ÕIGUSLOOME JA KOHTULAHENDID

Õigusloome arengutest

2019. aasta oli õigusloomeliselt kirev. Vaja oli muuta siseriiklike õigusakte nii valdkondlike eriseaduste kui määruste tasandil, et need kooskõlla viia kehtiva andmekaitseõigusega.

Eelnõude ettevalmistamisel küsiti arvamust ka inspektsioonilt, kuid paraku ei olnud võimalik väiksel asutusel piiratud ressursside juures kõigile eelnõudele tagasisidet anda. Tagasiside saanud eelnõude osas toome välja üksnes kõige tähelepanuväärsemad. Etteruttavalt võib öelda, et mitte kõigi kavatsuste osas ei olnud eelnõude koostajad andmesubjekti ning tema õiguste kaitsmise vaatenurgast olulist läbi mõelnud.

Andmekaitseõiguse uuenemisest

Muudatuste aluseks oli Euroopa Parlamendi ja nõukogu 2016. aasta aprillis vastu võetud kaks õigusakti, milleks olid

- määrus nr 2016/679, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (IKÜM);
- direktiiv nr 2016/670, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK (nn õiguskaitseasutuste direktiiv).

Õigusaktide üle võtmine Eesti õigusesse oli vajalik Euroopa Liidu tasemel sarnase õiguskorra kehtestamiseks.

Isikuandmete kaitse seadusega (IKS) tuli reguleerida teatud IKÜM-i üldisemaid ning õiguskaitseasutuste direktiivi sätteid. IKS- st tulevad ka Andmekaitse Inspektsiooni tegevust reguleerivad sätted, järelevalve korraldus ning väärteokaristuste määramine.

Justiitsministeerium soovis algselt teha muudatusi kahes etapis – esimesena võtta vastu uus IKS ning seejärel IKS-i rakendamise seadus. Kuigi mõlemad eelnõud olid pikka aega kooskõlastamistel ning ettevalmistamisel, siis soovitud tähtajaks (25.05.2018) neid siiski vastu võtta ei suudetud. Uut IKS-i menetleti Riigikogus isegi kaks korda. Lõpptulemusena võeti seaduse vastu 12.12.2018 ning jõustumise kuupäevaks sai 15.01.2019. Teine siseriiklikus õiguses korrektiive teinud isikuandmete kaitse rakendamise seadus võeti vastu alles 20.02.2019 ning selle jõustumise kuupäevaks sai 15.03.2019. Rakendamise seadusega tehti muudatusi 127 seaduses.

Õigusloome nõuab alati põhjalikku eeltööd ning eelnõude koostamine erinevate huvigruppide arvamusega arvestamist. Kuigi võiks arvata, et muutmist vajavate seaduste eelnõudes on inspektsioonilt arvamuse küsimise hetkeks juba piisava põhjalikkusega kõik läbi mõeldud ja analüüsitud, ei pruugi see nii olla ning peale inspektsioonilt tagasiside saamist lisatakse eelnõusse sätteid, millega andmekaitseliselt ei saa nõustuda. Lisaks ei võeta ka alati inspektsiooni antud

tagasisidet kuulda, kuid andmekaitsereformi käigus antud inspektsiooni seisukohad on leitavad aki.ee võrgulehelt.[9]

Karistusseadustiku (KarS) muutmise eelnõu[10]

Üks andmekaitseõigusega seotud olulistest muudatustest oli siseriikliku karistusõiguse muutmine. Kuna Eesti õiguses puudub haldustrahvi instituut ning IKÜM põhjenduspunkti 151 kohaselt määrab inspektsioon trahve väärteomenetluse raames, tuli selleks muuta karistusseadustikku (KarS).

Enne eelnõu jõudmist Riigikogusse esitas inspektsioon oma arvamuse, milles korrati juba varasemalt esitatud seisukohti, mis puudutasid vajadust tuua Eesti õigusesse sisse haldustrahvi instituut[11]. Inspektsioon leidis, et uue IKS-i alaseid karistusi tuleks määrata haldustrahvina, mitte väärteomenetluse raames väärteotrahvina.

Inspektsioon juhtis Justiitsministeeriumi tähelepanu asjaolule, et andmekaitse valdkonnas on karistuste määramise reguleerimine vajalik mitte ainult IKÜM, vaid ka muude Euroopa Liidu õigusaktide tõttu. Lisaks üldmäärusele on ka õiguskaitseasutuste direktiivi artiklis 57 märgitud, et liikmesriigid peavad kehtestama tõhusad karistused (penalties) direktiivi üle võtvate sätete (Eestis IKS-i 4. peatüki sätete) rikkumise korral. Selle kõrval on ka direktiivi nr 2016/681 (nn broneeringuinfo direktiiv) artiklis 14 märgitud, et tuleks ette näha karistused, sh rahalised karistused (*penalties, including financial penalties*) direktiivi siseriiklikult üle võtvate normide rikkumise korral. Näiteks konkurentsiõiguse alal pannakse Euroopa Komisjoni ettepaneku kohaselt ka neile liikmesriikidele, kel veel pole haldustrahve, kohustus need kehtestada.

