutatavad vahendid konkreetsete andmete taasisikustamiseks. Komisjoni töödokumendi punktis 1.2.2.1 on põhjendatud muudatuste tegemist asjaoluga, et huvigruppide arvates on kaudse tuvastamise ümber selgusetust. Edasi on selgitatud, et kuigi Euroopa Kohus on teinud lahendi pseudonüümimise kohta, mis on olemuselt kaudne tuvastamine, võtab Komisjon pseudonüümimise kohta tehtud kohtu lahendi arvesse kogu kaudse tuvastamise mõtestamise kontekstis. AKI on seisukohal, et pseudonüümimise kontekstis tehtud lahendi laiendamine kõikidele kaudse tuvastamise juhtumitele on meelevaldne ning nõrgestab oluliselt isikuandmete kaitse taset. Komisjon laiendab seda loogikat juhtumitele, kus andmete saaja võib olla sellises ökosüsteemis, kus teistel osapooltel on tuvastamisvahendid olemas, kuid teave ei kvalifitseeru konkreetse üksuse jaoks isikuandmeteks. Lisaks ei arvesta Komisjon potentsiaalse järgmise saaja tuvastamisvõimet, ehkki Euroopa Kohtu varasemas praktikas (nt C-582/14) on tuvastatavust hinnatud laiemalt, võttes arvesse kõiki mõislikult kasutatavaid vahendeid ja viise, sealjuures on Euroopa Kohus viidatud lahendi punktis 46 sedastanud, et vahendi puudumise kriteerium on väga kõrge: identifitseerimise oht peab olema olematu või ebaoluline.	

		Komisjon ei ole ettepanekus viidanud vahendi puudumise kriteeriumi hindamise kohustusele. Näiteks harvikhaiguste kontekstis loetakse praeguse isikuandmete mõiste järgi üks diagnoos aastas isikuga seotud teabeks, kuna see võimaldab tuvastada konkreetse füüsilise isiku. Seega kvalifitseerub selline teave isikuandmeteks igale andmesubjekti identifitseerida püüdvale osapoolele. Uue mõiste kohaselt ei ole meie tänase arusaama kohaselt see info isikuandmed nende jaoks, kes ei saa konkreetset isikut mõistlikult tuvastada, võttes arvesse nende käsutuses olevad vahendid ja võimalused. See tähendab, et kuigi üksikdiagnoosi puhul võib olemasoleva teabe põhjal teoreetiliselt isiku tuvastada, ei muutu see automaatselt isikuandmeteks üksusele, kellel puuduvad realistlikud vahendid tuvastamiseks. Teise näitena võib tuua isiku defineerimise teatud asjaolude kaudu, näiteks kui viidata isikule kui punase peaga poisile Ruhnust. Praeguse mõiste järgi kvalifitseerub selline kirjeldus isikuandmeteks, kuna see viitab tuvastatavale füüsilisele isikule. Uue mõiste kohaselt ei ole info siiski isikuandmed nende jaoks, kes ei suuda poissi mõistlikult tuvastada, näiteks kolmandate osapoolte jaoks, kellel puudub lisateave. Isikuandmeteks muutub teave ainult nende jaoks, kellel on praktiliselt kasutatavad vahendid ja võimalused konkreetse poisi tuvastamiseks. Kaudse tuvastamise kontekstis toob uus definitsioon kaasa sisulise nihke. Kehtiva IKÜMi järgi tuleb hinnata, kas füüsiline isik on tuvastatav kolmandate isikute käsutuses olevate mõistlikult	

		kasutatavate vahendite abil, mis tähendab, et kaudne tuvastamine toimib objektiivse standardi alusel. Komisjoni ettepanek muudab kriteeriumi subjektiivseks: kui konkreetse andmetöötleja käsutuses ei ole vahendeid tuvastamiseks, ei ole teave tema jaoks isikuandmed, isegi juhul, kui teised isikud suudaksid füüsilise isiku hõlpsasti tuvastada. Praktikas tähendab see, et kaudselt tuvastatavad andmed võivad langeda IKÜMi kohaldamisalast välja, mis vähendab andmesubjektide kaitset ja killustab vastutust. See tekitab ühtlasi ümberpööratud tõendamiskoormise, kus AKI või andmesubjekt on kohustatud tõendama, kas andmetöötlejal olid vahendid isikute tuvastamiseks või kas tal oleks mõistlikult tõenäoliselt olnud võimalik selliseid vahendeid kasutada. AKI toob välja, et mõiste muutmisel võiks Komisjon võtta arvesse ka kolmandate isikute mõistliku võimaluse isikuid tuvastada. Täpsemalt tuleks isiku tuvastamise puhul arvesse võtta, kas mõnel mõistlikult ettenähtaval kolmandal isikul võivad olla vahendid isiku tuvastamiseks. Juhul, kui analüüsi tulemusel selgub, et sellised kolmandad isikud võivad olemas olla (näiteks internetti pilte või videoid üles laadides tuleb peaaegu alati seda võimalust möönda), on tegemist isikuandmetega. Lisaks eelmainitud murekohtadele tekitab väljapakutud isikuandmete mõiste riske ka rahvusvaheliste andmeedastuste kontekstis. Nimelt võivad andmetöötlejad asuda seisukohale, et isikuandmete kolmandatesse riikidesse edastamisel ei ole vajalik IKÜM 5. peatükis toodud kaitsemeetmete kohaldamine, kuivõrd isikuandmete importijal ei pruugi olla vahendeid andmesubjektide	

		tuvastamiseks. Alternatiivselt võivad andmetöötlejad asuda ka seisukohale, et IKÜM 5. peatükk ei ole üldse kohaldatav. **[1.1.] Põhiõiguste hartaga tagatud õiguste seos ettepanekuga** Isikuandmete mõiste kitsendamine ja abstraktsemaks muutumine ei puuduta ainult kaitseala kitsenemist, vaid õigusselguse ja ettenähtavuse nõrgenemist. Euroopa Liidu Põhiõiguste Harta (edaspidi Harta) artikkel 8 sätestab igaühe õiguse oma isikuandmete kaitsele. Harta artikkel 8 ei taga isikuandmete kaitset abstraktselt, vaid kui reaalselt kasutatavat õigust. Liidetud kohtuasjades C-468/10 ja C-469/10 on selgitatud, et Harta artiklitega 7 ja 8 tunnustatud õigus eraelu austamisele isikuandmete töötlemisel puudutab igasugust teavet tuvastatud või tuvastatava füüsilise isiku kohta. Kui isikuandmete mõiste ja sellele lähenemine on abstraktne või ebamäärane, ei ole andmesubjektil enam võimalik mõistlikult ette näha, kas ja millisel alusel tema õigused rakenduvad. Selline lähenemine võib vähendada usaldust, mis ei pruugi hõlmata mitte ainult segadust andmete kasutamise osas, vaid nõrgestada andmesubjekti õiguste mahtu oma isikuandmete üle. Kirjeldatu aga omab otsest mõju andmesubjekti õiguste jõustamisele. IKÜM-ga tagatud õigused nagu isikuandmetele juurdepääs, nende parandamine, kustutamine ja töötlemisele vastuväidete esitamine võivad muutuda juhuslikuks, sest andmesubjektil võib puududa kindel veendumus, kas tema isikuandmetele konkreetses olukorras IKÜM kohaldub. Kui puudub arusaam kaitsemehhanismide	

		kohaldatavusest, on andmesubjektidel omakorda keeruline rakendada oma õigusi. Harta artikliga 8 on lähedalt põimunud Harta artikkel 7, mis sätestab eraelu puutumatuse kaitse. Isikuandmete mõiste muutmisega kaasneb eraelu piiride hägustumine, kuivõrd ettenägematu ja ebaselge andmete töötlemisega võib kaasneda eraellu sekkumine. Harta artikkel 7 eeldab, et sekkumine eraellu oleks selgelt määratletud, ettenähtav ja piiratud. Olukorras, kus teabe isikuandmeteks kvalifitseerumise otsustab teabe valdaja, võib esineda oluline risk eraelu riiveks. Riive võib olla ulatuslik, sest isikuandmete töötlemine on osa eraelust ning isikuandmete määratlus on ettepaneku kohaselt abstraktne, mistõttu võivad subjektiivse hinnangu pinnalt leida aset pidevad eraelulised sekkumised, sest isikuandmete määratlus eraelu osana on kitsas ja vaieldav. Järelevalveasutus peab kindlaks tegema, millised andmed kvalifitseeruvad isikuandmeteks ja kas neid töödeldi õiguspäraselt või mitte. Ebamäärane subjektiivne hinnang isikuandmetele ei taga tõhusat ja efektiivset menetlust, sest järelevalveasutusel tuleb selgitada ebamääraseid puutepunkte, mistõttu võib õiguste jõustamine viibida. Harta artikkel 41 sätestab õiguse heale haldusele ja eeldab tõhusat õigeaegset ja läbipaistvat haldust. Kui isikuandmetele lähenemine on sisuliselt ebaselge, kannatab õiguste tegelik kaitse. Küsimus vaidluse eseme üle, mida võib kutsuda esile isikuandmete ebaselge määratlus võib omada mõju Harta artiklile 47, mis tagab õiguse efektiivsele õiguskaitsele. Kõigi eelduste järgi	

		kutsub isikuandmete ebaselge määratlus esile vaidlused andmete kvalifitseerimise üle, kuivõrd esmalt tuleb välja selgitada, kas vaidluse esemeks on isikuandmed või mitte. Kuigi eesmärk võib olla legitiimne, kaasneb abstraktse, subjektiivsel hinnangul põhineva isikuandmete mõistega õiguste nõrgenemine ning õigusselguse kadu, mida on Euroopa Kohus pidanud korduvalt oma lahendites põhiõiguste tõhusa kaitse eelduseks. Selle tagajärjel võivad andmesubjektide õigused muutuda formaalseks ja raskendatuks nii haldus-, kui kohtumenetluses.	
74.		**2. Teadusuuringud** **Kokkuvõte***: Kuigi teadusuuringu mõiste määratlemine on tervitatav, on ettepanekus pakutud definitsioon äärmiselt lai ja osaliselt vastuoluline, hõlmates mistahes uurimistöö, ilma et oleks selgelt nõutav teaduslik metoodika või uue üldistatava teadmise loomine. Samuti jäävad ebaselgeks viited eetikanormidele, mis vähendab praktilist selgust ning võib viia selleni, et väga erinevad, sh puhtalt rakenduslikud või ärilised tegevused kvalifitseeritakse teadusuuringutena. Ettepanekus on selgitatud, et teadusuuringu eesmärgil andmete töötlemisel võib õiguslikuks aluseks olla õigustatud huvi. Selline sõnastus võib tekitada riski, et eesmärgi olemasolu hakatakse võrdsustama õigusliku aluse olemasoluga. Kui seadusandja soov on tõlgendada põhjendust selliselt, et eesmärgi kooskõla tähendab ka õigusliku aluse olemasolu, tuleks AKI hinnangul muuta IKÜM artikli 5 lõike 1 punkti a. Ettepanek pakub välja täiendava erandi andmesubjekti	Arvestatud.

		teavitamiskohustusest, mis koos laia teadusuuringu definitsiooniga võimaldab ulatuslikku teisesel eesmärgil töötlemist andmesubjekti teadmiseta. Selline lähenemine nõrgestab läbipaistvuse, eesmärgipärasuse ja minimaalsuse põhimõtteid, raskendab andmesubjekti õiguste, sh vastuväidete esitamise õiguse tegelikku kasutamist ning tekitab kahtlusi ettepanekute kooskõlas Hartaga, eriti proportsionaalsuse, ettenähtavuse ja tõhusa õiguskaitse nõuetega, nihutades tasakaalu andmesubjekti õiguste kahjuks. Teadusuuringutega seoses on Euroopa Komisjon oma ettepanekus pakkunud välja mitmeid täiendusi. Käesolevaga esitab Andmekaitse Inspektsioon oma arvamuse väljapakutud muudatuste kaupa.	
75.		**[2.1.] Teadusuuringu mõiste (IKÜM artikkel 4 punkt 38)** Euroopa Komisjon on ettepanekus defineerinud teadusuuringu kui igasuguse uurimistöö, mis võib toetada ka innovatsiooni. Need tegevused peavad panustama olemasolevatesse teaduslikesse teadmistesse või rakendama olemasolevaid teadmisi uudsel viisil, neid tuleb läbi viia eesmärgiga aidata kaasa ühiskonna üldise teadmise ja heaolu kasvule ning need peavad järgima asjakohase uurimisvaldkonna eetikanorme. See ei välista, et uurimistöö eesmärk võib olla ka ärihuvide edendamine. AKI väljendab oma poolehoidu teadusuuringu defineerimiseks, arvestades et IKÜM mainib teadusuuringuid erinevates kontekstides ka ise, mistõttu suurem õigusselgus teadusuuringute mõiste ümber on vajalik. IKÜMi põhjenduspunktides 33	Arvestatud.

		(nõusoleku kontekstis) ja 159 (õigusliku aluse kontekstis) on selgitatud teadusuuringuga seotud õigusi ja kohustusi. Ettepanekuga soovitakse lisada täiendavad põhjenduspunktid, milledes viidatud metodoloogiline lähenemine, teadustöö kvaliteet, eetikanormide järgimine ja avaliku huvi või statistika eesmärgil täiendav töötlemine on reguleeritud juba kehtivas IKÜMis, mistõttu nende lisamine määrusesse ei anna selgust ega täpsusta teadusuuringute määratlust. Tegelik mõju võimalikele ettepaneku eesmärkidele (andmesubjektide kaitse või teadusvabaduse tagamise) jääb seega piiratuks ning lisatavad põhjenduspunktid ei suurenda õiguslikku selgust. Ettepanekus esitatud kujul mõiste on sisustatud vastuoluliselt. Esmalt ütleb termin, et teaduslikuks uuringuks on mistahes uurimistöö. AKI on seisukohal, et mistahes uurimistöö defineerimine teadustööks devalveerib teaduse ning teadusuuringute väärtust. Selline lähenemine ei arvesta asjaoluga, et teadusuuring eeldab enamat kui pelgalt uurimusliku tegevuse läbiviimist. Teaduslik uurimistöö peab tuginema teaduslikule metoodikale, olema teooriapõhine ning suunatud uue, üldistatava teadmise loomisele. Kui teadusliku uuringu mõiste alla hõlmatakse ka kirjeldavad, rakenduslikud või halduslikud analüüsid, ähmastub piir teadusliku ja muu uurimistöö vahel. Selle tulemusel kaob teadusuuringu eriline staatus kui süstemaatilise ja kontrollitava teadmise loomise viis. Seetõttu on AKI hinnangul põhjendatud lähenemine, mille kohaselt ei saa iga uurimistööd käsitada	

		teadusliku uuringuna, vaid teadusuuringuks kvalifitseerumine eeldab kindlate sisuliste ja metodoloogiliste kriteeriumide täitmist. Järgmiseks lisab ettepanek kriteeriumi „võib toetada ka innovatsiooni“, sh käib selle mõiste alla ka tehnoloogiaarendus ja demonstratsioon. See tähendab, et tootearendus, prototüüpimine ja muud rakenduslikud tegevused, mis tavaliselt ei kvalifitseeru akadeemiliseks teaduslikuks uurimiseks, võivad nüüd formaalselt olla teadusuuringud. Senine praktika piirdub pigem teadusliku uurimistööga, mis järgib akadeemilist või teaduslikku metoodikat ning mille eesmärk on genereerida üldist teaduslikku teadmistepagasit. Ettepanekus toodud määratluse kohaselt võib pidada teadusuuringu eesmärgiks ka ärihuvide edendamist, mis erineb akadeemilisest tavapärasest teadusuuringu käsitlusest. Kokkuvõttes on tegemist laia, kuid samas osaliselt vastuolulise määratlusega, mis suurendab ettevõtetele võimalust vormistada väga erinevaid tegevusi teadusuuringutena, kuid ei taga täielikku õigusselgust ega kooskõla teadusvabaduse põhimõtetega. Teisalt, teadusliku uurimistöö mõiste kitsalt piiritlemine isikuandmete kontekstis võib olla vastuolus võimaliku teadusuuringute regulatsiooniga muudes valdkondades. Üldiselt ongi teadusuuringute mõiste üldjuhul konkreetselt defineerimata eelkõige teadusliku ja akadeemilise vabaduse tagamiseks. Teadusuuringu enda eesmärk ja uuringu läbiviimine peab olema kooskõlas eetikanõuetega. Seejuures ei selgitata	

		põhjenduspunktides ega sättes “vastava uurimisvaldkonna eetiliste standardite” tähendust. Teadustööde puhul on normiks üldjuhul teadustöö valdkonnast, uuringu metoodikast ning heast teadustavast tulenevate põhimõtete järgimise kohustus. Ka IKÜM võiks sarnast lähenemist kasutada ning konkreetse mõiste sõnastamise asemel rõhutada, et lisaks isikuandmete kõrgetasemelise kaitse tagamisele tuleb isikuandmetega tehtavates teadusuuringutes järgida head teadustava (näiteks Euroopa teaduse eetikakoodeks).	
76.		**[2.2.] Eesmärgipiirangu muutmine teadusuuringute kontekstis (IKÜM artikkel 5 lõige 1 punkt b)** Seoses eesmärgipärasusega on digitaalses omnibusis ettepanek muuta IKÜM artikli 5 lõike 1 punkti b selliselt, et andmed kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda edasi viisil, mis on nende eesmärkidega vastuolus; edasist töötlemist avalikes huvides arhiveerimise eesmärgil, teadus- või ajaloouuringute eesmärgil või statistilisel eesmärgil loetakse vastavalt artikli 89 lõikele 1 esialgsete eesmärkidega kooskõlas olevaks, olenemata käesoleva määruse artikli 6 lõike 4 tingimustest. Esmapilgult võib tunduda, nagu väljapakutud täiendus looks uue ja laiemalt kohaldatava aluse andmete edasiseks töötlemiseks. Siiski ei ole see tõlgendus ainuvõimalik, kuivõrd kehtivat sätet lugedes on ka praegu võimalik samale järeldusele jõuda. Praktikas on kujunenud erinevad lähenemised, kus osa andmetöötlejaid ja järelevalveasutusi peavad vajalikuks rakendada täiendavalt artikli	Arvestatud.

