

Aastaraamat

21 | 22



ANDMEKAITSE INSPEKTSIOON

Sisukord

01	Peadirektori eessõna Lk 2	15	Andmekaitse meedias Lk 30
02	Põhilised vead andmetöötluses Lk 6	16	Guugeldatavus Lk 32
03	Pilveteenuste seire Lk 8	17	Veebiküpsiste kasutamine Lk 34
04	Andmeladude seire Lk 10	18	Rämpspost Lk 36
05	Tervishoiu teenused Lk 12	19	Isikuandmete töötlemine erakondade tegevuses Lk 38
06	Terviseandmed kindlustuses Lk 14	20	Keskkonna teemade läbipaistvus Lk 42
07	Isikuandmed teadusuuringutes Lk 16	21	Avaliku teabe seaduse täitmisest Lk 46
08	Andmekaitse töösuhetes Lk 18	22	Õigusloome, kohtupraktika ja väärteomenetlused Lk 54
09	Kaamerate ja helisalvestiste kasutamine Lk 20	23	Euroopa Andmekaitse nõukogu olulisemad suunised aastal 2022 Lk 62
10	Kaamerad korteriühistutes Lk 24	24	Euroopa Andmekaitse nõukogu neli strateegilist sammu Lk 64
11	Biomeetrilised andmed ja näotuvastus Lk 26	25	Infoliin Lk 65
12	Maksehäirete avaldamise tähtaegadest Lk 27	26	Aasta tegevused statistikas Lk 66
13	Krediidiregister Lk 28	27	Lühiseletused Lk 68
14	Võlaandmete avaldamine sotsiaalmeediagrupis Lk 29		

Peadirektori eessõna

Hea lugeja!

Aitäh, et oled leidnud tee Andmekaitse Inspeksiooni aastaraamatuni.

Esimest korda ajaloos ilmub see topeltnumbrina. Tegelikult ei ole see midagi, mille üle uhkust tunda. Kahjuks näitab see, et eelmisel aastal ei olnud me oma ülesannete kõrgusel. Muidugi võiks ju öelda, et avaliku teabe seadusest ja isikuandmete kaitse üldmäärusest ei tulene meile sellist otsest kohustust. Meil on kohustus avaldada üksnes statistiline ülevaade oma tegevusest ja see sai loomulikult ka tehtud. Siiski on kujunenud traditsiooniks – mida ka meie lugejad väga ootavad – sisukas aastaraamat ühes artiklitega isikuandmete kaitse ja avaliku teabe valdkonnast.

Minu jaoks on ametis oldud aeg olnud mitmeti „huvitav.“ Esimesele aastaraamatule sain eessõna kirjutada siis, kui meid oli just tabanud koroonakriis. Järgmisel aastal ei olnud olukord parem. Nii olen varasematel kordadel ikka pidanud tõdema, et oli keeruline aasta. Tahaks, et sel korral saaks teisiti. Koroonakriis on ju enam-vähem möödas või vähemasti ei mõjuta see enam sedavõrd meie tööd. Tõsi, aasta tagasi algas Euroopas sõda ja ehkki otseselt ei saa öelda, et see oleks meie igapäevatöid oluliselt puudutanud, on ilmselt sel mõningane mõju meile olnud. Nimelt oli 2022. aasta meile kui organisatsioonile viimase aja kõige keerulisem. Nagu öeldud, mitte otseselt, aga kaudselt, sõja ja muude väliste mõjurite tõttu.

Ehkki tööjõu volavus on kimbutanud inspeksiooni isikuandmete kaitse üldmääruse jõustumata hakkamisest viis aastat tagasi, saavutasime 2022.

aastal sootuks uue taseme ja seda mitte heas mõttes. 2022. aastal vahetus meie suurepärasest inimestest lausa 40%. Kindlasti mõjutas seda ka sõja puhkemine – isegi kui keegi seda nii ei põhjenda, usun, et meie kõigi turvatunne sai sellega löögi. Paratamatult suunas see rohkem oma tuleviku kindlustamisele mõtlema.

Meie spetsialistid on tööturul olnud alati väga hinnatud. Andmekaitse teadmistega inimesed on kuldaväärt ja selle valdkonna praktilise kogemusega inimesed veelgi enam. Seetõttu on konkurents meie inimestele ääretult suur ja mis siin salata, riigiasutuseksena palgarallit kaasa teha on samuti väga keeruline. Ega inimestele miskit ette heita saagi – missioonitunne ja huvitav töö kahjuks suurenevaid elektri- ja küttearveid ei tasu. Nii me vaatasimegi eelmisel kevadel otsa olukorrale, kus inimesi, kes sedasama aastaraamatut sisuga täidaks ja kokku paneks, ei olnud. Tahan siinkohal tänada kõiki kolleege, kes jõudsid oma panuse enne edasi liikumist aastaraamatusse anda. Mõistagi mitte üksnes aastaraamatusse, vaid kogu valdkonda, ükskõik kui pikaks või lühikeseks see peatus meie juures jäi. Igasugune panus valdkonna arengusse on olnud ülioluline.

Aga et mitte minevikku kinni jääda ja otsida põhjendusi, miks midagi teha pole saanud, tuleb suunata pilk helgema tuleviku poole. Ma päriselt usun, et tulevik on täiesti teisest puust ja heledamates toonides.

Esiteks oleme eelmise aasta šokist üle saanud ja vanad võlad enam-vähem likvideerinud. Vabandan ka kõigi inimeste, ettevõtete ja asutuste ees, kes on pidanud oma pöördumistele kannatlikult meie vastust ootama.



Teiseks on meie toad taas rahvast täis. Isegi seda-võrd, et ruumi hakkab väheks jääma. Meie senised kohad on täidetud ja esimest korda üle väga pika aja meie koosseis ka suureneb. Muidugi oleme ikka veel teiste asutuste seas kääbuse rollis, ent protsentuaalselt on 21 ametikohalt 33-le laienemine ikkagi märkimisväärne. Tänu sellele oleme teotahet ja ootusärevust täis.

Loomulikult ei pea tundma hirmu, et nüüd hakkab trahvimasin täistuuridel tööle, mida on mingil põhjusel ikka 2018. aastast pikisilmi oodatud. Tõele auandes on kindlasti ka selles vallas elavnemist oodata, ent see ei ole olnud ega saa ka lähiajal olema eesmärk omaette.

Meie plaan on suunata oma tegevus rohkem ennetustöösse, nõustamisse, koolitamisse, teadlikkuse suurendamisse ja rahvusvahelisse koostöösse. Ehkki meie menetlusvaldkond ja sealhulgas järelevalve on endiselt kõige suurem, on koosseisu suurenemine võimaldanud luua struktuuri, mis rõhutab ja tõstab esile ka teiste valdkondade olulisust.

Usun, et ennetus viib paremini sihile kui järelevalve ja soovin siiralt selle nimel ka tööd teha. Loodan, et seda mõistab igaüks, et tõhus ja laiapõhjaline järelevalve on väga kallis – see on ajaliselt ja inimressursilt meeletult mahukas. Seda teab juba igaüks, et aeg, eriti inimeste aeg, on väga hinnaline.

Seega koolitamine, nõustamine ja teadlikkuse suurendamine on see, millega tuleb tööd teha. Teadlikkuse juures, eriti kui räägime üldsuse ja ühiskonna teadlikkusest, ei pea ma silmas teadlikkust sellest, kellele saab kaebuse esitada, kui naaber on valvekaamera üles pannud. Eelkõige mõtlen teadlikkust, miks üldse tuleb andmeid kaitsta ja riigi läbi paistvuse eest seista.

Mis on see õigushüve, mida me sellega kaitseme? Kuidas nende õigushüvede eest seismine või mitte seismine meie kõigi elu mõjutab? Seisame selle eest, et kõik inimesed oskaksid ja teaksid teenuseid ja kaupu tarbides jalgadega hääletada nende ettevõtete poolt, kes meie andmetest hoolivad, ja nende vastu, kellel on sellest ükskõik.

Siinkohal on oluline, et meie teadlikkus andmekaitsest ei piirduks vaid sellega, et las riigiamet tegeleb, vaid et me ise oskaksime oma küsimuste, nõudlikkuse ja lõpuks ka õiguskaitsevahenditega nõuda isikuandmete hoolikat kasutamist.

Toon esile ka meie rahvusvahelise koostöö. Ent see võib tekitada küsimuse: kas siis Eestis pole piisavalt tööd? Sellel on kaks põhjendust. Esiteks on Eesti ikkagi väga väike. Oodata, millal siin ühes või teises küsimuses praktikat ja selgust tekib, on suhteliselt ajamahukas. Samal ajal määravad suured Euroopa riigid trahve valdkondades ja teemades, kus meie võime lahendust oodata aastaid ja hakata taas jalgratast leiutama. Seepärast ongi oluline olla aktiivselt teiste liikmesriikidega ühises infoväljas.

Sama lugu on suuniste ja juhenditega. Kahjuks ei jõua me hoida tempot, et olulistest küsimustest uusi ja ajakohaseid suuniseid välja töötada. Samas panustame Euroopa Andmekaitsekoogu juhendi

loomisesse. Teiste riikide andmekaitseasutused on juhendmaterjalide tootmisel üsna aktiivsed ja kuna üleeuroopalist määrust peaks riigiti suuresti ühetaoliselt kohaldama, on need vähemalt üldpõhimõtete tasandil kasutatavad meilgi. Nii olemegi rahvusvahelises koostöös ja sealt saadava praktilise teadmise Eestisse integreerimises näinud suurt kasu ja sinna ka oma jõudu suunanud.

Teiseks aitab Euroopas toimuva, olgu need siis juhendid või hoopis teiste asutuste trahviotsused, meie inimesteni toomine ehk rohkem mõista ka valdkonna olulisust ja sedagi, miks on tähtis oma andmeid kaitsta.

Kasvõi seetõttu, et viimasel ajal palju kõlapinda saanud tehisintellekti areng peaks panema meid veelgi enam mõtlema sellele, et isegi kui me näeme tehnoloogia arengus suurt kasu, võib see kätkeada endas ka mõningaid ohte.

Tehisintellekti ja masinõppe kasutamine on muutunud laialdaselt levinuks paljudes valdkondades, nagu tervishoid, pangandus, turvalisus ja paljud teised. Kuigi tehisintellekt ja masinõppe võivad aidata meil lahendada keerukaid probleeme ja parandada meie elukvaliteeti, kaasnevad nendega ka tõsised ohud inimeste privaatsusele.

Üks suurimaid probleeme on see, et tehisintellekti algoritmid ja masinõppe mudelid võivad koguda ja töödelda suuri andmehulki, sealhulgas tundlikke isikuandmeid. Need andmed võivad sisaldada teavet meie tervisliku seisundi, perekondlike suhete, poliitiliste vaadete ja muu sellise kohta, mis peaks olema privaatne. Kui need andmed satuvad valedesse kättesse või neid kasutatakse valesti, võib see põhjustada suurt kahju meie privaatsusele ja isiklikule vabadusele.

Lisaks võivad tehisintellekti algoritmid ja masinõppe mudelid olla tundlikud eelarvamustele ja diskrimineerimisele. Kui andmed, mida kasutatakse tehisintellekti arendamisel, on ebatäpsed, moonutatud või diskrimineerivad, võib see viia ebaõiglase või ebaõiglase käitumiseni, mis võib kahjustada inimeste õigusi ja vabadusi.

Kokkuvõttes võib öelda, et tehisintellekti areng võib tuua kaasa palju positiivseid muutusi, kuid see võib ka ohustada inimeste privaatsust ja isiklikku vabadust. Seetõttu on väga oluline, et tehisintellekti arendamisel ja rakendamisel võetaks arvesse privaatsuse ja turvalisusega seotud riske ning tagataks andmekaitse põhimõtete ja privaatsusstandardite järgimine. Ainult siis saame tagada, et tehisintellekti kasutamine on kasulik ja vastutustundlik.

Nii räägib endast kurikuulus ChatGPT ise. Jah, viimased lõigud on ChatGPT koostatud. Muljetavaldav. Suhteliselt enesekriitiline, seega tuleks seda ehk tõsiselt võtta? Ja olgem ausad, ma oleks võinud ka terve eessõna koostamise tehisintellektile jätta ja seeläbi hoidnud hulga aega kokku. Kuid kas me selle lihtsuse ja kiiruse võlus tegelikult adume ka kaasnevaid riske ja seda, kui palju informatsiooni see meie kohta kogub? Ma ei pea silmas seda, et me sisestaksime sinna otseselt enda terviseandmeid või asutusesiseseks kasutamiseks mõeldud dokumente, aga ainuüksi seda, mida me tal kasvõi naljaviiluks teha palume.

Minu kohta ta näiteks juba teab, et ma huvitun viisil või teisel andmekaitsest, olen hiljuti käinud Itaalias, sest palusin tal teha reisikava punktist A punkti B ning ilmselt üht-teist veel, mida olen katsetuste käigus talle sisse söötud. Nii see panebki juba tükki tüki haaval kokku minu profiili, nagu LEGO. Kuid pole

kindel, kas igaüks, kes ChatGPT-d õhinal katsetama on asunud, seda ka adub. Veelgi enam, ma ei imestaks, kui inimesed sinna lausa arsti epikriise huvi pärast sisestavad.

Nii ongi riigil laiemalt ja sealhulgas meil suur roll suurendada inimeste teadlikkust kaasnevatest ohtudest. Mõistagi mitte hirmutades või kõike keelates, vaid mõistlikku tasakaalu leides ja hoides, aga samal ajal ka eeskuju näidates. Ärme unusta, et Eestis on üks suuremaid andmetöötlejaid riik ise. Samuti soovib riik endiselt olla e-riigina ja innovatsiooni vedajana eeskujuks teistele. Püüdkem siis olla siinjuures eeskujuks igas mõttes – läbimõeldud ja läbipaistval, samal ajal inimeste privaatsust austaval viisil. Vanasõnalt šnitti võttes: „Enne mõtle ja siis tegutse!“ Ja võtku mõni asi vahel või pisut kauem aega, kuid olgu kaasatud kõik vajalikud osapooled. Kui tarvis, pidada maha kasvõi ühiskondlik debatt, sest riigi ettevõtmised ja arendused inimeste andmetega olgu mitte õhinapõhised, vaid nii nagu üks teine vanasõna ütleb: „Üheksa korda mõõda, üks kord lõika!“

Tahan tänada kõik andmekaitse ja avaliku teabe valdkonna arengusse panustajaid – praeguseid ja varasemaid kolleege, koostööpartnereid Justiitsministeeriumist ja teistest ministeeriumitest ning asutustest, erasektorist ja kõiki, kes meie poole on pöördunud. Igaüks neist on aidanud astuda samuke edasi selgema andmekaitse ja läbipaistvama riigi poole.

Pille Lehis

Andmekaitse Inspeksiooni peadirektor

Põhilised vead andmetöötluses

Viimaste aastate statistikat silmas pidades on rikkumisteadete arv igal aastal kasvanud. Kui 2020. aastal sai Andmekaitse Inspeksioon 138 rikkumisteadet, siis juba 2021. aastal esitati neid 145 ja 2022. aastal 154. Tavapäraseks on saanud, et rikkumisteadet sisaldavad infot inimlikest eksimustest, lohakusest ja teadmatuses põhjustatud rikkumistest. Tunduvalt on kasvanud ka teavitamine küberrünnete tagajärjel toimunud rikkumistest.

2021.-2022. aastal Andmekaitse Inspeksioonile esitatud 299 rikkumisteadetest koguni 72 tegi avalik sektor. Olgugi et avaliku sektori rikkumisteadet moodustasid veerandi rikkumisteadete koguarvust, siis sellel perioodil oli Andmekaitse Inspeksiooni tähelepanu suunatud just neile. Avalik sektor

peab olema eeskujuks erasektorile, mistõttu viidi avaliku sektori osas läbi mitu põhjalikku menetlust.

Kõige kurioossem juhtum toimus Politsei- ja Pääriivalveametis, kus patrullpolitseinik salvestas oma telefoniga lõigu politseiauto pardakaamera videost ja jagas seda sotsiaalmeedias. Olgugi et patrullpolitseinik saatis selle vaid mõnele adressaadile, siis lõpuks levis see video igal pool ning selle kustutamine ei olnud võimalik. Siinkohal on sobilik öelda, et mis on internetis, see jääb internetti.

Alustatud järelevalvemenetlustest saab järelda, et üldiselt on avaliku ja erasektori rikkumised sarnased. Toome välja põhilised ja osalt ka fundamentaalsed vead, millest saavad rikkumised alguse.

1. Andmetöötajatel puudub ülevaade toimuvast andmetööstusest, andmete liikumine on kaardistamata ja mõnel juhul ka ebaseaduslik. Samal põhjusel on paljudel andmetöötajatel koostamata isikuandmete kaitse üldmäärusest kohustuslikud dokumendid (andmekaitsetingimused, lepingud volitatud töötajatega, õigustatud huvi analüüsid jne) või need on koostatud valesti. Keskseks teguriks on saanud see, et andmetöötajate arvates on stamp andmekaitsetingimuste avalikustamine veebilehel kooskõlas isikuandmete kaitse üldmäärusega. Tegelikult see nii ei ole. Andmekaitsetingimused koostatakse vastavalt enda andmetööstusele ja see eeldab andmetööstuse kaardistamist ning sellest aru saamist.

2. Andmetöötajatel puuduvad pädevad spetsialistid (andmekaitse- ja IT-spetsialistid). Kuna avaliku sektori puhul on andmekaitse spetsialisti määramine kohustuslik, siis enamasti määratakse seda rolli täitma isik, kes pole andmekaitsega varasemalt kokku puutunud. On juhtumeid, kus andmekaitse spetsialisti rollis on näiteks asutuse infoturbspetsialist, kellel on juba oma põhikohas ülesandeid küllaga. Seetõttu on näiteks küberrünnete tagajärjel andmekaitse kohustused sootuks unustatud ning pärast vabandatakse ja öeldakse, et kiire oli. Isikuandmete kaitse üldmäärus näeb ette selge kohustuse Andmekaitse Inspeksiooni rikkumistest teavitada ja selle mitte tegemisel on mujal Euroopas ettevõtteid trahvitud miljonitesse ulatuvate summadega. Erasektoris puudub andmetöötajal reeglina teadmine, et neil üldse selline kohustus – määrata andmekaitse spetsialist – eksisteerib. Kui teataksegi, ega siis naljalt ei soovita lisatöökohta luua ja määratakse samamoodi muid ülesandeid täitev isik andmekaitse spetsialistiks. Mõlema sektori puhul tehakse asju linnukese kirja saamiseks, aga see on vale.

3. Eelmises punktis välja toodud puudus põhjustab selle, et andmetöötleja infosüsteemid ei saa pidevat tähelepanu, sest ei ole inimest, kes neid hooldaks ja hindaks. Kui infosüsteemid on uuendamata, siis on häkkeritel eriti mugav isikuandmeid varastada. Andmetöötlejad peaksid oma infosüsteeme auditeerima pidevalt ning tegema pisemaid kontrole iga kvartal, et välistada nende vananemise tõttu esile kerkivate turvanõrkuste ärakasutamist.

4. Mitmes menetluses tuli nii avaliku kui erasektori praktikast välja asjaolu, et volitatud töötlejatega olid isikuandmete kaitse üldmäärusest tulenev leping sõlmimata. Mõningatel juhtudel oli see küll sõlmitud, kuid ei vastanud isikuandmete kaitse üldmääruse artikli 28 tingimustele.

5. Andmetöötlejad on vastutavate töötlejadena võtnud kasutusele mitu teenusepakkujat, kes on volitatud töötleja rollis. Andmekaitse Inspeksioon avastas mitmes menetluses, et isegi kui volitatud töötlejaga oli leping sõlmitud, siis vastutaval töötlejal ei olnud aimugi, kuidas volitatud töötleja andmeid tegelikult töötleb. Näiteks kasutas üks kohaliku omavalitsuse asutus eraettevõtte teenuseid kirjade saatmiseks. Menetluses selgus, et volitatud töötleja võimaldas kohaliku omavalitsuse asutusel kasutada spioonipikslit, millega kohaliku omavalitsuse asutus nägi igakordselt kirja adressaadi kirjade avamist. Andmekaitse Inspeksioon leidis, et selline andmetöötlus ei ole kooskõlas isikuandmete kaitse üldmäärusega ja tegi ettepaneku muuta andmetöötlus selliselt, et kirja avamist oleks võimalik näha vaid kirja esmakordsel avamisel. Samuti leidsime samas menetluses asjaolu, et kirjade saatmisel edastatakse isikuandmeid Ameerika Ühendriikidesse, millest tuleks õiguslike ja praktiliste sobivate kaitsemeetmete puudumisel hoiduda. Seega peaksid andmetöötlejad enne teenusepakkuja palkamist analüüsima, kas pakutav andmetöötlus on õiguspärane.

6. Paljudel juhtudel ei peeta Andmekaitse Inspeksiooni teavitamist rikkumistest vajalikuks või seda tehakse liiga hilja. On ülimalt oluline, et Andmekaitse Inspeksiooni teavitataks esimesel võimalusel ja hiljemalt 72 tunni jooksul rikkumisest teada saamisest. Andmekaitse Inspeksioon üritab seejärel kaasa mõelda võimalike lahenduste peale ja teeb ettepanekuid andmekaitse tugevdamiseks. Kui andmetöötleja asub asja lahendama õndsas üksinduses, siis võib hilisema teavituse korral kaasneda andmetöötlejale topelt töö ja on võimalik, et kogu andmetöötlust tuleb ümber mõelda. See aga tähendab andmetöötlejale lisakulutusi, mistõttu ongi Andmekaitse Inspeksiooni varajane kaasamine ülimalt oluline. Meie asutuse eesmärk on küll järelevalve teostamine, kuid see ei tähenda, et Andmekaitse Inspeksioon ainult karistab. Vastupidi, me eeldame, et andmetöötlejad saavad andmetöötlusega ise hakkama, aga vajadusel aitame, kus vaja.

Ülaltoodud põhivead ei ole ilmtingimata ainukesed, kuid nende vigade vältimisega läheks üldpilt tunduvalt paremaks ja tõenäoliselt kahaneks ka rikkumisteadete arv. Andmekaitse on Eestis jätkuvalt kasvufaasis ja arusaam õigetest andmekaitse põhimõtetest pole veel täielikult juurdunud.

Pilveteenuste seire

Möödunud aasta oli Euroopa Liidu andmekaitseasutuste ja Euroopa Andmekaitsekoostöökoostöö oluline – teoks sai Euroopa Andmekaitsekoostöökoostöö eestvedamisel läbiviidud esimene ühisjärelvalve, mis võttis luubi alla pilveteenuste kasutamise avalikus sektoris.

Eri tüüpi pilveteenused on saamas asutuste infosüsteemide osana ja andmetöötluse toetamisel uueks normaalsuseks. Asutused töötlevad juba praegu suures koguses isikuandmeid. Sageli on need väga tundliku iseloomuga. Uute tehnoloogiate kaasamisel andmetöötlusprotsessidesse peab jätkuvalt olema tagatud inimeste üks põhiõigus – õigus eraelu puutumatusele ja isikuandmete kaitsele. Suundumuses, kus roll õiguspärase andmetöötluse tagamisel liigub üha rohkem väliste teenuseosutajate kätte, on väga oluline saada enne aru võimalikest riskidest ja asjakohaste kaitsemeetmete vajalikkusest.

Kokku osales järelvalves 22 andmekaitseasutust üle Euroopa, nende hulgas Eesti Andmekaitse Inspeksioon. Inspekteeriti ligi sadat Euroopa Liidu ja riikide avaliku halduse institutsiooni, mis tegelevad tervishoiu, rahanduse, hariduse, transpordi ja infotehnoloogiaga. Uuringu alus oli liikmesriikide ühiselt koostatud küsimustik, mida sai vastavalt vajadusele ka kohandada. Eelkõige uurisid järelvalveasutused, millised on avaliku sektori asutuste peamised probleemid isikuandmete kaitse üldmääruse järgimisel pilvepõhiste teenuste kasutamisel.

Eestis olid seiresse kaasatud Transpordiamet, Eesti Haigekassa, Haridus- ja Teadusministeerium ning Tallinna Linnavalitsus. Inspeksiooni seire eesmärk oli eelkõige välja selgitada hetkeolukord edaspidiste soovitude andmiseks, mitte alustada sunnimeetmete rakendamise. Tähelepanu all olid avalikud pilveteenused. Olgu selle näideteks kas kontoritarkvara, e-post, virtuaalsuhtlus, infosüsteemide turvalisust tagavad teenused (nt pilvepõhised tulemüürid), töökorralduseks või koolitustegevuseks kasutatavad teenused, tagasiside kogumiseks kasutatavad teenused (nt küsitlusvormide loomine), analüütika-teenused (nt veebilehtede kasutusstatistika, asutuse tööks vajaliku andmeanalüüsi läbiviimise teenused).

