ANDMEKAITSE INSPEKTSIOON

Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest 2017. aastal

Soovitused aastaks 2018

ERAELU KAITSE JA RIIGI LÄBIPAISTVUSE EEST

Koostanud: Maire Iro, avalike suhete nõunik
Peadirektori eessõna: Viljar Peep

Valdkonnapõhise sisendi andsid:

Raavo Palu, õigusdirektor
Maarja Kirss, koostöödirektor
Urmo Parm, tehnoloogiadirektor
Elve Adamson, peainspektor
Merit Valgjärv, juhtivinspektor
Helina-Aleksandra Lettens, vaneminspektor
Sirje Biin, vaneminspektor
Raiko Kaur, vaneminspektor
Kristjan Küti, vaneminspektor
Liisa Ojangu, vaneminspektor
Andrus Altmeri, andmeturbeinspektor
Alvar Jõekaar, andmeturbeekspert
Helve Juusu, vanemspetsialist
Kaja Puusepp, arendusdirektor
Eret Kobin, vanemspetsialist

Andmekaitse Inspektsioon
Väike-Ameerika 19, 10129 Tallinn

SISUKORD

KOKKUVÕTE JA SOOVITUSED PEADIREKTORILT

Liigume digiühiskonda

Andmekaitseõigus tekkis reaktsioonina infotehnilisele arengule – et maandada sellest tekkivaid riske. See areng kiireneb üha. Meie igapäevaelu võrgustub üleilmses arvutivõrgus. Andmeanalüütikat, automaatprofileerimist kasutatakse üha laiemalt.

Infotehnilise arengu osas toimus Eestis nii mullu kui ka tänavu palju märkimisväärset:

- 2017. aasta märtsis algas isejuhtivate sõidukite katsetamine, millele riigikantselei töörühma lõppraport „Isejuhtivate sõidukite ajastu algus" andis rohelise tule – juhul, kui vastutav isik viibib sõidukis ja saab juhtimise üle võtta.
- 14. juunil 2017. a seadustati kokkuleppeveod ehk sõidujagamine. Infotehniline areng toob jagamismajanduse mudeleid nii veondusse, majutusse kui ka muudesse tegevusaladesse.
- Samal kuupäeval anti seaduse kaitse sõidu- ja kõnniteedel vuravatele pakirobotitele. Autojuht peab ülekäigurajal arvestama robotiga sama palju kui jalgratturiga.
- 16. juunil 2017. a asutati Eesti ja Soome valitsuse ühine instituut andmekogude andmevahetuskihi (x-tee) piiriüleseks kasutamiseks. X-tee on Eestis loodud lahendus, mis võimaldab andmete turvalist edastamist, krüptimist ja ajatembeldamist. See loob uue taseme piiriüleseks andmekasutuseks riikide vahel (rahvastikuregistrid, maksuametid jpt asutused).
- 20. juunil kirjutasid Eesti ja Luksemburgi peaministrid alla leppele maailma esimese andmesaatkonna rajamise kohta. Eesti riigi toimimiseks oluliste infosüsteemide varukoopiad dubleeritakse suurhertsogiriigis asuvasse turvalisse andmemajutuskeskusse.
- Elasime üle esimese suurema küber-ehmatuse – septembris jõudis avalikkuse ette ID-kaardi kiibi tarkvara turvarisk. Risk jäi õnneks teoreetiliseks. Seega on meil jätkuvalt maailma parim digitaalse identiteedi haldus ning suhtarvuna suurim igapäevakasutus.
- 2018. a märtsis otsustasid Riigikantselei ning Majandus- ja Kommunikatsiooniministeerium kokku kutsuda tehisintellekti töörühma. See peab koostama nii õiguslikud lahendused („kratiseaduse") kui ka riikliku strateegia. Kuidas reguleerida vastutust, kui iseõppiv seade võtab iseseisvalt vastu otsuseid, mida algoritmi loonud inimene ei saa enam ette näha?

Eesti on maailma infotehnilises arengus üks rajaleidjaid. Et see väide ei ole sõnakõlks, tunnetasin omal nahal 2017. aasta septembris Hongkongis üleilmsel andmekaitsevolinike konverentsil, kus käisin avapaneelis e-Eestit tutvustamas.

Arusaadavalt on kõige selle juures infoturve ning isikuandmete korrektne kogumine ja kasutamine tähtsamad kui kunagi varem.

