ANDMEKAITSE INSPEKTSIOON

AVALIKU TEABE SEADUSE TÄITMISEST JA ISIKUANDMETE KAITSE TAGAMISEST AASTAL 2019

Aastaettekanne

Aitäh panuse eest aastaraamatusse

Pille Lehis, peadirektor
Maris Juha, järelevalvedirektor
Raavo Palu, õigusdirektor
Urmo Parm, tehnoloogiadirektor
Maarja Kirss, koostöödirektor
Elve Adamson, peainspektor
Sirje Biin, juhtivinspektor
Raiko Kaur, vaneminspektor
Kaspar Uusnurm, andmeturbeinspektor
Kristjan Küti, vaneminspektor
Kadri Levand, vaneminspektor
Maria Muljarova, vaneminspektor
Sirgo Saar, vaneminspektor
Signe Kerge, vaneminspektor
Helve Juusu, vanemspetsialist
Triin Kask, vanemspetsialist

Toimetaja Signe Heiberg, avalike suhete nõunik
Küljendus Kiri Paber Käärid OÜ
Print ja köide Koopia Niini & Rauam
Illustratsioonid: freepik.com, pixabay.com

Andmekaitse Inspektsioon 2020
Tatari 39, Tallinn

Sisukord

AASTA PEADIREKTORI PILGU LÄBI

Vaadates tagasi ja ammutades inspiratsiooni Andmekaitse Inspektsiooni varasematest aastaraamatutest, hakkas silma, et juba mitu aastat on alanud sissejuhatus tõdemusega, et möödunud aasta on olnud muutuste aasta. Ja mis seal salata, kardan, et see eessõna algab üsna samamoodi. Mitte niivõrd seepärast, et 2019. aasta oleks olnud sedavõrd suurte muutuste aasta, vaid see hetk ja olukord, kus me täna viibime, on uudne ja murranguline. Ilmselt veel kaks kuud tagasi oleksin alustanud teisiti.

Täna kirjutan neid ridu hoopis teistsugusest maailmast, kui see oli kaks kuud tagasi – kodust, karantiinist, olles osaline ülemaailmse pandeemiaga võitlusest. Nii mõnedki on öelnud, et maailm ei ole enam kunagi selline, milline ta oli enne viirust COVID-19 ning tulevikus hakkamegi rääkima ajast enne ja pärast laastavat viirust. Võibolla tõesti.

Milline oli siis andmekaitse vaatest maailm enne kevadet 2020 ehk siis aastal 2019?

Andmekaitse Inspektsiooni tööd mõjutas 2019. aastal endiselt isikandmete kaitse üldmääruse jõustumine. Ühelt poolt võib juba kummastav tunduda, et me endiselt räägime üldmäärusest kui uuest nähtusest. Ent teisalt tuleb paraku tunnistada, et selle rakendamise väljakutsed ja kardan, et ka sellest tingitud avastamisrõõmu jätkub veel aastateks. Ärgem unustagem siinjuures ka seda, et eestisisene andmekaitseõigus uueneski alles aastal 2019, mil muutuste aluseks olev isikuandmete kaitse seadus vastu võeti.

Et aga meile kui andmekaitseasutusele üldmäärus veel pikalt uudsena näib ja avastamist pakub, on kindlasti tingitud ka Eesti väiksusest – nii mõnigi olukord võib meie lauale jõuda pikema ooteajaga, kui mõnes suurriigis. Olles osaline väga aktiivselt tegutseva Euroopa Andmekaitsenõukogu töös, on näha, et nii mõnigi üldmääruse tõlgendus- ja rakendusraskus on siiski sama suur sõltumata riigi suurusest. Mis kindlasti aga väikeriigi positsiooni keerukamaks teeb, on ressursi piiratus.

Eesti andmekaitseasutus on pea ainuke asutus Euroopa Andmekaitsenõukogu liikmete seas, kes ei saanud (ega ole saanud siiani) lisaressursse uute ülesannetega toimetulekuks. Jätkuvalt oleme ka üks väiksemaid riigiasutusi Eestis. Samal ajal on ainuüksi rahvusvaheline koostöö kasvanud hüppeliselt. Statistiliste numbritega meie tegevustest on võimalik tutvuda käesoleva aastaraamatu leheküljel 61, kust nähtub, et ainuüksi Euroopa ühise andmekaitseasutuste infosüsteemi kaudu saime enam kui tuhat pöördumist, millest üks osa jõudis ka menetlustena inspektorite töölauale. Euroopa andmekaitse asutuste *„one stop shop"* koostöö käivitamisest ülepiiriliste juhtumite lahendamiseks on pikemalt juttu leheküljel 19.

Ent mitte statistilised numbrid üksi pole olulised. Rahvusvaheline koostöö oma sisult on väga oluline, sest just sealt tekib suur osa teadmist, kuidas üht või teist üldmääruse sätet või meedet tõlgendada või rakendada. Seda nii teiste asutuste kogemustele tuginedes, andmekaitsenõukogu poolt väljatöötatavate juhendmaterjalide koostamise juures aktiivne osaline olles kui ka osaledes ühiskontrollides.

Täna peame oma ressursi piiratuse tõttu tegema veel väga selgeid valikuid, kuhu ja palju panustada saab. Harva oleme kasutanud võimalust pakkuda end andmekaitsenõukogus raportööriks mõne teema vedamisel. Kahjuks oleme loobunud isegi siis, kui teema oleks meie jaoks ühtviisi huvitav ja vajalik, sest raportööriks ehk eestvedajaks olemine andmekaitsenõukogus

tähendab intensiivset tööd, mis saaks toimuda vaid teiste kohest tegelemist nõudvate tööde arvelt.

Siit edasi jõuame veel ühe juba alates üldmääruse jõustumisest üleval olnud põletava küsimuseni. Kus on trahvid? Nagu näitab aastaraamatu statistika, sisu ning ka vaikus uudistes, ei ole me ühtegi üldmääruse järgset hiigeltrahvi teinud. Siit ja sealt Eesti naaberriikide seast on juba kosta esimestest nn pääsukestest. Nii vaadataksegi ühelt poolt hirmunult, kuid teisalt ka etteheitva ja vahel ka üleoleva pilguga meie otsa, et kus on meie trahvid. Ei ole mullegi teadmata nn linnalegend, et inspektsioon ei oska, taha ega suudagi trahvida. See on osati tõsi, aga osati ka mitte. Ühest küljest on, nagu eespool juba kirjeldatud, meie ressurss piiratud ja seda millega, millal ning kuidas tegeleda, tuleb hoolikalt valida. Nii on ka trahvimisega. Teisalt olen mitmel korral juba välja öelnud ja kordan seda siingi, et minu hinnangul ei sobitu üldmääruse hiigeltrahvid Eesti õigusruumi, kuna need on pigem mõeldud haldustrahvidena, mida meie õigusmaastik ei tunnista.

Öelgu skeptikud mida tahes, aga väärteomenetlus on andmekaitseasjades ebamõistlik ja eesmärgipäratu. Seda nii oma karistusmenetlusele omaste kitsaste reeglite, lühikeste aegumistähtaegade kui ka juriidilise isiku vastutuse korral tõendamisraskustega. Väärteomenetlus sobib hästi näiteks kiiruseületamiste või kalastuslubade olemasolu kontrolliks ja rikkumise korral karistamiseks, aga mitte trahvimaks äriühingut ulatusliku andmelekke võimalikuks saamise eest. Keegi ei oota ju, et trahv tabaks õnnetut IT-poissi, kes nupule vajutas. Trahvi peaks saama ikka organisatsioon, kes oma reeglitega või nende puudumisega ja läbimõtlemata ning ebaturvaliste protsesside tõttu sellel juhtuda lasi. Aga mul on hea meel, et jõudsime ka Justiitsministeeriumiga selles küsimuses üksmeelele ning kui elu pöördub tavalise töörütmi juurde, võetakse see ambitsioonikas plaan, mis juba haldustrahvi ellu kutsumiseks loodud oli, taaskord lauale ja töösse.

Aga selle kõigega ei tahtnud ma sugugi trahviootajatele mõista anda, et me jääme vaikselt haldustrahvi regulatsiooni ootama. Sugugi mitte! Lisaks trahvile on meil suurepärane võimalus kasutada mõjutusmeetmena ka sunniraha instrumenti. Sunniraha määramisel on veel lisaks üks boonus – seda saab teha korduvalt ja ta on suunatud mõjutama andmetöötlejat asju korda tegema. Just see on suund, mida peame oluliseks – õiguspärasele käitumisele suunamine, andmetöötlejateni teadmise viimine, miks on oluline inimeste privaatsust kaitsta.

Teemadespekter on lai

2020. aasta üheks läbivaks teemaks ja märksõnaks saab kindlasti olema jälgimisseadmed, eelkõige videojälgimisseadmed. Eelmisel aastal valmis ka Euroopa Andmekaitsenõukogu vastavasisuline juhend, mille juurutamine Eestis on meie üks 2020 eesmärke. Ent ka siin on olulisem trahvidest inimeste mõttemaailma muutmine ja muutumine. Et uueks normaalsuseks saaks avatus ja läbipaistvus, ka videojälgimises. Ehkki silte kaamerate kohta on avalikus ruumis näha justkui küll, ei anna need üldiselt infot selle kohta, kellele parasjagu meid jälgiv kaamera kuulub ning kes andmeid töötleb. Selles vallas tuleb teha selge arenguhüpe.

Olles ise reisihuviline, jäi mulle hiljuti suusareisilt tulles silma Saksamaa kauban-

Foto Gleb Makarov

duskeskus, kus iga poekese eraldi uksel või vaheseinal oli silt selle kohta, kelle kaamera ja mis põhjusel jälgib. Ehkki infot sildil oli omajagu, ei pakkunud see sugugi suuruse poolest konkurentsi poe nimele või seganud vaatevälja nagu tihti on Eestis arvatud. Et kui kogu info sildile panna, ei näe enam poe aknast või uksest väljagi. See ei vasta tõele. Tahtmises on küsimus ja eeskuju on juba võtta küll.

Hiljuti on tõusetunud nii mitmedki teravad andmekaitselised küsimused infotehnoloogia valdkonnast - nagu näiteks mobiilsideandmete kasutus nii riigi kui ka teadusarendajate poolt, terviseandmetel tuginevate mobiilirakenduste arendamine, distantsilt toimuv suhtlus ja selleks kasutatavad e-lahendused – olgu see siis õppetöös, e-meditsiinis või kaugtööl. Kõik need teemad on ühelt poolt väga tehnilised, ent teisalt väga selgelt ja intensiivselt seotud isikuandmete töötluse ja privaatsusega. Just andmete töötlemine infotehnoloogiliste vahendite abil läbiviidavates teadusuuringutes ning infosüsteemide ja e-keskkondade kasutus meditsiini - ja haridusvaldkondade asutustes, oleme markeerinud endale oluliste 2020 märksõnadena.

Isegi kõige parimaid lahendusi ühiskonnale pakkudes tuleb arvestada, et ilma andmekaitselise läbimõtlemiseta on lahendus puudulik ning heast ideest saab hoopis kasvulava probleemidele. Kõigepealt tuleb riigil, olles ühe suurema kui mitte suurima andmetöötleja rollis, vastutust tunnetada ja eeskujuks olla. Kindlasti ei ole hea eeskuju kiirustades ja mõtlemata ning mis veelgi olulisem – läbi arutamata seadusmuudatuste sisseviimine näiteks egiidi all, et „kiired ajad vajavad kiireid otsuseid“, kuid teades seejuures hästi, et kellelgi ei tule pärast „kiiret aega“ meelde ajutiste sätete juurde tagasi tulla, et need siiski lõpuni läbi mõelda ja arutada. Nii võib juhtuda, et inimestele mitte üksnes ei jää tunne, et kriisi varjus püütakse sisse viia muudatusi, mis riivavad nende privaatsust ja mis jäävad mõjutama nende elu ka siis, kui kriis möödas, vaid nii võib ka minna.

Üsna sama lugu on innovatsiooni ja IT-arendustega. E-riigis on mõlemad väga vajalikud. Nii mina isiklikult, kuid ka usun, et enamik eestlasi on pigem avatud mistahes uutele lahendustele, mis elu lihtsustavad, sealhulgas tehisintellektidele. Nii mõnigi

meist astuks igapäevaelu korraldamise lihtsustamise nimel sammu kaugemale ning tervitaks näotuvastustehnoloogiaid, kui see tema aega aitab kokku hoida, aga me ju tahame olla kindlad, et teenuse osutamise taga ei toimu nähtamatuid andmetöötluse protsesse, mis õõnestavad privaatsust. Seda ka suhtes riigiga.

E-riigi areng on väga oluline ja oodatud. Ent mistahes IT-arendusi luues ja arendades tuleb silmas pidada, et selle protsessi käigus me ei mängiks inimeste pärisandmetega. Iga arendus olgu läbimõeldud, turvaline ja läbipaistev.

Lõpetuseks tahan tänada oma meeskonda. Nagu öeldud, ei olnud 2019 inspektsioonile lihtne aasta. Konkurents tööjõuturul lõi valusalt ka inspektsiooni töötajaskonda. Samas andis see võimaluse kaasata meie tegemistesse mitmeid uusi ja tegusaid inimesi, kelle esimestest saavutustest saame juba järgnevatel lehtedel lugeda, kuid kes sära silmades ootavad juba uusi väljakutseid aastal 2020. Samas jätab iga õppeprotsess oma jälje – näiteks jõudlusesse. Nii võibolla olid plaanid 2019. aastaks ambitsioonikamad, just järelevalve valdkonnas, kui teoks said. Ent sellegipoolest võib öelda, et oli tegus ja õpetlik aasta ning inspektsioonil tuli tegeleda lisaks igapäevatööle nii mõnegi märgilise tähtsusega projektiga.

Ma tänan koostööpartnereid ja kolleege ministeeriumitest, ametitest, omavalitsustest ning partnerorganisatsioonidest. Samuti tänan avaliku teabe nõukogu liikmeid.

Tänan ka kõiki inimesi, kes on meie poole ühel või teisel viisil pöördunud ning tänu kellele on meil lihtsam mõista, kuhu oleme oma sõnumiga jõudnud, milliste edusammude üle võime uhked olla aga ka seda, kuhu oma teravikku edaspidi suunata võiks.

Pille Lehis
Andmekaitse Inspektsiooni peadirektor

Muutus veebiküpsistest teavitamise kord

Andmekaitse Inspektsiooni üks kohustustest on olnud teostada järelevalvet veebiküpsiste kui isikuandmete õiguspärase kasutamise üle.

Märgiline kohtuotsus

Veebiküpsiste õiguspärane kasutamine nõudis aasta teises pooles teenuseosutajatelt senise praktika muutmist. Kui Euroopa Kohus võttis vastu 1. oktoobril 2019 otsuse C-673/17[1], tuleb võtta kõikide veebiküpsiste osas, mis ei lähe e-privaatsusdirektiivi erandi alla, kasutajatelt aktiivne nõusolek. Olenemata sellest, kas veebiküpsised võimaldavad isikuandmete töötlemist või mitte.

Meenutuseks, et küpsiste varasem regulatsioon tugines e-privaatsusdirektiivil 2002/58/EÜ[2], mida muudeti direktiiviga 2009/136/EÜ[3]. Selle kohaselt pidid võrgulehed hakkama kasutajalt alati võtma nõusolekut, kui leht salvestab tema seadmesse teavet ja omab ka eelnevalt salvestatud infole juurdepääsu. Nõusolekut ei pidanud küsima ainult juhul, kui teabe salvestamine ja sellele juurdepääs on teenuse osutamiseks hädavajalik või selle ainus eesmärk on side edastamine elektroonilises sidevõrgus.

Kuna Eesti õigusruumi ei ole e-privaatsusdirektiivi küpsiste sätet üheselt üle võetud, lähtus inspektsioon kuni oktoobris tehtud kohtuotsuseni isikuandmete kaitse üldnormidest, mille järgi ei olnud vaja võtta kasutajalt nõusolekut, kui veebiküpsiste abil ei toimu inimeste tuvastamist ehk isikuandmete töötlemist. Piisas, kui võrgulehtedel oli teave veebiküpsiste kasutamise kohta.

[1] https://op.europa.eu/en/publication-detail/-/publication/fc7c68f2-1a57-11ea-8c1f-01aa75ed71a1/language-et

[2] https://eur-lex.europa.eu/legal-content/ET/LSU/?uri=CELEX:32002L0058

[3] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex:32009L0136

Mis on veebiküpsised?

Veebiküpsised on väiksed tekstifailid, mis salvestatakse kasutaja seadmesse võrgulehtedel käies. Küpsiste eesmärk on parandada kasutuskogemust ja isikupärastada navigeerimist.

Euroopa Kohtu otsus muutis nii mõndagi. Muutus see, et erandeid ei ole ja igasugune veebiküpsis nõuab nõusolekut. Millises mahus peab aga küpsiste kasutamisel rakendama isikuandmete kaitse üldmääruse (IKÜM) artikleid 13 või 14, jäi ebaselgeks. Kohtuotsuse kohaselt peavad veebikasutajad olema samuti teadlikud küpsiste kasutamise kestvusest ning olema informeeritud, kas kolmandatel isikutel on küpsistele juurdepääs.

Nagu me teame, koguvad statistikat ja jälgivad käitumist sageli nn kolmanda osapoole küpsised, millele tugineb täna valdavalt ka interneti reklaamitööstus. Kuna kolmanda osapoole küpsised on kasutajatele üldjuhul arusaamatud ja kasutuseesmärgilt läbipaistmatud, kujutavad need inimeste privaatsusriivele kõige enam ohtu.

Euroopa Andmekaitsenõukogu on asunud selle pilguga oma varasemaid juhiseid üle vaatama ja võtnud eesmärgiks 2020 aasta esimesel poolel anda täiendavad suunised. Euroopa andmekaitseasutustel tuleb 2020. aastal tegeleda sellega, et suures plaanis oleks veebiküpsiste praktika Euroopas ühetaoline ja kindlasti tuleb anda ettevõtjatele suurem õigusselgus. Eriti puudutab see piiriüleseid teenuseid.

Samuti peavad veebiteenuse osutajad küpsiste teavituses kasutajatele selgitama, mis on konkreetse küpsise eesmärk, kes küpsise seadmesse paneb ja selle üle kontrolli omab ning kas ja kuidas lahendada nõusoleku võtmine erinevate eesmärkide korral.

Biomeetriliste andmete käsitlus uuenes

Euroopa Andmekaitsenõukogu 2019. aastal avaldatud videojälgimise juhis nutikatele ja traditsioonilistele kaameratele asus biomeetriliste isikuandmete osas võrreldes varasema arusaamaga teisele seisukohale, kuid kaamerate kasutamise reeglid jäid uues videojuhises põhimõtteliselt endiseks.

Uuenenud biomeetria käsitluse järgi kuuluvad eriliigiliste andmete alla liigituvate biomeetriliste isikuandmete hulka nii inimese kohta saadud unikaalne info ilma, et tema isikut nimeliselt tuvastataks kui ka biomeetria töötlemisest saadavad koodid ehk räsi. Varem käsitleti räsi tavaliste isikuandmetena. Meenutuseks, et varasem andmekaitsedirektiiv võimaldas sellist õiguslikku konstruktsiooni, kus räsitud biomeetrilised kujutisi ehk koode või malle oli võimalik käsitletada nn tavaliste, mitte eriliigiliste (varasemalt delikaatsed andmed) isikuandmetena. Selliste isikuandmete töötlemise õiguslik alus sai olla ka isikuga sõlmitud leping.

Isikuandmete kaitse üldmääruse (IKÜM) rakendumisel olukord aga muutus. Isikute kordumatuks tuvastamiseks kasutatavast biomeetriast said eriliigilised isikuandmed ning kohaldama tuli hakata IKÜM artikkel 9 erisusi, sõltumata sellest, millisel kujul biomeetriat töödeldakse või säilitatakse (nt kujutis, mall, või räsi). Eriliigilisi andmeid ei ole lubatud töödelda lepingu täitmiseks või õigustatud huvi alusel ning ainsaks sobivaks õiguslikuks aluseks sai nõusolek, mille võtmiseks on oma kindlad reeglid.

Muutusest täpsemalt

Biomeetrial põhinevate lahenduste kasutamisel tuleb nüüd lähtuda IKÜM artiklis 6 toodud õiguslikelt alustest, koosmõjus artikkel 9 erisustega. Siseriiklikult võib biomeetria töötlemist täpsustada, aga 2019. aasta jaanuaris jõustunud isikuandmete kaitse seadus (IKS) ega sama aasta märtsis kehtima hakanud isikuandmete kaitse seaduse rakendusseadus organisatsioonidele vajalikku erisätet biomeetria kasutamiseks ei toonud. Sestap ei ole töö- ja kliendisuhetes enam õigust biomeetriat töödelda näiteks ruumidesse ligipääsudel, videovalves või teeninduses ning turunduses, ilma et isik ei oleks andnud selleks vabatahtlikku nõusolekut.

> Inimeste kordumatuks tuvastamiseks kasutatavast biomeetriast said üheselt eriliigilised isikuandmed.

Nõusoleku kui õigusliku aluse kasutamisel ei tohi unustada, et see on isiku vabatahtlik tahteavaldus ja nõusolek peab olema antud eespool toimingut, ehk siis enne, kui sõrmejälg seadmesse loetakse või nägu kaameraga skaneeritakse. Nõusolekut saab kasutada ainult nende töötajate osas, kes on selleks nõus. Teiste töötajate jaoks peab tööandja võimaldama alternatiivseid tuvastusvahendeid (nt kiipkaart).

Nõusoleku kasutamise juures tuleb arvestada, et isik võib selle iga ajal tagasi võtta. Põhimõtteliselt tuleb arvestada, et kui tööandja kasutab ruumidesse ligipääsuks või tööajaarvestuseks biomeetrial põhinevat lahendust nõusoleku alusel, on see igal hetkel tagasipööratav ehk teadmata pikkusega ajutine lahendus.

Oluline on rõhutada, et biomeetrilisteks andmeteks loetakse kõiki inimese unikaalseid füüsilisi, füsioloogilisi ja käitumuslikke omadusi ka siis, kui ei ole nimeliselt teada, kellele biomeetria kuulub. Näiteks ei ole nõusolekuta lubatud olukord, kus kaubanduset-tevõte soovib biomeetrilise tehnoloogiaga jälgida, milline

on iga poodi siseneja liikumisharjumus, suutes eristada inimese täpsusega, milliste kaubakategooriate juurde ning millises järjekorras konkreetne ostleja läheb.

Inspektsioon on juhtinud seadusandja tähelepanu biomeetrilise andmetöötlusega seonduvale õiguslikult ebakindlale olukorrale ja vajadusele kehtestada täiendavad siseriiklikud normid. Seni, kuni seda tehtud ei ole, on Eestis võimalik biomeetrilisi isikuandmeid töödelda ainult avalikul sektoril kindlate toimingute raames. Näiteks on võimalik biomeetriat töödelda isikut tõendavate dokumentide seaduse alusel toodud eesmärgil ja olukorras. Erasektor saab biomeetrilisi isikuandmeid töödelda ainult nõusoleku alusel.

Millised olid rikkumised ja nende põhjused?

Inimeste privaatsus oli inspektsioonile edastatud rikkumisteadete järgi ohus 2019. aastal 115. korral, kuna inspektsioon registreeris aasta jooksul selles arvus intsidente.

Intsidente juhtus nii riigi- ja omavalitsusasutustes, tervishoiu,- finants,- transpordi,- side - kui haridusteenusteste valdkonnas. Suur osa nendest leidis aset veebiteenuste osutamisel.

Sageli oli eksimise põhjus aegunud või turvamata tarkvara kõrval just töötaja tähelepanematus või puudulik teadlikkus, näiteks finantsasutuse aegunud võlaandmete avaldamine. Kui rikkumisi üldistada, siis võibki need jagada kahte kategooriasse – (1) tehnoloogiast tingitud intsidendid ning (2) inimtegevus, olgu siis kas üksikeksimus või lohakus mille tagajärjel võib sündida kahju paljudele teistele inimestele.

> Isikuandmetega seotud rikkumine tähendab andmete ebaseaduslikku või juhuslikku hävimist, kättesaamatuks muutumist või lubamatut juurdepääsu ja avalikuks saamist.

Paljud eksimused juhtusid hooletusest ja teadmatusest. Näiteks oli üks sellistest õngitsuskirja avamine. Kõik andmetöötlejad peaksid olema õngituskirjade ärahoidmiseks suutelised rakendama levinud turvatehnoloogiad nagu DMARC protokoll või e- kirjade turvalist edastamist võimaldavat STARTTLS krüpteerimismeetodit.

> Üldine teadlikkus andmekaitsest ei ole kahjuks veel kindlasti jõudnud tasemele, kus võiksime igas olukorras teenusesaajatena end alati turvaliselt tunda.