		6 lõike 4 analüüsi, seega saab väljapakutud muudatust mõista seadusandja algset soovi selgitava ja täpsustavana, mis ei loo uut erandit, vaid kõrvaldab senise tõlgendusliku ebakindluse. Kombineerituna ettepanekus toodud äärmiselt laia teadusuuringu määratlusega, võib aga antud säte õõnestada IKÜMiga tagatavat kaitsetaset. Mistahes eesmärgil kogutud isikuandmeid oleks antud sätetele tuginedes hiljem võimalik kasutada näiteks mõne tehisintellektil põhineva keelemudeli arendamiseks, pidades silmas, et innovatsiooni toetamise kriteerium on valikuline ning ka uute teadmiste loomine ei ole nõutav, kuivõrd piisab ka olemasolevate teadmiste uudsel viisil rakendamisest. Eriti probleemne on võimalus sätet tõlgendada viisil, mis lubab järeldada, et edasise töötlemise korral teadusuuringu eesmärgil ei ole vajalik õigusliku aluse sobivuse hindamine, st ka õiguslikule alusele laieneks kooskõla eeldus. AKI märgib, et sellise tõlgendusega nõustuda ei saaks, sest muudatused räägivad endiselt eesmärkide, mitte õiguslike aluste kooskõla eeldusest ning nagu nähtub IKÜM artiklist 5 lg 1 p-dest a ja b on need eraldiseisvad põhimõtted.	
77.		**[2.3.] Teadusuuringute läbi viimise õiguslik alus (Ettepaneku põhjenduspunkt 32)** Ettepaneku selgituses ja põhjenduses 32 on öeldud, et kui liidu ega liikmesriigi õigusega ei ole vastuolus, siis on teadusuuringu eesmärgil isikuandmete töötlemise õiguslikuks aluseks õigustatud huvi (IKÜM artikkel 6 lõige 1 punkt f). Põhjendus 32 nendib küll, et vastutava töötleja kohustus tagada punkti f tingimuste täitmine	Arvestatud.

		ei ole piiratud. Siiski tekib küsimus, et kas juhul kui isikuandmete töötlemine vastab määruses toodud teadusuuringu definitsioonile ja töötlemine on juba eelduslikult eesmärgiga kooskõlas ilma, et seda peaks eraldi hindama, siis on ka õigustatud huvi olemasolu juba põhimõtteliselt eeldatav. Muudatuse tulemusel võib õigustatud huvi hindamine muutuda tarbetuks formaalsuseks. Kui seadusandja soov on tõlgendada põhjendust selliselt, et eesmärgi kooskõla tähendab ka õigusliku aluse olemasolu, tuleks AKI hinnangul muuta IKÜM artikli 5 lõike 1 punkti a. Vastasel juhul oleks selline tõlgendus IKÜMi (ja mõnel juhul teaduseetikaga) vastuolus.	
78.		**[2.4.] Andmesubjekti õigused teadusuuringute läbiviimisel (IKÜM artikkel 13 lõige 5)** Lisaks IKÜMi artiklite 5 ja 6 muudatusele puudutab isikuandmete kaitset teadusuuringute kontekstis ka artikli 13 lõike 5 lisamine IKÜMi. Nimetatud lõike kohaselt kui töötlemine toimub teadusuuringute eesmärgil ning /.../ teabe esitamine osutub võimatuks või nõuaks ebaproportsionaalselt suuri pingutusi /.../ või kui käesoleva artikli lõikes 1 osutatud kohustus tõenäoliselt muudaks töötlemise eesmärkide saavutamise võimatuks või kahjustaks seda oluliselt, ei pea vastutav töötleja esitama lõigetes 1, 2 ja 3 osutatud teavet. Sellistel juhtudel võtab vastutav töötleja andmesubjekti õiguste, vabaduste ja õigustatud huvide kaitsmiseks asjakohaseid meetmeid, sealhulgas teeb teabe avalikult kättesaadavaks. Lisaks on ettepaneku põhjenduspunktis 37 selgitatud, et teabe esitamine nõuaks ebaproportsionaalselt suuri	Arvestatud.

		pingutusi eelkõige juhul, kui vastutav töötleja isikuandmete kogumise ajal ei teadnud ega näinud ette, et ta töötleb isikuandmeid hiljem teadusliku uurimistöö eesmärgil. Pakutud artikli 13 lõike 5 lisamine koos ettepanekus toodud teadusuuringu väga laia määratlusega loob praktikas ulatusliku võimaluse töödelda isikuandmeid teisesel eesmärgil andmesubjekti teavitamiseta. Teadusuuringu definitsioon annab võimaluse teha teadusuuringuid ka sellistel andmetöötlejatel, kes koguvad isikuandmeid otse andmesubjektilt näiteks teenuse osutamisel. Kui sellised andmetöötlejad soovivad isikuandmeid teisesel eesmärgil kasutada teadusuuringu läbiviimiseks, ei ole nad kohustatud isikut sellest teavitama. Seega puuduks andmesubjektil sisuliselt ülevaade, kas ja kuidas andmetöötleja tema andmeid kasutab. See nõrgestab läbipaistvuse põhimõtet ning muudab andmesubjekti õiguste kasutamise suurel määral teoreetiliseks. Lisaks on teabe esitamata jätmise eelduste hindamine jäetud suures osas vastutava töötleja enda otsustada, kuna mõisted nagu „võimatus“ ja „ebaproportsionaalselt suured pingutused“ ei ole selgelt piiritletud. See suurendab õiguskindlusetust ja loob riski, et erandit hakatakse kasutama laialdaselt ka olukordades, kus individuaalne teavitamine oleks tegelikult võimalik. Ettepanekus viidatud võimalus piirduda teabe avalikult kättesaadavaks tegemisega eeldab, et andmesubjekt ise aktiivselt otsib infot tema andmete töötlemise kohta. Väljapakutud muudatuste koosmõju kahjustab ka eesmärgipärasuse ja andmete minimaalsuse põhimõtteid, kuna	

		teadusuuringu eesmärgile viitamine võib muutuda üldiseks õigustuseks ulatuslikule teisesel eesmärgil töötlemisele. See vähendab survet hinnata, kas konkreetsete isikuandmete töötlemine on teadusuuringu eesmärgi saavutamiseks tegelikult vajalik, ning suurendab riski, et teadusuuringu eesmärk sõnastatakse tagantjärele juba kogutud andmete õigustamiseks. Lisaks eelnevale tekib küsimus, kuidas saab andmesubjekt kasutada õigust esitada vastuväiteid IKÜM artikkel 21 lõike 6 alusel (kui isikuandmeid töödeldakse teadus- või ajaloouuringute või statistilisel eesmärgil), kui tal puudub teave, kas tema andmeid teadusuuringu raames töödeldakse. Ettepanek nihutab tasakaalu andmesubjekti õiguste kahjuks ning võib pikemas perspektiivis kahjustada usaldust nii andmetöötlejate kui ka teadusuuringute vastu. Arvestades, et IKÜMi muudatuste eesmärk on regulatiivne lihtsustamine ja VKE-de koormuse vähendamine, ei ole selge, kas läbipaistvuse oluline nõrgenemine ja õiguskindluse vähenemine on selle eesmärgi saavutamiseks põhjendatud.	
79.		**[2.5.] Põhiõiguste hartaga tagatud õiguste seos ettepanekuga** Ettepanek laiendab teadusuuringute mõistet viisil, mis tekitab kahtlusi selle kooskõlas Hartas sätestatud proportsionaalsuse ja eesmärgipõhisuse põhimõtetega. Liialt avar teadusuuringute mõiste võib võimaldada selliste tegevuste kvalifitseerimist teadusuuringutena, mis ei ole sisuliselt seotud ei avaliku huvi,	Arvestatud.

		teadusliku metoodika ega uue teadmise loomisega, ning seeläbi piirata andmesubjekti õigusi ulatuslikumalt, kui see on vajalik. Põhiõiguste harta artikli 52 lõike 1 kohaselt on põhiõiguste piiramine lubatav üksnes juhul, kui piirang on selgelt määratletud, teenib legitiimset eesmärki ning on proportsionaalne. Kui teadusuuringute mõiste on ebamäärane, muutub keerukaks hinnata nii piirangu vajalikkust kui ka seda, kas eesmärgi saavutamiseks oleks võimalik kasutada vähem piiravaid meetmeid. Samuti kannatab läbipaistvus, kuna andmesubjektil võib puududa piisav ülevaade tema andmete tegelikest kasutusviisidest. Kuigi põhiõiguste harta artikkel 13 tagab teadusuuringute ja akadeemilise vabaduse kaitse, ei saa seda tõlgendada üldise õigustusena isikuandmete kasutamiseks väljaspool selgelt piiritletud teaduslikku konteksti. Akadeemilise vabaduse austamine eeldab, et tegemist on tegeliku teadustegevusega, millel on selge metodoloogiline raamistik ja teadmiste loomise eesmärk. Seetõttu on teadusuuringute mõiste täpsem normatiivne määratlemine vajalik selleks, et tagada tasakaal teadusuuringute vabaduse ning andmesubjekti põhiõiguste tõhusa kaitse vahel.	
80.		**3. Isikuandmete eriliikide töötlemine tehisintellekti arendamisel ja toimimisel (IKÜM artikkel 9 lõige 2 punkt k; IKÜM artikkel 9 lõige 5)** **Kokkuvõte:** *Ettepaneku eesmärk vältida tehisintellekti arendamise ebaproportsionaalset takistamist on mõistetav. Küll aga on*	Osaliselt arvestatud ja teadmiseks võetud.

		kavandatav erand korraga liiga lai ja samas põhjendamatult kitsas. Erand võib hõlmata sisuliselt igasugust tehisintellekti arendamist ja kasutamist sõltumata eesmärgist, seades ohtu eriliiki isikuandmete kaitse, kuid samal ajal seob nn kogemata isikuandmete töötlemise kontseptsiooni üksnes tehisintellekti ja eriliiki isikuandmetega, jättes välja muud tehnoloogiad ja tavalised isikuandmed. Lisaks nihutab ettepanek rõhu töötlemise tegelikult toimumiselt vastutava töötleja kavatsusele, mis ei ole kooskõlas IKÜMi artikli 9 ega andmete minimaalse kogumise põhimõttega ning tekitab paradoksaalse olukorra, kus eriliiki isikuandmed võivad olla nõrgemalt kaitstud kui muud isikuandmed. *Kavandatav artikli 9 lõige 5 tugineb ebarealistlikele tehnoloogilistele eeldustele, eelkõige seoses eriliiki isikuandmete eemaldamise võimalikkusega juba treenitud tehisintellekti mudelitest. Selline lähenemine normaliseerib eriliiki isikuandmete olemasolu tehisintellekti süsteemides ja on vastuolus IKÜMi artikli 9 lõike 2 erandliku iseloomuga.* *AKI rõhutab, et erandi olemasolu ei vabasta andmetöötlejat IKÜMi artikli 6 kohase õigusliku aluse nõudest ning konkreetne tehnoloogia ei saa asendada eesmärgipõhist ja proportsionaalset andmetöötluse analüüsi.* *Arvestades ka põhiõiguste hartast tulenevaid eraelu, isikuandmete kaitse, inimväärikuse ja tõhusa õiguskaitse nõudeid, peab AKI põhjendatumaks käsitleda tehisintellekti arendamisega seotud erandeid ja kohustusi tehisintellekti määruse raames, kus laiemad*	

		õigused oleksid tasakaalustatud selgemate ja rangemate kohustuste ning nende täitmise järelevalvega. Digitaalne omnibus sisaldab ettepanekud täiendada eriliigiliste isikuandmete töötlemise erandeid IKÜM artikli 9 punktiga k, mille kohaselt on andmetöötlejal õigus töödelda eriliiki isikuandmeid, kui andmetöötleja tegeleb tehisintellekti süsteemi või mudeli arendamise või toimimisega. Ettepanek täpsustab hiljem IKÜM artikli 9 uues lõikes 5, et isikuandmete eriliikide kogumise ja muul viisil töötlemise vältimiseks rakendatakse asjakohaseid korralduslikke ja tehnilisi meetmeid. Kui vastutav töötleja tuvastab vaatamata selliste meetmete rakendamisele treenimiseks, testimiseks või valideerimiseks kasutatavates andmekogumites või tehisintellekti süsteemis või mudelis isikuandmete eriliikidesse kuuluvaid andmeid, eemaldab vastutav töötleja need andmed. Kui nende andmete eemaldamine nõuab ebaproportsionaalselt suuri pingutusi, kaitseb vastutav töötleja neid andmeid igal juhul tõhusalt ja põhjendamatu viivituseta väljundite tootmiseks kasutamise, avalikustamise või muul viisil kolmandatele isikutele kättesaadavaks tegemise eest. Selle täiendava erandi eesmärk on vältida tehisintellekti arendamise ja kasutamise ebaproportsionaalset takistamist, võttes arvesse töötleja võimekust tuvastada ja eemaldada tundlikke isikuandmeid, nagu on selgitatud ettepaneku põhjenduspunktis 33. Erand kehtib olukordades, kus töötleja ei kavatse teadlikult töödelda eriliiki isikuandmeid, kuid sellised andmed on juhuslikult süsteemi sattunud. Andmetöötleja peab rakendama asjakohaseid	

		tehnilisi ja korralduslikke meetmeid, et vältida eriliiki isikuandmete töötlemist kogu tehisintellekti süsteemi või mudeli elutsükli jooksul. Komisjoni hinnangul selgitab ettepanek olukordi, kus varem on olnud ebaselge, kas selline töötlemine on kooskõlas IKÜMi artikli 9 lõike 2 nõuetega, ning aitab seeläbi otseselt toetada innovatsiooni ja tehisintellekti arendamist, mis on usaldusväärne, diskrimineerimisvaba ja säilitab kõrge andmekaitsetaseme. AKI on seisukohal, et uus erand on väga lai ja näib potentsiaalselt hõlmavat mis tahes tehisintellektimudeli või -süsteemi arendamist ja toimimist, sealhulgas mis tahes eesmärgil. Sellega kaasneb märkimisväärne oht eriliiki ehk kõige suuremat kaitset vajavatele isikuandmetele. Teisalt on uus erand kitsas, kuivõrd hõlmab kõikvõimalike tehnoloogiliste võimaluste seast vaid tehisintellekti arendamist ja toimimist, arvestamata näiteks klassikalisi algoritme ja muid automatiseeritud süsteeme. AKI toob lisaks välja, et erand hõlmab vaid eriliiki isikuandmete töötlemist, samas muude isikuandmete puhul selline erand puudub, mis justkui tekitab olukorra, kus eriliiki isikuandmed on vähem kaitstud kui tavalised isikuandmed. Ettepaneku artikli 9 lõike 2 punktis k sätestatud uus erand koos uue lõikega 5 viitavad sellele, et erand hõlmab eriliiki isikuandmete töötlemist vaid juhul, kui vastutav töötleja ei kavatsenud selliseid andmeid töödelda. Seega fakt, kas konkreetne isikuandmete töötlemine kuulub punktis k sätestatud erandi alla, näib tuginevat hinnangule, kas vastutav töötleja kavatseb töödelda eriliiki isikuandmeid, samas kui artikli 9 lõikes 1 sätestatud keelud	

		sõltuvad sellest, kas eriliiki isikuandmeid tegelikult töödeldakse või mitte. Eeltoodu on vastuolus ka andmete minimaalse kogumise põhimõttega, mis on kirjas IKÜM artikli 5 lõike 1 punktis b. Tuleb rõhutada, et selline kogemata isikuandmete töötlemise kontseptsioon ei saa olemuslikult olla seotud üksnes tehisintellektiga ega eriliiki isikuandmetega. Kui sellist lähenemist peetakse vajalikuks, peaks see kehtima horisontaalselt kõikides sektorites ja kõigi isikuandmete puhul, mitte looma erandi üksnes konkreetsele tehnoloogiale. Vastasel juhul tekib põhjendamatu ebavõrdsus erinevate töötlemisviiside ning majandussektorite vahel ning risk, et tehnoloogia ise muutub isikuandmete kaitse nõrgendamise aluseks. Probleemseks saab pidada ka lisatava artikli 9 lõike 5 sõnastust, et juhul kui tehisintellektisüsteemis tuvastatakse isikuandmete eriliigid, siis vastutav töötleja need eemaldab välja arvatud juhul, kui nende eemaldamine osutub ebaproportsionaalselt suureks jõupingutuseks. Tegelikkuses on levinud seisukoht, et tehisintellektist isikuandmete eemaldamine on võimalik küll teoorias, kuid mitte praktikas. Võimalik on kasutada isikuandmete maskeerimise või blokeerimise meetmeid, et mudel enam nendega ei arvestaks, kuid täielik eemaldamine pole võimalik. Kui tehisintellekti mudelid on juba treenitud, on praeguse tehnoloogilise taseme juures (täna on ebaselge, mis ajaraamis nt masinõppe tehnoloogia areneb, mis võimaldaks andmeid päriselt kustutada) peaaegu võimatu sellest mudelist teatud meelde jäetud isikuandmeid eemaldada, välja arvatud juhul, kui seda mudelit	

		teadlikult selliselt ümber treenitakse. Nii rajaneb kavandatav säte juba valedele eeldustele. On selge, et eriliiki isikuandmete eemaldamine tehisintellekti süsteemist või mudelist osutub ebaproportsionaalselt suureks jõupingutuseks, mis juba vaikimisi loob eelduse, et need võivad seal olla. Samas IKÜM artikli 9 lõike 2 järgi peaks eriliiki andmete töötlemine olema erand ja eriliiki isikuandmed peaksid olema erilise kaitse all, mis tähendab, et vaikimisi lubatud andmetöötlus artikli 9 lõikes 5 ei ole lõikega 2 kooskõlas. Eriliiki isikuandmete töötlemise erandi olemasolu ei tähenda, et IKÜMi artikli 6 kohane õiguslik alus muutub eeldatavaks. Ka tehisintellekti arendamise kontekstis peab isikuandmete töötlemisel alati eksisteerima selge ja sobiv õiguslik alus IKÜM artiklist 6 ning selle olemasolu ei saa asendada viitega tehnoloogilisele paratamatusele või juhuslikule andmete sattumisele süsteemi. Oluline on märkida, et ettepanek keskendub eelkõige tehnoloogiale, mitte töötlemise eesmärkidele. IKÜMi loogika lähtub aga eesmärgipõhisest andmetöötlusest ning tehnoloogia on seejuures vahend, mitte iseseisev õigustav alus. Kui tehisintellekti arendajatele soovitakse anda laiemad õigused, peab sellega paratamatult kaasnema ka täpsem ja rangem kohustuste raamistik. Sellest tulenevalt oleks süsteemselt põhjendatum käsitleda selliseid erandeid ja kohustusi tehisintellekti määruses, kus on piiritletum kohaldumisala, määratud riskitasemed ning riskitasemetele vastavad teatud õigused ja kohustused ning on loodud reeglistik järelevalveks nende täitmise üle. Laiemad õigused tehisintellekti	

		arendamisel peavad olema tasakaalustatud selgemate, konkreetsemate ja rangemate andmekaitseliste kohustustega, mitte üldise ja tehnoloogiapõhise erandiga IKÜMis.	
81.		**3.1. Põhiõiguste hartaga tagatud õiguste seos ettepanekuga** Ettepanek võimaldab tehisintellekti süsteemide arendamisel ja kasutuselevõtul ulatuslikku isikuandmete, sealhulgas eriliiki isikuandmete töötlemist üksnes põhjendusel, et tehisintellektisüsteemid vajavad suuri andmemahtusid või keerukaid andmestikke. Selline lähenemine ei sisalda nõutavat vajaduse ega proportsionaalsuse analüüsi ning ei arvesta põhiõiguste hartas sätestatud põhimõttega, mille kohaselt peab eriliiki isikuandmete töötlemine olema erandlik, rangelt põhjendatud ja selgelt tasakaalus taotletava eesmärgi ning põhiõigustele avalduva mõjuga. Harta artiklite 7 ja 8 valguses kujutab massiline andmekogumine, profileerimine ja andmete tuletuslik töötlemine endast sügavat sekkumist eraellu ja isikuandmete kaitse õigusesse. Tehisintellekti süsteemid ei piirdu üksnes olemasolevate andmete töötlemisega, vaid võimaldavad tuletada uusi andmeid, sealhulgas tervisliku seisundi, seksuaalse sättumuse või poliitiliste vaadete kohta. Arvestades, et eriliiki andmed on nii Harta artikli 8 kui ka IKÜM artikli 9 alusel erilise kaitse all, toob sellise töötlemise normaliseerimine kaasa olulise kaitsetaseme nõrgenemise. Lisaks võib tehisintellekti põhine andmetöötlus riivata Harta artiklis 1 sätestatud inimväärikuse põhimõtet, kuivõrd isikuid	Arvestatud.

		käsitletakse pelgalt andmepunktide ja riskiprofiilidena, kaotades kontrolli oma identiteedi ja haavatavuste üle. Süsteemid, mis õpivad inimeste käitumisest ja „haavatavustest“, võivad sekkuda inimväärikuse olemusse viisil, mis ei ole kooskõlas põhiõiguste kaitse eesmärgiga. Harta artikli 47 seisukohalt on problemaatiline ka tehisintellekti otsuste piiratud läbipaistvus ja vaidlustatavus. Kui otsused põhinevad eriliiki andmete töötlemisel või nendest tuletatud järeldustel, ei pruugi isikul olla võimalik mõista, miks tema suhtes konkreetne tulemus kujunes, mis omakorda pärsib tõhusat õiguskaitset. Kõnealune lähenemine tõstatab Harta artikli 52 lõike 1 valguses riski, et eriliiki andmete töötlemisest saab tehisintellekti arenduses tavapärane praktika ning põhiõiguste kaitse taandub formaalseks. Lisaks ei saa välistada võimalikke riiveid Harta artiklite 20 ja 21 (võrdne kohtlemine ja diskrimineerimiskeeld) osas, samuti Harta artiklite 10 ja 11 osas, kuna maailmavaadete ja hoiakute kaardistamine võib kaasa tuua enesetsensuuri ning piirata mõtte- ja sõnavabaduse tegelikku kasutamist.	
82.		**4. Isikuandmete eriliikide töötlemine biomeetriliste andmete puhul (IKÜM artikkel 9 lõige 2 punkt l)** Ettepanek sisaldab uut eriliiki isikuandmete töötlemise erandit artikli 9 lõike 2 punktis l. Punkti l kohaselt on eriliiki isikuandmete töötlemine lubatud, kui biomeetriliste andmete töötlemine on vajalik andmesubjekti isikusamasuse kinnitamiseks	Arvestatud.