Maikuust uus andmekaitseõigus

2018. aasta 25. maist hakatakse rakendama isikuandmete kaitse üldmäärust, mis on kõikides Euroopa Liidu liikmesriikides otsekohalduv. Ühtlasi muudetakse sellega seoses rohkem kui sadat Eesti seadust. Maikuus jõustub ka uus küberturvalisuse seadus. Tõlgin need uudised juristide keelest arvutiinimeste keelde: nii isikuandmete kasutamiseks kui ka infoturbe tagamiseks tuleb operatsioonisüsteemi uuendada.

Miks seda kõike vaja on? Suuremad rahvusvahelised pahavara-taudid ja isikuandmete väärkasutusskandaalid on seni Eestist õnneks mööda läinud. Elu kolib aga üha enam küberruumi ning pahalased tulevad järele. Teabehalduse ja infoturbe paremale järjele aitamine on nii meie ettevõtetele kui ka avaliku sektori asutustele kasulik, sest nii saame:

a) paremini kaitsta oma (info)vara,
b) olla oma töös tõhusamad ja konkurentsivõimelisemad ning
c) olla kodanikele/klientidele/töötajaile usaldusväärsemad.

Ei äris ega avalikus sektoris pole võimalik edukalt e-teenuseid arendada, kui inimesed ei usalda seda, kuidas nende kohta käivat teavet hoitakse. Uus õigustik peaks tugevdama inimese kontrolli oma andmete üle.

Kas on oodata hiigeltrahve?

Suurt tähelepanu on pälvinud üldmääruses ettenähtud kõrged trahvimäärad. Mitmed koolitajad ja nõustajad on seda oma teenuste reklaamimisel võimendanud.

Jah, andmekaitseasutuste tegevuste kohta käivad üldmääruse sätted on tõepoolest keskendunud kaebustele, rikkumistele ja nende eest karistamisele. Sellele vaatamata kinnitan, et me ei muutu 25. maist trahvivabrikuks. Erinevalt mitmest teisest liikmesriigist on Eesti andmekaitseasutusel kogu aeg olnud õigus sanktsioone rakendada. Sellealane praktika on kahe kümnendi jooksul paika settinud ning põhimõttelisi muutusi ei ole ette näha.

Inspektsioon on olnud keskendunud ennetusele ja teavitusele. Rikkumiste puhul on meie käitumismustriks olnud selgitamine ja hoiatamine. Karistusi ja sundi rakendame viimase abinõuna. Selle juures teen kaks reservatsiooni:

1) meie väiksus seab selgitustöös piirid – üksiku ettevõtte/asutuse tasandil põhjalikuma nõustamise võimalused on kasinad,
2) pahatahtlikkuse, samuti korduva tõsise rikkumise puhul ei ole hoiatamisel ja uue võimaluse andmisel mõtet, sellistel juhtudel on rangus kohane.

Mida inspektsioon uue andmekaitseõiguse rakendamiseks teeb?

Meil on kolm prioriteetset eesmärki.

1. Täita uuest õigusest tulenevaid liikmesriigi andmekaitseasutuse kohustusi (21 konkreetset ülesannet ja 26 võimuvolitust).[1] Ettevalmistustöö nii Eestis kui ka

[1] Vt üldmääruse art 57 ja 58.

Euroopa töörühmas on mahukas (juhendiloome, teavitustöö, infosüsteemi uuendamine, töökorralduse muudatused).

2. Samas pakub üldmäärus võimalusi tasakaalukaks ja paindlikuks rakendamiseks. Need tuleks ära kasutada, arvestades Eesti digiarengut, ühiskonna avatust ning ettevõtete-asutuste väiksust. Olen inspektsiooni nimel esitanud sellealased seadusloome-ettepanekud justiitsministeeriumile ning valmis neid selgitama ka Riigikogu menetluses.
3. Kasutame uue andmekaitse- ja küberturbeõiguse rakendamist ära teabehalduse ja infoturbe taseme tõstmiseks Eesti ettevõtetes ja asutustes – tõstame oma konkurentsivõimet, ennetame uusi ohtusid, loome uusi võimalusi.