Möödunud aastasse jääb ka selliseid juhtumeid, kus töötaja eksimuse pärast andmekaitsereeglite vastu otsustas ettevõte ta vallandada. Äärmuslikku meedet rakendati näiteks ettevõttes töötajate suhtes, kes vaatasid aluseta teise inimese andmeid infosüsteemist. Samuti lõpetati tööleping töötajaga, kes lubas turvasalvestistele ligi kolmandaid isikuid. Töötaja hooletus põhjustas vallandamise neljal korral.

Rikkumisest teatajate arv oli võrreldes 2018. aastaga suurem. Samuti kasvas rikkumisteadete kuupõhine koguarv 16%. võrra. Kuid arvestades ainuüksi inspektsioonile edastatavaid märgukirju võib järeldada, et kõik vastutavad andmetöötlejad juhtunud intsidentidest veel ei teavita ning isikuandmetega juhtub ilmselt rohkem, kui registreeritakse.

Üldine teadlikkus andmekaitsest ei ole kahjuks veel kindlasti jõudnud tasemele, kus võiksime igas olukorras teenusesaajatena end alati turvaliselt tunda. Selliseid juhtumeid, kus töötaja

avaldab valele adressaadile näiteks e-postiga kellegi tundlikud andmed, ei saa kunagi lõpuni ära hoida. Kui aga valed inimesed saavad infosüsteemi puuduliku seadistuse tõttu ligipääsu suure hulga klientide tundlikule eraelulisele infole või kasutajakonto andmetele, siis niisuguseid juhtumeid peaks saama küll koolitustega ära hoida. Samuti saab ennetada lekkeid dokumendiregistritest, kus ka möödunud aastal avastati mitme riigiasutuse dokumendiregistritest avalikke piiratud juurdepääsuga dokumente.

Isikuandmete kaitse üldmääruse (IKÜM) kohaselt peab vastutav andmetöötleja isikuandmetega seotud rikkumisest inspektsiooni teavitama. Rikkumisteadete esitamise kohustus algas 2018. aasta 25. maist.

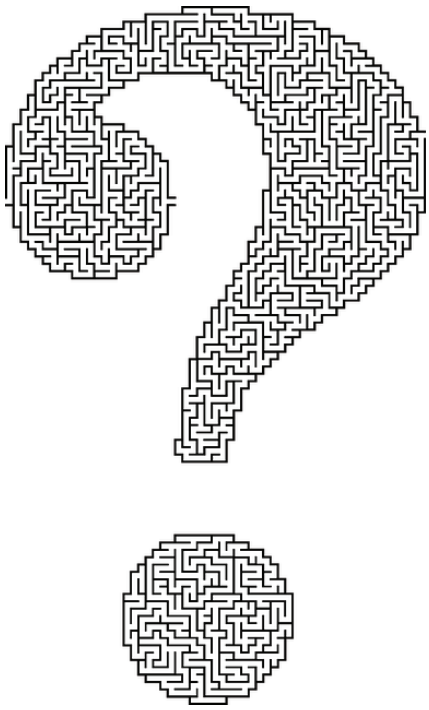
Isikuandmetega seotud rikkumine tähendab andmete ebaseaduslikku või juhuslikku hävimist, kättesaamatuks muutumist või lubamatut juurdepääsu ja avalikuks saamist. Kui juhtum põhjustas või võib tõenäoliselt põhjustada inimestele märkimisväärset kahju, tuleb sellest 72 tunni jooksul inspektsioonile teatada.

Rikkumine ei toonudki suurt trahvi

Kuigi ootus Eesti esimese suure trahvi määramiseks oli olemas, ei määratud rikkumiste eest 2019. aastal suurt trahvi. Näiteks jäi selline trahv määramata rattaringluse süsteemis toimunud andmekaitselise rikkumise eest, kus piirduti noomitusega.

Tartu Linnvalitsus edastas inspektsioonile 8. juunil rikkumisteate, mille kohaselt oli volitamata isikutel võimalik Tartu rattaringluse süsteemis API kaudu juurde pääseda 20 0000 registreerunud kasutajate andmetele. Seda nii kasutaja enda poolt sisestatud andmetele kui ka kasutajate teostatud sõitude andmetele.

Lisaks oli võimalik muuta rataste parklate asukohti, neid kustutada ning lisada juurde uusi parkla-alasid ehk andmetega manipuleerida. Andmetele juurdepääs toimus kahel erineval



viisil: avalike veebilinkide kaudu oli nähtav informatsioon kasutajate kohta: nimi, e-posti aadress, telefoninumber, kasutaja ID, registreerimise aeg, staatus (aktiivne/mitteaktiivne). Lisaks oli võimalik näha isiku bussikaardi numbrit kasutaja kasutaja ID-ga kokku viies.

Süsteemi registreerunud kasutajale sai võimalikuks näha järgmisi andmeid: kasutajate sõitude andmed (millisest dokist/peatusest on võetud ratas ning võimalik oli tuvastada kasutaja poolt läbitud sõiduteekond ja aeg).

Juurdepääs andmebaasile avalike veebilinkide kaudu sai küll kiiresti kõrvaldatud, kuid vaatamata sellele alustas inspektsioon 9. juulil järelevalvemenetlusega rikkumisteates esitatud asjaolude väljaselgitamiseks.

Inspektsioon monitooris põhjalikult rattaringluse süsteemi ja tutvus Tartu Linnavalitsuse esitatud raportitega ning leidis, et sisuliselt oli tegemist rattaringluse süsteemi turvanõrkusega, mille põhjuseks ei olnud inimlik pahatahtlikkus. Kuna turvanõrkus sai kiiresti likvideeritud, lõpetas inspektsioon menetluse soovitusega teha enne uue rakenduse tööle laskmist põhjalikumat kontrolli.

Selgines teadusuuringute lubade taotlemise kord

Kuni uue isikuandmete kaitse seaduse (IKS) jõustumiseni 15. jaanuaril 2019 andis inspektsioon lubasid kõikidele teadusuuringutele, sõltumata sellest, kas uuringus kasutati tavalisi või eriliigilisi isikuandmeid. Uus IKS muutis teadusuuringuteks lubade väljastamise korda ja lisandus uus teadusuuringu valdkond - poliitikakujundamise eesmärgil tehtavad uuringud.

Inspektsiooni hinnata ei olnud enam need teadusuuringud, kus kasutatakse eriliigilisi isikuandmeid ja kus teadusvaldkonnal oli oma eetikakomitee. Inspektsiooni pidi tegelema teadusuuringu loa väljastamise protsessiga ainult siis, kui teadusvaldkonnal puudus eetikakomitee. Seega, suurema vastutuse said uue seaduse jõustumisega teadusvaldkondade eetikakomiteed, kellele pandi ülesandeks lubade väljastamine eriliigiliste andmetega läbiviidavateks uuringuteks.

Inspektsioon sai ülesandeks hoopis poliitikakujundamise uuringute hindamise juhtudel, kui asutus soovis kasutada uuringus teise vastutava (nt teise ministeeriumi) või volitatud töötleja andmekogus olevaid isikuandmeid ning uuringu läbiviimise eesmärki ja töötlemise ulatust ei olnud sisse kirjutatud õigusakti.

Poliitikakujundamise uuringutega tõusetus aga mitmeid küsimusi. Näiteks, kes peale ministeeriumide veel võib läbi viia poliitikakujundamise uuringuid? Nimelt esitasid inspektsioonile loataotlusi ka ministeeriumi valitsemisalas olevad asutused, kes soovisid uuringuid teha ennekõike asutuse töö korraldamiseks. Inspektsiooni hinnangul ei võimalda IKS § 6 lg 5 uuringuid teha asutuse töö korraldamiseks. Selle seaduse § 6 lg 5 on mõeldud üksnes poliitika kujundamiseks, mida saavad teha üksnes poliitika kujundajad (ministeeriumid), kui uuring teostatakse tema seadusest tuleneva avaliku ülesande raames.

Teise olulise küsimusena tõusetus, kes peavad väljastama poliitikakujundamise uuringuks loa, kui uuringus kasutatakse eriliigilisi isikuandmeid? Kas piisab ainult inspektsiooni loast või peab loa andma ka eetikakomitee? IKS § 6 lõike 5 sõnastus on ebamäärane, mitmeti mõistetav ja tõlgendatav ning seletuskiri sellele kahjuks vastust ei anna, kas § 6 lõige 5 sätestab erisuse § 6 lõikest 4.

> Poliitikakujundamise uuringuteks, kus kasutatakse eriliigilisi isikuandmeid, tuleb läbida nüüd kaheastmeline kontroll.

IKS § 6 lõike 5 kolmas lause on järgmine: „Andmekaitse Inspektsioon kontrollib enne nimetatud isikuandmete töötlemise algust käesolevas paragrahvis sätestatud tingimuste täitmist, välja arvatud juhul, kui poliitika kujundamiseks tehtava uuringu eesmärgid ja isikuandmete töötlemise ulatus tulenevad õigusaktist.“ Samas tuleneb IKS § 6 lõikest 4, et kui teadusuuring põhineb eriliiki isikuandmetel, siis kontrollib asjaomase valdkonna eetikakomitee enne käesolevas paragrahvis sätestatud tingimuste täitmist. Seega tekib olukord, kus inspektsioonilt loa taotlemise eelduseks on eetikakomitee luba ja eetikakomitee loa eelduseks on inspektsiooni luba, sest mõlemad peavad kontrollima enne loa andmist „käesolevas paragrahvis sätestatud tingimuste täitmist“.

Justiitsministeeriumi ja Sotsiaalministeeriumiga toimunud kohtume viis kokkuleppeni, et enne inspektsiooni poole pöördumist peab olema eetikakomitee luba, kui teadusvaldkonnal on eetikakomitee olemas. Seega, poliitikakujundamise uuringuteks, kus kasutatakse eriliigilisi isikuandmetel, tuleb läbida nüüd kaheastmeline kontroll.

Asutati Eesti Bioeetika ja Inimuuringute Nõukogu

Inspektsioon on nõukogus ekspertliige

2019. aasta numbrisse jääb Eesti Bioeetika ja Inimuuringute Nõukogu (EBIN) asutamine. Oktoobrist alates, mil nõukogu asutati, on inspektsioon selle liige eksperdina.

EBINi asutamisega selgines mitmeid korralduslike küsimusi seoses eriliigiliste andmetega teadusuuringute läbiviimisel.

EBIN sai eetikakomiteena ülesandeks hakata menetlema teadusuuringute taotlusi nii geenivaramust kui e-tervisest pärinevate isikuandmete töötlemiseks.

EBINi loomisega ühendati ka varasemalt Sotsiaalministeeriumi juures tegutsenud biomeditsiiniliste ja inimuuringu eetikaga tegelenud komiteed.

Jälgimisseadmed ja õigustatud huvi

Üleeuroopalise isikuandmete kaitse üldmääruse (IKÜM) kehtima hakkamisega tõstatusid siseriiklikus õiguses päevakorda jälgimisseadmete kasutamisega seotud õiguslikud küsimused, kuna enam ei olnud võimalik jälgimisseadmete kasutamisel toetuda varasemalt enimkasutust leidnud üldsõnalisele turvalisuse tagamise eesmärgile, mida võimaldas isikuandmete kaitse seaduse (IKS) § 14 lg 3. Sellega seoses hakati erasektoris kasutama õigusliku alusena õigustatud huvi, kuid seda puudujääkidega.

> Õigustatud huvi kui õiguslikku alust isikuandmete töötlemiseks ei tohiks valida automaatselt ega põhjendamatult laiendada selle kasutusala, eeldades, et see võiks olla andmetöötleja jaoks vähem piiravam, kui seda on teised alused.

IKÜM 2016/679 artikli 6 lõike 1 punkti f kohaselt on isikuandmete töötlemine vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral, kui sellist huvi ei kaalu üles andmesubjekti huvid või põhiõigused ja vabadused ning seda eriti juhul, kui andmesubjektiks on alaealine, kelle eest saab otsustada tema seaduslik esindaja. Õigustatud huvi kui õiguslikku alust isikuandmete töötlemiseks ei tohiks valida automaatselt ega põhjendamatult laiendada selle kasutusala, eeldades, et see võiks olla andmetöötleja jaoks vähem piiravam, kui seda on teised alused.

Selleks, et isikuandmete töötlemine õigustatud huvi alusel oleks seaduslik, näeb IKÜM artikkel 6 punkt f ette kaks tingimust:

1) isikuandmete töötlemine peab olema vajalik vastutava töötleja või andmeid saava kolmanda isiku või kolmandate isikute õigustatud huvide elluviimiseks,

2) andmesubjekti põhiõigused ja vabadused ei kaalu neid huve üles. Seega kohustab viidatud säte vastutavat töötlejat võrdlema enda ja/või kolmanda isiku õigustatud huve andmesubjekti(de) huvide ja põhiõigustega.

Kahtlemata on õigus eraelu puutumatusele konfliktis põhiseaduses sätestatud õigusega ettevõtlusvabadusele. Siinkohal ongi vaja antud aluse kasutamise tingimuseks läbi viia huvide tasakaalustamine.

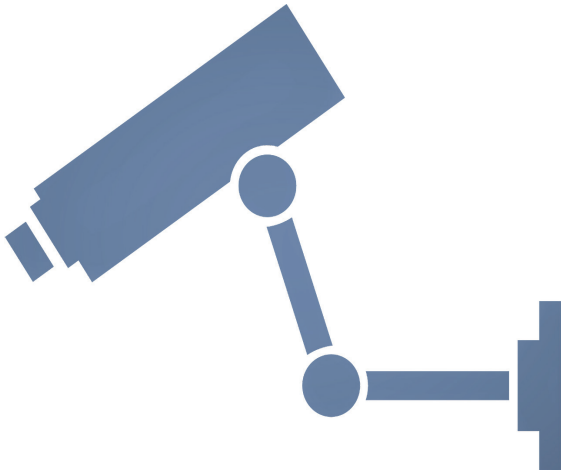
Ettevõtlusvabaduse piiramiseks piisab igast mõistlikust põhjusest ning saab asuda kindlalt seisukohale, et teiste isikute õiguste ja vabaduste kaitse vajadus on kaalukas ning õiguspärane piirangu alus. Proportsionaalsuse põhimõtte järgi peavad õiguste ja vabaduste piirangud olema demokraatlikus ühiskonnas vajalikud, mida tuleb hinnata kasutades proportsionaalsuse kontrollimise skeemi, mis koosneb kolmest astmest: 1) abinõu sobivus ja eesmärk, 2) abinõu vajalikkus ja 3) proportsionaalsus kitsamas tähenduses ehk mõõdukus.

Isikuandmete töötleja peab andmete töötlemisel alati eelnevalt hindama, kas andmetöötlus on ikka tõesti eesmärgi täitmiseks vajalik ning kas just sellises ulatuses.

„Eesmärgi" mõiste on omavahelises seoses „huvi" mõistega, kuid siiski sellest erinev. Näiteks võib ettevõtjal olla huvi oma ettevõttes töötavate inimeste tervise ja ohutuse tagamine, mis tagab üldise edukuse ja jätkusuutlikkuse. Sellega seoses võib ettevõtja eesmärgiks olla teatud meetmete rakendamine, mis aitavad tagada töötajate tervist ja ohutust.

Põhiõiguste ja vabaduste riive pole vajalik ja on seadusevastane siis, kui on olemas mõni teine vahend, mis aitab seatud eesmärki saavutada sama hästi, kuid ei riiva isiku õiguseid nii tugevalt. Isikuandmeid tuleb töödelda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks. Isikuandmete töötleja peab andmete töötlemisel alati eelnevalt hindama, kas andmetöötlus on ikka tõesti eesmärgi täitmiseks vajalik ning kas just sellises ulatuses või siiski on muid vähem riivavamaid meetmeid selle eesmärgi täitmiseks. Valikuvõimaluse korral tuleb eelistada isiku põhiõigusi vähem riivavaid meetmeid.

Tuleb lähtuda reeglist, et abinõu on proportsionaalne üksnes siis, kui see on püstitatud eesmärgi saavutamiseks sobiv (kohane),



vajalik ja mõõdukas. Mõõdukas on abinõu niivõrd, kuivõrd põhiõigusesse sekkumise ulatust ja intensiivsust õigustab eesmärgi kaalukus.

Sõltumata sellest, missugusele alusele andmetöötleja tugineb, peab ta tagama, et andmesubjektide andmete töötlemine peab olema seaduslik, õiglane ja läbipaistev.

Seaduslik saab isikuandmete töötlemine olla üksnes siis, kui isikuandmete töötlemiseks esineb seadusest tulenev alus. Õiglane on andmetöötlus juhul, kui andmetöötleja arvestab töötaja andmete töötlemisel viimase õiguspäraste ootustega privaatsuse kaitse osas. Läbipaistvuse põhimõte eeldab aga seda, et isikuandmete töötlemisega seotud teave ja sõnumid on lihtsalt kättesaadavad, arusaadavad ning selgelt ja lihtsalt sõnastatud.

Oluline on ka töötlemise eesmärgi piirang, mille järgi peab tagama, et isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ja õiguspärastel eesmärkidel ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus. Lisaks ei ole vähem olulised ka teised andmete töötlemise nõuded, milleks on minimaalsuse ehk võimalikult väheste andmete kogumise, samuti õigsuse, säilitamise piirangu ning usaldusväärsuse ja konfidentsiaalsuse nõuded.

Isikuandmete säilitamisest ettevõtte õiguste kaitseks

Inspektsiooni menetlusse jõudis mitme juhtumi kaudu küsimus, kui pikk saab olla klientide isikuandmete säilitamise tähtaeg äriühingu õiguste kaitseks. Näiteks oli üks äriühing sätestanud isikuandmete säilitamise tähtajaks 10 aastat ning viidanud seejuures tsiviilseadustiku üldosa seaduse (TsÜS) § 146 lõikele 4, mille kohaselt on nõuete aegumistähtaeg kümme aastat, kui kohustatud isik rikkus oma kohustusi tahtlikult.

Äriühing viitas sellele, et tal on vajalik säilitada kliendilepingutega seotud tõendeid 10 aastat pärast lepinguliste suhete lõppemist, sest klientidel on TsÜS § 146 lõikest 4 tulenevalt võimalus kohtusse pöörduda põhjusel, et äriühing on tahtlikult kliendi õigusi rikkunud või oma lepingujärgsed kohustused täitmata jätnud. Inspektsioon seadis sellise isikuandmete üldise säilitamise tähtaja kahtluse alla ning menetluse raames vähendas äriühing isikuandmete üldist säilitamistähtaega kolmele aastale.

> Inspektsioon seadis sellise isikuandmete üldise säilitamise tähtaja kahtluse alla ning menetluse raames vähendas äriühing isikuandmete üldist säilitamistähtaega kolmele aastale.

Esmalt tuleb rõhutada, et igasuguseks isikuandmete töötlemiseks (sh andmete säilitamiseks oma õiguste kaitseks), peab olema õiguslik alus. Õiguslik alus saab seejuures tuleneda isikuandmete kaitse üldmääruse (IKÜM) artiklist 6. Kui vaadata TsÜS § 146, siis nimetatud paragrahv räägib nõude aegumistähtajast ning ei anna otsest kohustust andmete säilitamiseks. Seega, konkreetse juhtumi puhul, sai õiguslikuks aluseks olla IKÜM artikkel 6 lg 1 punkt f (õigustatud huvi), millele andis kaalu TsÜS § 146.

Selleks, et andmetöötleja saaks õigustatud huvi alusel andmeid töödelda, on ta kohustatud muuhulgas läbi viima huvide kaalumise, hindamaks kas ja millises ulatuses on andmete säilitamine lubatud. Õigustatud huvi alusel andmete töötlemisel tuleb hinnata selle vajadust igal konkreetsel juhul eraldi, seda nii andmetöötlejal kui ka vajadusel inspektsioonil. Kas ja mis ulatuses on see lubatud, võib sõltuda nii andmetöötleja põhjendustest, tegevusvaldkonnast, töödeldavate andmete hulgast kui ka muudest olulistest teguritest.

Kui lähtuda TsÜS § 146 lõikest 1, siis tegemist on konkreetse sättega, mille kohaselt tehingust tuleneva nõude aegumistähtaeg on kolm aastat. Nimetatud säte puudutab kõiki inimesi, kes on andmetöötlejaga tehingu teinud, sh kõiki kliente, kes kasutavad mingit konkreetset teenust või on soetanud kauba. Siinjuures ei kahtle inspektsioon isikuandmete säilitamise vajalikkuses äriühingu õiguste kaitseks, kuid andmete säilitamise aeg tuleb inimesele lähtuvalt IKÜM artiklitest 12-14 siiski selgelt ja arusaadavalt teatavaks teha.

Pikemaks kui kolmeks aastaks säilitamine nõuab kaalukat põhjust

Olukorras, kus aga kõikide klientide andmeid soovitakse äriühingu õiguste kaitseks säilitada üldkorras üle kolme aasta, tuleb teha andmetöötlejal väga kaalukas ja põhjalik hindamine selle osas, kas pikem andmete säilitamine sellisel eesmärgil on reaalselt vajalik ja proportsionaalne eesmärgi täitmiseks.

Kui lähtuda andmete säilitamisel TsÜS § 146 lõikest 4 ning 10 aastasest andmete säilitamisest, siis nimetatud aluse üheks oluliseks tingimuseks on see, et kohustatud isik on rikkunud oma kohustusi tahtlikult. Ehk nii äriühingul kui ka kliendil on võimalik viidata ja kasutada nimetatud alust kohtus üksnes

juhul, kui üks osapooltest on tahtlikult rikkunud oma kohustusi. Lisaks nagu ka eelnevalt märgitud, peab andmete säilitamise aeg olema reaalselt vajalik.

Olukorras, kus kõikide klientide andmeid soovitakse äriühingu õiguste kaitseks säilitada üldkorras üle kolme aasta, tuleb teha andmetöötlejal väga kaalukas ja põhjalik hindamine selle osas, kas pikem andmete säilitamine sellisel eesmärgil on reaalselt vajalik ja proportsionaalne meede eesmärgi täitmiseks.

Selleks, et vajalikkust saaks hinnata, peab andmetöötleja õigustatud huvi olema seaduslik ning piisavalt selgelt sõnastatud. Seega on oluline, et andmetöötlejal oleks eelnevalt tehtud põhjalik hindamine, mis põhineb tegelikel ja konkreetsetel asjaoludel ning mille alusel on võimalik inspektsioonil hinnata ja veenduda selles, milline andmete säilitamisaeg on antud juhul reaalselt vajalik.

See, et klientidel on teoreetiliselt võimalik 10 aasta jooksul nõudeid esitada, kui äriühing on tahtlikult oma kohustusi rikkunud, võib olla üheks argumendiks andmete säilitamise osas, kuid inspektsiooni hinnangul ei ole ainuüksi nimetatud põhjendus piisav. Siinjuures on oluline, et võimalikud (kohtu) vaidlused seoses äriühingu poolse tahtliku rikkumisega oleksid ka piisavalt tõenäolised.

Samuti tuleb rõhutada, et olukorras, kus konkreetse kliendiga on tekkinud lepingu ajal või kolme aasta jooksul peale lepingu lõppemist mingisugune probleem (konfliktiolukord), kus äriühing põhjendatult leiab, et tegemist on või võib olla kas äriühingu või kliendi tahtliku rikkumisega, on võimalik tugineda õigustatud huvi alusel andmetöötlusele ning sellega seoses viidata ka TsÜS § 146 lõikele 4.

Minimaalsuse põhimõte

Siinjuures oleks võimalik põhjendada võimalikku (kohtu)vaidluse tekkimist, kuid sellisel juhul puudutaks pikem andmete säilitamine üksnes konkreetset klienti. Kui aga lepingu ajal või kolme aasta jooksul peale lepingu lõppemist ei ole kliendi ja äriühingu vahel toimunud mitte ühtegi kaheldavat situatsiooni ning klient ei ole äriühinguga ka kordagi ühendust võtnud (nt mingisugust nõuet esitanud), on inspektsiooni hinnangul väga vähe tõenäoline, et äriühingul võiks olla vajalik konkreetse inimese andmeid oma õiguste kaitseks üle kolme aasta säilitada.

Igas olukorras, kus kõikide klientide andmeid soovitakse äriühingu õiguste kaitseks säilitada üldkorras üle kolme aasta, tuleb teha andmetöötlejal väga kaalukas ja põhjalik hindamine selle osas, kas pikem andmete säilitamine sellisel eesmärgil on reaalselt vajalik ja proportsionaalne meede eesmärgi täitmiseks.

Iga andmetöötleja peab ennekõike ise hindama ja põhjendama, millises ulatuses (sh ajalises ulatuses) on andmetöötlejal andmete säilitamine reaalselt vajalik.

Võlaandmete avaldamise aeg pikenes

Alates 2019. aasta 15. jaanuarist jõustunud isikuandmete kaitse seaduses (IKS) pikenes võlateabe avalikustamiseks lubatud aeg.