Kõnealuse seaduseelnõu seletuskirjas oli (KarS § 14 lõike 2) muudatuse üheks põhjuseks märgitud, et selle eelnõu „koostamise käigus kaaluti, kas oleks põhjendatud loobuda ka konkreetse füüsilise isiku tuvastamise nõudest. Kuigi kõneolev eelnõu sellist muudatust ette ei näe, ei ole sellise muudatuse tegemine tulevikus välistatud (seda eeskätt tegevusetusdeliktide korral)".

Inspektsioon pooldas mõtet, et tuleks analüüsida selle olukorra muutmist. Hetkel on vajalik juriidilise isiku vastutusele võtmise puhul tuvastada teo toime pannud füüsilise isiku käitumine (kelle tegevust juriidilisele isikule omistatakse) on koosseisupärane, õigusvastane ja süüline. Andmekaitsealaste nõuete rakendamata jätmine võib olla tingitud segastest, sageli peidetud vastutusest ning olukorrast, kus isikuandmete töötleja tegevusetuse tulemusena toimus andmekaitsealane rikkumine. Kui loobutakse konkreetse füüsilise isiku tuvastamise nõudest, siis selle muudatuse tulemusena ei oleks juriidilisest isikust isikuandmete töötlejal võimalik vältida vastutuse kandmist, kui ta on mingi rikkumisega hakkama saanud. Sama olukord on ilmselt ka finantssektoris ning konkurentsialastes olukordades.

Kavandatava KarS § 471 (kõrgendatud ülemmääraga rahatrahv) osas juhtis inspektsioon tähelepanu võimalikele selgusetustele, et kuidas tuleks trahvi määramisel arvutada protsendipõhist käivet. Eelnõu seletuskirjast puudusid selgitused, kuidas andmekaitsealaste väärtegude puhul toimuks väärteotrahvi suuruse arvutamine. Seetõttu märkis inspektsioon oma tagasisides, et andmekaitsenõukogu eelkäija, direktiivi 95/46/EÜ artikli 29 alusel asutatud andmekaitseasutustest koosnev töörühm võttis 07.10.2017 vastu suunised IKÜM kohaste trahvide kohaldamise ja määramise kohta[12].

Inspektsioon juhtis tähelepanu, et ehk oleks kõrgendatud ülemmääraga rahatrahvide sätte lisandumisega vajadus täiendada ka KarS §-i 47. Nimelt on selle paragrahvi lõike 1 kohaselt

[9] https://www.aki.ee/et/teavitus-uudised/andmekaitse-reform

[10] Sellele eelnõule antud tagasiside leitav: https://adr.rik.ee/aki/dokument/6595123

[11] https://adr.rik.ee/aki/dokument/6595123

[12] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

lubatud kohtuvälisel menetlejal füüsilisele isikule määrata väärteo eest rahatrahvi trahviühikutena. Kui muudatusi ei tehta, siis võib tekkida oht, et kõrgendatud ülemmääraga väärteo eest määratud rahatrahvi hakatakse vaidlustama, kuna KarS § 47 lg 1 ütleb selgelt, et väärteomenetluses on võimalik füüsilisele isikule määrata rahatrahvi trahviühikutes. Sisuliselt on oht, et need sätted on omavahel vastuolus.

Justiitsministeeriumi tähelepanu oli vaja juhtida ka kõrgendatud ülemmääraga väärteo aegumise ja aegumise katkemisega seotud probleemidele. Ennekõike on probleemiks, et kaheaastase väärteomenetluse aegumise tähtaja jooksul ei ole praktiliselt võimalik süüdlast väärteokorras vastutusele võtta.

Algses eelnõus ei olnud ühtegi muudatust selle kohta, et andmekaitsealaste rikkumiste puhul oleks pikem väärtegude aegumistähtaeg. Kui arvestada ka arvamuse avaldamiseks esitatud eelnõu muudatusi, siis KarS § 81 lõigete 3 ja lõike 42 teise lause (neid kumbagi ei muudeta) koosmõju tulemusena on võimalik kõrgendatud ülemmääraga väärtegude korral süüdlast väärteokorras vastutusele võtta nelja aasta jooksul teo toime panemisest. Ning sedagi ainult siis, kui kohtuvälise menetleja otsus vaidlustatakse kohtus. See on praktikas keerukas ja vahel võib-olla isegi võimatu, sest tihti viiakse esmalt läbi riiklik- või haldusjärelevalvemenetluse ning alles seejärel väärteomenetlus.

Mõlemale menetlusele kuluv aeg, lisaks võimalikud kohtumenetlused, ei võimalda etteantud ajaraamis hakkama saada. Olukorda ilmestamaks tõime näite Uber'i andmelekke kohta, mis toimus oktoobris 2016, kui häkkerid said ligi Uber'is hoitud isikuandmetele ja millest teavitati alles novembris 2017 Hollandi järelevalveasutust, kes kaasas ka teisi EL-i andmekaitse järelevalveasutusi uurimistegevusse. Menetlus lõppes novembris 2018, mil Uberile tehti haldustrahv[13].