2017. aasta tegevuse kokkuvõte

Arvude keeles võtan mulluse töö kokku nii:

TEGEVUSNÄITAJAD	2014	**2015**	2016	**2017**
Juhendiloome, poliitikanõustamine				
juhendid (arvestamata seniste uuendamist)	6	**4**	1	**2**
arvamused õigusaktide eelnõude kohta	28	**35**	27	**34**
Teavitustöö				
selgitustaotlused, märgukirjad, teabenõuded	1144	**1369**	1417	**1520**
kõned valveametniku infotelefonile	1141	**1136**	1419	**1527**
nõustamised (ettevõtetele, asutustele)	34	**33**	79	**148**
koolitused (korraldatud või lektorina osaletud)	24	**18**	23	**17**
Järelevalvetöö				
ringkirjad (ilma järelevalvet algatamata)	-	**5**	5	**4**
sh ringkirjade adressaate		**149**	34	**26**
suuremahulised võrdlevad seired	6	**14**	9	**10**
sh seiratute arv		**412**	148	**129**
kaebused, vaided, väärteoteated (esitatud)	413	**446**	390	**462**
omaalgatuslikud järelevalveasjad (algatatud)	152	**384**	86	**149**
sh ennetavad andmekaitseauditid	16	**24**	24	**1**
kohapealsed kontrollkäigud (järelevalves)	48	**35**	33	**45**
soovitused ja ettepanekud (järelevalves)		**299**	56	**125**

ettekirjutused (reeglina eelneb ettepanek; reeglina sisaldab sunniraha-hoiatust)	86	**77**	59	**64**
sh registreerimise alal (eelneva ettepanekuta)	45	**28**	26	**35**
väärteoasjad (lõpetatud)	11	**16**	16	**9**
trahvid (väärteokaristus), sunniraha (järelevalves)	8	**15**	16	**4**
Loa- ja erimenetlused				
registreerimistaotlused (delikaatsete andmete töötlemiseks või vastutava isiku määramiseks)	902	**540**	547	**641**
andmekogude kooskõlastustaotlused (asutamiseks, kasutusele võtmiseks, andmekoosseisu muutmiseks, lõpetamiseks)	115	**167**	139	**99**
loataotlused teadusuuringuiks andmesubjektide nõusolekuta	13	**29**	18	**54**
loataotlused isikuandmete välisriiki edastamiseks	13	**8**	18	**22**
taotlused iseenda andmete suhtes Schengeni, Europoli jt piiriülestes andmekogudes	6	**10**	10	**8**
Asutuse tööpere ja eelarve				
koosseisulisi ametikohti	18	**18**	19	**19**
aastaeelarve (tuhat eurot)	654	**671**	700	**714**

Nende numbrite taga on mu kolleegide terve aasta töö. Järgnevates peatükkides analüüsivad nad ise lähemalt oma vastutusvaldkondi ning kirjeldavad olulisemat, mida nad tegid. Peatun valikuliselt vaid mõnel üksikul sündmusel ja arengul.

Õigusloome

23.03.2018 esitas Justiitsministeerium uue isikuandmete kaitse seaduse eelnõu valitsusele, samal kuupäeval teistele ministeeriumidele kooskõlastamiseks teiste seaduste muudatused. Inspektsiooni kommentaarid eelnõudele ja muud materjalid on avaldatud meie võrgulehel reformirubriigis.

Tegin 2013. aasta aastaettekandes (lk 18, p 1) ettepaneku kaasajastada menetlus-dokumentide kättetoimetamise reegleid. Haldusmenetluse seadus (HMS) nõudis elektrooniliseks kättetoimetamiseks erinevalt paberpostist eelnevat nõusolekut. Ametlikul e-posti aadressil (isiku- või registrikood@eesti.ee) puudus õiguslik tähendus. Kontaktandmete põhiregistri (rahvastiku- ja äriregistri) kaudu kasutamise asemel korjasid asutused kontaktandmeid üksikmenetluste kaupa. Tulemuseks menetluste venimine, kõrged postikulud ning kontaktandmestiku halb kvaliteet. Asjaomaste ministeeriumide kantslerite heakskiidul kutsusin 2013. a septembris kokku mitteametliku töörühma. Meie ettepanekud realiseerusid Justiitsministeeriumi õiguspoliitika osakonna energilise töö tulemusena kõigest neli aastat hiljem – 2017. aasta augustis esitatud HMSi eelnõuna, mis võeti vastu detsembris.

Juurdepääs avalikule teabele, AK-teabe kaitse, andmekogude pidamine

„Teenuste korraldamise ja teabehalduse aluste“ määruse kohaselt loodi inspektsiooni juurde ministeeriumide jt keskasutuste esindajaist avaliku teabe nõukogu. Koordineerime selle kaudu nii juurdepääsu avalikule teabele kui ka isikuandmete kaitse alast tööd avalikus sektoris.