Inspeksioonil on plaanis 2023. aasta esimesel poolel kohtuda kõigi seires osalenud Eesti asutustega. Tutvustame seire käigus välja tulnud nõrku kohti ja selgitame, miks konkreetsetest vajakajäämistest arusaamine on vastutustundliku ja õiguspärase andmetöötluse vaates olulised.

Euroopa avaliku sektori pilveteenuste ühisjärelvalve pikemat kokkuvõtet on võimalik lugeda Euroopa Andmekaitsekoostöökoostöö kodulehelt.

Üle Euroopa koorusid välja kindlad mustrid, milles asutuste teadlikkus pilveteenuste kasutuselevõtul vajab parendamist. Olulisemad seirejärgsed soovitused on:

1. enne pilveteenuse kasutamist viia läbi andmekaitseline mõjude hindamine;
2. kontrollida korraliselt, kas andmetöötlus vastab mõjuhinnangus toodule;
3. tagada, et asutuse ja pilveteenuse osutaja isikuandmete töötlemise rollid on selgelt ja ühemõtteliselt kindlaks määratud;
4. tagada, et pilveteenuse osutaja tegutseb volitatud töötlejana ainult asutuse nimel ja juhistel. Tuvastama olukorrad, mil pilveteenuse osutaja on iseseisev vastutav töötleja;
5. tagada, et pilveteenuse osutaja soovile kaasata uusi all-volitatud töötlejaid, on asutusel võimalik esitada vajadusel vastuväiteid;
6. tagada, et pilveteenuses toimuv andmetöötlus vastab asutuse eesmärkidele;
7. tagada, et pilveteenuse osutajaga lepingusse astumisel toimub asutuse andmekaitse spetsialisti õigeaegne kaasamine;
8. teha asutuste ülest koostööd pilveteenuse tingimuste läbirääkimisel;
9. tagada, et pilveteenuse hankemenetlus näeb ette vajalikud nõuded isikuandmete kaitse nõuete tagamiseks;
10. teha kindlaks, kas ja mis osas toimub pilveteenuse raames piiriülene andmeedastus ning kas kolmandatesse riikidesse edastamisel on rakendatud täiendavad kaitsemeetmed;
11. hinnata, kas pilveteenuse osutajale kehtivad mõne kolmanda (mittepiisava andmekaitse tasemega) riigi õigusaktid, mis võimaldavad sellel riigil küsida pilveteenuse osutajalt välja isikuandmeid, mida töödeldakse Euroopa Liidu andmekeskustes.

Andmeladude seire

2021. aasta suvest 2022. aasta kevadeni viis Andmekaitse Inspeksioon valitsussektoris läbi andmeladude ehk andmeaitade seire.¹

Seire eesmärk oli saada ülevaade valitsussektori andmeladudest, selgitada välja probleemid ja nende põhjused. Seire viidi läbi küsimustiku vormis, küsimustele vastas 20 asutust.

Vastustest tuvastas inspeksioon 28 andmelao tunnustega andmetöötluskeskkonda, millest enamik sisaldas kas osaliselt või täielikult isikustatud andmeid.

Andmeladude all peetakse silmas andmekogumit, mis koondab esmastest (primaarsetest) andmekogudest saadud andmeid kindlal eesmärgil. Üldjuhul on andmelao eesmärk andmete analüüs poliitikakujundamine või statistika koostamine. Info andmelaos võib olla kas isikustatud, pseudonüümitud või anonüümitud.

Andmeladude loomise eesmärgidena toodi välja, et andmekogude tehniline arhitektuur ja teenusdisain ei võimalda teha mahukatel päringutel põhinevaid analüüse, päringud võivad koormata ja häirida lähteinfosüsteemi toimimist. Samuti nimetati vajadust konsolideerida andmeid mitmest andmekogust. Markantsemate näidetena vastati, et andmeladu võimaldaks andmeid säilitada kauem kui primaarandmekogus endas või et andmekogu võimaldab tagada parema andmekvaliteedi kui primaarandmekogus.

¹ Andmekogude seire kokkuvõte (www.aki.ee/sites/default/files/seired/andmeladude_seire_kokkuvote.pdf)

² Seirest selgus, et andmeladudes kombineeritakse mitme andmekogu andmeid isikustatud kujul ja kasutatakse seda ka konkreetsete inimeste kohta detailandmete saamiseks, sh profileerimiseks. Selline tegevus peab olema seaduslik, st õigusaktiga ette nähtud. Tuleb veenduda, et selliseks andmetöötluks on seadusega pandud ülesanne, pädevusnorm (kellele ülesanne on pandud) ja menetlusnorm (mis näeb ette andmete sellisel viisil töötlemise).

³ Pseudonüümitud andmete lähteandmekogust uuendamiseks vajaliku sidumise saab teha andmete laadimisprotsessis. Depseudonüümimine peab olema rangelt ja selgelt õiguslikult reguleeritud. Kui andmeladu igapäevaseks operatiivtööks ei kasutata, siis ei ole isiku tuvastamist võimaldavaid andmeid vaja andmelattu kanda.

⁴ <https://eits.ria.ee/>

⁵ Lahendus võiks olla loogiline andmeladu, kuhu ei koondata andmeid kokku, vaid lahendatakse andmepäringute kihina (virtuaalne andmeladu).

Seire järeldused

- Andmeladu tuleb asutada seadusega ja sellel peab olema põhimäärus. Vaid ühe andmekogu andmetest koosnev andmekogu saab olla reguleeritud lähteandmekogu põhimääruses.
- Andmelao asutamisel tuleb selgelt esile tuua andmelao eesmärk. Selge peab olema see, mida tehakse lähteandmekogus ja mida andmelaos.
- Tuleb veenduda, et andmelaos toimuv andmetöötlus on seaduslik. Isikuandmete kaitse üldmääruse (IKÜM) artiklite 5 ja 6 kohaselt tohib isikuandmeid koguda ja töödelda üksnes selgelt kindlaks määratud eesmärgil. Edasine muul eesmärgil andmete töötlemine on lubatud vaid IKÜM artikkel 6 lõikes 4 sätestatud tingimustel.²
- Andmetöötlus andmelaos peab olema läbipaistev. Läbipaistvus on IKÜMi üks põhinõuetest, millele aitab esmajoones kaasa andmelao piisav reguleerimine seaduse ja seejärel põhimääruse tasemel.
- Andmevahetus andmelaoga peab toimuma infosüsteemide andmevahetuskihi (X-tee) kaudu. Eran-diks võiks olla andmevahetus andmekogu ja vaid selle andmekogu andmetest koosneva andmelao vahel. Seda eeldusel, et andmelao olemasolu on andmekogu põhimääruses selgelt välja toodud ja andmelao kaudu pole loodud andmete väljastamiseks mingeid X-teeväliseid võimalusi.
- Andmelaos peaks võimalusel kasutama anonüümitud või vähemalt pseudonüümitud andmeid.³
- Andmelao testimiseks tuleks kasutada sünteetilisi või hägustatud andmeid.
- Andmelaol võivad olla asutusevälised otsejuurdepääsud ja X-tee teenused vaid juhul, kui selle pidamisel järgitakse kõiki andmekogudele kehtivaid nõudeid. On nõuetekohaselt seadusega asutatud, andmeväljastus reguleeritud ja andmevahetuseks kasutatakse X-teeid.
- Andmekvaliteeti tuleb parandada lähteandmekogus, mitte üksnes andmelaos.
- Andmelaole kehtib e-ITSi⁴ (varasemalt ISKE) rakendamise, sh auditeerimise kohustus. Andmelaole peab olema määratud turvaklass, kusjuures ei saa näiteks konfidentsiaalsuse turvaklass olla madalam kui lähteandmekogus.
- Andmelao päringud tuleb kasutajapõhiselt logida.
- Andmeladu ei või minna vastuollu riigi infosüsteemi hajusa arhitektuuriga ega tuua kaasa riigile julgeolekuriski. Eesti riigi infosüsteemi arhitektuur on üles ehitatud hajusalt, see tähendab eraldi andmekogusid, mis suhtlevad omavahel turvalise kanali (X-tee) kaudu. Paljude seni eraldatud andmekogude andmestike ühte kokku koondamine viib selleni, et riigi infosüsteem ei ole enam piisavalt hajus, millega kaasneb suurem julgeolekurisk riigile.⁵

Tervishoiu teenused

Üks meie 2022. aasta eesmärk oli kindlasti teha teavitustööd tervishoiuteenust osutavates ja sellega kokku puutuvates asutustes – nii haiglates, perearstikeskustes, kindlustustes, koolides kui ka lasteaedades.

Oleme viimastel aastatel kirjutanud, kuidas tervishoiuteenuse osutajad kasutavad ära oma õigusi pääseda juurde tervise infosüsteemi ning kontrollivad sageli sõprade ja sugulaste – aga ka kaastöötajate – terviseandmeid. Hoolimata meie vastustest nii teenusepakkujatele kui ka pöördujatele – ning läbi viidud menetlustest – ei ole olukord muutunud.

Siiski on lootust, et see hakkab varsti paranema. Inimesed on järjest enam oma õigustest teadlikud ja jälgivad aktiivselt, kes ja millal nende kohta päringuid teeb. Lisaks on hakatud rohkem tähelepanu pöörama ka sellele, mis andmeid täpselt vaadatakse. Näiteks saab välja tuua pöördumise, kus isik käis üldises tervisekontrollis ja pärast seda patsiendiportaali kontrollides selgus, et perearst oli vaadanud ka tema tahteavaldusi, mis puudutas elundite loovutamist.

Võrreldes eelmise aastaga suurenes arstide ebaseaduslike päringute tegemise kohta tehtud kaebuste hulk pea kaks korda.

Ent vääртеomenetlusi inspeksioon nii palju teinud ei ole. Nimelt on paljud päringud olnud ka põhjendatud. Sageli on andmeid vaadanud hoopis haigla registratuuri töötaja või sekretär, kes on kontrollinud saatekirja või koostanud arvet. Sageli ei osata arvestada sellega, et lisaks arstile puututakse tervishoiuteenuse osutaja juures kokku paljude teiste töötajatega alates vastuvõtuteenindajast kuni õeni.

Samuti ei tea inimesed peaaegu kunagi, mis on kõigi töötajate nimed, kellega oli suhtlemine vajalik.

Sellest tulenevalt oleme suunanud inimesi rohkem ise toimunut uurima ja enda õiguste eest seisma. Sageli soovitame neil esmalt ise teha päring ja küsida andmete vaatamise kohta selgitusi haiglalt või konkreetselt töötajalt. Juhul kui kaebus on keerulisem, võtab inspeksioon selle ülesande enda kanda. Siiski on ka sellistes olukordades nii mõnelgi juhul inimesed kohe piisava selgituse saanud, kuna peale vastuse saamist ei ole pöörduja soovinud järelvalvemenetluse alustamist.

Ent siiski on peaaegu kõigi päringute tegemise põhjus isiklik huvi ja tervishoiuteenuse osutajal on olnud kaebajaga isiklik seos. Mõnel harval juhul on uurimise põhjus olnud inimlik – inimesel on mure lähedase pärast, ta tahab sõpra lohutada või olla kindel enda turvalisuses, kui puutub kokku raske terviseprobleemiga tuttavaga. Enamikes olukordades aga ei ole põhjused nii siirad. Väga tihti on tegemist sassis armusuhete, kättemaksu või lihtsalt uudishimuga. Nendes situatsioonides on inspeksioonil üsna keeruline asja menetleda, kuna tegemist võib olla väga emotsionaalse olukorraga.

Mõned päringud on tehtud ka ekslikult. Näiteks korraga paljude testide tulemusi kontrollides on töötajad vajutanud kogemata isiku nimele, kes ei ole nende patsient või ei kuulu nende nimistusse. Sarnane on olukord ka patsiente koroonaviiruse vastu vaktsineerima kutsumisega. Mitu perearsti on avanud nimekirja ja vaadanud järjest klientide andmeid, pööramata tähelepanu näiteks sellele, et mõned isikud ei kuulu enam nende nimistusse. Süsteemi pole uuendatud, nii et isikuid kuvatakse endiselt.

Keeruliseks teeb olukorra ka valitsuse korraldus, millega lubati tööandjatel küsida tõendeid, mis on seotud koroonaviiruse läbipõdemise, testi tulemuse või vaktsineerimisega. Siiani oli inspeksioon seisukohal, et terviseandmed ei kuulu mitte ühelgi alusel tööandjale avaldamisele, välja arvatud juhul, kui töötaja seda ise vabatahtlikult teeb. See on kaasa toonud juhtumite laine, kus juhuslikult tervishoiuteenust osutav tööandja on juba tervise infosüsteemist kontrollinud, mis on töötaja tervislik seisund. Siiski ei tohi tööandjad, kel on selline võimalus, seda ära kasutada. Tööandja saab nõuda tõendit vaid kindlate tingimuste täitmisel ja põhjendatud vajadusel.

Oleme seisukohal, et ekslikud rikkumised võib otstarbekuse kaalutlusel lõpetada ka hoiatusega. Siiski ei ole me saanud seda väga palju rakendada, kuna terviseandmed on tundlikud ja riivavad isiku privaatsust väga tugevasti. Seega ei saa me kuidagi anda sisendit, et mõnel juhul on ikkagi selliste päringute tegemine lubatud ja väärteomenetlust sellele ei järgne.

Seega viime sageli väärteomenetlused läbi ka väikeste rikkumiste puhul. Isegi kui trahv ei ole suur, tunneme, et oleme valesti käitunud isikutele vähemalt selgeks teinud, mida täpselt on valesti tehtud ja mis ei tohiks tulevikus kindlasti korduda. Isikud on siiani oma rikkumistest aru saanud ja selle vajaliku info ka oma tööandjateni viinud.

Ootame huviga, mida toob kaasa käesolev aasta ning kuidas kaebuste ja pöördumiste arv muutub, samuti kas meie aktiivsest teavitustööst on kasu.



Andmekaitse Inspeksioonil tuli ühe menetluse käigus välja, et kindlustusjuhtumi lahendamisel rikuti mitut isikuandmete kaitse üldmäärusest (IKÜM) tulenevat nõuet, mistõttu tegime kõikidele kindlustusseltsidele ringkirja, et selgitada, kuidas peaks kindlustusseltsi ja tervishoiuasutuse vahel kindlustusaluse isiku andmete edastamine toimuma.

Kindlustusandjal tuleneb kindlustusjuhtumi korral õigus isikuandmete töötlemiseks seadusest. Kindlustustegevuse seaduse § 218 lg 2 punkt 2 sätestab, et terviseandmete töötlemine on lubatud juhul, kui see on vajalik kindlustusandja kindlustuslepingu täitmise kohustuse ja selle ulatuse kindlaksmääramiseks ning tagasinõuete esitamiseks, kui kindlustusjuhtumiks on andmesubjekti surm või kui kindlustuslepingu täitmise kohustuse ja selle ulatuse kindlaksmääramine ning tagasinõuete esitamine eeldab andmete töötlemist andmesubjekti tervises seisundi või puude kohta. Täitmaks kindlustuslepingust tulenevaid kohustusi, on kindlustusseltsil õigus töödelda isiku terviseandmeid ning võimalus kaasata terviseandmete hindamiseks eksperte (nt oma usaldusarsti).

Tihtilugu kasutavadki kindlustusseltsid meditsiiniliste hinnangute andmiseks oma usaldusarste. Sel juhul on üldiselt tegemist volitatud

töötaja kasutamisega (v.a. kui usaldusarst ei ole kindlustusseltsi oma töötaja), kus on väga oluline, et oleks ka sõlmitud korrektne vastutava ja volitatud töötaja leping. Küll aga töötab sama usaldusarst väga tõenäoliselt arstina ka mõnes haiglas või kliinikus. Seega võib tekkida olukord, kus arst võib kindlustusseltsi tarbeks isiku andmeid töödelda, aga ei või sama isiku andmeid töödelda kui meditsiini asutuse töötaja. Meie kaasuse puhul sai arst väärtekorras karistada, sest tegi tervise infosüsteemi kliendi kohta päringuid, milleks tal ei olnud õiguslikku alust.

Kindlustusselts pani piltlikult arsti olukorda, kus ta palus küll töö tegemist, aga ei andnud töövahendeid. Seega kasutas arst kindlustusseltsile töö tegemiseks talle üksnes oma põhitööks antud infosüsteemide ligipääse õigusvastaselt (tegi haigla töötajana päringuid isiku kohta, kellega tal puudub ravisuhe, mis on seetõttu teo eest väärtekorras karistatav). Samuti võib seetõttu olla selline kindlustusotsus tsiviilkohtus vaidlustatav, kuna puudub kontroll, kas arst vaatas andmeid põhjendatud mahu (konkreetselt kindlustusjuhtumi tarbeks).

Selgitame, et kindlustusselts peab alati ise pöörduma oma kliendi terviseandmete küsimiseks vastava meditsiini asutuse poole. Sealjuures

on andmete väljastajal kohustus kontrollida, kas kõik küsitud andmed on põhjendatud ja vajalikud, et vajadusel mingis osas andmete väljastamisest keelduda. See on vajalik selleks, et ei küsitaks rohkem terviseandmeid, kui on tarvis konkreetse kindlustusjuhtumi lahendamiseks. Pärast seda saab kindlustusselts terviseandmete hindamiseks kasutada oma volitatud töötajat ja anda selleks volitatud töötaja kasutusse saadud kliendi terviseandmed. Teise variandina võib kindlustusseltsi usaldusarst kindlustusseltsi volitusel (nt volikirja alusel) pöörduda meditsiinasutuse poole andmete saamiseks. Ka sel juhul peab arst pöörduma meditsiinasutuse poole, mitte teostama päringuid ise. V.a kui ka haigla ei ole teda volitanud haigla eest kindlustusseltsile andmete väljastamise nõuet täitma.

Kaasuse käigus tõi kindlustusselts välja, et selliselt võib tekkida probleem, kus haigla väljastab vaid viimasest haigusjuhtumist andmed, aga jääb märkamata, et kliendil esines sama tervisekaebus juba enne kindlustusjuhtumit (tegemist on kroonilise haigusjuhuga). Mõõname, et selline probleem võib esineda, aga väga üksikute juhtumite puhul. Seega ei peaks see olema põhjuseks, miks anda kindlustusseltsidele laialdasem ligipääs kliendi kõigile tundlikele terviseandmetele. Samas võib

olla põhjendatud, et keerulistel juhtudel saab kindlustusselts nt kliendi perearstilt nõuda ka laialdasemat andmete vaatamist. See aga vajaks täpsemat analüüsi ja ka eelnevalt lisaregulatsiooni. Sel juhul piisaks meie hinnangul arsti kinnitusest, et kliendil ei ole samalaadseid, enne kindlustusjuhtumit, ilmnunud haigussümptomeid. Kuna see paneks perearstile lisakohustuse ja ka vastutuse (nt et ta ei avaks neid epikriise, mis kuidagi ei seostu kindlustusjuhtumiga).

Selleks, et muuta arstide tööd lihtsamaks, peaks alustuseks tegelema sellega, et nii tervise infosüsteemi päringute kui ka haiglate infosüsteemide kuvatavad metaandmed oleks üheselt selged (ei oleks vaja teha õige asja leidmiseks põhjendamatuid muid päringuid) ja et kõik infosüsteemid oleks alati ajakohastatud (tarkvarauuendused tehtud). Samuti on puudujääke arstide infosüsteemide kasutusoskustes ja mitmed vead on tekkinud kiirus-
tamisest kui ka teadmatusest.

Isikuandmed

teadusuuringutes

Andmekaitse Inspeksioon annab kooskõlastuse poliitikakujundamise uuringutele. Viimastel aastatel on uuringutaotluste arv jäänud 20 juurde.

Peamine murekoht, mis endiselt taotluste läbivaatamisel esineb, on seotud isikuandmete töötlemise läbipaistvuse tagamisega. Enamasti leiavad vastutavad töötlejad, et andmesubjekte ei ole vaja andmetöötlemisest teavitada, kuna andmete töötlemine ei kahjusta andmesubjekti huve, sest väljund on teaduslik üldistus või/ja teavitamine oleks ebamõistlikult kulukas.

Isikuandmete kaitse seaduse § 6 sätestab erisused teadusuuringutes isikuandmete töötlemisele, kuid uuringute läbiviimisel tuleb lähtuda ka isikuandmete kaitse üldmääruse põhimõtetest.

Üldmääruse üks oluline põhimõte on läbipaistvus. Isikuandmete vastutaval töötlejal on kohustus esitada läbipaistvalt teavet isikuandmete töötlemise kohta.

Üldmääruse artiklid 12–14 sätestavad, milline teave tuleb andmesubjektile esitada. Isikuandmete vastutav töötleja peab võtma aktiivseid meetmeid teabe esitamiseks andmesubjektile või suunama andmesubjekti aktiivselt selle asukohta.





Üldmääruse artikli 14 lõikes 5 on küll sätestatud teavitamata jätmise erandid, kuid ka teadusuuringute kontekstis saab nendele alustele tugineda vaid väga erandlikel juhtudel. Tavapäraselt hõlmatakse uuringusse väga suure hulga isikute andmeid ja seetõttu peetakse isikute teavitamist koormavaks. Kuid tänapäeval on andmetöötlustest teavitamiseks lihtsaid võimalusi, näiteks avaldada vastav teave vastutava töötaja kodulehel, teavitada meedia (sh sotsiaalmeedia) kaudu vms. Seega teavitamata jätmist ei saa põhjendada ebamõistlike kuludega.

Tihti esineb ka olukordi, kus ekslikult arvatakse, et kui inimese andmekooseisust on välja võetud nimi, kontaktandmed ja isikukood ehk eemaldatud on inimest otseselt tuvastada võivad andmed, on juba tegemist anonüümitud andmetega. Tuleb arvestada, et inimene võib olla kaudselt tuvastatav ka kindlate andmete koosmõjus ja sellisel juhul on tegemist pseudonüümitud isikuandmetega. Üldmääruse mõistes on pseudonüümitud isikuandmete puhul tegemist isikuandmetega ja tuleb järgida isikuandmete kaitse reegleid.

Andmekaitse töösuhetes

Ilmselt pole uudis, et töösuhetega seotud küsimused võtavad inspeksiooni töölaualt julgelt kolmandiku. Kuigi küsimused on aasta-aastalt jäänud suuresti samaks, paistab siiski suundumusi, mida soodustab tehnoloogia areng ja mõnevõrra ka tööandjate vähenenud teadlikkus.

Kõige rohkem pöördui inspeksiooni poole seoses videovalvega, samuti küsimustega, mis puudutasid töötaja andmetele ligipääsu ja e-posti sulgemist. Suuremat huvi tunti ka selle vastu, kas ja kuidas on lubatud töökohal heli salvestamine. Enamikul juhtudest käib heli salvestamisega kaasas videovalve küsimus ja vastupidi. Kuigi kaamerad ja videovalve on meie elus olnud juba kaua, siis paraku kipuvad tööandjad neid endiselt läbi mõtlemata paigaldama. Ei selgitata välja, millisel õiguslikul alusel see on võimalik ja millist dokumentatsiooni nõuab.

Miks ei piisa, kui töötaja kinnitab, et on kaameraga nõus?

Isikuandmete töötlemiseks peab olema mõni Euroopa isikuandmete kaitse üldmääruses välja toodud õiguslik alus. Töösuhete ajal töötaja isikuandmete töötlemine saab olla seaduslik, kui see on seotud lepinguliste kohustustega, tööandjale seadusest tulenevate kohustuste täitmisega või kui tegemist on tööandja või kolmanda isiku õigustatud huviga. Harva tuleb õigusliku alusena kõne alla ka töötaja nõusolek. Tööandja peab läbi viima põhjaliku ja dokumenteeritud õigustatud huvi analüüsi. Ekslikult arvavad paljud tööandjad, et kui töötajad on kaamerate kasutamisega nõus, ei pea õigustatud huvi analüüsi läbi viima. Pärast nii see ei ole.

Töötaja nõusolek saab aluseks olla vaid neil juhtudel, kui isikuandmete töötlemine ei ole vältimatu ja töötajal on tõepoolest võimalik vabalt otsustada, kas ta soovib anda nõusoleku. See tähendab, et nõusolekut peab olema võimalik alati tagasi võtta.

