ANDMEKAITSE INSPEKTSIOON

# AVALIKU TEABE SEADUSE TÄITMISEST JA ISIKUANDMETE KAITSE TAGAMISEST AASTAL 2020


ANDMEKAITSE INSPEKTSIOONI AASTARAAMAT

ANDMEKAITSE INSPEKTSIOON

# AVALIKU TEABE SEADUSE TÄITMISEST JA ISIKUANDMETE KAITSE TAGAMISEST AASTAL 2020

ANDMEKAITSE INSPEKTSIOONI AASTARAAMAT

Aitäh panuse eest aastaraamatusse

Pille Lehis, peadirektor
Maris Juha, järelevalve juht
Urmo Parm, tehnoloogia nõunik
Maarja Kirss, väliskoostöö nõunik
Liisa Ojangu, õigusnõunik
Elve Adamson, jurist
Sirje Biin, jurist
Raiko Kaur, jurist
Mehis Lõhmus, jurist
Kadri Levand, jurist
Ingrid Lauringson, jurist
Sirgo Saar, jurist
Signe Kerge, jurist
Helve Juusu, tugiteenuse haldur
Triin Kask, juhiabi

Toimetaja Signe Heiberg, avalike suhete nõunik
Küljendus ja illustratsioonid Kustas Budrikas
Algupärased fotod: pixabay.com
Print ja köide Koopia Niini & Rauam

Andmekaitse Inspektsioon 2021
Tatari 39, Tallinn

# Sisukord

# AASTA MÄRKSÕNAD

2020. aasta ei toonud suuri muutusi andmekaitsesse, kuid esile kerkis terviseandmete töötlemise teema, millele andis tõuke koroonapandeemia. Inspektsiooni juristid on aastaraamatusse välja noppinud olulisemad või enam päevakorras olnud küsimused koroonapandeemia ajal. Samuti andis koroonapandeemia hoogu mitmetele õigusloomelistele muudatustele, mille kohta inspektsiooniltki arvamust küsiti. Mõnede puhul oli märgata kiirustamist ja läbimõtlematust, ent eks tuleb ka mõista olukorda, milles me kõik sel hetkel olime.

Lisaks on üks huvipakkuvamaid teemasid vahekokkuvõte juba mitu aastat kestnud majandusinfoportaalide seirest. Inspektsiooni vaatest on see kindlasti tähelepanuväärne teema, sest põrkuvad ju siin ühiskonna sõnavabadus ja inimese õigus privaatsusele. Kuid vahekokkuvõte on kõigest üks peatus kogu protsessis ning tegevus sellel suunal jätkub, et inimeste andmete kogumine ja avalikustamine saaks olema läbipaistev ning vastaks nõuetele.

Selles aastaraamatus käsitleb inspektsioon ühte seni üsna vähetuntud õigust, mis on vastulause esitamine. Võib arvata, et andmekaitse saab ühiskonnas tugevaks alles siis, kui inimesed on teadlikud oma õigustest.
Kui hästi tunneb end aga Eesti avalik sektor inimeste privaatsuse kaitsel ja ka teabe kättesaadavaks tegemisel? Mitte väga enesekindlalt, aga iga aastaga on üldpilt jälle veidike parem. Möödunud aastasse jääb inspektsiooni kohalike omavalitsuste veebilehtede ja dokumendiregistrite seire, mille tulemustest saab pikemalt lugeda inspektsiooni veebiküljelt, kuid üldiseid tähelepanekuid kogu avaliku sektori problemaatikast leiab ka aastaraamatu lehekülgedelt.

Ühe suurema teemana jääb möödunud aastasse küsimus sellest, kas ja millal on õigus saada juurdepääs asutuse sisedokumentatsioonile. Küsimus tõstatus tänu avalikkuse kasvanud huvile keskkonnateemade vastu ja inspektsiooni sekkumine lõppes asutuse pakendikomisjoni protokollide väljastamisega teabenõudjale. Samuti selgines, kust maalt alates ei ole teave kavandijärgus ja on saanud valmisdokumendiks olenemata millisel kandjal see on. Digiajastul, mil teave pole enam ammugi vaid paberikandjal, oli vajalik luua õigusselgust ka avaliku teabe saamise õigusele mistahes muudel infokandjatel, milleks sageli on näiteks infosüsteemid.

2020. aasta oli väga viljakas ka õigusloomeliselt. Milliste eelnõude osas inspektsiooni arvamust oluliseks peeti ning millised just inspektsiooni vaatest tähelepanu väärivad, saab lugeda rubriigist õigusloome. Kuna väga paljud eelnõud puudutavad just andmekogudega seonduvat, siis oleme sealsamas teinud ka tagasivaate andmekogude kooskõlastusmenetlusele Riigi Infosüsteemi Haldussüsteemis RIHA. Seaduste ja põhimääruste eelnõudest, mis puudutavad erinevaid andmekogusid jäi peamiselt silma riigi soov koguda üha enam andmeid. Kogu maailm on liikumas üha enam andmepõhiseks - räägitakse, et targad otsused just andmetel peaksidki tuginema. Seetõttu ei ole selline riigi soov üllatav, samuti ei pea selles mingit hoiatust nägema. Küll aga on inspektsiooni kohus seejuures pidevalt meelde tuletada, et kogumise tuhinas endalt ikka küsitaks – kui palju, mis eesmärgil ja kui kauaks. Just neid küsimusi tuli andmetöötlejatele möödunud aastal üsna tihti meelde tuletada.

Ehkki kohtumenetlus jäi 2020. aastal tagasihoidlikumaks oma jõustunud lahendite poolest, selgus sealtki uut teadmist või saadi senisele kinnitust. Mitmed inspektsiooni jaoks olulised küsimused aga on veel ootel, et meie kohtute seisukohti saada. Kohtumenetlus ei ole küll tihti pooltele meeldiv ega ka kiire viis lahendusteni jõudmiseks, kuid aeg-ajalt paratamatult vajalik elu osa, et teatud olulistes küsimustes kindlustunne saavutada. Seetõttu on inspektsioon põnevil ja järgnevate lahendite ootel.

2020. aastasse jääb maha ka Eestit kui e- riiki raputanud sündmus. Oleme ju harjunud nägema riiki kui teadlikku andmetöötlejat, kelle kätte võib oma isikuandmed teenuste saamiseks usaldada, aga nüüd sattus ka riik ise küberrünnaku ohvriks.

Kurioossust lisab toimunule asjaolu, et rünnati ka Majandus- ja Kommunikatsiooniministeeriumi, kes seisab selle eest, et Eesti kui e-riik oleks toimiv ja turvaline. Küsimusi, kui ulatusliku, millises mahus ja kui suurte kahjudega juhtunu oli, peab selgitama välja menetlus, mida veab prokuratuur. Eelmisest aastast tuleb kaasa ka teine märkimisväärne juhtum, kus IT- asutuse valdusest lekkisid ligi 10 000 inimese koroonapositiivsed tulemused. Andmekaitse Inspektsiooni menetlus peab selgitama välja vastutava andmetöötleja andmeturbe ja andmekaitsereeglitest kinnipidamise ning analüüsima, kas asutus on teinud pärast seda piisavalt, et tagada isikuandmete kaitstus.

Pisikese Eesti riigi jaoks on ülimalt oluline, et andmete hoiustamiseks loodaks korralik vundament. Vundamenti andmete töötlemisel luuakse eelkõige isikuandmete kaitse üldmäärusest tulenevate printsiipide põhjal. Üheks nendeks printsiipideks on turvalisus ja senine praktika on näidanud, et seda ei suudeta alati tagada, kuigi peaks. Inspektsiooni eesmärk ongi menetlusega see raskusaste seljatada ning tagada, et edaspidi selliseid olukordi ei tekiks. Nii avalik sektor kui ka erasektor peavad mõlemad tagama isikuandmete töötlemise turvalisuse ja ei oma tähtsust infosüsteemide loomise kiireloomuline vajadus. Kui on kiire ja turvalisusele tähelepanu ei pöörata, siis paraku andmed ka lekivad.

Paljuski saavad rünnakud võimalikuks just puudulikust andmeturbest või andmekaitsereeglite mittetäitmisest. Aasta 2020 kinnitas, et turvalise e-ühiskonnani on liikuda veel üksjagu maad ja mida kiiremini me sinna jõuda soovime, seda teadlikumaks peame saama andmekaitses.

Kuid iga aastaraamatu sisu peab peegeldama mõistagi kõige enam muret tekitavate teemade kokkuvõtet, seepärast leiab sellest raamatust kõik need teemad, mis läksid enim korda inimestele. Tõsi, osa nendest teemadest on jõudnud mitmesse eelnevasse aastaraamatusse, aga kuna andmekaitse juba kord on nüansirikas, siis iga käsitluskord on sageli siiski erinev.

**Pille Lehis**
peadirektor

Eriliselt suur tänu läheb inspektsiooni väiksele kollektiivile, kes sel keerulisel ajal on teinud ennastsalgavat tööd.

Suur aitäh kõigile, kes meie poole on pöördunud. Täname koostööpartnereid ja kolleege, kaasamõtlejaid ministeeriumitest, ametitest, omavalitsustest ning partnerorganisatsioonidest.

Tegelikult mahub ju kogu terve aasta kenasti maailmaklassikasse.

„Üks kõigi eest ja kõik ühe eest!“

# ÕIGUSTATUD HUVI KÄSITLUS SAI JUHENDIKS

Isikuandmete kaitse üldmääruse (IKÜM/üldmäärus) tulek tõi Eesti andmekaitseõigusesse ühe olulise muudatuse – õiguse töödelda isikuandmeid õigustatud huvi alusel. Kuigi seda nägi ette ka varasemalt kehtinud EL andmekaitse direktiiv (95/46), ei oldud seda kuni 2019. aasta alguseni kehtinud isikuandmete kaitse seadusesse üle võetud.

Jutt käib niisiis IKÜM artikkel 6 lg 1 punktist f, mille kohaselt on isikuandmete töötlemine seaduslik, kui "töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral, välja arvatud juhul, kui sellise huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused, mille nimel tuleb kaitsta isikuandmeid, eriti juhul, kui andmesubjekt on laps".

## Õigustatud huvi juhendi rakendamine praktikas

Erinevalt mitmetest muudest isikuandmete töötlemise õiguslikest alustest eeldab sellele õiguslikule alusele tuginemine reeglipärast, kolmeastmelist analüüsi. IKÜM-i alusel tegutsev Euroopa Andmekaitsenõukogu (EAKN) on küll võtnud päevakorda sel teemal juhendi koostamise, kuid ei ole sellega kuigi kaugele jõudnud. Siiski saab juhinduda EAKN-i eellase, direktiivi 95/46 artikkel 29 alusel tegutsenud liikmesriikideülese andmekaitse töögrupi 2014. aastal koostatud juhisest 06/2014 õigustatud huvi mõiste kohta. Seda seetõttu, et võrreldes direktiiviga on IKÜM-i õigustatud huvi sätte sõnastus küll veidi muutunud, kuid olemus ja kohaldamisloogika on jäänud samaks.

> ***„Erinevalt mitmetest muudest isikuandmete töötlemise õiguslikest alustest eeldab sellele alusele tuginemine reeglipärast, kolmeastmelist analüüsi."***

Eelnimetatud 2014. aasta juhisele tuginedes ning võttes arvesse Eesti praktikat, koostas inspektsioon 2020. aasta kevadel juhendi, mis selgitab, kuidas õigustatud huvi kui andmetöötluse õiguslikku alust rakendada.

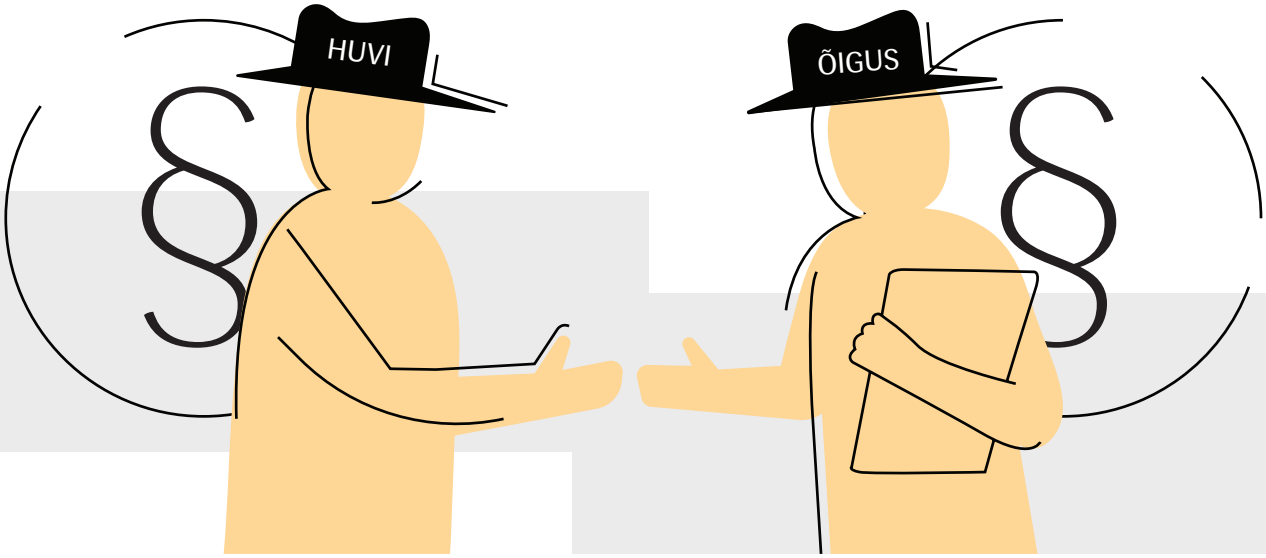
Lühidalt toimub õigustatud huvi hindamine kolmes etapis:

**I** defineeritakse, kellel (andmetöötleja, kolmas isik või üldsus) mis huvi on, mille tarbeks isikuandmeid on vaja töödelda.
**II** määratletakse, kuidas ja milliseid andmesubjekte andmetöötlus mõjutab.
**III** kaalutakse kummagi poole huvide kaalukust, vajadusel leitakse täiendavaid tasakaalustavaid meetmeid.

Erasektoris toimub märkimisväärne osa andmetöötlusest just sellele alusele tuginedes. Õigustatud huvi saab olla õiguslikuks aluseks näiteks veebipoe klientide profileerimisel neile reklaami kuvamisel. Samuti kaupa ostnud kliendi ja ostuandmete säilitamisel hilisemate õigusvaidluste tarbeks, turvakaamerate kasutamisel (nii teenusepakkuja kui tööandja rollis) aga ka lepingu sõlmimisele eelnevalt, näiteks isiku maksevõimelisuse kontrollimisel. Inimestel on paljuski tekkinud üldmääruse kohta olnud meediakajastuse tagajärjel ettekujutus, et see annab neile täieliku kontrolli oma andmete üle ning õiguse iga kell nõuda andmete töötlemise lõpetamist. Tõsi, üldmäärus sellise õiguse annab, kuid paljude piirangutega.

Oma roll väärarusaamade tekkel on olnud kindlasti ka ettevõtjatel endil, kelle lepingutingimustes varasemalt tihtipeale sisaldus muuhulgas lause, et „Lepingule alla kirjutamisega annab klient nõusoleku enda andmete töötlemiseks niisugustel ja teistsugustel eesmärkidel". Alles siis, kui inimene tuleb sooviga oma nõusolek tagasi võtta, selgub, et ettevõte ei saa kuidagi andmete töötlemist ära lõpetada, sest lepingut on ju vaja edasi täita ning tekkinud nõudeid tahaks ju ka kohtus kaitsta. Nii avastavadki paljud inimesed suure üllatusega, et ettevõtte võib nende isikuandmeid töödelda veel palju aastaid pärast tehingut, olgu selleks siis kasvõi ühekordne e-poe ost.

Keeruliseks muudab asja veel see, et erinevad andmetöötluse õiguslikud alused – lepingu täitmine, nõusolek ning õigustatud huvi võivad eksisteerida kõik kõrvuti ühe ja sama andmesubjektiga tekkinud suhte raames. Andmekaitsetingimustes tuleb neid eristada andmekoosseisude kaupa, tuues selgelt välja missuguseid andmeid millisel õiguslikul alusel töödeldakse.




Eelmisel aastal sattus inspektsiooni töölauale korduvalt juhtumeid, kus andmetöötleja advokaadist esindaja viitas turvakaamerate puhul täie tõsidusega kehtetule isikuandmete kaitse seadusele (IKS). Turvakaamerate kasutamine teatavasti tugines kuni 2019. aasta alguseni kehtinud IKS-i erisättele, mida enam ei ole. Ka on selge, et õigustatud huvi analüüs valmistab isegi suurettevõtetele tõsiseid raskusi. Paraku on oma osa selles ilmselt ka suhtumisel. Väga levinud on, et õigusabiteenust asutakse otsima alles siis, kui inspektsioon on teele läkitanud ettekirjutuse või sunniraha sissenõude. Samas kui inspektsiooniga vaidlemisele kulunud õigusabikulu oleks saanud varem kulutada kvaliteetse andmekaitsereeglistiku loomisele ja dokumenteerimisele.

## Portaalide andmetöötlus

Näitena võib tuua ka palju aastaid Eestis tegutsenud majandusinfoportaalid, kelle tegevus põhinebki õigustatud huvil. Kuigi inspektsioon koostas kõikide infoportaalide tegevuse kohta põhjaliku õigusliku analüüsi (www.aki.ee veebiraamatkogus), mille pinnalt oleks pidanud olema lihtne igal infoportaalil oma dokumentatsioon korda teha, pole portaalid senimaani sellega toime tulnud.

Levinud eksimustest võib esile tõsta arusaama, et õigusnõuete kaitseks võibki 10-15 aastat kõikide tehingute (ja nendega seotud inimeste) andmeid säilitada. Tõsi, tsiviilseadustiku üldosa seadusest tuleneb küll nõuete 10-aastane aegumistähtaeg, kuid seda üksnes kohustuste tahtliku rikkumise puhuks. See tähendab, et kui ettevõte tahab inimese andmeid sel põhjusel 10 aastat säilitada, peab ta olema valmis näitama, et selleks on põhjust (et tal tõesti on nõue kliendi vastu ning et kohustusi rikuti tahtlikult). Nimelt tuleneb õigustatud huvi kohaldamise reeglitest, et andmete töötlemise (säilitamise) põhjendus peab olema konkreetne ja reaalne, mitte üksnes hüpoteetiline, spekulatiivne.

> *„Kõige enam on inspektsiooni lauale sattunud siiski andmete kogumise eksimusi. Nimelt arvatakse, et see, mis internetis leitav, on ka vabalt kasutatav.“*

Kõige enam on inspektsiooni lauale sattunud siiski andmete kogumise eksimusi. Nimelt arvatakse, et internetis leitav on vabalt kasutatav. Paraku peab igasuguseks isikuandmete töötluseks, mida ei tehta puhtalt isiklikul otstarbel, olema õiguslik alus. Et ka kord avalikustatud isikuandmete uueks kasutamiseks peab olema õiguslik alus, on kinnitanud aastaid tagasi ka Riigikohus. Nii ei võigi internetist (sh äriregistrist, kuulutusteportaalidest ega sotsiaalmeediast) kokku rehitseda inimeste kontaktandmeid selleks, et neile siis oma kaupa reklaamida (või metsaostu pakkumist teha). Seda eeskätt põhjusel, et inimene on oma telefoninumbri või e-posti aadressi avaldanud muul eesmärgil. E-posti aadressile kommertsteadaannet (milleks on ka metsaostu pakkumine) ei või üldse saata ilma inimese nõusoleku või eelneva kliendisuhteta.

*„Paraku peab igasuguseks isikuandmete töötluseks, mida ei tehta puhtalt isiklikul otstarbel, olema õiguslik alus.“*

Omaette probleemvaldkond on isikuandmete avalikustamine portaalides ning sotsiaalmeedia gruppides (eelkõige võlgnike häbipostid). Ka sellise avalikustamise puhul peaks avaldaja olema läbi viinud õigustatud huvi hindamise (sest muu õiguslik alus kõne alla ei tule). Olgu öeldud, et ka ajakirjanduslikul eesmärgil avaldamine (ning sellekohane säte isikuandmete kaitse seaduses) tugineb IKÜM-i õigustatud huvi sättele.

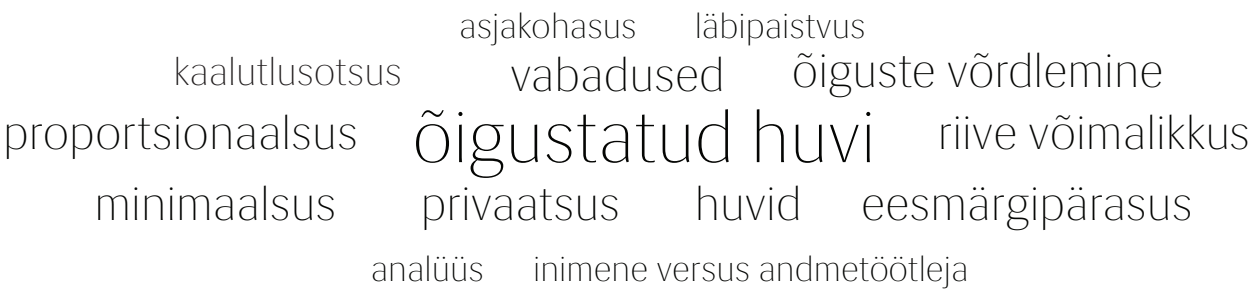
Õigustatud huvile tugineva andmetöötluse puhul on andmesubjektil õigus igal ajal esitada oma konkreetsest olukorrast tulenevalt andmetöötlejale vastuväide. Paraku näib kohustus andmesubjekti pöördumisele vastata olevat andmetöötlejatele täiesti tundmatu. Paljudel juhtudel on inimene oma küsimustele andmetöötlejalt vastuse saanud alles pärast inspektsiooni pöördumist. Seejuures on andmetöötleja tavapäraseks põhjenduseks, et kiri läks rämpsposti või nende töötaja oli tähelepanematu. See juhtub eriti tihti siis, kui andmesubjekt küsib, kust tema andmed on saadud. Seevastu leiavad osad ajakirjandusväljaanded ikka veel, et neile ei kehtigi kohutus andmesubjekti vastuväiteid läbi vaadata.

*„Õigustatud huvile tugineva andmetöötluse puhul on andmesubjektil õigus igal ajal esitada oma konkreetsest olukorrast tulenevalt andmetöötlejale vastuväide.“*

Nagu eelnevast näha, läbib õigustatud hindamise vajadus kõiki valdkondi ning puudutab pea kõiki andmetöötlejaid – valvekaameraga tänavat filmivast majaomanikust kuni andmemüügist elatuvate ettevõtjateni välja.

Siiski, olemas  on ka üks suur erand. IKÜM-i art 6 lg 1 viimasest lausest ning põhjenduspunktist 49 tuleneb, et avalik sektor ei saa õigustatud huvile tugineda oma põhiülesannete täitmisel, kuid põhitegevusega mitteseotud haldustegevuses, nt asutuse majandamine, hoone ja infosüsteemide turvamine, võiks ka õigustatud huvi andmetöötluse alusena kõne alla tulla.

Kokkuvõttes võib öelda, et õigustatud huvi korraliku hindamiseni on andmetöötlejatel veel pikk tee käia, kuid loodetavasti aitab inspektsiooni juhis ning kujundatav praktika sellele kaasa.



# AJALOOLINE SCHREMS II KOHTUOTSUS

Euroopa Kohus võttis 2020. aasta juulis vastu ajaloolise kohtuotsuse, millega tühistas *Privacy Shield* programmi kehtivuse, kuid mida see endaga kaasa tõi?

Nimelt Ameerika Ühendriike loetakse mittepiisava andmekaitsetasemega riigiks, kuhu andmete edastamisel tuleb kohaldada isikuandmete kaitse üldmääruse (IKÜM) 5. peatükis toodud tingimusi. Küll aga oli loodud erandtingimus – kasutades *Privacy Shield* programmi (USAs asuv ettevõte liitus programmiga ja tagas Euroopa Liiduga samaväärse andmekaitsetaseme), siis loeti sellist edastamist piisava tasemega edastamiseks ning andmetöötleja ei pidanud kohaldama eelmainitud 5. peatükki.

*Privacy Shield* eelkäija *Safe Harbour* programm tühistati Euroopa Kohtu otsusega aastal 2016. *Safe Harbour* on tuntud kui Schrems I otsus. Mõlema kohtuvaidluse hagejaks on olnud andmekaitseadvokaat Max Schrems.

Schrems II otsuse juures oli üks tähelepanuväärivasjaolu – nimelt viitas ka kohus, et muude andmete edastamisel kasutavate lisakaitsemeetemete (loetletud IKÜM artiklis 46) puhul tuleb hinnata, kas andmete edastamisega on tagatud piisav andmekaitsetase ning andmesubjekti õigused. See tähendab, et kasutades andmete edastamiseks näiteks standardseid andmekaitseklausleid, mis on ühtlasi ka enimkasutatavaks kaitsemeetmeks andmete edastamisel, on vaja nende piisavust igakordselt eraldi hinnata. Vajadusel tuleb võtta kasutusele täiendavad kaitsemeetmed ning kui seda ei suudeta, siis ei tohi andmeid edastada.

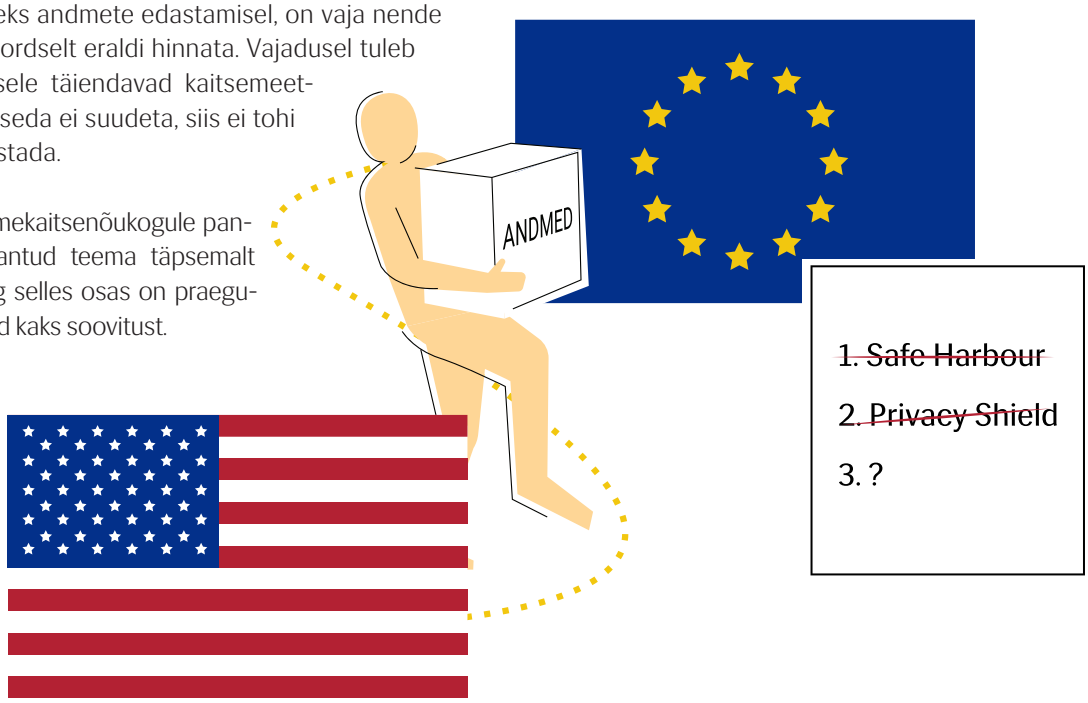
Euroopa Andmekaitsenõukogule pandi kohustus antud teema täpsemalt sisustada ning selles osas on praeguseks koostatud kaks soovitust.

### Schrems II otsuse järgselt anti välja

I „Soovitused edastusvahendeid täiendavate meetmete kohta, et tagada vastavus isikuandmete kaitse ELi tasemega“ Dokument EAKN veebis.

II „Soovitused Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis“ Dokument EAKN veebis.

Euroopa Komisjon hakkas koostama uusi, täiendatud standardseid andmekaitseklausleid, mis peaksid arvestama nii kohtuotsuses toodud asjaoludega kui ka Euroopa Andmekaitsenõukogu soovitustega. Siiski ei saa veel öelda, et antud teema oleks aastaraamatu välja andmise ajaks lõppenud ning kindlasti ei saa öelda, et nende juhendite ja uute andmekaitseklauslitega on andmete USA-sse edastamise probleem lahendatud. Senikaua soovitab inspektsioon andmetöötlejatele, kel on USAs asuvad partnerid (olgu need siis vastutavad töötlejad või volitatud töötlejad), kriitiliselt hinnata andmete edastamise vajadust ning kui see siiski peaks olema vältimatult vajalik, siis kohaldada eeltoodud soovituste sätteid.



### Brexiti andmekaitse aspekt

Ühendkuningriigi (UK) lahkumisel Euroopa Liidust saab temast mittepiisava andmekaitsetasemega riik, kui käesoleva aasta 30. juuniks ei tehta UK-le piisavusotsust. Kuni 30. juunini toimub andmeedastus nagu varem, s.t et UK-d käsitletakse piisava andmekaitsetasemega riigina ning IKÜM 5. peatükki ei pea kohaldama.

Pärast lahkumist Euroopa Liidust hakkas UK taotlema kohe Euroopa Komisjonilt nimetatud piisavusotsust, kuid see on ajaliselt väga mahukas protseduur. Mõnel eelneval juhul on see võtnud aega aastaid.

Seega sel perioodil, kui UK-l ei ole piisavusotsust, oleks tegemist mittepiisava andmekaitsetasemega riigiga, kuhu andmeid edastades tuleb kohaldada isikuandmete kaitse üldmääruse (IKÜM) artiklis 46 ja 47 lisakaitsemeetmeid või artiklis 49 loetletud erandeid. See tähendab andmetöötlejale suurenenud koormust näiteks lisalepingute (standardsete andmekaitseklauslite) sõlmimise või siduvate korporatsiooni reeglite (artikkel 47) loomise näol.

Viimased uudised sel teemal leiab Euroopa Andmekaitsenõukogu veebilehelt.

## TEAVITUSTÖÖ MÄRKSÕNAKS OLI UUTMOODI

Tulevikuühiskonnas ei ole andmekaitse ilmselt vaid juristide, IT-spetsialistide ja lisaks mõne üksiku entusiasti teema, millest kõneldakse suuremas seltskonnas üliharva, sest enamasti see inimesi ei huvita. Igapäevaselt andmeid neelav digielu seab paratamatult inimesi fakti ette, kus mõistetakse toimiva andmekaitse olulisust, sest ilma selleta pole võimalik teada, kes kuidas ja kus isikuandmetega midagi teeb ning kellega jagab.
Inspektsioon on alati pidanud oluliseks panustada teadlikkuse kasvu suurendavale koolitus,- nõustamistegevusse ja juhendiloomesse ning möödunud aastal vastavalt ressurssidele seda ka tehti. Lisaks tavapäraseks saanud teavitustegevusele tõi inspektsioon juurde uusi võimalusi, mis aitaks teadlikkuse kasvatamisel puudutada erinevaid sihtrühmasid.

### Teadmiste testimise testid

Andmekaitse põhimõtete selgitamiseks ja iseenda jaoks õigete vastuste leidmise ettevalmistuseks tegi inspektsioon möödunud aastal 2 veebitesti “Andmekaitse ja raketiteadus?” ja “ Digivegan”.

“Digivegani” testi eesmärk oli anda endale võimalus saada teada, kas tavapärane mõtteviis igapäevastes arvuti taga tehtavates toimingutes on tehtud digielu - keskkonnateadlikult. See, kui inimene käitub oma isikuandmetega säästlikult, mis tähendab, et jagan läbimõeldult ja ei jäta laokile, on andmekaitse oluline osa. Testiga “Andmekaitse ja raketiteadus?” sai iseenda


jaoks proovile panna oma baasteadmisi andmekaitse põhimõtetes. Kui inimene on teinud endale selgeks põhimõtted, oskab ta vähesema vaevaga leida õigeid vastuseid mistahes olukorras. Ilma isikuandmete kasutamiseta ei saa toimida ju ükski teenus ning valdkondi, mida andmekaitse ei puuduta praktiliselt olemas ei ole.