Mullu kontrollisime kümnes asutuses juurdepääsupiiranguga teabe kaitset, sh kuuel korral koos Riigi Infosüsteemi Ametiga. Suuri puudusi õnneks ei avastatud. Tänavu II poolaastal on plaanis „tuletõrjeõppused“ – etteteatamata kontrollkäigud mõnda asutusse, kus hindame kriisiohjeks valmisolekut ja personali instrueeritust.

2016. aasta jaanuaris võttis inspektsioon üle andmekogude järelevalve. Mullu kasvas andmekogude arv, mille kasutuselevõtt on kooskõlastatud, 277-lt 539-ni. See ei näita siiski andmekogude arvu järsku kasvu, vaid seda, et riigiasutused hakkasid andmekogude kooskõlastamise nõudeid täitma.

Rahandus

Üheks huvitavamaks omaalgatuslikuks järelevalveks 2017. aastal oli *online*-panganduses kasutatavate mobiilirakenduste ehk äppide seire. See sai alguse kahtlusest, et ühe äpi kaudu pääseb pank ligi ka ärikasutajast kliendi telefoniraamatule seal olevate inimeste teadmata. Õnneks ei saanud kahtlused kinnitust. Kaheksast seiratud pangast üks küll sai kliendi telefonis telefoniraamatule ligipääsu, kuid kasutas asjaomase teenusega ühinenud isikute kontakte nende nõusolekul.

Tänuavaldused ja nõuanded

2018. aasta on väga eriline mitte üksnes sajandivanuseks saanud Eesti riigile, vaid ka andmekaitsevaldkonnale. Uus andmekaitseõigus sisaldab väga palju määramatust. Ettevalmistustöö maht nii Eestis kui ka Brüsseli ühisorganis on suur. Üle-euroopalise ühtlustava juhendiloome ning siseriiklike rakendusseaduste valmimise venimine on ettevalmistusi raskendanud.

Seda enam tahan tänada oma kolleege. Praegu on meil pingeline, kuid põnev aeg. Olete oma tööd teinud südamega ja hästi. Aitäh teile selle eest! Oleme üheskoos kujundanud asutuse, kes hoiab põhiõiguste kaitse ja avalike huvide vahel tasakaalu. Me ei otsi takistusi, et midagi teha ei saaks, vaid otsime lahendusi, et vajalikku saaks teha. Oleme oma valikutes keskendunud olulisele, et „puude“ kõrval tegeleda ka „metsaga“.

Samuti tänan inspektsiooni nõukoja liikmeid, kes on panustanud oma aega andmekaitse ja avaliku teabe küsimuste arutamisse. Tänan avaliku teabe nõukogu liikmeid kogemuste eest, mida olete oma valitsemisaladest kaasa toonud. Tänan häid kolleege ministeeriumidest, ametitest, omavalitsustest, Eesti Kaubandus-Tööstuskojast ning kõigist teistest partnerorganisatsioonidest.

Kõigist koostööpartneritest tõstan mulluse põhjal esile Tallinna Tehnikaülikooli, Tallinna Ülikooli, Tartu Ülikooli ning Tallinna Majanduskooli andmekaitsespetsialistide täiendkursuste hoogsa käivitamise eest. Andmekaitse ja infoturve on valdkonnad, kus on vajalik tänasega võrreldes suurem professionaliseerumine. Teie töö on sellele oluliselt kaasa aidanud.

SOOVITUSED

Soovitused ettevõtte juhile uue andmekaitseõiguse rakendamiseks

25. mail 2018. a tuleb kõigis Euroopa Liidu maades rakendada isikuandmete kaitse üldmäärust. Selleks soovitan:

1. Iga asi algab inimestest – hoolitsege, et Teie ettevõttes oleks olemas vajalik andmekaitse- ja infoturbe-alane oskusteave (oma personali hulgas või väljastpoolt). Kuid arvestage, et seaduse ees vastutab mitte andmekaitsespetsialist, vaid ettevõtte juhatus – samamoodi nagu näiteks raamatupidamise või maksukohustuse eest.
2. Laske läbi viia olemasoleva infovara kaardistamine, et koostada/uuendada omavahel seotud dokumente:
    a) bilansi-laadne andmetöötluse register isikuandmete kaitse üldmääruse art 30 kohaselt (inspektsioonil on õigus seda välja nõuda, lihtsamad näidised leiate meie võrgulehelt),
    b) klientidele-partneritele suunatud andmetöötlustingimused üldmääruse art 12 kohaselt,
    c) kui olete küberturvalisuse seaduses nimetatud teenusepakkuja, siis riskianalüüs turvameetmete võtmiseks.
3. Selle kaardistuse põhjal saate võtta vajalikke meetmeid, et olla valmis:
    a) iseenda andmete kohta esitatud päringuteks,
    b) andmete ülekandmise nõueteks,
    c) rikkumisteadete esitamiseks oluliste isikuandmetega seotud rikkumiste kohta inspektsiooni võrgulehe kaudu,
    d) kui olete küberturvalisuse seaduses nimetatud teenusepakkuja, siis ka küberintsidentidest teatamiseks Riigi Infosüsteemi Ametile.
4. Kui Teie tegevusalal on andmekaitse osas lahtisi otsi, siis tehke oma ettevõtlus- või erialaliidu kaudu koostööd ja koostage praktilisi hea tava toimimisjuhiseid. Üheskoos ise tehes saate materjalid, millest on kõige rohkem kasu. Inspektsiooni võimalused individuaaltasandil põhjalikumalt nõustada on kasinad, kuid sektoritasandil aitame meeleldi.