Kuna kohustuse rikkumine ei ole isikut püsivalt negatiivselt iseloomustav fakt, siis ei tohi vaadeldavaid isikuandmeid töödelda igavesti. Selle vältimiseks on kehtivas IKS §-s 10 sätestatud, et võlaandmeid ei või koguda ega kolmandatele isikutele edastada, kui kohustuse rikkumise lõppemisest (tasumisest) on möödunud rohkem kui viis aastat.

Võrreldes eelmise IKS-ga on tasutud võla avalikustamise aeg pikenenud kolmelt aastalt viiele. Sellega pikenes ka tasumata võla avalikustamise aeg kahe aasta võrra ning varasema 13 aasta asemel saab võlaandmeid töödelda 15 aastat. Siiski peavad andmete avalikustajad olema avaldamisel arvestanud sellega, et võlaandmete avaldamine ei kahjusta ülemääraselt andmesubjekti õigusi ja vabadusi.

> Varasema 13 aasta asemel saab võlaandmeid töödelda 15 aastat.

Näitena võib tuua olukorra, kus inimene on aastaid tagasi jäänud omalegi teadmata põhjustel võlgu näiteks viis eurot ning nüüd survestab inkassoettevõtja seda koos sissenõudmiskuludega tasuma, isegi kui võlg on kordades väiksem. Nõue on ammu aegunud ja jääks tõenäoliselt kohtus rahuldamata.

Avalikustamine ei tohi inimest ülemääraselt kahjustada

Sellise võla kanne maksehäireregistris aga võib takistada laenu saamist ja olla inimest muudeski olukordades ülemääraselt kahjustav. Võlausaldajal on olnud õigus ja võimalus võla sissenõudmiseks pöörduda kohtusse enne aegumistähtaja möödumist. On küsitav, kas väikeste aegunud võlgade pikaajaline avalikustamine täidab ikka krediidivõimelisuse hindamise eesmärki ning kas avaldaja on arvestanud ka inimese huvide ja õigustega.

Võitlus spämmijatega ei lõppenud

Üheks digiühiskonna probleemiks on saanud elektroonilistele kanalite kaudu otseturustuskirjade saatmine ehk spämmimine.

Kaebusi ja märgukirju spämmi saamise kohta on inspektsioon saanud sadade kaupa juba viimased 8 aastat. Spämmi saadetakse nii füüsilistele kui juriidilistele isikutele kuuluvatele telefoninumbritele sms sõnumitena ja e-posti aadressidele. Üks selline sihikindel rikkuja häirib inimesi pelletite müügiga. Inspektsioonile teadaolevalt omab pelletite müüja alates 2013. aastast otseturustuse tegemiseks vähemalt 5 juriidilist keha ja 9 e-posti aadressi. Isik saadab kirju ja sõnumeid ilma vastuvõtja eelneva nõusoleku või kliendisuhteta. Saadetavas e-kirjas olev kommertsteadaannetest loobumise link ei tööta ja kirjades varjatakse kommertsteadaande saatjat, s.t et ei ole selge, kelle nimel reklaami tehakse.

Isik on rikkunud pidevalt nii elektroonilise side kui isikuandmete kaitse seadust, samuti infoühiskonna teenuse seadust. Isik on keeldunud korduvalt täitmast Inspektsiooni ettekirjutusi ja jätnud maksmata sunniraha.

Mida aeg edasi, seda enam on inspektsiooni muutnud murelikuks asjaolu, et sellises õiguslikus olukorras on keeruline ebaseaduslikku tegevust peatada ning seista inimeste õiguse eest mitte saada soovimatuid reklaamteadaandeid.

Rikkumise lõpetamiseks on inspektsioonil võimalik riikliku järelevalve raames teha otseturustajale esmalt ettekirjutus rikkumise lõpetamiseks ning seejärel selle mittetäitmisel asuda sunniraha rakendama, aga kuna tänases Eestis on äärmiselt lihtne seadustega pahuksisse sattunud juriidiline keha hülgata ja uus teha, siis sunniraha määramine ei taga tulemust. Vana juriidiline keha jäetakse tankistiks määratud juhatuse liikme käe all sundlõpetamist ootama ning sellisele surnud ettevõttele trahvi või sunniraha määramine tähendab probleemi lahendamise asemel hoopis riigile lisakulu, sest sunniraha sissenõudmiseks peab esmajoones ära maksma kohtutäituri tasu, sõltumata sellest, kas nõuet täita õnnestub või mitte.

Probleemi aitab lahendada haldustrahv

Kui siseriiklik õigus võimaldaks teha haldustrahvi, muutuks menetlus ökonoomsemaks ja inspektsioon saab määrata korduvrikkujale trahvi väikse ajakuluga. Eesti õigus aga kahjuks haldustrahvi ette ei näe. Sestap nõuab kogu protsess igal rikkumise korral koormavat tõendamis- ja uurimismenetlust ja õiguskorda rikkuv juriidiline isik saab viia juriidilise keha pankroti enne, kui on võimalik teda sisuliselt vastutusele võtta.

Üks meede, mida inspektsioon saab korrakaitse seaduse (KorS) § 26 lg 1 ja 2 alusel kaudselt inimeste privaatsuse tagamiseks teha, on avalikkust hoiatada, kuid kindlasti ei saa seda lugeda probleemi lahendamiseks. Spämmimine probleemina aga kasvab iga aastaga aina mastaapsemaks.

Euroopa Andmekaitsenõukogu ja *one stop shop*'i käivitamine Eesti vaatest

Kui aastat 2018 võis andmekaitse järelevalveasutuste jaoks nimetada tänu isikuandmete kaitse üldmääruse (IKÜM) kehtimahakkamisele murranguliseks, siis 2019. aasta näitas, et nii mitmedki uued nõuded (nt rikkumisteated) on muutumas tavapäraseks. Kuid endiselt vajavad paika loksumist teatud protsessid, sest selleks ongi vaja pikemat ajaperioodi. Andmekaitseasutuste ühiseks proovikiviks osutusid möödunud aastal ülepiirilised menetlused ja omavaheline koostöö.

Koostöö on üha enam oluline, sest tehnoloogiaajastul hägustunud riikide piirid on loonud olukorra, kus teenusepakkujad ei piiritle ennast vaid ühe riigiga, vaid vaatavad ka oma koduriigist väljapoole, osutades teenuseid nii Euroopa Liidu sees kui ka väljaspool liitu asuvates riikides.

Teenuse osutamine nõuab isikuandmete töötlemist. Seepärast on IKÜM-s ettenähtud omad tingimused ja kord, kui peaks toimuma ülepiiriline andmetöötluse intsident, sh kui inimene tunneb, et tema õigusi rikub andmetöötleja, kes üldse ei asugi inimese koduriigis.

Euroopa ühine *one-stop-shop* (ühe akna süsteem)

Euroopa ühine *one-stop-shop* tähendab seda, et inimene saab oma koduriigi andmekaitseasutuse poole pöördudes kaitset ka ülepiirilise

juhtumi korral. Koduriigi andmekaitseasutus lahendab ära juhtumi koostöös teiste andmekaitseasutustega. Siinkohal tuleb juhtida tähelepanu, et selliseid koostöökohustusi ning *one-stop-shop*'i reeglite nõudeid saab peale panna vaid Euroopa Liidu liikmesriikide ning Euroopa Majanduspiirkonna andmekaitse järelevalveasutustele.

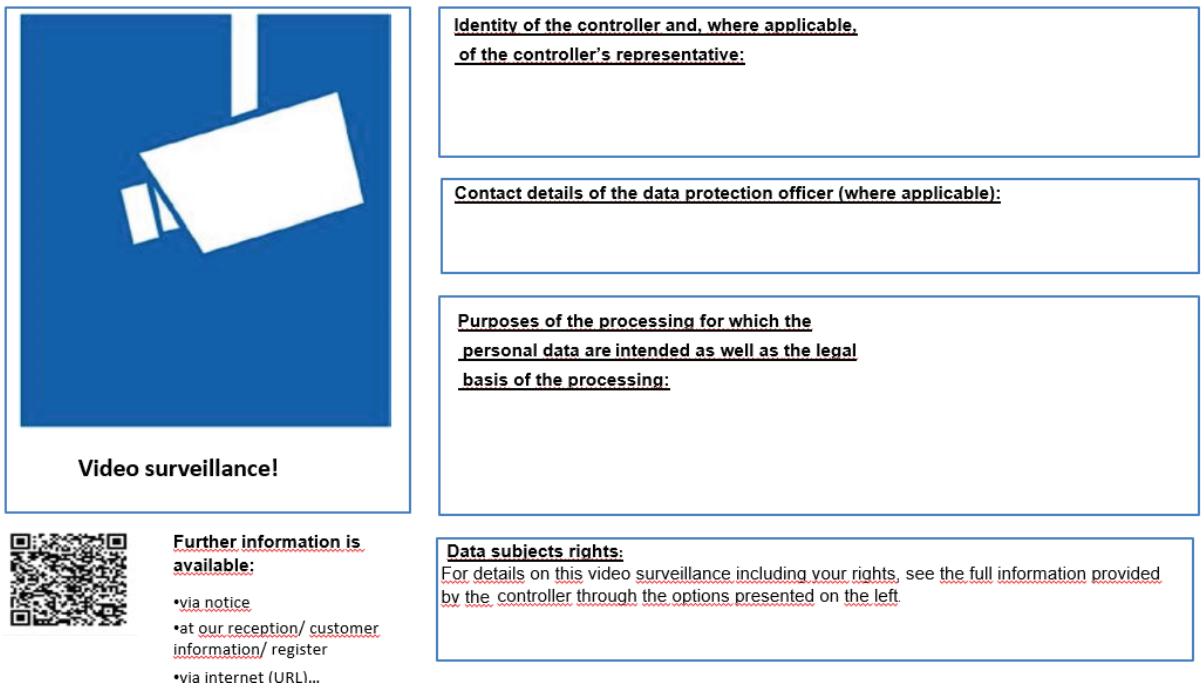
IMI kaudu liigub tuhandeid algatatud menetlusi, aga enne kui sisuliselt kaasusega tegelema saab hakata, tuleb kindlaks määrata, kes on juhtiv andmekaitseasutus ning kes on kaasatud asutused.

One-stop-shop protsessireeglite alusel käiva menetluskoostöö läbiviimiseks on Euroopa Andmekaitsenõukogu kasutusele võtnud Euroopa Liidu siseturu infosüsteemi (IMI), millega harjumine ning sealt tuleneva töömahuga hakkama saamine oligi möödunud aastal väljakutseks ilmselt kõikide andmekaitsenõukogu liikmete jaoks.

IMI kaudu liigub tuhandeid algatatud menetlusi, aga enne kui sisuliselt kaasusega tegelema saab hakata, tuleb kindlaks määrata, kes on juhtiv andmekaitseasutus ning kes on kaasatud asutused. See aga ainuüksi tähendab, et iga algatus, mis IMI-sse laetakse, tuleb läbi vaadata, et olla veendunud, kas näiteks Eesti andmekaitseasutusel on puutumus asjasse või mitte. Kui asutused on paika saadud, hakkab sisuline menetlus, sh riikide vaheline koostöö asjaolude tuvastamisel. Enne otsuse vastuvõtmist peavad olema kõik kaastaud asutused otsusega ühel meelel, vastasel korral on andmekaitsenõukogu see, kes vaidlusi lahendab.

Ühiselt kujundatud seisukohad ja järjepidevuse mehhanism

Kuna Euroopa Andmekaitsenõukogu tegeleb ühelt poolt järjepideva praktika loomisega ning andmekaitseasutuste omavaheliste vaidluste lahendamisega ning teisest poolt andmekaitseliste seisukohtade loomise ja



Euroopa Andmekaitsenõukogu pakkus välja videovalve sildi visuaali[4]

[4] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en

tõlgendamisega, siis möödunud aastasse jääb mitmeid olulisi seisukohti ja arvamusi, mille seast peaks esile tooma kauaoodatud videovalve juhise.

Videovalve juhise lõplik vastuvõtmine peale avalikku konsultatsiooni toimus küll 2020. aasta alguses, kuid arvestades juhise pikka valmimisaega ning avalikustamist 2019 suvel, võiks seda siiski lugeda olulisimaks andmekaitsenõukogu juhiseks sel perioodil.

Kaamerate kasutamine nii eraotstarbel kui avalikes kohtades, töösuhetes ja kaubanduses, on olnud väga pikka aega üks olulisemaid vaidluskohti andmekaitse valdkonnas. Lisaks tekkis IKÜM-i kehtima hakkamisega mõningane arusaamatus videovalve piirkonna tähistamisega. Kui varasemalt oli siseriikliku seadusega videovalve tähistamine kirjeldatud, siis IKÜM-s ja uues isikuandmete kaitse seaduses seda enam ei ole kirjeldatud. Seega ei ole kahtlustki, et antud juhend sai palju tähelepanu ning selle koostamine tekitas pikki vaidluseid.

Kuid see ei olnud ainuke oluline juhis, mille Euroopa Andmekaitsenõukogu koostas. Lisaks said nö joone alla toimimisjuhendite juhis, lõimitud ja vaikimisi andmekaitse juhend, andmetöötluse õiguslikust alusest interneti teenuste puhul jne.

Kui vaatleme Euroopa Andmekaitsenõukogu ülesandeid seoses järjepidevusmehhanismi tagamisega ning ülepiiriliste menetluste läbiviimisel, siis oli 2019. aasta väga tegus.

IKÜM näeb ette päris paljude nõuete juures, et andmekaitseasutus on kohustatud kohaldama järjepidevuse mehhanismi. Lihtsustatult öeldes tähendab see, et enne teatud nõuete või kohustuslike nimekirjade koostamist peab andmekaitseasutus pöörduma Euroopa Andmekaitsenõukogu poole ning saama enda koostatud nõuetele heakskiidu. Näiteks, kui andmekaitseasutus otsustab koostada nimekirja ülepiirilise andmetöötluse liikidest, mille puhul on kohustuslik läbi viia mõjuhinnang, siis tuleb sellele nimekirjale heakskiit küsida. Heakskiidu küsimine tähendab, et nõuded ja nimekiri vaadatakse läbi kõigi andmekaitsenõukogu liikmete poolt, koostatakse arvamus ettepanekutega nõuete/nimekirja täiendamiseks (kui on vajadus) ning pärast nõutud muudatuste tegemist võib andmekaitseasutus dokumendi avalikustada ning andmetöötlejad saavad sellest juhinduda.

> Kokku avaldas Euroopa Andmekaitsenõukogu 2019. aastal seonduvalt järjepidevuse mehhanismiga 17 arvamust, enamik neist puudutas mõjuhinnangute nimekirjasid ja kontsernisiseste reeglite heakskiitmist.

Valdkondi, mille puhul on kohustus järgida järjepidevuse mehhanismi, on päris palju. Lisaks eespool mainitud mõjuhinnangute kohustusele, tuleb seda veel rakendada vastutava ja volitatud töötleja vaheliste lepingu tüüptingimuste koostamisel, toimimisjuhendite koostamisel, sertifitseerimisreeglite koostamisel, teatud juhtudel andmete välisriiki edastamiste lepingute heakskiitmisel ning siduvate kontsernisiseste reeglite heakskiitmisel jne.

Kokku avaldas Euroopa Andmekaitsenõukogu 2019. aastal seonduvalt järjepidevuse mehhanismiga 17 arvamust, enamus neist puudutas mõjuhinnangute nimekirju ja kontsernisiseste reeglite heakskiitmist.

Koostöö Euroopa Andmekaitsenõukoguga on olnud ja saab jätkuvalt olema oluline. Inspektsioon osaleb igakuistel Euroopa Andmekaitsenõukogu plenaaristungitel.

Samuti on inspektsioon enda jaoks valinud prioriteetsed alagrupid, mille tegevuses osalevad inspektsiooni töötajad kohapeal käies. Prioriteetsed alagrupid on tehnoloogia, vastavus ja e-valitsemine, koostöö, menetlus ja trahvimine, võtmesätete, sotsiaalmeedia ning piiride, reisijate ja korrakaitse alagrupid. Inspektsioon hoiab end kursis ka teiste valdkondade töögruppide aruteludega ning vajadusel räägib kaasa.

Osalemine rahvusvahelistes töögruppides

Kui Euroopa Andmekaitsenõukogus teevad koostööd kõik Euroopa Liidu liikmesriikide ja Euroopa Majanduspiirkonna andmekaitse järelevalveasutused, siis lisaks sellele on tegutsemas veel rahvusvahelisi töögruppe. Inspektsioon jätkas 2019. aastal osalemist erinevates töörühmades vastavalt oma ressurssidele. Aktiivsemalt jõudis inspektsioon panustada Üleilmse Eraelu Kaitse (GPEN) töögrupi töösse ja telekommunikatsioonialases andmekaitse töörühma tegevusse (IWGDPT).

Millistes Euroopa ja ülemaailmse haardega töörühmades Andmekaitse Inspektsioon osaleb, sellega saab tutvuda aki.ee veebis

https://www.aki.ee/et/inspektsioon-kontaktid/piiriulene-koostoo

GPEN

2019. aasta septembris toimus Üleilmse Eraelu Kaitse Võrgustiku ehk tuntud lühendina GPEN seire teemal rikkumisteated. Tegemist oli seitsmenda privaatsusõigusega seotud seirega, mis on siis läbi viidud GPEN-i eestvedamisel.

Seires uuriti, kuivõrd hästi organisatsioonid talletavad teavet andmeleketest ning kuidas ja millal nad teavitatakse rikkumistest andmekaitse järelevalveasutustele.

Kokku esitati küsimusi 1145 organisatsioonile ning vastus saadi 258-lt (21%). Vastajatest 84% teavitasid, et neil on olemas mingi töörühm või üksus, mis tegeleb rikkumisteadetega. 75% vastanutest leidsid, et neil on olemas kohased protseduurid rikkumisteadetega tegelemiseks. Inspektsioon 2019. aastal selle seire läbiviimises ei osalenud.

IWGDPT

Telekommunikatsioonialane andmekaitse töörühm tegutses aktiivselt isikuandmete töötlemise põhimõtete analüüsi ja selgitustööga telekommunikatsiooni ning tehnoloogia valdkonnas ning andis välja teemakohaseid suuniseid.

2019. aastal avaldati kaks suunist

(1) *Protecting the Privacy of Children in Online Services*. Lapsed on võrguteenuste kasutamisel haavatavad. Nende vähene võimekus ja suutlikkus ohte adekvaatselt tajuda võib tuua kaasa veebikäitumisel soovimatuid tagajärgi. Mõnel juhul võib lastega seotud andmete kogumine ja kasutamine kujutada endast eraelu puutumatuse ja andmekaitse rikkumisi. Teisalt võivad tagajärjed viia näiteks küberkiusamiseni. Suunise eesmärk on tuua välja peamised privaatsusriskid ja probleemid, mis on seotud laste võrguteenuste kasutamisega, ning anda soovitusi poliitikakujundajatele, võrguteenuste arendajatele ja pakkujatele ning regulaatoritele.

(2) *Privacy Risks with Smart Devices for Children*. Dokument keskendub lastele mõeldud või nendega seotud seadmetele nagu nutikad mänguasjad, nutikellad või näiteks beebimonitorid. Need seadmed on internetti ühendatult võimelised reaalajas määrama näiteks seadme kasutaja asukohta, teda jälgida või temaga suhtlema. Seadmed võivad salvestada nimesid, fotosid ja geograafilisi asukoha andmeid. Samuti võib toimuda kasutaja terviseandmete töötlemine. Dokument analüüsibki selliste seadmete kasutusega seonduvaid eraelu riivavaid riske ning annab soovitusi, kuidas riske ära tunda ning mis osas eriti tähelepanelik olla.

PRAKTIKUTE TÖÖLAUALT

Andmekaitse Inspektsiooni eesmärk on aidata kujundada ühiskonda, kus väärtustatakse üksikisiku õigust eraelule ja riigi tegevuse läbipaistvust. Selleks teostavad inspektorid järelevalvet järgmiste õigusaktide täitmise üle:

- ❒ isikuandmete kaitse üldmäärus,
- ❒ isikuandmete kaitse seadus,
- ❒ avaliku teabe seadus,
- ❒ elektroonilise side seadus.

Inspektsioon arvestab oma töös samuti rahvusvaheliste õigusaktidega, mis reguleerivad piiriülest isikuandmete töötlemist. 2019. aasta mööndus õiguspraktikutele nii selgitustööd tehes, jälgides andmekaitse reeglite täitmist kui lahendades vanu probleeme uute regulatsioonide kehtimisel.

Andmekaitse on saanud oluliseks teemaks nii suurele kui väikesele andmetöötlejale, sest üha enam mõistetakse, et ollakse osa hiiglaslikust ja kasvavast andmebaasist, mille sünonüümiks on internet.

Keegi ilmselt ei kujuta enam ette endist maailma, kus kindlustus, meditsiin, turism, pangandus, turundus ja avalik sektori ei oleks oma teenustega kättesaadav internetist.

Kas aga andmetöötlejad on valmis kaitsma inimeste privaatsust? Või kas inimene ise teab, millist kaitset peab andmetöötleja talle tagama? Need olid vaid mõned peamistest küsimustest, millega inspektsiooni õiguspraktikud oma menetlustes ja selgitustöös 2019. aastal tegelesid.

Järgnevates artiklites toob inspektsioon välja suuremaid või uuemaid probleeme, mis on esile kerkinud peale 2018. aasta 25. maid, mil jõustus isikuandmete kaitse üldmäärus.

Läbipaistmatu andmetöötlus

2019. aastal oli inspektsioonil mitu järelevalvemenetlust, mille käigus jäi silma ühe üldise probleemina see, et andmetöötlejate võrgulehtedel ei anta inimesele infot tema isikuandmete töötlemise kohta, ehk puudusid andmekaitsetingimused. Kõigil, kes oma tegevuse raames isikuandmeid koguvad, peavad inimestele ka andmekaitsetingimused kättesaadavaks tegema. Kui see nii oligi, ei vastanud veebilehel esitatud andmekaitsetingimused aga tihtipeale nõuetele. Kui vaadata isikuandmete kaitse üldmääruse (IKÜM) artikleid 13 või 14, siis nimetatud artiklites on välja toodud, mida peab inimesele antav teave minimaalselt sisaldama.

Lisaks on oluline rõhutada, et andmekaitsetingimused peavad olema inimestele arusaadavas, selges ja lihtsas keeles. Kõigil, kes

pakuvad oma teenuseid või kaupu erinevates riikides, tuleb arvestada sellega, et andmekaitsetingimused oleksid kättesaadavad iga konkreetse riigi keeles.

Inspektsioon kohustas andmetöötlejaid viia oma tegevus kooskõlla andmetöötluse läbipaistvuse põhimõttega. Lisaks tuleb viia andmekaitsetingimused vastavusse IKÜM artiklitest 12 - 14 sätestatud nõuetele, sh vaadata koostatud andmekaitsetingimused üle enne andmete kogumist.

Inspektsioon kohustas andmetöötlejaid mitmetes järelevalvemenetlustes oluliselt panustama andmetöötluse läbipaistvusesse. Seejuures kontrollis inspektsioon seda, et andmekaitsetingimused vastaksid täielikult IKÜM-i artiklites 12–14 sätestatud nõuetele.

Iga andmetöötleja kohustuseks on vaadata üle, kas ja mis ulatuses andmekaitsetingimused IKÜM nõuetele vastavad ning vajadusel koostada andmekaitsetingimused nii, et need oleks vastavuses IKÜM-i nõuetega.

Digiloo andmejälgija tõi kaebusi tervishoiutöötajate uudishimu kohta

Vaatamata tervishoiuasutuste nõustamistele terviseandmete vaatamiste õigsuse teemal, sai inspektsiooni tänu inimeste andmejälgija aktiivsele kasutusele jätkuvalt kaebusi ja märgukirju selle kohta, kus keegi on avastanud tema digiloo vaatajate hulgast nime, kellega tal ei ole olnud enda teada ühtegi kokkupuudet. Mõningatel juhtudel on olnud ühe päeva jooksul vaatamisi ühe inimese poolt tublisti rohkem kui kümnel korral.

Inspektsiooni menetlusesse jõudis ka selliseid juhtumeid, kus oma pääsu terviseandmete juurde on kuritarvitatud oma lähikondlaste kohta info uurimisel. Näiteks oli digiloost terviseandmeid vaadanud täisealise lapse arstina töötav vanem. Samuti pidi inspektsioon algatama menetluse perearstikeskuse juhtumi peale, kus tervishoiutöötaja vaatas oma sugulase terviseandmeid.

Kui tervishoiutöötaja kasutab oma töös terviseandmeid digilugu.ee süsteemist, peab ta arvestama, et sealt saadud info on alati kõrvaliste isikute jaoks piiranguga teave. Seda ka juhtudel, kui tervise infosüsteemis olevad isikuandmed võetakse üle näiteks oma raviasutuse sisesesse infosüsteemi, sest seda on vaja arvestada raviplaani koostamisel.