## IT-põhine tööriist Videovalve sildi saamiseks

Möödunud aastal lõi inspektsioon koostöös Registrite ja Infosüsteemide Keskusega ka videovalve sildi genereerija, mis aitab videovalve korraldajal saada nõuetekohane teavitussildi fail kas väljaprintimiseks või trükikotta saatmiseks.

Videovalve korraldajate üheks suurimaks komistuskiviks ongi olnud puuduv või mittepiisav teavitus. See aga on omakorda kaasa toonud väga palju probleeme nii töö - kui naabritevahelistes suhetes.

Videovalve sildi genereerijaga teavitussilti luues saab ühtlasi ka selgitusi, miks on oluline sildile nõutud info lisada ja milline see täpsemalt olema peab.



Lihtsam lahendus on kasutada AKI veebis videovalve sildi generaatorit - videovalvesilt.aki.ee

## Start videoseminaridele

Kui varasematel aastatel on inspektsioon korraldanud, koolitusi, seminare ja konverentse isikuandmete kaitse ja avaliku teabe seaduse teemade käsitlemiseks, siis möödunud aastal sai alguse AKI videoseminaride sari. Lisandväärtuseks teadmistele on kindlasti see, et videoseminari saab vaadata mistahes ajal ja nii mitu korda, kui seda vaja.

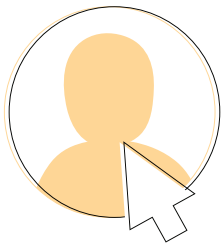
Esimene veebi striimitud videoseminar oli suunatud haridusasutuste töötajatele ning selgitas andmekaitselisi küsimusi distantsõppe läbi viimisel ja dokumendihalduses. Videoseminaril osalejad said esitada koolitajatele küsimusi nii enne seminari toimumist kui seminari toimumise jooksul.

Loodud testid, videovalve sildi genereerija ja videoseminar mitmekesistasid inspektsiooni senist teavitustegevust ning nagu öeldakse iga kild terviku kokku saamiseks on määrava tähtsusega.

# PRAKTIKUTE TÖÖLAUALT

Juristide töölauale jõudis 2020. aastal ligikaudu 150% rohkem nõudekirju ja 25% kaebusi. Samuti tuli juhtumeid lahendamiseks ligi 20% võrra kasvanud rikkumisteadetest. Ainsana vähenes selgitustaotluste ja märgukirjade arv ning seda ligi 35%. Kokkuvõttes oli väga töine aasta ja mõned märgilisemad lood saavad järgnevas peatükis kajastatud.

# MAJANDUSINFOPORTAALIDE SEIRE VAHEKOKKUVÕTE



Inspektsioon on saanud aastate jooksul sadu murelikke pöördumisi inimestelt, kes on leidnud internetiotsingu tulemustest linke majandusinfoportaalidele (infoportaalid), mis on avalikustatud nende isikuandmeid.

Infoportaalide tegevuse üle alustas inspektsioon järelevalvemenetlust 2017. aastal, kuid isikuandmete kaitse üldmääruse (IKÜM/üldmäärus) kehtima hakkamisega aastal 2018 muutus õiguskord ning see tähendas, et eelnevalt tehtu tuli uuesti üle vaadata uues andmekaitseõiguses.

2020. aasta 1. juunil saatis inspektsioon majandusinfoportaalidele (edaspidi infoportaal) õigusliku analüüsi ja ettepanekud oma tegevuse kooskõlla viimiseks IKÜMi nõuetega.

Inspektsioon leidis, et infoportaalide tegevus on vajalik, kuid inimeste andmete kogumine ja avalikustamise viis peab olema korrektne ning andmetöötluse protsess läbipaistev. Infoportaalide andmetöötlus peab olema kooskõlas andmekaitsereeglite ja põhimõtetega.

## Inspektsiooni seisukohad

Füüsilise isiku kohta käivate eraeluliste andmete (sh kohtulahendid, ametlikud teadaanded, meediakajastused) töötlemine infoportaalides on lubatud üksnes ulatuses, mis vastab täielikult isikuandmete kaitse seaduse (IKS) §-le 10 ja IKÜM artikkel 5 lõikele 1. Seejuures on näiteks keelatud töödelda (koguda, koostada, edastada):

a) eluloolisi andmeid (nt sünnikoht, emakeel, hariduskäik);
b) erakondliku kuuluvusega seotud andmeid;
c) kinnistu andmeid;
d) persoonilugusid, mis loovad inimestest negatiivse või kahtlustava mulje ning mis ei ole tihtipeale seotud konkreetse inimesega;
e) punktiskoori, kui puudub selle kujunemise läbipaistvus.

Koostada ja avalikustada tuleb võrgulehel andmekaitsetingimused, mis vastavad täielikult IKÜM artiklites 12 – 14 sätestatud nõuetele.

Koostada tuleb dokument, mis kirjeldaks piisava põhjalikkusega õigustatud huvi olemasolu (analüüs/hinnang).

Kohustus on tagada andmesubjektile vastuväite esitamise võimalus, sh on kohustus lahendada vastuväide lähtuvalt vastuväite sisust. Olukorras, kus andmesubjekti taotlust ei rahuldata, tuleb infoportaalil tõendada seda, et edasiseks töötlemiseks on mõjuv õiguspärane põhjendus.

Rakendada tuleb täiendavaid kaitsemeetmeid – näiteks tagada andmesubjektidele suurem läbipaistvus ja luua elektrooniline keskkond, mis võimaldab enda kohta käivaid andmeid näha, kasutada ja esitada vastuväiteid.

Kõikide inspektsiooni seisukohtadega saab tutvuda inspektsiooni rubriigi Teavitus, juhised all asuvas veebiraamatukogus www.aki.ee.

Kuigi infoportaalid avalikustasid äriregistrist võetud infot, tehti seda sageli koos lisaandmetega, mida inimese kohta on õnnestunud hankida teistest allikatest. Näiteks olid seotud äriregistri andmed ametlike teadaannetega, kohtuotsuste, ajaleheartiklite, kinnisvara, võlainfo, reitingute, erakondlik kuuluvuse ning isegi CV-ga. Sageli oli küll erinevatest avalikest allikatest kogutud info otsingumootoritele avatud, kuid see häiris paljusid inimesi.

Arvestades, et kui infoportaalide ülesanneteks on tagada ühiskonnale nii juriidilise isiku esindusõiguse ja usaldusväärsuse kui ka lisaks füüsilise isiku krediidivõimekuse kontroll, siis just lähtuvalt nendest ülesannetest tulebki teha andmetöötlustoiminguid. Seejuures tuleb järgida eesmärgipärasuse ja minimaalsuse põhimõtteid.

Alates ettepaneku tegemisest on inspektsioon kontrollinud iga infoportaali vastavust andmekaitsenõuetele, sh ettepanekus toodule.

Kui infoportaali vastutav töötleja on aru saanud, kuidas andmekaitsenõudeid täita ning viinud inspektsiooni hinnangul oma tegevuse teoreetiliselt ka vastavusse õigusaktides sätestatud tingimustega, siis peab inspektsioon vajalikuks kontrollida üle ka koostatud dokumentatsiooni (andmekaitsetingimused, õigustatud huvi analüüsi) ning tegeliku andmetöötluse ulatuse ja viisi kogu teabele, mis on konkreetse infoportaali võrgulehel. Selleks taotleb inspektsioon juurdepääsu isikuandmetele.

| | |
|---|---|
| 2017 | Seire algus |
| 2018 | Andmekaitseõigus muutus 25.05 |
| 2019 | Seire läbiviimine |
| 2020 | Vahekokkuvõte |

***„2020. aasta lõpu seisuga ei olnud ükski seires olevatest infoportaalidest viinud oma tegevust sinnamaani, kus andmetöötlus vastaks täielikult õigusaktides sätestatud nõuetele.***

Siiski võib öelda, et suures osas olid infoportaalid inspektsiooni ettepanekutega nõustunud ning teinud parandusi ja muudatusi selleks, et viia oma tegevus õigusaktidega vastavusse. Inspektsioonini jõudnud pöördumiste pealt võib ka välja tuua, et ühe positiivse tendentsina oli märgata, et infoportaalid ei jäta enam inimeste isikuandmete töötlemisega seotud küsimustele vastamata. Samuti on reageeritud ka inimeste vastuväidetele ning eemaldatud võrgulehelt isikuandmeid.

Infoportaalide seire läbiviimine jätkub 2021. aastal. Inspektsiooni tugevdatud tähelepanu koondub ka sellele, et infoportaalides oleksid andmesubjekti õigused tagatud, sh et inimestel oleks võimalik tutvuda enda kohta käivate andmetega. Inimeste vastuväidete saamisel isikuandmed kustutaksid või vastuväidet ka sisuliselt hindaks ning põhjendaksid, millisel mõjuval õiguspärasel põhjusel andmetöötlus jätkub (IKÜM artikkel 21 lg 1).

# VASTUVÄITE ESITAMISEL EI TOHI ANDMETÖÖTLUS JÄTKUDA

Isikuandmete kaitse üldmääruse (IKÜM/üldmäärus) artikkel 21 lg 1 annab andmesubjektile õiguse esitada igal ajal vastuväiteid teda puuduvate isikuandmete töötlemise suhtes, mille töötlemine toimub õigustatud huvi alusel, sh sellele sättele tugineva profiilianalüüsi suhtes.

Vastuväite saamisel ei tohi vastutav töötleja isikuandmeid edasi töödelda, v.a juhul, kui tõendatakse, et andmeid töödeldakse mõjuval õiguspärasel põhjusel, mis kaalub üles andmesubjekti huvid, õigused ja vabadused või kui olukord puudutab õigusnõude koostamise, esitamise või kaitsmise eesmärki. Andmesubjektil on õigus vastu vaielda oma konkreetsest olukorrast lähtudes ning põhjendada, miks tema seisukohalt on tema isikuandmete töötlemine ülemäärane. Sel juhul peab vastutav töötleja vastuväite alusel hindama uuesti konkreetse inimese osas olukorda, arvestama vastuväite sisuga ja tõendama, et tal on ka konkreetset juhtumit arvestades mõjuv õiguspärane põhjus andmeid edasi töödelda.

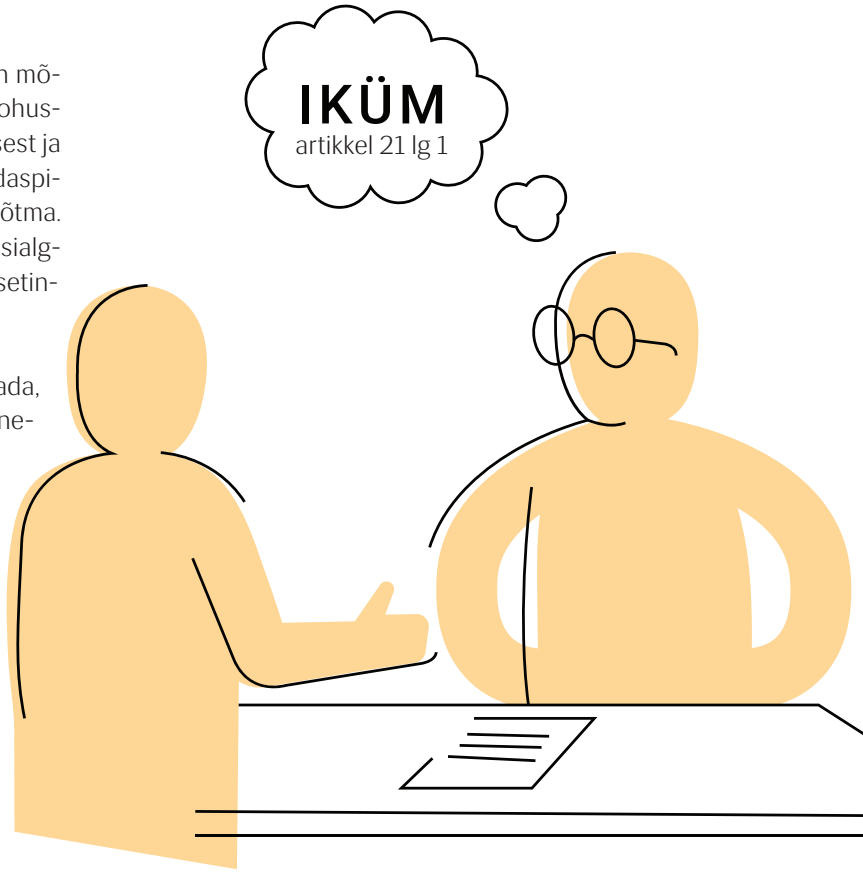
Vastuväite esitamise võimalus ongi loodud selleks, et inimesel oleks võimalik tuua välja ka selliseid olukordi, mille peale ei oleks mõistlik andmetöötleja ise varem saanud tulla või mille peale tulemine ei olnudki võimalik. See, kui vastuväite peale andmetöötlust konkreetse inimese osas muudetakse, ei tähenda automaatselt seda, et andmetöötleja oleks millegi vastu varasemalt eksinud. Andmetöötleja on lihtsalt valmis muutma vajadusel töödeldavate andmete koosseisu ning lähtuma õigusaktidest tulenevatest nõuetest.

Lisaks tuleb välja tuua, et vastuväite lahendamise ajaks tuleb andmete avalikustamine ja/või edastamine kuniks vastuväite lahendamiseni ka peatada (IKÜM artikkel 21 lg 1). Sama kinnitab ka IKÜM artikkel 18 lg 1, sh tuleb töötlemine peatada kuniks selgub, kas isikuandmed on õiged või kuniks veendutakse, et vastutava töötleja õiguspärased põhjused kaaluvad üles andmesubjekti põhjused. Töötlemise peatamine vastuväite saamisel tähendab, et andmete töötlemine (sh edastamine) lõpetatakse ajani, mil on hinnatud edasise töötlemise mõjuvat õiguspärast põhjust. Kui selline

## Vastuväide nõuab vastamist

Isegi kui isikuandmete edasiseks töötlemiseks on mõjuv õiguspärane põhjus, on igal andmetöötlejal kohustus vastuväite korral lähtuda konkreetsest inimesest ja tema konkreetsest vastuväitest ning analüüs edaspidise töötlemise osas peab seda kõike arvesse võtma. Vastuväite korral ei ole lubatud viidata lihtsalt esialgsele õigustatud huvi hindamisele või andmekaitsetingimustele.

Kui vastutav töötleja ei suuda inimesele tõendada, et ta vastuväitja olukorda arvestades saab tugineda enda ja/või kolmanda isiku õigustatud huvile ning andmetöötluseks on mõjuv õiguspärane põhjus, on andmete edasine töötlemine selles osas ka keelatud ning andmete töötlemine tuleb lõpetada ning andmed kustutada (IKÜM artikkel 17 lg 1 punkt c). Samuti võib vastuväite lahendamise tulemusel olla vajalik näiteks andmetöötluse ulatuse muutmine, ehk avalikustamise asemel edastatakse andmeid üksnes konkreetsetele kolmandatele isikutele lähtuvalt IKS §-s 10 sätestatud tingimustest.



põhjus andmete edasiseks töötlemiseks puudub, tuleb andmetöötlus lõpetada ning kui see on olemas, tuleb analüüsi tulemus ning andmete edasise töötlemise otsus edastada ka andmesubjektile ( IKÜM artikkel 18 lõige 3 ja artikkel 21 lg 1).

Igal andmesubjektil on õigus esitada vastuväide ka selle osas, et kolmandal isikul puudus õiguslik alus andmete saamiseks. Sel juhul tuleb välja selgitada, kas inimese vastuväide on õigustatud või mitte. Kui selgub, et andmeid edastati ebaseaduslikult, on andmetöötlejal kohustus hinnata, kas ebaseaduslik edastamine põhjustas või tõenäoliselt põhjustab inimese õigustele ja vabadustele ohu/kahju või suure kahju. Hindamise tulemusest lähtuvalt tuleb kas rikkumine üksnes dokumenteerida, rikkumisega seotud ohu korral teavitada inspektsiooni või suure ohu korral teavitada nii inspektsiooni kui ka inimest, kelle andmeid ebaseaduslikult töödeldi.

Igat vastuväidet tuleb lahendada konkreetsest olukorrast lähtudes.

Arvestama peab, et ka võlaandmeid ei saa õigustatud huvi alusel avaldada, kui see kahjustab ülemäära andmesubjekti õigusi ja vabadusi. Võlaandmete avaldajad just nimelt aga õigustatud huvile oma tegevuse põhjendamisel on toetunudki.

### Inimesel on õigus

- Tutvuda andmetega
- Parandada andmeid
- „Õigus olla unustatud“
- Andmete töötlemist piirata
- Lasta andmeid üle kanda
- Esitada vastuväide
- Olla teavitatud isikuandmete kasutamisest
- Õigused seoses automatiseeritud otsuste ja profiilianalüüsi tegemisega


Inspektsiooni menetluspraktikast paistab välja, et kui andmesubjekti võlaandmed on aegunud, siis andmetöötleja võlainfo avaldamise lõpetamisega arvestada ei taha. See on näide võlgniku kui andmesubjekti õiguste ja vabaduste ülemäärasest kahjustamisest. Tihti lisandub siia kas siis põhjendatult või mitte see, et andmesubjekti ei ole andmete edastamisest ja avaldamisest üldse teavitatud. Nii teavitamine kui ka andmetöötluse põhjendatuse hindamine on vastutava andmetöötleja ülesandeks. Kui see jäetakse tegemata, peab seaduse vastu eksinu arvestama järelevalveasutuse sekkumisega.

***„Iga andmetöötleja, sh nii maksehäireregistri kui ka portaalipidaja on kohustatud järgima IKÜM artikkel 5 lg 1 sätestatud põhimõtteid ja vastutama nende täitmise eest. Kui andmetöötluseks seaduslikku alust ei ole, tuleb isikuandmete töötlemisest loobuda.“***

# ETTEVÕTTEL TULI VÕLAANDMED VÕRGULEHELT EEMALDADA

Möödunud aasta menetluspraktikas oli mitmeid juhtumeid, mil ettevõte avalikustas oma võrgulehel inimeste nimesid ja võlgnevuse summasid. Aastaraamatus kirjeldab inspektsioon menetlusotsuseni jõudmise käiku reisikorraldaja juhtumi näitel, sest põhimõte võlaandmete töötlemisel on alati üks ja seesama. Nimelt avalikustas reisikorraldaja oma klientide võlad veebilehel.

Isikuandmete töötlemisel tuleb arvestada isikuandmete kaitse seaduse (IKS) ja isikuandmete kaitse üldmääruse (IKÜM/üldmäärus) nõuetega. Muuhulgas on andmetöötlejal kohustus järgida ka IKÜM artiklis 5 sätestatud põhimõtteid, sh lg 1 punktis a, b, c sätestatut:

- töötlemine on seaduslik, õiglane ja isikule läbipaistev;
- eesmärgi piirang – isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel;
- võimalikult väheste andmete kogumine – isikuandmed on asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt.

Kohustuste täitmist peab tõendama vastutav töötleja IKÜM artikkel 5 lg 2 alusel.

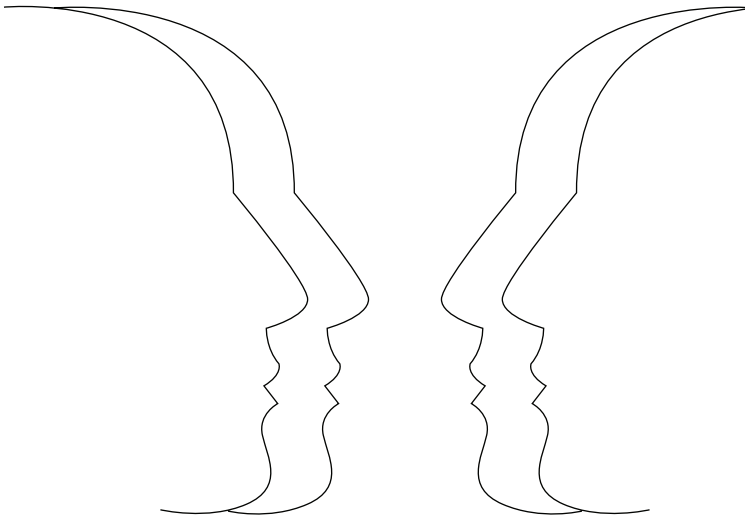
***Isikuandmeid võib töödelda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks ning seejuures peab tagama, et andmete töötlemise eesmärk riivaks võimalikult vähe inimese põhiõigusi.***

Andmetöötlejal tuleb eelnevalt alati hinnata, kas andmete töötlemine (sh avalikustamine) on eesmärgi täitmiseks vältimatult vajalik või on eesmärgi täitmisel võimalik piirduda vähem riivavamate meetmetega.

Lisaks tuleb isikuandmete töötlemisel seoses võlasuhte rikkumisega arvestada ka IKS §-ga 10. IKS § 10 lg 1 tuleneb järgnev: *„Võlasuhte rikkumisega seotud isikuandmete edastamine kolmandale isikule ja edastatud andmete töötlemine kolmanda isiku poolt on lubatud andmesubjekti krediidivõimelisuse hindamise eesmärgil või muul samasugusel eesmärgil ning üksnes juhul, kui vastutav või volitatud töötleja on kontrollinud edastatavate andmete õigsust ja õiguslikku alust isikuandmete edastamiseks ning on registreerinud andmeedastuse.“*

Lähtuvalt eeltoodust on keelatud avalikustada võlglaste andmeid võrgulehel ning andmete edastamine on lubatud üksnes juhul, kui on täidetud IKS § 10 lg 1 sätestatud tingimused. Lisaks tuleb arvestada enne andmete edastamist ka IKS § 10 lg 2, milles on sätestatud tingimused, mis keelavad andmete edastamise.

Kuna reisikorraldaja ei arvestanud võlaandmete töötlemisel eeltoodud nõuetega, siis rikkus ta võlaandmete avalikustamisel isikuandmete kaitse seaduse ja üldmääruse nõudeid. Inspektsiooni menetlusotsus kohustas eemaldada võrgulehelt võlasuhte rikkumisega seotud isikuandmed.



# ISIKUANDMETE SÄILITAMINE 10 AASTAT UUTE PETTUSTE AVASTAMISE EESMÄRGIL

Inspektsiooni menetluses oli rahusvaheline juhtum, kus sõidujagamisteenust pakkuv ettevõte jagas sõiduteenuse osutajatele (ettevõtte klientidele) soovituskoode, mille alusel on võimalik kutsuda uus inimene ettevõtte kliendiks ning saada tänu sellele ühekordne boonus. Üks klientidest aga kasutas soovituskoodi enda kahe seadme vahel, ehk kutsus ise ennast ettevõtte platvormiga (taas)liituma. Ettevõte blokeeris kliendi konto ning klient ei saanud oma kontoga ettevõtte teenuseid kasutada. Juhtumist lähtuvalt pidas ettevõte vajalikuks säilitada inimeste isikuandmeid uute pettuste avastamise eesmärgil 10 aastat ning ei rahuldatud inimese taotlust kustutada tema andmed peale kliendisuhte lõppemist.

Miks inspektsioon aastaraamatus selles juhtumist kõneleb, on põhjusel, et inimesel on õigus nõuda, et vastutav töötleja kustutaks põhjendamatu viivituseta teda puudutavad isikuandmed, kui isikuandmete töötlemiseks enam alust ei ole (vt isikuandmete kaitse üldmäärus (IKÜM) artikkel 17 lg 1). Näiteks, kui andmed on kogutud teenuse osutamise raames, kuid teenuse osutamine konkreetsele inimesele on lõpetatud, ei ole isikuandmete töötlemiseks õiguslikku alust ning need tuleb kustutada, kui ei esine ühte IKÜM artikkel 17 lõikes 3 toodud ajaoludest.

IKÜM artikkel 17 lg –s 3 on toodud järgnev – lg 1 ja 2 ei kohaldata sel määral mil isikuandmete töötlemine on vajalik:

a) sõna – ja teabevabaduse õiguse teostamiseks;
b) selleks, et täita vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õigusega ette nähtud juriidilist kohustust;

Selgituseks, et isikuandmete töötlemine (sh andmete säilitamine) nimetatud punkti (b) alusel on lubatud juhul, kui isikuandmete töötlemise kohustus tuleneb eriseadusest (nt raamatupidamise seadus § 12 lõige 1). Seejuures võib andmeid sellisel juhul töödelda ka üksnes eriseaduses sätestatud eesmärgil (nt üksnes säilitamise eesmärgil). Mis puudutab aga tsiviilseadustiku üldosa seaduse (TsÜS) §-i 146, siis nimetatud paragrahvist tuleneb nõude aegumistähtaeg ning sellest ei tulene otsest kohustust (seadusjärgset kohustust) andmete säilitamiseks. Lisaks ei viidanud ettevõte ka mõnele teisele eriseadusele, millest tuleneks seadusjärgne kohustus 10-aastasele andmete töötlemisele, sh mis annaks õiguse/kohustuse säilitada andmeid 10 aastat pettuste avastamise või ennetamise eesmärgil. Samuti ei ole sellist eriseadust teada ka inspektsioonile.

c) rahvatervise valdkonnas avaliku huviga seotud põhjustel;
d) avalikes huvides toimuva arhiveerimise, teadus – või ajaloouuringute või statistilisel eesmärgil;
e) õigusnõuete koostamiseks, esitamiseks või kaitsmiseks.

Selgituseks, et nimetatud punkt (e) on kohaldatav üksnes juhul, kui isikuandmete töötlemine on vajalik õigusnõuete koostamiseks, esitamiseks või kaitsmiseks. Selleks, et inimesel ja järelevalveasutusel oleks võimalik eeltoodut hinnata, tuleb ettevõttel tõendada, et andmetöötlus on konkreetse inimese osas vajalik ning andmetöötlus vastab seejuures ka IKÜM artiklites 5 ja 6 sätestatud nõuetele.

Antud juhtumis ei sobinud andmete töötlemise alusteks IKÜM artikkel 17 lg 3 punktid a, c ja d. Punk e alusel andmete töötlemine nõuab õigustatud huvi analüüsi. Ettevõte küll saatis inspektsioonile õigustatud huvi analüüsi, kuid see põhines pettuste tuvastamisel ja ärahoidmisel. Nimetatud eesmärgil ei ole aga õigustatud isikuandmeid 10 aastat säilitada. Seega puudus inspektsioonil ettevõte analüüs, mis õigustaks 10-aastast andmete säilitamist. Samuti oli inspektsioonil kahtlusi selles, et 10-aastane andmete säilitamine saaks konkreetset rikkumist silmas pidades olla vajalik ja õigustatud.

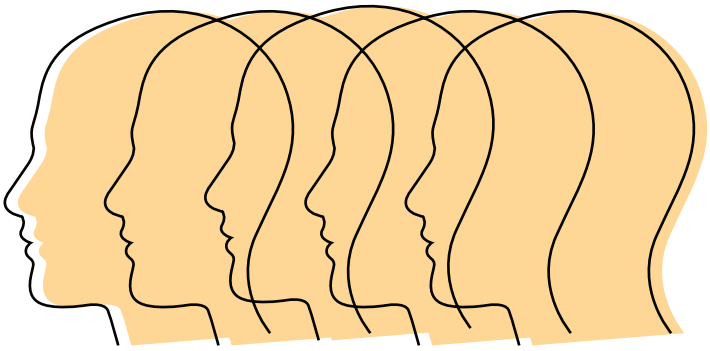
*„Inspektsioon leidis, et pettuste avastamise, ennetamise ja/või edaspidiste pettuste vältimiseks ei ole ettevõttel õigust/kohustust andmeid 10 aastat töödelda (sh säilitada, kasutada).“*

Menetluse käigus ettevõte kustutas kaebuse esitaja isikuandmed, välja arvatud dokumendid, mille säilitamise kohustus tuleneb raamatupidamise seadusest.

Selle kaasuse vaates on oluline rõhutada, et andmetöötlejal on üldjuhul kohustus kustutada isikuandmed, kui andmeid ei ole enam vaja sellel eesmärgil, millega seoses need koguti. Kui aga andmesubjekti kustutamise taotlust ei rahuldata, on andmetöötlejal kohustus tõendada nii inimesele kui ka vajadusel järelevalveasutusele, millisel IKÜM artikkel 17 lõikes 3 sätestatud õiguspärasel põhjusel andmetöötlust jätkatakse. Seejuures ei piisa tõendamisel üksnes viitest õigusakti sättele, vaid andmetöötlejal on kohustus tõendada, et viidatud säte on kohaldatav konkreetse juhtumi ja konkreetse andmesubjekti osas.

## ANDMEKAITSEST TÖÖSUHETES

Viimastel aastatel on üheks enim käsitletavaks teemaks olnud andmekaitse töösuhetes ning muutusi ei toonud ka 2020 aasta. Inspektsiooni poole pöörduti eelkõige seoses videovalve korraldamisega, kuid ka töötaja andmetele ligipääsu ja e-posti aadressi sulgemisega seonduvate küsimustega. Kuigi inspektsioon on eelnevates aastaraamatutes neid teemasid käsitlenud, tasub põhitõed siiski üle korrata ka möödunud aasta menetluste raames.



### TÖÖTAJATE JÄLGIMISE ÕIGUSLIK ALUS

Inspektsioon on tihti pidanud tööandjatele meelde tuletama, et isikuandmeteks on igasugune teave, mille järgi on võimalik inimest otseselt või kaudselt tuvastada. Praktikas on ette tulnud olukordi, kus tööandja soovib jälgida töötaja tegemisi ja liikumisi, kuid töökohustuste täitmist võib kontrollida üksnes viisil, mis ei riku töötaja põhiõigusi. Selline isikuandmete töötlemine saab toimuda tööandja õigustatud huvi alusel.

Reeglina töödeldakse töösuhte ajal isikuandmeid töötajaga lepingu täitmiseks, kuid nt töötaja e-kirjade, internetikasutuse jälgimine või muu taoline kontroll liigitub tööandja õigustatud huvi alla. Töötaja kontrollimine on küll tihedalt seotud töölepingust tulenevate kohustustega, kuid see ei ole samal ajal kindlasti vajalik töölepingu täitmiseks. Töötaja nõusolek saab aga töösuhetes isikuandmete töötlemise aluseks olla vaid neil juhtudel, kui isikuandmete töötlemine ei ole vältimatu ning töötajal on tõepoolest võimalik otsustada, kas ta soovib anda nõusoleku isikuandmete töötlemiseks ning tal on võimalus ka nõusolek tagasi võtta.
Õigustatud huvile tuginemine eeldab, et tööandja on läbi viinud ja kirjalikult dokumenteerinud põhjaliku huvide hindamise ja kaalumise. Sealhulgas peab hindama,

kas e-kirjade lugemine ning interneti ja muude programmide kasutuse jälgimine on mõistlik ja vajalik. Sellises olukorras soovitame kindlasti paika panna ka e-posti ning interneti ning programmide kasutamise reeglid.

Eelnev kehtib ka näiteks töötaja arvutisse paigaldatud tarkvara suhtes, mis teatud aja möödudes teeb töötaja arvutiekraanil olevast kujutisest pildifaile ning edastab selle tööandjale, kes neid pildifaile (vastavate isikutega seostatuna) säilitab. Samuti olukorras, kus tööandja nõuab, et töötaja paigaldaks isiklikku telefoni rakenduse, mis töötaja liikumist jälgib või olukorras, kus tööandja paigaldab GPS seadme töö tegemiseks mõeldud sõidukile ning sõiduki kasutaja on tuvastatav.

## ANDMETÖÖTLUS ENNE JA PÄRAST TÖÖSUHET VALMISTAS MURET

Inspektsioon sai mitmeid pöördumisi, mis puudutasid isikuandmete töötlemist tööle kandideerimisel. Üldiseks aluseks kandidaadi isikuandmete töötlemiseks on kandidaadi nõusolek, samas võib kandidaadi kohta koguda andmeid ka tema nõusolekuta (näiteks avalikest allikatest, mida kandidaat on ise avalikustanud sotsiaalmeedias jms). Lisaks on potentsiaalsel tööandjal võimalus võtta ühendust eelmise tööandjaga, kuid seda üksnes juhul, kui isik on andnud selleks enda selgesõnalise nõusoleku.

### E- posti juurdepääs

Rohkem põhjusi inspektsiooni poole pöördumiseks andis aga peale töösuhte lõppu toimuv andmetöötlus. Eelkõige pöörduti seoses endiste töötajate nimeliste e-posti aadressidega. Üldjuhul antakse töötajale nimeline e-posti aadress töölepingus ettenähtud ülesannete täitmiseks. Pärast töösuhte lõppu ei ole töötaja nimelise e-postiaadressi töötlemiseks enam algset seadusest tulenevat alust (puudub tööleping). Pärast töösuhte lõppu võib aluseks olla töötaja nõusolek (kui e-posti kasutamise reegleid ettevõttes loodud ei olnud) või e-posti kasutamise reeglite olemasolul tööandja õigustatud huvi.