Soovitused asutuse juhile uue andmekaitseõiguse rakendamiseks

1. Iga asi algab inimestest – hoolitsege, et Teie asutuses oleks pädev andmekaitsespetsialist ja infoturbejuht (oma personali hulgas või väljastpoolt). Kuid arvestage, et seaduse ees vastutab mitte andmekaitsespetsialist, vaid asutuse juht – samamoodi nagu näiteks raamatupidamise või maksukohustuse eest.
2. Laske läbi viia olemasoleva infovara kaardistamine, et koostada/uuendada omavahel seotud dokumendid:
    a) bilansi-laadne andmetöötluse register üldmääruse art 30 kohaselt (inspektsioonil on õigus seda välja nõuda, lihtsamad näidised leiate meie võrgulehelt),
    b) avaandmete mõjuhinnang AvTS § 3^1 (miks ja kuidas Teie asutus annab või ei anna oma avalikku digiandmestikku avaandmeteks),

c) avalikkusele suunatud andmetöötlustingimused üldmääruse art 12 kohaselt,
d) riskianalüüs turvameetmete võtmiseks küberturvalisuse seaduse kohaselt,
e) ülevaade infovara kohta vastavalt „Teenuste korraldamise ja teabehalduse aluste“ määruse §-le 12,
f) dokumentide liigitusskeem vastavalt „Arhiivieeskirja“ §-dele 6-8.

3. Selle kaardistuse põhjal saate võtta vajalikke meetmeid, et olla valmis:
   a) iseenda andmete kohta esitatud päringuteks,
   b) rikkumisteadete esitamiseks oluliste rikkumiste kohta inspektsiooni võrgulehe kaudu,
   c) küberintsidentidest teatamiseks Riigi Infosüsteemi Ametile.
4. Laske oma spetsialistidel jälgida avaliku teabe nõukogu tööd (riigi keskasutuste esindajate ühisorgan avaliku teabe ja isikuandmete kaitse alal). Kui olete riigiasutus, siis küsige vajadusel nõu oma ministeeriumi esindajalt nõukogus. Kui olete omavalitsusasutus, siis praktilist nõu saate ka Tallinna linna- ja Türi vallavalitsuselt, kes koostöös inspektsiooniga piloteerivad uue andmekaitseõiguse rakendamist. Tallinn osaleb ka omavalitsuste esindajana nõukogus.

Soovitused Justiitsministeeriumile

1. Nendin uue isikuandmete kaitse seaduse (IKS) eelnõu sanktsioonide peatüki ebaõnnestumist. Esiteks, kui erasektorile suunab Euroopa seadusandja kõrge ülempiiriga trahvid, siis avalikus sektoris on eelnõu järgi sama sisuga rikkumised karistamatud. See ei ole mõistlik ega õiglane. Kuna asutust trahvida ei saa, tuleks kohaldada ametiisiku väärteovastutust. Teiseks leian, et aeg on küps juriidiliste isikute haldustrahvide taastoomiseks Eesti õigusesse. Juriidiliste isikute sanktsioneerimine tänase väärteomenetluse kaudu on karikatuurselt ebatõhus ja kõigile osapooltele koormav. Täpsemad ettepanekud olen esitanud eraldi.[2]