Terviseandmeid tohib töödelda üksnes tervishoiuteenuse osutamiseks ja terviseandmetele juurdepääs on mõeldud vaid selleks otstarbeks, mis tähendab, et väljapoolt raviteenuse osutamist terviseandmeid vaadata ei tohi. Tervishoiuteenuse osutaja ei tohi oma ametipositsiooni ära kasutada isikliku uudishimu rahuldamiseks. Ilma aktiivse raviteenuse osutamiseta või inimese enda antud nõusolekuta ei tohi andmeid vaadata ega muudmoodi töödelda.

Uudishimu päringute eest on tehtud varasematel aastatel mitmeid väärteotrahve. Aastal 2019 tervishoiusüsteemis selliseid trahve ei määratud, kuna algatatud menetlused ei jõudnud veel aastalõpu seisuga lahenduseni.

Asutusel pole õigust küsida avaliku ülesande täitmiseks nõusolekut

Õigusliku aluse leidmise osas märkas inspektsioon 2019. aastal avaliku sektori andmetöötlejate hulgas teatavat ebakindlust.

Praktikutel tuli selgitada, miks on väär on küsida nõusolekut olukorras, kus tegelikult on isikuandmete töötlemiseks muu õiguslik alus. Selline tegevus on eksitav, sest jätab mulje, et inimesel on otsustusõigus olukorras, kus seda tegelikult ei ole. Näiteks oli üks selline olukord riikliku järelevalvemenetluse läbiviimisel, mis ei saa sõltuda isiku nõusolekust. Nõusoleku küsimine on asjakohane üksnes sellistes olukordades, kus isikul on ka reaalselt võimalik otsustada oma isikuandmete töötlemise osas.

Sestap tuleb arvestada, et isiku nõusolek on õigusliku alusena kehtiv siis, kui see on vabatahtlik. Nõusoleku küsimist saab pidada asjakohaseks üksnes sellistes olukordades, kus isikul on ka reaalselt võimalik otsustada oma isikuandmete töötlemise osas. Isik võib igal ajal oma nõusoleku vabalt tagasi võtta.

Kui isikuandmete töötlemiseks on avaliku võimu teostamine ja avaliku ülesande täitmine, saab andmetöötlus olla võimalik kas tulenevalt eriseaduse sättest või olla tuletatud ülesande täitmise vajadusest.

Kui tervishoiuteenuste korraldamise seadus ütleb, et tervishoiuteenuste osutajatele kehtestatud nõuete täitmise üle teostab riiklikku järelevalvet Terviseamet, siis nendeks nõueteks on muuhulgas ka tervishoiuteenuse osutamise nõuetekohane dokumenteerimine ja tervishoiuteenuse kvaliteedi tagamine.

Kui isikuandmete töötlemiseks on avaliku võimu teostamine ja avaliku ülesande täitmine, saab andmetöötlus olla võimalik kas tulenevalt eriseaduse sättest või olla tuletatud ülesande täitmise vajadusest.

Järelevalve raames saab Terviseamet muudelt isikutelt või asutustelt infot küsida haldusmenetluse seaduse alusel. Haldusmenetluse seaduse § 38 lõige 1 ütleb, et haldusorganil on õigus nõuda haldusmenetluse käigus menetlusosalistelt ning muudelt isikutelt nende käsutuses olevate tõendite ja andmete esitamist, mille alusel haldusorgan teeb kindlaks asja lahendamiseks olulised asjaolud.

Alaealiste andmete töötlemisest

2019. aastal sai inspektsioon mitmeid kaebusi ja märguandeid koolides toimuva andmetöötluse kohta. Ühe probleemina joonistus välja, et koolid küsivad andmeid liiga palju. Üldine reegel, mida inspektsioon soovitas järgida, on lähtuda andmete kajastamisel põhimõttest „nii vähe kui eesmärgi saavutamiseks vajalik“, aga nii, et midagi olulist ei jääks jällegi tegemata.

Koolil ei ole õigus küsida tervisetõendile lisaks täpsemat diagnoosi

Inspektsioon lahendas koostöös Haridus -ja Teadusministeeriumiga ühte kaasust, kus kool küsis õpilaselt lisaks arstitõendile ka diagnoosi, et otsustada kas kool lubab õpilasel puudutud ajal toimunud kontrolltööd järele teha. Haridus-ja Teadisministeerium

oli vastuses koolile selgitanud, et põhikooli- ja gümnaasiumiseaduse (PGS) § 36 lõike 2 alusel lisaandmete küsimine ei ole põhjendatud, kuna ei selgu, et koolil on tõendid ebaõigete andmete esitamise kohta.

Inspektsioon leidis samuti, et arstitõendi juurde lisaandmete küsimine on ülemäärane. Inspektsiooni hinnangul on arstitõend oma loomult nii õpilase kui ka töötaja puhul ilmselge tõend mõjuva põhjusega puudumisest, mis ei vaja eraldi hindamist, ega anna alust lisaandmete küsimiseks. Juhul kui on kahtlustusi tõendi õiguses vms, siis selle väljaandmisega seotud asjaolude kontrollimiseks saab esitada taotluse Eesti Haigekassale.

> Inspektsiooni hinnangul on arstitõend oma loomult nii õpilase kui ka töötaja puhul ilmselge tõend mõjuva põhjusega puudumisest, mis ei vaja eraldi hindamist, ega anna alust lisaandmete küsimiseks.

Terviseandmete kui eriliigiliste andmete saamiseks ei saa kasutada õigusliku alusena ka nõusolekut, sest nõusolek peab olema antud vabal tahtel. Diagnoosi kui eriliigiliste isikuandmete küsimisega võetakse ära võimalus avaldada neid ise vabal tahtel ehk nõusoleku alusel. Seda seetõttu, et kui kooli esindaja küsib andmeid lapsevanemalt, lapselt või töötajalt, siis on tegemist nõrgemal positsioonil oleva isikuga, kes ei saa oma vaba tahte üle ise otsustada. Inspektsioon leidis, et kool rikkus sellega andmekaitsenõudeid.

PGS § 35 lõige 2 ja § 36 lõige 2 alusel saaks kool hinnata ja täpsustada muid puudumisi (nt kui õpilane puudub seoses koolivälistе võistluste, pereürituste, reiside jms põhjustega), mis ei ole faktiliselt käsitletavad mõjuva puudumisena. Sel juhul lasub inspektsiooni hinnangul asjaolude tõendamise kohustus tõepoolest lapsevanemal ning kool võib küsida täpsustusi, nt konkursil osalemise kinnitust jms.

Õpilase diagnoosi ei ole õigust küsida ka kehalise kasvatuse õpetajatel. Piisab, kui arsti otsuses on välja toodud vastunäidustused. Seda eelkõige põhjusel, et ükski muu isik, kes ei ole meditsiinitöötaja ei saa asuda diagnoosi alusel vastu võtta otsuseid, mis on õpilasele lubatud ja mis mitte. Küll aga kutsub inspektsioon vanemaid üles koostööks õpetajatega, lähtudes perearsti soovitustest, sest see on lapse huvides, kui ta mingilgi määral olenemata oma tervislikust seisunist spordiga siiski tegeleks. Koos vanemaga oleks hea leida vastavale õpilasele alternatiivsed harjutused jms, mitte automaatselt vabastada igasugustest tundidest.

Vanema nõusolek lapse andmete töötlemiseks kehtib ainult selle küsijale

Inspektsioon sai märgukirja, et ühe laste päevahoiu juhataja kasutab lastest pilte ja videosid reklaamiks enda isiklikul Facebooki kontol. Inspektsioon tuvastas, et nõusolek laste andmete töötlemiseks oli küll võetud, aga see oli võetud lastehoiu kui juriidilise isiku nimel.

Kui nõusolek laste andmete töötlemiseks on võetud juriidilise isiku nimel, siis peab arvestama, et eraisikuna neid samu andmeid avaldada ei saa. Selleks on vaja võtta eraldi lapsevanemate nõusolek ja andmete avaldamisel tekib sel juhul kahe eraisiku vaheline õigussuhe. Antud juhul soovitas inspektsioon avaldajal veenduda, et vanemad on oma laste fotode ja videote avaldamisega nõus ja sellest teadlikud. Lisaks tuleb kasutada laste andmete avalikustamisel suhtluskeskkonnas privaatsussätteid, et andmed ei oleks kõigile nähtavad, vaid teha valik, kellele isik soovib need nähtavaks teha.

Samuti tuleb juhtida tähelepanu sellele, et kui lastehoid soovib laste andmeid avaldada ettevõtte võrgulehel, siis on võimalus kasutada sätteid, millega ei ole konkreetsed võrgulehed otsingumootoritele leitavad.

Meedial tuleb alaealiste andmete töötlemisel olla nende huvidega arvestav

2019. aastal sai inspektsioon mitmeid sekkumistaotlusi, millele oli vaja reageerida. Üks juhtumitest puudutas kadunud alaealise otsimist, kes oli üles leitud. Alaealine isik oli igati tuvastatav (pilt, eesnimi, vanus, elukoha piirkond jne) ning avatud oli samuti kommentaaride kirjutamise võimalus. Inspektsioon leidis, et ajakirjandus kannab olulist ja tänuväärset rolli kadunud isikute võimalikul leidmisel ja tagaotsimise artikli avaldamise hetkel olid avaldamise nõuded meediaväljaandel täidetud, küll aga sai eesmärk kohe pärast lapse leidmist täidetud. Kui eesmärk on täidetud, muutub avaldatu lapse õigusi ülemääraselt kahjustavaks. Artikkel võib mõjutada oluliselt lapse edaspidist elu, sh tuua kaasa põhjendamatuid kannatusi nii tema lähedastele kui talle endale. Juhtunu on tõenäoliselt olnud lapsele niigi traumeeriv ja ning selle igavene avaldamine ei ole põhjendatud.

Seetõttu saatis inspektsioon meediaväljaannete peatoimetajatele ringkirja, kus tegi ettepaneku lõpetada kadunud alaealiste isikuandmete avaldamine kohe pärast seda, kui avaldamise eesmärk on täidetud ehk isik on leitud.

Alaealiste andmete avaldamisel peab iga andmetöötleja olema veelgi kaalutlevam ja ettevaatlikum, kuna isikutel ei ole õigust enda andmete avaldamisel kaasa rääkida ning nende eest otsustavad seaduslikud esindajad. Seetõttu saatis inspektsioon meediaväljaannete peatoimetajatele ringkirja, kus tegi ettepaneku lõpetada kadunud alaealiste isikuandmete avaldamine kohe pärast seda, kui avaldamise eesmärk on täidetud ehk isik on leitud (kas artiklid kustutades või avaldades artikleid edasi isikustamata kujul). Soovitav on üle vaadata alaealiste õiguste kaitseks ka vanad artiklid ning vajadusel teha muudatusi.

Juhtumite lahendamistest haridusvaldkonnast

Koolidirektor ei saa koristaja töö kontrollimiseks kasutada turvakaamerat

Põhikooli- ja gümnaasiumiseaduse (PGS) § 44 lg 5 kohaselt on koolis videovalve kasutamine lubatud üksnes õpilaste ja koolitöötajate turvalisust ohustava olukorra ennetamiseks ning olukorrale reageerimiseks. Lisaks õpilaste ja kooli töötajate turvalisuse tagamisele võib turvakaameraid koolis ja muus lasteasutuses kasutada ilma inimeste nõusolekuta isikuandmete kaitse seaduse (IKS) § 14 lg 3 kohaselt siiski ka kooli või lasteasutuse vara kaitseks.

Turvakaameraid ja nende salvestusi ei või kasutada mitte ühelgi teisel eesmärgil, sh töötajate töökohustuste kontrollimise eesmärgil, kuna selleks peab tööandja alati kasutama töötajat vähemkahjustavamaid viise. Turvakaamerate ainus eesmärk võib olla isikute ja vara kaitse ning turvajuhtumi ilmnemisel võib salvestuse edastada vaid korrakaitseorganile, sh ei või turvakaamerate salvestusi näha isikud, kelle töökohustuste hulka see ei kuulu. Inspektsioon selgitab, et nende nõuete rikkumisel (kõrvaliste isikute ligipääs turvaruumi/turvakaamerate juurde) võib vastutada väärteokorras kooli direktor, kelle ametiülesannete hulka kuulub turvakaamerate korra loomine ja korra täitmise tagamine.

Kõrgkool kohustub tagama privaatsust ka ühiselamus

Inspektsioon sai kaebuse ülikooli endiselt üliõpilaselt, mille kohaselt on õpilaskodu juhataja käinud korduvalt ilma isikute teadmata nii kaebaja kui teiste isikute tubades ja tutvunud isiklike asjadega (sh isikuandmeid sisaldavate dokumentidega ja selle kohta kaebajale suulisi märkusi teinud), küll aga ei ole midagi varastanud.

Üliõpilaste ja teiste üliõpilaskodu kasutavate isikute privaatsuse kaitse on ülikooli tagada. Keegi ei tohi käia ühiselamu tubades ja tutvuda toaelanike isiklike asjadega ilma toaelanike endi teadmata. Leping üliõpilaskodu kasutamiseks sõlmitakse ülikooli ja üliõpilase või muu isiku vahel, mistõttu vastutab ülikool selle eest, et ei toimuks ka õigusliku aluseta isikuandmete töötlemist ja toa kasutamisel ei rikutaks isikute privaatsust.

Inspektsioon andis sellisest kaebusest teada ülikooli juhtorganile ning seda koos soovitusega üle vaadata nii õpilaskodu kasutamiseks sõlmitav leping, sisekorraeeskirjad kui õpilaskodu juhatajaga sõlmitud leping, kuna juhul kui rikkumise korda saatnud isik on töölepinguline töötaja, siis sellisel juhul saab vastavaid meetmeid kohaldada tööandja.

Vilistlaste isikuandmete avaldamisest

Peale isikuandmete kaitse üldmääruse (IKÜM) kehtimahakkamist on küsitud traditsiooniliste toimingute tegemise õigsuse üle olles üleeuroopalise õigusakti mõjusfääris.

Nii nagu enne IKÜM jõustumist, tuleb ka nüüd koolil endal otsustada, kas, kuidas ja kus avaldada oma koolilõpetajate nimekirjad ning see otsus tuleb ka asjaosalisteni viia. Inspektsioon selgitas haridusasutustele, et IKÜM ei sea keeldu vilistlaste nimede avaldamisele, aga seda tuleb teha kooskõlas andmekaitsereeglitega.

IKÜM-i põhjenduspunktis 4 on selgitatud, et isikuandmete töötlemine peaks olema mõeldud teenima inimesi. Õigus isikuandmete kaitsele ei ole absoluutne õigus, vaid seda tuleb kaaluda vastavalt selle ülesandele ühiskonnas ja tasakaalustada muude põhiõigustega vastavalt proportsionaalsuse põhimõttele.

Lisaks reguleerib IKÜM vilistlaste nimekirjade avaldamise kontekstis isikuandmete töötlemist ka siseriiklikult põhikooli- ja gümnaasiumiseadus (PGS) ning avaliku teabe seadus (AvTS). Seega ei ole IKÜM ainus isikuandmete töötlemist reguleeriv õigusakt. Avaliku sektori valduses olevate andmete töötlemist reguleerib AvTS, mis lubab asutuse valduses olevatele isikuandmetele juurdepääsu piirata eelkõige juhul, kui sellise teabe avalikustamine kahjustaks oluliselt isikute eraelu puutumatust (AvTS § 35 lg 1 p 11-15).

Siiski on inspektsioon soovitanud, et andmete avaldamisel peab lähtuma kindlasti andmekaitsereeglite minimaalsuse, eesmärgikohasuse ja asjakohasuse põhimõttest. Kool peab sõnastama, mis on nimekirja avaldamise eesmärk ning seejärel tuleb sisekorraeeskirjades ära kirjeldada nimekirja avaldamise kord ja teha see info kättesaadavaks kõigile asjaosalisetele. Kindlasti on põhjendamatu avaldada lisaks isikute nimedele ja lennule muid isikuandmeid.

Eraldi on soovitav kaaluda kuivõrd on vajalik avaldatu otsingumootoritele leitavaks tegemine. Enamasti häirib isikuid hoopis see, et leht on avalike otsingutulemuste tõttu leitav ja isikut on lihtne profileerida, mitte asjaolu, et isik on avaldatud vilistalasena ja leitav, kui otsida otse kooli kodulehelt. Seetõttu soovitame vilistlasi kajastav võrguleht otsingumootoritele peita.

Mittetulundusühingutel ja korteriühistutel tuli korrastada oma andmetöötlust

Mittetulundusühingute andmetöötluse õiguslikud alused tulevad kas seadusest või isiku vabatahtlikust nõusolekust. Inspektsioonini jõudsid mitmed märgukirjad, kus mittetulundusühinguna tegutsev spordiklubi on töödelnud isiku andmeid sotsiaalmeedias või veebilehel ilma tema nõusolekuta, mis on isiku õiguste rikkumine. Aastaraamatus pöörab inspektsioon tähelepanu juhtumile, kus korraga oli ohus 10 000 isiku privaatsus ja enamus nendest olid alaealised.

Nutisport.ee

Seda lugu kajastades tunnustab inspektsioon väga kahe matemaatikaõpetaja ettevõtmist, millest on saanud isegi õppevahend. Kuid iga hea tahte juures sündinud algatus võib anda vastupidiseid tagajärgi, kui ei pööra inimeste turvalisusele tähelepanu. Seega tuli ühe meediaväljaande märgukirja põhjal algatada järelevalvemenetlus 10 000 kasutajakontoga nutisport.ee veebilehe üle, kuna inspektsioon tuvastas mitmeid andmeturbelisi puudujääke ning andmetöötlejal puudus õiguslik alus laste andmete avaldamiseks.

> Alla 13-aastaste isikute kontode loomise ja andmete töötlemise üle peavad otsustama seaduslikud esindajad.

Kuna sellise veebilehe pidamine ei vastanud isikuandmete kaitse reeglitele, tegi inspektsioon ettepaneku see esmalt isikute privaatsuse kaitseks kiiresti sulgeda, mida andmetöötleja tegi. Alustatud järelevalvemenetluse käigus selgus, et tegemist oli äärmiselt ebaturvalise andmetöötlusega. Näiteks sai kontot luua suvalise aadressiga ja konto loomise paroolid edastati lahtise e- mailiga. Veebilehel avaldatud andmetele pääsesid ligi kõrvalised isikud, kes said vaadata laste isikuandmeid ja võistlustulemusi.

Isikuandmete kaitse üldmääruse (IKÜM) artikkel 8 ja isikuandmete kaitse seaduse (IKS) § 8 lõike 1 alusel on infoühiskonna teenuste pakkumiseks lapse isikuandmete töötlemine lubatud ainult juhul, kui laps on vähemalt 13-aastane. Seega alla 13-aastaste isikute kontode loomise ja andmete töötlemise üle peavad otsustama seaduslikud esindajad.

Inspektsioon tegi andmetöötlejale rikkumise lõpetamiseks ettepanekuid. Edaspidi peavad olema võistlustulemused edastatud nii, et need on nähtavad vaid osalejatele ning ei ole leitavad otsingumootoritele, sh ei ole nähtavad teades asukoha võrgulinki. Samuti peaks ka sel juhul oleme täidetud nõue, et avaldamine toimuks seaduslike esindajate teadmisel ja nõusolekul ning neid oleks teavitatud õigusest nõuda isikustatud kujul mitteavaldamise võimalust, nt asendades lapse nimi initsiaaliga.

Lisaks seadis inspektsioon nõudeks muuta kasutajakontode loomise ja haldamise keskkond turvaliseks, sh kehtestada nõuded parooli(salasõna) keerukusele. Lisaks peaks see hõlmama kasutajatele võimalust oma paroolide muutmiseks ja nende sellest teavitamist ning kasutajakonto loomisel meiliaadressi autentimist. Oluliseks nõudeks rikkumise lõpetamiseks sai samuti ettepanek avaldada veebilehel andmekaitsetingimused.

Järelevalvemenetlus nutisport.ee veebilehe üle lõppes peale kõikide nõuete täitmist.

Korteriühistud

Korteriühistute peale tehtud kaebused tulid paljudel juhtudel sisesuhetest. Inspektsioon pööras tähelepanu, et üldreegel on korteriühistu liikmete andmete avaldamisel see, et sisesuhtes (ühistu liikmete vahel) on isikuandmete avaldamine lubatud ning välissuhtes (kolmandatele isikutele) on selleks vajalik

eelnev isiku nõusolek. Tähelepanu tuleb juhtida ka sellele, et ka korteri omanike nimede avaldamine trepikojas vms ühisruumis on seadusega vastuolus, sest sinna on võõrastel juurdepääs. Keelatud on avaldada ka ainult korterinumber, kuna selle järgi on omanike nimed tuvastatavad kas kinnistusraamatust või muust avalikust registrist.

Korteriühistu saab töödelda ainult korteriomanike andmeid (sh mitte üürnike andmeid) ja seda minimaalses mahus ehk ainult ühistu tööks vajalikke andmeid. Kõikide korteriga seotud teemade eest vastutab korteri omanik või tema poolt ametlikult volitatud isik ning ühistul ei ole alust koguda kolmandate isikute andmeid või andmeid, mis kahjustavad üleмääraselt kolmandaid isikuid ja ei ole ühistu tööks vajalikud. Parkimise korraldamiseks ei ole ühistul vaja teada, kes on millise auto omanikuks või kasutajateks, sh veel koopiad autodokumentidest. Inspektsioon juhib tähelepanu asjaolule, et ükski isik ei saa anda kellegi kolmanda isiku eest nõusolekut tema andmete töötlemiseks (kolmanda isiku andmed tehnilises passis).

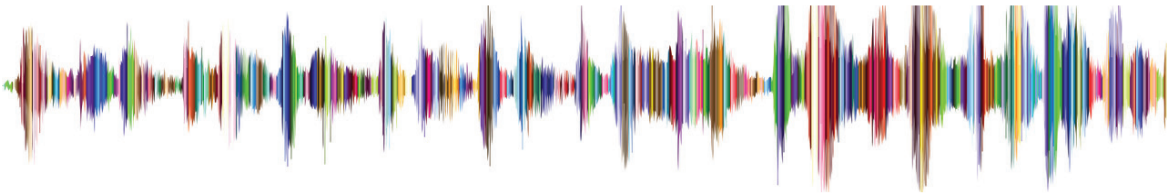
Oluline on märkida, et ka ühistu peab jälgima, et ühistu liikmeid tuleb enne isikuandmete edastamist volitatud töötlejale teavitada (nt kui ühistu kasutab väljapoolt raamatupidamisteenust jms) ja sõlmida tuleb volitatud töötlejatega alati leping.

Kõnesalvestis kui isikuanne

Kõnesalvestis on oma olemuselt mitte ainult isikuanne, vaid isikuandmete kogu, mille tundlikkus sõltub selle sisust ehk informatsioonist, mida inimene enda kohta avaldab. Olgu selleks näiteks teave inimese elukoha, majandusliku olukorra, tervisliku või psüühilise (hetke)seisundi kohta. Samuti on isikuandmeks ka helistaja hääl.

Kõnesalvestiste töötlemisele ei ole pööratud andmekaitselisest aspektist veel piisavalt tähelepanu nii era kui avaliku sektori asutustes. Aastaraamatu näide tuleb sel korral Politsei-ja Piirivalveamet (PPA) edastatud rikkumisteatest ja sellele järgnenud haldusjärelevalve menetlusest.

PPA tõi rikkumisteates välja, et toimus lähisuhtevägivalla konverents, mille jaoks küsis Ida Prefektuur Häirekeskuselt neile laekunud telefonikõnede salvestusi. Häirekeskuse Ida Keskus edastas politseile originaalfailid kõnedest. Ida Prefektuuri kriminaalbüroo eemaldas salvestustest isikutele viitavad andmed (nimed, aadressid), kuid isikute hääli ei moonutatud ja salvestised mängiti konverentsil ette. Kuna konverentsi päeval soovis Virumaa Teataja ajakirjanik saada konverentsil esitletud kõnesalvestisi, siis PPA ametnik andis ilma Häirekeskuse kooskõlastuseta mälupulgal kõik esitatud kõned ka kohaliku väljaande ajakirjanikule, kes Virumaa Teataja veebilehel need avalikustas. Avalikustamine oli lühiajaline, sest Häirekeskuselt saadud info kohaselt eemaldati salvestised veebilehelt kohe pärast seda, kui sai teoks meediaväljaande poole pöördumine.



Kuivõrd isikute hääli ei moonutatud, olid lähisuhtevägivalla all kannatavad isikud kaudselt tuvastatavad. Inspektsioon leidis, et on mõistetav õppe- ja koolituseesmärgil konverentsi läbiviimine ning on arusaadav ja vajalik teha ennetus-ja teavitustöid lähisuhtevägivallast, kuid see ei tähenda, et asutusele inimese poolt usaldatud infot kõnesalvestises võib ilma tema nõusoleku ja teadmiseta avaldada, seda enam, et suurele auditooriumile, kuhu võis kuuluda helistajat tundvaid inimesi.