Kui Uberi näide tuua Eesti konteksti, siis ei ole välistatud, et ka inspektsioonil võib suuremahulise (sh piiriülese mõõtmega) rikkumise uurimine võtta aasta või enamgi. Seega viidaks esmalt uurimine juriidiliste isikute osas läbi korrakaitseseaduse alusel ehk toimub riiklik järelevalvemenetlus. Kui selguks, et esineb alus väärteomenetluse alustamiseks (IKS 6. peatüki järgi), siis väärteo kaheaastase aegumistähtaja jooksul ei ole seda praktikas suure tõenäosusega võimalik läbi viia, arvestades võimalikke menetluste venitamisi jms-st. Paraku ei ole abi ka KarS § 81 lg 7 punktist 1 ning lg 8, kuna nende koosmõju tulemusena on inspektsioonil kui kohtuvälisel menetlejal aega ikkagi maksimaalselt 3 aastat menetluse läbiviimiseks. Kas ning kuivõrd see muudatus aitab inspektsioonis läbi viidavaid väärteomenetlusi, selgub mõne aja pärast, kui on rohkem praktikat. Riigikogus arutlusel olnud eelnõu (94 SE) kohaselt tehakse muudatusi ka IKS-s, mille tulemusena oleksid IKS-is toodud väärtegude aegumistähtajaks kolm aastat.

> Inspektsioon esitas 2019. aasta detsembris koos teiste Eesti riigiasutustega ühise seisukoha ka Riigikogu põhiseaduskomisjonile, kus ühiselt leiti, et väärtegude eest karistamise ebaefektiivne kord on kujunenud tõsiseks takistuseks ülesannete tulemuslikul täitmisel. Ühiselt rõhutati ka mõningaid olulisemaid väärteomenetlusega seotud probleeme ning selgitati, et nende probleemide lahendamiseks ei piisa väärteomenetluse seadustiku ja karistusseadustiku üldosa muudatustest, vaid otstarbekas on välja töötada siseriiklik haldus-karistuste rakendamist võimaldav õiguslik regulatsioon ning kohandada selleks haldusmenetluse norme.

[13] Täpsemalt vt siit: https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fine-data-breach-uber

Siseministri määruse „Dokumendi taotleja isiku tuvastamise ja isikusamasuse kontrollimise kord“ muutmise eelnõu[14]

Määruse muutmise eelnõu kohaselt sooviti anda mobiiloperaatoritele (MO) üle avalik ülesanne – kontrollida isikusamasust mobiil-ID lepingu sõlmimise käigus (eelnõu seletuskiri lk 2).

Kontrollimist teostatakse teatavate isikut tõendavate dokumentide ja andmete alusel, mis on kantud isikut tõendavate dokumentide andmekogusse ehk ITDAK-i (kavandatud § 31 lg 1).

Inspektsioon leidis, et kuna selle ülesande üleandmisega muutub MO oma olemuselt volitatud töötlejaks, siis on vajalik, et selle ülesandega seotud õigused ja kohustused reguleeritakse ka vastavalt ehk sisustatakse IKÜM artiklis 28 toodud nõuetega. Kuna neid nõudeid ei olnud esitatud eelnõus täiel määral sisustatud, siis inspektsioon võttis esitatud seisukohas eelduseks, et need õigused ja kohustused lisatakse MO ja Politsei- ja Piirivalveameti vahel sõlmitavasse halduslepingusse.

Eelnõus oli vaja tähelepanu juhtida sellele, et kehtiv isikut tõendavate dokumentide andmekogu pidamise põhimääruse § 16 reguleerib ITDAK-le juurdepääsu. Sinna kantud andmed on juurdepääsupiiranguga ning tunnistatud asutusesiseseks kasutamiseks.

> Inspektsioon väljendas seisukohta, et siseministeerium peab üle hindama kogutavate andmete säilitamise tähtaja. Kahetsusväärselt seda ei tehtud ning neid andmeid tuleb hoida 10 aastat.

Selle siseminstri määruse muutmise eelnõus ei saanud inspektsioon aru, mis on see seadusest tulenev ülesanne MO-de osas enne kavandatava eelnõu jõustumist – seletuskirja kohaselt oli juba enne eelnõu jõustumist MO-del juurdepääs ITDAK-sse kantud andmetele. Samas, inspektsioonil puudus teadmine, et MO-del oleks sedasorti seadusest tulenevat alust (ülesannet), mis õigustaks ITDAK-le juurdepääsu. Jah, selline õigustus tekkis kõnealuse eelnõuga ainult mobiil-ID osas, kuid muus osas jäi see õigustus selgusetuks.