Eelmisel aastal oli inspeksioonil juhtum, kus lisaks sellele, et kaamerate kasutamisel toetuti vaid töötajate nõusolekule, soovis tööandja kaamerast tööruumis teha avalikku otseülekannet, leides, et see on vajalik töölepingu täitmiseks.

Lepingulise kohustuse täitmise alusele saab tugineda siiski üksnes juhul, kui kaamerat ongi vaja reaalselt ja otseselt töölepingu täitmiseks.

Nõusoleku puhul on tähtis meele pidada, et kui tööandjal on vaja oma eesmärkide täitmiseks andmeid töödelda, ei saa ta tugineda töötaja nõusolekule, kuna seaduse mõistes ei sõltu andmetöötlus sellisel juhul töötaja tahtest. Lisaks ei loeta nõusolekut töösuhetes üldjuhul vabatahtlikuks, sest töötaja ja tööandja asuvad ebavõrdses positsioonis. Lisaks tasuks mõelda sellele, et nõusolekut on võimalik alati tagasi võtta ja sellisel juhul ei tohi töötaja kaamera vaatevälja enam sattuda. Tööandjal tekib kohustus sulgeda kaamera igal hetkel, kui töötaja kaamera ette satub, mis on tegelikult võimatu.

Tööandja ja töötaja ebavõrdse positsiooni tõttu saavad töötajad anda vabatahtliku nõusoleku vaid erandjuhtudel. Kui nõusoleku andmisel või andmata jätmisel on mingeid kahjulikke tagajärgi või töötaja tunneb kasvõi survet nõustuda, siis ei ole tegemist vabatahtliku nõusolekuga.

Heli salvestamine töökohal on keelatud

Videovalve on ajaga muutunud juba nii harjumuspäraseks, et nüüd soovitakse lisada sellele uusi funktsioone, näiteks heli salvestamist.

Hääle järgi on võimalik aga inimest tuvastada ja hääled vestluses loetakse isikuandmeteks. Lisaks võivad vestlused omakorda sisaldada isikuandmeid ja eriliigilisi isikuandmeid. Kui kaamerate puhul saab läbi mõelda, kuhu ja kuidas need paigutada, siis audiovalve puhul on võimatu välistada, et vestlusesse ei satuks tundlikku teavet.

2021. aastal tegi inspeksioon ettekirjutuse Olerex AS-ile, kuna nende teenindusjaamades kasutati helisalvestamist. Inspeksioon kohustas Olerex AS-i eemaldama kõikidest teenindusjaamadest audiovalve. Muu hulgas asus inspeksioon seisukohale, et audiovalve ei taga turvalisust, see ei ole proportsionaalselt vajalik kliendivaidluste lahendamiseks ja teistel sarnastel eesmärkidel. Müües kaup ja pakkudes teenuseid tuleb arvestada vaidluste või ka solvangutega. Audiovalve ei ole kindlasti selliste olukordade lahendamiseks ainuke ja vältimatult vajalik vahend. Võimalik on küsida pealtnägijalt, uurida videosalvestisi ja kui vaja, saab pöörduda ka politseisse.

Juba 2010. aastal märkis Euroopa Andmekaitseinspektor, et helisalvestiste kasutamine töökohal on keelatud. Samuti kinnitatakse seda Euroopa Andmekaitsekoostöökoostöö suunistes, kus tuuakse esile, et jälgimisseadmed ei tohiks sisaldada funktsioone, mis ei ole vajalikud (sh helisalvestamine).



Kaamerate ja helisalvestiste kasutamine

2021. aastal oli väga palju keskmisi või suurettevõtted, kelle osas inspeksioon järelevalvemenetlusi läbi viis – näiteks A. Le Coq AS, Olerex AS, Bauhof Group AS, Selver AS, Coop Eesti Keskühistu, Olympic Entertainment Group AS, Bondora Group AS, Bolt Technology OÜ, OnOFF Jaekaubanduse OÜ, Smarten Logistics AS. Järelevalvemenetlused puudutasid nii ebaseaduslikke isikuandmete avalikustamisi võrgulehel, inimesele enda kohta käivate

isikuandmete väljastamata jätmist kui ka andmekaitsetingimuste, kaamerate ja helisalvestiste kasutamise õigusliku aluse kontrolli.

Oluliste ja korduvate probleemidena tõstaks esile nii nõuetele mittevastavad andmekaitsetingimused, kaamerate liiga lai kasutus töökohtadel ja ebapiisav õigustatud huvi analüüs või selle koostamata jätmine.

Andmekaitsetingimuste koostamine

1. Andmekaitsetingimused tuleb koostada vastavalt tegelikule andmetöötlusele. Tingimused ei saa piirduda näidetega, vaid loetelu peab olema lõplik (välja tuleb tuua muu hulgas kõik eesmärgid, õiguslikud alused, vastuvõtjad (või nende kategooriad), päritoluallikad). Sõnade „näiteks, eelkõige, muu hulgas“ kasutamine ei ole lubatud. Samuti ei ole lubatud tuua välja neid eesmäärke või õiguslikke aluseid, mida tegelikult ei kasutata. Kui andmetöötluse eesmärgid/alused muutuvad, siis tuleb andmekaitsetingimusi vastavalt sellele ajakohastada.

2. Andmekaitsetingimustes tuleb üldjuhul välja tuua isikuandmete säilitamise ajavahemik. Tihti viidatakse sellele, et isikuandmeid kasutatakse kuni eesmärkide täitmiseni, kuid see ei ole piisav. Enne tingimuste koostamist tuleb hinnata, milliseid isikuandmeid kui kaua säilitatakse (nt paljudel juhtudel on võimalik tugineda isikuandmete säilitamisele seadusele), samuti õigustatud huvile (eeldab eelnevat hinnangut – sh säilitamise tähtsaja vajaduse osas).

3. Kui klientide isikuandmete töötlemise õiguslikuks aluseks on õigustatud huvi, siis tuleb koostatud õigustatud huvi analüüs lisada kas andmekaitsetingimustesse või tuua tingimustes välja, et analüüsiga tutvumiseks saata e-kiri konkreetsele e-posti aadressile. Töötajatel peab aga olema võimalik õigustatud huvi analüüsiga tutvuda igal ajal (nt puhkeruumis või asutusesiseses infosüsteemis). Töötajatele suunatud andmekaitsetingimustesse tuleb lisada asukoht, kus on võimalik õigustatud huvi analüüsiga tutvuda.

Kaamerad töökohtadel

Võimalus jälgida töötajaid terve tööaja vältel toob kaasa väga suure riive. Töötajal ei ole võimalik teha ühtegi liigutust nii, et tema tegemisi ei oleks võimalik jälgida. See võib omakorda põhjustada töötajates stressi, ärevust ja muid vaimseid probleeme. Kaamerate kasutamine töökohtadel on võimalik, kui eelnevalt on koostatud korrektne õigustatud huvi analüüs ning kaamerate kasutamisel (suunamisel) tagatakse ka tegelikult see, et töötajad jääksid kaamera vaatevälja minimaalselt (töötajate jälgimine kaameratega terve tööaja vältel on keelatud). Näiteks ei ole lubatud suunata kaameraid otse töötajale poe kassas, kui töötaja veedab enamiku oma tööajast kassas. Kui eesmärk on näiteks poemüüja selja taga oleva alkoholileti valvamine või sularaha üleandmise/vasutuvõtmise kontroll, siis tuleb kaamera suunata otsest turvariskile (vältides seejuures töötaja pidevat jälgimist). Kui kaamerate kasutamine töötaja pideva jälgimiseta ei ole võimalik, siis on kaamerate kasutamine üldjuhul keelatud ning kaamerad tuleb eemaldada. Võimalus on kasutada ka muid meetmeid vara kaitseks, nt lukustatud alkoholikapp.

Helisalvestiste kasutamine kaupade ja teenuste pakkumistega tegelevates ettevõtetes

Inspektsioon nõustub, et on olukordi, kus helisalvestistest on kasu. Ent turvalisuse tagamiseks, kliendivaidluste lahendamiseks jms eesmärgil helisalvestiste kasutamise lubatavuse aktsepteerimine viib samasuguse olukorrani, kus oleme videokamerateaga. Sellest saaks uus reaalsus igal sammul.

Kuid videovalve pole olnud alati igapäevaelu normaalsus. Aja jooksul eksploateeritakse videovalvet üha enam, seejuures täienevad videovalve funktsionaalsused ning kvaliteet. Inimesed on aja jooksul leppinud paratamatusega, et videovalvet kasutatakse nii ulatuslikult. Asudes samadel eesmärkidel kasutama audiovalvet, samm-sammult algul mõnedes ettevõtetes, laieneb see valimatult igale poole. Kõik need asjaolud (ähvardamine, solvamine, nõutud küsimuste küsimine) eksisteerivad paljudes teeninduskohtades. Ka näiteks ööpäev läbi avatud olek pole niivõrd eriline asjaolu, et õigustaks audiovalvet. Niisiis ei pea Andmekaitse Inspektsioon audiovalvet olemuslikult lubatavaks kaupade ja teenuste pakkumisega tegelevates ettevõtetes. Audiovalve kasutamist saaksid õigustada üksnes väga erandlikud asjaolud, mida mujal ei eksisteeri.

Nagu öeldud, saaks olla helisalvestiste kasutamine lubatud üksnes juhul, kui seda õigustavad väga erandlikud asjaolud. Seetõttu soovitame ettevõtetel, kes ei ole helisalvestiste kasutamise õiguspärasuses kindlad (puuduvad erandlikud asjaolud), need viivitamata eemaldada. Olukorras, kus audiovalvet soovitakse kas jätkuvalt kasutada või uue lahendusena kasutusele võtta, kontakteeruda eelnevalt inspektsiooniga. Seda seetõttu, et vältida võimaliku olulise rikkumise toime panemist või rikkumise jätkamist.

Õigustatud huvi analüüsi koostamine

Selleks, et õigustatud huvile tugineda, peavad olema täidetud kõik kolm tingimust:



Õigustatud huvid, mille raames isikuandmeid töödeldakse, peavad olema piisavalt selged ja arusaadavad. Oluline on see, et välja toodud huvid ei ole spekulatiivsed, vaid tuginetakse tegelikule olukorrale (sh tuuakse välja ka faktilised asjaolud). Näiteks kaamerate kasutamise analüüsis ei piisa sellest, kui piirduakse sellega, et kaamerate kasutamine on vajalik isikute ja vara kaitseks ning tööõnnetuste ärahoidmiseks (tuvastamiseks). Analüüsis saab välja tuua näiteks selle, mitu vargust kuus/aastas toime pannakse. On pandud, millist vara kaitstakse (kui see ei ole ilmselge, nt toidupoe puhul), kui tihti ja milliseid tööõnnetusi on juhtunud, kui tihti ja millistel juhtudel on olnud vajalik kaamerasalvestisi kasutada isikute kaitseks.

Analüüsis välja toodud teave peab andma vastuse sellele, millistes ettevõtte või kolmanda isiku konkreetses hvides on tegelikult vajalik kaameraid kasutada.

Teiseks on oluline välja tuua kõik andmesubjektide (klientide, töötajate) huvid, mida võidakse isikuandmete töötlemisega kahjustada. Näiteks kaamerate kasutamine võib põhjustada töötajates stressi ja ärevust – töötajatel võib tekkida hirm midagi valesti teha. Mõned näited ka inimestelt.

Need on ainult mõned üksikud näited selle kohta, kuidas praktikas kaameraid kasutatakse ning mida töötajad sellistes olukordades tunnevad.

Näide 1. Tööle minnes kästi mul kirjutada seletuskiri selle kohta, miks olin tööajal telefonis ja sooritasin ostu internetipoes. Minu jaoks on häiriv see, tööandja suumib oma kaamerat nii, et telefonis tehtav on talle nähtav ja ta filmib seda.

Näide 2. Kaamerate abil dokumenti lisatud andmed:

- jalas kontsadeta jalanõud;
- registreeritakse klient. Peale registreerimist temaga keegi enam ei suhtle;
- klient lahkub, tool laokil, koht üle vaatamata 18 min;
- pausil 24 min, kliente 6;
- kassas tööl lahtise soenguga;
- suhtleb kliendiga käsi puusas;
- vestles kliendiga käed nn kinnises asendis;
- teenindaja ei tee müügiringi korrektselt. Mõnelt kliendil küsib joogisoovi, mõnest möödub ja vaatab eemalt.

Kui eelnevalt oleme tööandjale öelnud, et see pole okei, et meid niimoodi jälgitakse, siis ainuke vastus, mis sellepeale tuleb, on see, et neil on õigus.

Näide 3. Paigaldati kaamerad ega selgitatud, miks neid vaja on. Proovitakse läbi jälgimise töötunde loendada. Ma ei tunne end mugavalt, kui ma ei tea, kuidas ja kes mind jälgib ja mis aegadel seda tehakse. Olen maininud juhatuse liikmetele, et see ei ole okei. Selle peale sain vastuse, et minu arvamus ei loe.

Kolmandaks tuleb tasakaalustada ettevõtte ja/või kolmanda isiku õigustatud huve andmesubjektide (töötajate, klientide) huvidega. Siinjuures võrreldakse isikuandmete töötlemisest (kogumisest, kasutamisest, säilitamisest) andmesubjektile tekkida võivat mõju vastutava töötleja õigustatud huvidega ning hinnatakse, kas ja millises ulatuses vastutava töötleja ja/või kolmanda isiku õigustatud huvi kaalub andmesubjekti huvid üles.

Inspeksioon ei kahtle, et teatud juhtudel on vajalik reguleerida ja kontrollida töökojal nii telefoni kasutamist, riietust, soengut kui ka suhtlemisviisi. Siiski ei saa nõustuda sellega, et selliseid kontrolle peaks tegema kaamerate ja muid ning vähem riivavaid meetmeid eesmärkide täitmiseks ei ole – näiteks on vajadusel võimalik teha pistelisi kontrolle.

Nagu ka varasemalt märgitud, siis töötajate pidev kaamerate jälgimine ei ole lubatud!

Tingimusi, mis võivad tasakaalustamist (kaamerate kasutamise õiguspärasust) mõjutada, on mitu – sh kaamerate asukohad, omadused ja kasutamise eesmärgid. Lisaks on oluline kasutada ka täiendavaid kaitsemeetmeid ehk luua andmesubjektile soodsamaid lahendusi, kui näeb ette õigusakt. Näiteks võib selleks olla kiirem vastamise tähtaeg kui õigusaktis ettenähtu, lihtsam ja kiirem võimalus tutvuda enda kohta käivate andmetega ja logikirjetega, veel suurem läbipaistvus, lihtne vastuväite esitamise võimalus ja sellele kiire reageerimine.

Kaamerad korteriühistutes

Palju oli ka naabritevahelisi ja korteriühistute kaameravaidlusi. Kuna kaameraid paigaldatakse aina enam, on ka kaebuste arv suurenenud, mis omakorda suurendab inspeksiooni töömahtu. Kaameraid paigaldatakse nii KÜ kui ka korteriomanike endi poolt. KÜ-s peab valvekaamera olema paigaldatud KÜ üldkoosoleku otsuse alusel. On olnud olukordi, kus otsus puudub sootuks või kaamera on paigaldatud korteriomaniiku poolt suunaga avalikule teeale, ilma KÜ-ga konsulteerimata ja kooskõlastamata.

Riigikohus on leidnud lahendis 2-18-11279, et oma akna peale kaamerat korteris paigaldada ei tohi, sest andmesubjektile on andmetöötlus läbi paistmatu ehk ei ole teada, kellele kaamera kuulub. Näiteks kui korteriomaniik paigaldab oma kolmanda korruse akna peale kaamera, öeldes, et tal on küll kaamera silt, siis sellest siiski ei piisa, sest silt ei ole nähtav tänavale, kus inimesed kõnnivad. KÜ alal peab KÜ ise vastu võtma otsuse kaamera paigaldamiseks üldkoosoleku otsuse alusel. Iga korteriomaniik valvekaamerat paigaldada ei saa. Seetõttu on suurenenud inspeksiooni ettekirjutuste arv valvekaamera sildi loomiseks; ettekirjutused kaamerapiltide väljastamiseks, kustutamiseks, kaamera demonteerimiseks ja järelpärimistele vastamiseks. Spämmimenetlused ja -kõned on ikka aktuaalsed (e-kirjad, SMS-id, kõned). 2021. aastal oli palju elektroonilisi otseturustuse menet-

lusi, kus andmetöötleja saadab korduvalt e-kirju ilma õigusliku aluseta. Paljuski on tegemist tehnilise süsteemiveaga, kus ei ole süsteemis märgitud, et inimene ei soovi e-kirju. Andmetöötleja peab olema valmis andmesubjektile tõendama nõusoleku olemasolu. E-kirju võib füüsilisele isikule saata eelneval nõusolekul. E-kirjas peab olema loobumislink, mis samuti ei ole paljudes otseturustuskirjades olemas. Andmesubjektile peab olema lihtne ja kiire viis elektroonse kanali kaudu kirjadest loobuda.

Sama käib SMS-ide kohta, milles tihtipeale puuduvad viited, kuidas järgmisi kirju või sõnumeid keelata. E-kirjade ja SMS-ide saatmine muutub aina riivavamaks viisiks ja seda tunnetavad kõik, kes soovimatuid kirju või sõnumeid saavad. Samuti peab mainima, et mõned riigiasutused saadavad uudiskirju ja ülevaateid, millest peab samuti olema võimalik loobuda.

Kõnedes on jätkuv metsamüügi või ostu temaatika ja samuti metsa hindamise teenuse pakumine. Inspeksioon on pidanud tuvastama kõne tegija, sest kõne käigus helistaja ei ütle, millisest ettevõttest ta helistab ning kust ta on saanud telefoninumbri. Seetõttu tuleb algtada järelevalvemenetlus.



Kõnesid on ka vitamiinimüüjatelt ja teistelt kaupade pakkujatelt. Inspeksioon on seisukohal, et internetist ei tohi numbreid kokku rehitseda ja helistada neile eesmärgipäratult. Numbrile, mis on avaldatud eesmärgiga müüa näiteks kasutatud autot, ei tohiks helistada eesmärgiga müüa vitamiine või osta inimese kinnistut.

Statistikaameti osas oli menetlus, kus inimesele helistati korduvalt ja survestati teda küsitlusele vastama. Selline survestav käitumine ei ole õige, kui inimene on korduvalt ka keeldunud. Selles menetluses selgitati Statistikaametile, et korduvalt helistada ei tohi, kui isik on avaldanud soovi nii kirjalikult kui ka telefonitsi, et ta ei soovi küsitlusele vastata. Inspeksioon tegi Statistikaametile ettepaneku muuta helistamise korda nii, et korduvalt ei tohi helistada.

Biomeetrilised andmed ja näotuvastus

Videovalvekaamerad on muutunud ajaga palju paremaks, kasutades videoanalüütikat, olles seeläbi jälgimises väga tõhusad. Ent kaamerarohkes maailmas muutub inimesel üha keerulisemaks säilitada privaatsust.

Videovalve ei ole igas olukorras vaikimisi vajadus ja sellega tasub kaamerate ülespanekul mõtlema hakates alati arvestada. Paraku see siiski aeg-ajalt unustatakse. Nii on Andmekaitse Inspektsiooni üheks ülesandeks jälgida, et videovalve puhul võetaks hoolikalt arvesse isikuandmete kaitse üldmääruses (IKÜM) sätestatud üldpõhimõtteid (artikkel 5).

Tänu tehisintellekti arengule on meil praegu juba võimalik kaamerapildis inimesi ka kaugtuvastada. Nagu tehnoloogiliste uuenduste puhul sageli on, toob selline tuvastamine kaasa ühelt poolt võimaliku kasu, olgu selleks näiteks parem turvalisus või võimalus protsesse lihtsustada. Teiselt poolt tekitab biomeetriliste tehnoloogiate levik juurde ka palju küsimusi, kuulugu need siis isikuandmete kaitse, eraelu puutumatuse või võimaliku diskrimineerimise valdkonda.

Eri riikides lähenetakse tehniliste vahendite abil kogutavatele isikuandmetele erinevalt. Kui Euroopa Liit on biomeetriliste isikuandmete käsitleuses range, siis näiteks Hiinas kasutatakse näotuvastust kooliraamatukogus laenutuste jälgimiseks ja õpilase toitumisarunde koostamiseks. Sealne valitsus kasutab näotuvastust muu hulgas uiguuride liikumise jälgimiseks ja piiramiseks.

Näotuvastustehnoloogiat kasutatakse avalikes kohtades veel näiteks Kõrgõzstanis, Indias, Ladin-Ameerikas, Iisraelis, USA-s, Austraalias ja Venemaal. Venemaal kasutati koroonapandeemia ajal üle 100 000 näotuvastuskaamera, et jälgida karantiini pandud inimesi. Ameerika Ühendriikide

Föderaalne Kaubanduskomisjon on kooskõlas tarbijakaitsemissiooniga välja andnud mõned juhised, mille kohaselt ei tohiks ettevõtteid oma tarbijaid eksitada selles osas, kuidas nad kasutavad näotuvastussüsteeme. Ameerika Ühendriikides arutatakse ka näotuvastustehnoloogia kasutamise võimalike piirangute kehtestamise üle.

Euroopa Liidu isikuandmete kaitse üldmääruse järgi on biomeetrilised isikuandmed tehniliste vahendite abil saadavad andmed inimese füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad inimest kordumatult tuvastada. Levinumad biomeetriliste andmete kasutamise viisid on isiku tuvastamine näokujutise või sõrmejälje abil ning silmaiirise skaneerimine. Euroopa Liidus kuuluvad biomeetrilised andmed eriliigiliste isikuandmete hulka, see tähendab, et neid loetakse kõige enam privaatsust riivavateks. Eriliigilised isikuandmed puudutavad näiteks inimese terviseandmeid, seksuaalelu ja -sättumust, seetõttu võib hooletus nendega viia näiteks diskrimineerimiseni. Ka võib biomeetriliste andmete kogumine ja kasutamine kaugtuvastuseks kujutada endast riski inimeste põhiõigustele. Üldjuhul on IKÜM artikli 9 järgi on biomeetriliste isikuandmete töötlemine keelatud.

Ka Euroopa Nõukogu näotuvastuse teemalises juhendis on selgelt kirjas, et eraõiguslikele struktuuridele on keelatud kasutada näotuvastustehnoloogiaid kontrollimatutes keskkondades, näiteks kaubanduskeskustes, seda eelkõige turunduse või ebaturvalisuse eesmärgil.

Kuigi biomeetriliste andmete kogumine ja töötlemine, eriti aga näotuvastus, võib elu mõnes valdkonnas mugavamaks teha, on parem pidada meeles rusikareeglit, et tavaelus ja tavaolukordades ei ole see Euroopa Liidus lubatud.

Maksehäirete avaldamise tähtaegadest

Möödunud aasta menetluspraktikas on enim probleeme tekitanud segased võlanõuded, mille tekkimise aluseid maksehäireregistrite pidajad või võlausaldajad põhjendada ei suuda. Kuna maksehäire avaldamise puhul on tegemist isikuandmete avaldamisega, siis peavad just maksehäireregistri pidaja ja võlausaldaja suutma tõendada, et andmed võla kohta on õiged. Selleks peavad nii võlausaldajal kui ka maksehäireregistri pidajal olemas olema nõuet tõendavad dokumendid, sh dokumendid, millest nähtub nõude tekkimise alus (sh leping). Seega ei piisa nõude tõendamiseks ainult arve olemasolust.

Näiteks tarbijale telefonimüügi puhul on probleemiks osutunud see, et müüja ei suuda tõendada lepingu sõlmimist vastavalt VÕS § 542 lg-le 1, mille kohaselt on tarbija telefonikõne käigus võetud kohustustega seotud üksnes juhul, kui müüja on telefonitsi edastatut kinnitanud püsival andmekandjal ja tarbija on oma tahet kinnitanud kirjalikku taasesitamist võimaldavas vormis (nt e-kiri). Nimetatud nõuete rikkumisel loetakse müüja poolt tarbijale edastatud asi, teenus või muu sooritus tellimata asjaks, teenuseks või muuks soorituseks VÕS § 99 lg 1 tähenduses, mis sätestab, et ettevõtjal ei teki tarbija suhtes tellimata asja saatmise, teenuse osutamise või muu soorituse tegemise korral nõudeid ja seega ei ole tarbijal kohustust ka sellise asja eest maksta.