PPA seisukoht oli, et isikud ei olnud kaudselt tuvastatavad, kuid inspektsioon sellega ei nõustunud.

PPA seisukoht oli, et isikud ei olnud kaudselt tuvastatavad, kuid inspektsioon sellega ei nõustunud. Sel korral lõpetas inspektsioon menetluse noomitusega nii PPA kui Häirekeskuse suhtes, sest menetluse käigus sai inspektsioonile selgeks, et isikutele intsident reaalselt siiski riivet ei põhjustanud. Inspektsioon viitas, et selliste isikuandmete edastamised tuleks eelnevalt nii organisatsioonisiseselt kui asutuste vahel kooskõlastada ja asjad läbi mõelda tulenevalt andmekaitsereeglitest. Samuti oleks tulnud kasutada meetmeid isikute varjamiseks. Selliseid juhtumeid, kus kannatanu olukorda halvendab oht privaatsusele, saab kindlasti ära hoida, kui asutused korraldavad oma töötajatele andmekaitsealaseid koolitusi.

Isikuandmete edastamisest kolmandatesse riikidesse

2019. aasta läbivaks märksõnaks võiks olla uue praktika paika loksumine.

Isikuandmete kaitse üldmääruse (IKÜM) kehtima hakkamine kaotas ära praktiliselt kohustuse taotleda järelevalveasutustelt luba andmete edastamiseks kolmandasse, mittepiisava andmekaitsetasemega välisriiki (edaspidi välisriiki) .

Uueks praktikaks on saanud see, et andmete edastamisel välisriiki ei ole kõige olulisem taotleda luba inspektsioonilt, vaid kui edastamine on vajalik, peab andmetöötleja kõigepealt endale selgeks tegema, milline on isikuandmete edastamise õiguslik alus. Andmetöötluse õiguslikud alused on loetletud IKÜM artiklis 6, eriliigiliste isikuandmete töötlemise õiguslikud alused on loetletud artiklis 9.

Seejärel tuleb kindlaks teha, kas edastamisel rakendatakse piisavalt kaitsemeetmeid ning millised on andmete edastaja ja saaja kohustused, kuidas rakendada andmete edastamisel minimaalsuse ja eesmärgipärasuse põhimõtteid jne.

Järgmisena tuleks vaadelda riiki, kuhu plaanitakse andmeid edastada. Kui andmeid edastatakse Euroopa Liidu ja Euroopa Majanduspiirkonna siseselt või riikidesse, mille puhul Euroopa Komisjon on andnud adekvaatsusotsuse[5] , siis edastamine on analoogne Eesti-sisese edastamisega (st ei ole vaja rakendada IKÜM 5. peatükki).

Uueks praktikaks on saanud see, et andmete edastamisel välisriiki ei ole kõige olulisem taotleda luba inspektsioonilt, vaid kui edastamine on vajalik, peab andmetöötleja kõigepealt endale selgeks tegema, milline on isikuandmete edastamise õiguslik alus.

[5] Euroopa Komisjoni nimekiri: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Kui aga soovitakse andmeid edastada riiki, mis ei kuulu eelnimetatud erandite alla, siis peab andmetöötleja uurima täpsemalt IKÜM 5. peatükki ning vajadusel rakendama artiklist 46 tulenevaid lisakaitsemeetmeid. Erandolukordades, üksikujuhtumite puhul, tuleks rakendada IKÜM-i artiklit 49.

Ka juhul, kui andmetöötleja valib ühe IKÜM artiklis 46 nimetatud lisakaitsemeetmest, ei tule alati inspektsioonilt luba taotleda. Loa taotlemine on kohustuslik vaid artikli 46 lõikes 3 nimetatud kaitsemeetmete kasutamisel (üldine, nn *ad-hoc* leping või avaliku sektori asutuste vahelised halduskokkulepped).

Mida tähendab inspektsioonilt loa taotlemise protseduur?

Inspektsioonil tuleb loa taotlemise menetlemisel rakendada järjepidevuse mehhanismi, mis tähendab, et esitatud andmete edastamise lepingu ja inspektsiooni otsuse mustandi peame edastama Euroopa Andmekaitsenõukogule otsuse tegemiseks. Taoline protseduur on ajaliselt mahukas ning peab arvestama, et kõik andmekaitsenõukogu liikmed saavad võimaluse avaldada lepingu ja inspektsiooni otsuse mustandi osas arvamust ning hääletama andmekaitsenõukogu otsuse osas.

> Loa taotlemine on kohustuslik vaid artikli 46 lõikes 3 nimetatud kaitsemeetmete kasutamisel.

Seega on pigem mõistlik teha valik üldmääruse artikli 46 lõikes 2 kirjeldatud kaitsemeetmete hulgast. Kõige enam kasutavam kaitsemeede ongi selle artikli punktis c nimetatud Euroopa Komisjoni koostatud standardsed andmekaitseklauslid (*standard contractual clauses*[6]) . Selle kaitsemeetme puhul on andmete edastamise tüüplepingu tekst etteantud ning lepingu osapooled lähtuvad sellest.

Teine väga tihti kasutatav kaitsemeede on siduvad kontsernisisesed eeskirjad[7] (binding corporate rules), mille kasutamine nõuab ka IKÜM artiklis 47 kirjeldatud protseduuride läbimist. Siduvad kontsernisisesed eeskirjad, nagu nimigi ütleb, on mõeldud suurtele ülemaailmsetele kontsernidele, kellel on tütaretevõtteid ning andmete liikumist väga paljudes eri riikides üle maailma.

Üldine kontsernisiseste eeskirjade heakskiitmise protseduur toimub analoogse järjepidevusse mehhanismi alusel, kuid on veel detailsem ja pikemaajalisem protseduur. Juhtival andmekaitseasutusel on kohustus enne järjepidevuse mehhanismi käivitamist kaasata dokumentatsiooni läbivaatamiseks vähemalt 2 andmekaitseasutust, aga kui eeskirjad saavad andmekaitsenõukogus lõpliku heakskiidu, saavad seda kaitsemeedet kasutada kõik eeskirjades nimetatud ettevõtted ilma eraldi lepinguid sõlmimata või täiendavaid lube taotlemata.

> Artikkel 49 kasutamisel on vaja silmas pidada põhitõde – tegemist on eranditega ehk eriolukorras andmete ühekordse (või ka vajadusel korduva) edastamisega.

Siduvate kontsernisiseste eeskirjade protseduuri vastavalt artiklike 47 algatab ja viib läbi juhtiv andmekaitse järelevalveasutus ehk selle liikmesriigi asutus, kus asub kontserni (Euroopa) peakontor või kontor, kus tehakse andmekaitsealaseid otsuseid, mis on teistele kontserni liikmetele siduvad.

Seega saab andmete välisriiki edastamise loa taotlemise vajaduse osas öelda, et IKÜM-i tulekuga on eelkõige andmetöötlejale endale pandud vastutus tagada andmete õiguspärane välisriiki edastamine ning eelnevat luba ja järelevalveasutuse hinnangut enamasti taotlema ei pea.

[6] Euroopa Komisjoni tüüplepingud: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[7] Euroopa Komisjoni BCR materjalid https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

IKÜM annab andmetöötlejatele rohkem võimalusi andmete edastamise kaitsemeetmete valiku osas (võrreldes varasemalt kehtinud korraga) – näiteks on võimalus kasutada toimimisjuhendeid, sertifitseerimist ja ka erandite kasutamine on võrreldes varasemaga laiem.

Mida tähendab erandolukordades andmete välisriiki edastamine?

IKÜM-i artikkel 49 loetleb erandid, mil võib mittepiisava andmekaitsetasemega riiki edastada andmeid ilma inspektsiooni loata ja artiklis 46 kaitsemeetmeid rakendamata. Sellisteks erandjuhtumiteks on isiku nõusolek, isiku ja andmetöötleja vaheline leping, avalikust huvist tulenevad põhjused, õigusnõuete koostamised või teatud juhtudel ka õigustatud huvi jms. Artikkel 49 kasutamisel on vaja silmas pidada põhitõde – tegemist on eranditega ehk eriolukorras andmete ühekordse (või ka vajadusel korduva) edastamisega. Kui on vajadus andmeid pidevalt ja püsivalt edastada, siis ei ole tegemist erandolukorraga ning artiklit 49 rakendada ei saa.

Euroopa Andmekaitsenõukogu on avaldanud ka soovituse koos praktiliste näidetega erandolukordades toimuva andmete edastamise osas, mille leiab https://edpb.europa.eu/our-work-tools

Õigusest tutvuda oma isikuandmetega

Isikuandmete kaitse üldmääruse (IKÜM) artikli 15 kohaselt on andmesubjektil üldjuhul õigus tutvuda enda kohta kogutud andmetega. Seda õigust võib piirata üksnes siis, kui andmete edastamine kahjustab teiste isikute õigusi ja vabadusi.

Inspektsiooni menetluses oli kaebus, mille kohaselt soovis isik kohaliku omavalitsuse (KOV) sotsiaalosakonnalt enda kohta kogutud andmete väljastamist. Muuhulgas soovis kaebaja kirjavahetust, mis oli kohalikule omavalitsusele sisse tulnud ning milles temaga seotud murekohtasid on käsitletud. KOV keeldus andmete väljastamist osas, mis puudutas teiste isikutega peetud kirjavahetust, tuginedes IKÜM artikkel 15 lõikele 4, kuna kirjavahetuse edastamine kahjustaks teise isiku õigusi ja vabadusi. Kaebaja ei olnud otsusega rahul ning leidis, et andmetöötleja ei ole kirjavahetuse väljastamata jätmist piisaval määral põhjendanud.

Sellist laadi kaebuste lahendamisel tuli inspektsioonil hinnata, kas andmete väljastamine kahjustaks teist isikut sedavõrd, et see kaalub üle andmesubjekti õiguse saada enda kohta käivaid andmeid ning kas teabevaldaja IKÜM artiklist 12 lõikest 4 tulenev põhjendamise kohustus on täidetud.

Inspektsioon palus KOV-le tehtud järelepärimises edastada hinnangu andmiseks kaebuse aluseks olev kirjavahetus ja selgitused.

Õige ja vale lahendus

KOV viitas vastuses järelepärimisele Riigikohtu Halduskolleegiumi 21.02.2019 lahendile nr 3-16-2348 punktile 18, milles kohus on leidnud, et „teise isiku õiguse riive all ei tule mõista üksnes olukorda, kus juurdepääsuõiguse andmisel avaneks võimalus tutvuda teise isiku isikuandmetega. Teise isiku õigusena tuleb kõne alla mistahes õigusnormile tuginev subjektiivne õigus.

> Keeldumine on lubatav, kui juurdepääs võib kaasa tuua teise isiku õiguste riive määral, mis on kaalukam, kui andmesubjekti juurdepääsuõigus.

KOV võimaldas inspektsioonile juurdepääsu kõnealusele kirjavahetusele, et hinnata andmetöötleja põhjenduste õigsust. Inspektsioo-

ni hinnangul toimis KOV küsitud kirjavahetuse väljastamata jättes tuginedes IKÜM artikkel 15 lõikele 4 õiguspäraselt, kuna kirjavahetuse väljastamine oleks kahjustanud kirja koostaja õigusi ja vabadusi. Arvestades kirja sisu, ei olnud KOV-il võimalik keeldumist detailsemalt põhjendada, kuna see oleks pannud kirja koostaja analoogsesse olukorda nagu kirja kaebajale edastamine.

Kui eeltoodud näites hindas KOV sotsiaalosakonna ametnik õigesti, et andmesubjekti IKÜM artiklist 15 tulenev õigus saada enda kohta käivaid andmeid ei ole absoluutne, siis praktikas on sagedased ka vastupidised näited.

Teises juhtumis pöördus inspektsiooni poole kaebusega lapsevanem, kes ei olnud rahul sellega, et KOV-i lastekaitsespetsialist edastas kolmanda isiku esindajale kaebaja lastega peetud vestluste kirjalikud kokkuvõtted.

Andmete väljastamist taotleti IKÜM artikkel 15 alusel, kuna vestlusest käis muuhulgas läbi ka kokkuvõtete edastamist taotlenud isik. Kuna lisaks sisaldas vestlus viiteid ka lapsevanemale, st neis olid tuvastatavad andmed kaebaja kohta, oli KOV ametniku roll hinnangu andmisel, kas andmete väljastamine IKÜM artikkel 15 alusel on õiguspärane või mitte ning see nõudis arvestamist rohkemate asjaoludega.

Arvestama pidanuks, et lisaks sellele, et kolmandale isikule andmete avaldamine võis kahjustada lapsevanema õiguseid, peab pöörama tähelepanu laste heaolu kaitsmisele ning hindama, milline on riive ja võimalik mõju laste õigustele, kui vestluse kokkuvõtted edastatakse kolmandale isikule ja lisaks sellele, kui kokkuvõtetele saab juurdepääsu lapsevanem, kelle kohta sisaldab kokkuvõte samuti hinnanguid.

Asutuste andmete hoiustamine pilveteenustes peab tagama turvalisuse

Inspektsioon juhtis riigiasutuste ja kohalike omavalitsuste tähelepanu pilveteenuse kasutamisega seotud riskidele, kuna Eesti avalik sektor on üha enam otsimas ja kasutusele võtmas kulutõhusamaid IT-lahendusi. Sageli on nendeks ühtsete kasutustingimustega avalikud pilveteenused, mida osutavad valdavalt piiriülesed teenusepakkujad peakorteritega väljaspool Euroopa Liitu. Olgu selle näiteks kontoritarkvara, kus dokumente või e-kirju ei hoita enam lokaalselt asutuse serveris, vaid maailma eri paigus asuvates andmekeskustes.

Eesti asutused ei saa lähtuda kulutõhusust ja hoiustada andmeid avalikes pilveteenustes. Avalikul sektoril on kohustus ning vastutus, et teabele oleks tagatud õigeaegne juurdepääs ka kriiside ja hädaolukordade ajal ning elutähtsate teenuste toimepidavuse tagamiseks. Kui teabele juurdepääs ja selle edastamine sõltub ainult välisest teenusepakkujast sh välislahendustest, ei pruugi õnnestuda neid kohustusi täita. Riigiasutused peavad suutma korraldada teabevahetuse ka olukordades, kus välisühendused halvatakse kas pahatahtliku ründe tõttu või on sunnitud riik ennetava meetmena ise ühendused katkestama.

Saadetud ringkirjaga saab tutvuda www.aki.ee veebilehel[8].

[8] https://www.aki.ee/et/inspektsioon-kontaktid/ringkirjad

AVALIKU TEABE SEADUSE TÄITMISEST

Kui mõni aasta tagasi võis pidada asutuste teadlikust avalikule teabele juurdepääsu võimaldamisel üsna heaks, siis peale kohalike omavalitsuste ühinemist ning Euroopa Isikuandmete kaitse üldmääruse jõustumist on eksimusi ja arusaamatusi tunduvalt rohkem. Nii näiteks ollakse tihti arvamusel, et kui avalik teave sisaldab isiku nime, siis ei tohi sellisele teabele juurdepääsu võimaldada.

Avaliku teabe seaduse tõlgendus tekitas jätkuvalt segadust

Põhiseaduse (PS) § 44 lg 1 sätestab riigi- ja kohalike omavalitsuste asutustele kohustuse anda isiku nõudmisel informatsiooni oma tegevuse kohta. Sellest sättest tuleneb ka avaliku teabe seaduse mõte, mille kohaselt on avaliku teabe seaduse eesmärgiks tagada üldiseks kasutamiseks mõeldud teabele avalikkuse ja igaühe juurdepääs ning anda avalikkusele võimalus kontrollida avalike ülesannete täitmist.

Siiski ei ole õigus saada infot avaliku võimu organite ja ametiisikute tegevuse kohta piiramatu. PS § 44 lõike 2 kohaselt ei laiene juurdepääs andmetele, mille väljaandmine on seadusega keelatud. Samuti ei saa anda juurdepääsu asutusesiseseks kasutamiseks mõeldud andmetele. PS § 44 lõikes 2 sätestatud põhiõigust võib piirata eeldusel, et kehtestatud piirangul peab olema legitiimne eesmärk ning piirang peab olema proportsionaalne seatud eesmärgiga.

Kui eraõiguslikes suhetes töödeldakse isikuandmeid valdavalt lepingu täitmiseks (IKÜM art 6 lg 1p b) või andmesubjekti nõusoleku alusel (art 6 lg 1 p a), siis avaliku võimu teostamisel ei ole isikuandmete töötlemiseks üldjuhul andmesubjekti luba vaja. Isikuandmete töötlemine on seaduslik ka siis, kui andmeid töödeldakse isikuandmete vastutava töötleja seadusjärgsete kohustuste täitmiseks või kui see on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks (IKÜM art 6 lg 1 p-d c ja e).

> Kehtestatud piirangul peab olema legitiimne eesmärk ning piirang peab olema proportsionaalne seatud eesmärgiga.

Seejuures ei ole vaja iga isikuandmete töötlemise toimingut reguleerida õigusaktiga. Piisab sellest, kui isikuandmete töötlemise eesmärk tuleneb Euroopa Liidu või liikmesriigi õigusaktist (IKÜM põhjenduspunkt 45 ja art 6 lg 3). Seega saab avalikule teabele, mis sisaldab isikuandmeid, juurdepääsu piirata ainult juhul, kui see oluliselt kahjustab isikute eraelu puutumatust. Ehk siis

peale IKÜM tuleb arvestada ka teisi seadusi, mis reguleerivad isikuandmetele juurdepääsu.

Teabenõuetele vastamise probleemidest

Kahetsusväärselt tekitas jätkuvalt segadust, millal on kodanik asutuse poole pöördunud teabenõudega, millal selgitustaotlusega või millal märgukirjaga. Ka ei teata seda, et inspektsiooni pädevusse kuulub ainult teabenõuetele vastamise üle järelevalve teostamine, mitte selgitustaotlustele ja märgukirjadele. Teabenõude korras saab teabevaldajalt küsida tema valduses olevaid dokumente või väljavõtteid andmekogudest, millest on võimalik teha koopiaid. Teabenõude korras ei saa nõuda endale sobival kujul tabelite, statistika vms koostamist, mis nõuab täiendavat andmete töötlemist, sh erinevatest dokumentidest andmete kogumist ja selle alusel uue dokumendi koostamist.

> Lepingu teine pool ei saa avaliku sektori asutusele ette öelda, mida võib avalikustada ja mida mitte, sest avaliku sektori asutus saab oma valduses olevale teabele juurdepääsu piirata üksnes juhul, kui selleks on seadusest tulenev alus.

Lisaks eeltoodule on jätkuvalt üheks suuremakas eksimuseks see, et teabenõuetele ei vastata seaduses sätestatud tähtaja jooksul. Ka juhul, kui kodaniku pöördumine ei ole oma olemuselt teabenõue, kuid on pealkirjastatud teabenõudena, tuleb sellele vastata viie tööpäeva jooksul. Vastata tuleb ka siis, kui keeldutakse teabenõude täitmisest. Keeldumise korral tuleb selgitada, et tegemist ei ole teabenõudega ning millal kodaniku pöördumisele vastatakse. Kodanik ei pea teadma, millal loetakse tema pöördumine teabenõudeks ja millal selgitustaotluseks (AvTS § 23 lg 2 p 5 ja lg 3). Kui teabenõudja on edastanud teabevaldajale pöördumise, mis on pealkirjastatud „teabenõue“, on teabenõudjal õigustatud ootus saada oma pöördumisele vastus viie tööpäeva jooksul ja teabevaldajal on kohustus vastata 5 tööpäeva jooksul.

Näitena võib tuua juhtumi, kus teabevaldaja jättis teabenõude täitmata põhjusel, et ei teadnud, kuidas tuleks teabenõude korral väljastada dokument, mis sisaldab ka piiranguga teavet. Samuti ei ole jätkuvalt harvad sellised juhtumid, kus jäetakse teabenõue täitmata põhjusel, et dokument sisaldab mingis osas piiranguga andmeid või lepingu teine pool erasektorist on keelanud dokumendi avalikustamise. Lepingu teine pool ei saa avaliku sektori asutusele ette öelda, mida võib avalikustada ja mida mitte, sest avaliku sektori asutus saab oma valduses olevale teabele juurdepääsu piirata üksnes juhul, kui selleks on seadusest tulenev alus.

Kas teabenõudjale võib juurdepääsupiirangulist infot sisaldavat dokumenti välja anda või mis alusel tuleks konkreetsele dokumendile juurdepääsupiirang kehtestada, sellele küsimusele on soovitud läbi aastate inspektsioonilt selgitusi. Siinkohal tuleb inspektsioonil küsijale selgitada, et inspektsioon järelevalveasutusena ei saa teabevaldaja eest otsustada ega kehtestada dokumentidele juurdepääsupiiranguid. Otsus tuleb teha teabevaldajal endal ning vaidluse korral ka oma otsust põhjendada.

2019. aasta lõpus sagenes ka pöördumiste hulk, kus inspektsioonile edastati teabenõuete vastuseid ja sooviti hinnangut, kas asutus on teabenõudele vastanud ikka korrektselt. Samas ei lisatud soovile teabenõuet. Selleks, et inspektsioon saab anda adekvaatset hinnangut teabenõude nõuetekohase täitmise osas, on tal kõigepealt vaja teada, mida teabenõudega küsiti. Kui teabenõude vastuses öeldakse, et meil Teie poolt soovitud dokumenti ei ole või väljastame soovitud dokumendi, siis selle põhjal ei saa anda konkreetset hinnangut. Seda põhjusel, et vastusest pole arusaadav kas väljastati kõik küsitud dokumendid või jäi mõni väljastamata.

Teabenõude sisu ja pealkiri ei lähe kokku

Läbiv probleem on olnud ka see, et paljud teabenõudena peakirjastatud avaldused ei ole seda sisult mitte. Näiteks soovis kinnipeetav informatsiooni naisterahva kohta, kes viibis arsti kabinetis tema visiidi ajal. Tegemist oli meditsiiniõega, kuid antud pöördumine ei olnud käesolevas asjas sisult teabenõue.

Veel võib välja tuua isiku enda kohta andmete küsimise, mille vangid sageli teabenõudeks nimetavad. Siia alla saab näiteks panna enda terviselogidega tutvumise. Tegemist on IKÜM rakendamisega, kus on paika pandud, et andmetöötlejal on vastamiseks kuni üks kuu. Vangid aga lahterdavad taolise nõude sageli teabenõudeks, millele vastamise tähtaeg on aga oluliselt lühem. Siin peab inspektsioon hindama lisaks muule esmalt ka seda, millise pöördumisega on tegemist. Lisaks tuleb analüüsida, kas asja peab menetlusse võtma ikkagi vaidena või on see kaebus. Olukorra selgitamine ning asjaolude uurimine võtab taas inimressurssi. Ka ei ole sageli kasu vangile situatsiooni selgitamisest, kuna järgmisel korral tuleb samasugune asi sisse järjekordse vaidena.

Teabe väljastamine volikogu liikmele

Eelmisel aastal registreeriti mitmeid märgukirju kohaliku omavalitsuse volikogu liikmetelt seoses sellega, et vallavalitsus kas ei võimalda neile dokumendiregistrile juurdepääsu või on kehtestanud mingitele kirjadele ebaseaduslikud juurdepääsupiirangud. Teisalt olid vallavalitsused mures, et kui volikogu liikmetele on avaldatud/võimaldatud juurdepääs ka piiranguga teabele, siis avalikustavad volikogu liikmed sellist teavet ka nn oma valijatele, leides, et neil on selleks õiguslik alus.

Volikogu liikmete teabe saamise õigus tuleneb kohaliku omavalitsuse korralduse seaduse §-st 26, mis sätestab, et volikogu liikmel on õigus saada omavalitsuselt teavet ja dokumente oma ülesannete täitmiseks, mis ei ole seadusega keelatud. Seega ei tulene volikogu liikme teabe saamise õigus avaliku teabe seadusest. Tegemist on asutuse sisesuhtega, mille üle inspektsioon järelevalvet ei teosta. Sellise seisukoha on andnud ka Riigikohus.

> Juurdepääsupiiranguga teabele on volikogu liikmel juurdepääsuõigus juhul, kui selline teave on vajalik tema tööülesannete täitmiseks.

Siinkohal tuleb aga märkida, et ükski seadus otseselt ei keela volikogu liikmetele teabele juurdepääsu. On küll mõned seadused, mis annavad kindla loetelu, kellel on vastavale teabele juurdepääs. Inspektsioon on siin seisukohal, et juurdepääsupiiranguga teabele on volikogu liikmel juurdepääsuõigus juhul, kui selline teave on vajalik tema tööülesannete täitmiseks. Sellist teavet ei tohiks avalikustada kolmandatele isikutele. Kuna avaliku teenistuse seadus ei kohaldu volikogu liikmetele, mis paneb ametnikele saladuse hoidmise kohustuse, siis on omavalitsustes problemaatiline, kuidas tagada, et volikogu liikmed ei avalikustaks neile tööülesannete täitmisel teatavaks saanud piiranguga teavet.