> Põhimääruse § 16 lg 5 sõnastus tekitas küsimusi: „Andmekogu vastutav töötleja otsustab kolmandatele isikutele infosüsteemide andmevahetuskihi kaudu andmetele juurdepääsu andmise selleks seadusest tuleneva aluse olemasolul ning kooskõlas avaliku teabe seaduse ja isikuandmete kaitse seadusega. Vajaduse korral sõlmitakse andmesaajaga leping, kus sätestatakse nende andmete koosseis, millele võimaldatakse juurdepääs ning andmetele juurdepääsu andmise õiguslik alus, eesmärk, tingimused, kord ja viis.“

Eelnõu kohaselt olevat MO-l võimalus (mitte kohustus) kasutada isiku tuvastamiseks infotehnoloogilist lahendust (kavandatav § 31 lg 2). Sellele viitab ka sama paragrahvi lõige 3 – tegemist on teise alternatiivsete isiku tuvastamise võimalustega. Kavandatud § 32 sisustab, kuidas infotehnoloogilist lahendust kasutatakse isiku tuvastamiseks (inimeselt võetakse reaalajas näokujutis (biomeetrilised andmed) ning seda võrreldakse ITDAK-is asuva näokujutisega).

Eelnõu § 32 lõike 3 kohaselt peavad sama paragrahvi lõikes 2 märgitud andmeid sisaldavad salvestised olema taasesitatavad kümne aasta jooksul pärast mobiil-ID vormis digitaalse isikutunnistuse kasutamise lepingu sõlmimist. Samas ei selgitanud ega põhjendanud eelnõu seletuskiri, miks on vajalik neid andmeid 10 aastat hoida? Inspektsioon leidis, et säilitamise tähtaeg on ebamõistli-

[14] Sellele eelnõule antud tagasiside leitav: https://adr.rik.ee/aki/dokument/6267913

kult pikk. Seda enam, kui arvestada, et isikut tõendavate dokumentide seaduse § 203 lg 2 kohaselt antakse mobiil-ID vormis digitaalne isikutunnistus välja kehtivusajaga kuni viis aastat. Inspektsioon väljendas seisukohta, et siseministeerium peab üle hindama kogutavate andmete säilitamise tähtaja. Kahetsusväärselt seda ei tehtud ning neid andmeid tuleb hoida 10 aastat.

Miks on vajalik neid andmeid 10 aastat hoida?

Selle eelnõu koostamisel ei olnud läbi viidud ka andmekaitsealast mõjuhinnangut – sellekohane kohustus on suunatud MO-dele. Kuna tegemist on isikuandmete juurdepääsu võimaldamisega eraettevõttele olukorras, kus riik on andmeid kohustuslikus korras kogunud, oleks pidanud eelnõus esitatud mingigi osa sellest mõjuhinnangust. Kuna MO-d hakkavad biomeetrilisi andmeid saama IDTAK-ist, siis selle andmekogu vastutav töötleja ehk Politsei- ja Piirivalveamet peab olema veendunud, et ta väljastab andmeid õigustatud isikutele minimaalses vajalikus mahus ning kindlaks määratud eesmärgil. Õigusaktil on suur mõju, sest isikutunnistuse kohustus on sisuliselt kõigil Eesti kodanikel (v.a. alla 15-aastastel lastel).

Eelnõu seletuskirja (lk 3-4, kavandatava § 31 lõike 4 osas) oli märgitud mõningad tulevikuvisioonid, kuidas mobiil-ID väljastamise protsess võiks välja näha[15]. Kuna sellekohaseid muudatusi ei tehtud kõnealuses eelnõus, siis sel teemal eraldi seisukohta inspektsioon ei esitanud. Siiski sai eelnõu koostaja soovituse selliste plaanide puhul läbi analüüsida ja ette mõelda, kuivõrd võib isikuandmete töötlemise protsess mõjuda inimese privaatsusele – ehk tuleb läbi viia kohustuslik andmekaitsealane mõjuhinnang.

Keskkonnaministri määruse „Täiselektriliste sõidukite ostutoetuse andmise tingimused ja kord“ eelnõu[16]

Selle määrusega sooviti kehtestada toetuse andmise tingimused elektrisõidukite soetamiseks. Eelnõu koostamiseks polnud analüüsitud mõju andmesubjektidele ning vastamata olid olulised küsimused:

- ❒ Mis teavet taotleja (sh füüsilisest isikust taotleja) kohta kogutakse?
- ❒ Kuidas tagatakse, et GPS ei edasta KIK-le elektrisõiduki asukohaandmeid, sh kui täpset teavet üldse edastatakse?