Samas on võlaandmete töötlemise tingimustes väärarusaamal tihti ka võlgnikud ise. Näiteks ei ole piisav alus esitada inspeksioonile kaebust võlaandmete maksehäireregistrist kustutamiseks, kui võlgnevus on äsja tasutud. Rõhutame, et isikuandmete kaitse seaduse kohaselt ei lõppe makse-

häire avaldamine võla tasumisega, vaid seda võib avaldada veel kuni viis aastat pärast võla tasumist. Tihti ollakse seisukohal, et selline viie aastane avaldamise aeg on „automaatne“, kuid see pole õige lähenemine. Maksehäirete avaldamisel tuleb järgida ka kõiki IKS § 10 lg-st 2 tulenevaid nõudeid, sh tuleb hinnata, mis hetkest alates pole nõude avaldamine enam proportsionaalne ja kas see ei kahjusta andmesubjekti ülemääraselt. Lisaks, kehtib aegunud nõuete puhul ka tingimus, et võlaandmeid võib maksimaalses ulatuses (viis aastat pärast aegumist) avaldada üksnes siis, kui võlausaldaja astus aegumistähtaaja jooksul aktiivseid samme võlgnevuse sissenõudmiseks.

Samuti on inspeksioon muutnud oma varasemat seisukohta seoses maksehäire avaldamise maksimaalse tähtajaga. Lähtekohaks võtame kaebuste lahendamisel tsiviilseadustiku üldosa seadusest (TsÜS) tuleneva üldise tehingulise aegumistähtaaja, milleks on kolm aastat. Kuna TsÜS ei eelda kohustuste rikkumise tahtlikkust, ei saa sellist juriidilist asjaolu eeldada ka inspeksioon, mis tähendab, et 10-aastase aegumistähtaaja kohaldumine peab olema tõendatud. Kui selle kohta tõendid puuduvad, võib järelikult maksehäiret avaldada üldise tehingulise aegumistähtaaja jooksul (kolm aastat), millele võib maksimaalselt lisanduda kuni viis aastat.

Rõhutame, et lepingu rikkumise fakti kui sellist, ei saa samastada rikkuja tahtlusega. Viimasele võivad viidata erinevad asjaolud, nt võlgniku käitumine (kas ta on hoidnud võlausaldajaga suhtlemisest kõrvale), võlgnevuste koguarv, -summa jms.

Andmekaitse Inspeksiooni uus maksehäirete juhend on saadaval ka asutuse koduleheküljel.

Krediidiregister

Möödunud aastal oli inspeksioonil võimalik avaldada arvamust nn positiivse krediidiregistri projekti kohta. Erinevalt juba tegutsevatest negatiivsetest krediidiregistritest (maksehäireregistrid) koondaks positiivne krediidiregister isikute kõik finantskohustused olenemata sellest, kas isikul esineb laenude tagasimaksmisel võlgnevusi või mitte. Registri eesmärk oleks seega isikute tege- likest võlakohustustest parema ülevaate andmine ja loodetavasti aitaks see kaasa vastutustundliku laenamise põhimõtte täitmisele.

Arvestades, et loodav register koosneks peamiselt isikute võlaandmetest, kaasneb selle välja- töötamisega mõistagi palju andmekaitsega seon- duvaid kitsaskohti, millele on AKI (Andmekaitse Inspeksioon) tähelepanu pööranud. Esiteks tuleb selgeks teha, milline saaks olema õiguslik alus isi- kute krediidiandmete pärimiseks registrit – kas selleks oleks IKÜM (Isikuandmete kaitse üldmää- rus) art 6 lg 1 p f kohane õigustatud huvi või loo- daks selleks sootuks uus siseriiklik norm. Makse- häireregistrite puhul näitab menetluspraktika, et paraku leiavad liiga paljud inimesed end omavat õigustatud huvi teise isiku võlaandmetega tutvumiseks. Kui lisaks puudub registripidajal andmete pärijate üle piisav kontroll, võibki tulemuseks olla andmete lubamatu väljastamine.

Lisaks on inspeksioon soovitanud positiivse krediidiregistri puhul mõelda läbi see, kuidas ta- gada inimeste kohta võimalikult väheste andmete kogumine ning registris kajastatavate andmete õigsus. Näiteks vähenevad isiku laenukohustused

regulaarselt ja selleks, et tagada registriandmete õigsus, tuleks registrit pidevalt ajakohastada. Maksehäireregistrite analoogia pinnalt saab öelda, et kui võlgnetav summa ei ole andmete väljastamisel laenu põhiosa, intresse ja viivist puudutavas osas lahti kirjutatud, tekitab see segadust võlgnikele ega anna piisavalt adekvaatset ülevaadet andme- subjekti maksekäitumisest ka andmete pärijale. Seega registrit väljastatav andmekoosseis peaks olema minimaalne, kuid võimalikult täpne.

Viimasena on oluline läbi mõelda ka registri in- fotehnoloogiline lahendus. Eelistatud oleks, et kre- diidiandjatel oleks võimalik andmeid pärida läbi andmevahetuskanali, mis eeldab, et igal kredii- diandjal on olemas enda andmekogu koos vajalike andmetega. Sel juhul saab teine krediidiandja, kui isik laenu taotlemiseks hoopis tema poole pöördub, teha päringu nt laenu taotleja kodupanga and- mekogusse. Alternatiivne variant oleks, et isikute krediidiandmed ei asu iga krediidiandja juures eraldi, vaid paisatakse kokku ühte andmekogusse, kust krediidiandjad saavad isikute kohta päringuid teha. Mida rohkem isikuandmeid ühes kohas asub, seda vähem on riskid maandatud, mis omakorda muudab sagedasemaks õigustamatute päringute teostamised, vale isiku krediidiandmete ekslikud väljastamised jms rikkumised.

AKI loodab panustada sellise registri loomisesse, mis ühest küljest aitab kaasa finantskeskkonna läbipaistvusele ning vastutustundliku laenamise põhimõttele, kuid teisalt tagab inimeste võlaand- mete kohase töötlemise.

Võlaandmete avaldamine

sotsiaalmeediagrupid

Möödunud aastal tegi inspeksioon suuri jõupingutusi, et lõpetada sotsiaalmeediagrupid ja -lehtedel inimeste võlaandmeid avaldavate isikute tegevus. Tegemist oli inspeksiooni omal initsiatiivil algatatud ulatusliku järelevalvemenetlusega, mis oli tingitud kodanike arvukatest kaebustest.

Menetlusi viidi läbi 7 andmetöötaja osas, kellest igaüks omakorda haldas 2–8 ebaseadusliku tegevusega Facebooki gruppi. Põhjus, miks teise inimese võlaandmeid ei tasuks sotsiaalmeedias avaldada, peitub selles, et vastav tegevus peab olema kooskõlas IKS (Isikuandmete kaitse seadus) §-s 10 sätestatud eesmärkide ja eeldustega. Nii on lubatud teise isiku võlaandmeid töödelda üksnes tema krediitdivõimelisuse hindamisel või muul samasugusel eesmärgil, kusjuures enne andmete avaldamist peab olema kontrollitud, et väidetavad võlaandmed oleksid õiged ning andmeid tohib edastada ainult isikule, kes tõesti soovib teise inimese krediitdivõimelisust kontrollida (nt enne temaga lepingu sõlmimist). Seega inimese võla piiramatu arvule isikutele internetis avaldamine nende nõuetele mõistagi ei vasta.

Asjaolu, et kirjeldatud viisil isikuandmete avalikustamine võlgniku eraelu puutumatust ebamõistlikult palju riivab, tõestavad näited menetluspraktikast. Isegi kui isikul esineb kellegi ees võlgnevus, ei saa kuidagi pidada õigustatuks käitumist, kus selle isiku Facebooki sõbralistist otsitakse üles sama perekonnanimega isikud (kel on võlgnikuga tõenäoliselt mingisugune sugulusaste) ning neid hakatakse ähvardama ja neile nõudekirju saatma.

Me keegi ei peaks vastutama kellegi teise tegude eest ning ka võlgnevus on seotud just selle isikuga, kes selle enda nimele võtta otsustas. Sarnaselt ei peaks inimest sotsiaalmeedias võlglaseks tembeldama näiteks siis, kui talle on soovimatult saadetud kaupa, mida ta tellinud pole, kuid mille eest hakatakse temalt tasu nõudma. Kuna erinevalt maksehäireregistrist ei kontrolli Facebooki gruppide pidajad avaldatavate võlaandmete õigsust, siis on valeväiteid kellegi väidetavast võlgnevusest just seal lihtne avaldada. See aga pole õige.

Sestap tegi inspeksioon selliste Facebooki gruppide ja lehtede haldajatele möödunud aasta kevadel ettepaneku inimeste võlaandmete avalikustamise lõpetamiseks. Osa administraatoreid ja moderaatoreid lõpetas seejärel enda tegevuse, kuid osa ei täitnud neile inspeksiooni edastatud ettepanekut. Seejärel viis inspeksioon läbi täiendava monitooringu ja analüüsi ning tegi ülejäänud menetlusosalistele ettekirjutuse, milles põhjalikult selgitas kirjeldatud tegevuse õigusvastasust ja tegi ka sunniraha rakendamise hoiatuse juhuks, kui ettekirjutusi ei täideta. Praegu on neli andmetöötajat neile tehtud ettekirjutused kohtus vaidlustanud, kuid taotletud esialgset õiguskaitset (kirjeldatud tegevusega jätkamiseks kuni kohtumenetluse lõppemiseni) halduskohus neile ei võimaldanud.

Seega juba praeguseks saab öelda, et suures osas on inimeste võlaandmete avalikustamine sotsiaalmeedias lõppenud ning inspeksiooni pikk ja ulatuslik menetlus on kandnud vilja.

Andmekaitse meedias

Ajakirjanduses ja sotsiaalmeedias teistest isikutest piltide, videote või artiklite avaldamine tõi 2021. aastal inspeksioonile arvukalt kaebusi. Suur hulk nendest oli seotud artiklitega, mis on isikute kohta avalikustatud ning mida meediaväljaanded ei ole nõustunud muutma või eemaldama. Lisaks oli kaebusi Google'i otsingumootori otsitulemuste kohta, kui otsinguga oli võimalik jõuda teabeni, mida veebilehel endal (enam) avaldatud ei olnud. Teine suur osa kaebusi oli seotud sotsiaalmeedias avaldatud postitustega.

Google'i indekseerimine

2021. aastal esitati mitu kaebust, mille kohaselt kohtulahendid, mis on Riigi Teatajas anonüümitud, avalikustati lehel Cases Legal täies mahus koos isiku nime ja isikukoodiga. Leht Cases Legal oli Google'i otsitulemustes kättesaadav, mistõttu oli võimalik isiku nime Google'i otsingumootorist otsides leida ka tema kohta käivad kohtulahendid, mis oleks pidanud olema anonüümsed. Andmekaitse Inspeksiooni töö tulemusel lõpetas Google oma otsingumootoris lehe Cases Legal indekseerimise ja nimetatud lehte ei ole enam võimalik leida.

Meediaväljaanded

2021. aastal esitati meediaväljaannete veebiartiklite eemaldamise või nendest isikute nimede eemaldamise kohta arvukalt kaebuseid. Kaebused pärinesid mh endistelt ja praegustelt vangidelt, kes soovisid kuritegude kohta avaldatud artiklitest oma nimede eemaldamist.

Suurem osa kaebustest jäid menetlusse võtmata, kuivõrd mõnel juhul oli sama isiku kohta avaldatud ka teisigi artikleid, mistõttu ei saa üks konkreetne artikkel kahjustada kaebajat ülemääraselt. Kaebused jäid menetlusse võtmata ka põhjusel, et nii konkreetse teema kui ka isiku osas on jätkuvalt avalik huvi, mille kohta andmete kättesaadavus panustab avalikku debatti ka aastate möödudes (sealhulgas isegi juhul, kui juhtumist on möödunud 20 aastat).

Euroopa Inimõiguste Kohtu praktika kohaselt tuleb artiklite eemaldamise asemel eelistada neile pealdiste lisamist. Veelgi enam, interneti arhiivid on kaitstud väljendusvabadusena, mistõttu ei saa kohtu ega meedia ülesandeks olla ajaloo ümber kirjutamine, kustutades internetis artikleid või neis avaldatut. Seetõttu on oluline meelde tuletada, et meediaväljaandelt saab nõuda artikli kustutamise asemel vaid isikustamise lõpetamist, asendades nimi tähemärkide või X-ga.

Sotsiaalmeedias postituste avalikustamine

Eelmisel aastal levis sotsiaalmeedias trend filmida patrullpolitseinikke, turvamehi ja klienditeenindajaid teadmata, et ka sellisel avalikustamisel peab olema õiguslik alus. Suures osas põhjendati videot avalikustamist sellega, et tegemist on COVID-19-ga seotud postitustega. Selliste põhjendustega unustati, et isegi kui ühiskonnas on avalik huvi konkreetse teema, sh COVID-19, vastu, ei pruugi avalikku huvi olla isikute osas, keda seoses teemaga kajastatakse.

Levis vaele arvamus, et kõiki videoid, mis on avalikus ruumis tehtud, võib avalikustada. Oluline on, et ka selline avalikustamine vastaks isikuandmete kaitse seadusele, st et andmesubjekti nõusolekut asendab tema teavitamine sellises vormis, mis võimaldab tal heli- või pildimaterjali jäädvustamise faktist aru saada (salaja filmimine on keelatud) ja enda jäädvustamist soovi korral vältida. Mõnel juhul ei ole võimalik kaamera vaateväljast kõrvale jääda, seda näiteks politseinike või tuletõrjujate puhul, kes täidavad oma tööülesandeid. Sellisel juhul on avalikustamine lubatud juhul, kui videost ei ole isik tuvastatav, näiteks on hägustatud isiku nägu või moonutatud tema häält. Sellest hoolimata võib isik olla äratuntav ka näiteks riietuse või kõnnaku järgi.

Avalikustamisel peab olema õiguslik alus

Oluline on meelde tuletada, et igasuguseks avalikustamiseks meedias või sotsiaalmeedias peab olema õiguslik alus. Õiguslikuks aluseks võib olla isiku nõusolek. Nõusoleku puhul tuleb aga meeles pidada, et isikul on võimalus see igal hetkel tagasi võtta.

Nõusolekut ei ole vaja, kui avalikustamisel on ajakirjanduslik eesmärk. Ajakirjanduslik eesmärk on täidetud juhul, kui see vastab kolmele eeldusele: isiku suhtes on avalik huvi, avalikustamine on kooskõlas ajakirjanduseetika põhimõtetega ja selline avalikustamine ei kahjusta andmesubjekti õiguseid ülemääraselt. Praktikas oli kõige rohkem kaebuseid seotud esimese ja kolmanda eeldusega, kus isikud leiavad, et nende osas puudub kas avalik huvi või on nende õiguseid ülemääraselt kahjustatud.

Avalik huvi on olemas isikute vastu, kes on avaliku elu tegelased või muud inimesed, kes on oma tegevusega pälvinud avalikkuse tähelepanu. Oluline on teha vahet, et isegi kui kajastatava teema kohta on olemas avalik huvi, siis eelduse täitmiseks peab olema avalik huvi ka konkreetselt teemaga seoses kajastatava isiku osas. Praktikas järeltas inspeksioon, et avalik huvi puudus näiteks kultuurikeskuse direktori vastu, kes oli kohustatud kontrollima COVID-19 tõendit, kuid see ei tähenda, et COVID-19 tõendite osas avalik huvi puuduks.

Meedias isikute kohta teabe, piltide või videote avalikustamine kahjustab selliste isikute õiguseid, kuid oluline on veenduda, kas selline avalikustamine kahjustab õiguseid ülemääraselt.

Praktikas leidsid paljud kaebajad, et juhul kui artiklid meediaväljaannetes on avaldatud aastaid tagasi, on praegu artikli jätkuv avalikustamine neid ülemääraselt kahjustav. Küll aga on siinkohal oluline analüüsida õiguste kahjustamise võimalikkust koos teiste faktidega, näiteks kas isiku kohta on ka muud, sarnast teavet (näiteks vangide puhul, kes soovivad konkreetselt ühe kuriteo kohta käiva artikli kustutamist, kuigi teiste sarnaste kuritegude puhul artikli osas pretensioonid puuduvad) või kas teema ise on niivõrd oluline, et selle kajastamine koos isiku nimega võib jätkuvalt olla oluline (juhul, kui tegemist on rahapesukahtlustusega inimesega).

Guugeldatavus

Eelmise aasta üks läbiv märksõna meie töös oli guugeldatavus ehk teisisõnu inimese kohta teabe esitamine Google'i (jt interneti otsingumootorite) tulemustes. See häirib inimesi kõige enam – seda tunnetatakse kõige suurema privaatsuse riivena –, mistõttu saame sel teemal palju kaebusi.

2021. aastal (ning jätkuna 2022. a) tegime ettekirjutused infoportaalidele, kes pakuvad inimese ja ettevõttepõhist teavet, mida nad on ise kokku kogunud kõikvõimalikest allikatest (äriregister, kohtulahendid, Ametlikud Teadaanded, kinnistusraamat, maksehäired, meediakajastused). Üks probleem oligi isikuandmete avaldamine otsingumootoritele indekseeritavalt. Nii andis Google inimese ees- ja perekonnanime sisestades kõigepealt 5–6 infoportaalide vastet inimese seostest juriidiliste isikutega. See aga tähendas, et nime alusel guugeldades oli lihtsasti leitav tema kuulumine korteriühistu juhatusse (mis ilmselgelt viitab enamjaolt sellele, kus inimene elab) ja muudesse mittetulundusühingutesse (mis võivad olla ka väga spetsiifilised, nt vähihaigete lapsevanemate liit või seksuaalvähemuste ühendus).

Selgitasime juba 1.06.2020 avaldatud seisukohas, et isikuandmete avaldamine saab toimuda üksnes õigustatud huvi alusel ning isikuandmete avalikustamine piiramatu isikute ringile internetis otsingumootoritele indekseeritavalt lubatav ei ole. Inspektsiooni hinnangul on infoportaalide eesmärk füüsilise isiku nime indekseeritavusel oma teenuse

reklaam ning seeläbi kliendi saamine ja/või talle teenuse müümine. Paraku ei luba ka reklaamiseadus inimese andmeid ilma tema enda nõusolekuta reklaamis kasutada.

Samuti tuleb arvestada, et Google salvestab andmed vahemällu, mis tähendab isikuandmete töötlemist kolmandas riigis (väljaspool ELi ja ELi majanduspiirkonda). Avalikustades isikuandmed oma veebilehel otsingumootorile indekseeritavana, võimaldab andmetöötaja teadlikult andmete edasist kogumist ja kolmandasse riiki edastamist. Sellise tagajärjega peab andmete avalikustaja arvestama ning sel viisil avalikustamiseks peab tal olema õigustus – õiguslik alus.

Töö sel teemal jätkub, sest vaatamata saadud ettekirjutustele avaldavad kahjuks mitmed infoportaalid jätkuvalt isikuandmeid guugeldatavana (Äripäeva infopank sai ettekirjutuse märtsis 2022, scorestorybook ja inforegister - Register OÜ juunis 2021, ent vaidlustas selle kohtus).

Samasugune probleem on arstide hindamise portaali tervisetrend.ee. Ka selles avalikustatavad arstide andmed on indekseeritavad.

Eelmisel aastal üllatas meid aga negatiivselt Äriregistri platvormiuuendus, millega kaasnes äriregistri andmete guugeldatavus. Asja uurides selgus, et äriregistrisse kantud isikuandmete guugledatavana avalikustamine oli Justiitsministeeriumi teadlik valik.

Justiitsministeerium põhjendas seda muu hulgas avaandmete regulatsioonile viidates, et avaliku teabe seaduse § 31 lg 8 alusel avaandmeteks olevate isikuandmete taaskasutamise viisi piiranguid saab seada vaid juhul, kui taaskasutamiseks andmise viis kahjustab oluliselt isiku eraelu puutumatust. Justiitsministeeriumi hinnangul see, et otsingumootoritest on leitav inimese nimi, isikukood ja ühingu juhatuse liikmeks oleku fakt, ei kahjusta oluliselt inimese eraelu puutumatust. Andmekaitse Inspeksioon sellega nõustuda ei saa. Isikukoodi otsingumootorite tulemustes pole varem kunagi aktsepteeritavaks peetud. Samuti pole tegemist pelgalt „juhatuse liikmeks oleku faktiga“, vaid nende pinnalt saab teha järeldusi.

Interneti otsingumootori pidaja on küll eraldi seisev vastutav andmetöötaja, kellelt saab nõuda andmete eemaldamist. Ent see ei õigusta andmete avalikustaja poolt andmete avalikustamist sellisel viisil, et neid saavad otsingumootorid indekseerida. Sellisel viisil isikuandmete avalikustamine suurendab eraelu puutumatuse riivet ning kallutab kaalukaasi selgelt inimese kahjuks. Sobivaks ei saa pidada vaikevalikut, et kõikide inimeste andmed avalikustatakse indekseeritavalt (sisuliselt paisatakse internetti) ning iga inimene peab selle tagajärje likvideerimiseks hakkama esitama interneti otsingumootorite pidajatele taotlusi. Eriti ei peaks seda tegema riik ise.

Veebiküpsiste kasutamine

Andmekaitse Inspeksioon kirjutas 2019. aastal oma aastaraamatus põgusalt veebiküpsistest ja nende teavitamise korrast (vt Andmekaitse Inspeksiooni 2019 aastaraamat lk 9).

Praegu, sh eelmisel aastal, teeb Andmekaitse Inspeksioon jõudsalt järelevalvet veebiküpsiste kogumise üle. Enamasti avastab Andmekaitse Inspeksioon puuduseid veebiküpsiste kasutamises muus asjus alustatud järelevalvemenetluste käigus. Seni on enamik menetlusi päädinud sellega, et Andmekaitse Inspeksioon teeb andmetöötlejale ettepaneku veebiküpsiste kogumise korrastamiseks ja need parandatakse ära. Äärmistel juhtudel oleme andmetöötlejale teinud ettekirjutuse koos sunniraha hoiatusega. Seni ühelgi korral sunniraha reaalset rakendatud ei ole, sest andmetöötlejad on vastavalt Andmekaitse Inspeksioonile veebiküpsiste kogumise andmekaitsealiselt korda teinud.

Enamikel juhtudel on andmetöötlejate veebilehtedel aktiveeritud analüütilised küpsised (nt Google Analytics), aga on ka muid variante.

Põhiline murekoht veebiküpsiste kogumisel on see, et veebilehe külastajatelt ei küsita küpsiste kogumise kohta korrektselt nõusolekut. Isikuandmete kaitse üldmääruse artikli 6 punkt a sätestab, et isikuandmete töötlemine on seaduslik ainult juhul, kui andmesubjekt on andnud nõusoleku töödelda oma isikuandmeid ühel või mitmel konkreetsel eesmärgil.

Isikuandmete kaitse üldmääruse põhjenduspunkt 30 sätestab, et füüsilisi isikuid võib seostada nende seadmete, rakenduste, tööriistade ja protokollide

jagatavate võrguidentifikaatoritega, näiteks IP-aadresside või küpsistega, või muude identifikaatoritega, näiteks raadiosagedustuvastuse kiipidega. See võib jätta jälgi, mida võidakse kasutada füüsiliste isikute profileerimiseks ja nende tuvastamiseks, eelkõige juhul, kui neid kombineeritakse serveritesse saabuvate kordumatute identifikaatorite ja muu teabega. Seega on küpsiste kogumine selgelt isikuandmete töötlemine ja selleks on vaja seadusest tulenevat õiguslikku alust, milleks saab Euroopas väljakujunenud praktikas olla ainult andmesubjekti nõusolek.

Oleme andmetöötlejatele seletanud, et eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi kohaselt peaks kasutajatel olema võimalik keelata küpsiste või muude selliste vahendite salvestamine oma lõppseadmes. Teavet kasutaja eri lõppseadmesse salvestatavate vahendite kohta ja õigust neist keelduda võib pakkuda korra ühe ja sama ühenduse ajal ning see võib hõlmata ka kõnealuste vahendite edaspidist kasutamist järgmiste ühenduste ajal. Teabe edastamine, keeldumisevõimaluse pakkumine või nõusoleku küsimine tuleks teha võimalikult kasutajasõbralikuks. Juurdepääs teatavale rakenduse sisule võib oleneda küpsise või muu sellise vahendi teadlikust vastuvõtmisest, kui seda kasutatakse õiguspärasel eesmärgil. Oluline on saada kasutaja vabatahtlik, konkreetne, teadlik ja ühemõtteline nõusolek või loobumine küpsistest. Kui kasutaja ei nõustu, peab siiski olema tagatud rakenduse põhifunktsioonide toimivus. Andmesubjekti nõusoleku andmise tingimused on muu hulgas sätestatud isikuandmete kaitse üldmääruse artiklis 7.