Tähelepanekuid vaidemenetlustest

Avaliku teabe seaduse kohaselt on isikul kelle õigusi on rikutud teabe kättesaadavuse osas õigus pöörduda vaidega inspektsiooni poole. Siinkohal tuleb rõhutada, et seadus ei anna ühele poolele ainult õigust ega pane teisele poolele ainult kohustust, vaid mõlemal poolel on nii õigused kui kohustused. Ehk siis, selleks et teabevaldajal oleks arusaadav, millist teavet teabenõudja soovib, tuleb teabenõue esitada võimalikult selgelt. Tõsi, teabevaldajal on kohustus teabenõudjat teabenõude esitamisel abistada ning kui teabenõudest pole võimalik aru saada, millist teavet teabenõudja soovib, siis on teabevaldajal kohustus teabenõuet täpsustada.

Eeltoodu ei tähenda aga seda, et teabevaldaja peaks iga teabenõude korral üle küsima, kas ta sai teabenõudest ikka õigesti aru. Ei saa eeldada, et kui teabenõudest ei ole võimalik aru saada, milliseid muid dokumente teabenõudja soovis lisaks väljastatud teabele, peab teabevaldaja aru saama küsija tegelikest soovidest. Kui teabenõudest ei olnud võimalik aru saada, mida vaide esitaja tegelikult soovis , siis ei saa ka inspektsioon kohustada teabevaldajat väljastama teavet, mida teabenõudes küsitud ei ole. Inspektsiooni menetluste ajalukku jääb ka selliseid juhtumeid, kus vaidemenetluse käigus soovib vaide esitaja, et inspektsioon kohustaks teabevaldajat väljastama talle dokumente, mida tegelikult teabenõudes küsitud ei ole.

Ärisaladus

Üsna palju oli 2019. aastal ka vaidemenetlusi seoses teabe väljastamata jätmisel põhjusel, et soovitud dokumendid sisaldavad ärisaladust. See, kui dokument sisaldab ärisaladust, ei tähenda see veel seda, et selliseid dokumente teabenõude korral üldse ei väljastata. Tihti teabevaldajad ei hinda, kas ärisaladuseks tunnistatud teabe puhul on ikka tegemist ärisaladusega ja mis osas soovitud dokument sisaldab ärisaladust, vaid lähtutakse äripartneri soovist. Siinkohal tuleb rõhutada, et kohus on mitmel korral asunud seisukohale, et teabe ärisaladuseks tunnistamisel ei saa lähtuda ainult äripartneri soovist vaid tuleb hinnata, kas ärisaladuseks tunnistatud teave vastab ärisaladuse tunnustele ning hinnata kas ja kuidas see võib kahjustada äripartneri ärihuve. Vajadusel tuleb selleks küsida selgitusi äri partnerilt.

Kohus on mitmel korral asunud seisukohale, et teabe ärisaladuseks tunnistamisel ei saa lähtuda ainult äripartneri soovist vaid tuleb hinnata, kas ärisaladuseks tunnistatud teave vastab ärisaladuse tunnustele ning hinnata kas ja kuidas see võib kahjustada äripartneri ärihuve.

Ärisaladusega seotud vaiete puhul on olnud ka vaide esitaja sooviks saada inspektsiooni abiga võimalikult palju informatsiooni konkurendi tegevuse koha. Inspektsioonil on üsna keeruline hinnata erinevaid valdkondi puudutavat teavet, mis võib olla ärisaladus ning kahjustab teise poole ärihuve. Siinjuures on kindlasti abiks ettevõtete selgitused oma ärisaladuste kaitsmise/hindamise osas. Mida põhjalikumad on selgitused, seda lihtsam on inspektsioonil oma otsuseid teha. Paraku praktikas aga ettevõtted tihti ei oska ka ise põhjendada, kuidas mingi teabe avalikustamine võib nende ärihuve kahjustada, vaid soovitakse, et kogu dokument oleks ärisaladus. Sellega inspektsioon nõustuda ei saa.

Juurdepääsupiirang

Vaidemenetluse käigus on samuti ilmnenud, et juurdepääsupiirangu kehtivus 5+5 aastat ei ole asutuste hinnangul piisav. Kuna inspektsioon järelevalveasutusena saab kontrollida seaduse täitmist, kuid ei saa lubada/anda nõusolekut seadusest erinevate piirangute kehtestamist, mida sageli eeldatakse, siis ei saa inspektsioon anda luba kehtesta

piirangut pikemaks kui 10-ks aastaks, kui mõnest eriseadusest ei tulene teisiti. Kui asutused leiavad, et piirangu kehtestamise maksimaalne pikkus 10 aastat, v.a. isikuandmed, jääb liiga lühikeseks, tuleb pöörduda seadusandja poole ja teha vastava teabe osas erisus.

Rahuldamata vaie liiga suure mahu tõttu

Vaiete puhul saab välja tuua, et viimasel aastal suurenes vaiete hulk, kus soovitakse teabenõude korras koopiaid erinevatest järelevalvetoimikutest. Nii näiteks sooviti teabenõudes Terviseametilt koopiaid 26 toimikust, mis sisaldasid ca 1300 lehekülge teavet. Ilmselgelt on sellisel juhul tegemist suure mahuga, mis takistab asutusele pandud ülesannete täitmist. Seda enam, et antud juhul sisaldasid toimikud ka piiranguga andmeid, mis nõudis toimikute läbi vaatamist ja piiranguga teabe kinni katmist. Siinkohal on ka küsitav, kas seadusandja mõte teabenõuete esitamisel on ikka olnud asutuste tegevuse osas lauskontrolli tegemise võimaldamine, mille käigus oleks võimalik küsida välja kogu asutuse valduses olev piiranguta dokumentatsioon, sh ka dokumendid, mis sisaldavad piiranguga teavet ning vajavad enne väljastamist täiendavat töötlemist. Eeltoodud vaide puhul nõustus inspektsioon teabevaldajaga, et tegemist on suure mahuga, mis nõuab asutuse töökorralduse muutmist ja takistab talle pandud ülesannete täitmist, mistõttu jättis inspektsioon vaide rahuldamata.

Rahuldamata vaie pädevuse puudumise tõttu

Inspektsiooni menetluses oli ka ühe kooliõpilase vaie, kus õpilane soovis, et kooli poolt koostatud käskkirjad tunnistataks kehtetuks, kuna need ei vastanud tema hinnangu haldusakti nõuetele ja kohustaks kooli vormistama käskkirju tema poolt soovitud kujul. Kuna inspektsioon ei teosta järelevalvet haldusaktide vormistamise üle, jäi vaie rahuldamata.

Vaided kinnipidamisasutustest

Üsna suure osa inspektsiooni töömahust võtsid enda alla kinnipeetavate poolt esitatavad vaided ning muud pöördumised. Üks kinnipeetav võis esitada ühes päevas kuni kümme teabenõuet. Ühes vaides võib olla kajastatud kümmekond küsimust. Käsitleme vangide kaasusi aastaraamatus seetõttu, et teabe nõudmise kaudu ilmneb mitmeid probleeme, mida esineb ka seoses teiste asutustega.

Käsitleme vangide kaasusi aastaraamatus seetõttu, et teabe nõudmise kaudu ilmneb mitmeid probleeme, mida esineb ka seoses teiste asutustega.

Teabenõudega saab küsida asutuses olemasolevaid dokumente, mis on saadud või loodud avalikke ülesandeid täites. Näiteks, asutuse käskkiri on juba loodud dokument, mida võib teabenõudega saada, kui sellele ei kehti avaliku teabe või eriseadusest tulenevat juurdepääsupiirangut.

Kui küsitakse välja informatsiooni enda kohta, enda liikumiste kohta, ettevõtete ja asutuste töötajate kohta ja palju muu sarnase kohta, on küsitav, kas tegemist on avaliku teabega AvTS mõttes. Näiteks on tavapärastes küsimisteks saanud:

- ❒ Millal vahetatakse katkine aken?
- ❒ Mis kuupäeval on pildistamine?
- ❒ Kuidas toimub vangla ventilatsioonisüsteemi eest hoolitsemine?
- ❒ Kuidas kasutada vangla osakonna külmikut?

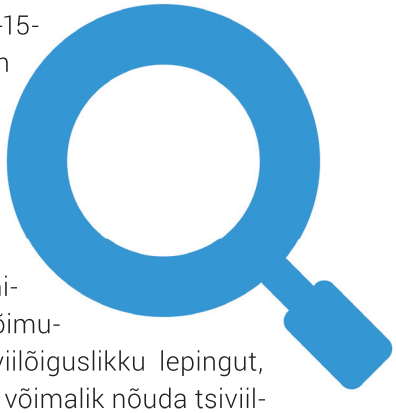
Kui küsitakse välja informatsiooni enda kohta, enda liikumiste kohta, ettevõtete ja asutuste töötajate kohta ja palju muu sarnase kohta, on küsitav, kas tegemist on avaliku teabega AvTS mõttes.

Kuna tegemist oli peamiselt selliste olukordadega, kus vang oli esitanud teabenõude mõnele ametiasutusele ning ei olnud sealt ette nähtud tähtaja jooksul vastust saanud, siis tuli inspektsioonil hakata juhtumit uurima. Sageli ilmnes, et kinnipeetavatele on juba vastatud, kuid vastus on tulnud peale teabenõudele vastamiseks ette nähtud aega, milleks on viis tööpäeva, sest kui tegemist ei ole juba valmis dokumendiga ja informatsiooni tuli koguda erinevatest dokumentidest, võtabki vastamine kauem aega. Selliseid ebakorrektsed vaided jäävad rahuldamata.

Vanglapood ja riigikohtu lahend

Teabenõudega küsisid kinnipeetavad informatsiooni ka vangla poe kaupade hindade kohta. Vanglapood on küll eraõiguslik juriidiline isik ega teabevaldaja avaliku teabe seaduse mõistes, kuid inspektsioonil tuleb teatud juhtudel välja selgitada, kas tegemist ettevõttega, mille kohta saab öelda monopol, mis muudab olukorda ja annab küsijale õiguse saada infot hindade kohta.

Riigikohus on aga oma lahendis 3-3-1-72-11 öelnud, et kaupade ostmine toimub eraõiguslikule regulatsioonile alluva müügilepingu alusele. Seega allub kauba müügihind tervikuna eraõiguslikule regulatsioonile. Riigikohtu praktikas (otsus asjas 3-4-1-15-07 ning 3-2-1-55-08) on rahalise kohustuse avalik-õiguslikuks tasuks lugemisel muu hulgas oluliseks peetud järgmisi kriteeriume: poolte vahel tekib tasu nõudmisel avalik-õiguslik (võimusuhe); ei sõlmita tsiviilõiguslikku lepingut, mille täitmist oleks riigil võimalik nõuda tsiviilkohtumenetluse korras; tasu maksjal puudub õigus nõuda teiselt lepingupoolelt vastusooritust; sellist tasu saab nõuda ainult riik; riik kasutab tasu kogumisel võimuvolitusi. Vangla kaupluses müüdava kauba eest nõutav hind loetletud kriteeriumitele ei vasta. Poolte vahel sõlmitakse võlaõigusseaduse regulatsioonile alluv müügileping. Oste sooritav kinnipeetav saab vangla kauplusele makstava tasu eest vastusoorituse – kauba. Analoogset tasu kauba müügiteenuse eest saab nõuda iga eraõiguslik isik. Seega on tegemist nõudega, mis tuleks lahendada maakohtus tsiviilmenetluse korras.



Vangla kaupluste puhul ei ole sellest tulenevalt tegemist valitsevas seisundis oleva ettevõttega. Monopoli näideteks on veevarustus ja elekter, kuid kindlasti mitte vangla kauplus.

Sooviti sekkumist kohtumenetlusse

Möödunud aastal sai inspektsioon ka selliseid kaebusi, mille lahendamiseks tal pädevust ei ole. Näiteks sooviti, et järelevalveasutusena teeks inspektsioon kohtule ettekirjutuse tunnistada kehtetuks kohtutoimikule juurdepääsu pannud kohtu määrus.

Samuti sooviti inspektsiooni sekkumist kohtumenetlusse, et keelata kohtu poolt antud korraldus võimaldada advokaatidel juurdepääs isikute e-postkastidele. Kuna Eestis mõistab kohut ainult kohus ning kellelgi pole õigust sekkuda kohtumenetlusse, siis ei saa ka inspektsioon sekkuda kohtumenetlusse ning kontrollida ega tühistada kohtu poolt tehtud otsuseid/määrusi.

Kui tavakodaniku puhul võib olla arusaadav sellise vaide esitamine, siis äärmiselt kahetsusväärne on olukord, kui sellise vaide esitab advokaat, kes peaks teadma, et järelevalveasutus ei saa sekkuda kohtumenetlusse.

Dokumendiregistrite pidamisest

2019. aastal juhtus mitmeid andmelekkeid, kus dokumendiregistrites said avalikuks juurdepääsupiiranguga dokumendid. Enamikel kordadel oli tegemist inimliku eksimusega. Sellistel eksimistel ei ole õigustust, sest selle taga on kogu riigi usaldusväärsus isikuandmete hoidmisel. Keegi ei kahtle selles, et kui riik avalikustab kodanike andmeid ilma õigusliku aluseta, on see äärmiselt kahetsusväärne. Selleks, et selliseid olukordi vältida, tuleb asutustel vaadata aeg-ajalt oma dokumendiregistreid avalikust (kodaniku) vaatest, millisel juhul on eksimused lihtsalt leitavad.

> Inspektsioonil on edaspidi kindlasti kavas jätkata asutuste dokumendiregistrite kontrollimist nii dokumentide nõuetekohase registreerimise kui avalikustamise osas.

Suur probleem on samuti dokumendiregistris dokumentide registreerimisega. Kuigi eelmisel aastal inspektsioon dokumendiregistrite seiret läbi ei viinud, siis pisteliste kontrollide käigus selgus, et jätkuvalt ei võimaldata ligipääsu e-kirjadele, millele ei ole kehtestatud juurdepääsupiirangut. Dokumendiregistri metaandmed on täidetud puudulikult ja seega pole tihti arusaadav, kas dokumendid on digitaalsed, piiranguga või millisel põhjusel ei võimaldata neile juurdepääsu. Samuti oli osadel asutustel puudujääke dokumendiregistris sellega, et ka asutustelt saadud kirju registreeriti eraisikute kirjadena ning kehtestati ebaseaduslikult juurdepääsupiirangu eraelu kaitseks. Inspektsioonil on edaspidi kindlasti kavas jätkata asutuste dokumendiregistrite kontrollimist nii dokumentide nõuetekohase registreerimise kui avalikustamise osas.

Inspektsioon saab infot dokumendiregistrite puudulikkuse kohta mitte ainult seirete või vaidemenetluste käigus. Inspektsiooni teavitavad puudustest ka asutuste endised töötajad, mis on viinud ka järelduseni, et Andmekaitse Inspektsiooni püütakse ära kasutada kättemaksu organina. Näiteks selliseid juhtumid, kus ametnik on kas koondamise või muul põhjuse teenistusest vabastatud ja esitab oma endise asutuse peale kaebuse dokumendiregistri puuduste kohta, paludes teha asutusele ettekirjutuse, aga hiljem menetluse käigus selgub, et kaebus on esitatud dokumentide osas kui kaebaja on ise on vastutav dokumentide nõuetekohase registreerimise eest.

Aasta tõi uue ülesande: Juurdepääsetavuse nõuete täitmise kontroll

Vastavalt 28.02.2019 jõustunud avaliku teabe seaduse rakendusaktile, milleks oli ministri määrus „Veebilehtede ja mobiilirakenduste ligipääsetavuse nõuded ja ligipääsetavust kirjeldava teabe avaldamise kord“ tuleb teabe valdajatel tagada juurdepääs teabele vastavalt rahvusvaheliste suuniste standardile WCAG (Web Content Accessibility Guidelines), mis on väljatöötatud veebidele ja mobiilirakendustele.

WCAG nõudeid võib kokkuvõtvalt kirjeldada kui tööriista arendajatele, disaineritele ja sisutoimetajatele ja seda kasutajasõbraliku ning enamlevinud ekraanidel töötavat veebilehe või mobiilrakenduse saamiseks lähtuvalt erivajadustest ning arvestades väiksemaid internetikiirusi.

WCAG 2.1 versiooni juurdepääsetavuse nõuetele hakkab inspektsioon järelevalvet teostama 2020. aastast.

ÕIGUSLOOME JA KOHTULAHENDID

Siinses peatükis anname mõningase ülevaate inspektsiooni antud seisukohtadest õigusaktide eelnõudele ning möödunud aastal lõppenud kohtuasjadest.

Õigusloome arengutest

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

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

Andmekaitseõiguse uuenemisest

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

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

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

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

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

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

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

Karistusseadustiku (KarS) muutmise eelnõu[10]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Miks on vajalik neid andmeid 10 aastat hoida?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

> Tuleb teostada ka kohane andmekaitsealaste mõjude hindamine.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

KOHTULAHENDID

Üheks järelevalveasutuse tegevuse tulemuslikkuse mõõdupuuks on tema tehtavate otsuste ja toimingute vastavus seadusandlusele. Inspektsiooni tegevuse kontrollimiseks on võimalik esitada inspektsioonile vaie, et asutus saab hinnata oma tegevust uuesti üle või esitada kaebus halduskohtusse. Viimast varianti on igal aastal kasutatud ning 2019. aastal jõudsid lõpuni mõned kohtuasjad, mis olid seotud varasemate inspektsiooni toimingute või haldusaktidega. Aastaraamatus anname lõpuni jõudnud kohtulahenditest põhjalikuma ülevaate.

Eraisik vs Sotsiaalkindlustusamet (3-18-544)

Selle vaidlusega seotud vaideotsus koostati veebruaris 2018 ning kohtuotsus jõudis lõpplahenduseni veebruaris 2019. Selles kohtuotsuses selgub, kas eraisikul on võimalik meediale mõeldud isikuandmete töötlemise ja avaldamise sätte alusel võimalik küsida teabevaldajalt isikuandmeid.

Sündmuste kronoloogiline järjestus

> Edaspidi toodud õigusaktide viidete puhul on arvestatud protsessi toimumise ajaga.

Eraisik esitas 23.12.2017 (täpsustatud 27.12.2017) Sotsiaalkindlustusametile (SKA) teabenõude, milles palus saata endale ühele riigireetmises süüdistatud isikule eripensioni maksmise lõpetamise dokument või selle puudumisel info edasimakstava eripensioni suuruse kohta. Eraisik leidis, et tal on kuni 14.01.2019 kehtinud isikuandmete kaitse seaduse (IKS) § 11 lõike 2 (sisu: isikuandmeid võib ilma andmesubjekti nõusolekuta ajakirjanduslikul eesmärgil töödelda ja avalikustada meedias, kui selleks on ülekaalukas avalik huvi ning see on kooskõlas ajakirjanduseetika põhimõtetega; andmete avalikustamine ei tohi ülemääraselt kahjustada andmesubjekti õigusi.) alusel õigus nõuda seda teavet SKA-lt.

SKA keeldus teabenõude rahuldamisest, mistõttu esitas eraisik vaide inspektsioonile. Inspektsioon leidis, et eraisikul puudus õigus saada seda teavet. Eraisiku soovitud andmed olid sotsiaalkaitse infosüsteemis, mille põhimääruse § 19 lõike 1 (tol hetkel kehtinud sõnastuse) kohaselt võimaldatakse andmekogu andmetele juurdepääs kooskõlas avaliku teabe seadusega ja isikuandmete kaitse seadusega. Sama paragrahvi lõige 2 ütles, et infosüsteemi kantavad andmed määratakse piiratud juurdepääsuga teabeks avaliku teabe seaduse (AvTS) § 35 lõike 1 punktide 11 ja 12 alusel. Inspektsioon oli seisukohal, et andmete saamiseks peab olema seadusest tulenev alus. Kui seadusest tulenevat alust andmete saamiseks ei ole, siis ei ole lubatud andmeid väljastada ei isikustatud kujul ega ka kujul, mis võimaldab isikut [kaudselt] tuvastada.

Eraisik leidis vaides, et kõnealused isikuandmed tuleks väljastada kuni 14.01.2019 kehtinud isikuandmete kaitse seaduse § 11 lõike 2 alusel. Vaides inspektsioon selgitas, et ajakirjanikel ega ka muudel isikutel ei ole õigust nõuda juurdepääsupiiranguga teavet selle sätte alusel. Nimetatud sätte alusel võib meedias andmeid avalikustada, kuid mitte teabevaldajalt nõuda (ajakirjanikel ei ole teabe saamisel suuremaid õigusi kui teistel). Kui meedia või muu isiku valduses on isikuandmeid sisaldav teave, tuli kuni 14.01.2019 kehtinud IKS § 11 lõike 2 järgi enne andmete avalikustamist hinnata, kas nende andmete vastu on ülekaaluks avalik huvi, kas avalikustamine on kooskõlas ajakirjanduseetika põhimõtetega ja kas selliste andmete avalikustamine võib kahjustada ülemääraselt isikute õigusi. Ehk see säte puudutas juba isiku valduses oleva teabe meedias avalikustamist.

Samuti leidis eraisik, et SKA oleks pidanud läbi viima kaalutluse avaliku ajakirjandusliku huvi ja andmesubjekti subjektiivsete õiguste vahel. Vaideotsuses selgitati, et kui küsitakse kolmandate isikute kohta käivaid juurdepääsupiiranguga isikuandmeid, siis peab teabevaldaja hindama üksnes seda, kas teabenõudjal on taotletavale teabele juurdepääsuõigus, ehk seadusest tulenev alus. Antud juhul SKA seda ka tegi ning leidis, et kuni 14.01.2019 kehtinud IKS § 11 lõige 2 ei ole pädev alus juurdepääsupiiranguga isikuandmete nõudmiseks. Samuti peab teabevaldaja enne andmete väljastamist hindama, kas teabenõudja poolt soovitud teavet on võimalik väljastada isikustamata kujul. Kui isik on tuvastatav ka siis, kui teabe väljastamisel tema isikuandmed kinni katta, on tegemist siiski isikuandmete töötlemisega, mis saab toimuda üksnes seaduse alusel või isiku nõusolekul. Antud juhul oleks isik ilmselgelt tuvastatav, kuna eraisik küsis informatsiooni konkreetse isiku kohta. Eraisik selle tulemusega ei nõustunud, mistõttu esitati kaebus halduskohtusse.

Tallinna Halduskohus

Kohus leidis oma otsuses, et eraisiku kaebus tuleb jätta rahuldamata. Kohus leidis, et soovitud teave on juurdepääsupiiranguline teave AvTS § 35 lg 1 punkti 12 alusel ning sotsiaalkaitse infosüsteemi põhimääruse § 19 lõike 2 (tol hetkel kehtinud) sõnastuse tõttu. Kohus leidis, et andmesubjekti eraelu puutumatust riivavad nii teave temale pensioni maksmise lõpetamise kohta kui ka teave temale makstava pensioni suuruse kohta.

Kohus selgitas, et kui isik taotleb juurdepääsupiiranguga isikuandmeid kolmandate isikute kohta, teatab ta teabevaldajale teabele juurdepääsu aluse ja eesmärgi. Eraisik taotles juurdepääsu soovitud teabele eesmärgiga kirjutada ajakirjanduslik artikkel ning avalikustada andmed meedias. Samuti põhjendas eraisik andmetele juurdepääsu soovi avalikkuse sooviga teada saada, kas kehtiv seadusandlus vajab eelarvevahendite kasutamise seisukohast muutmist.

Kohus leidis, et SKA on põhjendatult keeldunud teabe väljastamisest AvTS § 23 lg 1 p 1 alusel. Samuti leiti, et konkreetsel juhul ei olnud ühtegi õiguslikku alust selle teabe väljastamiseks.

Kohus ei nõustunud ka kaebuses toodud etteheitega, et SKA ei ole täitnud AvTS § 15 lõikest 2 tulenevat teabenõudja abistamise kohustust. SKA võttis eraisikuga ühendust teabenõude saamise järgselt, et välja selgitada juurdepääsu õiguslikku alust ja eesmärki. SKA teabenõude vastuses selgitatigi, et eraisiku näidatud eesmärgi ja alused ei viita seadusega pandud ülesande täitmisele või muule asjaolule, mistõttu oleks olnud võimalik soovitud teavet väljastada. Teabevaldaja kohustused teabenõudja abistamisel ei hõlma täiendavate eesmärkide sedastamist teabenõudja eest. SKA on lähtunud eraisiku poolt esile toodud juurdepääsu eesmärgist ja selle alusel õigesti leidnud, et taotletud andmete avaldamisest tuleb AvTS § 23 lg 1 p 1 alusel keelduda, kuna taotletava teabe suhtes kehtivad juurdepääsupiirangud ja teabenõudjal ei ole taotletavale teabele juurdepääsuõigust. SKA ei saanud eraisiku abistamisel määratleda sobivamat juurdepääsu alust, kui sellist juurdepääsu alust ei esine.