Eelnõu § 8 lg 1 järgi peab taotleja esitama oma taotluse e-toetuste keskkonnas täidetud taotlusvormil, millele on lisatud ka teatavad dokumendid (nt elektrisõiduki müügipakkumine, koopia elektrisõiduki EÜ tüübikinnitustunnistusest jne). Kõik taotlusvormi lahtrid peavad olema korrektselt täidetud (eelnõu § 8 lg 2 p 1). Samas ei olnud eelnõust selgelt aru saada ega võimalik ette näha, mis teavet taotleja (sh füüsilisest isikust taotleja) kohta kogutakse. Lisaks on ka võimalus, et (füüsilisest isikust) taotleja kohta kogutakse või nõutakse lisateavet (eelnõu § 10 lg 8), kuid jääb selgusetuks, mis teabega võib olla tegemist. Seetõttu ei olnud võimalik ka anda hinnangut, kas isikuandmete kogumisel lähtutakse IKÜM artikli 5 lg 1 punktis c olevast võimalikult väheste andmete kogumise põhimõttest: isikuandmed on asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt.

Eelnõu § 10 lg 2 teise lausega[17] seonduvalt juhtis inspektsioon tähelepanu haldusmenetluse seaduse 27 lg 2 punktile 1, mille järgi loetakse elektrooniliselt kättesaadavaks tehtud

[15] Selle korra järgi tuvastatakse inimese isikusamasus MO juures ning selle järel peab inimene lisaks sisse logima ja autentima end vastavas Politsei- ja Piirivalveameti taotluskeskkonnas; tuleviku plaanide kohaselt soovitakse, et MO-d kontrolliksid mobiil-ID lepingu sõlmija kui ka dokumendi taotleja isikusamasust.

[16] Sellele eelnõule antud tagasiside leitav: https://adr.rik.ee/aki/dokument/6768630

[17] Eelnõus kavandatud lause: „E-toetuse keskkonna kaudu edastatud dokumendid loetakse taotlejale ja toetuse saajale kätte toimetatuks.“. Eelnõu koostaja seda lauset ei muutnud.

või edastatud dokument kättetoimetatuks, kui asjakohane infosüsteem on registreerinud dokumendi avamise või vastuvõtmise. Selle järgi ei ole dokument kätte toimetatud, kui see on saadetud infosüsteemi. Seletuskirja kohaselt andis taotleja küll selle kohta nõusoleku ning ka enda e-posti aadressi, kuid seletuskirjast ei selgunud, mida see nõusolek endast sisaldab, sh kas ning kuivõrd on kohaldatavad IKÜM artikli 4 punktist 11 ja artiklist 7 tulenevad nõusoleku nõuded (füüsilisest isikust taotleja korral).

Eelnõu § 15 lg 3 p 1 järgi tuleb maksetaotlusele lisada ka elektrisõiduki müügi- või liisinguleping. Samas võivad need lepingud sisaldada ka muud teavet, mis ei ole vajalik toetuse maksmise kontrollimiseks. Seetõttu inspektsioon soovitas üle hinnata, kas ikka on vaja kogu lepingut või mingit osa/väljavõtet või kinnitust selle kohta. Kahjuks eelnõu vastu võtmisel siin muudatusi ei tehtud.

Kui tegemist on eraisikule mineva elektrisõidukiga, siis eelduslikult kantakse registreerimistunnistusele ka muid isikuid (ennekõike pereliikmeid), kes ka kasutaksid seda sõidukit. Inspektsioonile jäi arusaamatuks, kas seda teavet oleks Keskkonnainvesteeringute Keskusele (KIK) üldse vaja – eelduslikult mitte. Eeltooduga sarnane olukord on ilmselt ka kaskokindlustuse lepingu puhul, mille sõlmimine on kohustuslik eelnõu järgi. Eelduslikult ei ole ka selle puhul KIK-l kogu teavet vaja, eriti kui arvestada eelnõu § 16 lõike 13 nõudeid[18].

[18] Selle lõike sisu on vastu võetud määruse § 16 lõike 15 sisu: „Toetuse saaja kohustub kindlustama elektrisõiduki kaskokindlustusega hiljemalt elektrisõiduki valduse toetuse saajale ülemineku ajaks. Elektrisõiduki ostmisel on toetuse saaja kohustatud kindlustuslepingus sätestama tingimuse, mille kohaselt on elektrisõiduki hävimise, röövimise või varguse korral soodustatud isikuks KIK viie tuhande euro ulatuses. Liisingu puhul on toetuse saaja kohustatud liisingulepingus sätestama tingimuse, mille kohaselt kindlustusjuhtumi toimumise korral tasutakse kindlustushüvitis liisinguandjale, kes kannab juhul, kui kindlustushüvitis on suurem kui liisinguvõtja (toetuse saaja) elektrisõiduki liisingulepingust tulenev kohustuste jääk liisinguandja ees, liisingukohustuste kustutamisest ülejääva kindlustushüvitise viie tuhande euro ulatuses KIKile."

> Eelnõu § 15 lg 3 p 5 kohaselt tuleb maksetaotlusele lisada ka elektrisõiduki registreerimistunnistuse koopia, millest nähtub, et toetuse saaja on elektrisõiduki omanik või vastutav kasutaja.