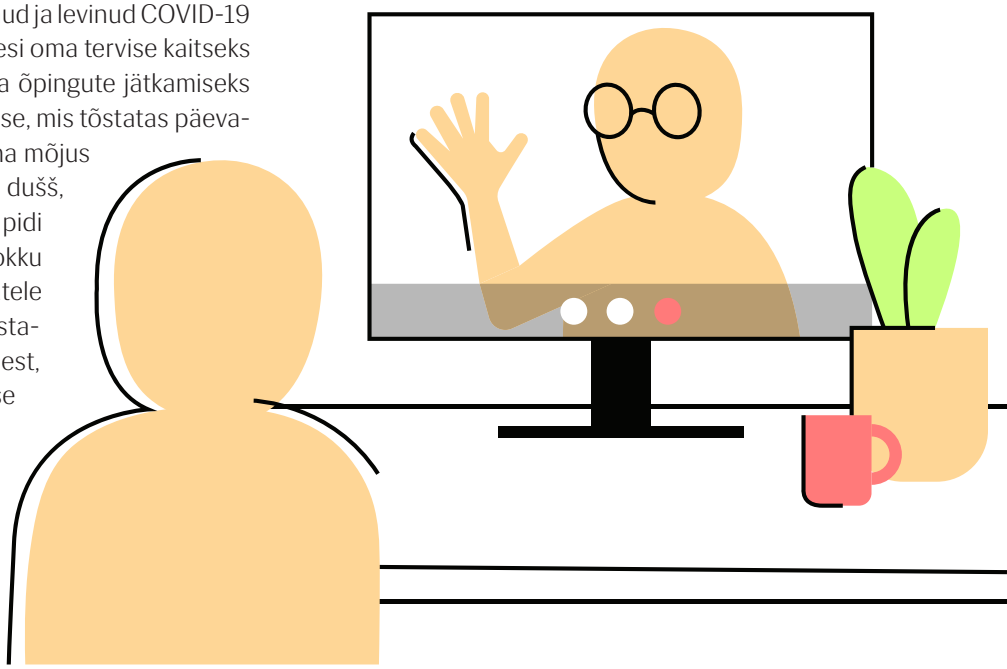
Tööandjal ei ole mingit takistust säilitada ja lugeda töökohustuste täitmisega seotud e-kirju, mis on töösuhte (lepingu) ajal tööalase e-posti aadressi kaudu liikunud. Küll aga ei ole õigust töötaja erakirju avada ega lugeda. Selleks, et vältida või vähendada tõenäosust, et erakirju loetakse, tuleb kehtestada korrektsed reeglid e-postkasti kasutamiseks. Näiteks võib keelata tööalase e-postiaadressi isiklikuks otstarbeks kasutamise ning sätestada reeglid erakirjade eraldi kaustas hoidmise ja kustutamise kohta.

Tuleb märkida, et mida üksikasjalikumalt ja konkreetsemalt on reeglid sõnastatud, seda lihtsam on töötajal nendest juhinduda. Kindlasti tuleb arvestada, et eeskirjadega ei saa tööandja siiski kehtestada selliseid piiranguid ega luua endale õigusi, mis on põhiseaduse või teiste seadustega vastuolus.

Kui e-posti kasutamise reegleid ettevõttes reguleeritud pole ning endine töötaja nõusolekut e-posti avatuna hoidmiseks ei anna, peaks tööandja nimelise e-posti aadressi koheselt pärast töösuhte lõppemist sulgema. Sulgemisega on sealjuures tegemist siis, kui e-postile ei saa kirju kohale toimetada. Kui tööandja ei ole siiski töötaja nimelist e-postkasti sulgenud ja selle jätkuvalt avatuna hoidmiseks puudub õiguslik alus, on inimesel õigus nõuda endiselt tööandjalt oma isikuandmete kustutamist toetudes isikuandmete kaitse üldmääruse (IKÜM) artiklile 17.

# ANDMEKAITSEST KOROONAPANDEEMIA AJAL

Möödunud aastal Eestisse jõudnud ja levinud COVID-19 ehk koroonaviirus sundis inimesi oma tervise kaitseks elukorraldust muutma. Töötamise ja õpingute jätkamiseks tuli paljudel kolida virtuaalruumidesse, mis tõstatas päevakorda andmekaitse teemad. Koroona mõjus ühiskonnas nagu hommikune külm dušš, kuid sellega tuli kiirelt kohaneda. Nii pidi ka inspektsioon oma jõuvarud kokku koguma ja suure hooga täiendavatele tööülesannetele vastu astuma. Aastaraamatusse sai vaid valik teemadest, millega inspektsioon koroonaviiruse saabumisel tegelema hakkas.



## TÖÖANDJAD, TÖÖTAJAD JA TERVISEANDMED

Koroonaviirus tõi inspektsiooni arvukalt selgitustaotlusi töötajate terviseandmete töötlemise teemal. Küsiti nii tervishoiuasutustest, koolidest, tootmis- kui meelelahutusettevõtetest ja mujaltki. Inspektsioon sai anda selgitusi lähtuvalt kehtivast siseriiklikust õigusest. Isikuandmete kaitse üldmäärus (IKÜM/üldmäärus) lubab töösuhte raames terviseandmeid töödelda niivõrd kuivõrd see on lubatud liikmesriigi õigusega, millega on kehtestatud ka asjakohased kaitsemeetmed.

Teave töötaja tervisliku seisundi kohta on eriliigilised isikuandmed, mille puhul rakendub üldmääruse artikkel 9. Seda ka juhul, kui tegemist on kahtlusega, mitte kindla diagnoosiga. Ja ka nohust rääkimine on seaduse mõistes terviseandmete töötlemine.

> *„Terviseandmeid tohib töödelda üksnes üldmääruse art 9 lõikes 2 välja toodud alusel.“*

IKÜM art 9 lg 2 punkt a kõneleb nõusolekust, mille alusel võib tööandja töödelda nii tavalisi kui eriliigilisi isikuandmeid. Põhinõue on, et üldmääruse toodud nõusoleku nõuded on täidetud, sh et tegemist oleks tõepoolest vabatahtlikult antud nõusolekuga. Nõusoleku andmiseks ei tohi töötajale mingit survet avaldada ega talle järgneda mingeid sanktsioone nõusoleku andmata jätmise eest.

IKÜM art 9 lg 2 punkt c kõneleb eriliiki isikuandmete töötlemisest, kui see on vajalik teiste inimeste elulise huvide kaitseks ning andmesubjekt pole füüsiliselt võimeline nõusolekut andma (nt tulenevalt oma haigusseisundist). Teoreetiliselt annab see justkui aluse töötajate teavitamiseks ka ilma nõusolekuta, kuid lähtuda tuleb ikkagi eesmärgipärasuse ja minimaalsuse põhimõtetest. Ehk kui eesmärki on võimalik saavutada teisiti, ei või isikuandmeid edastada.

### Nõuded tööandjale ja töötajale

Tööandja peab tagama ohutu töökeskkonna. Nõuded selleks tulenevad töötervishoiu ja tööohutuse seadusest (TTOS). Samas ei ole antud õigusaktis täpselt reguleeritud, kas ja millist tervisealast teavet võib töötaja kohta koguda. Üldine seisukoht on, et töötaja andmeid tuleks küsida ja koguda nii palju kui vaja ja nii vähe kui võimalik.

*„Töötaja peab silmas pidama, et tööle võib ta asuda üksnes siis, kui ta on terve ning ei kujuta teistele töötajatele ohtu. Tööandjal on õigus küsida, kas töötaja on viibinud hiljuti riskipiirkonnas või kokku puutunud nakatunud inimestega.“*

Sealhulgas on tööandjal õigus nõuda sellekohast kinnitust, mis aga ei tähenda, et tööandjale tuleks esitada täpne diagnoos. Ka sümptomite esinemise infot peaks vahetama vastastikusel mõistmisel.

Tihti soovisid tööandjad kollektiive nakatunutest teavitada ja küsiti, kas tööandja võib saata vastava sisulise teate kõikidele töötajatele, kasutades töötaja nime, kui töötaja on selleks nõusoleku andnud. Terviseandmete töötlemisel tuleb arvestada eesmärgipärasuse, minimaalsuse ja proportsionaalsuse ja õigluse põhimõtetega, sestap jääb arusaamatuks, mis põhjusel on vajalik isiksustatud teate saatmine kõigile töötajatele, kes ei pruugi olla nakatunud töötajaga kokku puutunud.

Nakkushaigega kokku puutunute väljaselgitamine peaks käima selliselt, et tööandja ei anna kogu kollektiivile haigestunust teada, vaid püüab koos haigestunuga lähikontaktsed välja selgitada ning neid teavitada. Samamoodi tuleb toimida ka tööväliste inimestega – nt kui on peetud ühist koosolekut.

Tulenevalt töötervishoiu ja tööohutuse seaduses § 14 lg-st 1 on töötajal mh kohustuseks:

1. osaleda ohutu töökeskkonna loomisel, järgides töötervishoiu ja tööohutuse nõudeid;
2. kasutada ettenähtud isikukaitsevahendeid nõuetekohaselt ning hoidma neid töökorras;
3. koheselt teatada tööandjale või tema esindajale ja töökeskkonnavolinikule õnnetusjuhtumist või selle tekkimise ohust, tööõnnetusest või tööülesande täitmist takistavast tervisehäirest ning kõikidest kaitsesüsteemide puudustest.

Selleks peaks esmalt küsima haigestunud töötajalt endalt, kellega ta potentsiaalselt nakkusohtliku perioodi jooksul on haiguse levikuks piisavas kontaktis olnud ning seejärel nende töötajatega personaalselt rääkima. Kui haigestunud töötajaga pole võimalik ühendust saada, peaks tööandja ise analüüsima, kes võiks lähikontaktsed olla (ühine ruum, toimunud koosolekud).

Tööandja kõigile suunatud hoiatava kiri sisuga „Mart jäi haiguslehele ja pole välistatud, et tal on COVID-19“ pole õigustatud.

*„Teiste töötajate informeerimine haigestunust on lubatud vaid juhul, kui sellise info edastamine teistele töötajatele on vajalik nende elu, tervise või vabaduse kaitseks ning haigestunud töötajalt ei ole võimalik nõusolekut saada.“*

## Miks ei tohi tööandja küsida diagnoosi?

Viiruse diagnoosimine ning lähikontaktsete ja levikuteede väljaselgitamine on arstide ja Terviseameti ülesanne. Seega arst, kes diagnoosib patsiendil koroonaviiruse, peaks ka temalt uurima, kellega ta kokku on puutunud ning edasi saab asjaga tegeleda Terviseamet, kel on õigus sel eesmärgil ka isikuandmeid töödelda, sh neid tööandjalt saada.

Seetõttu juhtis inspektsioon tähelepanu, et ühelgi muul andmetöötlejal ei ole seadusest tulenevat õiguslikku alust ega eesmärki hakata omaalgatuslikult ise lisaandmeid koguma või edastama kellelegi, kel pole õigust neid töödelda.

Nakkushaiguse levikutee ning lähikontaktsete välja selgitamise õigus ja kohustus on seadusest tulenevalt tervishoiuteenuse osutajal (vt NETS[2] § 6 lg 1 p 3) ja Terviseametil (NETS § 18 lg 1 p 1). Viimasel on sel eesmärgil õigus ka isikuandmeid töödelda, sh neid tööandjalt saada.

## ANDMETE TÖÖTLEMINE KOROONA-PANDEEMIA AJAL MEELELAHUTUSASUTUSTES

Inspektsiooni jõudsid mitmed küsimused, kas meelelahutusasutustel on õigus edastada Terviseametile üritusel osalenud inimese andmeid (e-posti aadress, telefon, nimi), kui on alust kahtlustada, et üritusel osales viirusega nakatunud inimene.

Nakkushaiguste ennetamise ja tõrje seaduse § 18 lg 1 kohaselt on Terviseameti ülesanne uurida nakkushaige nakatumise ja nakkushaiguste leviku asjaolusid ning võtta vajaduse korral ühendust nakkushaigete ja kontaktsete isikutega.

Selle ülesande tarvis on Terviseametil õigus küsida ürituse korraldajalt (meelelahutusasutustelt) välja seansil osalenute andmeid, eeldusel, et korraldajal on need isikustatult olemas (nt klient on pileti ostmisel kasutanud kliendikaarti). Neid andmeid võib Terviseamet küsida ikka vaid eesmärgipäraselt, st tuvastamaks seansil osalenu lähikontaktsed. Eelduslikult pole vaja selleks kõikide üritusel osalenute inimeste andmeid.

Küll aga ei ole meelelahutusasutustel õigust ega põhjust omaalgatuslikult hakata edastama ametile kõiki seansil osalenute andmeid. Meelelahutusasutustel puudub võimekus terviseseisundit hinnata selliselt, et tekiks piisav alus mõnd külastajat konkreetselt koroonaviiruses kahtlustada ja teavitada sellest Terviseametit.

## KOROONAVIIRUSESSE HAIGESTUNUTE TERVISEANDMETE VAATAMINE TÕI HOIATUSE

Inspektsiooni töölauale jõudis terviseandmete vaatamisega seoses mitu kaebust Kuressaare Haigla ravijuhi peale, kes oli tervise infosüsteemis teinud inimeste terviseandmete kohta päringuid. Kuressaare Haigla juhatuse korraldusega kohustati hädaolukorras ravijuhti läbi viima auditit haigla infosüsteemis võetud COVID-19 proovide osas. Haigla selgituste kohaselt on Kuressaare Haigla elutähtsa teenuse osutaja, kes peab tagama Saaremaal ka hädaolukorras nii kiirabiteenuse kui haigla teenuse osutamise ja seetõttu oli haiglal vaja teada, kui palju oli Saaremaal positiivse koroonaproovi andnud isikud, et tagada võimekus osutada neile vajadusel meditsiinilist abi.

Tervishoiuteenuste korraldamise seadus ja selle määrused sätestavad väga selgelt, kellel ja millisel juhul on õigus tervise infosüsteemist andmeid vaadata. Läbiviidud järelevalvemenetluse käigus tuvastas inspektsioon, et Kuressaare Haigla juhatuse käskkirjaga kohustati ravijuhti läbi viima eriolukorras auditit, et COVID-19 proovide vastused ei olnud õigeks ajaks haiglasse saabunud ning vaja oli saada ülevaadet Saaremaa valla COVID- haigetest. Arvestades koroonaviiruse pandeemiast tulenenud hädaolukorda ja selle põhjustatud segadust, ning et tegu ei olnud uudishimu päringutega, ei karistanud inspeksioon ravijuhti väärteokorras. Inspektsioon tegi ravijuhile hoiatuse oma volituste ületamise eest.

## KAHE ASUTUSE KOOSTÖÖ VÕIMALIKKUS KOROONAPANDEEMIA AJAL NÕUDIS LAHTI HARUTAMIST

Inspektsioon sai osaleda möödunud aastal nii mõnelgi korral protsessis, mille eesmärgiks on välja selgitada, millised on asutuse pädevused isikuandmete töötlemisel oma ülesande täitmisel. Möödunud aastal aitas inspektsioon lahti harutada ka sellist küsimust, kuidas ja mis alusel üldse edastab Terviseamet koroonasse nakatunute andmed Politsei- ja Piirivalveametile.

Lahenduskäik väärib kirjutamist, sest aastaraamatut loevad kindlasti ka tõsisemad andmekaitsehuvilised.

Vastavalt nakkushaiguste ennetamise ja tõrje seadusele (edaspidi NETS) § 18 lg 1 p 1 on nakkushaiguste ennetamise, seire ja tõrje valdkonnas on pädev asutus Terviseamet, kes muuhulgas teeb epidemioloogilisi uuringuid haige nakatumise ja nakkushaiguste leviku asjaolude väljaselgitamiseks, võtab vajaduse korral ühendust nakkushaigete ja kontaktsete isikutega ning juhendab inimeste rühmaviisilise haigestumise korral tõrjemeetmete rakendamist. NETS § 18 lg 6 sätestab, et NETS-is ettenähtud ülesandeid täites teeb Terviseamet koostööd kohalike omavalitsustega nakkushaiguste ennetamiseks, seireks, leviku tõkestamiseks ja tõrjeks.

Politsei- ja Piirivalveameti (PPA) ülesanneteks on PPVS § 3 lg 1 p 1 alusel karistusseadustiku 9., 12., 13., 16., 17., 21. ja 22. peatükis sätestatud süütegude ennetamine, kui see ülesanne ei ole seadusega antud muu korrakaitseorgani pädevusse ning avaliku korra kaitse korrakaitseseaduses sätestatud alusel ja korras. Sinna hulka kuulub ka karistusseadustiku § 192, mis sätestab nakkushaiguse ja loomataudi leviku põhjustamise normi. Selleks, et antud süütegu ennetada, on vaja PPA-l andmeid Terviseametilt. Ülesanne tuleb hädaolukorraseadusest (HOS), mis pannakse PPA-le HOS §24 lõikega 2.

Kui vaadata politsei ja piirivalve seaduse (PPVS) § 7[46], siis selle kohaselt on politseil sama seaduse § 3 lõikes 1 sätestatud, samuti välislepingust või Euroopa Liidu õigusaktist tulenevate ülesannete täitmiseks õigus töödelda eriseaduses sätestatud arvestades isikuandmeid, sealhulgas eriliiki isikuandmeid ja üldsusele suunatud ja avalikest allikatest kättesaadavaid andmeid. Antud norm on isikuandmete töötlemise volitus, mis eeldab, et seadusest tuleneb ülesanne, mille täitmiseks on vajalik isikuandmete töötlemine. Selle juurde tuleb PPA-le andmete edastamise osas juurde võtta ka halduskoostöö seadus (HKTS) § 18 lg 1 punkt 2, mille järgi võib haldusorgan taotleda teiselt haldusorganilt ametiabi, kui haldusülesande täitmiseks on vaja andmeid, mis haldusorganil puuduvad või mida haldusorgan ei ole võimeline välja selgitama.

*„Terviseamet annab PPA-le nakatunute ja lähikontaktsete andmed, sest PPA-l endal neid pole ning ilma nendeta ei ole võimalik ka seadusest tulenevat ülesannet täita.“*

## VIDEOKOOSOLEKUST KUVATÕMMISED SOTSIAALMEEDIAS TEKITASID MEELEHÄRMI

Koroonapandeemia tõttu pidid paljud tööandjad töökorralduse ümber mängima ja võimaldama kodust töötamist. Olukorras, kus paljud töötasid kodudes ja suhtlus käis tihti videokõnede kaudu, oli uudne oma mõtteid ja tähelepanekuid olukorra kohta sotsiaalmeedias jagada, sageli koos piltidega. Enne aga tuleb vestluskaaslastelt küsida nõusolek või muuta pilti enne postitamist nii, et inimesed ei ole enam äratuntavad. Seega tuli inspektsioonil tegeleda ka lihtsamate meeldetuletustega, rõhutamaks infoturbe olulisust, et kellegi andmed ei lekiks ega satuks avalikkuse ette inimese tahte vastaselt.

## MEEDIA JA KOROONATESTIMISE KAJASTAMINE

Arusaadavalt sai 2020. aasta ka ajakirjanduses suurt tähelepanu koroonakriisiga seonduv. Eriti kevadise esimese laine ajal ilmus tihti pildi- või videoreportaaže koroonatestimise punktidest. Pahatihti jäid aga pildi- või videomaterjali peale äratuntaval moel testima läinud inimesed. Reeglina pildistati autosid, kuid pildile jäid ka autos istunud inimesed. Sellistele piltidele või videotele jäänud inimesed olid sageli sellest häiritud ja soovisid inspektsioonilt abi. Samuti avaldati uudislugu koos mahuka galeriiga kaubanduskeskust külastanud maskita inimestest, kusjuures inimesed olid piltidelt tuvastatavad.

Inspektsiooni jõudis juhtum, kus ühe väljaande ajakirjanik tegi artikli erihooldekodu igapäevaelust ning lisas loole inimest tuvastava pildigalerii seal elanud erivajadustega inimestest. Elanike lähedased said sellisest ajakirjaniku külastusest ja pildistamisest teada alles väljaannet lugedes ning pöördusid kaebusega inspektsiooni poole.

Inspektsioon tegi väljaandele ettepaneku hägustada inimeste näod ja muud inimest tuvastada võimaldavad andmed pildi- või videomaterjalist. Isikuandmeid võib inimese nõusolekuta töödelda ajakirjanduslikul eesmärgil, kui selleks on avalik huvi ja see on kooskõlas ajakirjanduseetika põhimõtetega ning kui isikuandmete avalikustamine ei kahjusta ülemäära inimese õigusi. Riigikohus on selgitanud, et isiku kujutise kasutamine ilma tema nõusolekuta on siiski üldjuhul lubatav vaid selle isiku endaga seotud aktuaalse päevasündmuse kajastamiseks. Sellele lisandub eeldus, et isiku kujutise kasutamine on päevasündmuse kajastamiseks vajalik ning avalikkuse huvi kaalub üles isiku huvi.[1]

*„Inspektsiooni hinnangul ei tulene kohtuotsusest, et päevauudiste taustaks ei või üldse inimesi enam näidata.“*

*„Avalikus kohas juhuslikest inimestest tehtud salvestis koos uudisega ei tohi kokkuvõttes jätta mingil moel muljet nagu käiks uudis salvestiselt nähtuvate konkreetsete inimeste kohta.“*

Tundlikes kohtades (näiteks Töötukassa vastuvõtusaal, haigla, erikool) tuleks uudisloo jaoks pildistada nii, et inimeste eraelu puutumatust ei kahjustataks. Kui sellises kohas pildistades konkreetse isiku vastu puudus avalik huvi, siis peaks ajakirjandus kas pildistama nii, et inimene pole äratuntav või siis andma inimesele võimaluse kaamera vaatevälja jäämist vältida.

Kokkuvõttes ei ole ka ajakirjanduslikul eesmärgil lubatud inimese nõusolekuta isikuandmeid avalikustada ilma, et selle konkreetse inimese andmete avalikustamise vastu esineks avalik huvi. Ilmselgelt oli avalikkuse huvi koroonatestimise jms temaatika kajastamise suhtes, kuid see ei õigustanud seda, et juhuslikult kaamera ette jäänud inimesed olid sellise uudisloo juures äratuntavad.

[1] Riigikohtu otsus kohtuasjas nr 3-2-1-152-09.

## DISTANTSÕPPELE MINEK OLI ANDMEKAITSELISELT KEERULINE

Koroonaviirus tõi haridusvaldkonda uue olukorra ning vaatamata digipädevusele ja tehnilisele valmisolekule tuli kõigil lühikese aja jooksul minna distantsõppele, mis tõi hulgaliselt kaasa ka andmekaitselisi küsimusi. Inspektsioon andis kõigile koolidele suuniseid ning sügisel toimus ka videoseminar haridusasutustele. Distantsõppele minemisel tuli esmalt selgitada, millisel õiguslikul alusel toimub videotunni andmetöötlus ning kümneid teisi juurdepääsu ja salvestamisega seotud küsimusi, mis lühikäsitluses jõuavad ka aastaraamatusse.

Tundide voogedastamine põimõppe ja distantsõppe korral toimub avaliku ülesande täitmiseks ning ei vaja eelnevaid nõusolekuid.

Distantsõppe korral toimub kogu õppetöö virtuaalselt õppetöö korraldamise eesmärgil. Põimõppe korral peaks aga esinema igal korral reaalne vajadus (nt kokkulepe mõne vanemaga, kelle laps peab olema karantiinis, haiguslehel jms). Kooli tuleb enda otsustada, kas üldse ja mis tingimustel kellelegi põimõppe võimalust pakutakse.

Alati on võimalus eemalolevate laste osas kasutada õpetajaga eraldi suhtlust nagu koduõppel või anda ajutiselt järeltöid ja teha nõustamisi. Põimõpet on tehniliselt keerukas läbi viia, sest õpetaja liigub klassis ringi ja pole pidevalt kaamera ees, tema hääl ei kostu mikrofoni, taustamüra segab õpetaja kuulamist. Sellisel viisil õppetöös osalemine ei pruugi anda soovitud eesmärki. Võimalus klassiga videosilla kaudu suhelda aitab siiski eemaloleval lapsel tunda, et ta on osa kollektiivist. Inspektsioon juhtis tähelepanu, et põimõppe võimaluse kasutamiseks igasuguse statsionaarse kaamera paigaldamine klassiruumi ei ole põhjendatud.

Ligipääs otseülekandele saab olla vaid selleks ettenähtud isikutel. Kui teenus võimaldab, võiks juurdepääsu ülekandekeskkonnale täiendavalt kaitsta salasõnaga. Õpetajal peaks olema võimalik veenduda, et ülekannet jälgivad vaid ettenähtud lapsed, sh ei või seda ilma kokkuleppeta jälgida ka lapsevanemad. Õpetaja võib nõuda, et õpilane peab oma videopilti jagama. Kui eesmärk on tunnis osalemine ja tunni läbiviimine, siis puudub põhjendus järele vaatamiseks ja salvestamiseks. Kui õpilane tunnist puudub, siis peaks ka järele vastamine toimuma nii, nagu see toimuks ilma distantsõppeta kontaktõppes.

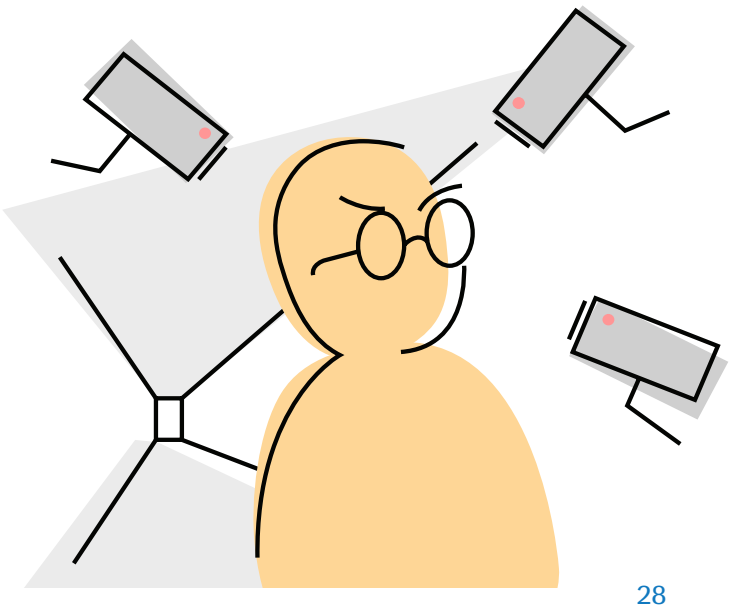
## MIKS ON SAANUD VALVEKAAMERATE KASUTAMISEST TÜLIÕUN?

Inspektsioon sai ka möödunud aastal suurel hulgal nördinud inimeste pöördumisi naabrite videovalve pärast. Konflikti põhjustab enamasti kas teadmatus, kes jälgib või tuntav riive privaatsusele.

„Maja on kaasaomandis ja ühel päeval paigaldas naaber valvekaamera ilma et minult küsiks."

„Kaamerad jälgivad spordiplatsi, aga ma ei tea kelle kaamera see on."

„Naaberkrundil on garaažiboksid ja ühe boksi peale on pandud pika toru otsa kaamera, mis vaatab minu aknasse. Elan teisel korrusel ja tunnen, et minu õigus kodu puutumatusele ja privaatsusele on riivatud."



„Hoonele on paigaldatud valvekaamerate vaatevälja jäävad naaberkrundi aiad. Elanikud ei ole sellega nõus ja nõuame kaamerate kohest maha võtmist.“

2020. aastal alustas inspektsioon süsteemsemat teavitustööd, et videovalvekorraldajad oskaksid arvestada paremini inimeste õigustega ning et tegevus oleks läbipaistev.

Koostöös Riigi Infosüsteemide Keskusega valmis IT-põhise videovalve sildi genereerija. Selleks tuli kaardistada, millised on miinimum teavitusnõuded, mida iga silt peaks sisaldama. Nõuded teavitussildile tulevad isikuandmete kaitse üldmääruse (IKÜM) artiklist 14.

***„Teavitussildile tuleb märkida videovalve eesmärk, seejärel õiguslik alus, vastutava töötleja nimi ja info, kust saab valvealasse jõudev inimene tutvuda andmekaitsetingimustega või küsida oma isikuandmete töötlemise kohta.“***

## VIDEOVALVE ÜHISALAL

Kuna valvekaamera põhjustab sageli tüli ja pahandust korteriühistutes, siis inspektsioon koostas aki.ee veebi põhjaliku artikli selle kohta, kuidas toimida valvekaameratega elamualal (v.t Kaamerate kasutamine elamualadel - www.aki.ee ).

Artikli üks eesmärkidest oli soov panna mõtlema, kas valvekaamera kasutamine täidab eesmärki ning kuidas kasutada kaamerat nii, et sellega ei kahjustata ühiselus kellegi õigust privaatsusele ülemäära.

### Mõned olulisemad asjaolud artiklist

Statsionaarse kaamera kasutamisel saab isiklikul otstarbel filmida vaid juhul, kui filmitakse üksnes enda valduses olevat ala (oma korter või ainult enda korteri uks või enda eramaja ja selle hoov). Sel juhul ei ole vajalik sellest ka kedagi teavitada, küll aga ei või filmitut kasutada muul eesmärgil, kui selleks on isiklik otstarve (nt internetis avalikustada). Seega, statsionaarse kaamera kasutamisel ei ole isiklik otstarve kasutatav avalikul ega ühiskasutuses oleval alal, milleks on tänav, kortermaja trepikoda, kõrvalmaja hoov jne.

Otsuse tegemisel peaks alati hindama ohtude tõsidust ja realiseerumise tõenäosust ning analüüsima alternatiive turvariskide maandamiseks (nt turvauks, signalisatsioon, täiendav valgustus). Näiteks, kui soovitakse kaitsta ühiselt trepikojas hoiul olevaid jalgrattaid, siis on vaja kaamera paigaldada selliselt, et vaatevälja jääb vaid rataste hoiu ala, mis tähendab, et kindlasti ei pea paigaldama kaameraid trepikoja kõikidele korrustele. Kui pärast hindamist selgub, et muud turvameetmed on end ammendanud ja kaamerate paigaldamine on mõõdapääsmatu, tuleb valida selline viis, et sellega ei kahjustata ülemääraselt ühegi korteriomaniku privaatsust (nt kaamera on suunatud ühe konkreetse ukse filmimisele). Valida tuleb, milline on vajalik ala, mis kaamera vaatevälja jääb ning kas kaamera on suumitav ja salvestab lisaks pildile ka heli jms. Helisalvestava kaamera kasutamine vara kaitseks ei ole põhjendatud. Kui eesmärk on tabada teolt võimalikud vargad, siis eelduslikult nad ei räägi kaamera juures ja selline funktsioon ei hõlbusta nende leidmist, vaid kahjustab ülemääraselt muude salvestisele jäävate isikute privaatsust.

***„Euroopa kohtu otsuses nr C-708/18 on öeldud, et töötlemise vajalikkuse tingimuse hindamisel peab vastutav töötleja näiteks hindama, kas piisab sellest, kui videovalve töötab üksnes öösel või väljaspool tavalist tööaega ning kas blokeerida või muuta ähmaseks videokujutised neis kohtades, kus videovalvet ei ole vaja.“***

Ühistu otsus tuleb vastu võtta hääleõiguslikul üldkoosolekul ja ei piisa juhatuse otsusest.

Inspektsioon juhtis tähelepanu, et kaamera maketi või ühendamata kaamera kasutamine loob inimestele mulje, et neid filmitakse, mistõttu peab sellise seadme omanik olema valmis jagama selgitusi nii kaamera ette jäänud inimestele kui järelevalveasutusele.

## VIDEOVALVE LAIENES KA TUALETTI

Inspektsiooni töölauale jõudis kaebusi tualetti paigaldatud kaamerate kohta. Sel põhjusel tegi inspektsioon Rakvere Kroonikeskusele ettekirjutus-hoiatuse tualettidesse paigaldatud kaamerate eemaldamiseks. Kaamerad eemaldati inspektsiooni järelepärimise tulemusena ka Jõhvis asuva Pargi Keskuse tualettruumidest.