		(kontrollimine), kusjuures biomeetrilised andmed või kontrollimiseks vajalikud vahendid on andmesubjekti ainukontrolli all. Ettepaneku põhjenduspunktis 34 on selgitatud, et säilitades biomeetrilisi andmeid turvaliselt ainult andmesubjekti juures või vastutava töötleja juures tipptasemel krüpteeritud kujul ning krüpteerimisvõtit või samaväärset vahendit valdab ainult andmesubjekt, ei tekita selline töötlemine tõenäoliselt olulisi ohte tema põhiõigustele ja -vabadustele. Vastutav töötleja ei saa biomeetrilistest andmetest teada või saab neid teada ainult väga piiratud aja jooksul kontrolliprotsessi käigus. AKI tervitab biomeetriliste andmete töötlemiste õiguslikku alust ning nõustub põhjenduspunktis toodud näitega. Täiendus, et isikusamasuse kinnitamine biomeetria abil on lubatud vaid juhul, kui kontrollimiseks vajalikud vahendid on andmesubjekti ainukontrolli all, on oluline tingimus isikuandmete kaitse kontekstis.	
83.		**5. Andmesubjekti juurdepääs andmetele (IKÜM artikkel 12 lõige 5)** Digitaalse omnibusi ettepanekus on IKÜM artikkel 12 lõiget 5 täiendatud ning välja on pakutud, et artiklite 13 ja 14 kohaselt esitatav teave ning artiklite 15–22 ja 34 alusel tehtavad teated ja võetud meetmed esitatakse tasuta. Kui andmesubjekti taotlused on ilmselgelt alusetud või ülemäärased, eelkõige nende korduva iseloomu tõttu või ka artikli 15 alusel esitatud taotluste puhul	Arvestatud.

		seetõttu, et andmesubjekt kuritarvitab käesoleva määrusega antud õigusi muul eesmärgil kui oma andmete kaitse, võib vastutav töötleja kas: (a) nõuda mõistlikku tasu, võttes arvesse teabe või teate edastamise või taotletud toimingu tegemise halduskulusid; või (b) keelduda taotluse alusel tegutsemast. Vastutav töötleja kannab kohustust tõendada, et taotlus on ilmselgelt alusetu või et on mõistlik alus arvata, et see on ülemäärane. Seega, ettepanek lisab andmetöötlejale võimaluse keelduda andmete väljastamisest artikli 15 kohaste taotluste puhul, kui andmesubjekt kuritarvitab IKÜM-iga antud õigusi muul eesmärgil kui oma andmete kaitsmine. Juurdepääsu andmisest keeldumise võimalus on andmetöötlejatel IKÜM artikkel 12 lõikes 5 olemas juba praegu. Kavandatud muudatus pöörab sisuliselt tõendamiskoormise andmetöötlejatelt andmesubjektidele: kui käesoleval hetkel on andmetöötlejal kohustus oma keeldumist põhjendada, siis edaspidi on esmalt andmesubjektil vaja tõendada, et tal on andmetele juurdepääsu vaja andmete kaitsmiseks ning andmetöötlejal on madal lävend oma keeldumist põhjendada. AKI möönab, et andmesubjektide taotlused oma andmetele juurdepääsuks võivad teinekord olla ülemäärased või pahatahtlikud, näiteks naabrikaamerate vaidlused võivad alata sellest, et naaber soovib kaamera paigaldanud naabrilt saada enda liikumist sisaldavat kaamerapilti eelneva kuu lõikes. Ehkki naaber kasutab sellises olukorras oma IKÜM artikkel 15 õigust, võib olla tema tegelikuks eesmärgiks koormata kaamera paigaldanud naabrit tülika järelevalvemenetlusega. Sellest hoolimata on AKI	

		arvamusel, et käesoleva ettepaneku sõnastus on mõneti ebaõnnestunud, kuivõrd jätab mulje, et andmetöötlejal on laiaulatuslikud õigused jätta taotlused lahendamata ülemäärasuse põhjendusel. Selged juhised, kuidas ülemäärasust või õiguse kuritarvitamist hinnata, puuduvad. Selliste juhiste puudumine tekitab tõenäoliselt vaidlusi hindamise õiguspärasuse üle nii järelevalveasutuste vaates kui ka kohtumenetluses. See tähendab, et andmesubjektid tõenäoliselt jätavad selle õiguse kasutamata, kui on oht, et andmetele juurdepääsule võib eelneda aastatepikkune järelevalve- ja kohtumenetlus. Ettepanek piirab andmesubjektide õiguste kasutamist juhtudele, kui andmesubjekt soovib andmeid oma andmete kaitsmiseks. Tegemist on väga kitsa käsitlusega, millal andmesubjekt võib soovida oma andmetele ligipääsu. Andmesubjekt võib soovida andmeid mitmetel teistel eesmärkidel, näiteks töösuhete kontekstis võib andmesubjekt soovida värbamisprotsessis kogutud andmetele ligipääsu, et hinnata, kas otsus põhines ebaõigetel hinnangutel või kindlustusvaidluse ettevalmistamisel võib andmesubjekt taotleda kindlustusandjalt andmeid, mis on seotud kahjukäsitlusega. Sellistel eesmärkidel andmete väljastamine ettepaneku kohaselt kohustuslik ei ole, kuivõrd andmete taotlemise eesmärgiks ei ole andmete kaitsmine. IKÜM artikli 12 lõike 5 sõnastuse viimase lause muutmine “on mõistlik alus arvata” paneb rõhu taaskord subjektiivsele hinnangule. Ettepanekus toodud sõnastuse kohaselt on andmetöötlejal õigus pärida põhjendust andmesubjekti andmete	

		saamiseks. Vaid juhul, kui andmesubjekti eesmärk on oma andmete kaitsmine, on andmetöötleja kohustatud andmed väljastama. Ettepaneku põhjenduspunkt 35 täiendab, et andmetöötlejal on ülemäärasest taotlusest keeldumisel madal tõendamiskohustus ning täpsustab, et igal juhul peaks andmesubjekt IKÜM artikli 15 alusel juurdepääsu taotlemisel olema võimalikult täpne ehk liiga laiaulatuslikke ja eristamata taotlusi tuleks samuti pidada liigseks. Tuleb arvestada, et teinekord tuleb pidada põhjendatuks andmesubjekti taotlust küsida välja kõik andmed, mis andmetöötlejal tema kohta olemas on selleks, et hinnata, kas andmete töötlemine konkreetse andmetöötleja poolt on seaduslik ja õiguspärane. Ettepaneku kohaselt on iga selline taotlus edaspidi ülemäärane ning andmetöötleja ei pea põhjendama sellisest taotlusest keeldumist. Ettepaneku põhjenduspunktide kohaselt peaks andmesubjekt teadma, mis andmed andmetöötlejal tema kohta on, kuid praktikas tekitavad vaidlusi just need andmed, mida andmetöötlejal olla ei tohiks. Ehkki ettepanek täpsustab, et ülemääraseks võib pidada taotlusi, mille eesmärk ei ole andmete kaitsmine, tuleb märkida, et andmesubjekt võib taotluses küll tuua põhjenduseks andmete kaitsmise, kuid andmetöötlejal on õigus hinnata andmesubjekti põhjendust subjektiivselt, kas taotluse eesmärk on tõesti see, mida andmesubjekt väidab. See tekitab tulevikus vaidluskohti, mida täna olnud ei ole, ning järelevalveasutuste halduskoormus võib kasvada. Euroopa Kohtu otsus kohtuasjas FT, C-307/22 punktides 38 ja 43 on selgitatud, et andmesubjekt ei pea vastutavale töötlejale esitama	

		andmetele juurdepääsu taotluse põhjuseid. Kohtu sõnul on vastutav töötleja kohustatud andma andmesubjektile tasuta tema töödeldavate isikuandmete esimese koopia, isegi kui taotluse põhjus ei ole töötlemise seaduslikkusest teadasaamine ja selle kontrollimine. Samal seisukohal on Kohus olnud ka mitmetes hilisemates lahendites. Antud muudatus paistab olevat kantud pooleliolevast Euroopa Kohtu menetlusest C-526/24, kuid üksnes üks menetlus ei peaks laskma mõjutada senist praktikat, eriti kui see menetlus pole jõudnud Euroopa Kohtu lõpliku lahendini. Ettepanek toob kaasa õigusliku ebakindluse nii andmesubjektide kui ka vastutavate töötlejate jaoks, tuues kaasa keerulisi äärmuslikke juhtumeid ja ettenähtavaid edasi-tagasi suhtlusi. Vastutavate töötlejate jaoks võib muutuda juurdepääsutaotluste hindamine keeruliseks. Selleks, et hinnata, kas andmesubjekt soovib juurdepääsu andmete kaitsmiseks, peab andmetöötleja tõenäoliselt edaspidi rohkem andmeid töötlema. Seetõttu on väga küsitav, kas see kavandatav muudatus tegelikult vähendaks vastutavate töötlejate administratiivset koormust. Andmesubjekti vaatest tekitab olukord teadmatust, kuivõrd hindamine oleks ettepaneku kohaselt iga andmetöötleja subjektiivsetel alustel, mistõttu sama põhjendus erinevate andmetöötlejate juures võib viia erineva lahenduseni. Seega asjaolu, kas andmetöötleja saab oma õigust kasutada või mitte, sõltub andmetöötleja diskretsioonist ja heast tahtest. **5.1. Põhiõiguste hartaga tagatud seos ettepanekuga**	

		Harta artikkel 8 lg 2 kätkeb endas õigust tutvuda enda kohta kogutud andmetega ja nõuda nende parandamist. Harta tasandil on tegemist fundamentaalse õigusega ja Harta ei täpsusta, et sellise õiguse rakendamine eeldab teatud tingimustele vastamist. See tähendab, et andmesubjekt, kelle andmeid on kogutud, võib tutvuda oma andmetega ilma igasuguse põhjenduseta, eesmärgiga tagada inimväärikus ja autonoomia, kuid ühtlasi praktiliselt omada kontrolli oma andmete üle. Sõltumine andmetöötleja õigusest küsida põhjendusi on vastuolus Harta artikkel 8 lõikega 2, kuivõrd seab andmesubjekti enda andmete üle kontrolli teostamise tingimuslikuks.	
84.		**6. Erandi täpsustamine, kui andmed on saadud andmesubjektilt (IKÜM artikkel 13 lõige 4)** Ettepanekuga täpsustatakse IKÜM artikli 13 lõike 4 teksti. Ettepaneku eesmärk on muuta erandit, mis lubab andmetöötlejatel mitte anda andmesubjektidele teavet juhul, kui isikuandmeid kogutakse otse andmesubjektilt. Kuigi kehtiv määrus loob artikli 13 kohase läbipaistvuskohustuse erandi juhuks, kui andmesubjektil on kogu teave juba olemas, soovitab ettepanek teha teabe esitamisest erandi juhul, kui vastutav töötleja mõistlikult eeldab, et andmesubjektil on juba teatav teave olemas (näiteks vastutava töötleja identiteet ning töötlemise eesmärk ja õiguslik alus). See täiendav erand kehtiks teatud tingimustel: i) isikuandmed on kogutud andmesubjektide ja vastutava töötleja vahelise selge ja piiritletud suhte kontekstis ning ii) vastutav töötleja tegutseb viisil, mis ei ole andmemahukas.	Teadmiseks võetud.

		IKÜM artikkel 13 lõige 4 erand kehtib vaid juhul, kui ei kohaldu ükski välistustest. Näiteks on üheks välistuseks, et andmeid ei tohi edastada teistele vastuvõtjatele, seega näiteks raamatupidamisteenuse osutajale, makseteenuse osutajale, veebiserveri teenusepakkujale, e-mailiteenuse pakkujale jms, kes on vastuvõtjateks IKÜM artikkel 4 punkti 9 alusel. Välistuseks on ka andmete edastamine kolmandasse riiki, kuid mitmeid veebiserveri teenusepakkujad on just selliselt üles ehitatud, mistõttu oleks juba mitu alust erandi mittekohaldamiseks. Käesoleva sõnastusega muudab ettepanek IKÜM artikkel 13 lõiget 4 drastiliselt, kuivõrd hetkel on andmetöötlejal võimalik toetuda erandile, et andmesubjektil on teave juba olemas. Ettepaneku järgi muutuvad erandi kasutamise tingimused aga nii kitsaks, et enamik andmetöötlejatest ei saa seda enam rakendada. Põhimõtteliselt kohalduks muudatus vaid mõnele ühemeheettevõttele või käsitöö tegijale, kes sularaha eest oma kaupu kuskil laadal müüb. Arvestades, et kõikide IKÜMi muudatuste eesmärk on vähendada VKE-de kohustusi ja halduskoormust, võtab käesolev muudatus võimaluse toetuda kehtivas IKÜMis olevale teabe teatavaks tegemise erandile.	
85.		**7. Automatiseeritud otsuste tegemine (IKÜM artikkel 22 lõige 1)** Digitaalse omnibussi ettepanekuga soovitakse muuta IKÜMi artikli 22 lõikeid 1 ja 2 selliselt, et olemasolev sõnastus eemaldatakse, pannakse kokku lõiked 1 ja 2 ning uue sõnastuse kohaselt otsus, millel on andmesubjektile õiguslikud tagajärjed või mis teda	Teadmiseks võetud.

		sarnasel viisil oluliselt mõjutab, võib põhineda üksnes automatiseeritud töötlusel, sealhulgas profiilianalüüsil, ainult juhul, kui see otsus vastab lõike 1 tingimustele. IKÜM artikli 22 lõike 1 punkti a (kehtiva sõnastus artikli 22 lõike 2 punktis a) lisatakse allajoonitud tekst: on vajalik andmesubjekti ja andmetöötleja vahelise lepingu sõlmimiseks või täitmiseks, olenemata sellest, kas otsuse saaks teha muul viisil kui üksnes automatiseeritud vahenditega. Muudatuse kohta on ettepaneku põhjenduspunktis 38 selgitatud, et asjaolu, et otsuse võiks langetada ka inimene, ei takista vastutaval töötlejal langetamast otsust üksnes automatiseeritud töötlemise teel. Kui eksisteerib mitu võrdselt tõhusat automatiseeritud töötlemise lahendust, peaks vastutav töötleja kasutama vähem riivavat. Uus sõnastus näib alandavat automatiseeritud otsuste kasutamise künnist ning kuigi otsuse võiks langetada ka inimene, ei takista see enam automatiseeritud otsuse tegemise võimalust. Kehtiva IKÜM-i kohaselt piirab vajalikkuse kriteerium automatiseerimist ainult juhtudele, kui teistmoodi ei ole võimalik lepingut täita. Ka olemasolev kohtupraktika tõlgendab vajalikkuse kriteeriumit selliselt, näiteks lahendites C-252/21 (Meta vs Bundeskartellamt), C-634/21 (SCHUFA Holding AG) ja C-817/19 (Ligue des droits humans/PNR). Artikli ümbersõnastamine toob kaasa olulise õigusliku muudatuse, võttes fookuse üksikisiku õiguselt keelduda automatiseeritud	

		otsusest ning pannes selle vastutava töötleja tegevusõiguse määramisele. Sealjuures tuleks panna tähele, et artikkel 22 on IKÜM II peatükis, mis on pealkirjastatud kui "Andmesubjekti õigused". IKÜM artikkel 12 lõige 2 viitab samuti, et vastutav töötleja aitab kaasa artiklite 15-22 kohaste andmesubjekti õiguste kasutamisele. IKÜM artikli 22 väljapakutud sõnastus ei tugevda andmesubjekti õigust mitte alluda üksnes automatiseeritud otsustele, vaid nihutab regulatiivse tasakaalu selgelt andmetöötleja huvide kasuks. Kui automatiseeritud otsuse lubatavus seotakse üksnes lepingulise vajalikkusega, sõltumata sellest, kas otsus oleks võimalik teha ka muul, vähem riivaval viisil, kaotab artikkel 22 oma kaitsefunktsiooni ning erand muutub sisuliselt reegliks. Selle tulemusel kaotab andmesubjekti õigus oma sisu ning artikli paiknemine IKÜMi andmesubjekti õigusi käsitlevas peatükis muutub normatiivses plaanis formaalseks, mitte tegelikku õiguskaitset tagavaks. Komisjon on ettepaneku põhjenduspunktis 38 selgitanud, et suurema õiguskindluse tagamiseks tuleks selgitada, et otsuseid, mis põhinevad üksnes automatiseeritud töötlemisel, on lubatud teha siis, kui on täidetud eritingimused. AKI toob välja, et juba täna seisavad andmesubjektid sageli silmitsi läbipaistmatute (automatiseeritud) otsustega näiteks tööle kandideerimisel või krediidilimiitide kasutamisel. Kui automatiseeritud andmetöötlus muutub lepingute puhul vaikimisi põhivalikuks, muutuvad artikli 22 lõikes 3 sisalduvad kaitsemeetmed veelgi olulisemaks, kuid ettepanek ei tugevda kaitsemeetmeid. Vastupidiselt annab ettepanek võimaluse vähendada kontrolli, kas sellise	

		automatiseeritud otsuse kasutamine oli tegelikult vajalik. Ehkki Komisjon on ettepanekuga soovinud tagada suuremat õiguskindlust, ei täida muudetud sõnastus eesmärki. Andmekaitse Inspektsioon juhib tähelepanu ka tehnilisele sõnastusveale. Kuigi ettepanek ühendab lõiked 1 ja 2, ei kajastu ettepanekus lõigete 3 ja 4 ristviidete täpsustamine.	
86.		**8. Rikkumisteated ja ühtne teavituspunkt (IKÜM artikkel 33)** **Kokkuvõte**: *Digitaalne omnibus muudab IKÜM artikli 33 rikkumisteadete reegleid, tõstes teavitamise lävendi suure ohu realiseerimisele, sätestades teavitamise ühtse teavituspunkti kaudu ning pikendades järelevalveasutuse teavitamise tähtaega 72 tunnilt 96 tunnile. AKI hinnangul aitab lävendi tõstmine vähendada halduskoormust ja vähendab liigsete teavituste survet andmetöötlejatele, kuid samas kaob järelevalveasutuste võimalus jälgida nn keskmise ohuga rikkumisi ning kaotatakse oluline varajase sekkumise mehhanism.* *Ühtne teavituspunkt võimaldab andmetöötlejatel edastada rikkumisteated korraga mitmele järelevalveasutusele, toetades haldusprotsesside koordineerimist. Samas tuleb arvestada, et erinevad õigusaktid sätestavad rikkumisest teavitamisele erinevad tähtajad ja künnised: ettepaneku kohaselt tuleb andmekaitsega seotud suure ohuga rikkumistest teavitada 96 tunni jooksul, samas kui NIS2 direktiiv ja Komisjoni määrus 611/2013 näevad ette lühemaid tähtaegu ja teisi lävendeid, mis võivad samale intsidendile kehtida. Kuna ettepanek ei täpsusta nende tähtaegade*	Arvestatud ja selgitame: Eesti ei toeta ohu lävendi tõstmist teavitamisel, kuna see raskendab järelevalveasutusel oma kohustuste täitmist. Vormide osas leiab Eesti, et EAKN pädevusi ei tuleks anda Euroopa Komisjonile. Eesti toetab erinevates õigusaktides olevate teavituste tähtaegade ühtlustamist. Komisjoni määrus 611/2013 on üks näidetest, mille osas tuleb samuti selgus saada.

		ja lävendite kooskõla, võib see tekitada õiguslikku ebaselgust rikkumisteadete esitamisel ning vajab täiendavat selgitamist ja koordineerimist. Digitaalse omnibusi ettepanek lisab IKÜMi artiklile 33 lõike 6, mille kohaselt koostab ja edastab Euroopa Andmekaitsenõukogu (EAKN) Komisjonile ettepaneku ühtse vormi kohta, mille alusel teavitatakse lõikes 1 osutatud pädevat järelevalveasutust isikuandmetega seotud rikkumisest, ning loetelu asjaolude kohta, millal isikuandmetega seotud rikkumine võib tõenäoliselt kujutada endast suurt ohtu füüsilise isiku õigustele ja vabadustele. AKI toetab mõtet anda ühiste vormide väljatöötamise juhtimine EAKNile. Küll aga on AKI on seisukohal, et EAKN väljatöötatud vormide vastuvõtmise autonoomsus peab jääma EAKNile kui iseseisvale Euroopa institutsioonile. Andes vormide muutmise õiguse ja rakendusaktina vastuvõtmise õiguse Euroopa Komisjonile, on küsimuse all esmalt EAKNi kui organi sõltumatus ning teisalt ei ole kindel, kas rakendusaktiga vastu võetu väljendab EAKNi soovitusi ja praktikaid. Seetõttu tuleks teha artikli 33 lõikes 6 täpsustus, et EAKNi väljatöötatud vormid tuleb Euroopa Komisjonil rakendusaktina vastu võtta muutmata kujul. Peamine muudatus seoses rikkumisteadetega sisaldub artikli 33 lõikes 1 (allajoonitud tekst), mille kohaselt teavitab vastutav töötleja isikuandmetega seotud rikkumise korral, mis tõenäoliselt kujutab endast <u>suurt ohtu</u> füüsiliste isikute õigustele ja vabadustele põhjendamatu viivituseta ja võimaluse korral hiljemalt <u>96 tunni</u> jooksul pärast rikkumisest teadasaamist <u>direktiivi (EL) 2022/2555</u>	

		artikli 23a kohaselt loodud ühtse teavituspunkti (single entry point) kaudu artiklite 55 ja 56 kohaselt pädevat järelevalveasutust. Allajoonitud tekst viitab kolmele muudatusele: 1) rikkumisteavitused tuleb teha vaid suure ohu tõenäolisel ilmnemisel (praeguse ohu ilmnemise asemel); 2) rikkumisteated tuleb esitada 96 tunni jooksul (varasema 72 tunni asemel) ning 3) rikkumisteade tuleb esitada ühtse teavituspunkti (single entry point) kaudu. AKI esitab analüüsi iga muudatuse kohta eraldi. **Rikkumisteadete esitamine suure ohu tõenäolisel ilmnemise** Kehtiv IKÜM sätestab kaheastmelise rikkumise hindamise loogika. Esmalt teavitavad vastutavad töötlejad IKÜM artikli 33 lõike 1 kohaselt andmekaitse järelevalveasutusi alati, kui rikkumine on seotud riskiga isikuandmete kaitsele ning teiseks teavitavad vastutavad töötlejad IKÜM artikli 34 kohaselt rikkumisega seotud andmesubjekte juhul, kui oht[5] on suur. Selline kaheastmeline loogika võimaldab täna järelevalveasutustel säilitada ülevaade erinevatest rikkumistest ja annab võimaluse otsustada sekkumise vajaduse ning ulatuse või hinnata, kas on täiendavalt vaja teavitada andmesubjekte. Eeldus on, et juhul kui rikkumine on suur ning on vajalik teavitada andmesubjekte, peab sellele eelnema alati järelevalveasutuse teavitamine.	