Toome välja põhilised probleemkohad veebiküpsiste kogumisel:

1. Andmetöötledjad ei küsi veebiküpsiste kogumisel andmesubjektilt nõusolekut.
2. Andmetöötledjad küsivad veebiküpsiste kogumisel andmesubjektilt nõusolekut, kuid teevad seda ebakorrektelt. Nõuetele vastav teade küpsiste kasutamisest sisaldab selgitust, mis eesmärgil küpsiseid kasutatakse, kui kaua ja kes on need osapooled, kellega on kavas neid jagada. Muu hulgas peab teavitust sisaldama viidet andmekaitsetingimustele, kus on selgitatud ka küpsiste kasutamise tingimusi. Andmesubjekt peab aru saama, milliseid küpsiseid veebileht kogub ja tal peab olema võimalik iga küpsiseliigi kohta anda eraldi nõusolek või keeldumine.
3. Andmetöötledjad loovad veebilehe kliendipoolsesse (ingl front end) vaatesse nõusoleku küsimiseks hüpinkakna, kuid see on jäetud täielikult liidestamata veebilehe tagasüsteemiga (ingl back end). Ehk lühidalt on tehtud nõusoleku küsimiseks hüpinkaken, mis tegelikkuses ei rakendu ja küpsiste kogumist ei keelusta, kui andmesubjekt peaks selle keelama. Selline tegevus on vale. Muu hulgas ei tohiks küpsised rakenduda veebilehele sisenedes, vaid alles siis, kui andmesubjekt on andnud oma nõusoleku. Näiteks külastades mõnda veebilehte, kus kogutakse küpsiseid, peaks esimese asjana veebileht kuvama nõusoleku küsimiseks hüpinkakna. Seejärel saab andmesubjekt valida, kas a) nõustun, b) nõustun osaliselt (ehk talle avaneb valik erinevate küpsistega) või c) keeldun. Alles seejärel saab veebileht vastavalt andmesubjekti valikutele küpsiseid koguma hakata, kui üldse.

Andmekaitse Inspeksioon kavatseb veebiküpsiste andmekaitse poolega edasi tegeleda ja ükski andmetöötleja ei peaks võimalikke ettepanekuid isiklikult võtma. On ilmselge, et Andmekaitse Inspeksioon ei jõua kõikide ettevõteteneni, kes küpsiste kogumisega isikuandmeid töötlevad, kuid annab oma parima, et riigi üldpilt oleks selgem ja korrektne, et väiksemad eeskujud võtaksid.

Rämpspost

AKI-I on palju elektroonilise otseturustuse menetlusi, kus andmetöötaja saab korduvalt e-kirju ilma õigusliku aluseta. Paljuskki on tegemist tehnilise süsteemiveaga, kus ei ole süsteemis märgitud, et inimene ei soovi e-kirju. Andmetöötaja peab olema valmis andmesubjektile tõendama nõusoleku olemasolu. E-kirju võib füüsilisele isikule saata eelneval nõusolekul. E-kirjas peab olema loobumislink, mis samuti ei ole paljudes otseturustuskirjades olemas. Andmesubjektil peab olema lihtne ja kiire viis elektroonse kanali kaudu kirjades loobuda.

Sama käib SMS-ide kohta, milles tihtipeale puuduvad viited, kuidas järgmisi kirju või sõnumeid keelata. E-kirjade ja SMS-ide saatmine muutub aina riivavamaks viisiks ja seda tunnetavad kõik, kes soovimatuid kirju või sõnumeid saavad. Samuti peab mainima, et mõned riigiasutused saadavad uudiskirju ja ülevaateid, millest peab samuti olema võimalik loobuda.

Kõnedes on jätkuv metsamüügi või ostu temaatika ja samuti metsa hindamise teenuse pakkumine. Inspektsioon on pidanud tuvastama kõne tegija, sest kõne käigus helistaja ei ütle, millisest ettevõttest ta helistab ning kust ta on saanud telefoninumbri. Seetõttu tuleb algatada järelevalvemenetlus.

Kõnesid on ka vitamiinimüüjatelt ja teistelt kaupade pakkujatelt. Inspektsioon on seisukohal, et internetist ei tohi numbreid kokku rehitseda ja helistada neile eesmärgipäraselt. Numbrile, mis on avaldatud eesmärgiga müüa näiteks kasutatud autot, ei tohiks helistada eesmärgiga müüa vitamiine või osta inimese kinnistut.

Statistikaameti osas oli menetlus, kus inimesele helistati korduvalt ja survestati teda küsitlusele vastama. Selline survestav käitumine ei ole õige, kui inimene on korduvalt ka keeldunud.



Selles menetluses selgitati Statistikaametile, et korduvalt helistada ei tohi, kui isik on avaldanud soovi nii kirjalikult kui ka telefonitsi, et ta ei soovi küsitlusele vastata. Inspektsioon tegi Statistikaametile ettepaneku muuta helistamise korda nii, et korduvalt ei tohi helistada.



Isikuandmete töötlemine erakondade tegevuses

Enne 2021. aasta kohaliku omavalitsuse valimisi saatsime kõikidele erakondadele meeldetuletuseks ringkirja, mida peaks jälgima isikuandmete töötlemisel. Eelkõige puudutas see valimisreklaami tarbeks valijate andmete töötlemist. Samuti palusime üle vaadata, et äriregistris ei oleks liikmete kohta vigaseid ega topelt kandeid https://ariregister.rik.ee/est/political_party. Sellest hoolimata jõudis meieni pärast valimisi kolm rikumist, mille osas pidime tegema isikutele noomitused:

1

Narva Kunstikooli direktor, kes kasutas lastevanemate e-posti aadresse ilma nende eelneva nõusolekuta selleks, et saata neile kooli üldaadressilt enda kohta valimisreklaami.

2

Erakonna nimekirjas kandideerinud isik, kes kasutas äriregistri avalikke andmeid korteriühistute juhatuse liikmete kohta (elukoha piirkond, e-posti aadress), saates seejärel viimastele e-posti teel oma valimisreklaami.

3

Erakonna nimekirjas kandideerinud tervishoiutöötaja, kes kasutas töötades saadud patsientide kontaktandmeid, helistades neile aastaid hiljem ning paludes kohalikel valimistel enda poolt hääletada.

Sellest võib järeldada, et erakonnad ei ole ise oma kandidaate piisavalt juhendanud. Arvestama peaks ka seda, et tihtilugu võib kandidaat sellise ebakohase käitumisega tuua kaasa tervele erakonnale negatiivset mõju.

Enne valimisi tekib paljudel huvi ka üle kontrollida, kas nad on end „unustanud“ mõne erakonna nimekirja. Nt võib nii avastada end ka hoopis teise erakonna nimekirjast, kui erakond on vahepeal ühinenud (nt Eesti Rahvaliidu liikmed, kes ootamatult said EKRE liikmeteks). Tuletasime erakondadele meelde, et isiku taotlusel peavad nad ta erakonna nimekirjast kustutama. Kiirem variant erakonna poole pöördumise asemel on see, kui minna äriregistri ettevõtjaportaali. Sinna tuleb kas ID-kaardi või pangalingi kaudu sisse logida ning seejärel valida link "Erakonna nimekirjad". Seal tuleb üles otsida link nimega "Erakonnast väljaastumise teate koostamine", millele klikkides on võimalik täita erakonnast väljaastumise avaldus. Samas keskkonnas saab väljaastumise avalduse ka allkirjastada, peale mida on isik automaatselt erakonna liikmete nimekirjast välja arvatud. Allkirjastatud dokumenti on hiljem võimalik näha menüüpunkti „Erakonda kuuluvus“ alajaotuses „Lahkumisavaldused“.

Samas saab isik ise või erakond ainult luua/muuta liikmelisuse lõpetamise kannet. Juhul, kus isik leiab, et ta on algusest peale kantud ekslikult mõne erakonna nimekirja, siis peaks ta kande kustutamiseks pöörduma tsiviilkohtumenetluse seadustiku alusel kohtute registriosakonna poole.

Aastal 2022 algatasime järelevalvemenetluse riigi valimisteenistuse suhtes seoses kandideerijate andmete töötlemise ja valimisteenistuse kodulehel avaldatud andmekaitsetingimustega. Menetluse tulemusel said 2023. aasta riigikogu valimiste kandidaadid esitada oma andmed uuendatud kandideerimisavaldusel, kus on kandidaadi jaoks selgelt kirjas, milliseid kandidaadi esitatud isikandmeid avalikustatakse, kas seaduse või nõusoleku alusel, ja milliseid mitte. Lisaks saab korrigeeritud

andmekaitsetingimustest täpse ülevaate, milliseid isikuandmeid, millisel eesmärgil ja õiguslikul alusel valimistega seoses töödeldakse ning kui kaua isikuandmeid säilitatakse. Kuigi valimised.ee lehel sai isikuandmete töötlemisega seonduv selgemaks nii kandidaadile kui lehe külastajale, siis on seadusandja regulatsioonidega jätnud teatud erisused.

Kohaliku omavalitsuse volikogu valimise seaduse § 33 lõige 4 sätestab, et riigi valimisteenistus avaldab käesoleva paragrahvi lõike 2 punktides 1, 3, 6, 7 ja 8 ning lõikes 3 sätestatud andmed. Täpsemalt tähendab see, et avaldatakse kandidaadi ees- ja perekonnanimi, erakondlik kuuluvus, kontaktandmed, andmed hariduse ning töökoha ja ameti kohta. Kolmas lõige kohaldub kui kandidaadil on teine kodakondsus, mis sel juhul ka avaldatakse. Analoogne säte on ka Riigikogu valimise seaduse § 28 lõikes 3.

Antud juhul avaldatakse lehel valimised.ee lisaks seaduses reguleeritule kandidaadi sünniaeg. See- ga nende andmete avaldamise ainsaks aluseks saaks olla isiku nõusolek, mis osas peab arvestama, et isik võib igal hetkel oma nõusoleku tagasi võtta ja nõuda andmete avaldamise lõpetamist. Samuti ka seda, et isik peab saama valida, kas ta nende andmete avalikustamisega nõustub. See ei tohi seada teda teiste kandidaatidega võrreldes halvemasse seisu.

Võrdluseks erakonnaseaduse § 8¹ lõike 1 alusel kantakse äriregistris peetavasse nimekirja isiku ees- ja perekonnanimi, isikukood, liikmeksastumise ning väljaastumise või väljaarvamise aeg. Avalikus vaates näidatakse isikukood/sünniaeg real isikukoodi asemel sünniaega, mis on isikuid vähemkahjustavam valik ja täidab ära sama eesmärgi (nimekaimude vältimine).

Seega on seadusandja oma regulatsioonidega jätnud kummalise erisuse, kus kõikide erakonna liikmete kohta võib avalikustada äriregistris lisaks nimele ka nende isikukoodi (kuigi sellest avaldatakse vaid sünniaeg). Seejuures on aga valimistel kandideerijate puhul nende sünniaja avaldamiseks vajalik isiku eelnev nõusolek. Selgelt suurem põhjendatud huvi on avalikkusel just kandidaatide andmete vastu, mitte kõigi erakonna nimekirjas olevate isikute vastu. Kandidaate võib olla samanimelisi, mistõttu on sünniaja lisamine üldiselt põhjendatud. Kuniks seda ei lisata regulatsiooni, ei ole võimalik kasutada sünniaja avaldamiseks muud alust, kui isiku eelnev nõusolek. Seadus ei reguleeri ühelgi juhul andmete avalikustamise tähtaegu. Seega peaks avaldaja lähtuma üldisest põhimõttest, et andmeid avalikustatakse nii kaua ja

selles mahus, mis on vajalikud eesmärgi täitmiseks. Valimised.ee lehel eemaldatakse nt kandideerijate andmetest avalikust vaatest poole aasta möödudes mõned andmeväljad (töökoht ja amet, kontaktandmed). Leiame, et see on hea praktika näide. Äriregistris olevad andmed on nähtavad, aga igavesest ajast igavesti. Kas igaühel on tarvis teada iga isiku kohta erakonda astumiste teavet, jääb küsitavaks. Kandideerinud isikute osas on avalikkuse huvi oluliselt selgem ja põhjendatum. Veel suurem põhjendus on nende osas, kes on saanud valitud ja täidavad/on täitnud valijate ees avalikku ülesannet.

Andmetöötaja peaks alati valima meetmed, millega kaasneks võimalikult väike riive isikute eraelu puutumatusel. See tähendab, et eesmärgi saavu-



tamiseks tuleb isikuandmeid töödelda minimaalselt ja kustutama koheselt, kui eesmärk on täidetud. Nt kui avalikustaja valib variandi, et isikud on oma nime alusel avalikele otsingumootoritele leitavad, siis on see isikute privaatsust oluliselt rohkem kahjustavam. Soovitame seetõttu alati tungivalt valida võimalus ka seaduse alusel andmete avaldamisel valida viis, kus andmed on leitavad vaid otse lehelt otsides, mitte nõ guugeldades. Kui avalikustatakse ka isikute kontaktandmeid, siis lisaks privaatsuse riivele loob see võimaluse korjata robotitel kokku isikute kontaktandmeid, et kasutada neid muul eesmärgil.

Seega võiks kaaluda kas endiste erakonna liikmete andmed jääks teatud aja möödudes äriregistris nähtavaks, kuna eelkõige tundub,

et seadusandja peamine mõte on olnud see, et avalikkus saaks kontrollida hetkelist liikmelisust. Põhjendatud võib olla jälgida liikmete liikumisi ja erakondade vahetamist, aga kas see on põhjendatud, kui liikmelisuse lõppemisest on juba nt 10 aastat möödunud? Jätame selle teema mõtisklemiseks ja tuletame sellega meelde, et isikuandmete töötlemise üks oluline aspekt on alati aeg. Igavene töötlemine ja säilitamine ei peaks olema mitte vaikimisi valik, vaid erand. Mida rohkem me arvutimaailma kolime, seda suuremalt puudutab kõikide andmete säilitamise teema ka digiprügi teemasid, kus lisaks turvariskide vähendamisele peaks andmetöötaja eelistama ebavajalike andmete kustutamist ka rohelise mõtteviisi toetamiseks.



Keskkonna

teemade läbipaistvus

Võrreldes eelmise aastaga on näha selget kasvu keskkonnasektoris esitavate vaiete osas nii ajakirjanduse esindajate kui ka keskkonnaorganisatsioonide poolt. See näitab ühiskonna suurenenud huvi riigi tegevuse ja selle läbipaistvuse vastu seoses keskkonnateemadega, milles kindlasti mängib suurt rolli kliima soojenemine ja Eesti riigi kliimakokkulepped Euroopa Liidus. 2021. aasta tõi kaasa suure huvi eelkõige metsandusteemade osas.

Juba 2020. aastal esitati inspeksioonile kaks vaiet, kus sooviti, et Keskkonnaagentuur väljastaks kõik statistilise metsainventuuri alusandmed (SMI andmed), sh proovitükkide koordinaadid. SMI mõõtmistulemuste peamine siseriiklik eesmärk on saada statistiline ja objektiivne hinnang Eesti metsaressursi kohta, et kavandada riigi strateegilisi metsamajandamise otsuseid. Vaatasime teabe üle ega leidnud, et mingis osas oleks küsitav teave juurdepääsupiiranguga (vastav alus teabele juurdepääsu piirata puudus), mistõttu tegime ettekirjutuse kõikide andmete väljastamiseks. Ajutiste proovitükkide koordinaadid väljastati, aga alaliste proovitükkide kohta asus Keskkonnaministeerium ruttu juurdepääsupiirangu alust looma, algatades selleks ka metsaseaduse muutmise eelnõu. Paraku seaduseelnõu on jäänud toppama ja ühtlasi on keskkonnaühingud esitanud ministeeriumi vastu kohtusse hagi.

Ajakirjandust lugedes jääb mulje, et Eesti riiki kahtlustatakse liigses metsa raiumises ja Euroopale valede tulemuste esitamises. See on ka väidetavalt peamine põhjus, miks nii järjepidevalt soovitakse mõõtmistulemusi kontrollida ja kõik andmed riigilt kätte saada. Seega jätkus SMI andmete vaidlus ka 2021. aastal, kui SMI andmete kohta esitati kaks

vaiet, kus ei soovitud küll enam koordinaate, aga hakati küsima riigi arvutustulemuste kontrollimiseks muid lisaandmeid.

Teabevaldajatel asub järjest enam andmeid eri infosüsteemides, mitte konkreetsetes dokumentides. SMI andmete väljastamisel on teabevaldaja toonud välja, et sellise päringu teostamiseks pidid nad kirjutama teabenõudja teabenõude täitmiseks eraldi skripti, kuna neil endal ei ole sellises andmekoosseisus teavet olemas. Leidsime, et kui teabevaldaja kasutab sellist andmebaasi, millest andmete välja võtmiseks on neil endal tavapärane praktika selleks skriptide kirjutamine, siis on ka võimalik täita teabenõuet. See tähendab, et selline oskus on olemas ja seda kasutatakse tavapäraselt, mistõttu tuleks asuda seisukohale, et olemasolevate andmete väljavõtmiseks skripti kirjutamise vajadus ei ole piisavaks põhjuseks, miks lugeda pöördumist selgitustaotluseks või keelduda teabenõude täitmisest. Küll aga võib skripti kirjutamise vajadus olla oluliseks põhjuseks, miks pikendada teabenõude täitmise tähtaega. Selline skripti kirjutamise võimekus riigiasutustel peaks olema erandlik. Küll aga ei saa vaidlust olla siis, kui süsteem võimaldab teha just sellist väljavõtet nagu teabenõudja küsib. Sel juhul ei saa olla argument, teavet mitte väljastada, põhjenduseks, et eelnevalt ei ole sellises koosseisust teavet loodud. Juhul kui teabenõude täitmiseks peaks teabevaldaja eelnevalt mingeid andmeid sisestama või mõnest teisest süsteemist võtma ja lisama, siis on päring oma loomult juba selgitustaotlus.

Avalikkuse huvi suurendab kahtlemata ka Euroopa kliimaseaduses olev kohustus, mis kätkeb tervet Euroopa Liitu saavutama 2050. aastaks CO₂-neutraalsuse. Metsal on selles võitluses väga oluline roll.

Eesti Maaülikooli uuringu järgi seovad õhust süsinikku noored ja keskealised puud, samal ajal, kui vanemad metsad muutuvad süsinikuallikateks. Seega võiks väga lähimõeldud metsa majandamine tuua kaasa olulisi tulemusi. SMI andmeid kasutab Eesti riik ühtlasi selleks, et näidata oma maakasutusest, maakasutuse muutusest ja seehulgas metsandusest (LULUCF) tulenevat kasvuhoonegaaside heite andmeid Euroopale. SMI proovitükkide andmete mõõtmine on toimunud 20 aastat ja seda mudelit kasutavad ka mõned teised liikmesriigid.

Kõik liikmesriigid peavad tagama, et esitatud andmed on täpsed, täielikud, järjepidevad, võrreldavad ja läbipaistvad. Keskkonnaministeerium on selgelt väljendanud, et kui SMI koordinaadid saaks avalikuks, ei oleks enam tulemused objektiivsed. Seega ei saaks andmeid esitada ka LULUCF-i raporti jaoks. Samal ajal on ülikooli teadlased juhtinud tähelepanu, et Eesti vajab jätkamiseks uut metsa arvestamise meetodikat. Väidetavalt on küsijatel juba endil oordinaadid teada ja välja arvatud. Siiski küsitakse lisaandmeid, kuna tulemused ei klapi. Seega näis, mis saab SMI meetodikast ja kas pidev riigi tegevuse vastu huvi tundmine muudab ka Eesti metsapoliitikat. Loodetavasti sel juhul järjest nutikama, säästvama ja läbipaistvama metsamajandamise suunas.

Metsateemade üle oli mitu vaidemenetlust ka Riigimetsa Majandamise Keskuse (RMK) kohta. Avalikkus tundis huvi, mis hinnaga Eesti riik metsa müüb (riigi ja puidufirmadega sõlmitud kestvuspinguid), kuidas uuendusraiate mahte arvutatakse ja planeeritakse ning sooviti saada kõrgendatud avaliku huviga (KAH) alade kohta lisaks muule infole ka kaardikihti.

Puidumüügifirmadega sõlmitavates kestvuspingutes saime taaskord selgitada, et ärisaladuse piirangut saab kasutada väga piiratud osale teabele. Tihtilugu hindab ettevõtja oma ärisaladust palju suuremaks, kui see reaalsuses olla saab. Enamasti saab ärisaladuseks lugeda vaid üksikud sõnad või lauseosad. Leiame, et peamine probleem on selles, et riigiasutused ei ole eraettevõtetele juba lepingut sõlmides selgitanud, et riigiga sõlmitavates lepingutes peaks ettevõtja juba arvestama, et on valmis teabe avalikkusega. Oluline on ka meelde tuletada, et ärisaladuse juurdepääsupiirangut ei saa kasutada kauem, kui seadus seda lubab ehk 5 aastat, mida saab ühe korra pikendada veel kuni 5 aastat. Küll aga pärast maksimaalset 10 aastat ei ole tegemist enam ärisaladusega. Sellistesse lepingutesse ei peaks juhatuse liikmed lisama nt ka oma isiklikke kontaktandmed, mida tegelikult inspeksioon ei käsitse isiklikena, kui need on ühtlasi toodud äriregistris ettevõtte kontaktandmetena.

Uuendusraiate arvutuskäigu kohta väitis teabenõudjast ajakirjanik, et talle on jäetud mulje, et teda huvitava teabe on saanud ühe riigiasutuse töötaja teiselt riigiasutuse töötajalt meili teel, aga see ei ole eraldi dokumendiregistris registreeritud ja tegemist on erakirjaga. Selgitasime, et asutuse töötajad ei pea tööpoolest dokumendiregistris registreerima oma erakirjavahetust. Nt kahe töötaja vahelised kirjad, kus arutatakse lõunale mineku plaane, sünnipäevaõnnitlusi, asutusevahelisi nõu küsimisi jms. Aga kui ühe riigiasutuse töötaja saadab teisele riigiasutuse töötajale tööalaselt vajaliku teavet, sealjuures selleks, et teine asutus saaks saadud arvutustulemusi kasutada, et täita enda seadusest tulenevat kohustust, siis ei ole tegemist erakirjavahetusega.

Seega sellised kirjavahetused peab kindlasti asutuste dokumendiregistris registreerima ja kui need ei ole registreeritud, siis ei tähenda see suguigi seda, et keegi ei võiks asutuselt ka ainult töötaja e-postkastis olevat avalikku teavet välja küsida. Sellega paneme asutustele südamele, et kõik olulised kirjad saaks registreeritud. Seda ka seetõttu, et töötajate vahetuse tõttu midagi tähtsat kaotsi ei läheks.

KAH alade kohta soovis üks keskkonnaorganisatsioon saada KAH alasid puudutavat kaardikihti SHP failina. Selles osas otsustas teabevaldaja, et avalikustab sellise kaardikihi faili avalikkusele oma kodulehel ja uuendab seda igal aastal.

Lisaks väärrib mainimist Keskkonnaametile tehtud ettekirjutus, kus palusime väljastada teabepõhjal mitmeaastased loodusobjektide kaitse planeerimise komisjoni ning liikide kaitse ja võõrliikide ohjamise planeerimise komisjoni istungite protokollid. Analoogete vaidemenetluse viisime läbi

ka 2020. a Keskkonnaministeeriumi osas, kus leidsime, et peab väljastama pakendikomisjoni istungi protokollid. Mõlemal juhul saab kinni katta vaid väga piiratud osa, kui mõnes konkreetses protokollis esineb vastav lõik, mis annab juurdepääsu-piirangu aluse. Selliste komisjonide tegevus peaks olema avalikkusele läbipaistev. Tihtilugu ei kinnita minister kõiki komisjoni ettepanekuid, aga avalikkusel peab olema võimalus saada selgust, kuidas ühe või teise otsuseni on jõutud, sh mis on olnud komisjoni algsed ettepanekud.