Inspektsiooni seisukoht on jätkuvalt, et puhkeruumis, riietusruumis, wc-s ja duširuumis ei ole aktsepteeritav kaameraid kasutada – seda muuhulgas kontorites ja kaubandus- või spordikeskustes. Olukorras, kus eesmärgiks on näiteks hoida ära vandaalitsemist, narkootilise aine käitlemisega või kasutamisega seotud intsidente, tuleb kindlasti kaaluda alternatiivseid meetmeid, mis võrreldes jälgimisseadmete kasutamisega on isikute privaatsust vähem riivavad.

## TÖÖTAJAD TEADMATUSES

Üheks suurimaks probleemiks oli andmetöötluse läbipaistmatus. Töötajaid pole nõuetekohaselt teavitatud ning sageli puudub informatsioon ka töökorralduse reeglites. Isikuandmeid tohib kaamerate kasutamisega töödelda seadusest tulenevatel alustel - näiteks õigustatud huvi alusel või kui kaamerate kasutamise kohustus tuleb eriseadusest. Õigustatud huvile isikuandmete töötlemise alusena saab üksnes siis toetuda, kui andmetöötleja on teostanud töötaja ja tööandja huvide kaalumise ning jõudnud järelduseni, et kaamerate kasutamine ei riiva ülemääraselt töötajate huvisid.

*„Õigustatud huvile isikuandmete töötlemise alusena saab üksnes siis toetuda, kui andmetöötleja on teostanud töötaja ja tööandja huvide kaalumise ning jõudnud järelduseni, et kaamerate kasutamine ei riiva ülemääraselt töötajate huvisid.“*

Üks tähtsamatest nõuetest on videovalve alasse jäävate inimeste teavitamine nii andmetöötluse õiguslikust alusest kui täpsematest valve eesmärkidest, sh tuleb võimaldada töötajatel tutvuda kõigi asjakohaste dokumentidega. Kahjuks näitas ka möödunud aasta, et sageli seda ei tehta, kuigi teavet ja selgitusi peab tööandja suutma töötajatele igal hetkel anda. Samuti peavad väljas olema kaamerast teavitavad sildid. Kuna nendel teemadel tuleb küsimusi ja kaebusi tihti, on inspektsiooni kodulehele lisandunud videovalve korraldajale mitmeid selgitavaid materjale.

Kokkuvõttes peavad tööandjal olema:
(a) dokumenteeritud õigustatud huvi hindamine,
(b) kaamerate kasutamise tingimusi ja eesmärke tutvustavad andmekaitsetingimused ja
(c) teavitussildid.

# ELEKTROONILINE OTSETURUSTUS JA TELEFONIMÜÜK TÕID JÄTKUVALT PALJU KAEBUSI

Möödunud aastal ei saanud otsa spämmimisega seotud mured. Inimeste kaebustest peegeldus, et probleemiks olid jätkuvalt erinevate füüsiliste isikute e-posti aadresside saamine ning nendele e-kirjade saatmine ilma eelneva nõusolekuta. Tihtipeale ei jaganud andmetöötlejad ka selgitusi, kust on saadud tema e-posti aadress ning millisel õiguslikul alusel talle e-kiri saadeti.

Probleeme põhjustasid möödunud aastal ka metsaärimehed, kes helistasid inimestele lootuses osta kinnistut või aidata müüa olemasolevat maatükki.

Andmed maa kohta saadakse kinnistusraamatust ja kõikvõimalikest teistest andmebaasidest. Küll aga on küsitav, et kust kohast saadakse füüsiliste isikute mobiiltelefoninumbreid. Teatud juhtudel saadakse neid äriregistrist, kui keegi on seal oma ettevõttele lisanud oma isikliku numbri, või korteriühistu liikmed jms.
Kuid küsitavusi tekitavad ka olukorrad, mil inimese number ei ole mitte kuskilt avalikult kättesaadav, kuid helistaja teab isegi inimese nime ning et talle kuulub kinnistu. Helistatud on näiteks ka maaomaniku lapsele, teades, et kõne vastuvõtja vanematele kuulub mingi kinnistu. Andmetöötleja ise on huvitaval kombel väitnud seda, et number on genereeritud? Teine standardvastus on, et number on saadud vanast andmebaasist, mida enam ei eksisteeri.


Suvalistest andmebaasidest numbrite kogumine ei ole eesmärgipärane numbri algse avaldamisega. Seega ei saa kõikidest andmebaasidest numbreid koguda eesmärgil neile helistama hakata. Kui number on avaldatud eesmärgiga müüa oma kasutatud autot, siis ei saa helistada ja pakkuda võimalust müüa oma kinnistut või teha reklaami näiteks tolmuimejatele.

Probleeme põhjustasid jätkuvalt ka telefoni teel müüjad, kes helistavadki arvutiga genereeritud numbritele, teadmata, kes kõne vastu võtab. Selliseid kaebusi saabus inspektsioonile samuti, kuid nendega ei ole inspektsioonil midagi ette võtta, kuivõrd kõiki müügikõnesid ei saagi välistada. Küll aga on võimalik lisada sellisel puhul oma number keelunumbrite listi.

Enamat peale selgitustöö ei saa inspektsioon teha ka siis, kui juriidilised isikud pöörduvad inspektsiooni poole murega, et neile saadetakse ilma eelneva nõusolekuta elektroonilist otseturustust. Kui füüsiliselt isikult peab võtma eelnevalt nõusoleku reklaami saatmiseks, siis juriidilisele isikule võib saata seda ilma eelneva nõusolekuta, kuid e-kirjas peab sisalduma keeldumise võimalus elektroonilise võrgu kaudu ehk loobumiselink. Kui peale keelamist siiski saadetakse uus kiri, on tegemist elektroonilise side seaduse nõuete rikkumisega.

Kui Eesti õigusruumis oleks haldustrahv, siis menetlemine oleks kindlasti tõhusam. 2019. aasta aastaraamatus kirjutasime sarispämmijate probleemist pikemalt.

## POLIITIKAKUJUNDAMISE UURINGUTE LÄBIVIIMISSE OODATI ROHKEM SELGUST

Inspektsioon väljastab lubasid poliitikakujundamise uuringuteks. Möödunud aastal väljastati lubasid 32-l korral. Loataotluste menetlemise käigus selgus probleem, et teadusuuringute läbiviijad ei taha andmesubjekte uuringutest teavitada. Põhjuseid on selleks mitmeid, alates ebamõistlikult suurest töökoormusest suurte kulutusteni.

Inimesel kui andmesubjektil tekib aga sellega seoses tunne, et mõnel juhul võib olla uuringu läbiviimise protsess varjatud. Inspektsiooni seisukoht on, et alati ei ole isikute teavitamine vajalik, kuid siiski tuleks vaadata olukorda ka inimeste poolelt – me kõik tahaksime teada, kui meie andmetega midagi tehakse ning selleks on meil ka õiguspärane ootus. Samale asjale on tähelepanu juhtinud ka eetikakomiteed.

Poliitikakujundamise uuringute tegijad peaksid kindlasti vaatama, kui suur on uuringu valim ning hindama inimeste teavitamise võimalust. Eesti poole pealt räägib selle toetuseks ka e-riik ning võimalus inimestega kergesti elektroonilisel viisil suhelda. Seega peaksid poliitikakujundajad siiski võimaluse korral tegema kõik, et inimesi nende andmete töötlemisest teavitada. Kontaktinformatsioon on olemas kas rahvastikuregistris või sageli ka andmekogudes. Inspektsioon on seda meelt, et edaspidi peaksid poliitikakujundamise uuringu läbiviijad rohkem panustama isikuandmete töötlemise läbipaistvuse suurendamisse.

## TAUSTAKONTROLLIDE TEGEMISE ÕIGUSE VÄLJASELGITAMISE MENETLUS: LENNUETTEVÕTE, LENNUJAAM JA KAITSEPOLITSEIAMET

Inspektsioon sai möödunud aastal sekkumistaotluse, kus pöörduja soovis selgust, mis roll on AS Tallinna Lennujaamal Kaitsepolitseiametile (KAPO) lennuettevõtte Regional Jet OÜ läbipääsu loa taotlemise ankeetide läbivaatamisel ning kas selleks on olemas õiguslik alus.

Selline seisukoht on vastuolus andmekaitseliste põhimõtetega. Tegelikkuses tuleb tööandjal üksnes kontrollida krüpteeritud failide konteineri või suletud ümbriku olemasolu. Sama põhimõte kehtib ka riigisaladuse loa taotlemiseks täidetavate ankeetidega.

Inspektsiooniga on samal seisukohal ka õiguskantsler, kes jõudis seisukohale, et kontrollitaval peab olema võimalus esitada ankeet ise otse isiklikult julgeolekukontrolli teostajale, kas krüpteeritult või muul viisil. Olgugi, et julgeolekukontrolli regulatsioon sellist võimalust praegu ette ei näe, siis andmekaitseliselt on see üks ja ainuõige viis.

Viide sellele, et tööandjal on kohustus kontrollida ankeedi vormilistele nõuetele vastavust, tuleb tõlgendada kooskõlas isikuandmete kaitse üldmääruse (IKÜM) ja isikuandmete kaitse seadusest (IKS) tulenevate põhimõtetega. Üheks selliseks põhimõtteks on minimaalsus, mille kohaselt tuleb andmeid koguda nii vähe kui võimalik soovitud eesmärgi saavutamiseks. Riigisaladuse juurdepääsuloa andmise otsustab Kaitsepolitseiamet või Välisluureamet ja inspektsiooni hinnangul ei tohi asutuses või ettevõttes riigisaladust korraldav üksus või isik tutvuda ankeedis olevate eriliigiliste isikuandmetega. Tuleb tõdeda, et Rriigisaladuse ja salastatud välisteabe kaitse kord (RSVKK) § 23 punkt 5 on sõnastatud kehvasti ja vormilistele nõuetele vastavuse kontroll võiks justkui sisaldada ka ankeedi sisu kontrollimist. Siiski, kui tõlgendada seda sätet IKÜM-ist ja IKS-ist lähtuvalt, siis peab vormilistele nõuetele vastavuse kontroll piirnema kõigest failide olemasolu kontrolliga.

Ankeedis tuleb esitada mh väga isiklikke ja tundliku iseloomuga andmeid, nt alkoholi ja narkootikumide tarvitamine (ka ühekordne proovimine), psühholoogi ja psühhiaatri poole pöördumised, hasartmängude mängimine jne. Isikuandmete ankeet sisaldab seega selgelt eriliiki andmeid, mille töötlemine on rangemalt reguleeritud. Mh võib eriliiki andmeteks kvalifitseeruda

ka andmed endiste ja praeguste elukaaslaste kohta, millest saab teha järeldusi seksuaalse sättumuse kohta. Sellest tulenevalt töödeldakse olemuselt väga isiklikke ning sügavalt eraellu tungivaid, IKÜM-i mõistes eriliigilisi isikuandmeid. Seega tuleb eriti rangelt võtta arvesse IKÜM-ist ja IKS-ist tulenevaid isikuandmete töötlemise põhimõtteid. Puuduste tuvastamiseks ei ole vaja tööandja struktuuriüksusel ankeedis olevate andmetega tutvuda, nendele puudustele saab osundada julgeolekukontrolli teostav asutus ise.

Kui ankeedis on puudused, saab menetlusökonoomikast ning minimaalsuse põhimõttest tulenevalt julgeolekukontrolli teostav asutus isikuga otse suhelda. See on kiirem ja koormab osapooli vähem. Veelgi enam – haldusõiguslik suhe tekib taotleja ja julgeolekukontrolli teostava asutuse vahel, mitte julgeolekukontrolli teostava asutuse ja tööandja vahel, sest luba väljastatakse isikule, mitte asutusele või ettevõttele.

Inspektsioon lõpetas menetluse lennujaamale ettekirjutusega, millega kohustas lennujaama edaspidi esitama LennS § 46[9] kohaselt lennuettevõtte töötajate läbipääsuloa taotleja isikuandmete ankeet KAPO-le krüpteerituna või kinnises ümbrikus. Samuti ei ole lubatud lennujaamal teha paberil esitatud ankeedist endale koopiat ning kogutud isikuandmete ankeetide paberkoopiaid oli vaja anda üle KAPO-le või hävitada, kui KAPO neid ei vaja. Lennujaam täitis inspektsiooni ettekirjutuse.

## MIKS MINU TERVISEANDMEID ON VAADATUD?

Koroonapandeemia aasta kasvatas inimeste teadlikkust oma terviseandmete osas ning seetõttu osati rohkem jälgida ka patsiendiportaali logisid, mis pani küsima kas vaatamiseks on ikka olnud põhjust.

Kuid palju kaebusi oma terviseandmete vaatamise pärast patsiendiportaalis tuli möödunud aastal uue teenuse tarkvaralise vea tõttu. Tervise ja Heaolu Infosüsteemide Keskus (TEHIK) lõi koostöös Sotsiaalministeeriumi ja Eesti Perearstide Seltsiga teenuse, kus perearstid saavad tervise infosüsteemist teha nimistupõhise päringu kogu nimistu patsientide osas seoses COVID testi tulemustega. Programm tegi aga tervise infosüsteemi tihedalt regulaarse intervalliga päringuid, mille tulemusel tekkis ebamõistlikult palju logisid.

Inspektsioonil oli antud lahendusega seotud probleemide osas teavitamist täitev roll, kuna paljud inimesed polnud kindlad, kelle poole oma küsimustega pöörduda. Andsime lihtsas keeles edasi TEHIKult saadud infot ning hoidsime ennast olukorraga kursis, et tagada arusaadav ülevaade sellest, kes ning mis põhjusel isikute terviseandmetesse päringuid teeb.

Enamasti sai inspektsioon kinnitada, et „üleliigse“ päringu eesmärgiks ei olnud saada infot konkreetse patisendi kohta, vaid tegemist on lihtsalt süsteemiga, mis kuvab kõigi COVID-19 testi teinute nimed. Seejärel on võimalik logide alusel selgeks teha, kelle terviseandmeid on tervishoiuteenuse osutajad reaalselt vaadanud. Ebaseadusliku terviseandmete töötlemise tõttu algatas inspektsioon ka väärteomenetlusi isikuandmete kaitse seaduse (IKS) § 71 alusel.

Nagu ka varasematel aastatel oli menetluse algatamise põhjus meditsiinitöötajate huvi ennekõike oma sugulaste või tuttavate terviseandmete vastu, mis muutis sageli menetluse emotsionaalseks ning tavapärasest keerulisemaks. Inspektsioon pidi omalt poolt jälgima, et kumbki osapool ei satuks ebavõrdsesse seisu ning tegema kõik selleks, et õigusnormi rikkunud tervishoiuteenuse osutajad saaksid aru oma tegude õigusvastasusest.

Tervishoiuteenuse osutaja ja tervishoiuteenuse osutamisel osalevad isikud ei tohi oma ametipositsiooni ära kasutada. Juurdepääs eriliiki isikuandmetele on mõeldud üksnes tervishoiuteenuse osutamiseks ning erinevalt tervishoiutöötajast ei oma muud inimesed terviseandmetele juurdepääsu. Seetõttu ei ole kuidagi põhjendatud taoline seadusandja võimaldatud „eelise“ ära kasutamine isiklikes huvides.

Menetlustrahvid ei olnud suured, kuid arvestatud on asjaoluga, et üldjuhul said inimesed oma teguviisist aru ning trahvi on kasutatud vahendina, mis tulevikus sarnased olukorrad ära peaks hoidma. Nii mõnelgi juhul oli juba isiku väljakutsumine ütluste andmiseks talle juba piisav karistus.

# PÄRIJA ÕIGUSEST SAADA TERVISEANDMEID

Lisaks terviseandmete põhjuseta vaatamisele pöörduti inspektsiooni poole tervisega seotud küsimustes veelgi. Üheks olulisemaks näiteks võib tuua pärija poolt isiku terviseandmete küsimise. Sageli ei väljastatud haiglate poolt inimestele nende surnud lähedaste haiguslugusid.

Isikuandmete kaitse seaduse (IKS) § 9 kohaselt saab surnud inimese isikuandmeid töödelda pärija nõusolekul. Küsimus tekkis selle tõendamise osas, mida saab teha pärimistunnistusega. Muret tunti, et pärimismenetlus võib kesta kuni 30 aastat, kuid tegemist on tsiviilseadustiku üldosa seadusest tuleneva nõuete aegumistähtajaga ning pärimismenetlus ise kindlasti nii kaua ei kesta.

Siin tuleb sellest aru saamiseks vaadata pärimisseadust, mis ütleb, et pärandi vastuvõtmisega lähevad pärijale üle kõik õigused ja kohustused, välja arvatud need, mis oma olemuselt on lahutamatult seotud parandaja isikuga. Tallinna Halduskohus on oma lahendis 3-20-1519 leidnud, et isikuandmete näol on tegemist õiguste ja kohustustega, mis on seotud pärandaja isikuga. Kohus on selgitanud, et IKS § 9 lg 2 tõlgendamisel tulebki sätet mõista nii, et isikul tuleb esmalt tõendada, et ta on pärija. Seda saab teha pärimistunnistusega. Inspektsioon on varem öelnud, et juhul, kui terviseandmeid vajatakse varem, on pärijaks olemist võimalik tõendada siiski ka pärandi vastuvõtmise avaldusega. Tõsi, see ei tõenda, et isik saab kindlasti vara pärijaks, kuid eelduslikult kontrollib notar juba pärimisavalduse esitamisel, et inimene on üldse pärima õigustatud. Lõpliku hinnangu, millist dokumenti pärimisõiguse tõendina aktsepteeritakse, langetab siiski andmetöötleja (tervishoiuteenuse osutaja, TEHIK jms). Siiski ei pea see kohtulahendi valguses paika ning isikul peab olema surnud inimese terviseandmete saamiseks siiski reaalne pärimistunnistus.

# MIKS TULI PEATADA E-APTEEKIDEST RETSEPTIDE VÄLJAOSTMINE TEISELE INIMESELE?

Eelmise aasta novembri viimasesse päeva jääb e-apteekides teise inimese retseptiinfo avaldamise peatamise otsus, mille tagajärg tõi n-ö välja ühe digilahenduse anatoomia ja näitas, kui keeruline võib olla lahenduse leidmine, kui protsessis on palju osapooli. Lahendust ei ole veel leitud käesoleva aastaraamatu väljaandmise ajaks, kuid olulisemad tegevused kuni tänaseni leiavad kirjeldamist selles artiklis.

2020. aasta novembri lõpus avastas inspektsioon, et kolmes e-apteegis (apotheka.ee, sydameapteek.ee ja azeta.ee) on võimalik tutvuda igaühel suvalise teise inimese isikukoodi sisestades talle välja kirjutatud retseptidega.[1] E-apteeki tuli ID-kaardiga sisse logida ning sisestada teise isiku isikukood, misjärel koheselt kuvati kõik teise isiku väljaostmata retseptid. Seejärel sai retseptiravimi välja osta või ostu sooritamata e-apteegist väljuda. Inimesel, kellele on retsept välja kirjutatud, puudus aga ülevaade, kes ja millal tema retseptiinfot on vaadanud, sest www.eesti.ee vahendusel retseptikeskuse andmejälgijast näeb inimene üksnes seda, milline apteek ja millal tema andmeid on vaadanud. Selles protsessis ei tuvastatud kuidagi, kas teise inimese retseptide (terviseandmete) kuvamiseks sisse loginud kasutajal on õiguslik alus (seadusjärgne või volitatud esindusõigus) retsepti andmeid saada.

Internetipangas ei kujutaks tänapäeval ilmselt keegi ette, et teise inimese arvelduskonto väljavõtet saab näha või veelgi enam- ka tema arvelt makseid teha lihtsalt teise inimese isikukoodi teades. Seejuures retseptide andmed on terviseandmed ehk isikuandmete kaitse üldmääruse (IKÜM) järgi eriliigilised isikuandmed, mis peaksid olema veel hoolikamalt kaitstud.

Inspektsioon hindas ohtu andmesubjektidele väga kõrgeks, mistõttu kasutas erandlikult haldusmenetluse seaduse (HMS) § 40 lõike 3 punkti 1 antud õigust anda haldusakt ilma menetlusosalise vastuväiteid ära kuulamata. 30. novembril 2020 tegigi inspektsioon

[1] Kuvatud infos oli kirjas: retsepti välja kirjutamise aeg, väljakirjutaja nimi, retsepti kehtivusaeg, toimeaine(d) ning viide haigusele (või haiguste rühmale), mille puhul ravimit kastutatakse (nt astmavastased ravimid; aknevastased preparaadid; teised närvisüsteemi toimivad ravimid; südame- ja veresoonkond; urogenitaalsüsteem ja suguhormoonid).

24-tunnise täitmistähtajaga ettekirjutuse peatada e-apteekides isikukoodi alusel inimese kehtivate retseptide loetelu kuvamine teistele isikutele. Ettekirjutuse said OÜ Mustamäe Apteek, Veerenni Apteek OÜ ja OÜ PharmaMint.

Otsuse tagamaade selgitamiseks, tuleb anda esmalt ülevaade, milline on süsteem täna.

Retseptide süsteemi osalised on: patsient, arst ja tema kasutuses olev infosüsteem, tervise infosüsteem (digilugu.ee, patsiendiportaal), retseptikeskus, apteek ja apteegi infosüsteem.[2]

## Süsteemi kirjeldus

Retseptiomaniku eest retsepti väljaostmiseks loodi aastaid tagasi süsteem, mille kohaselt peaks arst retsepti välja kirjutamisel patsiendi tahte alusel määrama kindlaks väljaostja. Valida saab kolme variandi vahel: retseptiomanik ehk isik ise, nimeliselt määratud kolmas isik, määratlemata isik. Teist valikut ehk „nimeliselt määratud isik" saab realiseerida vaid juhul, kui patsient ise on patsiendiportaalis digilugu.ee volitanud konkreetset kolmandat isikut. Retseptile endale pole võimalik märkida retsepti välja ostma määratud volitatud isikuid. Kirjeldatud aastaid tagasi loodud süsteem ei ole paraku praktikas realiseerunud. Retseptikeskuses on vaikimisi määratud retseptiravimi apteegist väljaostjaks „määramata isik". Arstid ega patsiendid ei ole teadlikud, et retsepti väljakirjutamisel üldse eksisteerib valiku võimalus. Patsiendid ei ole teadlikud samuti digilugu.ee volitamise võimalusest.

## Õiguslik vaade

Inimese tervise- (sh retsepti)andmeid võib näha tema ise, tema arst, apteeker, kes retseptiravimit müüma asub ning inimese enda volitusel või nõusolekul keegi kolmas, kelle ta saadab apteeki ravimi järgi. Lapse ja piiratud teovõimega täisealise inimese eest teeb tehinguid seaduslik esindaja, lapsevanem või eestkostja.

Apteekril tuleb tuvastada, kas ravimit välja ostma tulnud inimesel on patsiendi volitus või esindusõigus. Kui patsient on eelnevalt määranud patsiendiportaalis volitatud isiku ning arst on retsepti väljakirjutanud valikuga „nimeliselt määratud isik" või ka „määratlemata", saab e-apteek tugineda patsiendiportaalist apteegile kuvatavatele volituse andmetele ning kuvada/müüa ravimi patsiendi tahteavalduse alusel, mis on selgelt kontrollitav.

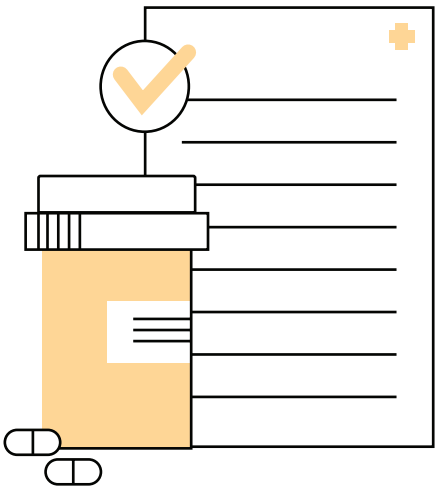
[2] Need on eraõiguslike tervishoiuteenuse pakkujate, perearstikeskuste ja haiglate, endi igapäevatöös kasutatavad infosüsteemid, kust andmed edastatakse riigi keskses andmekokku – tervise infosüsteemi -kokku. Retseptide andmed edastatakse Eesti Haigekassa poolt peetavasse retseptikeskusesse.

Koheselt peale inspektsiooni ettekirjutust võttis teema üles ka Riigikogu sotsiaalkomisjon ning hiljem ka Õiguskantsler. Inspektsioon esitas Sotsiaalministeeriumile lahendusettepanekud:

1) Arstide, apteekrite ja inimeste teadlikkust tuleb tõsta, et retsepti väljaostja liik valitaks teadlikult, mitte vaikimisi ning et inimesed oskaksid patsiendiportaalis volitusi anda;
2) Retsepti väljaostja liiki võiks inimene ka tagantjärele patsiendiportaalis muuta saada;
3) Ideaalis peaks inimene saama volitatud isikuid lisada retseptikaupa (pole aegkriitiline);
4) Arst peaks saama lisada volitatud isikuid retseptile (nt kui inimene ise arvutit ei kasuta ja ta kohe ütleb arstile, kes ravimi välja ostab) ja muuta retsepti väljaostja liiki;
5) Arst peaks saama määrata ise, patsiendi tahteta retsepti väljaostmise viisi, kui ta teab, et patsient on otsusevõimetus olukorras;
6) Rahvastikuregistri päringu abil tuleks luua seadusjärgse esindusõiguse (alaealised, eestkostetavad) kontroll, mis oleks ühtviisi kasutatav nii tavakui e-apteegis;
7) E-apteegis saab retseptiravimeid osta vaid tugeva autentimisvahendiga isikusamasuse tuvastamisel;
8) E-apteek peaks näitama andmesubjektile tema retsepti vaatamiste logisid koos vaataja isikukoodiga;
9) Ravimite kättesaadavuse tagamiseks saab ravimi väljaostmisel kasutada ka digi- ja pabervolikirju.

Kui aga volitatud isikut patsiendiportaalis määratud ei ole, peaks väljaostja muul viisil tõendama esindusõigust. Just siin osapoolte arusaamad lahku lähevadki. E-apteekide pidajad leidsid, et määratlemata väljaostja valikuga retsepti puhul on andmesubjekt andnud eriliiki isikuandmete saamise nõusoleku (või esindusõiguse) määratlemata isikute ringile. Praktikas aga ei ole patsiendi tegelik tahe retsepti välja kirjutamisel selle väljaostja osas kuidagi realiseeritud – keegi ei ole seda välja selgitanud ega fikseerinud. Nii ei saa kuidagi öelda, et patsient oleks andnud oma, IKÜM art 9 lg 2 p a ja art 7 kohase, informeeritud nõusoleku oma eriliigiliste isikuandmete avaldamiseks kolmandatele isikutele.

Inspektsioon ei saa nõustuda, et e-apteek võiks usaldada igaüht, kes väidab endal olevat esindusõiguse (või veelgi enam, selle kontrollimisest üldse vaikimisi mööda minna). Taas pangandusega võrdlust tuues tähendaks see, et pank usaldaks pimesi igaüht, kes pangakontorisse sisse jalutab ja väidab, et tal on õigus teise inimese arvelt raha üle kanda. IKÜMi kohaselt peab apteek kui vastutav andmetöötleja tagama, et ta ei väljastaks eriliiki isikuandmeid õigusliku aluseta.
Lisaks leidis inspektsioon, et kõikide väljaostmata retseptide automaatne kuvamine on ülemäärane.
Menetluse vältel selgus, et osades apteekides antakse igale küsijale ka retseptide loetelude välja trükke.
Kui tõesti füüsilises apteegis on samuti võimalik saada üksnes teise inimese isikukoodi öeldes retseptide loetelu väljatrükk, on ka see seaduserikkumine.
Rahvastikuregistri liidestumise saaksid teha apteegid ise või retseptikeskus tsentraalselt. Kõnealused kolm e-apteeki liidest arendada ei soovinud, vaid ootavad seda riigilt. TEHIK on Õiguskantslerile vastanud, et neil on valmisolek arenduste tegemiseks olemas, kui vaid Haigekassa ja Sotsiaalministeerium konkreetsed arendusvajadused annavad. Haigekassa vastas Õiguskantslerile üldsõnaliselt, et lahenduste leidmiseks on vaja mitme asutuse koostööd. Ravimiameti kirjutas 2021. aasta märtsis, et lähikuudel ei ole näha, et see rahvastikuregistri liidestumise võimalus praktikas realiseeruks, kuigi Eesti Haigekassa otsib lahendusi.



4 kuud pärast ettekirjutuse tegemist ei ole rahvastikuregistriga liidestuse loomine sugugi edasi arenenud. Ehk siis alaealiste ning piiratud teovõimega isikute puhul ei saa realiseerida seadusjärgse esindusõiguse (sh laste puhul ka hooldusõiguse) kontrolli rahvastikuregistri päringute kaudu.

*„2020. aasta osteti välja 10 526 571 retsepti. Neist 2 430 212 osteti teisele isikule (23%). Teistest isikutest omakorda 16% on alaealised.“*

Liidestus rahvastikuregistriga lahendaks ära olukorra pea 400 000 retseptiga seoses.

Turul tegutsevad kolm e-apteeki on enda poolt ainsa lahendusena välja pakkunud, et tehingulise esindusõiguse kontrollimiseks võiks apteeker küsida kontrollküsimusi. Kahjuks jätavad kõik välja pakutud kontrollküsimused üles riski. Nii näiteks ei piisa ravimi või toimeaine nimetuse teadmisest, sest levinud ravimite nimede alusel saaks huvipakkuvate inimeste osas järjest katsetada, kas ta ehk mõnda neist võtab. Samuti võib varasemast teada olla, et inimene on ravimit võtnud. Ka retsepti väljakirjutanud arsti nime teadmine poleks lahendus, sest maapiirkonnas ongi kogu küla peale üks arst.

Eesti Proviisorapteekrite Liit on esitanud Sotsiaalministeeriumile seaduse muudatuse ettepaneku, millega soovis legitimeerida mittemidagitegemise: et kui retsept on väljastatud „määratlemata väljaostja“ valikuga, siis apteeker midagi rohkem kontrollima ei pea.

Mustamäe Apteek OÜ (Apotheka) on ühtlasi vaidlustanud inspektsiooni ettekirjutuse kohtus, kohtumenetlus on pooleli.

Niisiis on käesoleva ülevaate valmimise ajal seis endiselt nukker. Paraku ei saa inspektsioon anda ei e-apteekidele ega riigile korraldust rahvastikuregistri liidestus või muu vajalik arendus ära teha. Valguskiirena paistab siiski üks uus, turule sisenev e-apteek, kes näib võtvat tõsiselt turvaliste lahenduse loomist.

# AVALIKU TEABE SEADUSE TÄITMISEST

Inimestel on õigus teada, mida avalikud asutused igapäevaselt teevad – millist poliitikat järgitakse, missuguseid seaduseid ja regulatsioone valmistatakse ette, missugused on käsilolevad programmid ja projektid, kuidas kasutatakse avalikku raha ning missuguste rahvusvaheliste kokkulepete alal käivad läbirääkimised.

**Avaliku teabe seaduse eesmärk** on tagada üldiseks kasutamiseks mõeldud teabele avalikkuse ja igaühe juurdepääsu võimalus, lähtudes demokraatliku ja sotsiaalse õigusriigi ning avatud ühiskonna põhimõtetest ning luua võimalused avalikkuse kontrolliks avalike ülesannete täitmise üle.

Juurdepääs avalikule teabele on oluline, et inimesed saavad avalikus elus osaleda. Ilma võimaluseta pääseda juurde avalikule teabele ei saa oma arvamusi kujundada ja neid arutada.