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

		Ettepanekus tõstetakse IKÜM artikli 33 künnis kõrge ohutasemeni ja artiklite 33 ning 34 ohutasemed ühtlustuvad. Sellega kaotatakse justkui järelevalveasutuste vaatest vajalik esmane filter ja jäetakse alles ainult olulisematest kõrvalekalletest teavitamine. Sellest tulenevalt kaotavad järelevalveasutused teadmise enamikest intsidentidest, mis ei ole tavapäraselt suure ohuga, kuid annavad olulist teavet turvalisuse suundumuste ja vastutavate töötlejate nõuete täitmise kohta. AKI nõustub, et tänase praktika kohaselt on andmetöötlejatel suundumus pigem teatada ka väga väikestest rikkumistest ning halduskoormust arvestades on tervitatav, et praegust sõnastust soovitakse muuta. Küll aga tundub, et kuigi muudatus on kasulik andmetöötlejatele (puudub enamasti teavitamiskohustus), kaob järelevalveasutustel oluline võimalus seirata andmekaitsealaste nõuete täitmise kohustusi. Praegu on IKÜM artikli 34 lõikega 4 antud andmekaitse järelevalveasutustele õigus vastutava töötleja hinnang riski kohta ümber hinnata. Kui vastutav töötleja väidab, et rikkumine ei ole suure riskiga, kuid järelevalveasutus ei nõustu, võivad järelevalveasutused siiski anda vastutavale töötlejale korralduse andmesubjekte teavitada. Ettepaneku kohaselt ei pea vastutav töötleja vähem kui suure ohu puhul järelevalveasutust teavitama. Järelevalveasutus ei saa sellisel juhul vajalikku esialgset teavitust, mis on vajalik teisese hindamise (kas tegemist võiks olla suure riskiga juhtumiga) läbiviimiseks. See muudab artikli 34 lõike 4 sisuliselt kehtetuks, jättes ainsa kontrolliõiguse vastutavale töötlejale. Kuigi vastutaval töötlejal	

		jääb alles rikkumise dokumenteerimise kohustus, peaks järelevalveasutus neid edaspidi eraldi igalt andmetöötlejalt hakkama välja küsima, mis loob halduskoormust juurde. AKI teeb ettepaneku tõsta teavitamise lävend ohtudele, mida ei saa pidada väikeseks. Selliselt jääks alles kohustus teavitada ka nn keskmistest ohtudest, mille realiseerumise korral oleks järelevalveasutustel vajadusel võimalik kasutada oma IKÜM artikli 34 lõikes 4 ettenähtud õigust. **Tähtaja pikendamine 72 tunnilt 96 tunnile** Kehtiva õiguse kohaselt tuleb andmetöötlejal andmekaitse järelevalveasutust teavitada rikkumisest 72 tunni jooksul. Ettepanek pikendab teavitamiskohustust 96 tunnile. See annab vastutavatele töötlejatele piisavalt aega põhjalikuma uurimise tegemiseks, mis võib parandada esitatud teabe kvaliteeti. Teisalt jätab ettepanek alles andmetöötleja võimaluse hiljem rikkumisteadet täpsustada, mistõttu jääb ebaselgeks teavitamiskohustuse aja pikendamise vajadus ja kuidas see teenib lihtsustamise eesmärki. **Ühtse teavituspunkti kaudu pädevate järelevalveasutuste teavitamine** Ettepaneku kohaselt luuakse ühtne teavituspunkt direktiivi 2022/2555 (NIS2) artikli 23a alusel. Pärast teavituspunkti loomist on andmetöötlejatel kohustus järelevalveasutusi (sh andmekaitse kui ka küberturvalisuse) rikkumistest teavitada vaid ühtse teavituspunkti kaudu ühel korral. Täpsemalt on ettepanekus NIS2	

		artikli 23a lõike 3 punktis f kohta toodud, et üksuse poolt ühtse teavituspunkti kaudu esitatud teabe ühekordset teavitust saab kasutada aruandluskohustuste täitmiseks, mis on sätestatud mis tahes muus liidu õigusaktis, mis näeb ette intsidentide teatamise ühtse teavituspunkti kaudu. AKI märgib, et intsidentidest teavitamise kohustus ühtse teavituspunkti kaudu on ettepanekus toodud välja IKÜM-i, direktiivi 2022/2557 (elutähtsa teenuse osutajate direktiiv), NIS2, määruse 910/2014 (EIDAS) ning määruse 2022/2554 (tegevuskerksuse määrus ehk DORA) puhul. Eeltoodud õigusaktidest võib olla rikkumiste korral ühisosa näiteks IKÜMi ja NIS2 rikkumiste puhul. NIS2 rikkumistest teavitamise aeg on NIS2 artikli 23 kohaselt vastavalt kas 24 või 72 tundi. Kuigi rikkumistest teavitamine käib ettepaneku kohaselt ühtse teavituspunkti kaudu, on andmetöötlejal kaks erinevat tähtaega rikkumisest teavitamiseks. See võib tekitada õiguslikku ebaselgust, kuivõrd ettepaneku kohaselt on andmetöötlejal tarvis esitada rikkumise kohta teade ühtse teavituspunkti kaudu korraga kõikidele järelevalveasutustele vaid ühel korral. Veelgi enam, NIS2 rikkumistel ei ole teavitamiskünnist kõrge ohutasemega rikkumistel, seega tuleb andmetöötlejal küberrikkumiste korral rikkumisteade teha isegi siis, kui seda teadet ei esitata IKÜMi järelevalveasutusele. Sellest tulenevalt ei ole AKI-le arusaadav seadusandja eesmärk lõdvendada rikkumisteadete esitamise kohustuse piire, kui seda tehakse vaid andmekaitsega seotud rikkumiste puhul.	

		Eeltoodust hoolimata pooldab AKI initsiatiivi luua ühtne teavituspunkt, mille kaudu on võimalik andmetöötlejal esitada rikkumisteateid korraga mitmetele järelevalveasutustele, mis omakorda toetab digitaalse omnibusi eesmärki vähendada andmetöötlejate halduskoormust. AKI märgib, et ühtse teavituspunkti ülesehituse tehniline ja organisatoorne pool vajab täpsustamist. **8.1. Isikuandmetega seotud rikkumistest teavitamine muude õigusaktide alusel** Ettepanek näeb ette, et direktiivi 2002/58/EÜ artikkel 4 tuleks kehtetuks tunnistada. Selle põhjenduseks tuuakse, et isikuandmete töötlemise turvalisuse osas, vastavalt e-privaatsuse direktiivi artikli 4 lõigetele 1 ja 1a, ning isikuandmete rikkumistest teatamise osas, vastavalt artikli 4 lõigetele 3–5, on IKÜM-is juba sätestatud põhjalikud ja ajakohased reeglid. Seetõttu peaksid need tingimused kehtima nii elektrooniliste sideteenuste osutajate kui ka sidevõrkude pakkujate suhtes, tagades ühtsed nõuded vastutavatele ja volitatud töötlejatele. Ühtlustamise põhimõttega võib AKI põhimõtteliselt nõustuda, kuid samas märgib, et kehtib ka Komisjoni määrus 611/2013, mille kohaselt on üldkasutatava elektroonilise sideteenuse osutajal kohustus teatada isikuandmetega seotud rikkumistest. Määruse kohaselt tuleb rikkumisest teavitada andmekaitse järelevalveasutust hiljemalt 24 tunni jooksul pärast rikkumise tuvastamist. Ettepanekus ei ole selgitatud, kuidas Komisjoni	

		määrus 611/2013 edaspidi ettepaneku muudatustega kooskõlas oleks, ühtlasi ei ole ettepanekus viidet selle määruse tühistamisele.	
87.		**9. Andmekaitsealane mõjuhinnang (IKÜM artikkel 35)** Seoses andmekaitsealase mõjuhinnangu tegemise kohustusega muudab ja täiendab digitaalse omnibussi ettepanek IKÜM artikli 35 lõikeid 4-6. Viidatud lõigete kohaselt koostab ja edastab EAKN Komisjonile ettepaneku loetelu kohta töötlemistoimingute liikidest mille suhtes kohaldatakse või ei kohaldata andmekaitsealase mõjuhinnangu nõuet. Lisaks koostab ja edastab EAKN Komisjonile ettepaneku mõjuhinnangu tegemise ühise vormi ja metoodika kohta. AKI toetab ettepanekut töötada välja ühtsed nõuded, millal on mõjuhinnangu tegemine kohustuslik ning millal ei ole, sest see teenib nende ettevõtjate, kes siseturul tegutsevad, halduskoormuse vähendamist. Samuti toetab AKI ettepaneku osa, et EAKNile antakse ülesandeks välja töötada andmekaitsealase mõjuhinnangu koostamiseks ühtne vorm ja metoodika. Järelevalveasutuste ja EAKNi autonoomsuse säilitamiseks peab AKI siiski vajalikuks jätta nõuete ja vormide koostamise volitused vaid EAKNile. Andes nõuete ja vormi koostamise muutmise õiguse ja rakendusaktina vastuvõtmise õiguse Komisjonile, on küsimuse all esmalt EAKNi kui organi sõltumatus ning teisalt ei ole kindel, kas rakendusaktiga vastu võetu väljendab EAKNi soovitusi ja järelevalveasutuste tegelikke praktikaid. Seetõttu tuleks teha	Eesti ei toeta Euroopa Komisjonile rakendusmääruste andmist, vaid juhised peaks koostama EAKN.

		artiklis 35 täpsustus, et EAKNi väljatöötatud nõuded ja vormid tuleb Komisjonil rakendusaktina vastu võtta muutmata kujul.	
88.		**10. Pseudonüümimine (IKÜM artikkel 41a)** Ettepanek lisab IKÜMi uue artikli 41a, mille kohaselt võib Komisjon vastu võtta rakendusakte, et täpsustada vahendeid ja kriteeriume, mille alusel teha kindlaks, kas pseudonüümimise teel saadud andmed ei ole enam teatud üksuste jaoks isikuandmed. Selline lähenemine annab Komisjonile rakendusaktide kaudu justkui võimaluse muuta IKÜMi kohaldamisala isikuandmete tõlgendamisele, mis võib omakorda tekitada õiguslikku ebakindlust. Õigusaktide tõlgendamise õigus peaks jääma järelevalveasutustele, Euroopa Kohtule ning EAKNile. AKI ei toeta võimalust, et Komisjon võiks läbi rakendusaktide sisuliselt muuta olulisi põhiõigustega seotud definitsioon.	Eesti ei toeta Euroopa Komisjonile rakendusmääruste andmist, vaid juhised peaks koostama EAKN.
89.		**11. Terminaliseadmed ja nõusolek (IKÜM artikkel 88a)** AKI tervitab Komisjoni eesmärki lihtsustada andmesubjektide digitaalset kogemust ja lahendada laialt levinud „cookie fatigue", mis on tingitud e-privaatsuse direktiivi praegustest tõlgendustest. Erandite kehtestamine auditooriumi mõõtmiseks ja kohustusliku „ühe klõpsuga" nõusoleku kasutuselevõtt on positiivsed sammud kasutajasõbralikuma interneti suunas. Ettepanek loob õigusliku lahknevuse. Seadmes olevaid isikuandmeid reguleerib edaspidi IKÜM artikkel 88a, kuid ettepaneku põhjenduspunkt 47 selgitab, et isikustamata andmeid	Arvestatud.

		reguleerib endiselt e-privaatsuse direktiivi artikkel 5 lõige 3. Praktikas tekitab see küsimuse, kuidas andmetöötleja, näiteks veebipood, saab kindlaks teha, kas lõppseade kuulub füüsilisele isikule ning kas kogutud teave toob kaasa isikuandmete töötlemise. E-privaatsuse direktiivi artikkel 5 lõige 3 nõuab selget ja arusaadavat teavet andmete töötlemise eesmärgi kohta. IKÜM artikli 88a lõike 1 sõnastuse kohaselt on isikuandmete salvestamine füüsilise isiku lõppseadmesse või juba salvestatud isikuandmetele juurdepääsu saamine lubatud ainult juhul, kui see isik on andnud oma nõusoleku vastavalt käesolevale määrusele. Seega e-privaatsuse direktiivile sarnast teabe esitamise kohustust lisatav artikkel 88a otsesõnu ei näe ette. Tekib küsimus, kas eeldatakse, et kuna kohalduvad IKÜMi üldised nõusoleku reeglid, ei ole eraldi kohustust teavet selgelt esitada. Ettepanekuga soovitakse lisada artikli 88a lõige 3, mille kohaselt on isikuandmete salvestamine füüsilise isiku lõppseadmesse või juba salvestatud isikuandmetele juurdepääsu saamine ilma nõusolekuta ja hilisem töötlemine seaduslik ulatuses, mis on vajalik punktide a-d eesmärkidel. AKI möönab, et punktid a-b on üle võetud e-privaatsuse direktiivist, punktide c-d puhul tutvustab Komisjon aga täiendavaid erandeid. Nõusolek IKÜMi mõistes tähendab vabatahtlikku tahteavaldust. Lõike 3 tekst viitab olukordadele, kus nõusoleku andmine ei ole vajalik. Samas jääb selgusetuks, kas seadusandja on tahtnud selles lõikes kehtestada kohustusliku nõusoleku olukorra või hoopis viidata artikli 6 lõike 1 punkti c aluse tekkimisele. Need kaks	

		õiguslikku alust kannavad erinevaid tagajärgi, näiteks nõusoleku puhul peab andmesubjektil alati olema võimalus seda tagasi võtta. Kui seadusandja on tahtnud lõikest 3 teha artikli 6 lõike 1 punkt c kohase õigusliku aluse, tekitab viide nõusoleku puudumisele segadust. AKI rõhutab, et artikli 6 lõike 1 nimetatud õiguslikel alustel puudub hierarhia ning nõusolek ei ole teiste aluste seas ülim. Artikli 88a lõike 3 rakendamisel on vajalik täpsustada, millistes olukordades punktid c ja d, kohalduvad. Näiteks punkt c lubab andmetöötlejal koondada teavet veebiteenuse kasutamise kohta ainult omaenda tarbeks. Põhimõtteliselt on tegemist statistikaga, mis näitab veebilehe pidajale, näiteks kui palju kliente, mis vanuses, mis soost ning mis riigist tema veebilehel käis. AKI nõustub, et praktikas ei saa veebilehe pidaja sellisele teabele ligi, mis võimaldaks isikuid tuvastada, mistõttu on erandi tegemine õigustatud. Oluline on selgitada, et kõik tegevused, mis väljenduvad väljaspool „koondamise“ mõistet, peaksid toimuma vaid täiendava õigusliku aluse olemasolul. Samuti tuleb selgitada, kui kaugele võib töötlemine ulatuda eesmärkide saavutamiseks, ilma et see ületaks artiklis sätestatud lubatu piire. AKI leiab, et ettepanekus IKÜM artikli 88a lõike 3 punktis d sisalduv ulatuslik turvalisuse erand õigustab pealetükkivaid skaneerimistehnikaid ilma vajalike proportsionaalsuse kontrollideta. See kaotab IKÜMist tuleneva tasakaalustamistesti ning muudab vastutava töötleja juurdepääsu terminaliseadmetele vaikimisi lubatavaks. Kehtiva õiguse kohaselt eeldab selline	

		juurdepääs õigustatud huvi olemasolu ning huvide kaalumist andmesubjekti õigustega. Kavandatav sõnastus annab vastutavatele töötlejatele sisuliselt piiramatu tegevusruumi, ilma et sekkumise ulatust ja intensiivsust tuleks hinnata. Ilma sõnaselge proportsionaalsuse ja rangelt vajaliku ulatuse nõudeta võib erand õigustada skaneerimise praktikaid, sealhulgas kogu kõvaketta skaneerimist, krüpteeritud sõnumite analüüsimist enne edastamist ning kohalike failide kaugotsingut, mis kujutavad endast sügavat sekkumist eraellu. Täpsustamist vajab ka artikli 88a lõige 4, mis reguleerib nõusolekut. Selle asemel, et suunata fookus konkreetsete kasutajaliidese elementide sätestamisele, tuleks veenduda, et nõusolekuga seotu oleks kooskõlas artikli 7 lõikega 4. Sellest tulenevalt tuleb pidada ettepanekus välja pakutud teksti kohmakaks, sest "nõusolekutaotlusest keeldumise" (in k to refuse requests for consent) asemel võiks olla kirjas, et nõusoleku andmine ning tagasi võtmine peaks olema võimalik ühe klikiga. AKI on arvamusel, et IKÜM artikli 88a lisamine on vajalik samm, et reguleerida isikuandmete töötlemist lõppseadmetes. Samas vajab artikli sõnastus täpsustamist, et tagada õigusselgus ja andmesubjekti õiguste tegelik kaitse.	
90.		**[12.] Andmesubjekti automatiseeritud ja masinloetavad valikud seoses isikuandmete töötlemisega füüsilise isiku lõppseadmes (IKÜM artikkel 88b)**	Võetud teadmiseks.

		Digitaalse omnibussi IKÜM artikkel 88b koosmõjus artikliga 88a loob raamistiku, mille kaudu andmesubjekt saab väljendada oma nõusolekut või keelduda sellest automatiseeritud ja masinloetava vahendi kaudu, näiteks brauseri tasandil. See tähendab, et andmetöötlejad peavad austama andmesubjekti antud valikuid ning Euroopa Komisjoni ülesanne on tagada standardite loomine masinloetavate signaalide tõlgendamiseks. Küsimusi tekitab ka nõusoleku andmise viis, mis on sätestatud artikli 88b lõigetes 1 ja 2. Andes nõusolek brauseri tasandil on tegemist tulevikku vaatava nõusolekuga. Kui andmesubjekt annab nõusoleku kõikide võimalike küpsiste paigaldamiseks, ei tea ta nõusoleku andmise hetkel, milliseid küpsiseid milline veebileht kasutada võib. Selliselt antud nõusolekut ei saa pidada teadlikuks. Teisalt tekitab küsimusi ka nõusoleku kehtimise aeg. Kui artikli 88a lõike 4 punkti c kohaselt on nõusoleku andmisest keeldutud, küsitakse nõusolekut kuue kuu pärast uuesti. Sarnast lähenemist võiks kasutada ka nõusoleku andmise korral, kus iga kuue kuu tagant on andmesubjektil võimalus oma küpsiste sätted üle vaadata ja vajadusel korrigeerida. Põhjenduseks ei saa olla asjaolu, et andmesubjektil on võimalus oma nõusolek igal ajal tagasi võtta, sest nõusolekut anda võib samuti igal ajal ka kuuekuulise teavituseta. Meediateenusepakkujate erand artikli 88b lõikes 3 võib viia olukorrani, kus automatiseeritud nõusolek ei kehti kõigi veebiteenuste puhul, vähendades standardiseerimise ja kasutaja kontrolli tegelikku ulatust. Ühtlasi on seadusandja	

		meediateenusepakkujate puhul ilmselt soovinud teha sarnast erandit nagu kehtivas IKÜMis on tehtud artikkel 85 lõikes 2 (andmetöötlus ajakirjanduslikel eesmärkidel). Kui seadusandja tahe selline oli, tuleks sõnastus kooskõlastada artikli 85 lõikega 2, kuivõrd meedia ja ajakirjandus ei ole sünonüümid.	
91.		**[13.] Tehisintellekti arendamine ja juurutamine (IKÜM artikkel 88c)** Digitaalse omnibussi ettepanek lisab IKÜMi artikli 88c. Artikli 88c kohaselt kui isikuandmete töötlemine on vajalik vastutava töötleja huvides tehisintellekti määruse artikli 3 punktis 1 määratletud tehisintellekti süsteemi või tehisintellekti mudeli arendamise ja käitamise kontekstis, võib sellist töötlemist teostada õigustatud huvi alusel IKÜM artikli 6 lõike 1 punkti f tähenduses, kui see on asjakohane, välja arvatud juhul, kui muud liidu või siseriiklikud õigusaktid nõuavad sõnaselgelt nõusolekut ja kui andmesubjekti huvid või põhiõigused ja -vabadused, mis nõuavad isikuandmete kaitset, on selliste huvide suhtes ülimuslikud, eelkõige juhul, kui andmesubjekt on laps. Sellise töötlemise suhtes kohaldatakse asjakohaseid korralduslikke, tehnilisi meetmeid ja kaitsemeetmeid andmesubjekti õiguste ja vabaduste jaoks, näiteks andmete minimeerimise põhimõtte järgimise tagamiseks allikate valiku etapis ning tehisintellekti või -süsteemi või -mudeli koolitamisel ja testimisel, et kaitsta tehisintellekti süsteemis või -mudelis säilitatud jääkandmete avalikustamata jätmise eest, et tagada andmesubjektidele suurem läbipaistvus ja anda andmesubjektidele tingimusteta õigus oma isikuandmete töötlemisele vastuväiteid esitada.	Eesti toetab seisukohta, et regulatsioonis tuleb selgelt eristada arendamise ja rakendamise etappe.