Kohus nõustus seisukohaga, et kuni 14.01.2019 kehtinud IKS § 11 lõige 2 ei ole õiguslik alus soovitud teabe saamiseks. Sätte sõnastusest nähtuvalt käsitab see paragrahv isikuandmete avalikustamist, mitte juurdepääsuõigust taotletavale teabele. See lõige viitab konkreetselt isikuandmete ajakirjanduslikul eesmärgil töötlemisele ja avalikustamisele.

> Selle kohtuotsuse järeldusi on võimalik üle kanda ja kasutada 15.01.2019 jõustunud IKS § 4 tõlgendamisel.

AS SmartCap teabevaldajana
(3-18-1741)

Sisuliselt oli kohtuasja küsimuseks, kas AvTS § 5 lg 2 mõistes olnud eraõiguslik teabevaldaja peab avaliku ülesande täitmisega seotud teavet väljastama ka siis, kui see avalik ülesanne on teabenõude esitamise ajaks lõppenud.

Vaidluse põhiküsimuseks on, kas AS-l SmartCap oli mingil ajahetkel avalik ülesanne, mis muutis teda avaliku teabe seaduse mõistes teabevaldajaks ning kas see on relevantne ka ajal, mil teabenõue esitati ehk siis, kui AS-l SmartCap seda avalikku ülesannet polnud.

Selle kohtuasja puhul tuleb anda lühike taustaülevaate ka AS-st SmartCap, et paremini välja tuua selle kohtuasja asjaolusid.

Eesti Arengufond (Arengufond) asutati 2006. aastal Eesti Arengufondi seaduse (EAFS) alusel eesmärgiga toetada Eesti majanduskasvu, mh läbi investeerimistegevuse. Arengufond asutas 01.03.2011 tütarettevõtte AS-i SmartCap, kelle ülesandeks oli tegeleda riskikapitali investeeringutega. AS SmartCap valitses 2012. aastal moodustatud riigile kuuluvat lepingulist riskikapitalifondi Early Fund II, kelle nimel investeeriti Eesti innovaatilistesse varase faasi ettevõtetesse. Arengufond ja AS SmartCap 25.08.2016 välja konkursi, et leida erafondivalitseja riigi otseinvesteeringute portfellile.

Osalemiskutse kohaselt oli tulevase erafondivalitseja ülesandeks luua uus fond, hallata olemasolevaid investeeringuid ja teha jätkuinvesteeringuid. Valikumenetluses osutus edukaks Tera Ventures OÜ, kelle asutatud fondile anti 2017. aastal lepinguga üle otseinvesteeringute portfell ja jätkuinvesteeringuteks täiendava kapitali juhtimine. 29.06.2016 jõustus arenguseire seadus (ASeS), kus nähti ette Arengufondi tegevuse lõpetamine likvideerimise teel ja investeerimistegevuse üleandmine riigi loodud sihtasutusele. Majandus- ja Kommunikatsiooniministeeriumi (MKM), SA KredEx ja Arengufondi kolmepoolse lepinguga anti muu hulgas AS SmartCap aktsiad üle SA-le KredEx ja Early Fund II osakud riigile, kuigi need jäid SA KredEx kasutusse. AS-st SmartCap sai SA KredEx tütarettevõte, kes teeb investeeringuid erafondivalitseja juhitavatesse fondidesse, jätkates tegevust väikefondi valitsejana. Early Fund II ise on investoriks Tera Ventures OÜ asutatud usaldusfondis.

Sündmuste kronoloogiline järjestus

Teabenõudja esitas SA-le KredEx 16.05.2018 teabenõude, milles soovis saada koopiat dokumentidest, millega anti Arengufondile kuulunud investeerimisportfelli juhtimine üle Tera Ventures OÜ-le ja neid dokumente muutvatest dokumentidest. Samuti sooviti teavet selle kohta, kas ja kelle osas on SA KredEx või AS SmartCap andnud nõusoleku Early Fund II fondi investeerimiseks või kui nõusolek selle kohta puudub, siis tulnuks edastada otsus nõusolekust loobumise kohta. Osas, milles SA KredEx teavet ei valda, palus teabenõudja teabenõudele vastata SA KredEx omanduses oleval tütarettevõttel AS SmartCap.

SA KredEx ja AS SmartCap vastasid teabenõudele ühiselt 23.05.2018, leides, et esimene ei valda teabenõudes küsitud teavet ning teise näol pole tegemist teabevaldajaga avaliku teabe seaduse (AvTS) § 5 lg 2 mõistes. AS SmartCap leidis, et ei täida avalikke ülesandeid. Asjaolu, et AS SmartCap on SA KredEx tütarettevõte, ei laienda talle teabevaldaja kohustusi. Isegi kui AS SmartCap oleks teabevaldaja, ei saaks talle küsitud teavet – erafondivalitseja konkursiga seotud teavet – väljastada, kuna see ei puuduta avaliku ülesande täitmist. Isegi kui tegemist oleks avaliku ülesande täitmisega, on teave kaitstud ärisaladusega.

> Asjaolu, et AS SmartCap kuulub 100% riigile, ei tee teda teabevaldajaks.

Teabenõudja selle vastusega ei nõustunud ning esitas inspektsioonile vaide AS-i SmartCap esitatud teabenõude vastuse

peale. Inspektsioon leidis vaideotsuses, et AS SmartCap ei ole teabevaldaja, kuna talle ei ole pandud seaduse või haldusaktiga kohustusi, mille lõppvastustajaks oleks riik või avalik-õiguslik juriidiline isik. Isegi kui selline kohustus tulenes AS-le SmartCap EAFS-st, on tänaseks EAFS kehtivuse kaotanud ning avaliku ülesande täimine ei saa sealt enam tuleneda. Asjaolu, et AS SmartCap kuulub 100% riigile, ei tee teda teabevaldajaks. AS SmartCap ülesandeks on fondi valitsemine ja investeerimine riskikapitali fondidesse. Eraldi tuleb vaadata fondi valitsemise alast (juhtimisalast) tegevust ja investeerimist ettevõtlusesse, millega sooviti elavdada majandusalast tegevust. AS SmartCap on teabevaldaja teabe osas, mis puudutab, kuhu ja milliseid investeeringuid on riigile kuuluvast varast tehtud. Teabenõudja nõudis aga teavet konkursi kohta, mille eesmärgiks oli leida fond, millesse AS SmartCap saaks investeerida, ja selle fondi valitseja. See ülesanne ei ole avalik ülesanne, vaid ettevõtte äritegevus. Avalik teave ei ole see, millistel tingimustel investeeringud teostati, sh millistel tingimustel investeeriti varad Tera Ventures I Usaldusfondi.

Tallinna Halduskohus

Teabenõudja ei nõustunud vaideotsusega, mistõttu ta esitas kaebuse Tallinna Halduskohtusse. Halduskohtu 26.02.2019 otsusega rahuldati kaebus ning kohustati AS-i SmartCap täitma teabenõudja esitatud teabenõuet, arvestades võimalikke seadusest tulenevaid juurdepääsupiiranguid ning kohus tühistas inspektsiooni vaideotsuse. Halduskohus leidis, et AS-l SmartCap ei olnud teabenõude esitamise ajal seaduse või selle alusel vastu võetud õigusaktiga antud avaliku ülesande täitmist.

Avalik ülesanne saab tuleneda vaid kehtivast seadusest. Lisaks märkis halduskohus, et oluline on vaja tuvastada, kas AS SmartCap on kunagi täitnud avalikku ülesannet. AvTS § 5 lg 1 punktist 3 ja lõikest 2 tulevad olukorrad, millal eraõiguslik juriidiline isik on käsitletav teabevaldajana. AvTS ei nõua, et eraõiguslik isik säilitaks avaliku ülesande täitmisel tekkinud avalikku teavet. Samas, kui avalik teave on eraõiguslikul isikul olemas, st teave on tema valduses – AvTS § 4 lg 1 kohaselt tuleb teabevaldajal tagada juurdepääs tema valduses olevale avalikule teabele – on AvTS eesmärgiga kooskõlas, kui eraõiguslik isik lugeda selle teabe osas teabevaldajaks ka ajal, mil ta avalikku ülesannet enam ei täida. Teabe olemus avaliku ülesande lõppemisest ei muutu. Avalikkusele peab jääma ka võimalus vähemalt mingi aja pärast avaliku ülesande täitmise lõppemist kontrollida. Halduskohus leidis, et Arengufond oli avalik-õigusliku juriidilise isikuna avaliku ülesande täitja (ülesanded tulid EAFS-st) ning kui investeerimistegevuse elluviimiseks asutati tütarettevõte AS SmartCap, siis selle ettevõtte asutamine oli otseselt seotud EAFS-s sätestatud eesmärgi ja ülesannete täitmisega. Halduskohus leidis, et AS SmartCap täitis kuni 03.05.2017 avalikku ülesannet ehk kuni investeerimisvara üleandmiseni (ASeS § 8 lg 3).

> Avalikkusele peab jääma küll võimalus vähemalt mingi aja jooksul pärast avaliku ülesande täitmise lõppemist kontrollida avaliku ülesande täitmist, kuid inspektsioonile teadaolevalt ei ole seadusandluses selgelt paigas, kui kaua seda „järelkontrolli“ võimalust saaks/võiks avalikkus kasutada.

Tallinna Ringkonnakohus

AS SmartCap esitas apellatsioonikaebuse, kuid ka Tallinna Ringkonnakohus leidis, et puudub alus halduskohtu otsuse muutmiseks. Ringkonnakohus leidis, et kaebuse rahuldamine eeldab, et AS SmartCap täitis Arengufondi investeeringute valitsemisel avalikke ülesandeid või kasutas seda tehes avalikke vahendeid ning teabenõudes taotletud teave puudutab selle avaliku ülesande täitmist või avalike vahendite kasutamist. Kohus leidis, et AS SmartCap oli teabenõudja soovitud teabe osas teabevaldaja AvTS § 5 lg 3 punkti 2 alusel.

Tallinna Ringkonnakohtu põhjendustes on veel märgitud, et „AS SmartCap asutati Arengufondi poolt 01.03.2011 Arengufondile kuuluva tütarettevõttena. Riigikohus on leidnud, et avaliku ülesande täitmisega AvTS § 5 lg 2 ja lg 3 p 2 mõttes võib olla tegemist ka siis, kui eraõiguslik juriidiline isik ei täida avalikku ülesannet küll enda nimel, kuid avaliku võimu kandja on ta kaasanud haldusülesande vahetusse täitmisse, jättes talle seejuures ulatusliku otsustusõiguse (Riigikohtu otsus nr 3-3-1-19-14, p 13).

Asjas ei ole esitatud tõendeid, et AS SmartCap oleks tegutsenud erineval eesmärgil või erinevatest vahenditest kui Arengufond. Kaebaja on asjakohaselt viidanud AS SmartCap kodulehel avaldatud majandusaasta aruannetele, millest nähtuvalt oli AS SmartCap ainsaks majandustegevuseks Arengufondi investeeringute valitsemine ning Arengufondi nõustamine investeerimisküsimustes. Niisiis on õige ka kaebaja järeldus, et AS SmartCap on 100% Eesti Vabariigile kuuluv juriidiline isik, mille asutamise ja tegutsemise eesmärgiks oli Arengufondi investeeringute valitsemine ning Arengufondi nõustamine seoses investeeringute tegemisega, lähtudes Arengufondi avalik-õiguslikust ülesandest ja eesmärgist. Seega oli AS SmartCap poolt Arengufondi investeeringute valitsemine avaliku ülesande täitmine, mitte eraõiguslikku isiku poolt vabatahtlikult pakutav teenus.

Eelnevast tulenevalt ei ole oluline, kas riik paigutas raha AS SmartCap kaudu mh ka EAFS § 33 lg 41 kaudu või mitte, sest oluline on, et AS SmartCap kaudu investeeriti riigi raha avaliku ülesande täitmiseks. Ringkonnakohus nõustus halduskohtuga, et kuni investeerimisvara üleandmiseni 03.05.2017 täitis AS SmartCap avalikku ülesannet riigieelarvelistest vahenditest ning selle ajani olid tal ka ülesande täitmise osas AvTS-s sätestatud kohustused. „AS SmartCap apellatsioonkaebuses esitatud arutluskäik sellest, nagu oleks AS SmartCap avalik-õiguslikku ülesannet täitev tegevus lõppenud ASeS vastuvõtmise hetkest, on kunstlik ja otseses vastuolus ASeS § 8 lg-s 3 sätestatuga.“

Kokkuvõtlikult

AvTS-i alusel on võimalik avalikku teavet küsida teabenõude korras ainult teabevaldajalt. Eraõigusliku juriidilise isiku puhul sõltub teabevaldajaks oleks AvTS § 5 lg 2 mõistes ennekõike asjaolust, kas ta täidab avalikke ülesandeid või mitte. AvTS § 5 lg 2 mõistes teabevaldajaks olek ning seeläbi ka kohustus teabenõudele vastata ja avalikku teavet väljastada sõltub asjaolust, kas eraõiguslik juriidiline isik on tol hetkel käsitatav teabevaldajana ehk kas tal on olemas avalik ülesanne. Avalikkusele peab jääma küll võimalus vähemalt mingi aja jooksul pärast avaliku ülesande täitmise lõppemist kontrollida, kuid inspektsioonile teadaolevalt ei ole seadusandluses selgelt paigas, kui kaua seda „järelkontrolli“ võimalust saaks/võiks avalikkus kasutada. Selle kohtuotsuse valguses on ka neil eraõiguslikel juriidilistel isikutel, kes kunagi olid teabevaldajad AvTS-i mõistes, kohustus väljastada AvTS § 3 lõike 1 mõistes avalikku teavet, kui see teave on sellel teabevaldajal veel olemas. Sel juhul tuleb muidugi arvestada ka võimalike juurdepääsupiirangutega.

Kaebus AKI menetluse algatamata jätmise kohta ja sellega seotud vaideotsusele (3-19-579)

Selle kohtuasja sisuks on, et kuidas käsitleda andmesubjekti esitatud pöördumist inspektsioonile – kas tegemist võib olla selgitustaotlusega või kaebusega.

Sündmuste kronoloogiline järjekord

Eraisik esitas 16.01.2019 inspektsioonile allkirjastamata elektroonilise pöördumise, mille sisuks oli: „Palun abi. Minu isiklikke andmed on ebaseaduslikke korduvalt avaldatud.“ Sellele lisaks oli ta märkinud linke mitmete elektrooniliste meediaväljaannete uudistele ja artiklitele.

Kirja lõpus oli kaebaja nimi ja kontaktandmed. Inspektsioon leidis, et tegemist on selgitustaotlusega ning sellele vastati 17.01.2019 kui selgitustaotlusele. Selles selgitati, et me üldju-

hul eraõiguslikesse, sh meedias ja ühismeedias tekkivatesse, suhetesse (privaatsus vs sõnavabadus). Olukorras, kus isikul endal on võimalik oma õiguste kaitseks pöörduda otse andmete avalikustaja ja kohtu poole ning asi ei ole seotud suure hulga inimeste põhiõiguste rikkumisega (puudub avalik huvi), ei sekku inspektsioon sellesse korrakaitseseaduse § 4 lõikes 2 sätestatut silmas pidades. Lisaks selgitati, millal meedia tohib isikuandmeid avalikustada isikuandmete kaitse seaduse § 4 alusel ning kuidas inimene saab enda õigusi kaitsta maine kahjustamise korral tsiviilkohtus.

Eraisik ei olnud selle vastusega rahul, mistõttu ta esitas inspektsioonile vaide inspektsiooni edastatud vastuse kohta. Esitatud vaidedokumendi sisu sisaldas väljavõtteid seadustest ning arvamusi erinevate kuriteo kvalifikatsioonide ja kohtuotsuste kohta. Kuna tegemist oli segase taotlusega, anti eraisikule korduvalt võimalusi puuduste kõrvaldamiseks tähtaegasid – ennekõike, et ta selgitaks ja põhjendaks, kuidas vastus selgitustaotlusele tema õigusi rikub. Eraisik esitas oma seisukohad hilinenult ning selle saabumisele järgneval päeval koostati vaide tagastamise otsus. Selles otsuses selgitati, et tema pöördumist läbi vaadates ei olnud kohe alust sekkuda meedia tegevusse ning vaidemenetluse käigus ei olnud ta samuti esitanud tõendeid, et ta oleks oma õigusi kuidagi kaitsma asunud. Vaidemenetluse väliselt selgitati ka, et kui tema sooviks on saada täiendavaid selgitusi, siis tuleks esitada selgitustaotlus ning kui sooviks on järelevalvemenetluse algatamist, siis esitada allkirjastatud ja tõenditega varustatud kaebus. Lisaks selgitati, et enne kaebuse esitamist peaks kaebaja ka ise kontakteeruma isikuandmete töötlejaga, et enda õigusi kaitsta. Märkuseks tuleb lisada, et konkreetsel juhul eraisik ise enne inspektsioonile pöördumise esitamist meediaväljaannetega kontakti ei olnud võtnud.

Tallinna Halduskohus

Eraisik AKI vastusega ei nõustunud, mistõttu esitas ta kaebuse Tallinna Halduskohtusse. Algselt halduskohus leidis, et inspektsiooni esitatud kaebus tuleb HKMS § 121 lg 1 punkti 1 alusel läbivaatamiseta tagastada. Halduskohus leidis, et eraisikul puudub kaebeõigus, sest selgitustaotluse vastus ning selle peale esitatud vaide tagastamine ei riku tema õigusi. Kohus leidis, et vaide tagastamine on menetlustoiming, mille peale ei saa esitada tühistamisnõuet. Kaebusest ei nähtu, et vaideotsus võiks rikkuda kaebaja õigusi sõltumata vaide esemest. Kaebusest saab järeldada, et eraisiku arvates pidanuks inspektsioon käsitama tema 16.01.2019 pöördumist kaebusena, mitte selgitustaotlusena, ning eraisiku eesmärk on kohustada vastustajat tema 16.01.2019 kaebust menetlema. Eraisikul puudub ilmselgelt kaebeõigus ka inspektsiooni kohustamiseks vastata 16.01.2019 pöördumisele tema soovitud viisil (st käsitada seda kaebusena). Kohus leidis, et eraisikul on jätkuvalt võimalus esitada inspektsioonile kaebus vastavalt esitatud juhistele.

Tallinna Ringkonnakohus

Eraisik AKI vastusega ei nõustunud, mistõttu ta esitas määruskaebuse halduskohtu tagastamise määruse peale. Tallinna Ringkonnakohus leidis 08.07.2019 otsuses, et eraisikul on kaebeõigus inspektsiooni tegevuse vaidlustamisel, kuna ka halduskohus möönis, et eraisiku

> Halduskohtu kohtuotsuse seisukohad tekitavad küsitavusi, kuna sellest lähtuvalt peaks pea igasugune inspektsiooni andmekaitse valdkonnas esitatud andmesubjekti pöördumine olema kaebus.

> Ringkonnakohtu hinnangul ei saanud AKI olukorras, kus [eraisiku] pöördumises oli palutud abi seoses tema isikuandmete ebaseadusliku avaldamisega ja viidatud hulgale isikuga seotud kriminaalasja kajastavatele veebiartiklitele, eeldada, et isik soovib saada AKI-lt üksnes selgitusi oma õiguste kaitse võimaluste

kohta, mitte ei ole esitanud taotlust meediaväljaannete tegevuse suhtes järelevalvemenetluse algatamiseks. Kui AKI-le jäi pöördumise eesmärk arusaamatuks, tulnuks paluda isikul seda täpsustada. Toimiku materjalide ja kohtute infosüsteemist nähtuvate andmete pinnalt saab küll järeldada, et [eraisik] ei ole seni iseseisvalt püüdnud oma õigusi kaitsta, kuid pelgalt asjaolu, et pöördumine ei vastanud sekkumistaotlusele esitatavatele sisu- ja vorminõuetele ning täidetud ei olnud AKI poolt välja töötatud sekkumise tingimused, ei anna alust käsitada 16.01.2019 pöördumist kaebuse / järelevalvetaotluse asemel selgitustaotlusena.“ Ringkonnakohus leidis, et andmesubjektil on õigus esitada kaebus nii isikuandmete kaitse üldmääruse (IKÜM) kui ka isikuandmete kaitse seaduse (IKS) alusel. Lisaks leidis ringkonnakohus, et kummaski õigusaktis ei ole sätestatud „järelevalveasutusele esitatava kaebuse vorminõudeid ega piiratud kaebuse esitamise õigust näiteks tingimusega, et andmesubjekt peab olema eelnevalt pöördunud sama nõudega otse tema isikuandmeid töötleva isiku poole, kuid see pole olnud tulemuslik.“ Ringkonnakohus leidis, et inspektsioon oleks pidanud eraisiku jaanuaris 2019 esitatud pöördumist käsitama IKS § 28 lg 1 / IKÜM art 77 lg 1 alusel esitatud kaebusena ning ka inspektsiooni vastust ei saanud käsitleda toiminguna (st selgitustaotlusele vastamine), vaid haldusaktina HMS § 43 lg 2 ls 1 tähenduses. Ringkonnakohus tühistas halduskohtu määruse osas, milles kaebus tagastati ning see saadeti halduskohtule ettevalmistava menetluse jätkamiseks.

sooviks oli, et inspektsioon alustaks tema pöördumise alusel järelevalvemenetlust meediaväljaannete suhtes. Ringkonnakohus leidis, et eraisiku vaidemenetluses esitatud selgituste pinnalt oleks inspektsioon pidanud lahendama tema jaanuaris 2019 esitatud pöördumist mitte selgitustaotlusena, vaid kaebusena. Seetõttu oli ka vaide tagastamine õigusvastane.

Tallinna Halduskohus

Tallinna Halduskohus võttis selle järel kohtuasja menetlusse ning 22.11.2019 otsusega rahuldas kaebuse. Otsusega tühistati inspektsiooni 17.01.2019 vastuskirjas sisalduv järelevalvemenetluse algatamisest ja järelevalvemenetluse raames ettekirjutuste tegemisest keeldumise otsus ning vaide tagastamise otsus. Inspektsioon pidi eraisiku kaebuse uuesti läbi vaatama. Halduskohus lähtus otsuse tegemisel eelnevalt välja toodud ringkonnakohtu seisukohtadest. Kohus leidis, et kui isikul on õigus IKS § 28 lg 1 alusel esitada kaebus inspektsioonile ning kus inspektsiooni pädevuses on ka samas valdkonnas riikliku ja haldusjärelevalve teostamine, saab avaldust, kus isik palub abi seoses tema õiguste rikkumisega, käsitada üksnes taotlusena teha kõik AKI pädevuses olevad toimingud, et selline rikkumine lõppeks. “Isik ei pea kaebuses ette kirjutama, milliseid konkreetseid järelevalvetoiminguid ta vajalikuks peab. Ta ei pea ka üksikasjalikult teadma, milliste meetmete võtmine on AKI võimuses. Seda kas üldse ja kui siis milliste järelevalvetoimingute tegemine kaebuses esile toodud asjaoludel vajalik on, peab AKI kaalutlusõiguse alusel ise otsustama ning kui ta leiab, et mistahes tema pädevuses olevate meetmete võtmine ei ole vajalik ega otstarbekas, tuleb seda nõuetekohaselt põhjendada.“ Halduskohus leidis, et eraisiku jaanuaris 2019 esitatud kirja eesmärk oli algusest peale esitada kaebus ning märkis: „Haldusorgan ei tohi rangelt juhinduda üksnes isiku esitatud avalduse pealkirjast või soovi sõnastusest. Eelnev ei tähenda seda, et AKI oleks tingimata pidanud tekkinud olukorras kaebaja avalduses nimetatud meediaväljaannete suhtes järelevalvemenetluse algatama või mingisuguseid konkreetseid järelevalvemeetmeid rakendama, küll aga oleks tulnud

seda kaaluda ning sellest keeldumist nõuetekohaselt põhjendada. Nagu ka ringkonnakohus 8. juuli 2019 määruses tõdes, ei võimalda IKS-i alusel läbiviimine keelduda pelgalt sellele argumendile tuginedes, et isikul oleks võimalik oma õiguste kaitseks esitada tsiviilõiguslikke nõudeid tema õigusi vahetult väidetavalt rikkuvate isikute vastu.

Halduskohtu arvates sai eraisik konkreetsel juhul esitada kaebuse IKS § 28 lõike 1 alusel.