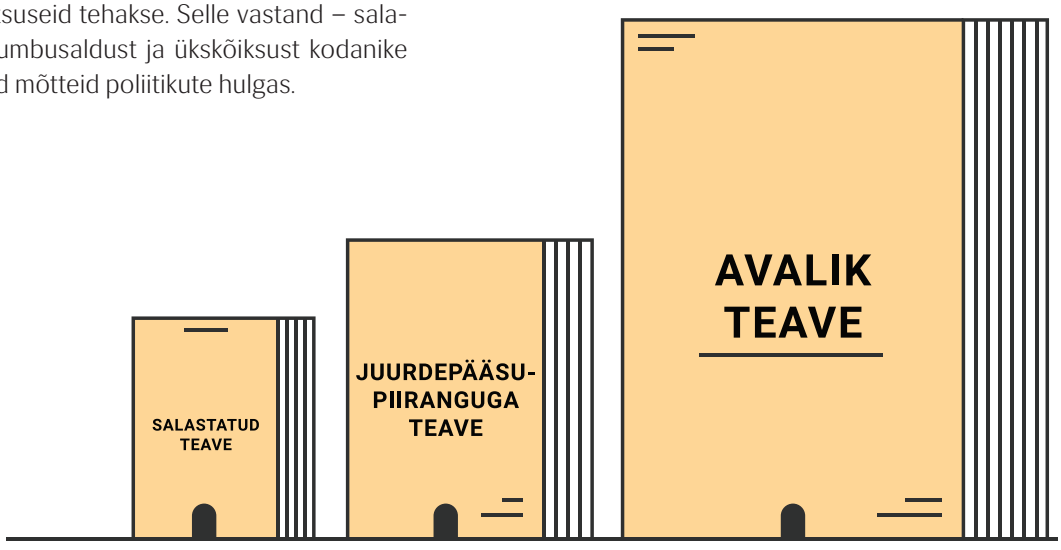
Juurdepääs teabele on olulise tähtsusega ka tagamaks riigiametite avatust ja juurdepääsetavust. Samuti selleks, et asutused töötavad ühiskonna huvides. Ühiskond võib oodata, et valitsus võimaldab juurdepääsu vähemalt teatud teabele, mis selgitab ja õigustab valitsuse poliitikaid ja tegevust. Näiteks, miks võimuesindajad on otsustanud müüa riigiettevõtte või selgitada ja esitada dokumentatsiooni selle kohta, kuidas kavandatav jäätmekäitlusjaam mõjutab keskkonda jms.

Seega on igal isikul õigus saada vähemalt teatud teavet riigiametite tehtud avaliku tähtsusega otsuste kohta. Avatud ja läbipaistev otsuste tegemine on iga demokraatliku süsteemi alus, st kodanikel on õigus teada, kuidas ja miks otsuseid tehakse. Selle vastand – salalikkus – tekitab umbusaldust ja ükskõiksust kodanike seas ning suletud mõtteid poliitikute hulgas.

## Teabe kättesaadavusest

Probleeme avaliku teabe kättesaadavaks tegemisega esines nii riigiasutustel kui kohalikel omavalitsustel. Kui küsida riigiasutuselt avalikku teavet, mis on üldiselt kättesaadav, ei pea teabe küsija selgitama, miks ta mingit teavet soovib. Praktikas on siiski juhtumeid, kus teabevaldaja on jätnud teabenõude täitmata põhjusel, et teabenõudja ei ole põhjendanud, miks ta konkreetset teavet soovib. Samuti on olnud juhtumeid, kus teabevaldaja jätab teabenõude täitmata põhjusel, et leiab, et teabenõudjal puudub soovitu osas teadmise vajadus. Kui tegemist on avaliku teabega, millele ei ole alust juurdepääsu piirata, siis ei saa teabevaldaja teabenõudja eest otsustada ega hinnata, kas ja milleks ta teavet vajab. Teabevaldaja saab keelduda teabenõude täitmisest üksnes juhul, kui tegemist on juurdepääsupiiranguga teabega või teabele juurdepääsuks on eriseaduses ette nähtud erikord, millisel juhul tuleb lähtuda eriseadusest. Samas tuleb olla tähelepanelik, et piiranguga andmed ei saaks avalikuks.

Tänapäeva digitaalne ajastu võimaldab informatsiooni kiiresti koguda, töödelda ja levitada. Kui andmed saavad kord internetis avalikuks, on edaspidi väga raske nende levikut pidurdada. Ei piisa sellest, et avalikustaja need internetist eemaldab, sest need on juba jõudnud mitmete või koguni kümnete tuhandete inimesteni, kes võivad neid töödelda ja levitada. Seega tuleb informatsiooni avalikustamisel väga hästi mõelda, mida ja kuidas avalikustada ning millistele andmetele juurdepääsu piirata.



Kõige sagedamini kasutatav piirangu alus on AvTS § 35 lg 1 p 12 - teave, mis sisaldab isikuandmeid, kui nende avalikustamine võib oluliselt kahjustada isikute eraelu puutumatust.

*„Piiranguga ei ole alati mitte iga isiku nimi, vaid sellise teabe avalikustamine peab oluliselt kahjustama isiku eraelu puutumatust.“*

Inspektsioon nõustub, et iga isikuandmete avalikustamine riivab mingil määral kellegi eraelu puutumatust, kuid piirangu kehtestamiseks peab olema tegemist siiski olulise riivega. See on kaalutlusotsus, mida tuleb alati hinnata ja vajadusel oma otsust ka põhjendada. Kui aga valimatult kehtestada piirang kõikidele dokumentidele, mis sisaldavad kellegi nime, siis võiks põhimõtteliselt kõikidele dokumentidele kehtestada juurdepääsupiirangu, mis ei ole kindlasti eelnimetatud sätte ega ka seadusandja mõte. Kuna eeltoodud sätte puhul on tegemist kaalutlusotsusega, siis ei saa inspektsioon asutuste eest otsustada piirangu kehtestamise vajaduse üle.

Jätkuvalt sai inspektsioon küsimusi, et kas ühele või teisele dokumendile peaks piirangu kehtestama. Sellistel juhtudel saab asutust ainult nõustada, mida tuleks kaaluda või arvestada, kuid lõppotsus tuleb siiski asutusel endal teha. Lisaks isiku nime esinemisele dokumentides tuleb piirangu kehtestamisel hinnata siiski kogu kirja sisu. Ka juhul, kui dokument ei sisalda ühegi isiku nime, kuid on kirjeldatud väga täpselt mingi sündmuse asukohta ja sündmuses osalenud isikuid, võivad isikud olla tuvastatavad ka muude andmete kaudu. Sellise dokumendi avalikustamisel võib saada nende eraelu oluliselt riivatud

## Dokumendiregister

Küsimusi on tekitanud ka olukord, kus seadus ei luba dokumendiregistri avalikus vaates avalikustada andmeid füüsiliste isikute kohta, kuid dokumendile, mis sisaldab füüsilise isiku nime ei ole alust juurdepääsupiirangut kehtestada. Siin tuleb arvestada asjaoluga, et dokumendiregistri avalikust vaatest peab olema võimalik teha otsingumootori abil ületekstiotsinguid, mis tähendab, et otsinguid peab saama teha kõigi dokumendiregistri metaandmete alusel. Kui dokumendiregistri avalikus vaates oleksid avalikud ka füüsilisest isikust saaja/saatja nimi, siis oleks ühe otsingu abil võimalik saada ülevaade kõigi selle isiku poolt edastatud pöördumistest ja talle edastatud dokumentidest, mis muudaks isiku kergesti profileeritavaks. Kui aga otsida dokumente näiteks ainult pealkirja järgi, siis saamaks teada, millised dokumendid puudutavad just konkreetset isikut, tuleks kõik need dokumendid avada ja ka sellisel juhul saab teada ainult seda, kas isik on konkreetseid dokumente saanud/saatnud.

*„Füüsiliste isikute nimede mitte avalikustamine dokumendiregistri avalikus vaates väldib isikute profileerimist.“*

Isikute nimede mitteavalikustamine saaja/saatja andmetena dokumendiregistris kaotab aga oma mõtte, kui saaja/saatjana on märgitud küll eraisik, kuid samas on dokumendi pealkirjas isiku nimi avalik. Sellised eksimusi on just sotsiaalvaldkonda puudutavates dokumentides, kus võib riive olla just suurem. Seda tingib eelkõige see, et enamik ametnike registreerib oma dokumendid ise, kuid ei olda teadlikud, millised dokumendiregistri sisevaate väljad kuvatakse dokumendiregistri avalikus vaates või ei pöörata sellele tähelepanu. Selliste eksimuste avastamisel on inspektsioon probleemile ka möödunud aastatel korduvalt teabevaldajate tähelepanu juhtinud.

## Ärisaladus

Teiseks sagedamini kehtestatavaks piirangu aluseks on olnud AvTS § 35 lg 1 p 17. See on teave, mille avalikustamine võib kahjustada ärisaladust. Üsna levinud on olukord, kus eraõiguslike juriidiliste isikutega sõlmitud lepingusse kirjutatakse sisse konfidentsiaalsuskohus ning teabenõude korral keeldutakse lepingute väljastamisest viitega ärisaladusele. Siiski tuleb märkida, et mitte igasugune teave ei saa olla avaliku sektori asutusega lepingu sõlminud ettevõtte ärisaladus. Ärisaladusel on oma kindlad tunnused, millele see peab

vastama. Samuti peab ettevõte, kes sõlmib avaliku sektori asutusega lepinguid või esitab avaliku sektori asutusele mingeid dokumente, arvestama sellega, et avaliku sektori asutus ei saa ettevõttega kokku leppida teabe konfidentsiaalsuses. Avaliku sektori asutus saab teabele juurdepääsu piirata üksnes juhul, kui selleks on seadusest tulenev alus. Nii näiteks ei saa ükski leping olla täies ulatuses kaetud ärisaladusega. Kindlasti on avalikud lepingus osalevad pooled, lepingu ese ja teenuse osutamise lepingute puhul ka lepingu summa. Kui leping sisaldab ka vaidluste lahendamise korda, väärамatu jõu kohta käivaid sätteid jms, siis ei saa ka sellised lepingu osad olla kaetud ärisaladusega.

*„Üsna tihti saab inspektsioon vaideid, kus jäetakse teabenõue täitmata põhjusel, et teine lepingu pool on seisukohal, et kogu teave on ärisaladus ning teabevaldaja ei ole üldse hinnanud, kas ja mis soovitud dokumentides on ärisaladus.“*

Reeglina lõpevad sellised vaidlused ettekirjutusega, kus teabevaldajal tuleb hinnata soovitud dokumentides ärisaladuse esinemist ja ulatust.

Inspektsiooni menetluses oli eelmisel aastal ka selline vaie, kus teabeavaldaja tunnistas dokumendid AvTS § 35 lg 1 p 17 alusel piiranguga teabeks, kuigi ettevõte ise leidis, et kõik dokumendid ei sisalda tema ärisaladust. Et piiranguid ei kehtestataks igaks juhuks, soovitab inspektsioon enne lepingute sõlmimist lasta ettevõttel ära märkida, mida käsitletakse mingis dokumendis ärisaladusena. Isegi juhul, kui seda pole võimalik küsida dokumentide edastamise käigus ning dokumendile on piirang kehtestatud, siis teabenõude korral tuleb teabevaldajal siiski välja selgitada, kas ja millises konkreetses dokumendis on ärisaladus. Vajadusel tuleb küsida selleks selgitusi teiselt osapoolelt.

Möödunud aastal tekitas üllatavalt palju segadust, millisel juhul on tegemiste teabenõudega avaliku teabe mõistes ja millisel juhul enda kohta andmete küsimisega isikuandmete kaitse üldmääruse mõistes. Kui enne üldmääruse kehtima hakkamist ei tekitanud see probleeme põhjusel, et mõlemal juhul oli vastamise tähtajaks viis tööpäeva, siis pärast jõustumist tuleb enda andmete küsimisele vastata kuu aja jooksul. Nii mõnigi kord esitati kaebus enda andmete küsimise korral peale viie tööpäeva möödumist.

## VAIDEMENETLUSTEST

Möödunud aastal esitati tavapärasest rohkem vaideid inspektsiooni enda menetluste lõpetamise otsuste peale. Kaebaja ei olnud rahul menetluse lõpetamisega ja leidis, et inspektsioon peaks tegema teabevaldajale ettekirjutuse. Silma jäi just see, et kaebajatele on järjest olulisem see, et andmetöötleja saaks tingimata karistada. Tihti ei ole ka oluline, kas andmete töötlemine lõpetatakse või ei. Nii näiteks oli inspektsiooni menetluses vaideid, kus inspektsioon ei olnud rahuldanud vaide esitaja kaebust oma andmete küsimise osas, kuna see oleks kahjustanud teiste isikute õigusi. Vaide esitaja leidis, et kuna kirjavahetus on inspektsioonile edastatud, siis peaks inspektsioon selle talle edastama. Inspektsioon jättis vaide rahuldamata põhjendusega, et õigus saada juurdepääsu oma isikuandmetele ei ole absoluutne, vaid kaaluda tuleb isiku õigust saada enda kohta käivaid andmeid ning teise isiku õigust arvamusvabadusele ja eraelu puutumatusele.

*„Kui vaide esitajat puudutavate andmete väljastamine võib riivata teiste isikute õigusi, siis ei väljastata isikule ka tema kohta käivaid andmeid (Isikuandmete kaitse üldmääruse artikkel 15 lg 4).“*

Samuti ei küsi inspektsioon kaebaja eest asutustelt tema kohta käivaid andmeid ning ei vahenda neid kaebajale. Inspektsioon kontrollib andmete väljastamisest keeldumise õiguspärasust ning rikkumise tuvastamisel kohustab asutust andmed väljastama.

# TEABENÕUETELE VASTAMINE

Aasta aastalt on kasvanud kodanike arv, kes esitavad asutustele hulgaliselt teabenõudeid ning kui tähtaegselt või soovitud kujul vastust ei saa, siis esitavad vaide inspektsioonile. Iseenesest on igal isikul õigus teabenõudeid esitada, kuid kui see on saanud kellegi nn „täiskohaga tööks", siis tekib küsimus, kas sellisel kujul teabe küsimise võimaldamine on ikka olnud seadusandja eesmärk? Olenemata eeltoodust on teabevaldajal siiski kohustus teabenõuetele vastata. Selleks tuleb alati hinnata, mida teabenõudja oma teabenõudes on soovinud ning kas tegemist ikka on teabenõudega  või on hoopis selgitustaotlusega.

Kui teabevaldaja keeldub teabenõude täitmisest, siis tuleb seda ka põhjendada, nii ütleb AvTS § 23 lg 3. Seega ei saa pidada põhjendatuks keeldumist, kui teabevaldaja keeldub teabenõude täitmisest põhjusel, et teabele kehtivad juurdepääsupiirangud. Selliseid keeldumisi on praktikas üsna tihti, kus ei vaevuta hindama, kas ja mis osas dokumendile piirangud kehtivad. Teabevaldajad saavad keelduda teabe väljastamisest ainult juhul, kui keeldumiseks on seadusest tulenev alus.

***„Kui dokumendid sisaldavad mingis osas piiranguga teavet, ei tähenda seda, et dokumente teabenõude korral ei väljastata. Sellisel juhul tuleb väljastada see osa teabest või dokumendist, millele piirangud ei laiene (AvTS § 38 lg 2)."***

Samuti on üheks levinud rikkumiseks tähtaegselt teabenõudele vastamata jätmine. Juhul, kui kodanik on pealkirjastanud oma pöördumise „Teabenõue", kuid sisult on tegemist selgitustaotlusega, tuleb sellisele pöördumisele vastata viie tööpäeva jooksul, keeldudes teabenõude täitmisest ja selgitada, et tegemist on selgitustaotlusega. Kodanik ei pea teadma, millal on tema pöördumise puhul tegemist selgitustaotlusega ja millal teabenõudega. Küll aga peab seda teadma teabevaldaja. Kuigi eeltoodud probleemist on aastaid räägitud, oli see jätkuvalt kõige suurem vaiete esitamise põhjus.

Eelmisel aastal oli ka mitmeid juhtumeid, kus teabenõudja adresseeris oma teabenõude just konkreetsele ametnikule ja nõudis, et just see ametnik talle vastaks. Kuna teabevaldjaks on asutus, mitte tema töötaja, siis ei saa teabenõudja eeldada, et talle vastaks just see ametnik, kellele ta teabenõude esitas. Ka võib selline konkreetne ametnikule esitatud teabenõue tuua kaasa selle, et teabenõudele jääb vastus tähtaegselt saamata. Seda põhjusel, et kui isik viibib näiteks puhkusel või on haige või on tal jäänud teabenõue tähelepanuta. Kui teabenõuet ei ole saadetud ka asutuse üldisele meilile, siis  ei saa ka asutus tagada teabenõudele tähtaegselt vastamist. Eeltoodu ei tähenda seda, et ametnike e-posti aadressidele ei tohiks teabenõudeid saata, kuid soovitatav oleks see lisaks saata ka asutuse üldisele meilile.

# KOHALIKUD OMAVALITSUSED SEIRES

Möödunud aastal viis inspektsioon läbi järjekordse seire kohalike omavalitsuste veebilehtede ja dokumendiregistrite ülevaatamiseks ja puuduste tuvastamiseks. Seire viidi läbi ajavahemikus 26.08 - 21.09.

Eesmärgiks oli vaadelda, kuidas omavalitsused täidavad avaliku teabes sätestatud teabe avalikustamise nõudeid. Valiku tegemisel, millise teabe avalikustamist kontrollida sai lähtutud ka sellest, mille osas on esitatud kaebusi, mis on seaduses muutunud ning millise teabe leidmine võiks olla kodanikule oluline. Samuti kaardistada üldist teabele avalikustamise olukorda omavalitsustes.

Lisaks pidas inspektsioon vajalikuks hinnata dokumendiregistris dokumendile juurdepääsu võimaldamise ja AK (asutusesiseseks kasutamiseks) teabe kaitsmise olukorda.

Seire käigus vaadati:

1. Kas andmekaitsespetsialisti (AKS) andmed on leitavad võrgulehelt, äriregistrist?
2. Andmekaitsetingimuste avalikustamine.
3. Riigihangete avalikustamine, sh hankeplaani ja hankekorra leitavust.
4. Volikogu õigusaktide ja protokollide avalikustamist.
5. Eelarve avalikustamist.
6. Personalikäskkirjade avalikustamist (puhkus, lisatasud).
7. Sotsiaaltoetuste andmise kordade, sh avalduste vormide leitavaust.
8. Dokumendiregistri kaudu e-kirjadele juurdepääsu.
9. AK märgete kajastamist dokumendiregistris ja AK teabele juurdepääsu võimaldamist.
10. Füüsiliste isikute nimede avalikustamist dokumendiregistris.

Kuna alates 15.03.2019 ei luba AvTS § 36 lg 1 p 9 tunnistada asutusesisesiseseks kasutamiseks mõeldud teabeks dokumente riigi, kohaliku omavalitsuse üksuse või avalik-õigusliku juriidilise isiku eelarvevahendite kasutamise ning eelarvest töölepinguga töötavatele isikutele makstud töötasude ning muude tasude ja hüvitiste kohta, siis seires vaadati, kas ja kuidas omavalitsused avalikustavad nii puhkuste kui lisatasude ja preemiate maksmise käskkirju.

Inspektsioon kontrollis väljapool seiret veel pisteliselt detailplaneeringute avalikustamist, dokumendiregistris metaandmete korrektsust ja teavet veebilehtedele ligipääsetavuse kohta kas eriolukordades või kui veebikülastaja ei saa infot tarbida tavapärases tähenduses.

## Kokkuvõte

Kokku oli võimalik saada maksimaalselt 10 punkti. Maksimumpunktid sai Põlva Vallavalitsus, kelle osas pistelise kontrolli käigus puudusi ei tuvastatud.
9,75 punkti said 3 valda, kelleks olid Mustvee Vallvalitsus, Põltsamaa Vallavalitsus ja Jõhvi Vallavalitsus
Seire käigus anti asutustele ka värvid vastavalt seire tulemustele. Nii said rohelise värvi asutused, kelle tulemuseks oli 8-10 punkti, kollase värvi said need asutused, kelle tulemuseks oli 5 – 7,75 punkti ning alla viie punkt saanud asutused oleksid saanud punase värvi. Seekord seire tulemusena keegi siiski punast värvi ei saanud. 79-st omavalitsust said rohelise värvi 42 omavalitsust ning 37 omavalitsust said kollase värvi.

Seire tulemustega saab tutvuda www.aki.ee.

# VAIETEST

## Pakendikomisjoni protokollide väljastamine

Juhtum leiab aastaraamatus käsitlust seetõttu, et asutus jättis väljastamata teabenõudjale protokollid, mis olid asutusesiseseks kasutamiseks mõeldud.

Juhtumiga[1] saab tutvuda www.aki.ee menetluspraktika all, kuid kokkuvõttes leidis inspektsioon, et pakendikomisjoni protokollide mitteväljastamisel ei saa lugeda piisavaks põhjenduseks, kui Keskkonnaministeerium (asutus) piirab juurdepääsu AvTS § 35 lõike 2 punktiga 3 - põhjendatud juhtudel asutusesiseselt adresseeritud dokumendid, mida dokumendiregistris ei registreerita (arvamused, teated, memod, õiendid, nõuanded jm). Mõjuvad põhjendusi, miks juurdepääsu piirata vaja oleks, teabevaldaja ei esitanud.

Protokollide väljastamisel saab anda teabevaldaja vastava selgituse lisaks, mis peaks välistama arvamuse, et komisjon on protokolliga teinud ka otsuseid.

Lisaks oli teabenõudja teadlik, et tegemist on nõuandvate soovitustega ning ta sooviski vaadata, mis osas on minister nõuandva kogu arvamusega arvestanud. Teatud juhtudel võib olla oluline, et avalikkusele on loodud võimalus tutvuda ka otsust mõjutavate arvamuste ja soovitustega, mis aitab teha riigi otsused oma kodanikele läbipaistavaks ja kontrollitavaks.

Inspektsiooni kohustas asutusel väljastama pakendikomisjoni protokollid.

## Dokumendi kavandile seatud juurdepääsupiirang

Keskkonnaagentuurile tehtud ettekirjutus-vaideotsuses[2] leidis inspektsioon, et teabevaldaja on valesti tõlgendanud avaliku teabe seaduse (AvTS) § 35 lg 2 punkti 2.

Keskkonnaagentuur leidis, et alaliste proovitükkide koordinaadid on dokumendi kavand, kuna neid andmeid kasutatakse jätkuvalt ka tulevikus. Koordinaatidega proovitükid on juurdepääsupiiranguga teave, kuna need andmed kuuluvad dokumendi (milleks on SMI uuring) juurde enne selle dokumendi vastuvõtmist (samadele andmetele tuginedes avaldatakse ka SMI uuringud tulevikus). Lisaks väitis Keskkonnaagentuur algselt, et ka ajutiste proovitükkide asukohad on seotud alaliste proovitükkide asukohaga. Hiljem viimasest väitest loobuti.

Ettekirjutusega kohustas inspektsioon teabevaldajal väljastada ka alalised inventuurid või leida muu õiguslik alus nende juurdepääsu piiramiseks. Dokumendi kavandile saab kehtestada vajadusepõhiselt juurepääsupiirangu, aga selle eeldusteks on, et piirang kehtib vaid kuni dokument on vastu võetud või allkirjastatud ehk dokumendist on valminud lõplik versioon, mida enam ei muudeta. Seega, kui küsitud teave ei ole oma loomult enam muutmisjärgus, vaid lõplikult kinnitatud dokument, ei saa sellist piirangu alust kasutada kõikide olemasolevate ja tulevaste (alates 1999. aastast kuni käesolevani) metsainventuuride koordinaatide kohta.

> *„Teabe väljastamine tähendab ka väljavõtte tegemist olemasolevast teabest, olenemata millisel kujul või teabekandjal teave asub. See tähendab, et avalik teave võib asuda ka muudel andmekandjatel ja olla kättesaadav muul viisil.“*

Antud juhul tähendas see küsitud teabe väljavõtmise võimalust läbi vastava päringu ning ei eelda, et küsitav teave peaks juba küsitaval kujul enne teabevaldajal dokumendina olemas olema.

Inspektsioon leidis, et eelkõige peaks dokumendi kavandi kasutamise juurdepääsupiirangu alus tagama selle, et kavandijärgus olev teave ei lähe aktiivselt avalikuks, mis võimaldaks selle laialdase jagamise nii, et teabe saajal ei oleks enam selgust, kas saadud teave on õige. See aga ei tähenda seda, et teave ei võiks olla huvitatud isikutele teabenõude korras kättesaadav.

Keskkonnaagentuur tegi ajutiste SMI proovitükkide asukohad avalikuks.

[1] nr 2.1.-6/20/12
[2] nr 2.1.-3/20/3918 l

## Ärisaladus

Inspektsioonini jõudis üks avalikkust huvitav vaie, kus Rahandusministeerium keeldus AS-ile Ekspress Meedia ärisaladuse tõttu väljastamast Eesti riigi ja advokaadibürooga Freeh Sporkin & Sullivan vahel sõlmitud lepingut ja selle lisasid.

Ärisaladuse aluse kasutamine ei anna alust teabe väljastamisest keeldumiseks, vaid õiguse katta ärisaladust puudutav osa (laused või lauseosad) eelnevalt kinni. Ärisaladus ei saa olla tunnetuslik, vaid peab vastama ebaausa konkurentsi takistamise ja ärisaladuse kaitse seaduse § 5 lõikes 2 toodud tingimustele.

Inspektsioon tegi vaideotsus ja ettekirjutus-hoiatuse[1] kus leidis, et kuna ministeerium teabevaldajana kehtestab dokumentidele juurdepääsupiirangud, peab ta ka suutma hinnata ja põhjendada, kuidas sellise teabe avalikustamine ettevõtja ärihuve kahjustab (küsides vajadusel selleks neilt selgitusi oma). Pärast inspektsiooni sekkumist teave suures osas siiski väljastati ning ministeerium tunnistas, et juurdepääsupiiranguga teabe osakaal on vähene.

[1] nr 2.1.-3-20-2309

# ÕIGUSLOOME ARENGUD

2020. aasta oli väga viljakas eelnõude osas, mille kohta paluti inspektsioonilt arvamust. Kavandatavate õigusaktide muudatusi tuli pea kõigist ministeeriumitest. Kõige rohkem esitas eelnõusid arvamuse saamiseks Sotsiaalministeerium. Ka Siseministeeriumis ning Majandus- ja Kommunikatsiooniministeeriumis oldi viljakad ning lisaks saadeti inspektsioonile eelnõusid rahandus-, justiits-, haridus- ja teadus- ning keskkonnaministeeriumist.

Üldiselt küsiti möödunud aastal kõige enam arvamust õigusaktide muudatustele, mis puudutasid andmekogusid – olgu need muutused siis seaduse või põhimääruse tasandil. Nii saabki öelda, et kõige enam märkusi on tulnud teha andmekoosseisude osas – miks mingeid andmeid kogutakse ja miks just selliseid andmeid. Aga ka kogumise eesmärkide ja säilitamistähtaegade osas. Andmekoosseisud kipuvad eesmärgiga seonduvalt liialt laiaks minema, samuti ei ole selge, kuidas mingid koguda soovitud andmed andmekogu eesmärki saavutada aitavad või sellega sootuks kooskõlas on. Säilitamistähtaegade osas tuli tihti aga tähelepanu juhtida sellele, et need on liiga pikad või ei suudeta põhjendada, miks just sellise tähtajaga säilitada soovitakse. Niisiis, läbivaks mureks andmekogude eelnõude juures oli igaks juhuks kogumine.

## Kitsaskohad

Ilmselt valmistab õigusloojatele muret see, et õigusakti, eriti seaduse, muutmine on pikk ja keerukas protsess, mistõttu soovitakse võimalikult palju olukordi tuleviku tarbeks ette näha. Nii aga tekivadki inspektsioonil küsimused, miks mingeid andmeid nii kaua säilitada soovitakse või üldse kogutakse. Vastust tihti ei saa ka seletuskirjast. Näib, et alati ei mõisteta, mis eesmärki kannavad endas selged sätted ja võime omi valikuid seletuskirjas põhjendada. Inspektsiooni kohustus on jälgida, et õigusloojad jälgiksid andmetöötluses andmekaitse aluspõhimõtteid – seaduslikkus, eesmärgipärasus, läbipaistvus ja minimaalsus. Õigusaktid – olgu need siis seadused või andmekogude puhul põhimäärus- peavad andma isikule vastuse, mis andmeid tema kohta kogutakse, miks kogutakse ja mis eesmärgil kogutakse. Vahel jääb mulje, et selgitusi annavad õigusloojad iseendale või äärmisel juhul teistele kooskõlastusringis olevatele asutustele. Nii on selgitused kas liialt keerukalt kirjutatud või napisõnaliselt, et sellest ainult asjasse pühendatud aru saavad. Ent adressaadiks on ju andmesubjektid ehk inimesed.

Samuti kipuvad andmekaitsealased mõjuhinnangud kas puuduma või olema samuti napisõnalised. Sestap on tulnud mitmel korral tähelepanu juhtida vajadusele just andmekaitsealast mõjuhinnangut täiendada. Mõju inimeste privaatsusele kiputakse hindama ka pigem väiksemaks, kui see inspektsiooni hinnangul tihtipeale on.

Suur probleem näib jätkuvalt olema Riigi Infosüsteemi Haldussüsteemis ehk RIHA-s andmekoosseisude muudatuste kooskõlastamised.

> *„Enamikel juhtudel, kui muudatus puudutab andmekogu põhimäärust, oli inspektsioon sunnitud tegema märkuse selle kohta, et RIHA uuendused on tegemata.“*

Näiteks terviseinfosüsteem (TIS), mida möödunud aastal muudeti kolm korda ning mida kavandatakse 2021. aastal taaskord muuta, ei ole andmestike osas kooskõlastusi RIHA-s tehtud aastast 2014. Lisaks eelnevale esineb tihti mõistete ebaselgust – kord kasutatakse mingi asja kohta üht ja siis teist mõistet või jäetakse lahti seletamata, mida mingi mõiste all silmas peetakse. Taaskord võib näha, et eelnõu väljatöötajad on oma teemas niivõrd nö sees, et unustatakse ära õigusakti adressaadid ehk meie inimesed.

Eelnevalt sai juhitud tähelepanu juba sellele, et tihtipeale soovitakse andmeid säilitada väga kaua, ega osata selgitada, miks selline säilitustähtaeg valitud on. Lisaks aga võis näha eelnõudes probleeme ka sellega, et sätestamata oli jäetud, mis juhtub andmetega siis, kui säilitustähtaeg möödub. Kas andmed kustutatakse või säilitatakse mingil muul viisil, näiteks anonüümsetena arhiivis ja juhul, kui seda tehakse, siis omakorda, kui kaua.

Eelnev võttis üldistavalt kokku tähelepanekud inspektsioonile kooskõlastamiseks saadetud eelnõudele. Mõistagi mõjutas eelmist aastat COVID-19 viirusest tulenev kriis, kuid nagu täna juba öelda võib, jätkub see veel ka käesoleval aastal. Kuivõrd tegemist on eelkõige tervishoiukriisiga, siis kõige suuremat mõju avaldas see ka tervishoiu valdkonna õigusaktidele, sest ilmnesid mitmed puudujäägid õigusraamistikus. Ühelt poolt on see mõistetav, sest mitmed seadused nagu näiteks ka hädaolukorra seadus oli ju selle loomisest peale nö riiulil seisnud, kuid nüüd tuli seda rakendama hakata ja nagu selgus, polnud seda luues suudetud üldse mõelda sellisele kriisile nagu meid nüüd kevadel 2020 tabas. Seega on ühelt poolt arusaadav, et avastati puudujääke nii tervise infosüsteemi regulatsioonis kui ka nakkuste tõrje ja ennetamise seaduses ning mitmetes muudes asjasse puutuvates õigusaktides. Siiski võib seadusloome kõrvaltvaatajana öelda, et neid muudatusi iseloomustab kiirustamine ja kohatine läbimõtlematus.

Järgnevalt saab ülevaate inspektsiooni kommenteeritud eelnõudest, mille osas oli rohkem kas avalikku diskussiooni või olid need inspektsiooni vaatest olulisemad või suurema mõjuga.

# TERVISEINFOSÜSTEEMI PÕHIMÄÄRUSE MUUDATUSED

Nagu öeldud, oli Sotsiaalministeerium 2020. aastal kõige viljakam ning seda arusaadavatel põhjustel.