		Euroopa Kohtu praegune kohtupraktika (nt C-131/12 Google Spain) sätestab, et pelgalt ärihuvi ei ole automaatselt põhiõigustest ülimuslik ning „vajalikkust“ tuleb tõlgendada kitsalt. Artikkel 88c püüab sellest mööda minna, kehtestades eelduse, et tehisintellekti arendamine on artikli 6 lõike 1 punkti f kohaselt õigustatud huvi alusel teostatav. Ka olemasoleva regulatsiooni alusel ei ole välistatud, et tehisintellekti arendamiseks isikuandmete töötlemine õigustatud huvi alusel võib teatud juhtudel olla õiguspärane, võttes arvesse isikuandmete töötlemise põhimõtteid. Selline nn õigustatud huvi eriregulatsioon ühe tehnoloogialiigi jaoks jätab petliku mulje justkui lihtsustatud korras on õigustatud huvi juba ette õiguspärane ning välistab EAKNi poolt õigustatud huvi aluse puhul suunistes toodud kolmeastmelise huvi hindamise, sh andmetöötleja ja andmesubjekti huvide tasakaalustamise, mille nõue tuleneb IKÜM art 6 lg 1 p f enda sõnastusest. AKI pöörab tähelepanu ettepaneku sõnastusele, mis kasutab väljendeid „vajadusel” ja „võib taotleda”. Selliste väljendite kasutamine suure riskiga andmete töötlemiseks ei paku vajalikku õiguskindlust. Vastupidiselt jätab see seaduslikkuse kindlaksmääramise sisuliselt vastutava töötleja subjektiivse hinnangu hooleks, mida järelevalveasutustel on ilma selgete seadusjärgsete kriteeriumideta raske vaidlustada. Tekst hõlmab lisaks tehisintellekti treenimisele ka tehisintellekti opereerimist. See viib ebaloogilise tulemuseni: standardse SQL-andmebaasi kaudu andmeid töötlev vastutav töötleja peab oma õiguslikku alust rangelt põhjendama, samas kui vastutav töötleja,	

		kes töötleb täpselt samu andmeid samal eesmärgil tehisintellekti süsteemi kaudu, saab viidata artikli 88c õigustatud huvi eeldusele. Ettepanek keskendub treenimisele ja opereerimisele kuid ignoreerib tehisintellekti väljundit. Tehisintellekti mudelid tekitavad sageli „hallutsinatsioone“ ehk valeandmeid (nt isiku valesüüdistused kuriteos). Vastutavad töötlejad väidavad praegu parandamise või kustutamise taotluste esitamisel, et nende taotluste lahendamine on tehniliselt võimatu. Artikkel 88c tugevdab seda seisukohta, muutes andmesubjektide õiguskaitsevahendid praktiliselt olematuks. Parandamise ja kustutamise taotluse esitamine on aga vaid hüpoteetiline võimalus. Ettepaneku põhjenduspunktis 31 viidatakse andmesubjekti mõistlikele ootustele, läbipaistvusele ja vastuväite esitamise võimalusele. Praktikas ei saa andmesubjekt teadagi, et tema kraabitud isikuandmeid kasutatakse tehisintellekti treenimiseks ning läbipaistvuse tagamine on problemaatiline. Samuti on andmesubjektil võimatu esitada andmete töötlemisele vastuväidet, kuna ta isegi ei tea oma andmete töötlemisest.	
92.		**[14.] Põhiõiguste hartaga tagatud õiguste seos järelevalveasutuste tööga** Ettepanek vähendab sellisel kujul liikmesriikide järelevalveasutuste tegelikku võimalust kohaldada isikuandmete kaitse üldmäärust, mis on vastuolus Euroopa Liidu põhiõiguste harta artiklis 47 sätestatud tõhusa õiguskaitse põhimõttega. Ettepanekus sisalduvad normid on võrreldes kehtiva IKÜMiga oluliselt subjektiivsemad ja tehniliselt keerukamad, muutes nende	Arvestatud.

		ühtse ja järjepideva jõustamise praktikas oluliselt raskemaks ning ressursimahukamaks olukorras, kus ressursse juurde leida, eriti väikestel riikidel, on keeruline. Selline regulatiivne nihe suurendab riski, et andmesubjekti õiguste kaitse muutub ebajärjekindlaks ning järelevalvepraktika liikmesriikide vahel killustub. Selle tulemusel võib andmesubjektil rikkumise korral puududa reaalne ja tõhus võimalus oma õigusi maksma panna, isegi kui need on formaalselt õigusaktides sätestatud. Euroopa Kohtu praktika, sealhulgas kohtuasi C-333/22, rõhutab, et põhiõiguste kaitse peab olema praktiline ja tõhus, mitte üksnes teoreetiline või näiline. Selline olukord on problemaatiline ka harta artikli 52 lõike 1 tähenduses, kuna õiguste sisuline nõrgenemine jõustamise tasandil kujutab endast kaudset, kuid tegelikku põhiõiguste piiramist. Kui normatiivne raamistik ei taga tõhusat järelevalvet ega reaalselt toimivat õiguskaitset, kahjustab see põhiõiguste olemust ning ei ole kooskõlas proportsionaalsuse ega õiguskindluse põhimõtetega.	
93.		**[15.] Teiste õigusaktidega suhestumine** Digital Omnibusi ettepaneku põhjenduspunktis 44 on välja toodud, et määrus (EL) 2018/1725 (EUDPR) ja direktiiv (EL) 2016/680 (LED) tuleks viia kooskõlla käesoleva määrusega määrusesse (EL) 2016/679 tehtud muudatustega. Digital Omnibusi ettepanekute valguses tähendab LEDi ning sellele tuginevate siseriiklike õigusaktide kooskõlla viimine IKÜM-iga seda, et Eesti õiguses	Arvestatud.

		tuleb vajadusel täiendada või täpsustada juba kehtivaid LED-i rakendusakte, st isikuandmete kaitse seadust. EUDPR muudatused on ettepanekusse sisse toodud (ettepaneku lk 85 jj), kuid LED direktiivi muudatusi ei ole. Õiguskaitseasutuste jaoks muutub olukord keeruliseks, kui nad peavad erinevates olukordades juhinduma erinevatest sätetest (mis puudutab näiteks isikuandmete mõistet või rikkumisest teavitamise tähtaegu).	
94.		**Andmemäärus** **[16.] Andmete väljastamisest keeldumine (Andmemäärus artikkel 4 lõige 8)** Kehtiva andmemääruse artikkel 4 lõike 8 kohaselt on andmevaldajal, kes on ühtlasi ärisaladuse omaja, võimalik andmetele juurdepääsu taotlus rahuldamata jätta, kui on väga tõenäoline, et ärisaladuse avalikustamine põhjustab talle suurt majanduslikku kahju. Digitaalse omnibussi ettepaneku kohaselt lisatakse ärisaladuste kaitsmiseks juurde lisaalus andmete väljastamisest keeldumiseks. Nimelt on andmevaldajal võimalik andmete väljastamisest keelduda, kui ta tõendab, et on olemas suur risk, et ärisaladus võib jõuda kolmandate riikidega seotud üksusteni, kus ärisaladuse kaitse ei ole piisav. Praktikas võib tekkida olukord, kus ärisaladust puudutavad andmed sisaldavad ka isikuandmeid. IKÜM artikli 15 alusel on andmesubjektil õigus isikuandmetega tutvuda. Andmesubjekti õigust andmetega tutvuda saab piirata mh IKÜM artikli 23 kohaselt liidu õiguses sätestatud seadusandliku meetmega. Kehtiva	Arvestatud. Eraldi ärisaladuse seisukohta pole, kuid põhiõiguste kaitse sees.

		andmemääruse põhjenduspunkti 31 kohaselt ei tohiks määruses sätestatud erandid andmetele juurdepääsu õigusest mingil juhul piirata IKÜM-i kohast andmesubjektide juurdepääsuõigust. Ettepanekus ja põhjenduspunktides ei ole eraldi välja toodud, kuidas ärisaladuse kaitsega seotud lisaalus andmete väljastamisest keeldumiseks IKÜM-st tuleneva andmesubjekti juurdepääsuõigusega suhestub. Kehtiva määruse põhjenduspunktidele tuginedes ei ole siiski tegemist eraldiseisva alusega, mis lubaks andmevaldajal isikuandmete väljastamisest keelduda. Seega ei peaks andmete väljastamisest keeldumiseks loodav lisaalus isikuandmete väljastamisest keeldumisele kohalduma ja andmevaldaja peab isikuandmete väljastamisest keeldumisel tuginema IKÜM-st tulenevale alusele nagu ka praegu kehtiv regulatsioon ette näeb.	
95.		**[17.] Erasektorilt üldises hädaolukorras andmete taotlemine (Andmemäärus artikkel 14)** Kehtiva andmemääruse artikli 14 kohaselt on andmevaldajatel kohustus teha avalikule sektorile andmed kättesaadavaks erakorralise vajaduse tõttu. Erakorralist vajadust ei ole määruses otseselt defineeritud, kuid artiklis 15 on täpsustatud, et erakorralise vajadusena tuleks käsitleda näiteks olukorda, kus andmed on vajalikud üldisele hädaolukorrale reageerimiseks. Üldine hädaolukord on defineeritud kehtiva andmemääruse artikli 2 punktis 29, mille kohaselt on üldine hädaolukord ajaliselt piiratud erakorraline olukord (nagu rahvatervise, loodusõnnetusest tingitud hädaolukord või inimtegevusest tingitud suurõnnetus, sh ulatuslik	Arvestatud.

		küberturvalisuse intsident), mis mõjutab negatiivselt liidu, liikmesriigi või selle osa elanikkonda ning millega kaasneb oht, et see võib tõsiselt ja püsivalt kahjustada elamistingimusi või majanduslikku või finantsstabiilsust või oluliselt ja vahetult halvendada majanduslikke varasid liidus või asjaomases liikmesriigis, ja mis tehakse kindlaks või kuulutatakse ametlikult välja vastavalt liidu või riigisisese õiguse kohastele asjakohastele menetlustele. Kehtiva andmemääruse artikli 15 lõike 1 punkti b alusel ja põhjenduspunkti 72 kohaselt ei saa avalik sektor taotleda isikuandmete väljastamist, kui avaliku sektori taotlused põhinevad erakorralisel vajadusel, mis ei ole seotud üldise hädaolukorraga. Digitaalse omnibusi ettepaneku kohaselt lisatakse määrusesse artikkel 15a, millega eemaldatakse andmevaldajate kohustus väljastada andmeid avalikule sektorile erakorralise vajaduse tõttu ja andmete väljastamise kohustus kehtib üksnes üldises hädaolukorras või vahetult pärast üldist hädaolukorda olukorra leevendamiseks või taastumise toetamiseks. Ettepaneku kohaselt on avaliku sektori asutusel õigus esitada andmevaldajale taotlus eelkõige isikustamata andmete väljastamiseks. Andmemäärusele lisatava artikli 15a lõike 2 kohaselt peaks isikuandmete väljastamine toimuma olukorras, kus isikustamata andmed ei ole üldise hädaolukorraga tegelemiseks piisavad ja kus võimalik, pseudonüümitakse isikuandmed enne väljastamist. Tegemist on kehtiva andmemääruse artikkel 17 lõike 2 punkti e (ettepaneku kohaselt eemaldatakse säte andmemäärusest) sarnase	

		sättega, kuid märgata on olulist erinevust. Kehtiva sätte kohaselt võib isikuandmeid avalikule sektorile väljastada vaid pseudonüümitud kujul, kuid ettepanekus toodud artikkel 15a lõike 2 kohaselt on pseudonüümimine võimalus, mitte kohustus. Kuigi ettepanekuga eemaldatakse määrusest erakorralise vajaduse tõttu andmete väljastamise alus, eristab ettepanek siiski üldist hädaolukorda ja olukorda, kui avaliku sektori asutus taotleb andmeid üldise hädaolukorra leevendamiseks või taastumise toetamiseks (in k 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 ühtne ning jälgiks sama praktikat kõikides liikmesriikides.	
96.		**[18.] Andmehalduse määruse lisamine andmemäärusesse (Andmemäärus peatükk VIIa)** Kehtiva andmehalduse määruse artikkel 11 lõike 1 järgi pidid kõik andmevahendusteenuse osutajad, kes kavatsevad osutada artiklis 10 osutatud andmevahendusteenuseid, esitama teatise andmevahenduse pädevale asutusele. Digitaalse omnibusi ettepanekuga andmemäärusesse lisatav peatükk VIIa jätab lisatavas artikli 32 lõikes 2 edaspidi andmevahendusteenuse osutajatele teatise esitamise vabatahtlikuks. Digitaalse omnibusi ettepaneku põhjenduspunktis 8 on selgitatud, et turu praeguses arenguetapis näib olevat piisav vabatahtlik kord, mis võimaldab neutraalsetel osalejatel teistest	Mitte arvestada. Eesti on toetanud seda, et teatist ei peaks esitama. Muu regulatsioon ja järelevalve jäävad alles. Isikuandmete osas IKÜM kohaldub. Seda ei ole muudetud.

		osalejatest eristada. Jätkusuutlike ärimudelite võimaldamiseks tuleks korda muuta vähem rangeks, kaotades andmevahendusteenuste ja muude lisaväärtusteenuste õigusliku eraldamise nõude, mida teenusel peaks olema lubatud pakkuda, asendades selle funktsioonipõhise eraldamisega, säilitades samal ajal teatavad kaitsemeetmed. Kavandatavat VIIa peatükki soovitakse kohaldada isikuandmete ja isikustamata andmete suhtes. Järelevalveasutused on valmistunud, et olla valmis andmevahendusteenuse osutajate teatiste vastuvõtmiseks. Kehtiv raamistik oleks loonud järelevalveasutustele võimaluse olla sellistest teenuseosutajatest ja nende tegevusest teadlik. Andmevahendusteenuse osutajatele nende tegevusest teatamise vabatahtlikuks jätmine võib luua olukorra, kus teenuseosutajate üle puudub igasugune teadmine ja kontroll. Kui teatiste esitamine jääb vabatahtlikuks, tekib risk, et järelevalveasutustel puudub ülevaade teenuseosutajatest, kes vahendavad isikuandmeid. See omakorda vähendab võimalust hinnata, kas andmete töötlemine toimub kooskõlas IKÜMi nõuetega, näiteks seoses töötlemise õigusliku aluse, turvameetmete ja andmesubjektide õiguste tagamisega. Selline olukord võib suurendada ohtu, et andmeid vahendatakse piisava kontrollita, mis võib viia ebapiisava turvalisuse või andmesubjektide õiguste rikkumiseni. Isikuandmete kaitse kõrge taseme tagamise küsitavustele viitab ettepaneku andmemääruse artikli 32c punkt c, mille kohaselt võivad andmevahendusteenuse osutajad pakkuda lisateenuseid,	

		näiteks andmete säilitamine, hooldamine, teisendamine, krüpteerimine, anonüümimine ja pseudonüümimine. Punktis on nimetatud, et seda võib teha ainult andmevaldaja või andmesubjekti selgesõnalisel taotlusel või nõusolekul. Võib eeldada, et planeeritavas muudatuses peetakse silmas, et lisateenuste osutamine on lubatav kas andmevaldaja selgesõnalisel taotlusel või andmesubjekti nõusolekul. Konkreetne sõnastus aga võimaldab tõlgendada seda ka viisil, et sobivaks võib osutuda andmesubjekti selgesõnaline taotlus. Isikuandmete puhul on vaja töötlemiseks IKÜM artikkel 6 lõikest 1 tulenevat õiguslikku alust. Seega ei loo muudatus selgesõnalist ega ühtselt tõlgendatavat regulatsiooni. Andmemääruse artikli 32c punkti c tasuks võrrelda ettepanekus andmemääruse artikkel 32f lõikega 3, mille sõnastuses on andmesubjekti nõusolekut ja andmevaldaja luba selgelt eristatud.	
97.		**[19.] Avaandmetega seotud põhimõtete muudatused (Andmemäärus peatükk VIIc)** Andmemääruse muudatustega soovitakse ühildada avaandmete ning piiranguga avaliku sektori andmete taaskasutamise regulatsioonid. Käesoleval hetkel on avaandmete direktiiv ning andmehalduse määrus oma olemuselt erinevad osas, mis puudutab regulatsioonide piire, kuivõrd kui avaandmete direktiiv kohaldub nii andmetele kui ka dokumenditele, siis kehtiv andmemäärus piiranguga andmete puhul kohaldub vaid andmetele.	Arvestatud.

		Andmemääruse ettepaneku kohaselt on andmemääruse eesmärk ühildada avaandmete direktiiv 2019/1024 ja andmehalduse määrus 2022/868. AKI nõustub, et ühtne õigusakt on positiivne suund ühtlustamaks andmete taaskasutamise reegleid ja definitsioone. Käesoleval hetkel on avaandmete direktiivi erinevalt ülevõtmine toonud kaasa piiranguta andmete taaskasutamise piiride erinevad tõlgendused. Praktikas tekitab probleeme, kui avaldatud isikuandmeid taasavalikustatakse mujal, näiteks infoportaalides, ja neid kombineeritakse veel omakorda muude avalikest allikatest leitud isikuandmetega. Ettepaneku põhjenduspunkti 24 kohaselt ei tähenda isikuandmete sisaldus teabes seda, et neid ei tohi anda taaskasutamiseks, vaid nende kasutamist tuleb vajadusel piirata ja anda kasutamiseks kaitstud andmetena. Seega, kui isikuandmed on osa avalikust teabest, peab teabevaldaja enne nende taaskasutamiseks andmist hindama, kas avaldamine võib kahjustada andmesubjekti õigusi ja huve ning vajadusel anda see teave taaskasutamiseks kaitsemeetmetega. Ettepanekus on andmemääruse artikli 17 lõike 1 punktis g täpsustatud, et isikuandmete taaskasutamiseks andmisel peab enne andmete kasutamiseks andmist võtma kasutusele kaitsemeetmeid. Selline lähenemine näitab, et isikuandmeid ei tohi avaandmetena taaskasutamiseks kaitsemeetmeteta anda. Ettepaneku põhjenduspunktis 7 on selgitatud, et andmemäärus ei loo õiguslikku alust isikuandmete töötlemiseks. Selline käsitlus näitab, et isikuandmete töötlemise puhul peab lähtuma IKÜM-st.	

		See aitab tõsta teadlikkust, et isikuandmete taaskasutamine (ka juba avalikustatud isikuandmete) eeldab IKÜM artiklist 6 tuleneva õigusliku aluse olemasolu. Seda kinnitab ka ettepaneku kavandatav andmemääruse artikkel 32w lg 2 punkt c. Ettepanekus andmemääruse artikli 32w lõiked 3 ja 4 sätestavad konkreetsed viisid, kuidas isikuandmeid saab taaskasutamiseks anda. Eelkõige näevad sätted ette võimaluse isikuandmete anonüümimiseks või muul viisil ettevalmistamiseks; samuti võib kehtestada kohustuse töödelda andmeid üksnes turvalises töötlemiskeskkonnas või füüsilises ruumis. Lisaks võib taaskasutajale määrata konfidentsiaalsuskohustuse. Oluline on, et teabevaldajal säilib õigus kontrollida taaskasutaja teostatud andmete või dokumentide töötlemise protsessi, vahendeid ja tulemusi, et tagada andmete või dokumentide kaitse terviklikkus. Ettepanekus andmemääruse artikli 32w lõige 5 sätestab selgelt, et juhul kui eelnevate tingimuste kohaselt ei ole võimalik isikuandmeid sisaldavaid andmeid avaandmeteks anda, on nende taaskasutamine lubatud üksnes andmesubjekti nõusolekul. AKI hinnangul on tegemist tasakaalustatud ja asjakohase, aga eelkõige selgust loova lahendusega. Ettepanekus andmemääruse artikli 32x lõike 1 kohaselt on taaskasutaja kohustatud teavitama avaliku sektori asutust kavatsusest edastada teatavat liiki kaitstud andmeid, mis ei ole isikuandmed, kolmandasse riiki, ning teavitama edastamise eesmärgist andmete taaskasutamise taotlemise ajal. Küsitav on, mida tuleb selles kontekstis edastamisena käsitada, näiteks kas see	

		hõlmab ka andmete üleslaadimist teenustesse, kus andmed liiguvad, näiteks pilveteenused või analüütikakeskkonnad, mis paiknevad või mille alltöövõtjad paiknevad kolmandates riikides. Ettepanek eeldab teavitamist taotluse esitamise ajal, kuid praktikas puudub avaliku sektori asutustel ülevaade, kes avaandmete portaalist andmeid alla laadib või mida taaskasutajad teabenõude tulemusena saadud andmetega hiljem teevad. Seetõttu võib teavitamiskohustus tunduda taaskasutajate vaatest bürokraatlik ja raskesti rakendatav, teisalt puudub ka teavitamise üle järelevalvevõimalus. AKI on arvamusel, et avaandmete regulatsioon ettepanekus on selgem kui kehtiv avaandmete direktiiv ning kaitsemeetmete rakendamise kohustus tagab nii isikustatud kui ka isikustamata andmete taaskasutamise turvalisuse ja usalduse. Avaandmete avaldamisel ja taaskasutamisel on oluline leida tasakaal avatud juurdepääsu ja isikuandmete kaitse vahel, seda eelkõige juhul, kui avaandmed võivad sisaldada isikuandmeid.	
98.		**Tehisintellekti määrus** **[20.] Isikuandmete eriliikide töötlemine kallutatuse tuvastamiseks ja leevendamiseks (Tehisintellekti määruse artikkel 4a)** Tehisintellekti omnibusi ettepanekuga lisatakse tehisintellekti määrusesse artikli 4a kujul õiguslik alus isikuandmete eriliikide töötlemiseks kõigi tehisintellektisüsteemide ja -mudelite pakkujate ja juurutajate poolt, kui see on vajalik kallutatuse avastamiseks ja	Arvestatud.