Samas seletuskirjast ei selgunud, kuidas tagatakse, et GPS ei edasta KIK-le elektrisõiduki asukohaandmeid, sh kui täpset teavet üldse edastatakse. Seletuskirja mõjude osas ei oldud pikemalt analüüsitud mõjusid andmesubjektidele (füüsilistele isikuteke) ehk teostatud andmekaitsealast mõjuhinnangut IKÜM artikli 35 mõistes. Seetõttu eeldas inspektsioon, et see tehakse eraldiseisvalt enne sellekohaste isikuandmete töötlemise algust.

> Eelnõu § 13 lg 3 punkti 8 järgi kantakse taotluse rahuldamise otsusele mh ka iga-aastase kilometraaži KIK-le esitamise aeg või GPS-seadme tasuta paigaldamise võimalus. Seletuskirja kohaselt GPS paigaldatakse siis, kui taotleja sellega nõustub. Eelnõu seletuskirjas (lk 9) on öeldud: „GPS-seadmest tuleb KIK-le teave ainult läbitud kilomeetrite kohta ja väljaspool Eestit läbitud kilomeetrite kohta. Kus täpselt ja millal auto liigub, selle jälgimise teenust KIK ei hangi, seda keegi jälgida ei tohi. Andmete töötlemisel täidetakse IKS-s, selle rakendusaktides ja Euroopa Liidu IKÜM (EL 2016/679) sätestatud nõudeid."

Siseministri määruse „Riigipiiri valvamise korraldamise andmekogu põhimäärus“ muutmise eelnõu[19]

Eelnõu muudatuste peamiseks põhjuseks oli viia andmekogu põhimäärus kooskõlla Politsei- ja Piirivalveseaduse sätetega, mis reguleerivad selle andmekogu pidamist.

- ❒ Miks peaks kõigi teadete ja sündmuste kohta esitama neid kõiki andmeid, sh biomeetriat?
- ❒ Mis on selle teabe säilitamistähtajaks?

Eelnõu punktiga 4 täiendati andmekogu põhimäärust nii, et füüsilise isiku kohta kantakse kõik andmekogu põhimääruse § 5 lõikes 3 toodud andmed (nt ees- ja perekonnanimi, isanimi, isikukood, sugu, elukoht, dokumendi andmed, sidevahendi ja e-posti andmed, foto jne). Seletuskirja kohaselt lisatakse isiku kohta uute andmekategooriatena ainult seose liik ja põhjus, kuid tegelikkuses see nii ei olnud. Eelnõu muudatuse tulemusena lisatakse andmekogusse kõik § 5 lõikes 3 toodud andmed. Inspektsiooni jaoks ei tulnud seletuskirjast selgelt välja, miks peaks kõigi teadete ja sündmuste kohta esitama neid kõiki andmeid, sh biomeetriat?

> Tuleb teostada ka kohane andmekaitsealaste mõjude hindamine.

Eelnõust ja selle seletuskirjast ilmnes, et andmekogusse soovitakse kanda ka andmeid, mis on juba politsei infosüsteemis[20]. Avaliku teabe seaduse (AvTS) § 433 lõike 2 kohaselt on keelatud asutada ühtede ja samade andmete kogumiseks eraldi andmekogusid. Kuna eelnõust ei selgunud, mis saab politsei infosüsteemi kantud (eelduslikult dubleerivatest) andmetest, siis soovitas inspektsioon see aspekt eelnevalt läbi mõelda. Kui tegemist on dubleerimisega, siis tuleks esitada seletuskirjas põhjendused, miks neid andmeid dubleeritakse. Kui neid andmeid ei dubleerita, vaid need kantakse üle politsei infosüsteemist, siis tuleb ka vastavad selgitused esitada, sh selgitada, mis saab politsei infosüsteemi kantud andmetest.

Seletuskirja kohaselt on mõju andmesubjektile väike, sest andmetöötluse põhimõtteid eelnõuga ei muudeta. Samas jäeti tähelepanuta asjaolu, et eelnõu punkti 4 tulemusena lisatakse andmesubjekti kohta rohkem teavet, sh ka biomeetriat (vt eelpool toodud sisu). Eelnõu seletuskirjas puudus selle kohta analüüs. Seetõttu leidis inspektsioon, et tuleb teostada ka kohane andmekaitsealaste mõjude hindamine.

Inspektsioon viitas ka varasemalt sama andmekogu põhimäärusega seotud märkustele, mida selle eelnõuga ei olnud ära lahendatud. Ennekõike oli tolles seisukohas toodud probleemiks selgusetus, mis teavet siis sellesse andmekogusse kogutakse ning mis on selle teabe säilitamistähtajaks.