Menetluses tõime välja, et küsitakse sellist avalikku teavet, mis on antud juhul ka keskkonnateabe, millele kohaldub lisaks Arhusi konventsioon (keskkonnainfo kättesaadavuse ja keskkonnaasjade otsustamises üldsuse osalemise ning neis asjus kohtu poole pöördumise konventsioon) ja keskkonnainfo direktiiv. Seega saab keskkonnateabele piirata juurdepääsu vaid juhul, kui eelnimetatud regulatsioonid seda võimaldavad. Kui Eesti seaduse regulatsioon ei ole kooskõlas Arhusi konventsiooni



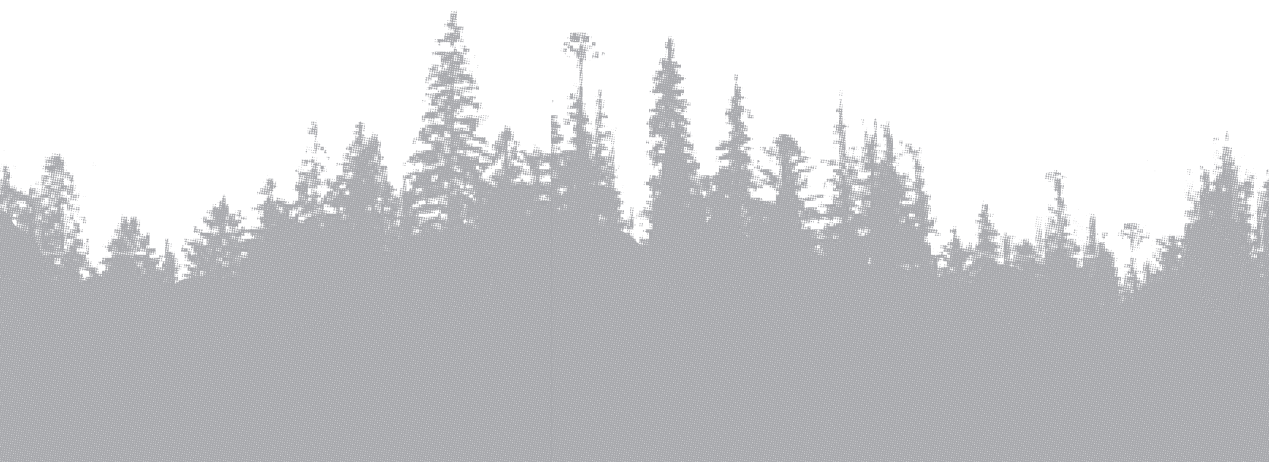
ja keskkonnainfo direktiiviga sisult konkreetsete sätetega, siis tuleb Eesti seaduse norm jätta kohaldamata vastavalt põhiseadusele ja EL-i õigusele – selle asemel kohalduvad vastavad konventsiooni ja direktiivi normid.

Saime taas selgitada kavandile kohalduvat juurdepääsupiirangut. AvTS §-i 35 teine lõige annab teabevaldajale erinevalt esimesest lõikest, kus on teabevaldajal kohustus määrata vastavad piirangud, vajadusepõhise võimaluse kasutada juurdepääsupiiranguid. Seega teises lõikes toodud piiranguid ei peaks teabevaldaja kasutama, kui selleks ei esine reaalselt ja põhjendatud vajadust, mis peab ühtlasi olema ajakohane.

Seega ei saa igale dokumendikavandile automaatselt vastavat juurdepääsupiirangu alust kehtestada, vaid eelnevalt peab teabevaldaja hindama, kas see on vajalik, mis on piiramise põhjused ja kas need kaaluvad üle avalikkuse huvi. Keskkonnateabe puhul eeldatakse juba seda, et avalikkusel

ongi kõrgendatud huvi. Lisaks saab teabevaldaja kavandite puhul alati kasutada juurdepääsu piiramise asemel dokumendil märget, et tegemist on kavandiga.

Eraldi selgitame, et kavandi juurdepääsupiirangu kasutamise eeldusteks on see, et see kehtib vaid kuni see sama dokument on vastu võetud või allkirjastatud ehk dokumendist on valminud lõplik versioon, mida enam ei muudeta. Selge on see, juba koostatud protokollid ei ole oma loomult enam muutmisejärgus, vaid lõplikult kinnitatud dokumendid. Kavandi piirang on oma loomult väga lühiajaline piirang ning seda ei saa kasutada põhjendusel, et äkki midagi dokumendis sisalduvat kasutatakse mingis järgnevas dokumendis (nt seaduseelnõus). Muul juhul võiks selline lähene mine tuua kaasa igaveste kavandite loomise, mis osas äkki kuskil keegi kasutab midagi oma järgmises kavandis jne. Seega leidsime, et komisjoni protokollid ei saa sellist juurdepääsupiirangut kanda.



Avaliku teabe seaduse täitmisest

Avaliku teabe seadus reguleerib avaliku teabe kasutamist ja kättesaadavust nii riigi- kui ka eraasutuses, mis täidab avalikke ülesandeid või on saanud riigieelarvelisi vahendeid. Avaliku teabe all mõistetakse avalikke ülesandeid täites loodud ja saadud teavet, mis on salvestatud teabekandjale, teisisõnu riigi- ja kohalike omavalitsuste asutuste töö käigus tekkinud talletatud informatsiooni.

Inimestel on õigus teada, mida avaliku halduse asutused teevad – missuguseid seaduseid ette valmistatakse, milliseid programme ja projekte läbi viiakse, kuidas kasutatakse raha ning milliseid rahvusvahelisi leppeid ette valmistatakse.

Ühiskond ootab, et tal oleks juurdepääs teabele, mis selgitab valitsuse poliitika ja tegevust. Näiteks, miks on otsustatud müüa riigiettevõtte või millistele dokumentidele toetudes kavandatakse keskkonda mõjutav jäätmekäitlusjaam. Avatus ja läbipaistvus on demokraatliku kodanikuühiskonna toimimise alus. Info vähene kättesaadavus tekitab vastandina inimestes umbusaldust ja ükskõiksust ning taasloob suletud mõtteviisi poliitikute hulgas.

Avalik teave on muutunud paljude jaoks iseennest mõistetavaks. Kui seaduse kehtima hakkamise ajal oli suurem osa teabest veel paberkandjal, siis täna on see enamasti digitaalsel kujul ning veebilehed muutuvad iga aastaga üha informatiivsemaks.

Infovabadus on demokraatliku riigi üks alustalasid, tehnoloogia areng muudab info järjest olulisemaks ja kättesaadavamaks ning seab oma ootused ja nõuded avaliku sektori veebilehtedele.

See on aga omakorda tekitanud olukorra, kus avaliku teabe seadus on jäänud nii mõneski osas ajale jalgu ja vajaks üle vaatamist. Ka on kodanikud muutunud aasta-aastalt teadlikumaks ja oskavad asutuste veebilehtedel vajalikku teavet otsida ning selle puudumisel pööratakse üha sagedamini ka Andmekaitse Inspeksiooni poole.

Samas muudab infovabaduse põhimõtte järgimise keeruliseks teabe hindamine selle avalikustamise seisukohalt, kuna õigus saada infot avaliku võimu organite ja ametiisikute tegevuse kohta ei ole siiski piiramatult. Põhiseaduse § 44 lõike 2 kohaselt ei laiene juurdepääs andmetele, mille väljaandmine on seadusega keelatud, ja asutusesiseseks kasutamiseks mõeldud andmetele. PS § 44 lõikes 2 sätestatud põhiõigust võib piirata eeldusel, et kehtestatud piirangul on legitiimne eesmärk ning piirang on proportsionaalne. Seega tuleb enne avalikule teabele juurdepääsu võimaldamist teabevaldajatel hinnata, kas ja millisele teabele on vajadus juurdepääsu piirata. Kahjuks on selles osas siiski palju eksimusi.

Teabe avalikustamisel on kaks viisi: teabe passiivne avalikustamine, millisel juhul saab teavet küsida teabenõude korras ja teabe aktiivne avalikustamine, millisel juhul teabevaldaja on kohustatud teabe omalgatuslikult veebilehel avalikustama. See, kui seadus ei kohusta teavet võrgulehel avalikustama või kui soovitud teave ei kuulu loetellu, millele seadus ei luba juurdepääsupiiranguid kehtestada, ei tähenda seda, et kogu ülejäänud teave oleks piiranguga. Praktikas valmistab jätkuvalt probleeme teabele juurdepääsu andmise või mitteandmise otsustamine.

Teabe avalikustamine riigiasutuste veebilehtedel

Kuna 2021. aastal edastati Andmekaitse Inspeksioonile mitmeid märgukirju, milles juhti inspeksiooni tähelepanu sellele, et riigiasutuste veebilehel ei ole nõuetekohaselt avalikustatud avalikku teavet ning dokumendiregistrite kaudu ei võimaldata juurdepääsu dokumentidele, siis kontrollis inspeksioon 2021. aasta sügisel riigiasutuste veebilehti, et saada ülevaade, kuidas riigiasutused täidavad avaliku teabe seadust veebilehete pidamisel.

Nii mõnigi kord on Andmekaitse Inspeksioonile heidetud seirete läbi viimisel ette, et miks kontrollitakse ainult teabe olemasolu veebilehtedel, kuid ei kontrollida, kas teave on avalikustatud ka näiteks masinloetaval kujul, mis võimaldaks teabe automatiseeritud töötlemist. Nõustume, et ka selline kontroll on vajalik, kuid mõttetu on seada eesmärgiks kontrollida teabe avalikustamist masinloetaval kujul, kui ikka ja jälle esineb olukordi, kus teavet pole veebilehel üldse avalikustatud. Siinkohal on Andmekaitse Inspeksioon seadnud endale esimeseks prioriteediks selle, et seaduses nõutud teave oleks veebilehel avalikustatud.

Veebilehed näevad kenad välja ja seal on enamasti ka teave selle kohta, millega asutus tegeleb ja milliseid teenuseid osutavad. Kui proovida otsida teavet, mida kohustab avalikustama avaliku teabe seadus, siis võib selle leidmine osutuda üsna keeruliseks.

Seekordne seire toimus pisut erinevalt kui tavapäraselt, st inspeksioon ei teavitanud asutusi eraldi ei seirest ega ka selle tulemustest. Teabe, mille olemasolu me veebilehtedel kontrollisime, panime kokku selle alusel, mille osas oli aasta jooksul enim pöördumisi, et teave ei ole leitav. Ehk siis seire eesmärgiks oli tuvastada riigiasutuste veebilehtedel teabe avalikustamise üldine olukord, ilma et sellest oleks asutusi eraldi teavitatud. Eelmisel aastal oli enim kaebusi selle osas, et asutused ei avalikusta oma veebilehtedel kõigi ametnike haridust ja eriala ning ametijuhendeid.

Kontrolli käigus selgus, et kui enamike ametnike puhul on teave, siiski avalikustatud, siis millegipärast on osade ametnike puhul eeltoodud andmed jäetud avalikustamata. Kuigi kontrolli käigus ei ole alati võimalik tuvastada, kas konkreetse asutuse töötaja puhul on tegemist ametnikuga või töölepingu alusel töötava isikuga, tekitab siiski küsimusi kui kahel samal ametipositsioonil töötava isiku puhul on ühe osas andmed avalikustatud, kuid teise osas mitte.

Teiseks vaatasime nii palgajuhendite kui palgaandmete avalikustamist, mis on pidevalt avalikkuse huvi keskmes. Avaliku teenistuse seaduse § 65 lg-te 1 ja 2 kohaselt tuleb ametnike palgaandmed avalikustada avaliku teenistuse kesksel veebilehel ning palgajuhend asutuse veebilehel (lg 3). Ligi 1/3 kontrollitud asutustest ei õnnestunud veebilehelt palgajuhendit leida.

Kuna seadus kohustab asutusi ametnike palgaandmeid avalikustama avaliku teenistuse kesksel veebilehel, siis vaatasime, kuidas asutused on juhatanud teabe otsijad avalikustatud teabe juurde.

Tavapärane on, et menüüpunkti või dokumendiregistri juures on link, mis juhatab avaliku teenistuse veebilehele. Kui see juhatab õigesse kohta on kõik korras. Kontrollimise käigus leiti mitmeid asutusi, kus oli küll vastav link olemas, kuid see ei juhatanud veebilehele, kus oleks palgaandmed avalikud, vaid juhatas veebilehele, kus avalikustatakse avaliku sektori tööpakkumisi, mida ei saa kuidagi lugeda nõuetekohaseks avaliku teabe juurde juhatamiseks. Seega tuleks asutustel üle kontrollida ka lingid kuhu need juhatavad.

Kolmandaks vaatasime riigihangetega seotud teabe avalikustamist, sh seda, kas on leitavad hankeplaan ja hankekord. Kui enamikel asutustel on riigihanked avalikustatud riigihangete registris ning link sellele lisatud, siis oli ka mõni asutus, kellel link puudus või ei töötanud kontrollimise ajal. Halvem oli lugu hankekorra ja hankeplaani avalikustamisega, kus mitmelgi juhul ei olnud vastavad dokumendid leitavad. Mõnede asutuste puhul kelle riigihanked korraldab Riigi Tugiteenuste Keskus (RTK), oli märges, et hankeplaan leitav RTK hankeplaanist ning lisatud ka link, mis viis küll RTK veebilehele, kuid mitte sellele veebilehele, kus oleks vastav teave, vaid teavet tuli hakata RTK veebilehelt otsima. Selline viitamine ei täida oma eesmärki, seda enam, et avaliku teabe seaduse üheks põhimõtteks on ka see, et teabe leidmine peab olema lihtne.

Seirete käigus vaadati ka asutuste dokumendiregistreid, mis aasta-aastalt pakub avalikkusele järjest enam huvi. Seire käigus jäi silma, et dokumendiregistrites on jätkuvalt palju dokumente, millele ei ole kehtestatud juurdepääsupiirangut, kuid millele ei võimaldata ka dokumendiregistri kaudu juurdepääsu.

Kuigi seire käigus ei ole võimalik anda konkreetset hinnangut dokumentidele kehtestatud piirangute õiguspärasuse osas, hakkab silma, et dokumendiregistrites on näiteks palju kirjavahetust juriidiliste isikute vahel, millele on kehtestatud piirang eraelu kaitseks (AvTS § 35 lg 1 p 12). Samuti hakkas silma dokumentide rohkus, millel oli piirang ärisaladuse kaitse (AvTS § 35 lg 1 p 17) ning üllatavalt palju oli dokumente, millel oli kehtestatud piirang AvTS § 35 lg 2 p 2 ehk peaks olema dokumendi kavand või sinna juurde kuuluvad dokumendid. Seda ka kirjade ja taotluste puhul. Siinkohal tahaks juhtida asutuste tähelepanu sellele, et iga pöördumine, mis eeldab vastust või otsuse tegemist ei ole alati dokumendi kavand ega sinna juurde kuuluv dokument. Selleks, et dokumendile kehtestada juurdepääsupiirang peab eksisteerima põhjendatud vajadus. Igaks juhuks piirangute kehtestamine ei ole lubatud.

Andmekaitse Inspeksioon on teadlik, et dokumendiregistrites on väga palju dokumente, millel on piirang lõppenud, kuid mis ei ole avalikud. Eelkõige on sellisteks dokumentideks järelevalvealased dokumendid, mille osas menetlus on lõppenud ja otsused jõustunud. Probleem on selles, et kuna avaliku teabe seadus jõustus 20 aastat tagasi, siis on see üsna paberkandjal dokumenti-

de keskne ning ei arvesta alati digitaalselt koostatud dokumentidega. Samuti oli 2001. aastal dokumentide maht oluliselt väiksem, kui käesoleval ajal, ning paberdokumentidele ei võimaldatud ka dokumendiregistri kaudu juurdepääsu. Seega on seadus jäänud ka ajale n-ö jalgu.

Nii näiteks kohustab AvTS § 42 tunnistama juurdepääsupiirangu kehtetuks, kui selle kehtestamise põhjus on kadunud ning tegema dokumendile selle kohta märke. Kui paberkandjal oleva ja omakäelselt allkirjastatud dokumendi puhul see probleemi ei tekita, siis digitaalselt allkirjastatud dokumendile ei ole võimalik sellist märget teha. Ka ei võimalda kõik dokumendiregistrid teha sellist märget dokumendiregistri metaandmetes. Kui tunnistada piirang enne lõpptähtaega kehtetuks ilma vastavat märget dokumendile tegemata ja see avalikustada, siis pole enam arusaadav, kas dokumendiregistris avalikustatakse piiranguga teavet või on dokumendi piirang tunnistatud kehtetuks.

Loomulikult on võimalik võtta ka need dokumendid digikonteinerist välja, eemalda piirang (tunnistada see kehtetuks) ja dokument uuesti üles laadida, kuid sellised toimingud on väga mahukad ning asutustel paraku sellist ressursi ei ole. Muidugi on Andmekaitse Inspeksioonil õigus teha igale teabevaldajale eraldi ettekirjutus seaduse täitmiseks küsimata, kas ja mil moel on ettekirjutus täidetav, kuid kuna see puudutab sisuliselt kõiki teabevaldajaid, siis on inspeksiooni hinnangul mõistlik leida kõiki rahuldav lahendus, mitte tegeleda iga teabevaldajaga eraldi, kas siis seaduse muutmise või täiendavate tehnoloogiliste lahenduste teel.

Ettekirjutuste tegemise korral ei ole asutustel töömahukuse tõttu võimalik lahendada probleemi mõistliku aja jooksul, kuna see eeldab suurte asutuste puhul dokumendihalduritelt täiendavalt igapäevase töö kõrvalt kümnete või sadade tuhandete dokumentide üle vaatamist ja piirangute hindamist. See ei tähenda siiski seda, et inspeksioon eeltoodud probleemiga ei tegeleks. Lahenduste leidmiseks on pöördutud ka Majandus- ja Kommunikatsiooniministeeriumi ja Justiitsministeeriumi poole, kuid kiiret lahendust hetkel ei ole.

Lisaks hakkas dokumendiregistris silma, et mõne asutuse dokumendiregistrist ei ole leitavad preemiade ja lisatasude maksmise käskkirjad või neile kehtestatud juurdepääsupiirangud, kas AvTS § 35 lg 1 p 12 alusel või TLS § 28 lg 2 p 13 alusel. Mõnel juhul võib AvTS § 35 lg 1 p 12 alusel piirangu kehtestamine olla põhjendatud, kui tasu maksmine on seotud mõne eraelu puudutava sündmusega. Kui aga enamik käskkirju on piiranguga eraelu kaitseks, siis ei ole usutav, et kõik need dokumendid sisaldaksid kellegi eraelu puudutavaid andmeid. Lisaks ei luba AvTS § 36 lg 1 p 9 kehtestada piirangut ka töölepinguga töötajatele makstud tasudele, kui tasu makstase eelarvelistest vahenditest. See, et eelarvest makstud vahendite osas on avaliku teabe seadus eriseaduseks töölepinguseaduse § 28 lg 2 p 13 suhtes, sellisele seisukohale on asunud ka kohus. Tõsi küll, seda kohalike omavalitsuste töölepinguga töötavate isikute osas, kuid peale seda muutis seadusandja ka avaliku teabe seadust vastavalt, et ka töölepinguga töötavatele isikutele eelarvest makstavatele tasudele ei tohi kehtestada piirangut, mistõttu peavad need käskkirjad olema dokumendiregistris avalikud.

Ka ei saa osade asutuste puhul rahul olla dokumendiregistris metaandmete avalikustamisega. Tihti on need poolikud ja pole arusaadav, kellelt on dokument laekunud, kellele väljastatud või kellele täitmiseks suunatud ja milline on vastamise tähtaeg. Samas leidub dokumendiregistris ka dokumente, kus on füüsiliste isikute nimed avalikud. Samas pole arusaadav, kas tegemist on juriidilise isiku esindajaga või füüsilise isikuga. Seega tuleks asutustel oma dokumendiregistri välisvaated kriitilise pilguga üle vaadata.

Teabenõue

Kui avaliku teabe küsimine on igaühe õigus, siis tuleks seda õigust kasutada ka vastutustundlikult. Aasta-aastalt on üha rohkem selliseid kodanikke, kes esitavad hulgaliselt teabenõudeid kõikvõimaliku teabe saamiseks, sh korduvalt ning leiavad, et neile tuleb vastata viivitamata. Siin peaks iga teabenõudja arvestama sellega, et ta ei ole ainus inimene, kes teavet soovib/vajab ning asutusel on ka muid kohustusi ja ülesandeid.

Eeltoodu ei tähenda seda, et asutused ei peaks tähtaegselt teabenõuetele vastama. Ei ole sugugi haruldane, kui keeldutakse teabenõude täitmisest põhjusel, et teabevaldaja ei pea põhjendatuks teabe väljastamist või teabele kehtivad juurdepääsupiirangud viitamata ühelegi piirangu alusele. Teabevaldajad saavad siiski keelduda teabe väljastamisest ainult juhul, kui keeldumiseks on seadusest tulenev alus ning ei saa siin otsustada, kas teabe küsimine on põhjendatud või mitte. See, kui dokumendid sisaldavad mingis osas piiranguga teavet, ei tähenda seda, et selliseid dokumente teabenõude korral ei väljastata. Sellisel juhul tuleb väljastada see osa

teabest või dokumendist, millele piirangud ei laiene (AvTS § 38 lg 2). Samale seisukohale on asunud ka Riigikohus asjas 3-3-1-57-03.

Jätakuvalt on ka üheks levinumaks rikkumiseks teabenõuetele vastamisel, teabenõudele tähtaegselt vastamata jätmine. Ka juhul kui kodanik on pealkirjastanud oma pöördumise „Teabenõudena“, kuid sisult on tegemist selgitustaotlusega, tuleb sellisele pöördumisele vastata viie tööpäeva jooksul, keeldudes teabenõude täitmisest ja selgitada, et tegemist on selgitustaotlusega. Kodanik ei pea teadma, millal on tema pöördumise puhul tegemist selgitustaotlusega ja millal teabenõudega. Küll aga peab seda teadma teabevaldaja. Kuigi eeltoodud probleemist on aastaid räägitud, on see jätkuvalt kõige suurem vaiete esitamise põhjus.

Enne teabenõuetele vastamist soovitan teabevaldajatel teabenõuded tähelepanelikult läbi lugeda, et ei jääks midagi tähelepanuta. Vaadata üle kas dokument sisaldab piiranguga andmeid, kas piirangud on kehtivad või lõppenud ja kas piirangu alused on õiged. Keeldumise korral tuleb alati ka keeldumist põhjendada, sest isikul peab olema arusaadav, miks talle soovitud teavet ei väljastata. Alati tuleks hinnata ka seda, kuidas teised kirjapandust aru saavad, seda nii teabenõuete kui ka nende vastuste puhul.

Vaiete esitamine

Äärmiselt kahetsusväärne on ka, kui püütakse omavahelisi tülisid lahendada Andmekaitse Inspeksiooni kaudu. Üheks selliseks näiteks võib tuua isiku tüli ühe spordiklubi töötajaga, kus isik leidis, et treener on määratud isolatsiooni juhi otsusega ilma õigusliku aluseta. Kui ühelt poolt soovis vaide esitaja tõendeid treeneri isolatsiooni määramise kohta, siis teisalt leidis, et avalikustatud on piiranguga teavet treeneri terviseandmete osas ning soovis spordiklubi töötaja karistamist. Asja tegi ka segasemaks see, et Terviseamet andis vaide esitajale eksitavat teavet, kinnitades vaide esitajale, et Terviseamet ei ole treenerit isolatsiooni määranud, mis aga ei vastanud tõele. Kuna menetluse käigus selgus, et spordiklubi töötaja ei ole vaide esitajale edastanud ebaõiget teavet ning treener oli teadlik sellest, et treeningul osalejaid teavitati tema isolatsiooni kohustusest, siis jäi vaie rahuldamata.

Samuti on äärmiselt kahetsusväärne, kui riigi või kohaliku omavalitsuse äriühingud ei tea, kas ja milliseid avalikke ülesandeid nad täidavad ning millised ülesanded ja kuidas on neile üle antud. Andmekaitse Inspeksiooni menetluses oli kodaniku vaie, kus ta soovis omavalitsuse äriühingult teavet ettevõtte poolt tellitud tööde ja teenuste osas, mida on finantseeritud omavalitsuse vahenditest. Omavalitsuse äriühing oli seisukohal, et ta ei täida avalikke ülesandeid ega ole ka teabevaldaja, mistõttu ei ole tal ka kohustus teavet väljastada. Vaidemenetluse käigus selgus, et antud juhul oli kohalik omavalitsus andnud oma äriühingule volitused, korraldada sadama kinnistu territooriumile moodulhoonete hankimine ja paigaldamine ja näinud selleks ka ette kulude katmise valla eelarvest äriühingu poolt esi-

tatud arvete alusel. Ühistranspordiseaduse § 11 lg 1 loetleb ühistransporditaristu objektid, milleks on ka reisiterminal, sadam, kai, ootekoda ja muud liiki rajatised ning seadmed ja nende teenindamiseks ettenähtud või vajalik inventar. Sama seaduse § 13 lg 1 p 4 kohaselt korraldab omavalitsusorgan oma territooriumil ühistranspordi taristu objektide rajamist, korrashoidu ja kasutamist. Eeltoodud paragrahvis loetletud omavalitsusorgani ülesannete täitja ja täitmise korra, kui need ei ole sätestatud käesoleva seaduse teistes paragrahvides, määrab kindlaks valla- või linnavolikogu või tema volitusel valla- või linnavalitsus. Seega on sadamarajatiste ehitamine ja korrashoid valla seadusest tulenev ülesanne ehk avalik ülesanne, mida võib täita vald ise või anda see üle mõnele eraõiguslikule juriidilisele isikule. Seega oli vallavalitsus andnud oma korraldusega äriühingule üle vallale seadusest tuleneva ülesande, mistõttu oli äriühing selles osas teabevaldjaks. Inspeksioon tegi äriühingule ettekirjutuse väljastada vaide esitajale tema poolt soovitud teave, mis puudutab äriühingu poolt avalike ülesannete täitmist ja selleks saadud avaliku raha kasutamist.