		kõrvaldamiseks, tingimusel et kohaldatakse asjakohaseid kaitsemeetmeid. Tehisintellekti omnibusi põhjenduspunkti 6 kohaselt kehtestatakse see alus kooskõlas IKÜM artikli 9 lõike 2 punktiga g. Kallutatuse tuvastamine ja selle korrigeerimine on selgelt iga tehisintellektimudeli või -süsteemi pakkuja ja juurutaja selge huvi. Seega võib arvata, tehisintellektimudelite ja -süsteemide pakkujad ja juurutajad peavad alati vajalikuks eriliiki isikuandmete töötlemist ja tegelikkuses ei teki ilmselt olukorda, kus vajalikkuse puudumist jaatada saaks. Nii luuakse ka tehisintellekti määruse artikliga 4a vaikimisi eeldus, et eriliiki isikuandmete töötlemine on alati aktsepteeritav. Samas arvestades IKÜM artikkel 9 lõiget 2 ei tohiks eriliiki isikuandmete töötlemist käsitleda kui vaikimisi lubatud tegevust. Vastupidiselt peab see olema rangelt piiratud, läbipaistvalt põhjendatud ja tehniliselt kontrollitud, et vältida nii õiguslikke rikkumisi kui ka ühiskondlikku kahju. Küsitavusi tekitab selle sätte loomisel ka õiguslike alustega seonduv. Digitaalse omnibusi ettepaneku kohaselt soovitakse IKÜMi lisada artikkel 88c, kehtestades sellega eelduse, et tehisintellekti arendamine on artikli 6 lõike 1 punkti f kohaselt õigustatud huvi alusel teostatav. Teisalt, mis puudutab isikuandmete eriliikide töötlemist kallutatuse tuvastamiseks ja leevendamiseks, siis tehisintellekti omnibusi ettepanekus tehisintellekti määruse artikkel 4a soovitakse kehtestada IKÜM artikkel 9 lõike 2 punkti g alusel. Viimane neist ütleb, et eriliiki isikuandmete töötlemine on lubatud, kui see on vajalik olulise	

		avaliku huviga seotud põhjustel liidu või liikmesriigi õiguse alusel ning on proportsionaalne saavutatava eesmärgiga, austab isikuandmete kaitse õiguse olemust ja tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks. Nii ei ole kallutatuse tuvastamine ja selle leevendamine enam tehisintellektimudeli või -süsteemi pakkuja või juurutaja huvi, vaid avalikkuse huvi. See viitab mõningasele ebakõlale, sest tegelikult on ka ilmselt tehisintellektimudeli või -süsteemi pakkujal või juurutajal äriline huvi, et loodud tehisintellekt oleks usaldusväärne, mis omakorda võimaldaks saada enam kasutajaid. Seejuures võib kallutatuse tuvastamine ja selle leevendamine toimuda juba arendamise etapis, mille puhul tõstatub küsimus, kas sellisel juhul töödeldakse eriliiki isikuandmeid korraga mitmele erinevale õiguslikule alusele tuginedes. Kavandatava artikkel 4a lõige 1 punkt e näeb ette tingimuse, et isikuandmete eriliigid kustutatakse pärast erapoolikuse parandamist või isikuandmete säilitamisperioodi lõppu, olenevalt sellest, kumb saabub varem. Käesoleva arvamuse peatükis 4 on AKI juba tõstatanud küsimuse, kas isikuandmete kustutamine juba süsteemi sattunud andmete puhul on ikka võimalik.	
99.		**[21.] Registreerimiskohustusest loobumine (Tehisintellekti määruse artikkel 49 lõige 2)** Kehtiva tehisintellekti määruse artikkel 49 lõike 2 kohaselt registreerib pakkuja või kohaldataval juhul volitatud esindaja enne sellise suure riskiga tehisintellektisüsteemi turule laskmist või kasutusele võtmist, mille kohta pakkuja on vastavalt artikli 6	

		lõikele 3 teinud otsuse, et tegemist ei ole suure riskiga süsteemiga, selle süsteemi artiklis 71 osutatud ELi andmebaasis. See nõue kavatsetakse tehisintellekti omnibusi eelnõu punkti 14 kohaselt kaotada, seega edaspidi jääb tehisintellekti määruse artikkel 6 lõike 3 kohane hindamine ja dokumenteerimiskohustus pakkuja vastutada (nii nagu see seni on olnudki), kuid muudatuse kohaselt ei pea pakkuja enam sellisest süsteemist teada andma. Kuigi tehisintellekti omnibusi põhjenduspunkti 9 järgi võivad riiklikud pädevad asutused nõuda pakkujatelt dokumendid välja, ei pruugi pädeval asutusel olla üldse teadmistki tehisintellekti pakkuja olemasolust. Dokumentide väljanõudmise eeldus on selliste dokumentide olemasolust teadmine. Nii võib turule sattuda ja seal mõnda aega tegutseda tehisintellektisüsteem, mille pakkuja on kvalifitseerinud tehisintellekti määruse artikkel 6 lõike 3 kohase süsteemina, kuid mille õigeaegse registreerimise korral oleks riiklikul pädeval asutusel tekkinud selle olemasolu kohta teadmine, et vajadusel järelevalvemeetmetega sekkuda.	
100.		**[22.] Tehisintellekti regulatiivliivakastid (Tehisintellekti määrus artikkel 57)** Kehtiv tehisintellekti määrus seab liikmesriikide pädevatele asutustele kohustuse luua riiklikul tasandil vähemalt üks tehisintellekti regulatiivliivakast. Ettepanekuga sätestatakse Euroopa tehisintellektiametile (tehisintellektiamet) võimalus luua selline regulatiivliivakast ka liidu tasandil. AKI on seisukohal, et EL-i tasandil regulatiivliivakasti loomine võiks aidata toetada innovatsiooni, eelkõige VKE-de ja start-upide kontekstis ning	Osaliselt arvestatud. Seisukohad leiame, et ei liivakastid ei tohi üksteist dubleerida. Lisaks selgitame, et regulatiivliivakastidel oma rakendusmäärus ka tulemas, milleks volitusnorm kehtivast AI määrusest (art 58). Volitusnormis ka järelevalve, digiomnibussiga lisajärelevalve raamistikku ei toetata.

		vältida „forum shoppingut“ ning killustunud lähenemist liikmesriikide lõikes. Samas tõstatuvad ettepanekuga ka potentsiaalsed ohukohad. Tegelikes tingimustes testimine ei tohiks viia kontrollimatu andmetöötluseni. Vajalik on kindlate protseduuride paika seadmine liivakastist väljumiseks ning andmete kustutamiseks kui testimine on lõppenud. Ettepanek tekitab küsimusi riiklike pädevate asutuste rolli kohta EL-i tasandi liivakastide disainimisel ja järelevalves. Nimelt mainitakse ettepanekus, et tehisintellektiamet peaks EL-i tehisintellekti regulatiivliivakaste rakendama koostöös pädevate riiklike asutustega, seejuures aga ei selgitata vastava koostöö tegemise kriteeriumeid ega erinevate asutuste rollide ja pädevuste jaotust. Kehtiva tehisintellekti määruse artikli 57 lõige 10 näeb riiklike tehisintellekti regulatiivliivakastide suhtes ette riikide pädevate asutuste kohustuse tagada, et niivõrd kui tehisintellektisüsteemid on seotud isikuandmete töötlemisega, on riiklikud andmekaitseasutused ja kõnealused muud riiklikud või pädevad asutused seotud tehisintellekti regulatiivliivakasti toimimisega ning osalevad oma asjakohaste ülesannete ja volituste ulatuses nende aspektide järelevalves. AKI leiab, et liiduülese tehisintellekti regulatiivliivakasti loomisel on sarnaselt eeltoodud sättega vajalik kindla järelevalveraamistiku kehtestamine seoses isikuandmete töötlemisega (näiteks juhul kui leiab aset isikuandmete töötlemisega seotud rikkumine).	
101.		**[23.] Üldotstarbelise tehisintellektisüsteemi järelevalve ja kontroll (Tehisintellekti määruse artikkel 75)**	Arvestatud.

		Tehisintellekti omnibusi raames täpsustatakse tehisintellekti määruse artiklit 75, millega tugevdatakse tehisintellektiameti rolli üldotstarbeliste tehisintellektisüsteemide järelevalves ja koordineerimises. Artikli eesmärk on tagada üldotstarbeliste tehisintellektisüsteemide ühtne käsitlus liidu tasandil ning vältida killustunud järelevalvet, arvestades nende süsteemide laia kasutusulatust ja piiriülest mõju. Tehisintellektiametile antakse pädevus koguda ja hinnata teavet üldotstarbeliste tehisintellektisüsteemide kohta, toetada liikmesriikide järelevalveasutusi ning teha koostööd Euroopa tasandi struktuuridega, et tagada määruse järjepidev kohaldamine. Tehisintellekti omnibusi ettepanekust jääb selgusetuks, kuidas jagunevad vastutus ja pädevus tehisintellektiameti ning riiklike andmekaitse järelevalveasutuste vahel olukordades, kus üldotstarbelisel tehisintellektisüsteemil põhinev lahendus toob kaasa IKÜMi rikkumise. Ilma selge rollijaotuseta võib tekkida regulatiivne lünk, kus tehniline järelevalve tehisintellekti alusel ja isikuandmete kaitse järelevalve IKÜMi alusel ei moodusta sidusat tervikut, vaid eksisteerivad paralleelselt, vähendades isikuandmete kaitse tegelikku tõhusust.	
102.		**[24.] Liikmesriigi järelevalveasutuste pädevuse piirid (Tehisintellekti määruse artikkel 77)** AKI tõlgenduse kohaselt on põhiõigusi kaitsvatel asutustel kehtiva tehisintellekti määruse artikli 77 alusel volitus dokumentatsiooni küsimiseks otse tehisintellektisüsteemide juurutajatelt ja pakkujatelt. Ettepaneku järgi peaksid põhiõigusi kaitsvad asutused	Osaliselt arvestatud, kajastub seletuskirja punktis 6.5.6.

		vastavat dokumentatsiooni hakkama taotlema turujärelevalveasutuste kaudu. Selline muudatus suurendab tõenäoliselt halduskoormust ja võib tekitada turujärelevalveasutuste juurde nn „pudelikaela“ kui neile lisandub kohustus lisaks olemasolevatele kohustustele igakordselt asuda põhiõigusi kaitsvatele asutustele dokumentatsiooni vahendava asutuse rolli. AKI on seisukohal, et kehtiv tehisintellekti määruse artikkel 77 tuleks jätta muutmata, kuivõrd see ei aita täita ettepaneku lihtsustavat eesmärki. Selle asemel muutub protsess keerulisemaks, kuivõrd sama eesmärgi täitmiseks on vajalik läbida täiendavaid samme. Ühtlasi kitsendatakse selliselt põhiõigus kaitsvate asutuste pädevusi.	
103.		**Küsimused Euroopa Komisjonile** Käesolevaga esitab Andmekaitse Inspektsioon oma tekkinud küsimused. 1. Kuidas tuleks mõista isikuandmete mõiste juures „mõistlikult tõenäoliselt kasutatavad vahendeid“ ning kuidas haakub sellega EK lahendi C-582/14 p 46 sätestatu, et vahendite kasutamisel peab identifitseerimise oht olema olematu või ebaoluline? 2. Miks ei ole Komisjon võtnud isikuandmete mõiste kontekstis arvesse kolmandate isikute mõistlikku võimalust isikuid tuvastada olukorras, kus teabevaldajal selline teave puudub?	Teadmiseks võetud: tegemist on küsimustega, mida on võimalik edastada komisjonile.

		3. Kas seadusandja soov on tõlgendada IKÜM artikkel 5 lõike 1 punkti b põhjendust selliselt, et eesmärgi kooskõla tähendab ka õigusliku aluse olemasolu? 4. Miks ei ole tehisintellektiga seonduvaid sätteid lisatud tehisintellekti määrusesse, vaid tehnoloogiliselt neutraalsesse IKÜMi? 5. Kuidas hinnata andmetöötleja kavatsust isikuandmete töötlemisel IKÜM artikkel 9 lõike 5 kohaselt? 6. IKÜM artikli 12 lõike 5 kohaselt võib pidada ülemääraseks neid andmesubjekti taotlusi, mille eesmärk ei ole andmete kaitsmine. Mida tähendab viidatud „andmete kaitsmine“ ning milliste kriteeriumite alusel tuleks hinnata andmesubjekti eesmärki? 7. IKÜM artikli 13 lõike 4 välistusi arvesse võttes kellel on võimalik antud artiklis viidatud erandit kasutada? 8. Ühtse teavituspunkti loomisel jääb arusaamatuks ENISA roll andmete saamisel. Kas ENISA-l on andmete nägemise õigus? Kuidas hakkab andmete liikumine andmetöötlejalt järelevalveasutusele täpselt toimuma? 9. Kuidas suhestuvad omavahel ühtse teavituspunkti kaudu erinevatele järelevalveasutustele edastatavate teadete tähtajad? Kas mõistlik ei oleks kehtestada ühtne tähtaeg ning järelevalveasutuse teavitamise lävend?	

		10. Kas saame õigesti aru, et kui ühtse teavituspunkti kaudu esitatakse teavitus NIS2 alusel RIAle tähtajaga 24 tundi ja AKIle tähtajaga 96 tundi sama intsidendi osas, siis kas need teavitused tulevad AKIle RIAga samaaegselt ning sellisel juhul on teavitustähtaeg lühem? 11. Rikkumisteate esitamise künnise tõstmise kasuks räägib asjaolu, et järelevalveasutused saavad suurel hulgal rikkumisteateid. Kui eesmärgiks on vähendada väheoluliste rikkumisteadete esitamist, kas künnis ei peaks olema madalam kui praegu väljapakutud „suur oht“? 12. Milline on ettepaneku suhe Komisjoni määrusega 611/2013? 13. Kas IKÜM artikli 88a lõike 4 nõusolekutaotlusest keeldumine ei ole vastuolus IKÜM artikli 7 lõikega 4? 14. Kas IKÜM artikli 88b raamistik on brauseripidajale vabatahtlik? 15. Milline on andmemääruses reguleeritud väärtuslike andmestike ja isikuandmete suhe? 16. Millised on Euroopa tehisintellektiameti ja riiklike pädevate asutuste koostöö tegemise kriteeriumid ning milline on vastavate asutuste rollide ning pädevuste jaotus EL-i tehisintellekti regulatiivliivakasti kontekstis?	
104.	Statistikaamet	Meie esialgsel hinnangul jääb riiklikku statistikat puudutav õiguslik regulatsioon ja eristaatus sarnaseks praegu kehtivaga, kuid	Teadmiseks võetud.

		mitmete õigusaktide üheaegse muutmise kumulatiivset tulevast mõju on hetkel raske hinnata. Meie seisukoht on, et digitaalne omnibuss peab võimaldama riiklikel statistikaasutustel andmete saamist avaliku ja erasektori andmevaldajatelt ning turvalist andmejagamist. Lisaks on oluline, et uuendatud õigusraamistik toetaks riikliku statistika koostamise lihtsustatud viise, sealhulgas uute tehnoloogiliste lahenduste (näiteks tehisaru ja privaatsust säilitav tehnoloogia) eetilist ja läbipaistvat kasutamist.	
105.	Tarbijakaitse ja Tehnilise Järelevalve Amet	Tarbijakaitse ja Tehnilise Järelevalve Amet (TTJA) toetab Euroopa Komisjoni Digital Omnibus paketi üldist eesmärki vähendada Euroopa Liidu digivaldkonna regulatiivset killustatust, parandada õigusraamistiku sidusust ning vähendada nii ettevõtjate kui ka järelevalveasutuste halduskoormust. Kehtiv digiregulatsioonide raamistik on viimastel aastatel kiiresti ja paralleelselt laienenud ning hõlmab mitmeid osaliselt kattuvaid õigusakte, mille kohaldamine on praktikas osutunud keerukaks nii turuosalistele kui ka pädevatele asutustele. Ühtlustamise ja konsolideerimise eesmärk on seetõttu põhjendatud ning põhimõtteliselt toetatav. Samas märgime, et regulatiivne lihtsustamine ei tohi toimuda tarbijate põhiõiguste arvelt. Eelkõige peab säilima kõrge isikuandmete kaitse, läbipaistvuse ja tõhusa õiguskaitse tase ning tarbijate huvid ei tohi jääda tehniliste või majanduslike kaalutluste varju. Digiteenuste usaldusväärsus ja turvalisus on tarbijate jaoks keskse tähtsusega ning nende nõrgenemine mõjutaks otseselt ka digitaalse ühtse turu toimimist.	Võetud teadmiseks

106.		TTJA toetab eelnõus ette nähtud erinevate intsidentidest teavitamise kohustuste koondamist ühtsesse teavituskanalisse (single-entry point). Praktikas seisavad ettevõtjad täna sageli silmitsi olukorraga, kus üks ja sama intsident – näiteks digiteenuse turvarike, millega kaasneb isikuandmete leke ja teenuse katkemine – toob kaasa mitmeid paralleelseid teavitamiskohustusi erinevate õigusaktide ja asutuste ees. Ühtne teavituskanal võimaldab vähendada dubleerimist, parandada teabe kvaliteeti ning soodustada tõhusamat piiriülest koostööd. Samas peab olema selgelt reguleeritud, kuidas ja millise ajaraamistiku jooksul liigub teave ühtsest kanalist edasi riiklike pädevate asutusteni ning millisel hetkel loetakse ettevõtja teavitamiskohustus täidetuks. Oluline on vältida olukorda, kus vastutus hajub või teave ei jõua õigel ajal tegeliku menetlejani.	Arvestatud ja selgitame: Eesti leiab, et erinevates EL õigusaktides olevaid teavitamise tähtaegu tuleks ühtlustada.
107.		TTJA hindab positiivselt avaandmete direktiivi sätete konsolideerimist andmemääruse raamistikku ning avaandmete reeglite muutumist vahetult kohaldatavaks Euroopa Liidu määruseks. Avaandmete parem kättesaadavus ja taaskasutamine toetab tarbijatele suunatud teenuste arengut, sealhulgas hinnavõrdlust, läbipaistvust ning teadlikumaid tarbimisotsuseid. Samas toob direktiivilt määrusele üleminek kaasa ka riske, kuna liikmesriikide senine paindlikkus oma andmekorralduse eripärade arvestamisel väheneb. Eesti kontekstis, kus avaandmete ja e-riigi lahendused on juba kõrgel tasemel, on oluline tagada, et uued ELi nõuded ei eeldaks toimivate süsteemide ümberkujundamist ilma selge lisandväärtuseta.	Teadmiseks võetud.

108.		Väärtuslike andmestike osas peab TTJA vajalikuks säilitada ühtne ELi raamistik, kuid samas võimaldada liikmesriikidel vajaduse korral paindlikumalt täiendada nimekirju, arvestades riiklikke prioriteete ja tarbijakaitsealaseid vajadusi. Digitaalsete turgude ja teenuste kiire areng eeldab, et väärtuslikeks andmeteks võivad kujuneda ka uued andmekategooriad, mis täna ei pruugi veel kehtivates loeteludes kajastuda.	Teadmiseks võetud.
109.		Samas leiame, et Digital Omnibus paketis on ebapiisavalt käsitletud B2G andmevahetuse rolli tarbijakaitses ja turujärelevalves. Kuigi eelnõu keskendub andmete kättesaadavusele ja taaskasutamisele üldiselt, ei ole piisavalt analüüsitud, kuidas B2G andmevahetuse ulatuse kitsendamine mõjutab riigiasutuste, sealhulgas järelevalveasutuste, võimet tuvastada rikkumisi ja kaitsta tarbijate huve. TTJA hinnangul on oluline selgelt määratleda, millistel tingimustel ja eesmärkidel peab avalik sektor saama ligipääsu erasektori andmetele, eriti olukordades, kus see on vajalik tarbijate kaitsmiseks, turukuritarvituste avastamiseks või süsteemsete riskide hindamiseks. TTJA näeb riski, et B2G andmevahetuse ulatuse vähendamine võib nõrgestada turujärelevalvet, eelkõige digiplatvormide, dünaamilise hinnastamise ning tehisintellektil põhinevate teenuste puhul, kus rikkumised ei pruugi olla üksikjuhtumid, vaid ilmnevad mustrite ja suurandmete analüüsi kaudu. Sellistes valdkondades on järelevalveasutuste ligipääs asjakohastele andmetele eelduseks tõhusale ja ennetavale tarbijakaitsele.	Mitte arvestada. Digiomnibussi muudatused on seotud üldregulatsiooniga. Erivaldkondade järelevalve sätted ei ole omnibussi kohaldumisala küsimus. Need tulevad vastava valdkonna eriregulatsioonist. Põhiõiguste kaitse seisukohad olemas. Ettepanekus B2G sätted puudutavad hädaolukorda ja on selgemaks kirjutatud.