Määrusesesse „Tervise infosüsteemi edastatavate dokumentide andmekoosseisud ning nende esitamise tingimused ja kord“

Määrusesse sooviti lisada määruse § 5 lõikesse 10, et nakkushaiguse kahtluse teatisi, nakkushaiguse teatisi ja HIV teatisi esitavad tervishoiuteenuse osutajad. Inspektsioonil tuli juhtida tähelepanu, et sisuliselt samu teatisi peab edastama ka Eesti Kohtuekspertiisi Instituut, kes ei ole tervishoiuteenuse osutaja. Selle määruse juures oli ka kolm eraldi lisa, mis sooviti uuesti kehtestada (need sisustasid nakkushaiguse kahtluse teatise, nakkushaiguse teatise ning HIV teatise andmekoosseisusid). Kõigis kolmes lisas on märgitud, et kogutakse ka patsiendi sünniaega, kuigi seda ei olnud tol hetkel kehtinud seadusandlusega võrreldes varasemalt kogutud. Samas ei olnud inspektsioonile selge, miks seda on vaja koguda, kui juba on andmete hulka arvatud isikukood ja

[19] Sellele eelnõule antud tagasiside leitav: https://adr.rik.ee/aki/dokument/6873647

[20] Lisandunud § 4 lõige 51: Andmekogusse kantakse reageeriva ressursi planeerimisele ja haldamisele ning riigipiiri valvamisele ja piirirežiimi tagamisele kaasatava eritehnika ja abiressursi kohta järgmised andmed: 1) liik; 2) teenuse osutaja nimi ja tema kontaktandmed (telefoninumber ja e-posti aadress).

vanus. Seetõttu soovitas inspektsioon üle hinnata, kas siin võib tegemist olla topelt andmete kogumisega, mis on keelatud. Samuti jäi HIV teatise puhul selgusetuks, kas ning mis põhjusel on vajalik koguda teavet patsiendi rahvuse kohta.

Eelnõuga oli mh ka koostatud teatavas osas andmekaitsealane mõjuhinnang. Samas ei nähtunud mõjuhinnangust, kas ning milliseid ohte on nähtud sellega, et edaspidiselt tervishoiuteenuse osutaja ei edasta eelnevalt mainitud teatisi otse Terviseametile, vaid seda tehakse läbi tervise infosüsteemi. Terviseamet kannab saadud teatised nakkushaiguste registrisse, millele juurdepääs on sama andmekogu põhimääruse kohaselt vägagi piiratud isikute ringil.

Terve lause: Eelnõu taotlus oli laiendada nende isikute ringi, kes eelnõu eelse korra järgi sedasorti informatsioonile juurdepääsu ei omanud. Andmekaitsealasest mõjuhinnangust ei nähtunud, kas ning mil määral on see risk andmesubjektile ning mis meetmeid tuleks võtta nende riskide maandamiseks, arvestades, et juurdepääsu sätte sõnastust nakkushaiguste registri põhimääruses tehakse üldisemaks.

Eelnõuga sooviti muuta nakkushaiguste registri juurdepääsu nõude sõnastust üldisemaks. Sama eelnõu muudatuse kaasabil tekib sama andmestik ka tervise infosüsteemi ning sellele andmestikule on juurdepääs ka teistel tervishoiuteenuse osutajatel, kes ei ole eelnevalt mainitud teateid esitanud (nakkushaiguste registri põhimääruse §-s 11 on loetletud, kellel on juurdepääs selle andmekogu andmetele; kuigi seda muudetakse sama eelnõuga, jääb selle paragrahvi lõike 1 sõnastus samaks).

Inspektsioon märkis veel üldise tähelepanekuna, et IKÜM art 9 lõikest 3 tuleb nõue, et kui eriliigilisi isikuandmeid töödeldakse sama artikli lõike 2 punkti h eesmärkidel[21] , siis peab sellel andmetöötleja töötajal olema liidu või liikmesriigi õigusest või pädevate riiklike asutuste kehtestatud eeskirjade alusel ametisaladuse hoidmise kohustus[22]. Ka sellisel juhul, kui eriliigilisi isikuandmeid töödeldakse IKÜM art 9 lg 2 punktis i toodud eesmärgil, on vajalik, et oleks olemas õigusaktist tulenev ametisaladuse hoidmise kohustus. Kuna muudatuse tulemusena jäetakse juurdepääs nakkushaiguste registrile üldisemaks, siis peab olema tagatud, et isikutele, kes sellele infole juurdepääsu saavad, kehtib seadusest tulenev saladuse hoidmise kohustus.

Valitsuse määruse „Tervise infosüsteemi põhimäärus“ muutmise eelnõu[23]

Eelnõu on vägagi seotud eelnevalt välja toodud ministrite määruste muutmise eelnõuga. Tervishoiuteenuse osutaja jt isikud hakkaks edaspidi edastama tervise infosüsteemi ka nakkushaiguse kahtluse, nakkushaiguse ja HIV teatisi.

Eelnõuga oli mh ka koostatud teatavas osas andmekaitsealane mõjuhinnang. Samas ei nähtunud mõjuhinnangust, kas ning milliseid ohte on nähtud sellega, et edaspidi ei edasta tervishoiuteenuse osutaja eelnevalt mainitud teatisi otse Terviseametile, vaid teeb seda läbi tervise infosüsteemi. Varasemalt kandis Terviseamet saadud teatised nakkushaiguste registrisse, millele juurdepääs on sama andmekogu tol hetkel

[21] Andmetöötlus on vajalik ennetava meditsiini või töömeditsiiniga seotud põhjustel, töötaja töövõime hindamiseks, meditsiinilise diagnoosi panemiseks, tervishoiuteenuste või sotsiaalhoolekande või ravi võimaldamiseks või tervishoiu- või sotsiaalhoolekandesüsteemi ja -teenuste korraldamiseks.