On äärmiselt kahetsusväärne kui teabevaldajad ei tea, milline nende valduses olev teave on avalik teave. See ei ole ainult see teave, mis on registreeritud dokumendiregistris, vaid kogu asutuse valduses olev teave, mis on loodud ja saadud avalikke ülesandeid täites. Näiteks leidis üks vallavalitsus, et arve ja maksekorraldus ei ole avalik teave AvTS § 3 mõistes. Arve on raamatupidamislik algdokument ning maksekorraldus makse teostamist tõendav dokument. Eelnimetatud dokumendid ei vasta avaliku teabe mõistele ning ei ole käsitletavad avaliku teabena. AvTS § 12 lõikest 2 lähtudes, Kehtna Vallavalitsuse dokumendiregistris raama-

tupidamisdokumente ja maksekorraldusi ei registreerita. Raamatupidamisdokumendid on sisemised töödokumendid.

Andmekaitse Inspeksioon eeltooduga ei nõustunud. Kuigi AvTS § 12 lõige 2 sätestab, et raamatupidamisdokumente ei pea dokumendiregistris registreerima, ei tähenda see, et tegemist pole avaliku teabega. Lihtsalt nende suhtes ei kehti dokumendiregistrisse kandmise kohustust (AvTS § 12 lg 2). Ka raamatupidamisdokumendid on avalik teave, neid saab küsida teabenõudega ning teabevaldaja peab need väljastama juurdepääsupiiranguteta osas nagu muugi avaliku teabe. Samuti olid teabenõudes küsitud arved ja maksekorraldused seotud lepinguga, mille eest tasub vald ning valla raha kasutamise seotud teavet ei saa tulenevalt AvTS § 36 lg 1 punktist 9 salastada.

Kokkuvõte

Kuigi asutuste veebilehed on muutunud palju kenamaks ja pilkupüüdvamaks, on tihti veebilehtedelt teabe leidmine muutunud ka keerulisemaks. Kui asutuse pakutavate teenuste kohta on teave enamasti leitav, siis avaliku teabe seaduse §-s 28 loetletud teavet on märksa keerulisem leida. Tihti nõuab üsna suurt vaeva ja leidlikust, et leida üles töötajate kontaktid, mis peaksid olema kergesti leitavad. Samuti on tihti keeruline leida nii ametijuhendeid kui ka ametnike haridust ja eriala tõendavaid dokumente.





On ka asutusi, kus on dokumendiregistrit keeruline leida – ka see peaks olema lihtsasti leitav. Kui teate, et teie asutusel on kogu kohustulikult avalikustatav teave veebilehel olemas, minge proovige seda veebilehe avalikust vaatest leida. See ei pruugi olla niisama lihtne. Mõelge ka sellele, et teile kui veebilehe omanikule on teada, millise loogika järgi on veebileht üles ehitatud. Kolmas isik, kes seda ei tea, ei pruugi teavet sama lihtsalt leida.

Kui oleme selle kohta mõnele asutusele märkuse teinud, on tihti vastuseks, et ka teiste asutuste veebilehel on teave samamoodi avalikustatud või dokumendiregistris kõik samalaadsed dokumendi piirangud (nt lisatasu käskkirjad). Selline vastus on üllatav, kuna oma eksimust ei peaks põhjendama teiste asutuste eksimustega, vaid püüdma just oma teabe kättesaadavust parandada ja olla nii ka teistele eeskujuks. Soovime teabevaldajatele tähelepanu, tarkust ja jõudu avalikule teabele juurdepääsu võimaldamisel, et see, mis peab olema avalik, oleks kõigile lihtsalt leitav ja kättesaadav. Teave, mis peab olema piiranguga, oleks turvaliselt kaitstud.

Õigusloome, kohtupraktika ja väärteomenetlused

AKI (Andmekaitse Inspektsioon) kontrollib arvamuse avaldamiseks saadetud eelnõude puhul eelkõige isikuandmete töötlemisega seonduvat, sh eelnõu kooskõla isikuandmete kaitse üldmääruse (IKÜM) nõuetega, aga ka laiemalt põhiseaduspärasust.

IKÜM näeb siseriiklikule õigusaktile, millega reguleeritakse isikuandmete töötlemine, ette rea tingimusi: õigusakt peab olema selge ja konkreetne, proportsionaalne ning eriliigiliste isikuandmete puhul nägema ette ka täiendavad kaitsemeetmed andmesubjektide õiguste kaitsmiseks – need peaksid olema midagi lisaks IKÜM-i kohustuslikele nõuetele. Näiteks võib täiendav kaitsemeetode olla andmete väga lühike säilitustähtaeg. Ulatusliku andmetöötlemise puhul peab seletuskirjas sisalduma ka IKÜM-i tingimustele vastav mõjuhindang.

Meie enda põhiseaduse § 26 näeb ette, et isikuandmete töötlemine kui eraelu puutumatuse põhiõigust riivav tegevus peab olema ette nähtud seaduse tasemel. Vähemasti peab olema seaduse tasemel ette antud kindel raam, mida alamate aktidega täpsemalt sisustada. Andmekaitse vaatest tähendab see kindlasti seaduse tasemel isikuandmete töötlemise eesmärgi, üldise andmekoosseisu ja andmete säilitamise maksimaalse tähtsaja paika panemist. IKÜM ei kohusta isikuandmete töötlemist seaduse tasandil reguleerima, seega Euroopa määrust ei saa selles küsimuses jäikuses süüdistada.

Ent praktikas kohtab tihti norme, kus reguleeritakse lakooniliselt, et see ja see asutus võib oma ülesannete täitmiseks töödelda isikuandmeid, sh eriliigilisi isikuandmeid, täpsustamata konkreetsemat eesmärki, andmekoosseisu või säilitamise tähtaega. Sama kohtab ka volitusedes, millega luuakse andmekogusid. Näiteks sõnastuses, et andmeid säilitatakse 50 aastat, kui põhimääruses ei sätestata teisiti, annab Riigikogu valitsusele või ministrile õiguse andmeid säilitada kas või tähtsajalt. Pahatihti eelnõude väljatöötajad AKI vaadet sätete konkreetsuse vajadusest ei jaga. Leitakse, et täpsema regulatsiooni saab paika panna määruste tasandil. Nii see on, aga asjata ei ole põhiseadus andnud oluliste küsimuste, sh eraelu puutumatuse reguleerimise õigust Riigikogule. Riigikogu menetluses saavad küsimused oluliselt suurema avalikkuse tähelepanu ja arutelu osaliseks. Samuti peab arvestama võimalusega, et ühel hetkel ei pruugi valitsus või mõni minister olla põhiõiguste ja vabaduste poolel ning selliseks puhuks ei tohiks neil olla lihtsat võimalust olulisi küsimusi Riigikoguta otsustada.

Positiivne on, et Justiitsministeerium on võtnud andmekogude teema analüüsida ja loonud andmekogude reguleerimise osas põhjalikud selgitused ja soovitusel – neil on käsitletud ka AKI muresid ja ettepanekuid.

2021. sai nii avalikkuselt kui ka AKI-lt palju tähelepanu nakkushaiguste ennetamise ja tõrje seadus (NETS) ning sellega seotult nakkushaiguste registri põhimääruse muudatused. Andmekogusse sooviti

koguda kõigi positiivse COVID-i testi andnute, vakt-sineeritute ja läbipõdenute andmed koos mh tööko-ha, sotsiaalmajandusliku seisundi jms andmetega ning säilitada need andmed tähtajatult. Sisuliselt oleks sinna sattunud kogu elanikkonna andmed. Kõike seda lubati väga üldsõnalise andmekogu re-guleeriva volitusnormiga, mis jättis taas täidesaat-vale võimule andmekoosseisus ja säilitustähtjas vabad käed. NETS-i muudatusi sellisel kujul siiski Riigikogus vastu ei võetud, tõsi küll, seda muudel põhjendustel.

Üldsuse ja AKI tähelepanu sai ka ABIS-e ehk au-tomaatse biomeetrilise isikutuvastuse süsteemi andmekogu loomise eelnõu, mis Riigikogus sea-dusena ka vastu võeti. Sellega loodi uus andmeko-gu, mis koondab kokku riigi kogutud biomeetrilised andmed, sh isikut tõendava dokumendi taotlemi-sel esitatud biomeetrilised andmed. Erakordne on, et andmekogu loomise volitusnorm sisaldub aga 13 seaduses. Murekoht oli ka selles, et ühe and-mekoguna luuakse süsteem, mida kasutavad eri otstarveteks eri asutused ning ei olnud arusaadav, kuidas tagatakse, et iga asutus saab vaid oma ülesannete jaoks vajalike andmete juurde. Ka and-mekogu põhimääruse sätted olid raskesti jälgita-vad, näiteks andmekoosseisud viitasid omakorda vastavale seadusele nii, et andmekoosseisust üle-vaate saamiseks tulnuks korraga avada põhimää-rus ja 13 seadust, mille alusel andmekogu loodi. AKI aitas põhimääruses selgemalt reguleerida andmekogu vastutava ja volitatud töötleja kohus-tused ja ülesanded, sh selle, et andmesubjektide jaoks oleks selgeks kontaktpunktiks PPA, mit-

te asutus, mis parasjagu andmeid töötles – see oleks inimesele ja isegi juristile liiga keeruline välja selgitada. Samuti aitas AKI selgemalt reguleerida PPA kui vastutava töötleja kontrollimise kohustu-se volitatud töötlejate tegevuse üle. ABIS-s nägi murekohti, sh õigusselguses, ka õiguskantsler, kes moodustas oma kantseleis eraldi töögrupi seadu-se põhiseaduspärasust analüüsima.

Kahtlemata oli üle-eelmisel aastal erakordne ja enneolematu koroonapasside kasutusele võtmine. Algselt olid koroonapassid ju väljamõeldud eelkõi-ge reisimiseks. Ka Euroopa Liidu määrus passide kasutusele võtmise kohta reguleeris just reisimise otstarvet. Euroopa Andmekaitse Nõukogus tuli ise-gi erakorralisele hääletusele küsimus, kas üldse lu-bada koroonapasse ka riigisiseseks kasutamiseks – osa riike nõudsid seda tungival. Nagu tagantjäre-le teame, tulidki koroonapassid ka riigisiselt laia-ulatuslikult kasutusele. Eestis sätestati kohustus koroonapasse kontrollida valitsuse korraldusega – nagu ka muud koroonapiirangud. Sel moel ula-tuslike ja pikaajaliste piirangute seadmine üldkorral-dusega pälvis mitme tunnustatud juristi kriitika. Ka AKI mure oli, et sellist voli ei anna valitsusele otse-sõnu ükski seadus. Nüüdseks on küsimust lahanud mitu kohtuastet.

Kuivõrd koroonapasside andmete puhul (va negatiivne test) on kindlasti tegemist terviseandmetega, mis on eriliigilised isikuandmed, oli IKÜM-i vaatest oluline, et norm, millega passide kontrollimise kohustus seati, sisaldaks ka inimesi kaitsvaid meetmeid. Seetõttu soovitas AKI normiga selgelt keelata koroonapasside kontrollimise järgse andmete säilitamise, va inimese vabatahtlikul nõusolekul. Hea meel oli selle üle, et TEHIK lõi kiiresti passide kontrollimise lahenduse, mis loodetavasti hoidis ära selle, et passe oleks kontrollitud välismaiste rakedustega, mille puhul polnuks teada, kas ja mida rakendus skaneeritud passide andmetega edasi teeb.

Segadust tekitas ka koolides kiirtestimise kasutuselevõtt. Andmekaitse vaatest oli selgusetu, mis õiguslikul alusel õpilaste terviseandmeid töödeldakse. Tõsi, lapsed testisid end ise, kuid siiski ühiselt koos klassiruumis ning positiivse testi andnu ei jäänud ju saladuseks. Samuti oli teadmata, kas ja kellele positiivse testi andnud õpilase andmed edastatakse. Haridus- ja Teadusministeerium oli seisukohal, et kiirtestimine on vabatahtlik ja andmete töötlus toimub seega nõusoleku alusel. Paraku ei täpsustanud ministeerium teadliku nõusoleku andmise eelduseks olevaid olulisi asjaolusid – andmete koosseis, säilitamise tähtaeg ja andmeid töötlevate isikute ja asutuste ring. Positiivne areng oli kiirtestide lastele koju kaasa andmine ja seega kodus privaatselt testimise võimaluse loomine.

Andmekaitse vaatest valmistas probleeme ka ministeeriumi väljatöötatud nõusolekuvorm õpilaste vaktsineerimiseks ja testimiseks, neis küsiti

põhjendamatult ülemääraseid andmeid, nt põhjust vaktsineerimisest keeldumiseks. Kokkuvõttes oleks saanud koolides kiirtestimise ja vaktsineerimisega seotud andmekaitselisi küsimusi lahendada kiiremini ja selgemalt, kui AKI oleks nende tegevuste ettevalmistamise faasi kaasatud olnud.

Tegelikult peab igas riigi- ja kohaliku omavalituse asutuses töötama andmekaitse-spetsialist, kes peaks nõustama ja suunama eelnõude koostamisel ja arvestama tegevuste planeerimisel andmekaitse nõuetega.

Paraku näib reaalsus olema selline, et andmekaitse spetsialistidel kas ei ole piisavalt teadmisi ja kogemusi või, mis on tõenäolisem, neid ei kaasata otsustamise protsessi. Reeglina teevad nad andmekaitse spetsialisti tööd muude ülesannete kõrvalt ja pahatihti tekib neil ka kohustuste konflikt – näiteks oodatakse poliitilisel tasandil, et eelnõu kiiresti valmiks ning juhtkonna tasandil ei soosita või mõisteta andmekaitse peensustele tähelepanu pühendamist.

Avaliku teabe suunalt tulid suuremad muudatused avaliku teabe seaduse (AvTS) muutmisest endast. Esiteks anti veebilehtede juurdepääsetavuse kontrollimine üle AKI-lt Tarbijakaitse ja Tehnilise Järelevalve Ametile, kuivõrd neil on selleks parem tehniline valmisolek.

Teiseks võeti AvTS-i üle avaandmete ja avaliku teabe taaskasutamise direktiiv, millega reguleeriti mh väärtuslike andmetike mõiste, aga ka deklareeriti, et üldjuhul tuleb avaandmed teha kättesaadavaks tasuta ja tingimusteta, va kui kättesaadavaks tegemise viiside piiramiseks on avalik huvi. Selle muudatusega käis kaasas ka avaandmete mõiste sisustamise muudatus – kui seni oli valdav arusaam, ka AKI-l, et avaandmeteks on andmed, mille asutus on avaandmetena määratlenud, siis nüüd selgitas Justiitsministeerium, et avaandmeteks on siiski automaatselt kogu avalik teave, va juurdepääsupiiranguga andmed. See tähendab, et avaandmeteks on ka isikuandmed, mis on seaduse alusel avalikult kättesaadavaks tehtud, nt äriregistris juriidiliste isikute juhatuse liikmete andmed ja kinnistusraamatus kinnistuomanike andmed. Samas selgitas ministeerium, et ka avaandmeteks olevate isikuandmete taaskasutamiseks, sh allalaadimiseks on vaja IKÜM-st tulenevat õiguslikku alust.

Märkimist väärrib ka Justiitsministeeriumi juba 2018. a kujundatud ning 2021. aastal üle kinnitatud seisukoht, et ettekirjutusi, mille AKI on teinud riigiasutustele, ei saa vaidlustada vabariigi valitsuse seaduse alusel ehk viisil, kus asjaomased ministrid lahendavad AKI ja teise riigiasutuse õigusvaidluse. Seetõttu on riigiasutustel nüüd ainuke võimalus AKI ettekirjutusega mitte nõustudes teatada ettekirjutuse täitmata jätmisest. Seejärel saab AKI 30 päeva jooksul pöörduda protestiga halduskohtusse. 2021. aasta AKI esimesed protestid halduskohtusse ka esitas.

Kohtupraktika

2020. lõpus tegi AKI e-apteekidele ettekirjutuse lõpetada pelgalt isikukoodi alusel inimeste retseptiandmete kuvamine. Sisuliselt võis e-apteegis segamatult kasvõi peaministri retseptide loeteluga tutvuda. Eestis on ju isikukoodid kergesti avalikest allikatest leitavad. Üks e-apteek vaidlustas AKI ettekirjutuse kohtus. Halduskohtus leidis, et AKI ettekirjutus oli õiguspärane, sest isikukoodi alusel isikuandmete avaldamiseks puudus e-apteekidel õiguslik alus, sest sellist alust siseriiklikus õiguses olemas ei ole ja muud õiguslikud alused kõne alla ei tule. Aptek vaidlustas otsuse ringkonnakohtus, kuid loobus menetluse kestel kaebusest. Loobumine oli suuresti tingitud sellest, et pärast pooleaastast Sotsiaalministeeriumi ja selle allasutuste, õiguskantsleri, Riigikogu sotsiaalkomisjoni ja AKI koostööd loodi retseptikeskusesse võimalus kontrollida rahvastikuregistrist seaduslike esindajate andmeid ehk retseptiandmetele said õiguspäraselt ligi seaduslikud esindajad, eelkõige lapsevanemad, aga ka täisealistele määratud eestkostjad. Lisaks muudeti digiloos teise inimese volitamine enda retseptide väljaostmiseks lihtsamaks ja leitavamaks.

2021. aastal jõudis lõpptulemuseni kohtuvaidlus, kus ettevõtte, kes jättis tähtjaks täitmata AKI ettekirjutuse IKÜM-ile vastavate andmekaitsetingimuste avaldamiseks oma kodulehel, vaidlustas AKI sunniraha määramise teate ning taotles esialgset õiguskaitset sunniraha sissenõudmise keelamiseks. Halduskohus ei näinud esialgse õiguskaitse vajadust, ringkonnakohus oli vastupidisel seisukohal ning Riigikohus leidis, et vaidluse ese oli kohtumenetluse ajal paisunud liiga laiaks. Nimelt oli kohtumenetluse käigus kujunenud olukord, kus ringkonnakohus keelas esialgse õiguskaitsega menetluse ajal AKI-l sunniraha täitmisele pöörata ning kohustas AKI-t kontrollima ettekirjutuse täidetust. Kusjuures samal ajal täiendas ettevõtte AKI-lt saadud tagasiside alusel oma andmekaitsetingimusi kuni need olid nõuetele vastavad ja seega ka ettekirjutus täidetud.

Täidetud ettekirjutuse puhul aga enam sunniraha sisse nõuda ei saa. Kuna kohtumenetluse jooksul ettevõtte AKI abiga ettekirjutuse täitis, siis rahuldaski ringkonnakohus ettevõtte kaebuse sunniraha sissenõudmise keelamiseks ning jättis menetluskulud AKI kanda. Sisuliselt saavutas ettevõtte olukorra, kus AKI aitas tal koostada andmekaitsetingimused ja maksis ettevõttele selle eest veel peale. Riigikohus toonitas, et edaspidi ei tohi lasta kujuneda olukorral, kus terve kohtumenetluse ajaks keelatakse AKI-l sunniraha sissenõudmine. See kohtuvaidlus tõi esile nõrgad kohad sunniraha mehhanismi rakedamisel, mh küsimuse, kui detailselt peab AKI oma ettekirjutuses korrektsete andmekaitsetingimuste loomist selgitama – sellest oleneb omakorda ettekirjutuse täidetuse hindamise võimalikkus ja sellest

omakorda sunniraha määramise õigus. AKI ettekirjutused ei saa reeglina olla lihtsakoelise resolutsiooniga nagu seda võib olla näiteks kergesti kontrollitav kohustus hoone lammutada vms. Enamasti on ettevõtetel puudulikud või olematud andmekaitsetingimused, õigustatud huvi analüüs või mõjuhinnaang. Ettekirjutust luua andmekaitsetingimused ei saa ju lugeda täidetuks pelgalt siis, kui koostatud on dokument pealkirjaga „Andmekaitsetingimused“, vaid ka selle sisu peab vastama IKÜM-iga seatud andmekaitsetingimuste nõuetele. Seda peab aga AKI eraldi hindama ning AKI ja ettevõtte arusaamad näiteks õigustatud huvi analüüsi põhjalikkusest võivad suuresti erineda.

2021. aastal tegi ringkonnakohus ka lahendi, kus leidis, et AKI ei saa jätta järelevalvemenetlust alustamata põhjusel, et väidetav isikuandmete töötlemise nõuete rikkumine on leidnud aset kohtumenetluse käigus, täpsemalt olukorras, kus üks kohtumenetluse pool on tõenditena esitanud teise menetlusosalise isikuandmeid. IKÜM-i preambulis aga tõdetakse, et järelevalveasutused ei peaks järelevalvet tegema olukorras, kus kohtud täidavad oma õigust mõistvat funktsiooni. Kuivõrd AKI-t kasutatakse tihti n-ö käitemaksukontorina endise tööandja, eksabikaasa või muule ebasümpaatsele isikule AKI järelevalvega ebaseadmiseliste valmistemiseks, annaks ringkonnakohtu tõlgendus AKI järelevalvepädevusest kohtumenetluses sellisele tegevusele veelgi hoogu juurde. Kui mõelda näiteks perekonnavaidluste peale, kus kohtumenetluse osapooltel on reeglina niigi väga teravad suhted ja vaidluse lahendamine eeldab ka üksteise

isikuandmete tõenditena esitamist, siis kindlasti leiavad vaenutsevate poolte kaebused tee ka AKI-ni. Asja võttis menetleda ka Riigikohus, kes jõudis järeldusele, et AKI-l ei ole järelevalvepädevust kohtu tegevuse üle isikuandmete töötlemisel, kuid on pädevus menetlusosaliste üle, kes omal algatusel esitavad kohtumenetluses isikuandmeid. AKI järelevalvepädevust menetlusosaliste üle ei välista ka asjaolu, et kohtul on kohustus hinnata tõendi lubatavust. Seejuures peab AKI Riigikohtu hinnangul silmas pidama keeldu sekkuda õigusemõistmisse ehk järelevalvemenetluse tulemusel ei saa ettekirjutusega kohustada andmetöötlejat võtma meetmeid, mille rakendamine sõltub kohtuasja lahendava kohtu seisukohast.

Riigikohus muutis ka AKI senist käsitlust teabenõudest kui sellisest. Nimelt on AKI seni olnud seisukohal, et teabenõude korras saab küsida konkreetset olemasolevat dokumenti. Kui küsitud teave tuleb alles kokku koguda, on tegemist selgitustaotlusega. Riigikohus aga leidis, et teabenõude korras tuleks välja anda ka selline teave, mida on võimalik kerge vaevaga välja selgitada, näiteks vangla töötajate aasta keskmine töötasu.

2022. aastal tegi AKI mitmed ettekirjutused infoportaalide pidajatele, kes kasutavad äriregistri andmeid ja lisavad juurde täiendavaid andmeid – nt juhatuse liikme iseloomustusi. Arvestades, et enamik infoportaale on kõigile avalikud ja tasuta kättesaadavad, on juhatuse liikmete kui andmesubjektide suhtes ülemäära kahjustav kui avali-

kustatakse ka andmeid, mis ei ole otseses puutumuses nende äritegevusega. Enamik ettekirjutuse saanud infoportaale vaidlustas AKI ettekirjutuse kohtus. 2022. aasta lõpuks oli halduskohus põhilistes küsimustes AKI ettekirjutused jõusse jätanud, kuid mitme ettekirjutuse osas jätkub vaidlus 2023. aastal ringkonnakohtus.