Esimene tervise infosüsteemi (TIS) muudatus toimus veel enne tervisekriisi puhkemist ning olulisim muudatus puudutas uusi andmestikke, mida TIS-i kantakse. Nimelt tuli teha märkuse selle kohta, et muudatuste tulemusel saab keskandmekogu üheks andmestikuks ka ravijuhiste andmestik, kuid tervishoiuteenuse korraldamise seaduse vastav säte (§ $59^1$ lg 4), mis määratleb ammendavalt, mis laadi andmeid võidakse terviseinfosüsteemis töödelda, sellist andmestikku ette ei näe. Lisaks juhtis inspektsioon juba teistkordselt tähelepanu terviseandmetele juurdepääsu küsimusele. Nimelt puudutas üks muudatus TIS põhimääruse §-i 17, mille lõike 1 punktide 4 ja 8 järgi on andmesubjektil õigus keelata ja lubada oma andmetele juurdepääs ning võimaldada oma andmete vaatamist ja muutmist. Ehkki tuli teha märkuse ka selles osas, et kahe kirjeldatud õiguse erinevus on raskesti arusaadav, viitas inspektsioon veel sellele, et juba detsembris 2019 olime juhtinud tähelepanu laiemalt TIS-i andmetele juurdepääsu küsimusele. Nimelt näeb üldmääruse art 9 lõige 3 ette, et kui eriliigilisi andmeid töödeldakse art 9 lõike 2 punkti h eesmärkidel (ennetav meditsiin, töömeditsiin, töötaja töövõime hindamine, meditsiinilise diagnoosi panemine, tervishoiuteenuste, sotsiaalteenuste või ravi võimaldamiseks, tervishoiu- või sotsiaalhoolekandesüsteemi ja -teenuse korraldamine), siis peab sellel andmetöötleja töötajal olema liidu või liikmesriigi õigusest tulenevalt ametisaladuse hoidmise kohustus. Tervishoiuteenuste korraldamise seaduse § $59^3$ lõikes $2^1$ on märgitud, millistel tervishoiuteenusel osalevatel isikute on veel juurdepääs TIS-ile.

Samas ei ole arvatavasti kõigil neil seadusest tulenevat saladuse hoidmise kohustust. Seega ka uus muudatus, mis võimaldab isikul juurdepääse hallata, võib kaasa tuua olukorra, kus andmetele saab ligipääsu keegi, kes ei ole kohustatud ametisaladust hoidma. Lisaks juhtis inspektsioon juba teistkordselt tähelepanu, et üks andmeandjatest TIS-i on Haridus- ja Teadusministeerium, kes edastab TIS-i õpilase andmed, lõpetatud haridustaseme andmed ja õppeasutuse andmed. Et selliste andmete kogumise vajadus ja eesmärk ei ole selge, on saanud tähelepanu juba aastal 2018.

## HOIA äpp

Järgnev TIS-i muudatus puudutas valdavalt nutirakenduse loomist (HOIA äpp).

Esmalt juhtis inspektsioon tähelepanu, et andmevahetus TIS-i ja nutirakenduse keskse serveri vahel peaks toimuma üle X-tee.

Teine tähelepanek puudutas koodide edastamist. Segadust tekitas protsess – kuhu milline kood ja millal edastatakse. Segamini nimetati nii kinnituskoodi kui ka tuvastamiskoodi, aga kohati ka anonüümset koodi. Nii jäi arusaamatuks, kas tegemist on sünonüümidega või erinevate koodidega. Ka seletuskiri ei andnud vastust nendele küsimustele. Selgus, et andmevahetus on loodud selliselt, et kinnituskood luuakse nutirakenduses, kust see edastatakse kasutaja poolt TIS-i. Kui TIS-is toimuvas kinnitusprotsessis selgub, et infosüsteemis tuvastatud isiku tervisedokumendid kinnitatavad diagnoosi, siis luuakse tuvastuskood. Seejärel edastatakse nutirakenduse serverisse nii kinnituskood kui ka tuvastuskood ning edasi rakenduse kasutajale vaid kinnituskood. Inspektsioon märkis, et kui anonüümne kood, mida ka osati kasutati, on erinev kinnituskoodist, tuleks mõistetesse kindlasti selgust tuua. Lisaks juhtis inspektsioon tähelepanu sellele, et andmekaitsealane mõjuanalüüs keskendus liialt tehnilisele poolele ja sellele samale koodide vahetusele ehk andmevahetusele nutirakenduses, ent näiteks tähelepanuta ja hindamata oli jäetud kaudsed riskid. Ehk et, kas mingil võimalusel kasvõi kaudselt on võimalik ikkagi tuvastada, kui oled kinnituse saanud, et oled nakatunuga ühes ruumis viibinud ja seetõttu lähikontaktne, kellega tegemist on. Samuti, kas ja milline risk on selles, et rakendus annab nö valepositiivseid teateid. Kas näiteks on võimalik, et õhukeste kortermaja seinte läbi kaks lähestikku piisavat aega olnud telefonid võivad andmeid vahetada ja anda seeläbi teate, et oled viibinud nakatunuga ühes ruumis, ehkki tegelikult ei ole või, kui koosolekul oli nii vähe inimesi ja pärast seda saad teate nakatunuga ühes ruumis viibimisest, kas siis ikkagi ei ole võimalik aru saada, et tegemist oli just selle koosolekul viibinuga.

Kuna seletuskiri ütles nutirakenduse kohta, et see ise isikuandmeid ei töötle, juhtis inspektsioon tähelepanu sellele, et see päriselt siiski nii ei pruugi olla. Nimelt, kui on mingigi võimalus, et nutirakendus töötleb kasvõi pseudonüümitud andmeid, sh kui isiku tuvastamine võib tänu rakendusele, kuid ka väljapool seda, olla kasvõi kaudselt võimalik, tuleb siiski kõiki andmekaitse nõudeid rakendada.

Lisaks tuli pöörata tähelepanu sellele, et ehkki nutirakenduse tunnuskood ja TIS-is loodav kinnituskood on eelduslikult unikaalsed, siis seletuskirjast võis aru saada, et TIS-i kinnituskood luuakse TIS-i andmete pinnalt. Kuna aga TIS-is tekivad mistahes andmetöötluse korral logid, mis omakorda tähendab, et infosüsteemi tekib teave (tuvastuskood ja logi), mille pinnalt on võimalik tuvastada nutirakenduse kasutaja isik ja nutirakenduse kasutatav kinnituskood. Seega saabki öelda, et andmetöötlus ei ole täielikult anonüümne.

> ***„Soovitus oli anda selge ülevaade andmetöötlusest rakenduse kasutajatele ka selle kasutajatingimustes.“***

Kolmanda TIS-i muudatuse osas oli olulisim märkus, mis puudutas paragrahvi 5 täiendust lõikega 1[1], mille kohaselt häirekeskusega liidestunud kiirabibrigaadi pidaja edastab infosüsteemi kiirabibaasi ja kiirabibrigaadi andmed viivitamata pärast asjakohase ressursi staatuse muudatust. Inspektsiooni hinnangul ei võimalda infosüsteemi pidamise eesmärgid üldse selliste andmete edastamist TIS-i. Seletuskirjas küll viidati, et samad andmed (ressursiandmed) on kehtiva õiguse kohaselt kiirabi kaardi osa, mille andmed edastatakse TIS-i, kuid tegemist ei ole võrreldava olukorraga. Nimelt kiirabikaart on loodud selleks, et anda kokkuvõtvat teavet osutatud tervishoiuteenuse kohta ja ehkki see sisaldab ka teavet teenust osutanud kiirabibrigaadi kohta, kuid kiirabikaardi eesmärk ei seisne selles, et selle alusel hallata kiirabi autode kui ressursi kasutamist. Lisaks ei selgunud eelnõust, milliseid andmeid hakkab häirekeskusega liidestunud kiirabibrigaadi pidaja TIS-i edastama. Nagu kehtivast TIS-i põhimäärusest nähtub, on sellest muudatusest ka loobutud.

Häirekeskuse poolt kiirabi hädaabiteate menetlemise käigus kogutud andmete edastamisele TIS-i oli inspektsioonil samuti oma märkus. Tähelepanu tuli juhtida sellele, et kas andmete töötlemise minimaalsuse ja eesmärgipärasuse printsiipi silmas pidades on kõiki eelnõus nimetatud andmeid siiski vajalik TIS-i edastada, arvestades seejuures terviseinfosüsteemi pidamise eesmärke.

Kui ennist sai viidatud, et TIS-i andmeid polnud RIHA-s alates 2014. aastast uuendatud, siis vahetult enne käesoleva ülevaate valmimist seda siiski tehti. Paraku aga selgus RIHA-sse laetud andmekoosseisust palju

1 TTKS § 59[1] lg 4

andmeid, mida TIS-i põhimäärus ei käsitle. Olgu öeldud, et tervishoiuteenuste korraldamise seadus, mis TIS-i aluseks on, annab vaid üldise määratluse sellest, mis andmeid TISi kogutakse. Ka TIS-i põhimäärus ei anna otseselt detailset loetelu andmetest. See, mis andmeid TIS-i kantakse, selgub paljusid erinevaid norme ja õigusakte uurides. Siiski ei näe ükski norm ette, et TIS-i kantaks isiku kodakondsust, Eestisse elama asumise aega või abikaasa andmeid. RIHA-sse laetud andmekoosseisu järgi liigub TIS-i ka apteegist retseptiravimi välja ostnud isiku isikukood. Samas digiloost patsient ise seda ei näe ning põhimäärus nende andmete TIS-i kandmist ei sätesta. Sama oli kiirabiteate teinud inimese andmetega – andmekoosseisust selgus, et see info liigub Häirekeskuselt TIS-i. Taolisi lahknevusi õigusakti ning tegelikkuse vahel oli teisigi.[2]

Kokkuvõttes, tervise infosüsteemi primaarne eesmärk on olla keskne andmekogu inimesele kvaliteetse tervishoiuteenuse osutamiseks seeläbi, et arstile on kättesaadav terviklik ülevaade patsiendi terviseandmetest. Paraku on imbunud, ning nagu näha, järjest rohkem TIS-i juurde andmeid, millel ei ole seost tervishoiuteenuse osutamisega. Eesti riigi infosüsteemide arhitektuuri üks kõige olulisem nõue on hajusus. St ühe suure andmepoti asemel on Eestis palju teemapõhiseid andmekogusid, mis vahetavad omavahel vajalikke andmeid. Nii tuleb hoolikalt jälgida, et ka TISi-st ei saaks andmekogu, kuhu lisaks inimese terviseandmetele kogutakse kokku pool tema muust eluloost.

## SISEMINISTEERIUMI ETTEVALMISTATUD EELNÕUDEST

Siseministeeriumi edastatud õigusaktide eelnõudest peatuks kahel – politsei andmekogu (POLIS) andmekogu, millesse tehtud muudatuste osas küsiti arvamust kahel korral ning isikut tõendavate dokumentide seaduse ja teiste seaduste muutmise eelnõu, millega luuakse automaatse biomeetrilise identifitseerimissüsteemi andmekogu (ABIS).

### Politsei andmekogu muutmise eelnõu

POLIS-e muudatused olid peamiselt seotud taaskord COVID-19 kriisiga või siis vähemasti sellest tõukunud. Esimene muudatus tuli arvamiseks juba aprillis ja teine juunis. Teadaolevalt vajas Terviseamet Politsei- ja Piirivalveameti (PPA) abi selleks, et kontrollida nii nakatunuid kui ka lähikontaktseid, kes on karantiini määratud, et need tõepoolest ka neile seatud liikumispiirangutest kinni peaksid. Ent selgus, et erinevate andmekogude vaheline andmevahetus ei olnudki ilma õigusakte muutmata võimalik.

Aprillis arvamiseks esitatud muudatuse eesmärgiks oli luua õiguslik alus andmete esitamiseks Terviseameti poolt POLIS-sse. Eelnõu kohaselt edastaks Terviseamet POLIS-sse andmeid ühiste infoobjektide, ennetava tegevuse ja otsimise andmestikku.

> Inspektsioon juhtis esmalt tähelepanu sellele, et ehkki eelnõus oli märgitud, et Terviseameti õigus nakkushaiguste registrist (NAKIS) andmeid edastada PPA-le tuleneb NAKIS-e põhimääruse § 11 lõikest 11, siis tegelikkuses andis viidatud säte õigusliku aluse NAKIS-le juurdepääsuks, mitte andmete edastuseks. Lisaks ei võimalda POLIS-e põhimääruse § 22 lõige 2 POLIS-sse kanda mitmeid andmeid, sh andmeid isikute tervisliku seisundi ja seksuaalelu kohta, välja arvatud kuriteo ennetamiseks, tõkestamiseks, avastamiseks või tagaotsitava tabamiseks. COVID-19 nakatunu karantiini nõuete täitmine ei kuulu ilmselgelt ühessegi nimetatud kategooriasse.

[2] Vt 13.04.2021 nr 2.2.-8/21/879 „Tervise infosüsteemi mittekooskõlastus“

Veel juhtis inspektsioon tähelepanu andmete säilitamise tähtaegadele. Nimelt sätestati küll, kui kaua Terviseameti andmeid aktiivsena säilitatakse, kuid jäi ebaselgeks, mis neist edasi saab. Eelduslikult kantakse arhiivi, kuid selgesõnaliselt seda välja öeldud ei olnud. Lisaks tuli märkida, et kui ka andmed kantakse arhiivi, siis POLIS-e põhimääruse § 25 sätestab arhiivile juurdepääsu õigused, kus öeldakse, et arhiivist on lisaks andmesubjektile endale õigus andmeid saada politseiametnikul ja muul isikul põhjendatud teadmisvajaduse olemasolul. Samas andmekaitsealane mõjuhinnang ei analüüsinud, millist riski see, et politseiametnik või muu isik võib ligipääsu saada ka COVID-19 haiguse diagnoosi saanud isiku andmetele. Samuti oli andmekaitsealane mõjuhinnang puudulik osas, mis puudutab teiste asutuste ligipääse POLIS-le ja seeläbi Terviseameti poolt edastatavatele andmetele. Nimelt sätestab POLIS-e põhimäärus § 19 lõige 2, kellel lisaks PPA-le on ligipääs POLIS-le.

Juunikuine POLIS-e põhimääruse muudatus kordas osati sama, mis eelnev, mis oli juba küsitavusi tekitanud. Kuna aprillikuise eelnõuga viidi juba sisse POLIS-e muudatused, kus piiritleti Terviseamet andmeandjana üksnes 2020. kevadel kehtestatud eriolukorraga, siis uues eelnõus sooviti luua säte, mis ilmselt oleks tulevikku suunatud, et Terviseamet oleks andmeandjaks POLIS-sse hädaolukorras, erakorralises seisukorras ja sõjaseisukorras, kuid piiritlemata siis 2020. aasta kevadise eriolukorraga.

Inspektsioon viitas, et kui eelmine POLIS-e põhimääruse eelnõu oli arusaadav selles osas, et andmeedastus on seotud nakkushaiguse leviku tõkestamisega, siis uue eelnõu puhul polnud võimalik aru saada, millistel juhtudel tekiks Tervisametil kohustus andmed PPA-le edastada. Nimelt võib olla hädaolukord välja kuulutatud väga erinevatel põhjustel ning aru ei olnud saada, kas andmeedastus toimuks mistahes hädaolukorra korral. Samuti jäi arusaamatuks, kas ja miks ning mis andmeid edastaks Terviseamet erakorralise seisukorra ja sõjaseisukorra ajal.

Taaskord tekkis küsitavusi andmete säilitamise kohta. Kuna seletuskirjas oli selgitatud, et organisatoorselt suudetakse tagada, et andmeid säilitatakse üksnes teatud sündmuseni, tuleks nii eelnõus selgesõnaliselt ka öelda. Nimelt toodi välja põhjusena, miks ei saa täpsemalt säilitamistähtaegu sätestada, soovimatus või võimatus uut infotehnoloogilist lahendust luua, kuid kinnitati, et organisatoorselt on lühemat säilitustähtaega võimalik tagada. Samuti ei selgunud, millest lähtuvalt oli hinnatud kavandatud säilitamistähtajad sobivaks ja eesmärgipäraseks.

Nii nagu eelmist eelnõud kommenteerides, tegi inspektsioon taaskord märkuse arhiivis säilitamise tähtaegade kohta – osati oli valitud tähtajaks lausa 50 aastat, kuid selgitusi, miks just selline tähtaeg, ei olnud. Kuna POLIS-e andmetele on ligipääs ka teistel asutustel, oli hinnatud mõjusid andmesubjektile ning leitud, et riive ei ole suur, mille osas jäime eriarvamusele. Nimelt ei anta kõigile sellisele asutustele, kellel on POLIS-le juurdepääs hädaolukorras, erakorralises seisukorras või sõjaseisukorras ülesandeid, mis õigustaksid Terviseameti poolt edastatavatele andmetele ligipääsu. Seletuskiri jäi selles osas napisõnaliseks ja keskendus viiruse vastu võitlemise vajaduse kirjeldusele, samal ajal, kui muudatus oli suunatud tulevikku ning olukorrad, mil Terviseamet peaks andmeid edastama, olid ühelt poolt laiendatud, kuid teisalt täpsustamata.

Võttes arvesse POLIS-e hetkel kehtivat regulatsiooni, tuleb siiski tõdeda, et kavandatav muudatus jäi ellu viimata.

## Automaatse biomeetrilise identifitseerimissüsteemi (ABIS) andmekogu loomine

Üks olulisemaid eelnõusid Siseministeeriumi sulest 2020. aastal oli isikut tõendavate dokumentide seaduse (ITDS) ja teiste seaduste muutmise eelnõu, mis loob õigusliku aluse automaatse biomeetrilise identifitseerimissüsteemi (ABIS) andmekogu loomiseks.

Siseministeerium selgitab oma veebilehel, et automaatse biomeetrilise isikutuvastuse süsteemi andmekogu ehk ABIS saab olema keskne riiklik andmekogu,

kus hakatakse säilitama täna erinevates andmekogudes ning erinevate riiklike menetluste raames kogutavaid biomeetrilisi isikuandmeid – näo- ja sõrmejäljekujutisi. ABIS andmekogu loomise eesmärgiks on aidata kaasa turvalisele identiteedihaldusele, avaliku korra ja julgeoleku tõhusamale tagamisele, kuritegevuse ennetamisele ja süüteomenetlustes tõendite kogumisele. ABIS aitab tõsta isiku tuvastamise ja isikusamasuse kontrollimise usaldusväärsust andes senisest veelgi paremal tasemel kindluse, et inimesel saab Eestis olla ainult üks identiteet.[3]

Inspektsioon juhtis tähelepanu[4], et biomeetria on üldmääruse art 9 lõike 1 mõistes eriliigilised isikuandmed ning nende töötlemine on üldreeglina keelatud. Selliste andmete töötlemine on lubatud üksnes siis, kui andmete töötlemise õiguslik alus vastab üldmääruse art 9 lõikele 2 või õiguskaitse eesmärgil toimuva andmetöötluse korral IKS §-le 20. Mõlemal juhul on eelduseks, et õigusakt võimaldaks vastavat isikuandmete töötlust.

Oluline oli rõhutada, et biomeetriliste ehk siis eriliiki andmete alusel isikusamasuse tuvastamine ei saa muutuda reegliks ning nö tavameetodil isiku tuvastamine erandiks. Kuivõrd eelnõuga ei muudeta mitte üksnes IDTS-i, vaid ka väga suurt hulka muid seadusi (14 erinevat seadust)[5], siis viitas inspektsioon, et isikusamasus tuleb tuvastada ikkagi muudatusega hõlmatud juhtudel esmajärjekorras esitatud isikut tõendavas dokumendis oleva foto võrdlemisel isikuga. Kui sellest ei piisa, tuleks kasutusele võtta täiendavad meetmed. Kui asjaolusid arvestades on proportsionaalne ja vajalik kohe kasutada biomeetriat, siis selline andmetöötlus peaks olema erand ning erandit põhjendavad kaalutlused peavad tulenema seadusest või vähemalt selle seletuskirjast. Lisaks juhtis inspektsioon tähelepanu, et näiteks IDTS-i § 116 lõige 1 näeb ette, et biomeetriliste andmete kogumine ja töötlemine toimub dokumendi taotleja nõusolekul. Sellises olukorras ei saa aga rääkida nõusolekust üldmääruse mõistes. Nimelt peab nõusolek olema antud vabatahtlikult, tagasivõetav ega tohi olla sõltuvuses vastusooritusest. Olukorras, kus isik taotleb isikut tõendavat dokumenti, millele kantakse ka biomeetrilised andmed ja ilma nendeta dokumenti luua ei ole võimalik, ei saa rääkida nõusoleku alusel andmetöötlusest. Seega eeldab selline olukord selget õiguslikku alust.

Veel ühe olulise aspektina tuli välja tuua, et eelnõu nägi ette sätted, millistel juhtudel on võimalik sisuliselt määratlemata juhtudel ning olukordades töödelda biomeetriat isiku tuvastamiseks (IDTS § 155 lõiked 6-8). Ka ABIS-e põhimääruse peatükis 5 kirjeldatakse, millistel juhtudel tehakse üks ühele (1:1) ning millal üks mitmele päring (1:n) ehk suurema osa ABIS-sse kantud andmete vastu. See omakorda tähendab, et ABIS-sse kantud andmeid kasutatakse ka muul eesmärgil, kui see, milleks need algselt kogutud on. Ent üldreeglina võib andmeid kasutada üksnes neil eesmärkidel, milleks need algselt on kogutud (üldmääruse art 5 lõige 1 punkt b). Inspektsioon juhtis tähelepanu ka veel sellele, et biomeetriliste andmete töötlemise võimaldamine teisesel eesmärgil lubamine ei tohi toimuda kergekäeliselt. Isikule, kelle andmeid töödeldakse, peab olema ettenähtav ja selge, et tema kohta kogutud andmeid võidakse kasutada ka muul eesmärgil ning millisel.

Ehkki eelnõu seletuskirja täiendati selles osas, jäädi selle juurde, et teisesel eesmärgil töötlemine on vajalik ning kooskõlas üldmäärusega. Seletuskirjas on selgitatud, et eelnõus on loodud õiguslikud alused andmete edasiseks töötlemiseks, mis on vajalikud avaliku korra ja julgeoleku tagamiseks ning hõlmavad loodava andmekogu üldise eesmärgi. Eelnõu näeb ette andmete töötlemise nende algsest kogumise eesmärgist erineval eesmärgil eelkõige isiku tuvastamisel ehk olukorras,

[3] Vt ka https://www.siseministeerium.ee/et/eesmark-tegevused/automaatse-biomeetrilise-isikutuvastuse-susteemi-andmekogu-ehk-abis

[4] Tähelepanekud puudutavad inspektsioonile esitatud eelnõu versiooni mitte kevadel 2021. Riigikogu menetluses olevat

[5] Vt ka https://www.riigikogu.ee/tegevus/eelnoud/eelnou/8bf5e47e-e45f-43c2-8189-6bb875bf51fc/Isikut%20t%C3%B5endavate%20dokumentide%20seaduse%20muutmise%20ja%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus

kus avaliku võimu asutusele ei ole isiku identiteet teada. Võimalus kasutada vajadusel mõnes teises avalikus menetluses kogutud biomeetrilisi andmeid on isiku tuvastamisel väga oluline, sest selle käigus tuleb kindlaks teha isiku identiteet. Isiku tuvastamisel peab pädev asutus veenduma erinevate andmete ning vajadusel ka biomeetriliste andmete alusel ja põhjalike päringute tulemusel, et isik on see, kes ta väidab end olevat. Avaliku võimu asutustel on seadusest tulenev kohustus isik tuvastada ning õigus ja kohustus teha toiminguid üksnes õige isiku suhtes ning seetõttu peavad avaliku võimu teostajad olema veendunud, et isik on just see, kellena ta esineb. Õigus võtta isiku tuvastamiseks ja isikusamasuse kontrollimiseks isikult biomeetrilisi andmeid ja neid töödelda on kehtivas õiguses sätestatud. Inspektsioon nägi siin kõige suurema murekohana, et kas ja kui selge saab ikkagi olema regulatsioon inimeste jaoks. Ehk kas igale isikule on selgelt mõistetav ja arusaadav ning ka ettenähtav, et kui tema biomeetrilisi andmeid kasutatakse tema isiku üldiseks tuvastamiseks, siis neid võidakse tegelikult kasutada mingis muus olukorras ka teistel eesmärkidel.

# VEEL INSPEKTSIOONI ARVAMUSE SAANUD EELNÕUDEST

Teiste ministeeriumite poolt inspektsioonile arvamuse avaldamiseks saadetud eelnõudest või väljatöötamiskavatsustest on olulisemad välja tuua:

- **Turismiseaduse eelnõu**
- **Krediiditeabe seaduse väljatöötamiskavatsus**

## Turismiseaduse eelnõu

Turismiseaduse muutmist andmekaitse osas selgitati seletuskirjas järgnevalt: eelnõuga nähakse ette majutusteenuse kasutajate elektrooniline registreerimine ja nende andmete töötlemine. Sellega soovitakse muuta Schengeni konventsioonist tulenevate külastaja registreerimise nõuete täitmine majutusettevõtte külastajale ja majutusettevõtjale kiiremaks ja lihtsamaks ning tagada külastajate isikuandmete tänasest parem kaitse, sealjuures tagades, et Eesti on jätkuvalt ohutu ja turvaline koht nii kohalikele elanikele kui külastajatele. Majutusteenuse kasutajate andmed on samuti vajalikud, et teha riiklikku statistikat ning analüüsida turismiarendust ja -turundust.

Schengeni konventsiooni artikli 45 lõige 1 punkt b ütleb, et konventsiooni osalised kohustuvad võtma vajalikke meetmeid, tagamaks et: täidetud registreerimislehti säilitatakse pädevate asutuste jaoks või edastatakse neile, kui need asutused peavad seda vajalikuks ohu ärahoidmiseks, kriminaalmenetluse otstarbel või kadunuks jäänud või õnnetuse ohvriks langenud isikute saatuse kindlakstegemiseks, kui siseriiklikus õiguses ei sätestata teisiti.

Inspektsioon juhtis seaduselooja tähelepanu sellele, et konventsiooni sõnastusest ei ole üheselt aru saada, kas andmeid edastatakse automaatselt ehk *push*-meetodil või võib neid edastada ka üksnes siis, kui õiguskaitseasutus küsib teavet päringu korras ehk *pull*-meetodil. Seletuskiri ütles, et paljud Euroopa Liidu riigid on valinud *push*-meetodi, kuid puudus analüüs, miks Eesti on valinud sama tee ning kas sama eesmärk oleks võimalik saavutada ka *pull*-meetodil. Seepärast leidis inspektsioon, et eelistada tuleks *pull*-meetodil andmete edastust kuivõrd on vale eeldada, et enamus majutusasutusi külastavad inimesed sellistele kriteeriumitele üldse kunagi võiks vastata, et oleks põhjendatud nende andmete edastamine automaatselt õiguskaitseorganitele. *Push*-meetodil andmete edastamine riivab kindlasti enam isikute privaatsust.

Eelnõuga plaanitakse minna üle majutusasutustes majutusteenuse kasutajate elektroonilisele registreerimisele ning selle lihtsustamiseks soovitakse hakata andmeid hõivama otse ID-kaardilt või passilt selle masinloetavalt koodilt. Inspektsioon viitas oma arvamuses sellele, et isikut tõendavate dokumentide masinloetav kood hõlmab endas märksa rohkem andmeid, kui on vajalik majutusteenuse osutajal koguda. Seda enam, et mida aeg edasi, seda enam võib see koodandmeid sisaldama hakata sh ka näiteks biomeetrilisi andmeid. Seega tuleks süsteem üles ehitada selliselt, et masinloetavalt koodilt hõlmataks üksnes selline andmekoosseis, mida majutusteenuse osutaja koguma peab. Rõhutada tuli ka seda, et mistahes elektroonne lahendus, mis edastab andmeid riiklikule andmekogule, peab seda tegema X-tee vahendusel.

Turismiseaduse muudatustega seonduvalt oli kavas muuta ka politsei- ja piirivalveseadust (PPVS). PPVS-i luuakse õiguslik alus majutusteenuse kasutaja andmekogu loomiseks, mis omakorda on lennureisijate broneeringuinfo andmekogu alamandmekogu, kuhu kantakse turismiseaduse § 24 lõikes 1 nimetatud majutusteenuse kasutaja andmed. Seaduse muudatuse tulemusel satub majutusteenuse kasutaja andmekogusse kantud isiku andmetega automaatselt ristkontrolli nende andmekogude ja jälgimisnimekirjade vastu, mis on olulised andmete töötlemise eesmärgi saavutamiseks. Ainult selle külastaja andmed, mis saavad ristkontrolli tulemusel tabamuse, kontrollitakse käsitsi üle, et menetlusasutus saaks otsustada vajaliku meetme kohaldamise. Kuivõrd eeltoodud selgitus oli üksnes seletuskirjas, siis selline teave peaks sisalduma seaduses endas.

***„Tähelepanu sai säilitamistähtaegade teema. Nimelt, kuigi oli öeldud, et majutusteenuse kasutaja andmed pseudonüümitakse kuue kuu möödumisel andmekogusse kandmisest, ei selgunud, kas ja kuidas säilitakse isikute andmed, kelle andmete ristkontrolli tulemusel ei saadud tabamust.***

***Inspektsiooni soovitus oli, et selliste isikute andmed tuleks viia koheselt pseudonüümitud kujule.“***

Eelnõu nägi ette, et teatud juhtudel võidakse pseudonüümitud andmed taasisikustada, ent ei selgunud, kuidas seda tehakse. Nii soovitas inspektsioon reguleerida täpselt, millistel tingimustel on see lubatud. Samuti juhtis inspektsioon tähelepanu, et ehkki kui isikuandmed pseudonüümitakse, siis kuna reisidokumendi liik ja number jääb nähtavaks, on näiteks PPA-l tulenevalt nende käes olevast teabest võimalik isik tuvastada, mistõttu ei pruugi olla siiski tegemist pseudonüümitud andmetega.

Märkusi oli ka ligipääsude küsimuses – ligipääsuõigus oli antud PPA-le ja riigi julgeolekuasutustele. Kuna julgeolekuasutuste mõiste on lai ja tuleneb julgeolekuasutuste seadusest, võimaldatakse ligipääs andmetele ka näiteks Välisluureametile. Kuna Välisluureameti juurdepääsuvajadust ei olnud seletuskirjas selgitatud, jäi vajadus arusaamatuks. Nii soovitas inspektsioon siiski nimetada ligipääsuõigustega asutused nimeliselt ja seletuskirjas ka ligipääsuvajadust põhjendada. Samuti tuli viidata vajadusele täiendada andmekaitsealast mõjuhinnangut nii selles kui ka pseudonüümitud andmetöötluse osas.

## Krediiditeabe seaduse väljatöötamiskavatsus

Krediiditeabe seaduse väljatöötamise eesmärk on õilis ja kindlasti ka vajalik. Väljatöötamiskavatsuse sissejuhatuses[6] on krediiditeabe vajadust kirjeldatud järgmiselt: *krediiditeabe seaduse eelnõu väljatöötamiskavatsuse (VTK) peamine eesmärk on tagada vastutustundliku laenamise põhimõtete tõhusam järgimine, adresseerides kahte peamist teemat: a) krediiditeabe seaduse kehtestamine ehk füüsiliste isikute finantskohustuste andmete vahendamise teenusega tegelevatele ettevõtjatele kehtestatakse tegevusnõuded ja järelevalve; b) krediidipakkujatele kehtestatakse kohustus hakata omavahel jagama füüsilistest isikutest laenutaotlejate finantskohustuste andmeid.*

Võimalike tehniliste vahenditena, mille läbi teavet vahetama hakata, nimetab VTK registripõhist andmevahetusplatvormi ning nende kahe hübriidi. Andmevahetuse korraldamise osas nähakse samuti ette kolm alternatiivi – riiklik süsteem, kus registri pidamist ja haldamis korraldavad riigiasutused (1), riiklik süsteem, kus registripidamine on tellitud riigihankega erasektorist (2) ning riiklikult kehtestatud tingimustele vastav, kuid erasektori poolt korraldatud süsteem, kus turuosalised ise loovad organisatsioonilise ja tehnilise võimekuse andmevahetuse korraldamiseks (3). Eelnõu eelistab selgelt kolmandat lahendust.

> ***„Inspektsioon väljendas seisukohta, et iga uue andmetöötluse jaoks ei ole vaja luua uut andmekogu või registrit. Eelistada tuleb andmevahetusplatvormi lahendust, mitte aga andmete koondumist ühte registrisse või andmekogusse.“***

Eesti avalikus sektoris juurutatakse turvalisuse kaalutlusel juba aastaid andmekogude hajusarhitektuuri lahendust. Kui toimub päringupõhine andmete vahetus, siis on andmete väljastajal ka parem võimalus hinnata, kas päringu tegemine on õigustatud.