[22] Andmete töötlemine on vajalik rahvatervise valdkonna avalikes huvides, nagu kaitse suure piiriülese terviseohu korral või kõrgete kvaliteedi- ja ohutusnõuete tagamine tervishoiu ning ravimite või meditsiiniseadmete puhul, tuginedes liidu või liikmesriigi õigusele, millega nähakse ette sobivad ja konkreetsed meetmed andmesubjekti õiguste ja vabaduste kaitseks, eelkõige ametisaladuse hoidmine (isikuandmete kaitse üldmääruse art 9 lg 2 punkt i)

[23] Sellele eelnõule antud tagasiside leitav: https://adr.rik.ee/aki/dokument/6908786

kehtinud põhimääruse kohaselt vägagi piiratud isikute ringil (kuigi ka ülalpool märgitud ministrite määruste muutmise eelnõu tõttu sooviti seda juurdepääsuõiguse käsitlust muuta üldisemaks).

Arvamuse avaldamiseks esitatud eelnõu muudatuse tulemusena tekib sama andmestik ka tervise infosüsteemi ning sellele on juurdepääs ka teistel tervishoiuteenuse osutajatel, kes ei ole eelnevalt mainitud teateid esitanud (nakkushaiguste registri põhimääruse §-s 11 on loetletud, kellel on juurdepääs selle andmekogu andmetele; kuigi seda muudeti teise eelnõuga, jäi selle paragrahvi lg 1 sõnastus samaks – vt selgitust eelpool). Andmekaitsealasest mõjuhinnangust ei nähtunud, kas ning mil määral on see risk andmesubjektile ning mis meetmeid tuleks võtta nende riskide maandamiseks.

Lisaks tuli inspektsioonil märkida eelnõu väliselt, et eeltooduga (kellel on juurdepääs tervise infosüsteemi kantud andmetele) on seotud ka IKÜM art 9 lõike 3 nõue, et kui eriliigilisi isikuandmeid töödeldakse sama artikli lg 2 punkti h eesmärkidel, siis peab sellel andmetöötleja olema liidu või liikmesriigi õigusest või pädevate riiklike asutuste kehtestatud eeskirjade alusel ametisaladuse hoidmise kohustus. Ka juhul, kui eriliigilisi isikuandmeid töödeldakse IKÜM art 9 lg 2 punktis i toodud eesmärgil on vajalik, et oleks olemas õigusaktist tulenev ametisaladuse hoidmise kohustus. Tervishoiuteenuste korraldamise seaduse (TTKS) § 593 lg 21 on märgitud, millistel tervishoiuteenusel osalevatel isikutel on veel juurdepääs tervise infosüsteemile tervishoiuteenusel osalemiseks[24].

Samas ei ole eelduslikult kõigil neist seadusest tulenevat saladuse hoidmise kohustust. Probleem võib tekkida ka siis, kui andmesubjekt annab juurdepääsu enda isikuandmetele enda nõusolekul (vt tervise infosüsteemi põhimääruse § 20) ning see juurdepääs on seotud nt ravi osutamisega.

Tervise infosüsteem ei pruugi olla õige koht, kuhu õpilase, lõpetatud haridustaseme ja õppeasutuse andmed tuleks kanda. Inspektsioon kordas varem esitatud seisukohta. Tervise infosüsteemi põhimääruse § 14 lg 3 kohaselt avalikustatakse tervise infosüsteemi andmelao avaandmed sama põhimääruse § 3 lg 2 nimetatud volitatud töötleja veebilehel masinloetaval kujul. AvTS § 29 lg 6 kohaselt peavad andmekogude avaandmed olema juurdepääsetavad Eesti teabevärava ehk praktikas Eesti Avaandmete Portaali (opendata.riik.ee) kaudu.

Tervise infosüsteemi põhimääruse § 6 lg 81 kohaselt on tervise infosüsteemi üheks andmeandjaks ka Haridus-ja Teadusministeerium. Selle järgi võidakse edastatada tervise infosüsteemi ka õpilase andmed, lõpetatud haridustaseme andmed ja õppeasutuse andmed.

[24] Juurdepääs on: 1) arstiõppe üliõpilasel, kes on läbinud õppekavas olevad 4. kursuse kohustuslikud ained; 2) füsioterapeudil; 3) tegevusterapeudil; 4) kliinilisel logopeedil; 5) kliinilisel psühholoogil; 6) optometristil; 7) radioloogia tehnikul; 8) tervishoiuteenuste korraldamise seaduse § 30 lõikes 32 toodud isikutel ehk isikul, kelle on tööpraktikale suunanud TÜ või tervishoiukõrgkool.