110.		Tasude küsimise osas andmete taaskasutamise eest leiab TTJA, et eelnõus vajab see teema täiendavat selgitamist. Kuigi rõhutatakse avaandmete kättesaadavust, ei ole piisavalt käsitletud, millistel juhtudel ja millistel tingimustel on andmete taaskasutamise eest tasu küsimine põhjendatud ning kuidas tagada, et tasud ei kahjustaks tarbijate huve ega piiraks konkurentsi. Eriti oluline on hinnata riski, et tasuline andmete taaskasutus võib tõrjuda turult väiksemaid teenusepakkujaid, sealhulgas iduettevõtteid ja VKE-sid, kelle teenused võivad pakkuda tarbijatele olulist lisandväärtust.	Võtta teadmiseks. Juhime tähelepanu, et kehtivas andmehaldusmääruses on tasu sätted ja küsimise alused juba olemas (vt art 6).
111.		Seoses isikuandmete kaitse üldmääruse ja küpsiste regulatsiooni muudatustega suhtub TTJA eelnõusse ettevaatlikult. Kuigi eesmärk vähendada nn nõusolekuväsimust ja suurendada õigusselgust on mõistetav, on oht, et liiga laialt sõnastatud erandid isikuandmete töötlemisele või terminaliseadmetele juurdepääsule võivad praktikas vähendada tarbijate tegelikku kontrolli oma andmete üle. Eriti oluline on tagada, et nn madala riskiga või teenuse osutamiseks vajalike töötlemiste erandid ei laieneks profiilimisele, käitumuslikule jälgimisele ega tarbijate mõjutamisele. TTJA hinnangul peab nõusoleku põhimõte säilima keskse kaitsemehhanismina ning erandid peavad olema selgelt ja kitsalt piiritletud.	Teadmiseks võetud.
112.		Tehisintellekti määrusega seotud digiomnibusi muudatused on TTJA hinnangul osaliselt toetatavad, eriti osas, mis puudutab VKE-de ja väikeste keskmise turukapitalisatsiooniga ettevõtjate koormuse vähendamist, regulatiivsete liivakastide arendamist ning õigusselguse suurendamist kallutatuse tuvastamiseks vajalike	Teadmiseks võetud.

		andmete töötlemisel. Samas leiame, et SMC-dele kavandatavate leevenduste mõju tarbijakaitsele ja järelevalvele vajab täiendavat hindamist. Oluline on vältida olukorda, kus tarbijate kaitsetase sõltub ettevõtja suurusest ning kus väiksematele või keskmise turukapitalisatsiooniga ettevõtjatele antavad erandid võivad praktikas vähendada tarbijate õiguste kaitset või järelevalve tõhusust. Samas tekitab muret kõrge riskiga tehisintellektisüsteemide kohustuste rakendamise edasilükkamine standardite valmimiseni. Kuigi praktilised rakendusraskused on arusaadavad, ei tohi see viia olukorrani, kus tarbijad jäävad ajutiselt ilma piisavast kaitsest. Leiame, et ka üleminekuperioodil peavad kehtima miinimumkohustused, sealhulgas riskide hindamine, läbipaistvus ning võimalus tarbijatel oma õigusi tõhusalt teostada.	
113.		Eesti jaoks on Digital Omnibus paketil mitmeid spetsiifilisi mõjusid, arvestades riigi kõrget digiteenuste taset ja andmevahetusmudelit. Eesti e-riigi lahendused, sealhulgas X-tee ja avaandmete portaalid, toimivad juba täna hästi ning uued ELi nõuded peaksid neid täiendama, mitte asendama või dubleerima. Lisaks täidab TTJA digiteenuste määruse alusel digiteenuste koordinaatori rolli, mistõttu on oluline, et uued koordineerimis- ja teavitusskeemid oleksid kooskõlas olemasolevate järelevalvepraktikatega ning ei tekitaks täiendavat ebaselgust pädevuste ja vastutuse jaotuses.	Teadmiseks võetud.

114.		Kokkuvõttes toetab TTJA Digital Omnibus paketi eesmärki vähendada ELi digiregulatsiooni killustatust ja halduskoormust ning mitmeid pakutud lahendusi. Samas rõhutab TTJA, et regulatiivne lihtsustamine ei tohi nõrgendada tarbijate õiguste kaitset, isikuandmete kaitset, läbipaistvust ega järelevalve ja õiguskaitse tõhusust. Eelnõu edukas rakendamine eeldab selgeid rakendussätteid, ühtseid tõlgendusi ning piisavat paindlikkust liikmesriikide eripärade arvestamiseks, et säilitada digitaalsete turgude toimimiseks vajalik kõrge usaldustase. Eelnõu edasine kujundamine eeldab selgeid rakendussätteid, täpselt piiritletud erandeid ning kindlust, et järelevalveasutuste tegelik suutlikkus tarbijaid kaitsta säilib ka konsolideeritud regulatiivses raamistikus.	Teadmiseks võetud. Selgete rakendussätete osas seisukoht olemas.
115.	Eesti Interneti Sihtasutus	**Kas toetame eelnõudes toodud eesmärke ja pakutud lahendusi?** Toetame digivaldkonna lihtsustamispaketi üldist eesmärki ja pakutud lahenduste suunda, milleks on Euroopa Liidu digivaldkonna õigusaktide lihtsustamine, regulatiivse killustatuse vähendamine ning dubleerivate kohustuste vältimine. Domeeninduse vaates peame eriti positiivseks: Andmealaste regulatsioonide koondamist andmemäärusesse Toetame andmealaste regulatsioonide (andmete vaba liikumise määrus, andmehalduse määrus ja avaandmete regulatsioon) koondamist andmemäärusesse, mis suurendab õigusselgust ja vähendab olukordi, kus domeenindusega seotud teenuseosutajad peavad samade andmete puhul eraldi analüüsima, kas ja millistel tingimustel kohaldub mõni nimetatud õigusakt. Samuti seda, millised piirangud või kohustused nendest tulenevad. Praktikas	Teadmiseks võetud

		tähendab see, et domeenindusega seotud registripidaja ei pea tegema mitut paralleelset õigusanalüüsi eri regulatsioonide alusel. Andmemäärus loob soovitud ühtse raamistiku, mis selgitab, millal ja millistel tingimustel andmeid võib jagada, millised nõuded kehtivad ning millised erandid kohalduvad, vähendades seeläbi õigusselgusetust ja halduskoormust. Terviklik lähenemine aitab süsteemi ühtlustada ja tagab õigusselguse ka teenusepakkujatele, kes igapäevaselt juriidikaga ei tegele. Intsidentide raporteerimise ühtse teavituskanali (single-entry point) loomist Peame oluliseks intsidentide raporteerimise ühtse teavituskanali loomist, mis on asjakohane nii .ee domeeniregistri kui ka domeenindusega seotud registripidajate vaatest, kelle suhtes võivad samaaegselt kohalduda NIS2, isikuandmete kaitse üldmäärus ning muud teavituskohustused. Ühtne teavituskanal aitab vähendada halduskoormust olukordades, kus sama tehniline intsident võib kvalifitseeruda mitme õigusakti alusel ning suurendab õigusselgust nii teenuseosutajatele kui ka järelevalveasutustele.	
116.		**Avaandmete direktiivi muutumine määruseks.** Põhimõtteliselt toetame avaandmete direktiivi muutumist Euroopa Liidu määruseks, kuna määrus tagab ühtlasema ja selgema rakenduse kogu ELis ning vähendab liikmesriikidevahelisi erinevusi, mis on oluline ka piiriüleselt toimiva digitaristu ja teenuste seisukohalt, sh domeeninduse puhul. Selgitame siiski, et .ee domeeniregister ei ole avaliku sektori asutus avaandmete regulatsiooni tähenduses ja .ee domeeniregister ei halda meie hinnangul avaliku sektori andmeid	Teadmiseks võetud.

		selle regulatsiooni mõttes. Seega nt domeeninimede otsingumootos WHOISi andmed ei ole automaatselt avaandmed. Kaudne mõju võib avaandmete määruses aga tekkida nt olukordades, kus riigiasutused kasutavad domeeni-, DNS- või muud domeenindusega seotud statistikat poliitikakujunduses või kus arutatakse teatud koondandmete võimalikku taaskasutamist. Siin on oluline EISI jaoks rõhutada, et ka muul võimalikul juhul (kui nt leitakse, et avaandmed võiks kohalduda ka riigi poolt asutatud eraõiguslikele SA-dele vms olukorras) domeenindusega seotud tehnilised ja turvalisust mõjutavad andmed (nt terviklik tsoonifail või DNS-logid või muu domeenindusega seotud statistika) ei kvalifitseeruks avaandmeteks. Samuti juhime tähelepanu, et igasuguseks avandmeteks muutmise puhul tuleb riigil kindlasti kaaluda turvalisust ja andmekaitse temaatikat, mis peavad jääma ülimuslikuks.	
117.		**Millised aspektid vajavad täpsustamist või lisaselgitusi?** Praktilise rakendatavuse huvides vajavad mitmed paketis sisalduvad ettepanekud täpsustamist. Täpsustamist vajab intsidentide raporteerimise ühtse teavituskanali praktiline toimimine, sealhulgas see, kuidas on tagatud, et ühe teavituse esitamine täidab tegelikult mitme õigusakti mõju. Näiteks NIS2 ja isikuandmete kaitse üldmääruse teavituskohustused ehk kuidas need ühtlustatakse - kuna tegemist on väga erineva eesmärgiga õigusaktid, on nende ühtse pidepunkti teavituskohustuse selgitamine oluline. Samuti see, kuidas jaotub vastutus riiklike asutuste vahel ja kuidas aitab see vältida olukorda, kus ettevõtjalt oodatakse hiljem täiendavat eraldi teavitamist.	Teadmiseks võetud. Ühtse teavitusakna, täpsemalt sellega seotud teavituste tähtaegade ja teavituste sisu osas on koostatud seisukoht.

		Samuti see, kuidas toimub hilisem aruandluskohustus. Käesolevas paketis kavandatakse ka muudatusi elektroonilise side ja isikuandmete kaitse regulatsioonis, eelkõige seoses küpsiste ja sarnaste tehnoloogiate kasutamist käsitlevate nõusolekunõuetega, mille eesmärk on vähendada veebilehtedel kuvatavate nõusolekuküsimuste hulka. Samuti on eesmärk viia nõusoleku andmine rohkem kasutaja seadme või brauseri tasemele ehk mitte enam kasutajalt enda nõusoleku küsimine. EISi hinnangul vajab selle raames selgitamist machine-readable nõusolekumehhanismide rakendamine, mis tähendab kasutaja nõusoleku edastamist ja arvestamist standardiseeritud tehnilise signaalina, näiteks brauseri või seadme seadistuste kaudu, mitte üksnes veebilehel kuvatava nõusolekuküsimuse kaudu. Oluline on täpsustada, millised tehnilised standardid selleks kasutusele võetakse ning millised üleminekuperioodid on ette nähtud, eelkõige väiksematele teenuseosutajatele, samuti kuidas toimida olukordades, kus selline tehniline nõusolekusignaal puudub või on vastuoluline, et vältida õigusselgusetust ja ebaühtlast rakendamist. Käesoleva muudatuse eesmärk peaks olema ka tagada, et kasutajale ei jääks teadmata, milliseid küpsiseid tema brauseris kasutatakse ja eesmärk peaks olema jätkuvalt kaitsta kasutajaid õigustamatute küpsiste kasutamise eest. Antud juhul jääb mulje, et kuna see liigub brauseri või seadme seadistusse, siis ebateadlikuma kasutaja jaoks tõuseb risk, et tema taustal kasutatakse küpsiseid, millele ta teadliku kasutajana poleks nõusolekut andnud.	
118.		**Täiendav märkus:**	Teadmiseks võetud.

		AI-määrus ja isikuandmete töötlemise kaudne mõju Kuigi AI-ga seotud digiomnibusi muudatused ei mõjuta domeenindust otseselt, on neil kaudne ja süsteemne mõju isikuandmete töötlemise üldisele raamistikule. Eriti tuleb esile isikuandmete töötlemise lubatavuse laienemine AI arendamise osas õigustatud huvi mõiste sisuline leevenemine. EISi hinnangul võib see leevendus pikemas vaates mõjutada ka digitaristu ja domeeninduse valdkonda, kus andmete töötlemine ja jagamine on seni tuginenud pigem kitsalt tõlgendatud õigustatud huvile. Nt seni on EIS väljastanud isikuandmeid kolmandale osapoolele väga piiritletud juhul GDPRi tõlgendades (valdkonna tava) ehk väljastatakse üksnes domeeninimi.ee registreerija isikuandmed (põhjendatud alusel). Samas võib õigustatud huvi aluse laiendamine tehisintellekti määruse kontekstis tuua kaasa olukorra, kus domeenidega seotud isikuandmeid hakatakse nõudma ka laiemates ja senisest erinevates kasutusjuhtudes, mis ületavad domeeninimi.ee õigustatud ulatuse ja eesmärgi. Kuigi iga konkreetset juhtumit tuleb ka edaspidi analüüsida eraldi, peab EIS oluliseks rõhutada, et õigustatud huvi mõiste üldine olemus peaks jääma kitsalt tõlgendatavaks ning selgelt piiritletuks, et vältida selle kontrollimatut ja laienevat rakendamist.	
119.	Eesti Linnade ja Valdade Liit	**Kas toetate eelnõudes toodud eesmärke ja pakutud lahendusi? Palun tooge välja, milliseid toetate ja miks? Milliseid ettepanekuid Teie ei toeta ja miks?** Eesti Linnade ja Valdade Liit tunnustab Euroopa Komisjon püüdlusi läbi digivaldkonna õigusaktide lihtsustamispaketi	Teadmiseks võetud. Andmeõiguse vaatest selgust on silmas peetud.

		"digiomnibus" muuta selgemaks andmehalduse ning andmete kasutamise regulatsioone. Peame oluliseks, et reeglid oleksid arusaadavad ning toetaksid kaasaegsete ja kasutajasõbralike avalike teenuste arendamist. See ei ole üksnes vajalik Euroopa riikide konkurentsivõime tugevdamiseks, vaid eelkõige elanike heaolu tõstmiseks vajalike lahenduste väljatöötamiseks ning kasutuselevõtmiseks. Regulatsioonide taasmõtestamine peaks aitama puhastada õigusaktid üleliigsest jättes alles vaid hädavajaliku ja muuta otsustus- ning valitsemisprotsessi läbipaistavamaks. Prioriteediks peaks olema inimene koos oma õiguste ja vajadustega. Silmas tuleks eelkõige pidada võimalusi, mida andmed otsustusprotsessis loovad ja püüelda eelkõige just võimaluste avardamise suunas. Kokkuvõtval nähti kaasatud kohalike omavalitsuste poolt positiivsena: • andmevaldkonna õigusaktide koondamist, mis teeb omavalitsuse kohustused selgemaks; • ühtse kanali loomine vähendaks dubleerimist ja lihtsustaks omavalitsuste tööd (praegu tuleb sama intsidendi kohta teavitada mitut asutust, näiteks Riigi Infosüsteemi Ametit (RIA/CERT-EE) ja Andmekaitse Inspektsiooni (AKI), sageli eri vormides ja erinevate tähtaegadega, samas, seda annaks ehk parandada ka siseriiklikult, mitte toetudes EL regulatsioonile); • tehisintellekti lahenduste testimise ja kasutamise selgemat raamistikku.	Ühtse teavitusakna osas ei piisa ainult siseriikliku õiguse muutmisest – konkreetsemad tähtajad ja teavituse sisud näeb ette EL õigus.

120.		**Palun tooge välja muud teemad, mis on nimetatud akti puhul Teile murekohaks.** Digivaldkonna arengul on võimaluste kõrval mitmeid ohte, mida peab läbi regulatsioonide ennetama. Õiguslike ohtude kõrval tuleks enam arvestada andmekasutuse piirangutega kaasneva „ääremaastumise“ eest. Avalike teenuste osutamine tiheasustatud aladel erineb sageli põhimõtteliselt võrreldes hõredalt asustatud maapiirkondadega (n. pole vaja linnades ühistransporti ümber korraldada kui elama saabub uus perekond, kuid maapiirkonnas võib uue perekonna elama asumine tuua kaasa vajaduse koolibussi teekond ümber teha, kuid selleks on vaja õigust andmete töötlemiseks). Õigusaktid ei tohiks võimendada erinevusi, vaid luua olukorra, kus digitaalsed lahendused annaksid võimaluse osutada teenuseid vastavalt piirkondlikele erisustele ja säilitada kohalikku autonoomiat. Enamik avalikke teenuseid, mida inimesed tarbivad, on seotud otseselt kohalike omavalitsustega ja nende poolt pakutavaga. Tänane „digiomnibusi“ regulatsioon ei arvestada piirkondlikke iseärasusi piisaval määral soovides ühtlustada põhimõtteid, mida võiks otsustada kohalikul tasandil. Õigusaktiga kaasneva mõju ulatuse analüüs näib liialt abstraktne. Kohalike omavalitsuste ja nende esindusorganisatsioonide kaasamine ei ole olnud piisav. Seda on tehtud kiirustades, mõjusid piisaval määral arvestamata. Mõjuanalüüsid ei arvesta piisaval määral kohalikke otsuseid ning seadusakti rakendamisega kohalikul tasandil. Eelkõige otsuste puhul, kus andmete kasutamisega kaasnevate otsustega oleks võimalik ressursse	Teadmiseks võetud. Tegemist on üldregulatsiooniga, sätestades ühtsed alused ja võimalused kõigile, sh omavalitsustele.

		otstarbekamalt kasutada. Praegusel kujul on Euroopa Komisjon digivaldkonna õigusaktide lihtsustamispaketi "digiomnibus" vormilt koondav ja sisult õiguslik, kuid kohalikul tasandil praktikas realiseeritavus ebamäärane. See omakorda süvendab hirme täiendavate kohustuste ja sellega kaasnevate kulude osas.	
121.		Omavalitsuste tagasisides toodi välja peamiste murekohtadena: • Uute andmenõuete rakendamine tähendab sageli vajadust muuta infosüsteeme või tööprotsesse, milleks ei ole alati ette nähtud eraldi rahastust. Uute nõuetega võivad kaasneda lisakulud ja personalivajadus. • Linna ametnikud vajavad praktilisi juhendeid ja koolitusi, et mõista, kuidas uusi reegleid teenuste arendamisel rakendada. • Ebapiisava selguse korral võib linn jätta kasutamata innovaatilisi lahendusi, näiteks AI-põhiseid analüüsitööriistu, kuigi need aitaksid parandada teenuste kvaliteeti.	Teadmiseks võetud.
122.	Eesti Keele Instituut	Viidatud kirjas tuuakse mitmeid näiteid, kus kavandatakse sätted kirjutada erinevates õigusaktides – olgu siis Euroopa Liidu direktiivis või määruses – selgemaks, lähtudes parimatest praktikatest. Instituut, tegeledes keeleandmete ja -tehnoloogiaga, töötleb andmeid teadusuuringute eesmärgil, milles sisalduvad nii isikuandmed kui tihti keeleandmestikena ka autoriõigustega kaitstud teosed. Seetõttu tuleks hinnata, kuivõrd on need kaks maailma omavahel teaduseesmärkideks tegelikult ühildatavad. Isikuandmete kasutus teadusuuringute eesmärgil on lubatud lähtuvalt eesmärgist, kus teadusuuring peab toimuma mingi laiema	Osaliselt arvestatud ja teadmiseks võetud.