[6] väljatöötamiskavatsus ja vastust sellele on registreeritud kirja numbriga 1.2.-4/20/3366

VTK näeb ette, et krediidipakkujatele tuleb teha nii andmete edastamine kui ka päringu tegemine kohustuslikuks. Kusjuures vähemalt praeguses staadiumis ei ole selge, kas selline kohustus tekiks mistahes krediidi taotlemise korral või kas näiteks loodavasse süsteemi kantaks teave ka juba olemasolevate kohustuste kohta. Ehk, et kas uue süsteemi loomisel saab olema edasiulatuv mõju või tagasiulatuv. Eeldatavasti viimane, mis aga omakorda tähendab, et kogutakse andmed ka kõigi nende isikute ja nende kohustuste kohta, kes võibolla enam kunagi ühtegi finantskohustust juurde võtta ei soovi. Siin on suur oht andmete nö igaks juhuks kogumiseks ning andmebaasi tekkimiseks vaatamata esialgsetele õilsatele eesmärkidele olemaks üksnes krediidipakkujate käsutuses. On tõsine hirm, et sellise andmebaasi vastu tekib väga suur huvi ka muudel isikutel ligipääsu saamiseks.

Inspektsiooni praktikast võib näitena võtta maksehäireregistri asutamise, mis algselt loodi vastutustundliku laenamise kohustuse täitmise eesmärgil ning ka eraõiguslike ettevõtete (pankade) endi poolt. Aja jooksul aga maksehäireregister iseseisvus ning väljastab maksehäireandmeid kõigile, kes väidavad endil olevat õigustatud huvi võlaandmete järele. Kui luuakse nn positiivne krediidiregister, on selgelt näha, et andmekogust on võimalik õigustatud huvi korral saada andmeid teistel huvilistel. Niisiis, isegi, kui luua register või andmekogu üksnes krediidiandjatele ja muudele seaduses sätestatud isikutele, on sisuliselt võimatu välistada sealt andmete andmine õigustatud huvi esinemisel. Õigustatud huvi olemasolu peab hindama vastutav töötleja, ent oma praktikast võime öelda, et Eestis naljalt keegi sellega hakkama ei saa. Nii peabki seadusandja endale ning elanikkonnale selgelt teadvustama, et uue, laenukohustusi sisaldava keskse andmekogu loomisel saavad neid andmeid kasutama hakata ka kõikvõimalikud muud isikud ning praegu ettenägematutel eesmärkidel.

Kõigi olemasolevate laenude kesksesse registrisse „igaks juhuks“ kokku kogumine oleks selgelt ka eesmärgipäratu. Vajadus andmeid töödelda tekib ju alles uue laenu võtmise soovi hetkel. Paljud inimesed, kel juba on eluasemelaen, ei pruugi kas üldse või paljude aastate jooksul kordagi rohkem laenu soovida. Selliste inimeste laenuandmete igaks juhuks registrisse kogumine ning seal aastaid või aastakümneid hoidmine

(ning tegelikult ka, nagu eespool öeldud, hoopis muudel eesmärkidel väljastamine) ei haaku kuidagi eesmärgiga, milleks registrit luua tahetakse.

Ettepanekuna VTK-s on toodud välja, et kaaluda tuleks, kas võiks teha krediidiandjatele kohustuslikuks litsentseeritud krediidibürood v.a juhul, kui krediidipakkuja ise hindab enda meetmed piisavaks. Siin tekkis esmalt küsimus, et miks siis üldse peaks krediidiandja kasutama krediidibürood, sest võimalik, et krediidiandja hindab omi meetmeid piisavateks. Samas aga peaks ta ise krediidibüroole ikkagi andmeid esitama. Ent olulisemana paistab siin oht, et krediidibürood küll koguvad andmeid (sest nende esitamine on ju krediidiandjale loodava seaduse kohaselt kohustuslik), kuid neid ei kasutatagi. Siit võibki tekkida krediidibüroodel majanduslik huvi neid andmeid muudel eesmärkidel kasutada anda. VTK-s mainitud ja krediiditeabe seadusega koos kavandatav muudatus võlaõigusseaduses viitabki pigem sellele, et kavandatav krediiditeabe seadus lähtub eeldusest, et tekivad nii (tsentraalsed) registrid kui ka andmevahetusplatvormid, mida tuleks kasutada vastutustundliku laenamise põhimõtte täitmiseks. Seega on inspektsiooni poolt peljatav stsenaarium pigem tõenäoline. Tegemist oli küll alles seaduse väljatöötamiskavatsusega, kuid inspektsioon loodab, et antud tagasiside on seaduse väljatöötajad mõtlema pannud olulistele andmekaitselistele aspektidele, kuid mõistagi hoiab inspektsioon arengutel ka ise teravalt silma peal.

# RIIGI INFOSÜSTEEMI HALDUSSÜSTEEMIS (RIHA) MENETLETUD ANDMEKOGUDEST

Aastaraamatus leiab käsitlust kahe uue andmekogu asutamise kavatsus.

- **Euroopa Sotsiaalfondi andmekorje register**
- **Tallinna Sotsiaalhoolekande Infosüsteem**

## Euroopa Sotsiaalfondi andmekorje register

Teatavasti kehtib nõue, et Euroopa Liidu struktuurifondidest rahastatavate projektide puhul tuleb osalejad nimeliselt kirja panna ning säilitada kuni projekti aruandlus- ja kontrolliperioodi lõpuni. Riigi Tugiteenuste Keskus (RTK) soovis asutada andmekogu Euroopa Sotsiaalfondist (ESF) rahastatavate tegevuste raames kogutavate isikuandmete jaoks.

Euroopa Liidu struktuurifondidest (vähemasti sotsiaalfondist) rahastatakse paljusid tundliku sisuga teenuseid (nt kodututele, eluasemeturult tõrjututele, lapsendajatele; teenused võib olla ka psühholoogiline abi). Laiemalt on selliselt rahastatud teenuste puhul olnud probleemiks, et osalejatelt kogutakse andmeid ilma, et nad teaksid, kui mitmed asutused (teenusepakkuja, korraldusasutus, rakendusasutus, sertifitseerimisasutus, auditeeriv asutus) neid andmeid hiljem töötlevad ning kui pikka aega säilitatakse. Või teistpidi, et võetakse inimeselt nõusolek andmete töötlemiseks, kuid nõusolekust keeldumise korral ei saa ka teenust. Paraku ei saa sellisel juhul nõusolek olla kuidagi andmete töötlemise aluseks.

Isikuandmete töötlemise nõusoleku andmise üle peab inimene saama vabalt otsustada ilma, et kaasneks negatiivseid tagajärgi. Selles olukorras oleks õige anda inimesele selge ülevaade struktuurfondist rahastatud teenusega kaasnevast kohustuslikust andmetöötlusest, nt vastava selgelt sõnastatud infolehe kaudu, kuid ilma nõusoleku võtmiseta.

Kuid andmekorje registri asutamise plaani juurde tagasi tulles, siis selle puhul oli esimeseks probleemiks andmete edastamine koopiana Statistikaametile. Probleem oli see seetõttu, et Statistikaametile edastataks andmed kui Rahandusministeeriumi volitatud töötlejale sel moel, et Statistikaametisse tekiks reaalajas koopia samast andmekogust, mis on Rahandusministeeriumil. Kuigi koostöökokkuleppega on Rahandusministeerium oma aruandluse ülesande Statistikaametile üle andnud, oleks õige anda Statistikaametile juurdepääs andmekogule, mitte luua andmekogust reaalajas koopiat.

Teiseks probleemiks oli ülesande üleandmisega ning Statistikaameti enda andmete kasutamisega. Seni käsitleti kõnealuseid aruandeid programmivälise statistikatööna, kuid inspektsioon kahtleb, kas need seda oma olemuselt on. Olemuslikult on Rahandusministeerium volitanud koostöökokkuleppega endal lasuva haldusülesande täitmise Statistikaametile. Tegemist ei ole oma olemuselt statistikaalase tööga, vaid Euroopa rahade kasutamise järelkontrolli eesmärgil tehtavate aruannetega. Täiesti lubamatu oleks olukord, kui selliste aruannete tulemiks võib olla isikule tagasinõude esitamine.

***„Statistikaameti nn statistiliste registrite andmete kasutamine on isikule õiguslike tagajärgedega otsuste tegemiseks täielikult keelatud."***

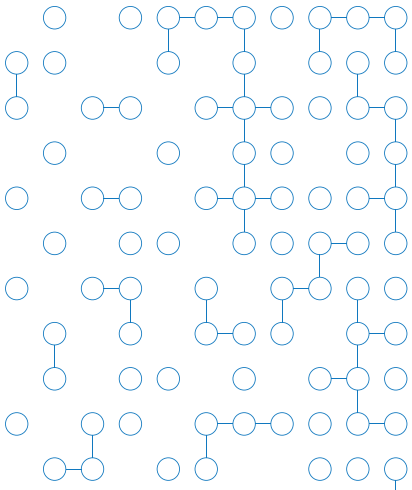
Inspektsioon leidis, et kogu andmetöötluse kontseptsioon tuleks uuesti läbi mõelda.

## Tallinna Sotsiaalhoolekande Infosüsteem

Uue andmekogu asutamine tõi lauale küsimuse dubleerivatest andmekogudest. Nimelt olime kümmekond aastat tagasi seisus, kus igal omavalitsusel oli sotsiaalhoolekande korraldamiseks mingi oma infosüsteem (valdavalt SIUTS). Riik leidis, et õige oleks omavalitsuste sotsiaalhoolekande andmete jaoks asutada tsentraalne riiklik andmekogu STAR - sotsiaalteenuste ja -toetuste andmeregister.

STAR-i andmekoosseis on üüratu – kõik andmed nii riigi kui omavalitsuse kõikvõimalike sotsiaalteenuste ja -toetuste, samuti lapsendada soovivate ja lapsendamist kohta. Eelmisel aastal aga jõudsime ringiga tagasi STAR-i eelsesse olukorda, kus Tallinna linn loob samaks asjaks oma enda infosüsteemi põhjendusega, et STAR-I pole omavalitsuse jaoks vajalikke funktsionaalsusi. Kuivõrd ühe ja sama ülesande täitmiseks kahe erineva andmekogu loomine pole kuidagi põhjendatud, palus inspektsioon Tallinna linnal ning Sotsiaalministeeriumil koos Sotsiaalkindlustusametiga selgitada, milliseid andmeid on vaja vaid omavalitsusele, milliseid riigile. Eesmärgiks on selgitada välja, mida siis riik tsentraalselt üldse koguma peaks ning millisel eesmärgil. Üksnes järelevalve teostamise õigus ei ole piisavaks põhjuseks andmete riigi kätte kogumiseks. Järelevalve eesmärgil saab Sotsiaalkindlustusamet igal ajal nõuda andmeid omavalitsuse andmekogust (või antakse ajutine juurdepääs). Samuti tuleb arvestada, et sotsiaalhoolekannet on mitmesugust: riigi enda osutatav, riigi poolt omavalitsusele pandud kohustuslikud teenused, omavalitsuse vabatahtlikud teenused.

Inspektsioon ootab endiselt Sotsiaalministeeriumilt ülevaadet STAR-i andmete kogumise põhjuste kohta.



# OMAVALITUSTE ANDMEKOGUD

Omavalitsuste andmekogude puhul hakkas kahjuks silma põhimääruste halb kvaliteet. Põhimäärused kirjutatakse maha mõne teise pealt, mõistmata, mida selle sätted tähendavad või kas see ka tegelikkusega kokku läheb. Üks silmatorkavamaid on kindlasti omavalitsuste huvihariduse andmekogud. Neisse kogutakse kõikide omavalitsuse territooriumil tegutsevate huviringide ning nendes osalevate laste andmed- kes millises huviringis ja millisel kuupäeval kohal käis. Põhjendatakse seda toetuse andmise kontrollimise vajadusega: kuigi toetust antakse huviringi korraldajale, mitte konkreetsele lapsele, tahetakse kontrollida, kas huviringis osalejate arv vastab tegelikkusele ning ega ühte ja sama last pole samaks kellaajaks mitmesse ringi kirja pandud. Üks omavalitsus aga üllatas sellega, et soovis registri põhjal välja selgitada lapsed, kes üheski huviringis ei käi. Huviringis käimine ei ole kohustuslik ning see ei tähenda, et tegemist oleks abivajava lapsega. Info lapse abivajaduse kohta peaks omavalitsuseni jõudma muul moel.

Huviringi korraldajale toetuse maksmise asjaolude kontrollimise eesmärgil isikustatud andmete kogumine peaks olema viidud miinimumini. Nii näiteks võiks vajalik kontroll toimuda automaatselt igakuiselt ning seejärel võiks andmed anonümiseerida, mis tähendab kõikide tuvastamist võimaldavate andmete hävitamist. Kindlasti pole põhjendatud selliste andmete säilitamine aastaid.

Tallinna linnalt aga ootaks jätkuvalt lemmikloomaregistri põhimääruse kooskõlla viimist registrisse kogutava andmestikuga. Hetkel näeb jätkuvalt põhimäärus ette vaid koerte (ja nende omanike) andmete kogumist.

## Mõned üldised tähelepanekud

Avaliku teabe seaduse § 43[5] järgi tuleb andmekogu põhimääruses välja tuua lisaks andmekoosseisule ka andmeandjad. Andmeandjateks on näiteks teised andmekogud, kust andmeid saadakse. Praktikas nähakse seda kui tüütut kohustust. Tegelikult säästaks asutus seeläbi aga oluliselt palju ressurssi. Nimelt nõuab isikuandmete kaitse üldmääruse (IKÜM) artikkel 14, et kui andmeid ei saada andmesubjektilt, tuleb andmesubjekti andmete saamisest mõistliku aja jooksul teavitada. Ilmselgelt pole praktikas selle normi rakendamiseni jõutud. Teavitama aga ei pea siis, kui andmete saamine on õigusnormis selgelt ette nähtud.

***„See on tavapärane, et ühel asutusel on oma tööks vaja teise asutuse käest andmeid, mida teine asutus on hoopis muul eesmärgil kogunud. Luues teise asutuse andmekoguga otseühenduse ja saades sealt andmed, peaks sellest andmesubjekti igakordselt teavitama. Igavesti saa IKÜM artiklite 13 ja 14 kohustusi eirata – teavitamiskohustus tuleb paratamatult kõigil asutustel oma tööprotsessidesse juurutada ning sellega harjuda.“***

[7] Vaata Sotsiaalteenuste ja -toetuste põhimääruse lisas olevat andmekoosseisu, mis on 11 lehekülge pikk. https://www.riigiteataja.ee/aktilisa/1120/3201/9055/SOM_05032019_m10lisa2.pdf#

*„Kui aga seaduses või andmekogu põhimääruses andmevahetus selgelt kirja panna, saaks igakordset teavitamiskohustust vältida.“*

Teine silma hakanud teema möödunud aastast on rahvastikuregistri päringute vale kasutus. Järgnevalt 3 enamlevinud viga.

- Esiteks kasutatakse liiga laia päringut. Kontrollida on vaja vaid infosüsteemis toimingut tegeva inimese andmeid, kuid selleks kasutatakse seotud isikuid hõlmavat päringut. Nii tekib inimese lähikondsetel andmejälgijat vaadates kohe küsimus, miks minu andmeid on vaadanud asutus, kellega mul mingit pistmist pole. Nii teevad asutused endale karuteene.

- Teiseks tehakse rahvastikuregistri päring kohe infosüsteemi sisenemisel, kuigi sisenemiseks seda vaja ei ole. Ehk siis päring tehakse ennatlikult.

- Kolmas probleem on vastupidine – päritakse liiga vähe. Lapse esindusõiguse kontrollimiseks on lisaks lapsevanemaks olekule vaja rahvastikuregistrit kontrollida ka hooldusõiguse olemasolu ja sisu. Vastasel juhul võib juhtuda, et lapse nimel saab toiminguid teha lapsevanem, kellelt on hooldusõigus üldse ära võetud.

Nö karbilahendusena arendatud infosüsteemide või RIHA mõistes standardlahenduste kasutajate puhul on näha, et ei teata, kuidas süsteem tegelikult töötab, rääkimata sellest, et see töötaks kasutaja kui vastutava töötleja juhiste järgi. Nii juhtub, et karbitootena arendatud infosüsteemi kasutades ei saa andmekogu pidaja määrata ise säilitamistähtaegu või kogutavate andmete ulatust. Samuti võib üllatusena selguda, et andmetöötluses kasutatakse allvolitatud töötlejaid kolmandatest riikidest.

*„Inspektsiooni fookuses on 2021. aastal andmelaod ning avaandmed“*

# KOHTUPRAKTIKA

Kui eelnõude osas oli õigusnõuniku töölaud üsna rikkalik ja tööpõld lai, siis kohtumenetluses jõuti jõustunud lahendini märksa vähematel juhtudel. Neist oleks paslik peatuda kahel lahendil. Mõlemad on paraku esimese astme lahendid. Üks isikuandmete kaitse asjas, teine avaliku teabe omas.

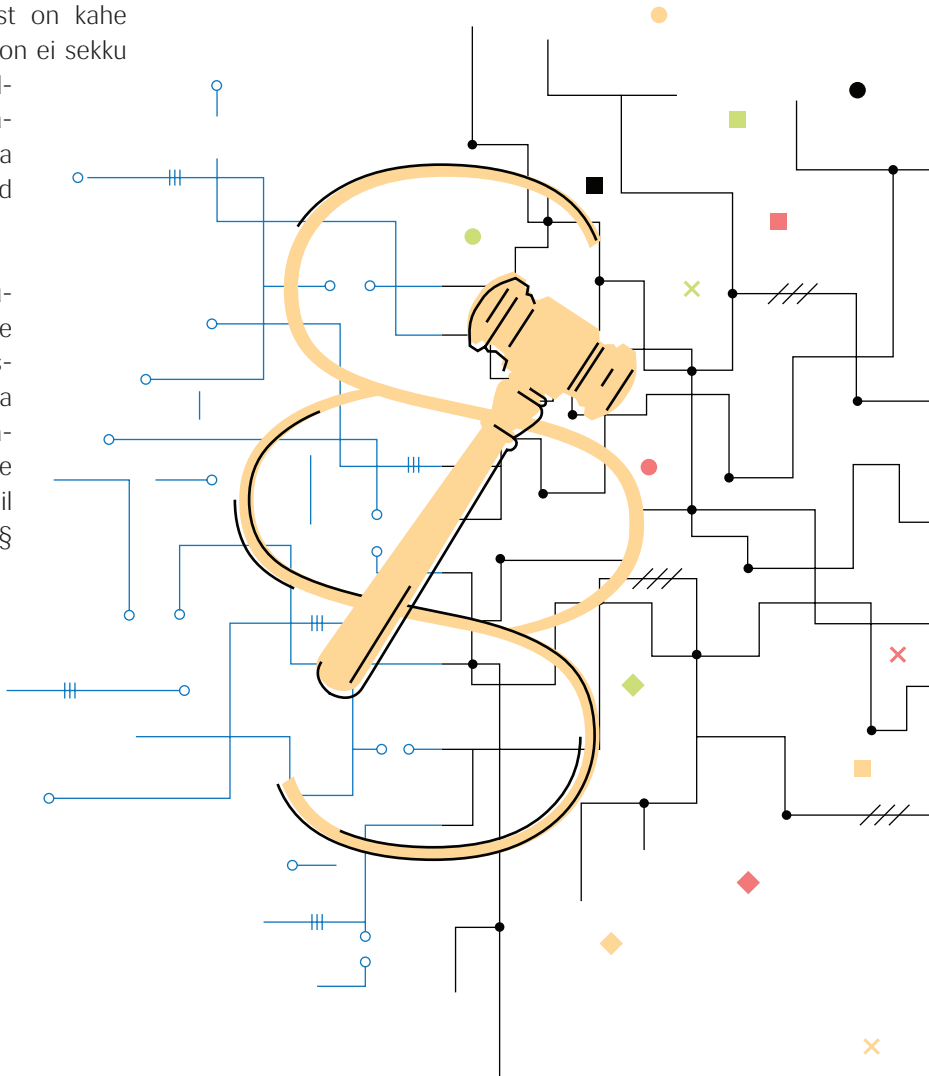
## Kohtuasi 3-20-375[1]

Kohtulahend isikuandmete kaitse asjas

Inspektsiooni poole pöördusid kaks isikut, kel oli tekkinud vaidlus äriühinguga, mille juhatusse nad olid kuulunud. Vaidlusmomente oli mõistagi mitmeid, kuid inspektsiooni poole ajendas isikuid pöörduma asjaolu, et nende juhatusest eemaldamise protsessi käigus võeti neilt ühtlasi etteteatamata ära ligipääs tööruumidele ja infosüsteemidele, mistõttu jäi neil äriühingu valdusesse isiklikke asju ja teavet sh isikuandmeid sisaldavaid failid. Äriühing keeldus neid ka väljastamast. Esmalt jättis inspektsioon nende taotluse menetluse algatamiseks rahuldamata, kuna tegemist on kahe isiku vahelise vaidlusega, kuhu inspektsioon ei sekku ning sellised vaidlused lahendatakse tsiviilkohtus. Isikud vaidlustasid menetluse algatamata jätmise vaidemenetluses, kuid ka vaie jäi rahuldamata ning isikud pöördusid halduskohtusse.

Põhjus, miks inspektsioon jäi vaidemenetluse otsuses kindlaks oma seisukohale mitte menetlust alustada seisnes asjaolus, et inspektsioonile laieneb kohustus kohaldada korrakaitseseadust (KorS). Varasema kohtupraktika kohaselt on eraõiguslike isikute vahelisse vaidlusse võimalik inspektsioonil sekkuda üksnes siis, kui on täidetud KorS § 4 lg 2 tingimused.

KorS § 4 lg 2 ütleb, et eraõiguse normide järgimine ja isiku subjektiivsete õiguste ning õigushüvede kaitstus on avaliku korra osa niivõrd, kuivõrd kohtulikku õiguskaitset ei ole võimalik õigel ajal saada ja ilma korrakaitseorgani sekkumiseta ei ole õiguse realiseerimine võimalik või on oluliselt raskendatud ning kui ohu tõrjumine on avalikes huvides. Inspektsioon oli lähtunud eeldusest, et eraisikute vahelisse vaidlusse sekkume vaid siis, kui see on vältimatult vajalik või isikul ei ole võimalik oma õigusi maksma panna kohtus. Samuti oli inspektsioon seisukohal, et sekkumistaotlus ei ole mitte taotlus haldusakti andmiseks, vaid taotlus menetluse algatamiseks, mille osas on haldusorganil avar kaalutlusruum. Andmesubjektil puudub järelevalvemenetluses õigus nõuda järelevalveasutuselt konkreetse järelevalvemeetme rakendamist.



[1] https://www.riigiteataja.ee/kohtulahendid/fail.html?id=270987799

Kohus nõustus, et inspektsioonil tuli lähtuda KorS § 4 lg-st 2. Kuna isikuandmete kaitse üldmäärus (IKÜM/üldmäärus) ei sätesta järelevalveasutusele esitatud kaebuste menetluskorda, tuleb selles osas lähtuda riigisisesest õigusest. Eesti õiguses tulenevad vastavad sätted haldusmenetluse seadusest ja KorS-ist. Seega tuli inspektsioonil muuhulgas lähtuda ka KorS § 4 lg-st 2. Samas aga ütles kohus, et inspektsioon pidi viidatud sätte kohaldamisel tõlgendama seda kooskõlas IKÜM-ga, et tagada selle eesmärgipärane õiguslik mõju andmesubjektile. Kohus leidis, et inspektsioon on oma kaalutlustes lähtunud vaid enne IKÜM-i kehtima hakkamist kujundatud praktikast ega pole üldmäärusest kaebajatele tulenevate õigustega arvestanud. Kuivõrd IKÜM-i art 57 lg 4 kohaselt võib järelevalveasutus keelduda taotlust menetlemast, kui taotlused on selgelt põhjendamatud või ülemäärased, eelkõige oma korduva iseloomu tõttu, siis leidis kohus, et keelduda saaks taotluse menetlemisest KorS § 4 lg 2 alusel, kui taotlus on selle sätte eelduste täitmata jätmise tõttu samaaegselt selgelt põhjendamatu ja ülemäärane IKÜM-i art 57 lg 4 mõttes.

Lisaks märkis kohus, et IKÜM-i artiklitest 77 ja 79 saab järeldada, et üldmäärusest tulenevate õiguste kaitsmine kohtus ei piira andmesubjekti õigust järelevalveasutusele kaebuse esitamiseks. Seega on lubatud ka paralleelsed menetlused. Ehk siis KorS § 4 lg 2 ei saa tõlgendada nii, et kui isik saab tsiviilkohtusse pöörduda, siis on inspektsioonil igal juhul õigus kaebuse menetlemisest keelduda. Üldmääruse eesmärk on tagada andmesubjektile lai kaitse ning tulenevalt artikkel 57 lõigetest 2 ja 3 peab isikul olema võimalik pöörduda järelevalveasutuse poole keerukusteta ja tasuta, et oma õigusi kaitsta.

Seega peaks inspektsiooni menetluse läbiviimisest keeldumine olema erandlik. Kohus ütleb selgesõnaliselt, et olukorras, kus kaebus ei ole selgelt põhjendamatu ega ülemäärane, on inspektsioonil kohustus seda menetleda.

> Kohus jõudis lõppastmes järeldusele, et inspektsioonil tuleb isikute taotlus uuesti läbi vaadata ning juhul, kui siiski keeldutakse menetluse alustamisest, tuleb põhjendada, miks see juhtum vaatamata väljakujunenud praktikale sekkumiskünnist ei ületa või anda selgitusi praktika muutmise kohta ning kuidas sellest tulenevalt on tegemist selgelt põhjendamatu või ülemäärase kaebusega IKÜM-i artikkel 57 lg 4 mõistes.

Tegemist oli lahendiga, mis muutis oluliselt praktikat. Nimelt pöördutakse inspektsiooni poole väga tihti just eraisikute vahelistes vaidlustes. Enam levinud on näiteks nn Facebooki kaebused, kus üks isik on avaldanud teise kohta mingeid isikuandmeid, millega teine nõus ei ole. Pärast kohtu vastavat lahendit, on meie võimalused selliste kaebuste menetlemisest keelduda. Mõistagi suunab inspektsioon jätkuvalt isikuid esmalt oma õigusi ise kaitsma. See tähendab pöörduma esmalt andmete avaldaja poole palvega need eemaldada, kuid kui see tulemust ei anna, on inspektsioon sunnitud sekkuma.

Võttes arvesse inspektsiooni inimressursi piiratust, võtavad sellised kaebused tööst märkimisväärse osa. Samal ajal on kohustuseks isikuandmete kaitse seadusest tulenevalt kaebus läbi vaadata 30 päeva jooksul. Alahindamata kuidagi seejuures inimeste muret ja vajadust nende õiguseid kaitsta, kelle kohta nt Facebookis nõusolekut andmata mingeid andmeid avaldatakse, on inspektsioon siiski olukorras, kus peamine ressurss läheb suures pildis vaadatuna väikeste kaebuste ja isikutevaheliste vaidluste lahendamisele, samal ajal, kui suurte andmetöötlejatega tegelemiseks mahti väga ei jäägi.

## Kohtuasi 3-19-2287[2]

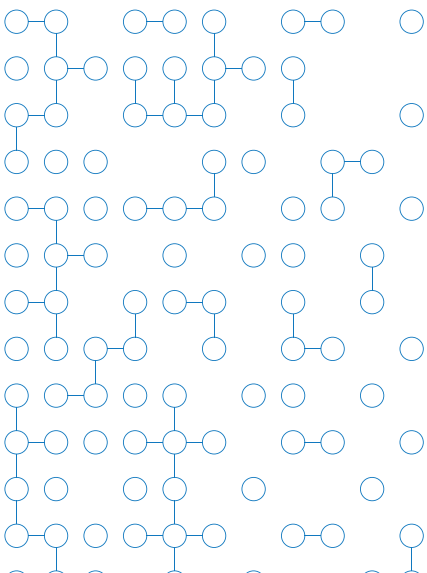
Kohtulahend avaliku teabe asjas

Isikud olid pöördunud teabenõudega Pärnu linna poole saamaks teavet selle majandusaasta aruande lisas kajastatud kulude kohta. Nimelt oli soovitud lisas kajastatud andmed kõikidest tavapärasest erineval viisil tehtud tehingute kohta, mille üheks osapooleks on Pärnu linn ja teiseks osapooleks seotud osapool. Pärnu linn keeldus sellise teabe väljastamisest tuginedes avaliku teabe seaduse (AvTS) § 23 lg 1 punktile 1, mis ütleb, et teabevaldaja keeldub teabenõude täitmisest, kui taotletava teabe suhtes kehtivad juurdepääsupiirangud ja teabenõudjal ei ole taotletavale teabele juurdepääsu. Isikud esitasid keeldumise peale inspektsioonile vaided ning inspektsioon rahuldas mõlemad vaided kohustades Pärnu linna taotlused uuesti läbi vaatama ja väljastama nõutud teabe, kui puudub alus juurdepääsu piirata.

Inspektsiooni seisukoht oli nii vaideotsustes kui kohtumenetluses, et teabevaldajal on kohustus teabenõudele vastata. Kuna Pärnu linn asus seisukohale, et teabenõuet ei saa täita, kuna majandusaasta aruande lisa, mille kohta teavet küsiti, tugineb teabel, mida küsiti seotud isikute enda käest ning seotud osapooled andsid deklaratsioonides hinnanguid oma lähedaste poolt Pärnu linnaga tehtud tehingutele, mis väljusid igapäevase majandustegevuse raamidest. Samuti sisaldusid teabes vastused küsimusele, kas nad olid teinud tehinguid linnaga tavapärasest erineval viisil. Kuna jaatava vastuse korral oli täidetud lahtris tehingu osapool ja tehingu summa ja saldo, siis on teave juurdepääsupiiranguga tuginedes isikuandmete kaitse üldmäärusele (IKÜM). Inspektsioon oli seisukohal, et isikud ei soovinud mitte deklaratsioone, millele linn viitab, vaid lepinguid ja muid dokumente üldistatud kujul, mille summad kajastuvad majandusaasta aruande vastavas lisas ning mis olid aluseks sellise lisa koostamisel. Inspektsioon selgitas, et IKÜM ei ole üldistatult võetuna aluseks juurdepääsupiirangu seadmiseks, vaid piirangu alus saab tuleneda AvTS-ist. Pärnu linn ühelt poolt kinnitas, et juurdepääsupiiranguid dokumentidele seatud pole, kuid teisalt keeldus jätkuvalt teavet väljastamast.

Kohus nõustus inspektsiooniga. Kuigi Pärnu linn on selgitanud, et jaotab dokumente selliste hinnanguliste kriteeriumite alusel nagu „riigihangete seadusest kinnipidamisel küsitavusi tekitanud hankelepingud“ või tavapärasest tehingust erinev dokument, aga samas on majandusaasta aruandes ise märkinud, et selliseid tehinguid on toimunud lisas 23 kajastatud ulatuses. Seega on Pärnu linn ise hinnanud osa lepinguid ja dokumente tavapärasest erinevaks, mille alusel vastavad summad ka majandusaasta aruandes on kajastatud, mistõttu peab talle olema ka teada ja arusaadav, milliseid dokumente isikud soovisid. Inspektsioon on juhtinud Pärnu linna tähelepanu ka sellele, et hoopis teabevaldajal on kohustus abistada teabenõudjat, kui jääb arusaamatuks tema nõude sisu, mitte aga vastupidi. Kohus leidis samuti, et isikute teabenõuetes oli piisava täpsusega kirjeldatud teavet, mida sooviti.

Kohus märkis, et kohaliku omavalitsuse asutusest teabevaldaja ei tohi asutusesesisese kasutamiseks mõeldud teabeks tunnistada dokumente kohaliku omavalitsuse üksuse eelarvevahendite kasutamise ning eelarvest makstud tasude ja hüvitiste (AvTS § 36 lg 1 punkt 9), andmeid oma varaliste kohustuste (AvTS § 36 lg 1 punkt 10) ega andmeid talle kuuluva vara kohta (AvTS § 36 lg 1 punkt 11). Seega oli isikute poolt nõutud teave avalik teave, mis tuleb neile väljastada.