Tegelikkuses tulenes konkreetsel juhul kaebuse esitamise õigus IKÜM art 77 lõikest 1, kuna IKS § 28 lõige 1 on ainult kohaldatav olukorras, kus isikuandmete töötlejaks on õiguskaitseasutus. Konkreetsel juhul esitati vaidlusalune kaebus meediaväljannete suhtes, millede tegevust ei reguleeri IKS-i 4. peatükk. Selle kohtuotsuse seisukohad tekitavad küsitavusi, kuna sellest lähtuvalt peaks pea igasugune inspektsiooni andmekaitse valdkonnas esitatud andmesubjekti pöördumine (milles on ilmingud võimalikule rikkumisele) olema kaebus. Samas võib konkreetsele pöördumisele kiirem ja konkreetsem lahendus tulla ka selgituste ning soovituste andmisega, mitte järelevalvemenetluse läbi viimisega.

Dokumendihaldussüsteemi logide väljastamine (3-19-743)

Selle kohtuasja põhiküsimus on, kas dokumendihaldussüsteemis Delta tekkivad dokumendi liikumise logid on avalik teave ja kas neid on võimalik teabenõude korras välja küsida. Samuti selgub, kas kriminaalmenetluses kaitsja tegevus teabevaldajalt avaliku teabe välja küsimusel on teabenõue, mida tuleb lahendada AvTS-i järgi või tegemist on erikorraga, millele inspektsiooni järelevalvepädevus ei kohaldu.

Sündmuste kronoloogiline järjekord

Eraisik esitas 07.09.2018 Politsei- ja Piirivalveametile (PPA) teabenõude, milles taotles seoses ühe tol hetkel aktiivse kriminaalasjaga mh ühe PPA dokumendihaldussüsteemis Delta asuva dokumendi liikumisega seotud logisid, millest nähtub dokumendi loomiseks korralduse andmine, delegeerimine, allkirjastamine jne, et seda kasutada tõendina kriminaalasjas. Veel sooviti nimekirja adressaatidest koos ametinimetustega ühe PPA e-posti aadressi listi osas.

Eraisik soovis PPA-lt dokumendihaldussüsteemis Delta asuva dokumendi liikumisega seotud logisid, millest nähtub dokumendi loomiseks korralduse andmine, delegeerimine, allkirjastamine.

PPA soovitud teavet ei väljastanud – keeldumise osas viidati kuni 14.01.2019 kehtinud isikuandmete kaitse seaduse § 19 lg 1 punktile 6, mille kohaselt peab isikuandmete töötleja teavitama andmesubjektile isikuandmete töötleja või tema esindaja nime ning isikuandmete töötleja aadressi ja muud kontaktandmed. E-posti listi adressaatide väljastamisest keelduti AvTS § 23 lg 2 punkti 3 alusel. Eraisik esitas PPA-le 22.01.2019 samasisulise teabenõude ning PPA keeldus 28.01.2019 selle teabe väljastamisest

PPA soovitud teavet ei väljastanud – keeldumise osas viidati kuni 14.01.2019 kehtinud isikuandmete kaitse seaduse § 19 lg 1 punktile 6.

põhjendusega, et varasemale samasisulisele teabenõudele on PPA juba vastanud.

Eraisik selle vastusega ei nõustunud, mistõttu esitas ta vaide inspektsioonile. 18.03.2019 vaideotsusega jäeti vaie rahuldamata. Vaideotsuses inspektsioon leidis, et tegemist oli

vaide esitaja kaitseõiguse realiseerimisega, mille raames kogub kaitsja täiendavaid tõendeid kriminaalmenetluse seadustiku (KrMS) § 297 tähenduses. Seega ei olnud antud juhul tegemist teabenõudega avaliku teabe seaduse (AvTS) mõistes, vaid täiendavate tõendite hankimisega KrMS-i sätete tähenduses. KrMS-i sätete osas inspektsioon järelevalvet ei teosta. Sellest hoolimata vastas PPA sellele pöördumisele kui teabenõudele. Vaidemenetluses oli PPA ka selgitanud, miks e-posti listi adressaatide nimekirja ei ole võimalik väljastada AvTS § 23 lg 2 punkti 3 alusel ning inspektsioon nõustus nende selgitustega, kui tegemist oleks AvTS-i kohase teabenõudega.

> Eraisik esitas vaide inspektsioonile. Vaideotsusega jäi vaie rahuldamata.

Tallinna Halduskohus

Eraisik AKI vaideotsusega ei nõustunud, mistõttu esitas ta kaebuse Tallinna Halduskohtusse. Halduskohus rahuldas eraisiku kaebuse ning tühistas inspektsiooni vaideotsuse ja kohustas PPA-d väljastama dokumendihaldussüsteemis Delta asuva dokumendi liikumisega seotud logid. Halduskohus leidis, et kõnealune dokument loodi avalikke ülesandeid täites ning tegemist oli avaliku teabega AvTS-i mõistes. Samuti leidis halduskohus, et teave, mida on võimalik saada dokumendi logidest, on samuti avalik teave.

> Tallinna Halduskohus leidis, et kõnealune dokument loodi avalikke ülesandeid täites ning tegemist oli avaliku teabega AvTS-i mõistes.

Halduskohus leidis, et tegemist oli teabenõudega AvTS-i mõistes. „AKI ei saanud teabe väljastamisest keeldumise õiguspärasuse osas seisukohta võtta, kuna ei teosta järelevalvet kriminaalmenetluse seadustiku nõuete täitmise üle. Halduskohus leidis, et PPA ei viidanud logide väljastamisest keeldumisel ühelegi õiguslikule alusele ning ei esitanud sellekohast põhistust. Seetõttu puudus PPA-l õiguslik alus keelduda logide väljastamisest ning samasugusele järeldusele oleks pidanud jõudma ka inspektsioon.

> Tallinna Halduskohus:
> “Dokumendi logide väljastamise nõude oleks kaebaja võinud esitada näiteks seoses sooviga, et välja selgitada, kes osalesid tema suhtes tõele mittevastava faktiväite – ta omastas PPA vara – esitamisel. Kui PPA oleks keeldunud logide väljastamisest, oleksid kõik muud asjaolud, va kaebaja eesmärk, olnud samad. Selles olukorras oleks AKI-l tulnud hinnata, kas tegemist on avaliku teabega ning kas PPA keeldus õiguspäraselt teabenõude täitmisest.“.

“AKI ei saanud teabe väljastamisest keeldumise õiguspärasuse osas seisukohta võtta, kuna ei teosta järelevalvet kriminaalmenetluse seadustiku nõuete täitmise üle,“ Tallinna Halduskohus.

Apellatsioonid Tallinna Ringkonnakohtusse

Nii inspektsioon kui PPA esitasid halduskohtuotsuse peale apellatsioonid Tallinna Ringkonnakohtusse. Inspektsioon esitas halduskohtule mh ka märkuse, et 15.03.2019 (kolm päeva enne vaideotsuse tegemist) jõustus AvTS § 46 lõige 2, mis ütleb: „Kui Andmekaitse Inspektsioon jätab vaide rahuldamata, siis on vaide esitajal õigus pöörduda teabevaldaja vastu halduskohtusse".

Seda seisukohta ei lisatud kohtuotsusesse ega põhjendatud, kas ning mil määral on see asjakohane konkreetses asjas, mida märkis ka inspektsioon esitatud apellatsioonikaebuses. Sel põhjusel ringkonnakohus leidis, et inspektsioon on kohtuasjas vastustajana valesti määratud ning muutis inspektsiooni kaasatud haldusorganiks. Ringkonnakohtu otsusega muudeti kehtetuks halduskohtu otsus osas, millega tühistati inspektsiooni vaideotsus ja menetluskulude jaotus.

Ringkonnakohtu otsuses leiti, et KrMS § 47 lg 1 punkti 1 ei saa pidada erinormiks AvTS § 2 lg 2 punkti 4 tähenduses, mis välistaks kriminaalmenetluses kaitsja esitatud dokumendinõude üle otsustamise AvTS-i normide alusel. „AvTS alusel tuleb seetõttu lahendada ka kaitsja esitatud teabenõudeid, kui teabevajadust põhjendatakse kriminaalmenetluse vajadusega. Teabevaldaja peab teabe väljastamist kaaludes võtma arvesse kaitsja erilist vajadust teavet saada ning teabenõude täitmisest keelduda saab vaid ülekaaluka avaliku huvi korral. Avaliku teabe seaduse kohaldamist kaitsja taotluse alusel teabe väljastamisele ei välista selle § 1 ja § 4 lg 1."

Ringkonnakohus leidis ka, et dokumendi liikumisega seotud logid on avalik teave AvTS § 3 lg 1 tähenduses, kuna need tekivad avalike ülesannete täitmise käigus. Ringkonnakohus siiski märkis, et inspektsioon oleks pidanud eraisiku esitatud teabenõuet AvTS-i alusel lahendama vaidemenetluse korras. Kohtumenetluses ei suutnud PPA piisavalt põhjendada, mis oleks sobiv juurdepääsupiirangu alus nende logide puhul. Ringkonnakohus sedastas, et kuna eraisik näitas, et teave on vajalik tema huvide kaitsmiseks, tuleks teabenõue täita ka juhul, kui PPA oleks logide andmed tunnistanud asutusesiseseks kasutamiseks mõeldud teabeks.

Kokkuvõtlikult saab öelda, et kui kriminaalmenetluses kaitsja küsib AvTS-i mõistes teabevaldajalt avalikku teavet, et saada kriminaalmenetluses tõendamiseseme seisukohalt tähtsust omavat teavet, siis sellekohased vaidlused on lahendatavad inspektsioonis vaidemenetluse raames. Lisaks peavad vaide esitajad arvestama sellega, et kui inspektsiooni vaideotsusega jäetakse vaie rahuldamata, siis on vaide esitajal õigus minna teabevaldaja vastu halduskohtusse. Sel juhul ei ole võimalik vaidlustada inspektsiooni vaideotsust, vaid on võimalik halduskohtus kohustamisnõude abil nõuda teabenõude täitmist

TEGEVUSED NUMBRITES

TEGEVUSNÄITAJAD	2016	2017	2018	**2019**
Juhendid (arvestamata seniste uuendamist)	1	2	1	**-**
Arvamused õigusaktide eelnõude kohta	27	34	42	**8**
Teavitustöö				
Selgitustaotlused, märgukirjad, nõudekirjad, teabenõuded	1417	1520	2384	**2343**
Kõned valveametniku infotelefonile	1419	1527	2556	**1578**
Nõustamised (ettevõtetele, asutustele)	79	148	200	**79**
Koolitused (korraldatud või lektorina osaletud)	23	17	23	**15**
Järelevalvetöö				
Ringkirjad (ilma järelevalvet algatamata)	5	4	8	**2**
sh ringkirjade adressaate	34	26	162	**110**
Suuremahulised võrdlevad seired	9	10	2	-
sh seiratute arv	148	129	85	**-**
Kaebused, vaided, väärteoteated (esitatud) IKS, AvTS, ESS alusel	390	462	462	**609**
Pöördumised IMI (EL infosüsteem, mille kaudu andmekaitseasutused vahetavad infot jt pöördumisi) kaudu	-	-	479	**1048**
Omaalgatuslikud järelevalveasjad (algatatud)	86	149	15	29
sh ennetavad andmekaitseauditid	24	1	1	**-**
Kohapealsed kontrollkäigud (järelevalves)	33	45	17	**-**
Soovitused ja ettepanekud (järelevalves)	56	125	10	**63**
Ettekirjutused (enamasti eelneb ettepanek; enamasti sisaldab sunniraha hoiatust)	59	64	46	**14**
sh registreerimise alal (eelneva ettepanekuta)	26	35	-	**-**
Väärteoasjad (lõpetatud)	16	9	23	**14**
Trahvid (väärteokaristus), sunniraha (järelevalves)	16	4	9	**5**
Loa - ja erimenetlused				
Registreerimistaotlused (delikaatsete andmete töötlemiseks või vastutava isiku määramiseks) – DIATR suleti 24.05.2018	547	641	192	**-**
Andmekogude kooskõlastustaotlused (asutamiseks, kasutusele võtmiseks, andmekoosseisu muutmiseks, lõpetamiseks)	139	99	36	**39**
Loataotlused teadusuuringuteks andmesubjektide nõusolekuta	18	54	61	**30**
Loataotlused isikuandmete välisriiki edastamiseks	18	22	3	1
Taotlused iseenda andmete suhtes Schengeni, Europoli jt piiriülestes andmekogudes	10	8	21	**31**
Inspektsiooni töötajate arv ja eelarve				
Koosseisulisi ametikohti	19	19	19	**19**
Aastaeelarve (tuhat eurot)	700	714	717	**750**

Andmekaitsespetsialistide register

Isikuandmete kaitse üldmäärus sisustas uue mõiste, milleks on andmekaitsespetsialist (ingl k *DPO ehk Data Protection Officer*).

Andmekaitsespetsialistide määramised asutustes ja ettevõtetes 31.12.2019 seisuga. Kui üks ja sama andmekaitsespetsialist teeb tööd mitmele asutusele, siis need asutused on loetud eraldi.

Juriidilise isiku õiguslik vorm	Määratud andmekaitsespetsialiste
Avalik-õiguslik juriidiline isik, põhiseaduslik institutsioon või nende asutus	22
Kohaliku omavalitsuse asutus	668
Täidesaatva riigivõimu asutus või riigi muu institutsioon	121
Mittetulundusühing	341
Sihtasutus	107
Tulundusühistu	7
Aktsiaselts	240
Euroopa äriühing (Societas Europea)	4
Füüsilisest isikust ettevõtja	50
Osaühing	2127
Tulundusühistu	28
Täisühing	5
Usaldusühing	8
Välismaa äriühingu filiaal	25
Korteriühistu	45
Kokku	3798

JÄÄ HAKKAS HOOGA LIIKUMA

Inspektsioon sai möödunud aasta jooksul ligi 2400 pöördumist, millest ca 1300 olid selgitustaotlused. Töömahult on see üsna tavaline aasta, kuid samas kujunes sellest murranguline aasta.

Inimeste teadlikkus enda õigustest oma isikuandmete haldamisel kasvas isegi mitme pügala jagu kümnepallisel skaalal. Polegi oluline, millise numbrini täpselt see ulatus, vaid tähtis on see, et jää hakkas liikuma. Mis selle alt välja hakkab paistma, seda näitab ehk juba aasta 2020.

Avalikkus ootas tõlgendamist ja selgitusi

Kui jää on hakanud liikuma, siis selle inerts tõukab käima ka teisi protsesse ja üks nendest on digiühiskonna polariseerumine.

Kui interneti masskasutuse ajastu esimestel aastatel ei pühendatud nii väga sellele, millistest kihtidest koosneb andmeside ja kuidas on rajatud võrgu arhitektuur, siis nüüd enam nii ei ole. Palju enam ollakse valmis sukelduma digiühiskonna nendesse soppidesse, mis pealiskaudsel vaatamisel silma ei paista. Ja nendes soppides elab oma elu ju tohutul hulgal isikuandmed.

Aastakümneid tagaplaanil olnud andmekaitsest on saanud nüüd ka Eestis üks peavooluteemadest, sest probleeme jagub, mille üle arutada. E-posti kirjade saatmise õigsusest kuni andmete mis iganes moel loata töötlemise teemadeni välja. Inimesed mõistavad üha enam, kui oluline on küsida, kellele ja missuguseid isikuandmeid jagada.

Mitmed olulised teemad, mis inspektsiooni lauale jõudsid, tulid ajakirjanikelt. Üks suurematest teemadest oli kaamerate kasutamise õigsus erinevates eluolukordades. Üks ajakirjanikest märkas kaamerat isegi sellises kohas, kus privaatsus võiks olla eeldatud rohkem kui 100%. Selleks kohaks oli kaubanduskeskuse tualeti sein suunaga pissuaaride ja kabiinide poole. Muidugi algatas inspektsioon menetluse, mille tulemusel tuli kaamera eemaldada.

Liiga palju andmeid tuleb anda?

Andmetöötlejate hulgas hakkas inimestele kahjuks liiga sageli silma n-ö teatud käitumismuster: andmeid kogutakse igaks juhuks või igaks juhuks natuke rohkem. Mine tea, kuna vaja läheb. Selline käitumine ei ole kindlasti tehisintellekti ajastus vastutustundlik, sest arvestades, et tehisintellektil pole huviks ainult tundma õppida inimest üldiselt, vaid tema huvi on selgitada välja igaühe ainulaadsus, siis igaks juhuks kogumine võib panna inimese ebasoodsasse olukorda. Näiteks ei oleks vaja e-poe pidajal küsida oma kliendilt kodust aadressi, kui pakk toimetatakse pakiautomaati.

Kuid alati ei pruugi inimesele kui andmesubjektile andmete kogumise põhjus välja paista, sest teatud juhtudel tuleb küsijal lähtuda seadusest, kust tuleb andmete küsimise kohustus.

Inspektsioonilt küsiti selgitust, miks peavad pangad saama oma klientidelt isikuandmete uuendamisel sellist teavet, mida inimene isegi ei tea. Klient on valmis jagama infot selle kohta, mis on talle hetkel teada, aga ennustamine on tänamatu ja enamasti ei kanna vilja. Näiteks ajas inimesi ajas kurjaks see, et kas tõepoolest on võimalik pangal küsida, kas tulevikus võib tulla raha pärandusest?

Kuna panganduse valdkonda reguleerivad nii krediidiasutuste seadus kui kümned teised õigusaktid kuni rahapesu ja terrorismi rahastamise tõkestamise seaduseni välja, siis pankade tegevus info kogumisel ei saa lähtuda panga suvast, vaid ettepandud seadustest. Samas saab pank kliendiandmete uuendamise protsessis oma tegevust läbi mõelda selliselt, et inimene saaks vastamata jätta nendele küsimustele, millele vastust ta ei saagi teada. Inimene peaks saama täita ainult need infoväljad, mille osas on ta kindel.

Andmekaitse ja autorikaitse

Üks mõnevõrra keerulisem teema oli inspektsiooni jaoks juhtum, kus raamatukaanel kasutati töödeldud kujul isiku fotot, ilma et inimene oleks seda teadnud. Inimesele on antud küll õigus oma isikuandmete kasutamist kontrollida, kuid kontroll ei tohi riivata teiste õigusi või vajadusi.

Kui raamatukaanele minevat algupärast isiku porteed töödeldakse joonistuseks, lisandub isikuandmete kaitsele ka autoriõigus, sest foto põhjal tehtud joonistus kuulub autorikaitse alla. Kuhu maani on inimesel kui andmesubjektil õigus oma isikuandmetele, ei ole üheselt vastatav. Sõltuvalt sellest, kui palju on sellel fotol säilinud algupära, tuleneb ka võimalik riive, mille olemasolu peab inimene ise tõendama.

Andmekaitse valdkond ei saa kunagi olla lihtsam või igavam kui elu ise, sest see on ühiskonnas seotud kõikide teemadega. Kehtivad küll ühtsed andmekaitsereeglid, aga olukorrad on eraldi käsitletavad, sest palju sõltub detailidest. Erinevaks kujunevad lahendused ka sel põhjusel, et ühesuguses olukorras tunnetavad inimesed riivet oma privaatsusele erinevalt, sest mis parata, inimeste vajadused, harjumused ja väärtushinnangud ongi ju isesugused.

Infoliini helistati enam kui 1500 korda

Vahemikus 1.01–31.12. 2019 helistati inspektsiooni infoliinile 1578 korda.

Võrreldes 2018. aastaga on kõnede arv mõningal määral vähenenud, sest tolle aasta kohta registreeriti 2556 kõnet.

Kõige sagedamini küsiti isikuandmete kaitse regulatsiooni kohta – kokku helistati 1257. korral. Avaliku teabe seaduse kohaldamise kohta küsiti 156 korda, elektroonilise side seaduse ehk elektroonilise otseturustuse kohta 41 korda.

Muudel teemadel, mida ei olnud võimalik liigitada inspektsiooni järelevalvealasse, oli kokku 124 kõnet. Nimetatud number on aasta-aastalt kasvanud, kuna tihti arvatakse, et inspektsioon saab anda nõu ka näiteks autorikaitse valdkonnas või oskab aidata telefoninumbrite leidmisel.

Enimkäsitletud teemad

Viimaste aastate kõige enam huvipakkuvaks teemadeks on olnud andmekaitse töösuhetes ja isikuandmete avalikustamine interne-

tis (sh veebilehtedel, meedias, sotsiaalmeedias). Seejärel võib suurema huvina välja tuua küsimused salvestusseadmete (kaamerate) kasutamise lubatavuse kohta.

Isikuandmete kaitse seadusega seotud küsimuste/probleemide hulgas olid kõige populaarsemad järgnevad valdkonnad:

1) Töösuhetega seotud küsimused – 171 kõnet. Enim küsiti töökohtadel kaamerate kasutamise kohta (kokku 32 kõnet) ning asjaolu osas, kas töölt lahkudes tuleb tööandjal sulgeda töötaja tööalane e-posti aadress.

2) Andmete avalikustamine – 158 kõnet. Pea kõikidel juhtudel oli mureks andmete (nime, isikukood, foto jms) avalikustamine internetis või meedias.

3) Salvestusseadmete kasutamine - 128 kõnet. Küsimused kaamerate kasutamise lubatavuse kohta avalikes kohtades ning eramajade küljes.

4) Korteriühistutega seonduvad kõned – 73 kõnet, neist 29 puudutas kaamerate kasutamist ühistu territooriumil.

5) Uuringute (sh teadusuuringute) läbiviimine – 33 kõnet. Seoses uue isikuandmete kaitse seaduse kehtima hakkamisega, muutus ka kord teadusuuringute läbiviimisel (loa taotlemise kohustuse osas)

6) Võlgnevused, kohtutäiturid ja inkasso – 42 kõnet. Võlgnevustega seonduvate probleemide puhul küsiti enim inkasso ja kohtutäiturite poolt võlaandmete avaldamise kohta (nt kas inkasso võib tööandjat teavitada võlgnevusest).

Avaliku teabe seadusega seonduvaid arupärimisi oli kokku 156, nendest juurdepääsupiirangute kohta küsiti 52-l korral, teabenõuete täitmise kohta 45-l korral.

Elektroonilise side seadusega seonduvaid kõnesid oli 38, kõik kõned puudutasid elektroonilise otseturustuse (nn spämmi) edastamist.

ANDMEKAITSE 10 SOOVITUST AASTAKS 2020

❒ Andmekaitsetingimused inimkeelde ja seda nii töötajate kui avalikkuse jaoks.
„Ära pillu presentaalseid tegevusi järgmise päeva riideriputi otsa“ pole ju nii arusaadav kui “ära lükka tänaseid toimetusi homsele“, aga saab veel lihtsamalt „tee täna ära“.

❒ Veendu, et andmetöötlusregister kajastab tegelikku andmetöötlust.
See on oluline ennekõike sellepärast, et ise üldse teaksid, millised isikuandmed infosüsteemidesse või andmete kogudesse kogunevad ja millisel eesmärgil neid töödeldakse. Nendele küsimustele vastamisest algab teadmine, mida tuleb kaitsta.

❒ Hinda kõrgelt pädevat andmekaitsespetsialisti (AKS), kes aitab andmekaitse kõikides küsimustes. Teda saad kaasata mistahes uuenduste juures juba arutelude algfaasi, et hiljem oleks kõikides toimingutes arvestatud lõimitud ja vaikimisi andmekaitsega.
Kuid see pole kõik, milles AKS - st on abi, v.t allpool.

❒ Uuenda turvameetmeid isikuandmete kaitseks või kui tead, et need on ajakohased, siis veendu, et need vastavad tänastele vajadustele.
IT spetsialisti teadmisi saab andmekaitseliselt täiendada pädev AKS.

❒ Ole valmis inimesele aru andma, kuidas tema isikuandmeid kasutad.
Selleks on Sul vaja andmetöötlusregistrit ja muidugi AKS-i teadmisi, milline peab olema andmekaitsereeglitega kooskõlas andmetöötlus.

❒ Uue tehnoloogia kasutuse võtu eel tee mõjuhinnang, et mängida läbi kõik ohud isikuandmetele. See peaks olema kirjalik.
Kindlasti on lihtsam mõjuhinnangut teha koos AKS-ga!

❒ Vaata, et veebis avaldatud isikuandmed on seal seaduspäraselt.
See on koht, kus AKS-i pädevus tuleb kindlasti kasuks.

❒ Koolita oma töötajaid andmekaitse küsimustes just selles valdkonnas hakkama saamisel, kus tegutsed.
Siin saab jällegi aidata AKS, kes omab pädevust või teab, kust leida parim koolitus arvestades spetsiifilisi küsimusi.

❒ Uuri, mida uut AKI on veebi lisanud, sest nii hoiad end viimaste uudistega kursis.
Ka uue infoga varustamisel saab alati AKS aidata.

❒ Kui toimub lubamatu juurdepääs isikuandmetele, teata sellest AKI-le. Rikkumisteate esitamise võib julgesti suunata pädevale AKSI - le, kes teab, kuidas ja kuna peab seda tegema.