		hüve eesmärgil (uus ravim, uus meetod, uus teadmus). Isikuandmete kaitse seadus võimaldab seega andmekasutust viisil, kus teavet ise ei omata, kuid teadust soovitakse teha, seejuures on võimalik taotleda isikuandmeid ka kolmandatelt isikutelt – kui töötlemiseks on õiguslik alus, on võimalik andmeid saada (IKS § 6). Seevastu autoriõigustega kaitstud teoste puhul on teadusuuringu läbiviimine komplitseeritum ning mitmed nüansid normis piiritlemata ja sisustamata ka kohtupraktikas. Jäädes viimast ootama, on seni teadusuuringute läbiviimine praktikas keeruline (vt AutÕS § 191). Näiteks seab andmekaitse üldmäärus esikohale just riiklikud registrid ja seega avaliku sektori käes oleva teabe kättesaadavuse teadusuuringuteks, nähes neis erilist väärtust (IKÜM pp 157). Samuti rõhutab üldmäärus, et teadusuuringu mõiste on lai, hõlmates seejuures ka tehnoloogiaarendust (IKÜM pp 159). Isikuandmete kaitse seadus ei keela kaasata teisi kaasvastutavaid töötlejaid või volitatud töötlejaid sellesse protsessi. Autoriõiguse seaduse aluseks oleva direktiivi põhjendused sarnaseid selgeid selgitusi ei anna (nn DSM direktiivi). Selles on toodud, et autori nõusolekuta ja autoritasu maksmiseta on teadus- ja kultuuripärandiasutusel õigus reprodutseerida teadusuuringutes teksti- ja andmekaeve eesmärkidel teost, millele tal on seaduslik juurdepääs (AutÕS § 191 lg 1). Sätte tõlgenduste järgi saab teadusuuringut teha teadusasutus teise teabevaldaja teabega vaid siis kui tal on sellele juurdepääs. Enamasti on see läbi avaandmete. Muul juhul lähenetakse läbi füüsilise isiku tõlgenduse, kes on nt raamatukogu kasutajaks, tekitades keerukaid konstruktsioone ja lepinguid teadusuuringu läbiviimisel ja alusmaterjali töötlemisel. Seegi tõlgendus ei kehti alati ja kõigi suhtes. Siin lähtutakse autori	

		algsest litsentsist, kus nt teaduspublikatsiooni autor annab litsentsi teose säilitamiseks elektroonilises repositooriumis ning teose avaldamiseks üldsusele. Kui eraldi litsentsi publikatsioonist koopia tegemiseks ja teadusasutusele väljastamiseks ei küsitud, ei olegi see otse asutuselt asutusele sellisel viisil koopia tegemine võimalik, kuigi seda palub teadusasutus ja teadusuuringu eesmärgil (nagu erand ette näeb). Seega ei ole ühelt poolt avalik teave kättesaadav mugavamal viisil, eeldades sisuliselt avaandmete kraapimist ning teisalt, kõik teosed ei pruugi otsejuurdepääsetavad olla, mistõttu tekib küsimus nende kättesaadavusest teaduseesmärkidel. Seejuures võib teabe korje sellisel viisil, isegi kui see on avalik, võtta eraldi ressursse ja aega kui samas võiks selle väljastada teabevaldaja, nagu seda isikuandmete puhul tehakse. Riive autoriõiguste kontekstis ei muutu ning küsimus on teadusuuringuks teabe kättesaadavuse kiiruses ja ressursides (kraapides oleks avalikustatud teost õigus teadusuuringus kasutada nii ehk nii). Peale teabe saamise eeldavad õigusselgust ka mitmed teised aspektid. Näiteks kuivõrd on autoriõiguste kontekstis lubatud koostöö erasektoriga, kes omab tihti ainulaadset pädevust või tehnikat, et teatud andmeid sellises mahus üldse töödelda või mustreid leida, rääkimata kus erasektor teatud valdkonda võibki eest vedada. Kuigi direktiivi põhjenduspunkt koostööle viitab, on õiguskirjanduses selle tõlgendused selle ulatuse osas ettevaatlikud (vt DMS direktiiv pp 11). Instituut austab autorite õigusi ning on selge, et autorite õiguste kaitseks tuli sätestada selge erand, et teoste kasutust piiritleda. Käesoleva kirja mõte on aga rõhutada, et andmete kättesaadavus on problemaatiline isegi teadus- ja arendusasutustel, kelle tarvis erand loodi. Kui andmete	

		kättesaadavus on takistatud seatakse eesti keele uurimine olemuslikult kahtluse alla (näiteks kasvõi uue ÕS-i tegemine, sõnaveebid vms). Lõpetuseks rõhutame, et keeleuurimisel või keeletehnoloogiate arendamisel on mõlema valdkonna normiselgus väga tähtis, nii nagu andmete kättesaadavus. Seetõttu loodame, et käesolevast diskussioonist on abi sätete selgemaks muutmisel või vähemalt eesmärgiäraste tõlgenduste andmisel). Loodame, et käivitatud tegevused loovad selgust ning võimalusel panustaksime omalt poolt ka teema edasistes aruteludes.	
123.	Eesti Vee-ettevõtjate Liit	Eesti Vee-ettevõtete Liit toetab kõrge riskiga tehisintellektisüsteemidele kehtestatud kohustuste jõustumise edasilükkamist, kuna ilma Euroopa Komisjoni juhiste ja standarditeta ei ole praktikas võimalik nõuetele vastavust tagada. Samas on oluline, et edasilükkamise korral oleks esitatud vähemalt indikatiivne ajakava juhiste ja standardite valmimise kohta, sest vastasel juhul puudub õigusselgus selle osas, millal vastavad kohustused jõustuvad. Ühtlasi palume Euroopa Komisjonilt konkreetseid suuniseid ja näiteid, millised veesektoriga seotud tehisintellekti süsteemid võivad kuuluda kõrge riskiga süsteemide regulatsiooni alla. Näiteks, kas ja millistel tingimustel võivad joogi- ja reovee puhastusprotsesside optimeerimiseks kasutatavad AI-süsteemid olla potentsiaalselt kõrge riskiga süsteemideks.	Arvestatud osas, mis toetab kõrge riskiga tehisintellektisüsteemide tähtaja edasi lükkamist ja konkreetseid tähtaegu. Komisjon annab erinevaid juhiseid juba välja. Vee-ettevõtjate osas saame eraldi saata Komisjonile küsimuse.
124.		Toetame ühtse intsidentidest teavitamise keskkonna (SEP1) loomist, kuid juhime tähelepanu, et erinevad teavitustähtajad (24h esmane teavitus NIS22 puhul ja 72h teavitustähtaeg IKÜM puhul) võivad praktikas vähendada SEP-i praktilist kasu. Seega palume	Arvestatud Ühtse teavitusakna, täpsemalt sellega seotud teavituste tähtaegade

		kaaluda erinevate teavitustähtaegade ühtlustamist, mis aitaks kaasa ettevõtjate halduskoormuse vähenemisele. Samuti võiksid SEP alla kuuluda ka AI määrusest tulenevad teavitused.	ja teavituste sisu osas on koostatud seisukoht.
125.		Seoses avaandmete direktiivi4 muutumisega andmemääruseks meil sisulisi ettepanekuid ei ole. Hetkel me ei näe vajadust ka muuta väärtuslike andmestike nimekirju.	Teadmiseks võetud.
126.		Meie hinnangul vajavad täpsustamist ja lisaselgitusi biomeetriliste andmete töötlemise alused.	Teadmiseks võetud.
127.		Meie hinnangul vajab täiendavat analüüsi isikuandmete nn „kontekstipõhine“ määratlus. Omnibus-paketis pakutud lähenemine looks olukorra, kus andmete edastamisel peaks töötleja iga kord eelnevalt hindama, kas ja mil määral on andmete saajal võimalik nende põhjal isikut tuvastada. See kehtiks ka näiteks volitatud töötlejate puhul, kellele vastutav töötleja edastab isikuandmeid oma ülesannete täitmiseks. Leiame, et selline üldine põhimõte ei vähendaks ettevõtjate halduskoormust ega suurendaks õiguskindlust, vaid pigem vastupidi. Taoline käsitlus võiks olla põhjendatud üksnes erandina teatud liiki isikuandmete puhul, näiteks juhul, kui tegemist on isiku kujutisega filmimaterjalil, kus kujutis on väike ja/või hägune ning isikut ei ole võimalik reaalselt tuvastada ilma eelneva teadmiseta tema viibimisest filmimise ajal konkreetses asukohas või näiteks isikule omase riietuse põhjal. Sellisel juhul on siiski oluline, et võimalikud erandid oleksid väga täpselt, selgelt ja üheselt mõistetavalt sõnastatud.	Arvestatud. Eesti ei toeta mõiste täiendamist, vaid palume täiendada põhjenduspunkti.

128.	Veriff OÜ	Artiklit 9 muudetakse järgmiselt: (a) lõikesse 2 lisatakse järgmised punktid: „(k) töötlemine tehisintellekti süsteemi, nagu see on määratletud määruse (EL) 2024/1689 artikli 3 punktis 1, või tehisintellekti mudeli arendamise ja toimimise kontekstis, järgides lõikes 5 osutatud tingimusi. (l) biomeetriliste andmete töötlemine on vajalik andmesubjekti isiku tuvastamise kinnitamiseks (verifitseerimiseks), kui biomeetrilised andmed või verifitseerimiseks vajalikud vahendid on üksnes andmesubjekti ainuvalduses.“ (b) lisatakse järgmine lõige: „5. Lõike 2 punktis (k) osutatud töötlemise korral rakendatakse asjakohaseid korralduslikke ja tehnilisi meetmeid, et vältida isikuandmete eriliikide kogumist ja muud töötlemist. Kui vaatamata selliste meetmete rakendamisele tuvastab vastutav töötleja isikuandmete eriliigid treenimiseks, testimiseks või valideerimiseks kasutatavates andmekogumites või tehisintellekti süsteemis või tehisintellekti mudelis, peab vastutav töötleja need andmed eemaldama. Kui nende andmete eemaldamine nõuab ebaproportsionaalseid jõupingutusi, peab vastutav töötleja igal juhul viivitamata ja tõhusalt kaitsma neid andmeid selle eest, et neid kasutataks väljundite loomiseks, avalikustataks või muul viisil kolmandatele isikutele kättesaadavaks tehtaks.“**	Teadmiseks võetud.

		Kommentaarid, tähelepanekud, ettepanekud Artikli 9 lõike 2 punkti (k) ja artikli 9 lõike 5 lisamine Ei ole selge, mis on selle täienduse kavandatav eesmärk, eelkõige: – Kuidas on see muudatus seotud määruse (EL) 2024/1689 (AI-määrus) artikli 10 lõikega 5, mis lubab isikuandmete eriliikide töötlemist kallutatuse vähendamise eesmärgil. Ei ole selge, kas AI-määruse artikli 10 lõiget 5 tuleks siis pidada kohaldatavaks ainult kõrge riskiga tehisintellekti süsteemidele ning artikli 9 lõike 2 punkt (k) oleks kohaldatav kõigile muudele kui kõrge riskiga süsteemidele, või kõigile süsteemidele, sealhulgas kõrge riskiga süsteemidele. – Kavandatav sõnastus („töötlemine tehisintellekti süsteemi /–/ toimimise kontekstis /–/ või tehisintellekti mudeli puhul“) jätab mulje, et tehisintellekti süsteemi käitamine on iseenesest töötlemistoiming, kuigi tehisintellekti süsteem või mudel on tehnoloogiline vahend ning seda ei tohiks kohelda teisiti kui muid tehnoloogilisi vahendeid andmete töötlemisel. Koos artikli 9 lõikega 5 võib see sõnastus tekitada isegi segadust tekitava kohustuse andmeid töötlemisest eemaldada. – Lisaks on sõnastus äärmiselt tehnoloogiaspetsiifiline ja keskendub praegusele tehnoloogilisele olukorrale, mis on vastuolus ELi keskse regulatiivse põhimõttega – tehnoloogianeutraalsusega. Selle põhimõtte kohaselt peaksid õigusnormid keskenduma tulemustele ja funktsioonidele, mitte konkreetsetele	

		tehnoloogiatele, et vältida innovatsiooni pärssimist, tagada reeglite tulevikukindlus ning lasta turul valida parimad lahendused. Kavandatav sõnastus ei arvesta biomeetrilise tehnoloogia kasutamise tegelikkust. Seadusandja peaks mõistma, et kui eksisteerivad tehisintellekti mudelid ja süsteemid, mis töötlevad biomeetrilisi andmeid, siis peavad need mudelid ja süsteemid olema korrektselt treenitud. Selliste mudelite treenimine ja kasutamine eeldab, et vastavad andmed on töötlemistoimingute osa. See tähendab, et neid andmeid kasutatakse väljundite loomiseks, vastasel juhul ei oleks need süsteemid toimimisvõimelised. Seetõttu on artikli 9 lõike 5 praegune sõnastus väga kaugel sellest, kuidas hästi toimiv ja „korrektselt käituv“ tehisintellektil põhinev biomeetriline süsteem tegelikult töötab. Lisaks seab nõue andmed eemaldada, välja arvatud juhul, kui see nõuab ebaproportsionaalseid jõupingutusi, äärmiselt kõrge standardi. See võib oluliselt takistada paljude tehisintellekti mudelite ja süsteemide arendamist ja toimimist. Väljend „kaitsta andmeid selle eest, et neid kasutataks väljundite loomiseks“ on ebaselge, kuna ei ole määratletud, mida „väljundite loomine“ tähendab. Kuna avalikustamine ja kättesaadavaks tegemine on käsitletud eraldi, saab „tootmist“ tõlgendada üksnes kui treeningandmete panuse välistamist tulemustesse. See oleks aga tehniliselt teostamatu, sest treeningandmed on olemuslikult osa tulemuste kujunemisest. Ettepanekud:	

		Eemaldada artikli 9 lõike 2 punktist (k) mõiste „toimimine“ (operation). Sõnastada artikli 9 lõige 5 ümber nii, et see kõlaks järgmiselt: „Lõike 2 punktis (k) osutatud töötlemise korral rakendatakse asjakohaseid korralduslikke ja tehnilisi meetmeid, et vältida isikuandmete eriliikide ebavajalikku töötlemist.“ Teise võimalusena sõnastada artikli 9 lõige 5 järgmiselt: „Lõike 2 punktis (k) osutatud töötlemise korral rakendatakse asjakohaseid korralduslikke ja tehnilisi meetmeid, et vältida isikuandmete eriliikide kogumist ja muud töötlemist. Kui vaatamata selliste meetmete rakendamisele tuvastab vastutav töötleja isikuandmete eriliigid treenimiseks, testimiseks või valideerimiseks kasutatavates andmekogumites või tehisintellekti süsteemi või tehisintellekti mudeli TOIMIMISE käigus, peab vastutav töötleja need andmed eemaldama ESIMASEL VÕIMALUSEL. Kui nende andmete eemaldamine nõuab ebaproportsionaalseid jõupingutusi VÕI ON VASTUOLUS TEHISINTELLEKTI SÜSTEEMI VÕI MUDELI EESMÄRGIGA, peab vastutav töötleja igal juhul viivitamata ja tõhusalt kaitsma neid andmeid selle eest, et neid kasutataks väljundite loomiseks, avalikustataks või muul viisil kolmandatele isikutele kättesaadavaks tehtaks, RAKENDADES ASJAKOHASEID KORRALDUSLIKKE JA TEHNILISI MEETMEID.“.	

129.		Artikli 9 lõike 2 punkti (l) ja põhjenduse (34) lisamine Ei ole selge, mis on selle täienduse kavandatav eesmärk, eelkõige: – Mida see säte peaks võimaldama? – Mille eest see säte peaks andmesubjekte kaitsma, arvestades üldisest keelust (artikli 9 alusel) tehtavat erandit? Meie lähenemisviis on, et leevendus peaks võimaldama kahte elementi: i) luua raamistiku biomeetria kasutamiseks turvalise ja üha laiemalt levinud turvafunktsioonina, mida ettevõtted saavad oma tavapärase äritegevuse käigus rakendada, järgides samal ajal juba niigi tugevat privaatsusraamistikku; ning ii) pettuste ennetamist suures ulatuses, tagades samal ajal hea ja sujuva kasutajakogemuse. Seetõttu ei arvesta üksnes kasutaja verifitseerimise nõuete leevendamine sellega, et paljud pettuste ennetamise protsessid põhinevad üks-mitmele („autentimine“), näiteks kontole sisselogimise ja parooli lähtestamise võimaldamisel biomeetria abil. Andmesubjektide kaitsmise osas võimalike riskide eest, mis tulenevad isikuandmete eriliikide töötlemisest, näib seadusandja rõhutavat „andmesubjekti ainukontrolli“. „Ainukontroll“ viitaks väga vähestele tehnoloogilistele lahendustele, mida praktikas tänapäeval peaaegu ei kasutata – enamasti kasutatavad tehnoloogiad jätavad andmed teenuseosutaja kontrolli alla	Teadmiseks võetud.

		verifitseerimise või autentimise eesmärgil. Täpsemalt ei täida andmesubjekti „ainukontroll“ eesmärki kaitsta tema õigusi, sest arvestades aluseks oleva tehnoloogia keerukust ei ole tehniline kontroll protsessi üle see, mis tegelikult kaitseb andmesubjekti peamiste riskide eest. Andmesubjekt saab suurema kaitse siis, kui: i) aluseks olev tehnoloogia on turvaline (nt kasutatakse krüpteerimist, nagu ettepanekus juba viidatud); ja ii) andmesubjekt on töötlemisest teadlik ning saab valida, kas ta soovib sellega hõlmatud olla või mitte. Seetõttu tuleks rõhk asetada mitte tehnilisele „ainukontrollile“, vaid asjaolule, et isiku tuvastamise kinnitamine isikuandmete eriliikide abil (nii verifitseerimine kui ka autentimine) toimub andmesubjekti taotlusel või tema poolt soovitud teenuste raames. Põhjenduse praegune sõnastus näib käsitlevat väga kitsast tehnoloogilist lahendust, mis on vaid üks või väga piiratud hulk privaatsust säilitavaid tehnoloogiaid. Ettepanekud: Laiendada biomeetria kasutusjuhtumeid ka autentimisele lisaks verifitseerimisele. Ideaalis hõlmaks laiendus ka pettuste ennetamist ja avastamist; Mõiste „ainukontroll“ tuleks üle vaadata nii, et kontroll oleks teenuseosutaja, mitte üksnes andmesubjekti käes. Selline lähenemine tagaks andmete tehnilise turvalisuse ning seoks töötlemistoimingud tegevustega, mis on otseselt või kaudselt seotud andmesubjekti poolt taotletud teenustega. Peamised	

		eesmärgid peaksid jääma andmete turvalisus ja andmesubjekti teavitatus (läbipaistvus).	
130.	Sotsiaalministeerium	Toetab Digitaalse Omnibus'e eesmärki vähendada bürokraatiat ja lihtsustada reegleid. Positiivne on, et väiksematele ettevõtetele antakse rohkem aega ja lihtsamaid nõudeid ning Euroopa tasandil luuakse ühtne järelevalve. Samas tekitab muret, et mõned inimeste kaitseks mõeldud reeglid hakkavad kehtima alles 2027–2028, mis võib kaasa tuua riske. Tundlike andmete kasutamine kallutatuse kontrolliks on vajalik diskrimineerimise vältimiseks, kuid see toob kaasa privaatsusriskid, mistõttu **tuleb andmeid rangelt kaitsta.** Lisaks võib AI kasutamise läbipaistvuse vähenemine muuta inimestele raskemaks aru saada, kus ja kuidas algoritme kasutatakse. Sotsiaalministeeriumi soovitus on hoida **inimeste õigused ja turvalisus esikohal**, tagada tugev järelevalve tundlike **andmete kasutamisel ning avalikus sektoris teavitada AI kasutusest** ka siis, kui seadus seda ei nõua. Andmete vaates juhime tähelepanu, et **isikuandmete mõiste muutmist** ei saa teha kiirustades – selle muudatuse mõjud vajavad põhjalikku kaalumist. See mõiste on kogu andmekaitse vundament. 1. Seni on **pseudonüümseid isikuandmeid** käsitletud isikuandmetena, millele kohalduvad samaväärsed kaitsemeetmed, mis isikuandmetelegi. Pseudonüümsete andmete eristamine võimaldab üle vaadata sellistele andmetele kohalduvad meetmed ja sellist reeglite lõdvendamist ka plaanitakse. Juhime tähelepanu, et kui pseudonüümsete andmete töötlusreegleid plaanitakse lihtsustada, siis ei tohiks järele anda andmete volitamata	1 – Eesti ei poolda mõiste täiendamist, vaid teeb ettepaneku täiendada põhjenduspunkti. 2 – teadmiseks võetud. 3 – teadmiseks võetud. 4 – Eesti leiab, et erinevates EL õigusaktides ette nähtud teavitamistähtaegu tuleks ühtlustada. 5- teadmiseks võetud.

		juurdepääsu kaitsmemeetmetes (korralduslikud ja tehnilised meetmed). Ka algatuses endas tuuakse esile erisusi, et pseudonüümsete andmete töötlemisel tuleb vältida isikuandmete kogumist, nende tuvastamisel tuleb need eemaldada ja kui nende eemaldamine on keeruline, siis tuleb kaitsta. Teeme ettepaneku mitte märkimisväärselt järele anda andmete volitamata juurdepääsu kaitsemeetmetes, sest risk isikandmete tuvastamiseks jääb igal juhul alles. 2. Andmete valdkonda reguleerivate määruste ja direktiivide ülevaatamisel, ühtlustamisel ja konsolideerimisel tuleb üle vaadata ka Euroopa Terviseandmeruumi määrus teemades, kus üldiselt planeeritakse reeglite lihtsustamist. Näiteks näeb määrus ette samaväärseid kaitsemeetmeid terviseandmetele isikuandmete ja pseudonüümsete andmete töötlusele teiseses andmekasutuses. **Terviseandmed eriliigiliste andmetena** vajavadki arusaadavalt rangemaid kaitsemeetmeid, kuid peaksime vältima olukorda, kus tekivad vastuolud EL määruse vahel, pärssides valdkondade vahelisi andmetöötlusi erinevalt kohalduvate reeglite tõttu ning mõnes kohas võib lihtsustamine ka selle määruse kontekstis kõne alla tulla analoogselt algatuses esitatuga. 3. Algatuses tuuakse esile, et **AI liivakastides kasutatavate andmete jagamise ja kaitse osas on ette nähtud täiendavad meetmed, et vältida andmete väärkasutust ja tagada andmete konfidentsiaalsus**. Juhime tähelepanu, et terviseandmete kontekstis räägitakse turvalistest andmetöötluskeskkondadest (SPE). AI liivakastide ja SPE-de nõuded võiksid olla vähemalt	

		sarnased, osaliselt samad. Võimalusel tuleks nimetatute koostalitusvõimes veenduda. Samuti tuleb jälgida, et ei tekiks siin vastuolusid, sest terviseandmeid võib töödelda vaid selleks ette nähtud SPE-des teiseses kasutuses, sh innovatsiooni eesmärgil. 4. **Andmelekkest teavitamine peab toimuma viivitamata ja võimaluse korral mitte hiljem kui 96 tunni jooksul pärast rikkumisest teada saamist.** Selle aja pikendamine ei taga andmelekete puhul kiiret sekkumist ja seeläbi tagajärgede leevendamist. Jääb arusaamatuks, miks on päriselt pikendamine vajalik. Kaasaegse tehnoloogilise võimekuse tingimustes on 96 tundi väga pikk aeg. 5. Suhtume üldiselt **ettevaatlikult AI treenimise käigus tekkivate eriliigiliste isikuandmete töötlemise lubamiseks juhtudel, kus see ei ole eesmärgi jaoks vajalik.** Kuigi sellise sätte kohaldumise tingimusi on kitsendatud, millistel juhtudel see oleks lubatud, siis eriliigiliste isikuandmete töötlemist ei tohiks sellisel viisil lubada. Selliste andmete kogumine ja kasutamine võiks jääda rangemate ja läbipaistvamate kaitsemeetmete alla. Sellisel viisil eriliigiliste andmetele lubatavuse piiri on praktikas keeruline rakendada ja ka kontrollida.	