[2] https://www.riigiteataja.ee/kohtulahendid/fail.html?id=266920440

Kohus nõustus inspektsiooniga ka selles, et AvTS § 3 lg-st 2 tulenevalt saab avalikule teabele juurdepääsu piirata üksnes seaduses sätestatud korras, pelk viitamine isikuandmete kaitsel IKÜM-le ei ole juurdepääsupiirangu seadmiseks piisav, vaid piiranguid tuleb seada AvTS-i konkreetse sätte alusel. See ei tähenda siiski, et väljastada tuleks isikuandmed, kui ekslikult on jäänud juurdepääsupiirang seadmata, kuid seda ei olnud ka inspektsioon väitnud, vaid sisulise ja põhjaliku menetluse tulemusel on kohtu hinnangul jõutud õigele järeldusele, et sisuliselt on teabenõude täitmata jätmine olnud põhjendamatu. Kuigi AvTS § 35 lg 1 punkt 12 kohustab tunnistama asutusesiseseks kasutamiseks mõeldud teabeks igasuguse teabe, mis sisaldab isikuandmeid, kui sellisele teabe juurdepääsu võimaldamine kahjustaks oluliselt andmesubjekti eraelu puutumatust, tuleneb AvTS § 3 lg-st 2 ja § 4 lg-st 3 kohustus ka eraldi kehtestatud juurdepääsupiiranguta teabele juurdepääsu võimaldamisel tagada isiku eraelu puutumatus. Teabevaldajal on õigus ja kohustus igal üksikjuhtumil hinnata, kas kaalukamaks tuleb pidada teabenõudja õigust saada juurdepääs avalikule teabele (põhiseaduse § 44 lg 2) või andmesubjekti õigust eraelu puutumatusele (põhiseaduse § 26). Juhul, kui huvi taotletud teabele juurdepääsu saamiseks on kaalukam andmesubjekti huvist eraelu puutumatuse kaitsele, ei ole teabe väljastamiseks andmesubjekti nõusolek vajalik, sest teabele juurdepääsu võimaldamine toimub seaduse alusel.

Kohus märkis lisaks, et kohtule ei nähtu, milles seisnevad nõutud teabe väljastamisel seotud isikute õiguste rikkumised, mida linn soovib teabenõude täitmisest keeldumisega kaitsta. Sõlmitud lepingutest jm dokumentidest nähtub, kui palju ja millistel tingimustel on saanud erinevad juriidilised või füüsilised isikud oma kasutusse avalikke vahendeid. Tegemist ei saa olla sellise teabega, mis nõuaks oma olemusest lähtuvalt kaitsmist. Pärnu linna väitel on valdavalt tegemist erinevatele juriidilistele isikutele eraldatud vahenditega. Juriidilistel isikutel pole eralelu ega isikuandmeid, mida kaitsta. Ka selliste juriidiliste isikute juhtorganite liikmete nimede avaldamine ei ole lubamatu isikuandmete avaldamine. Vastav info on kättesaadav ka äriregistrist. Avalike vahendite saamine ei ole „eraeluline majandustegevus“, nagu linn on viidanud. Isikud, kes saavad enda kasutusse kohaliku omavalitsuse eelarvevahendeid, peavad arvestama sellega kaasneva aruandluse ning avalikkuse kontrolliga. AvTS § 1 järgi on selle seaduse eesmärk tagada üldiseks kasutamiseks mõeldud teabele avalikkuse ja igaühe juurdepääsu võimalus, lähtudes demokraatliku ja sotsiaalse õigusriigi ning avatud ühiskonna põhimõtetest ning luua võimalused avalikkuse kontrolliks avalike ülesannete täitmise üle.

Ehkki tegemist ei ole inspektsiooni praktikat muutva või eriliselt õigusselgust loova lahendiga, on siiski oluline sellistes olukordades kohtu toetus inspektsiooni tõlgendustele. Avaliku teabe asjades on ju inspektsioon justkui ise vahekohtu rollis, kuna vaidlejateks on isikud ja teabevaldajad, kelle vahemeheks nii-öelda inspektsioon on.

***„Seega on inspektsioonil kandev roll avaliku teabe asjades praktika kujundamisel, aga ka õigusaktide tõlgendamisel.“***

Selles kohtuasjas tuli ka ehedalt esile nii riigi kui ka omavalitsusasutuste soov kiivalt kaitsta teavet just rahakasutuse küsimustes. Samasugust trendi võib kohata tihti palga-, preemiate ja lisatasu maksmiste küsimustes, aga samal ajal ei tunta ära tihtipeale neid olukordi, kui tuleb isikuandmeid kaitsta.

# AKI PIIRIÜLESES KOOSTÖÖS

Inspektsioon on aktiivne Euroopa Andmekaitsenõukogu liige ning osaleb mitmes rahvusvahelises töögrupis. Kõige tihedam koostöö oli möödunud aastal andmekaitsenõukoguga.

Alates isikuandmete kaitse üldmääruse (üldmäärus) kehtima hakkamisest 25. mail 2018. a on andmekaitseasutuste vaheline piiriülene koostöö täielikult ümberorganiseeritud võrreldes ajaga, mil peamiseks koostöövormiks oli artikkel 29 töögrupi tegevuses osalemine. Lühidalt kirjeldades tõi üldmäärus kaasa *one-stop-shop* süsteemi ning järjepidevuse mehhanismi rakendamise. Esimene neist tähendab asjaolu, et sõltumata isiku (andmesubjekti) asukohast Euroopa Liidus võib ta esitada oma asukoha riigi andmekaitseasutusele kaebuse teises liiduriigis asuva andmetöötleja peale ning antud andmekaitseasutus menetleb või edastab juhtumi menetlemiseks teise riigi andmekaitseasutusele. Selliseid menetlusi lahendatakse ja vahetatakse siseturu infosüsteemis (IMI). IMi kaudu liikuvate menetluste hulk oli 2020. aastal 884.

## Aga miks on vaja ülepiirilisi asju niimoodi menetleda ja mida tähendab järjepidevuse mehhanism?

Põhjus peitubki üldmääruse enda olemuses ehk siis teisisõnu tänapäeva kaubandus ja tehnoloogia maailmas ei ole enam „klassikalisi" riikide piire. Meil ei ole probleem näiteks osta kaupu Hollandis asuvast e-poest või tarbida Itaalias asuva firma teenuseid. Seega on äärmiselt oluline, et ühtsed andmekaitsereeglid ning isiku õiguste tase oleks tagatud kõigis neis riikides. Seda ühtsust ehk järjepidevust saabki tagada läbi andmekaitseasutuste koostöö, ühiste menetluste, ühtsete juhendite jne. Järjepidevuse mehhanismiga seonduvate otsustega saab tutvuda Euroopa Andmekaitsenõukogu veebilehel. Nende otsuste puhul on keskne roll Euroopa Andmekaitsenõukogul, mille liikmeteks on kõik liiduriikide andmekaitseasutused, Euroopa Majanduspiirkonna riikide andmekaitseaustused, Euroopa Andmekaitse Inspektor ning samuti osaleb selle töös (küll ilma hääletusõiguseta) Euroopa Komisjon. Seega Andmekaitse Inspektsiooni olulisim väliskoostöö suund on osalemine Euroopa Andmekaitsenõukogu töös.

Andmekaitsenõukogust on saanud tänu teemade rohkusele ja mahukusele üpris mitmetasandiline organisatsioon. Ei ole mõeldav, et korra kuus toimuv üldplenaar (kus osalevad asutuste peadirektorid) suudaks koostada ja analüüsida kõiki laual olevaid juhendeid, seisukohti, heakskiitmisi ja muid vajalikke otsuseid. Seepärast koosneb andmekaitsenõukogu ka alagruppidest ja rakkerühmadest. Kokku on neid 15. Alagrupid ja rakkerühmad on eriaalaspetsiifilised, näiteks tehnoloogia, sotsiaalmeedia, e-riik, koostöö toimimine jne. Andmekaiste Inspektsioon on üks väiksema töötajate arvuga andmekaitse asutusi Euroopas (nagu me oleme ka Eestis üks väiksemaid asutusi), seega oleme ka rahvusvahelise koostöö suunal sunnitud tegema valikuid, mis on meile prioriteetsed teemad, mille arengutes me tahame rohkem panustada. Sellest lähtuvalt osaleme ka mõnedes andmekaitsenõukogu töörühmades aktiivsemalt ning mõnedes oleme passiivsed liikmed.

Enim kõlapinda leidnud seisukohad ja juhendid, mis andmekaitsenõukogus 2020. aastal koostati ja heaks kiideti puudutasid andmete edastamist välisriiki.

Võib olla ongi paslik öelda, et 2020 oli andmete edastamiste aasta? Suvel ju võeti vastu kauaoodatud Schrems II Euroopa Kohtu otsus, mis mõjutas andmevahetust Ameerika Ühendriikidega, aga samuti oli katkematuks teemaks Brexit ja selle mõju andmevahetusele Ühendkuningriikidega. Lähtudes Schrems II kohtuotsusest koostati kaks väga olulist juhendit andmetöötlejatele: soovitused andmete edastusvahendite täiendavate meetmete osas ja olulised tagatised jälgimismeetmete osas.

Kuid lisaks oli 2020. aasta koroonaviiruse leviku alguse aasta ja see nõudis mitmete selgituste ja juhendite andmist, kuidas andmetöötlus uutes olukordades toimima peaks. Näiteks koostati juhendid asukoha andmete töötlemise lubatavuse osas ja terviseandmete kasutamist koroona-alaste teadusuuringute jaoks ning anti välja seisukoht andmete töötlemise osas koroona kontekstis.

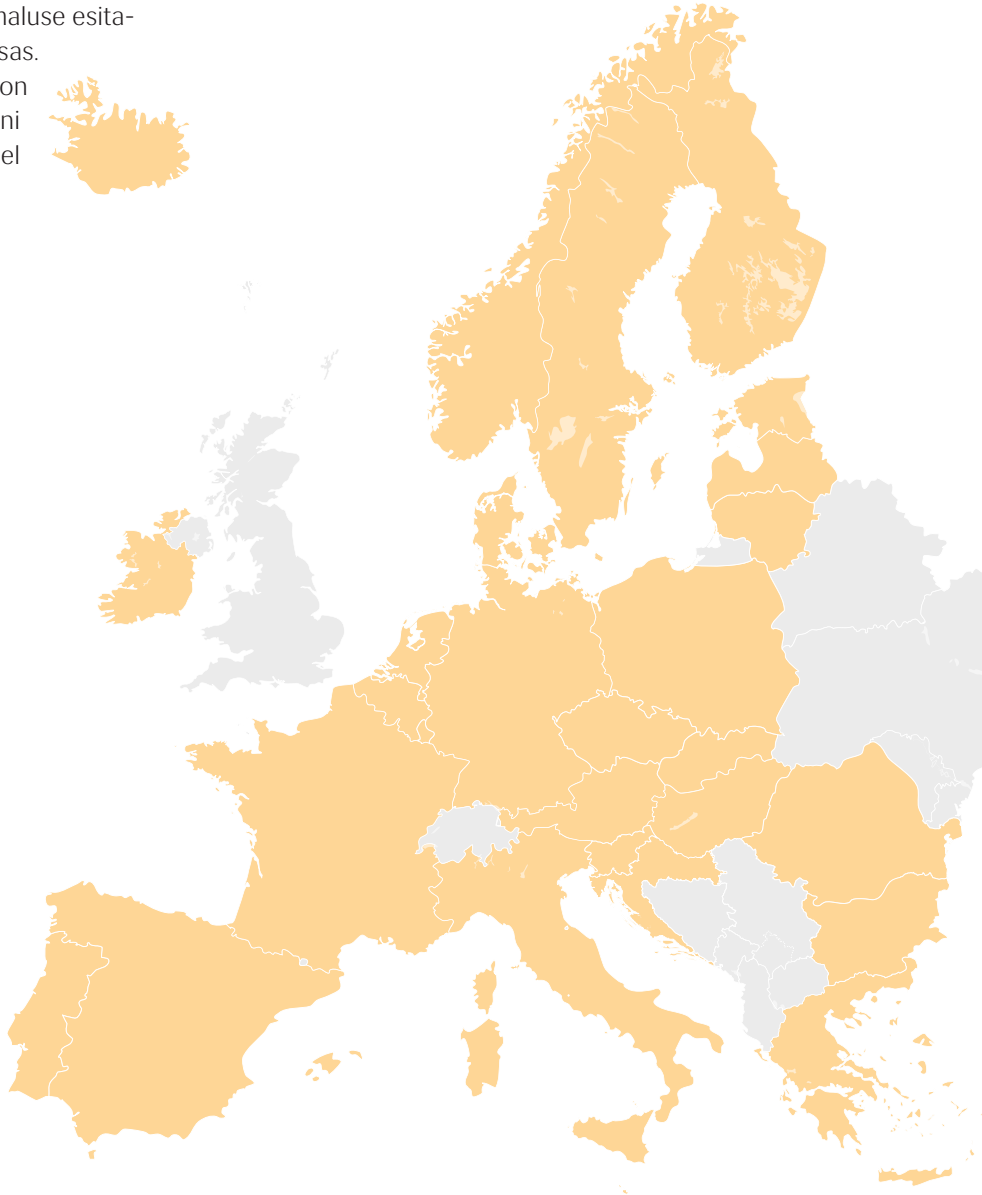
Uuendati ka varem välja antud juhendeid nõusoleku osas ja vastutava ning volitatud töötleja rollide osas. Samuti selgitati ka üldmääruste artiklite olemust, näiteks üldmääruse artikli 23 kohaldamist.

Samuti koostati juhendeid ka erialaspetsiifilisemates teemades, näiteks valmis juhend tehnikavaldkonnast ühendustega sõidukite osas, finantsvaldkonnas teiseste makseteenuste direktiivi ja üldmääruse osas; sotsiaalmeedia valdkonnas kasutajate sihistamise kohta.

Andmekaitsenõukogu tavapärane praktika juhendite koostamisel on ka nende suunamine avalikule konsultatsioonile, andes sellega igale ühele võimaluse esitada oma arvamus juhendi või soovituse osas. Nii mitmedki eelpool mainitud juhendid on alles lõpetanud avaliku konsultatsiooni protseduuri ja ei ole käesoleval hetkel veel lõplikult heaks kiidetud.

## Konventsoon 108

Euroopa Andmekaitsenõukogu ei olnud siiski inspektsiooni ainuke väliskoostöö suund, samas arvestades 2020.a erilisust ei saa näiteks rääkida suurtest rahvusvahelistest konverentsidest, mida loetakse üheks aasta tippsündmuseks. Sellegipoolest toimusid edukalt näiteks Konventsioon 108 andmekaitse komitee online kokkusaamised. Inspektsioon sai anda sisendit nii mõnegi juhendi osas ja heaks kiideti mitmeid märgilisi juhendeid, näiteks näotuvastuse, lasteandmete töötlemise ja hariduse osas, profileerimise, digitaalse identiteedi jms osas.



Euroopa Andmekaitsenõukogus on esindatud:

Austria, Belgia, Bulgaaria, Eesti, Hispaania, Holland, Horvaatia, Itaalia, Iirimaa, Kreeka, Küpros, Leedu, Luksemburg, Läti, Malta, Poola, Portugal, Prantsusmaa, Rootsi, Rumeenia, Saksamaa, Slovakkia, Sloveenia, Soome, Taani, Tšehhi, Ungari, Norra, Island ja Liechtenstein. Lisaks kuulub nõukogusse Euroopa Andmekaitseinspektor.

# TEGEVUSTEST NUMBRITES

## Rikkumisteadete arv kasvas

Andmekaitse Inspektsioon sai 2020. aastal 138 rikkumisteadet, mida oli aasta varasema ajaga võrreldes 20% rohkem. Kõige enam sisaldasid teated infot inimeste tähelepanematusest, lohakusest, teadmatusest põhjustatud eksimustest, kuid teavitati ka tarkvaravigadest põhjustatud rikkumistest ja kavatsetud pahatahtlikest tegevusest kliendiandmebaasidega ning paraku ka jätkuvalt õngitsuskirjadest ja lunavararünnetest.

Veerand kõikidest inspektsioonile tehtud rikkumisteadetest olid seotud õngituskirjade või lunavaranõuete tagajärgedega. Õngituskirjade rünnetest anti kõige rohkem teada erasektorist. Lunavararünnetest teatasid nii avaliku kui erasektori andmetöötlejad. 138-st rikkumisest 54 ehk 39% puudutas avalikku sektorit.
Tarkvaravea või rikke tõttu sai inspektsioon möödunud aastal rikkumisteateid ligikaudu paarikümnel korral. Näiteks registreeriti rikkumisena selline juhtum, kui inimesed said e-postidele teenuseosutaja otsuse, mis tegelikult oli kellelegi teisele mõeldud. Juhtus see aga selle tõttu, et automaatotsuse süsteemi tekkis info sisestamisega viga ja otsus saadeti seetõttu välja sadadele e-posti aadressidele, mis olid valed. See viga avastati ise ja rikkumine lõpetati kiiresti ilma inspektsiooni sekkumiseta.

Tarkvaralised intsidendid avalduvad teinekord ka täiesti ettenägematute asjaolude kokkulangemisel. Näiteks koges kaubandusettevõte juhtumit, mille põhjustas kahe erineva inimese samaaegne lojaalsusprogrammi lepingute allkirjastamine ettevõtte e-teeninduses. Ettevõtte infosüsteem tõlgendas seda aga kui ühte toimingut ja salvestas ainult ühe inimese lepingu, kuid mõlema inimese kliendiprofiili. Selle tulemusel said ühe inimese andmed kättesaadavaks ta teisele isikule.
Tehnilisi probleeme tuli ette nii avalikus kui erasektoris. Samuti registreeris inspektsioon juhtumeid, kus põhjuseks oli nõrk või aegunud turvalahendus. Näiteks oli võimalik kolleegi parooli teades pääseda infosüsteemi ilma, et jääks jälg maha reaalsest andmete vaatajast. Ühel juhul pääses pahalane ligi haridusasutuse infosüsteemi, kuna rakendamata oli VPN ühendus.

*„Kõige arvukamalt anti teada juhtumitest, mis oleks võinud ära jääda, kui töötaja oleks tähelepanelikum ja hoolikam.“*

Selliseid intsidente oli üle poole kõikidest rikkumisteadetest. Kahetsusväärselt palju juhtus inimlikke vigu avalikus sektoris ja seda veebiteenuste või dokumendiregistritega, kus jäetakse tundlikku sisu sisaldav dokument avalikuks või kättesaadavaks inimestele, kellele ei oleks tohtinud info olla kättesaadav.

Nii era- kui avalikus sektoris esines juhtumeid, kus telefoni teel väljastati teavet vale isiku kohta. Põhjuseks mitte piisav helistaja isikusamasuse tõendamine.
Varasematest aastatest rohkematel kordadel teavitati möödunud aastal kliendiandmebaasi vargustest. Kõiki juhtumeid ühendas seik, et kliendiandmebaasid kopeeriti infosüsteemist kaasa uue töökoha jaoks. Kas mindi teise tööandja juurde või alustati ise samalaadse teenuse osutamist.

Valdkonnapõhiselt juhtus kõige sagedamini intsidente tervishoius, sotsiaalvaldkonnas ning finantssektoris. Kindlasti ei anna see üldistus teada kõige probleemsematest andmetöötlejatest. Pigem kõneleb see vastutustundlikust käitumisest ja suuremast teadlikkusest. Andmekaitselise rikkumise registreerimine ja teatud juhtudel inspektsiooni teavitamine on iga andmetöötleja kohus, kui tagajärjeks on tõenäoline oht inimese õigustele ja vabadustele. Info tuleb anda inspektsioonile 72 tunni jooksul peale intsidendi toimumist. Suure ohu korral peab andmetöötleja teavitama ka puudutatud inimesi.

*„Inspektsioon algatas järelevalvemenetluse registreeritud rikkumisteadete peale ligikaudu ühel kolmandikul juhtumitest, et selgitada välja asjaolud ning ära hoida samalaadseid intsidente tulevikus.“*

# INFOLIINILE HELISTATI VÄHEM VÕRRELDES AASTA VARASEMA AJAGA

2020. aastal helistati inspektsiooni infoliinile kokku 1222 korda. Aasta tagasi oli helistamiste koguarv 1578. Väiksem helistamiste arv võis olla põhjustatud sellest, et koroonaviiruse tulek mõjutas töö ümberkorraldust ning seetõttu ei saanud infoliin märtsis kogu aeg töötada ja infoliini töötamise aeg lühenes.

Nõuandetelefoni kõige enimkäsitletud teema oli valvekaamera kasutamine. Helistamiste koguarvust küsiti ligikaudu 250-l korral valvekaamera omaniku kohustuste, inimese õiguste eiramise ja rikkuja karistamise kohta. Valvekaamera kasutamisest või väärkasutamisest tehti lisaks juttu teistes kõnedes, kus helistamise peamiseks põhjuseks oli muu andmekaitsega seotud probleem. Videovalve korraldajate vaatevinklist oli oluline teada saada, miks videovalvel on reeglid?

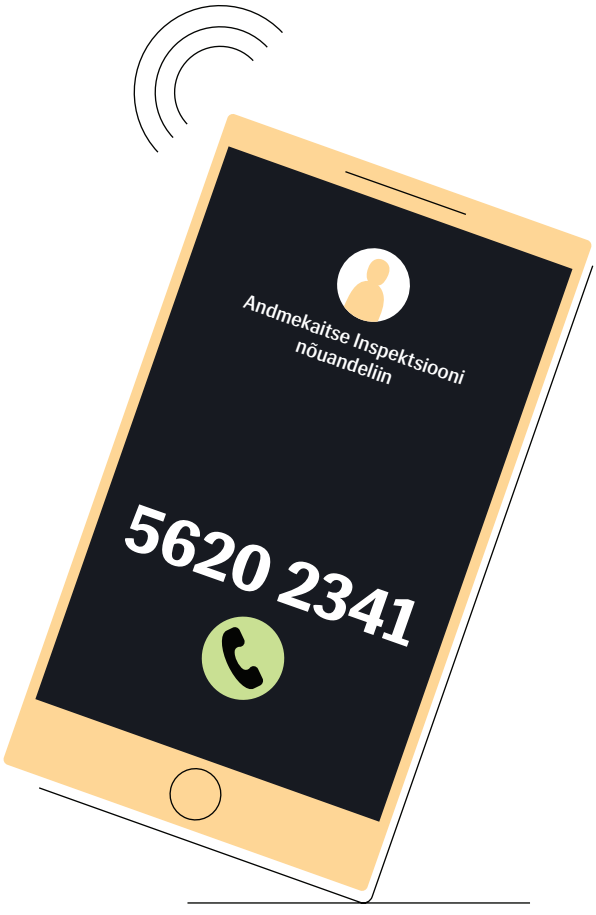
Teised kõned enimküsitud teemadel puudutasid andmete avalikustamist ning kümneid teisi andmekaitse rakendamisega seotud küsimusi.

Läbivad mured olid andmete avalikustamine internetis ja seda nii meediaväljaannetes, sotsiaalmeedias kui veebikülgedel. Samuti oldi murelik e-posti sulgemise pärast peale töölt lahkumist.

*„Uue teemana oli üleval küsimus, kuidas küsida iseenda kohta andmeid.“*

Nõu küsiti ka isikuandmete kaitse üldmääruse rakendamise kohta vastavalt enda tegevusspetsiifikale. Kuid selgitusi paluti samuti, kuidas küsida inimeselt nõusolekut ja millised peavad olema andmekaitsetingimused. Huvi tunti ka selle vastu, mida kirjutada vastutava ja volitatud töötleja vahelistesse lepingutesse ja kuidas teha mõjuhinnangut või kuidas käib andmekaitsespetsialisti ametisse määramine.

Korteriühistutega seonduvad kõned puudutasid kaamerate kasutamist ühistu territooriumil. Võlaandmete teemal küsiti enim inkasso ja kohtutäiturite poolt võlaandmete avaldamise kohta, nt kas inkasso võib töövandjat teavitada võlgnevusest.



# ANDMEKAITSESPETSIALISTIDE ARV KASVAB

Määratud andmekaitseametnike kontaktandmed on avalikustud ettevõtjaportaalis alates 25. maist 2018. Sama aasta lõpuks oli andmekaitsespetsialiste määratud 2782. Aastal 2019 lisandus uue ameti esindajaid 1016 ning 2020 aasta jooksul määrati ametisse 375 andmekaitsespetsialisti.

Seisuga 31.12.2020 oli Eesti äriregistri ettevõtjaportaali märgitud juba 4173 andmekaitsespetsialisti.

| Õiguslik kord | 2018 | 2019 | 2020 |
|---|---|---|---|
| Avalik-õiguslik juriidiline isik, põhiseaduslik institutsioon või nende asutus | 18 | 22 | 26 |
| Kohaliku omavalitsuse asutus | 328 | 668 | 666 |
| Täidesaatva riigivõimu asutus või riigi muu institutsioon | 99 | 121 | 118 |
| Riigiasutuste register | 445 | 811 | 810 |
| Mittetulundusühing | 238 | 341 | 404 |
| Sihtasutus | 90 | 107 | 114 |
| Tulundusühistu | 3 | 7 | 7 |
| MTÜ/SA register | 331 | 455 | 525 |
| Aktsiaselts | 221 | 240 | 231 |
| Euroopa äriühing (Societas Europea) | 4 | 4 | 4 |
| Füüsilisest isikust ettevõtja | 42 | 50 | 49 |
| Osaühing | 1664 | 2127 | 2419 |
| Tulundusühistu | 24 | 28 | 28 |
| Täisühing | 4 | 5 | 6 |
| Usaldusühing | 6 | 8 | 9 |
| Välismaa äriühingu filiaal | 21 | 25 | 24 |
| Äriregister | 1986 | 2487 | 2770 |
| Korteriühistu | | | |
| Korteriühistute register | 20 | 45 | 68 |
| **Kokku** | **2782** | **3798** | **4173** |

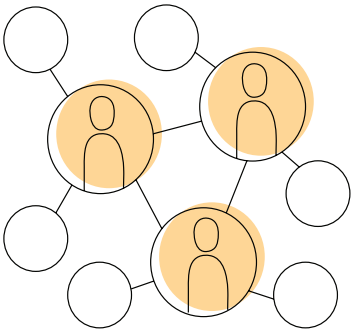
## AASTA TEGEVUSED STATISTIKAS

| TEGEVUSNÄITAJAD | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|
| juhendid (arvestamata seniste uuendamist) | 2 | 1 | - | **1** |
| arvamused õigusaktide eelnõude kohta | 34 | 42 | 8 | **29** |
| **Teavitustöö** | | | | |
| selgitustaotlused, märgukirjad, nõudekirjad, teabenõuded | 1520 | 2384 | 2343 | **1759** |
| kõned valveametniku infotelefonile | 1527 | 2556 | 1578 | **1222** |
| nõustamised (ettevõtetele, asutustele) | 148 | 200 | 79 | **60** |
| koolitused (korraldatud või lektorina osaletud) | 17 | 23 | 15 | **11** |
| **Järelvalvetöö** | | | | |
| ringkirjad (ilma järelevalvet algatamata) | 4 | 8 | 2 | **2** |
| *sh ringkirjade adressaate* | 26 | 162 | 110 | **1108** |
| suuremahulised võrdlevad seired | 10 | 2 | - | **1** |
| *sh seiratute arv* | 129 | 85 | - | **77** |
| kaebused, vaided, väärteoteated (esitatud) IKS, AvTS, ESS alusel | 462 | 462 | 609 | **701** |
| Pöördumised IMI (EL infosüsteem, mille kaudu andmekaitseasutused vahetavad infot jt pöördumisi) kaudu. | - | 479 | 1048 | **884** |
| omaalgatuslikud järelevalveasjad (algatatud) | 149 | 15 | 29 | **28** |
| *sh ennetavad andmekaitseauditid* | 1 | 1 | 0 | **0** |
| kohapealsed kontrollkäigud (järelevalves) | 45 | 17 | 0 | **2** |
| soovitused ja ettepanekud (järelevalves) | 125 | 10 | 63 | **223** |
| ettekirjutused (reeglina eelneb ettepanek; reeglina sisaldab sunniraha-hoiatust) | 64 | 46 | 14 | **37** |
| *sh registreerimise alal (eelneva ettepanekuta)* | 35 | - | - | **-** |
| väärteoasjad (lõpetatud) | 9 | 23 | 14 | **12** |
| trahvid (väärteokaristus), sunniraha (järelevalves) | 4 | 9 | 5 | **12** |
| **Loa- ja erimenetlused** | | | | |
| andmekogude kooskõlastustaotlused (asutamiseks, kasutusele võtmiseks, andmekoosseisu muutmiseks, lõpetamiseks) | 99 | 36 | 39 | **16** |
| loataotlused teadusuuringuteks andmesubjektide nõusolekuta | 54 | 61 | 30 | **32** |
| loataotlused isikuandmete välisriiki edastamiseks | 22 | 3 | 1 | **2** |
| taotlused iseenda andmete suhtes Schengeni, Europoli jt piiriülestes andmekogudes | 8 | 21 | 31 | **10** |
| **Inspektsiooni töötajate arv ja eelarve** | | | | |
| koosseisulisi ametikohti | 19 | 19 | 19 | **19** |
| aastaeelarve (tuhat eurot) | 714 | 717 | 750 | **751** |

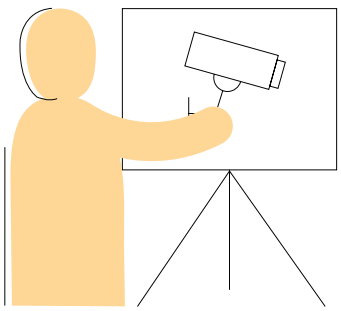
# PILK TULEVIKKU

Möödunud aastal viis inspektsioon (AKI) läbi valitud partnerite hulgas anonüümse küsitluse, et saada tagasisidet seni tehtud tööle. Oma pöördumises uuris AKI ka seda, milline võiks ta olla aastal 2024? Alljärgnev on nägemus partnerite ootustest AKI-le. Tuleviku aastaraamatutest saab teada, kas ka nii läheb.

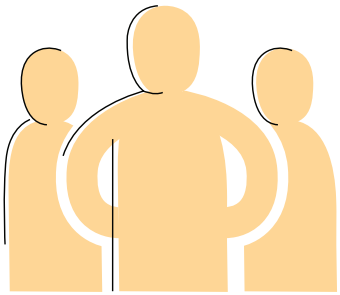
AKI-it näeme kui ennetavat, suunavat, nõustavat ja ühiskonnas diskussiooni vedavat institutsiooni. AKI on kiire ja efektiivne, vajadusel ka jõuline.



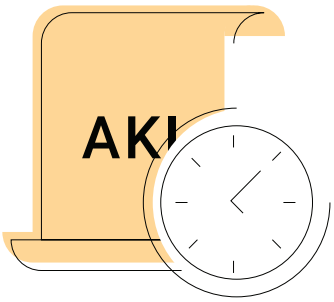
AKI on partner ja koostöövõrgustikud toimiksid (AKSidega nt).



AKI pakub infokirju, koolitusi, jätkuvalt juhendeid. Suhtlemine on läbi digilahenduste lihtne, kiire ja mugav.



AKI on rahastatud ja mehitatud.




Andmekaitse Inspektsiooni nimi on ajast ning viitab ainult järelevalvele ning karistamisele, mitte aga partnerlusele ja nõustamisele.

Sealt see teabenõue tuli
toon oli üsna kuri
väljastage protokoll
see on teie makstud roll.

Teabenõudeid tuli veel
väljastage need ja need
memosid käskkirju nõuti visalt
pidi otsima, et ära hoida  kisa.

Vähe närvi siis ei aja see
kui mõni kodanik nii päevast päeva teeb
kohvinurgas aru pean
Kas keegi lahendust üldse teab?

Kohvinurgas arutelu süttis
kasvav töökoormus kirgi küttis
kohvinurka siis ülemus tuli
kellest oli palju “abi”
ütles, parem tööle kobi
võta ette seadus AvTS
see ei ole üldse paks.

Nii ma laua taha jõudsin
Arvutis kutse AKI infopäevale leidsin
minu esimene küsimus on see
mida ma kujunenud olukorras teen!?

...

Lõpuks ometi ta raatsis
dokumendid ära saatis
küsisin ma 100 lehte
koopiaid palun juurde tehke.

Dokumente oli mulle väga vaja
teadma pean, kuis ehitati külamaja
mitte et ma kiusu ajan
mul on lihtsalt infot vaja.

Kui sõber teabenõudest  kuulis,
tähtsalt kohe suud ta pruukis
ütles “ära pilli lõhki aja”
kellele seda paberipahna on vaja?

Mida tema üldse teab
ise ehitusfirmat pankrotti veab
minul õiglane on meel
usun, et ma sirgel teel.

- S. Heiberg

Rahvusvahelise avaliku teabe päeva puhul toimus 29. septembril konverents, kus inspektsiooni töötajad käsitlesid aktuaalseid teemasid avaliku teabe vallas. Konverentsi juhatas sisse teadaolevalt Eesti esimene avaliku teabe seaduse teemaline luuletus, mis kõlas Contra esituses.