Lisaks tegi AKI ettekirjutuse ühele maksehäireregistri pidajale, kes avaldab füüsiliste isikute maksehäire andmeid isikutele, kes väidavad endal selleks õigustatud huvi olema. Iseenesest näeb nii IKÜM õigustatud huvi näol kui isikuandmete kaitse seadus ette võimaluse inimese krediitvõimekuse hindamise eesmärgil maksehäireid koguda ja kolmandatele isikutele avaldada. AKI ettekirjutus oli suunatud eelkõige viisidele, kuidas maksehäireregister andmeid kogub ja avaldab. AKI on seisukohal, et register peab kontrollima talle võlausaldaja poolt edastatud võlaandmete õigsust. Lisaks peab register kontrollima, kas andmete pärijatel tööpoolest on õiguspärane põhjendus võlaandmete saamiseks. Et andmekaitseõiguse läbiv põhimõte on läbipaistvus, peab register kontrollima, kas võlausaldaja, kes võlgniku andmed registrile edastab, teavitab sellest tegevusest võlgnikku ja kui ei teavitanud, peab register ise võlgnikku tema andmete saamisest teavitama. Halduskohus nõustus suures osas AKI ettekirjutusega, kuid leidis, et maksehäireregister ei saa ega pea talle edastatud andmete õigsuse kontrollimiseks tutvuma ka võlgnevuse aluseks olevate dokumentidega. Vaidlus jätkub 2023. aastal ringkonnakohtus.

2022. aastal avaldas AKI ka uuendatud maksehäirete avaldamise juhendi, mis avab täpsemalt maksehäirete avaldamise tingimused. Eelkõige ei tohi maksehäirete avaldamine võlgnikku ülemääraselt kahjustada. AKI sisustas juhendiga täpsemalt, mida ülemäärase kahjustamise hindamisel arvesse võtta. Üldreegel on, et kui tegemist on aastate taguse üksiku ja väikese võlaga, on selle maksehäireregistris avaldamine inimest ülemääraselt kahjustav, sest ei iseloomusta adekvaatselt inimese aktuaalset maksekäitumist. Ülemäära kahjustav on, kui inimene ei saa sellise maksehäire avaldamise tõttu laenu või soovitud töökohta.

Maksehäire avaldamise juhend pälvis aga hulgaliselt kriitikat Eesti Pangaliidult ja Finance Estonialt. Arutelud maksehäirete avaldamisest jõudsid ka Justiitsministeeriumisse. Arutelude käigus tõdesid kõik osapooled, et isikuandmete kaitse seaduse § 10, mis maksehäire andmete avalikustamist reguleerib, on mitmeti mõistetav ja vajaks hädasti täpsustamist. Näiteks kuidas sisustada kohustuse rikkumise lõppemise aega – kas see hõlmab ka kohustuse aegumist või tähendab kitsalt kohustuse täitmist? Kui viimast, siis võiks tasumata kuid aegunud võlgu maksehäireregistris avaldada lõpmatuseeni.

2022. aasta alguses tegi AKI ettekirjutuse lõpetada Facebookis eraisikutest võlgnike kohta andmete avalikustamine. Facebookis on rohkesti gruppe, kus hoiatatakse võlgnike ja petturite eest. Reeglina on avalikustajateks eraisikud, kes on teisele eraisikule laenu andnud. Facebookis avalikustatakse võlgniku nimi, kontaktid, pilt ja temaga peetud kirjavahetus. On arusaadav, et Facebookis isikuandmete avalikustamist kasutatakse sunnimeetmena võla tasumiseks. Olgugi, et AKI ei õigusta võlgu jäämist ja vastutustundetut laenamist, ei ole seaduslikku alust võlgnikku asuda avalikult häbimärgistama. Lepingu rikkumise tarvis on õiguskaitsevahendid ette nähtud võlaõigusseaduses. Tõsi, ka isikuandmete kaitse seadus lubab krediitdivõimelisuse hindamise eesmärgil isikuandmeid edastada, aga seda mitte piiramatule isikute ringile, nagu seda tehakse Facebooki avalikes või tuhandetesse ulatuvate liikmete arvuga gruppides. Enne võlaandmete avaldamist tuleb kontrollida, kas andmete saajal on põhjendus võlaandmeid saada. Kontrolli ei saa aga teostada, avaldades andmed piiramatule ringile. Halduskohus nõustus AKI ettekirjutusega. Vaidlus jätkub 2023. aastal ringkonnakohtus.

Kokkuvõttes võib öelda, et peamiselt vaidlustatakse kohtus kas AKI ettekirjutusi või menetluse alustamata jätmisi.

Väärteomenetlused

Palju on olnud erinevaid menetlusi seoses isikuandmete vaatamisega politsei infosüsteemides MIS, KAIRI ja Apollo. Ametnikel on siiski jätkuvalt huvi teiste inimeste või lähedaste vastu. Vaadatakse kontaktandmeid põhjendusel, et ei teata lähedase kontakti. Samuti on tehtud päringuid menetluste kohta, mis ei ole konkreetselt seotud politseiametniku tööülesandega. Üldiselt saavad politseiametnikud aru, et tegemist on rikkumisega, mistõttu on väärteomenetlused lõppenud kiirmenetlusega. Küll aga on erandeid, kus politseiametnik on kindlal seisukohal, et tema ülesanne ongi andmeid infosüsteemis vaadata, mistõttu selliseid menetlusi menetletakse väärteomenetluses üldmenetluse raamides. Inspeksioon on seisukohal, et andmete vaatamiseks peab olema selge alus ja eesmärk ehk see peab olema seotud konkreetse tööülesandega. Ei ole mõeldav, et iga pöördumise peale, milles mainitakse isikute nimesid, teeb ametnik kohe infosüsteemis päringu. See peab toimuma menetluse käigus ning olema eesmärgipärane ja vajalik.



Euroopa Andmekaitseenõukogu olulisemad suunised aastal 2022

Euroopa Andmekaitseenõukogu koostab suuniseid nii isikuandmete kaitse üldmääruse kui ka õiguskaitseasutuste direktiivi paremaks tõlgendamiseks ning praktikate ühtlustamiseks. Euroopa Andmekaitseenõukogu võttis 2022. aastal vastu üheksa suunist, millest seitse suunati huvigruppidele arvamuse avaldamiseks avalikku konsultatsiooni. Suunised on nii andmesubjektidele, -töötajatele, õiguskaitseasutustele kui ka järelevalveasutustele endale.

Aasta alguses võttis andmekaitseenõukogu vastu suunised õigusele oma andmetega tutvuda. Need on eelmise aasta ainsad konkreetselt andmesubjektile suunatud juhised.

Suunistes selgitatakse, et oma andmetega tutvumise õiguse eesmärk on anda üksikisikutele piisavat, läbipaistvat ja kergesti kättesaadavat teavet oma isikuandmete töötlemise kohta, et nad saaksid olla teadlikud töötlemise seaduslikkusest ja töödeldavate andmete täpsusest ning seda kontrollida. See lihtsustab, kuid ei ole tingimuseks, üksikisikul muude õiguste kasutamist, näiteks õigust andmete kustutamisele või parandamisele.

Lisaks täpsustati suunistes, et õigust tutvuda oma andmetega tuleb eristada teistest sarnastest õigustest, millel on teised eesmärgid, näiteks avalikele dokumentidele juurdepääsu õigus. Lisaks

täpsustati suunistes, millistest osadest koosneb õigus tutvuda oma andmetega.

Andmetöötajale olid eelmise aasta suunistest kõige olulisemad isikuandmete kaitse üldmääruse alusel esitatud rikkumisteadete suunised. Suunistes kirjeldatakse, mida tuleks pidada isikuandmetega seotud rikkumiseks ja kuidas saab nimetatud rikkumisi omakorda liigitada. Selgitati, keda ja millal tuleb rikkumisest teavitada ning millised tähtajad järelevalveasutusele teavitamisel kohalduvad. Seoses teavitamisega käsitleti mh, millal saab lugeda, et andmetöötajale on rikkumine teatavaks saanud.

Rikkumisteadete esitamise suunised toovad välja ka ohu hindamise kriteeriumid ja selle, kuidas on mõjuhindanguga võimalik hüpoteetiliselt võimaliku ohu tõrjuda. Lisaks on andmetöötaja kohustus pidada rikkumise kohta sisemist registrit.

2022. aastal avalikku konsultatsiooni jõudnud suunistest oli vaid üks õiguskaitseasutustele mõeldud – suunised näotuvastustehnoloogiate kasutamise kohta õiguskaitseasutustes.

Suunised puudutavad Euroopa Liidu ja liikmesriikide tasandi õigusloojaid ning õiguskaitseasutusi ning nende ametnikke näotuvastustehnoloogiate süsteemide rakendamisel ja kasutamisel.

Suuniste eesmärk on näidata näotuvastustehnoloogiate võimalikke kasutusviise (sh nii 1 : 1 olukordades, aga ka suurtes rahvahulkades) ja kohaldatavat raamistikku õiguskaitse valdkonnas (eelkõige õiguskaitseasutuste direktiivi arvesse võttes). Lisaks pakuvad suunised praktilisi juhiseid õiguskaitseasutustele, kes soovivad hankida ja võtta kasutusele näotuvastustehnoloogiate süsteemi, samuti kirjeldatakse tüüpilisi juhte ja loetakse asjakohaseid kaalutlusi, eelkõige seoses vajalikkuse ja proportsionaalsuse kontrolliga.

Järelevalveasutustele mõeldud haldustrahvide arvutamise suunised said 2022. aastal valmis ja edastati avalikku konsultatsiooni. Haldustrahvide suunised võeti vastu selleks, et ühtlustada metoodikat, mida järelevalveasutused trahvisumma arvutamisel kasutavad. Suunistes selgitatakse andmekaitsekoostöö välja töötatud metoodikat, mille kohaselt koosneb haldustrahvi arvutamine viiest etapist. Lisaks etappidele rõhutatakse suunistes, et trahvi arvutamine ei ole pelgalt matemaatiline tegevus, vaid pigem määravad lõpliku summa, mis võib varieeruda mistahes miinimumsumma ja seadusliku maksimumsumma vahel, konkreetse juhtumi asjaolud.



Euroopa Andmekaitseenõukogu neli strateegilist sammu

2022. aasta aprillis leppisid Euroopa Andmekaitseenõukogu liikmed Viini kohtumisel kokku, et tõhustavad strateegiliste juhtumite puhul veelgi koostööd ja mitmekesistavad kasutatavaid koostöömeetodeid. Rohkem, kui kunagi varem, on praegu oluline tagada isikuandmete kaitse üldmääruse ühetaoline tõlgendamine – et igaühel oleks samad õigused, vaatamata sellele, millises Euroopa Liidu riigis ta elab.

Kohtumisel Viinis koostati ühiselt deklaratsioon, milles Euroopa Andmekaitseenõukogu toob välja oma vastutuse tagada üldmääruse tõhus ja järjepidev rakendamine. Andmekaitseasutused omakorda kinnitasid eesmärgi tihendada ja tõhustada piiriülest koostööd.

Andmekaitseasutused leppisid kohtumisel kokku neli sammu

Esiteks, andmekaitseasutused toovad perioodiliselt välja strateegilise tähtsusega piiriüleseid juhtumid, mille lahendamiseks on oluline omavaheline koostöö ja Euroopa Andmekaitseenõukogu toetus. Siin panevad andmekaitseasutused erilist rõhku ka kogu asjakohase teabe õigeaegsele jagamisele, et saavutada võimalikult kiiresti konsensus.

Teiseks, Euroopa Andmekaitseenõukogu tegeleb õigusküsimustega, mis on seotud üldmääruse rakendamise õiguslike probleemidega üldises mõttes, konkreetsetes õigusküsimustes annab andmekaitseenõukogu välja rohkem arvamusi.

Kolmandaks, andmekaitseasutused kohustuvad täiendavalt vahetama teavet siseriiklike andmekaitsestrateegiate kohta, et leppida Euroopa tasandil kokku iga-aastastes ühistes prioriteet-

tides, mis kajastuks ka järelvalvemenetlustes. Andmekaitseasutused võivad ette valmistada ühise järelvalveraamistiku, sealhulgas ühised kontrollivahendid.

Neljanda sammuna toodi esile eesmärk tõhustada piiriülest teabevahetust.

Soovide nimekiri Euroopa Komisjonile

Pärast 2022. aasta aprillikuist kohtumist saatis Euroopa Andmekaitseenõukogu Euroopa Komisjonile arutamiseks nn soovide nimekirja menetlusõiguse küsimustest, mida tuleks ühtlustada.

Loetelus käsitletakse muu hulgas haldusmenetluse poolte õigusi, menetlustähtaegu, kaebuste vastu võtmise või tagasilükkamise nõudeid, andmekaitseasutuste uurimisvolitusi ja koostöömenetluse praktilisi küsimusi.

Samuti andis Euroopa Andmekaitseenõukogu 2022. aasta sügisel avalikkusele teada ka oma teisest ühisest järelvalvemenetlusest, mis keskendub andmekaitse spetsialisti määramisele ja ametikohale asutustes ja ettevõtetes.

Praeguseks on juba koostatud strateegilise tähtsusega piiriülese menetluste valiku kriteeriumid. Muu hulgas loetakse strateegiliseks juhtumit, kui see puudutab korduvat probleemi mitmes liikmesriigis, on seotud andmekaitse ja muu õigusvaldkonna ristumisega, mõjutab paljusid andmesubjekte mitmes liikmesriigis või kui mitmest liikmesriigist on sama juhtumi kohta suur hulk kaebusi.

Infoliin

Andmekaitse Inspeksiooni teabetelefon on olnud töös juba rohkem kui kümme aastat ja tõestanud oma vajalikkust. Pea pooled küsimused jõuavad meieni infoliini kaudu.

Infoliinilt saab kiire selgituse lihtsamatele olukordadele ja vastuse küsimustele, mis ei vaja sügavat analüüsi ja regulatsioonide uurimist. Infoliin võtab vähemaks ka kirjalike selgitustootluste koormat, mille arv on juba aastaid püsinud proportsioonis infoliini kõnede arvuga.

2021. aasta jaanuari algusest kuni 2022. aasta detsembri lõpuni helistati Andmekaitse Inspeksiooni infoliinile 2378 korda.

Analüüsides infoliinile tehtud kõnede sisu, saab öelda, et enim küsimusi võib liigitada isikuandmete kaitse regulatsiooni alla – kokku 1900 kõnet, mis on 80% kõigist infoliini kõnedest. Avaliku teabe seaduse kohaldamise kohta küsiti 219 korda, elektroonilise side seaduse ehk elektroonilise otseturustuse kohta 39 korda. Teemadel, mida ei olnud võimalik liigitada inspeksiooni järelevalvealasse, tehti 220 kõnet.

Kõige populaarsemad valdkonnad infoliinil on aastaid püsinud samad: andmekaitse töösuhetes, isikuandmete avalikustamine internetis (sh veebilehtedel, meedias, sotsiaalmeedias) ja salvestusseadmete kasutamine. Sarnaselt eelnevate aastatega on püsinud huvi iseenda isikuandmetele juurdepääsu kohta ja samuti üldisemad andmekaitse- ja andmekaitse küsimused (nt andmekaitsetingimuste koostamine, nõusoleku küsimise vormistamine jne). 2021-2022 aastal oli tuntav huvi kasv seoses võlgnike andmete töötlemisega.

Isikuandmete kaitse seadusega seotud enim esinenud küsimused:

1. Töösuhetega seotud küsimused – 375 kõnet. Enim küsiti töökohtadel kaamerate kasutamise kohta (kokku 56 kõnet).

2. Andmete avalikustamine internetis või meedias – 241 kõnet. Enamasti on selliste kõnede puhul mureks andmete (nimi, isikukood, foto jms) avalikustamine internetis või (sotsiaal)meedias.

3. Üldisemalt salvestusseadmete kasutamine – 170 kõnet. Küsimused, mis puudutasid kaamerate kasutamise lubatavust avalikes kohtades ja eramajade küljes ning teavitussiltide nõuded. Kui siia liita ka küsimused kaamerate kasutamisest töökohtadel, oli kaameratega seonduvaid küsimusi 263.

4. Andmete väljastamine – isikute küsimused iseenda kohta käivate andmete (sh logid) kättesaamise kohta. Umbes veerand nendest kõnedest puudutasid surnud isikute andmete väljastamist pärijatele – kokku oli kõnesid 127.

5. Korterühistutega seotud kõned – 122 kõnet. Nende hulgas oli nii salvestusseadmete kasutamisi kui ka üldisemat isikuandmete töötlemist korterühistutes.

6. Võgnevused, kohtutäiturid ja inkasso – 101 kõnet. Võlgnevustega seonduvate probleemide puhul küsiti enim võlaandmete avaldamise ja inkassode tegevuse kohta.

Tasub märkida, et väga palju tuli küsimusi ka haridusvaldkonnast – koolidelt, lastevanematelt, KOV-idelt. Teemad olid suuresti COVID-iga seotud, aga tihti küsiti andmete avalikustamise, kaamerate kasutamise jms kohta.

Tegevusnäitajad

2020 2021 2022

Juhendiloome, poliitikanõustamine

Juhendid	1	1	2
Arvamused õigusaktide eelnõude kohta	29	44	44

Teavitustöö

Selgitustootlused, märgukirjad, nõudekirjad, teabenõuded	1759	1813	1325
Kõned valveametniku telefonile	1222	1350	1028
Koolitused ja nõustamised	71	69	17*
Nõustamised (ettevõtetele, asutustele)	60	52	-
Koolitused (korraldatud või lektorina osaletud)	11	17	17

* 2022.a. nõustamiste osas statistikat ei peetud

Järelevalvetöö

Ringkirjad (ilma järelevalvet algatamata)	2	3	1
sh ringkirjade adressaate	1108	92	7
Suuremahulised võrdlevad seired	1	1	2
sh seiratute arv	77	65	11
Kaebused, vaided, väärteoteated (esitatud) IKS, AvTS, ESS alusel	701	693	936
Pöördumised IMI (EL infosüsteem, mille kaudu andmekaitseasutused vahetavad infot jt pöördumisi) kaudu	884	929	1520

2020 2021 2022

Omaalgatuslikud järelevalveasjad (algatatud)	28	30	37
Kohapealsed kontrollkäigud (järelevalves)	2	1	3
Soovitused ja ettepanekud (järelevalves)	223	214	215
Ettekirjutused (reeglina sisaldab sunniraha-hoiatust)	37	30	52
Väärteoasjad (lõpetatud)	12	11	7
Trahvid (väärteokaristus), sunniraha (järelevalves)	12	10	12

Loa- ja erimenetlused

Andmekogude koostööstustaotlused (asutamiseks, kasutusele võtmiseks, andmekoosseisu muutmiseks, lõpetamiseks)	16	31	31
Loataotlused teadusuuringuteks andmesubjektide nõusolekuta	32	20	21
Loataotlused isikuandmete välisriiki edastamiseks	2	2	1
Taotlused iseenda andmete suhtes Schengeni, Europol'i jt piiriülestes andmekogudes	10	14	14
Rikkumistead	138	145	154

Inspeksiooni töötajate arv ja eelarve

Koosseisulisi ametikohti	19	22	21
Aastaeelarve (tuhat eurot)	751	851	975

Lühiseletused

Andmekaitse spetsialist – IKÜMi kohaselt andmekaitseametnik, vastutava või volitatud töötaja poolt määratud isik, kes täidab IKÜMis ettenähtud ametiülesandeid.

Andmekogu – on riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses sätestatud ülesannete täitmiseks.

Andmeladu – ühiskasutusega andmekogu, mis võib koosneda mitmest mis tahes tüüpi andmeid sisaldavast andmebaasist ning hõlmab organisatsiooni kõiki andmeid.

Andmesubjekt – isik, kelle andmeid töödeldakse.

Andmetöötaja – vastutav, volitatud või kaasvastutav andmete töötaja.

Anonümiseerimine – isikuandmete viimine kujule, kus isik ei ole enam otseselt ega kaudselt tuvastatav; anonümiseeritud andmeid ei saa viia tagasi isikut tuvastavale kujule.

Avalik teave – mis tahes viisil ja mis tahes teabekandjale jäädvustatud ja dokumenteeritud teave, mis on saadud või loodud avalikke ülesandeid täites.

Biomeetrilised andmed – konkreetse tehnilise töötlemise abil saadavad isikuandmed isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist, näiteks näokujutis ja sõrmejälgede andmed.

Erililised isikuandmed – andmed, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, füüsilise isiku kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed (ennekõike sõrmejälje-, peopesajälje- ja silmaiirisekujutised), terviseandmed või andmed füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta.

Isikuandmed – igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta.

Isikuandmete töötlemine – isikuandmete või nende kogumitega tehtav toiming, sh kogumine, säilitamine, jäädvustamine, edastamine jne.

Isikuandmetega seotud rikkumine – turvanõuete rikkumine, mis põhjustab edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsiminekku, muutmise või loata avalikustamise või neile juurdepääsu.

Küpsised – väike tekstifail, mis salvestatakse seadmesse, kui külastatakse kellegi kodulehte. Küpsised võimaldavad kodulehel mugavamalt navigeerimist, jättes meelde kasutaja eelistusi, keele valikut, kirja suurus vms. Küpsiseid kasutatakse ka statistiliste andmete kogumiseks.

Metaandmed – mingeid andmeid kirjeldavad andmed ehk nii-öelda andmed andmete kohta, näiteks faili kohta on metaandmeteks faili autor, koostamise kuupäev jne.

Märgukiri – isik teeb adressaadile ettepanekuid asutuse või organi töö korraldamiseks või valdkonna arengu kujundamiseks; või annab adressaadile avaliku elu ja riigivalitsemisega seotud teavet.

Pseudonümiseerimine – isikuandmete viimine kujule, kus isikuandmeid ei saa täiendavat teavet kasutamata seostada konkreetse isikuga.

Seire – andmetöötajate praktikate kaardistamine üldisest olukorrast ülevaate saamiseks.

Selgitustootlus – isiku pöördumine, millega taotletakse teavet, mis eeldab adressaadi käsutuses oleva teabe analüüsi, sünteesi või lisateabe kogumist, sh õiguslase selgituse andmist.

Teabenõue – teabenõue on teabenõudja poolt teabevaldajale esitatud taotlus teabe saamiseks või taaskasutamiseks. Teabenõudega saab küsida asutuses olemasolevaid dokumente, mis on saadud või loodud avalikke ülesandeid täites.

Teabevaldaja – riigi- või kohaliku omavalitsuse asutus, avalik-õiguslik juriidiline isik ning teatud juhtudel ka eraõiguslik juriidiline isik, kui ta täidab avalikku ülesannet.

Vaie – kui isik leiab, et haldusaktiga või toiminguga on rikutud tema õigusi või piiratud tema vabadusi, võib ta selle vaidlustada ehk esitada vaide.

Vastutav töötleja – füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes üksi või koos teistega määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid.

Volitatud töötleja – füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötleja nimel.

Õiguslik alus – isikuandmete töötlemine saab olla seaduslik vaid siis, kui on täidetud vähemalt üks IKÜMi artiklites 6 või 9 loetletud alustest.

AKI – Andmekaitse Inspeksioon

AvTS – Avaliku Teabe seadus

ABIS – Automaatse Biomeetrilise Isikutuvastuse Süsteem

AKS – Andmekaitse spetsialist

E-ITS – Eesti infoturbestandard, <https://eits.ria.ee/>

ESS – Elektroonilise side seadus

GDPR ehk IKÜM – Isikuandmete kaitse üldmäärus, ametlik nimi EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) 2016/679, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)

IKS – Isikuandmete kaitse seadus

IMI – siseturu infosüsteem ehk Internal Market Information System

NETS – Nakkushaiguste Ennetamise ja Tõrje Seadus

SHP – Faililaiend (Eri 3D-disainiprogrammide loodud ja/või kasutatud objekt, tavaliselt kolmemõõtmeline pilt, mis on kujutatud tippude ja joontega määratletud hulknurkade abil - võib olla ka 2D joonis)

TsÜS – Tsiviilseadustiku Üldosa

VõS – Võlaõigus Seadus

Täname panuse eest!

Alissa Hmelnietskaja
Elve Adamson
Geili Keppi
Grete Lehemaa
Kadri Levand
Kaisa Rebane
Karin Uuselu
Katrín Haug

Kirsika Berit Reino
Liisa Ojangu
Maarja Kirss
Maire Iro
Marili Tammeorg
Maris Juha
Mehis Lõhmus
Merili Koppel

Pille Lehis
Raiko Kaur
Signe Kerge
Sirgo Saar
Terje Enula
Tiina Salumäe
Urmo Parm
Virve Lans

Küljendus, illustratsioonid, trükk

Ain Kaldra, Andre Poolma Iconprint OÜ

Esikaane foto

Liis Reiman

Andmekaitse Inspeksioon

2021-2022