2. Kordan eelmises aastaettekandes (vt lk 11) tõstatatud probleemi lauspäringute kohta. Pean silmas võimalust, kus korrakaitseasutus paneb masina inimeste kohta üle andmekogude infot traalima ning sellel tegevusel on traalimise objektile õiguslikud tagajärjed.[3] Täiesti lubamatu on kasutada üksikpäringuteks mõeldud üldnorme automatiseeritud lauspäringuteks. Maksu- ja Tolliametil on asjakohased erinormid riskihindamise ehk „maksuluure“ asjus. Automatiseeritud lauspäringud levivad ka teistesse valdkondadesse. 14. märtsil 2018. a võttis Riigikogu vastu sotsiaalhoolekandeseaduse täiendused mittehõivatud noorte väljaselgitamiseks. Minu hinnangul on täiendused poolikud päringule järgneva tegevuse osas. Juhin Justiitsministeeriumi tähelepanu üldmääruse nõudele, et kui liikmesriigi seadusandja näeb ette automaatandmetöötlusel põhinevate üksikotsuste tegemise, peab ta ette nägema ka kohased kaitsemeetmed.[4] Andmeanalüütika kasutamine avalikus halduses üha levib, seega pea liiva alla peitmine ei ole lahendus. Korrakaitseseaduse täiendamine taolise järelevalvemeetme asjus on hädavajalik.

[2] Kõige põhjalikumalt 16.10.2017 saadetud kirjas. Samad probleemid on välja toodud 14.10.2016 avaldatud ülevaates (III-10), 27.04.2017 avaldatud seisukohtades (2. ptk), 29. 05.2017 memos haldustrahvidest.
[3] Antud juhul ei pea ma silmas statistilist andmeanalüütikat, sest need ei too uuritavaile kaasa tagajärgi – uuringu tulemuseks on umbisikustatud üldistused.
[4] Isikuandmete kaitse üldmääruse art 20 lg 2 punkt b.

3. Kui avalikud on avaliku sektori palgaandmed? Ametniku palgad avaldatakse internetis, aga kas teabenõudega saab välja nõuda avalikust eelarvest töölepingu alusel välja makstud palku isikustatud kujul? Inspektsiooni tõlgendust, et AvTS § 36 lg 1 p 9 kohaselt saab, on ikka ja jälle vaidlustatud. Niivõrd olulise tähtsusega küsimuses peaks seadusandja selget tahet avaldama.

Soovitused Majandus- ja Kommunikatsiooniministeeriumile ning Riigi Infosüsteemi Ametile

1. Isikuandmete kaitse ja küberturvalisus on õigusregulatsioonilt justkui kaks eraldi valdkonda kahe järelevalveasutusega. Lõpprakendaja (ettevõtte ja asutuse) jaoks on nad aga suuresti kattuvad, eriti infoturbe osas. Keskne infoturbe rakendusjuhend, infosüsteemide kolmeastmeline etalonturbe süsteem (ISKE), hetkel isikuandmete kaitset ei sisalda. Soovitan vastavad osad lisada. Justiitsministeerium on eestindatud ISKE lähtematerjali (Saksa võrgu- ja infoturbe liiduameti infoturbe alusstandardi) andmekaitse mooduli.

   Jätkuvalt nendin, et ISKE on hea abivahend suurtele organisatsioonidele. Kindlaliigilised väiksemad andmetöötlejad vajavad lihtsamat, otse neile kohandatud juhendmaterjali (nt omavalitsused jt väiksemad asutused, perearstid jt väiksemad tervishoiuteenuse osutajad).
2. Eraisikute ja ametiasutuste kirjavahetus on paberpostist liikunud e-posti. Soovitan valmistuda järgmiseks tasandiks – kirjavahetuse suunamiseks veebirakendusse. Eraisik saab seda kasutades oma pöördumiste läbivaatamistest selge pildi ega pea otsima neid asutuste dokumendiregistritest. Dokumendiregister sisaldab küll vastamistähtaega ja läbivaatava üksuse/asutuse nime, kuid kuna pöörduja nimi tuleb asendada initsiaalidega, siis on sellest vähe kasu. Sisselogitav isiklik „töölaud“ oleks pöördujale parem lahendus. Asutus peab aga tegema palju käsitööd, mida veebirakenduse kasutamine võimaldaks automatiseerida. Inspektsioon on loomas omaenda veebirakendust. Soovitan sama mudeli üldiselt kasutusele võtta – selgitustaotlusi, märgukirju, teabenõudeid, vaideid jms dokumente käideldakse avaliku sektori asutustes sarnaselt.

Viljar Peep
Andmekaitse Inspektsiooni peadirektor

TEHNOLOOGIA JA PRIVAATSUS

Urmo Parm, tehnoloogiadirektor

Läinud aastanumber sisustas avalikkust järjekordselt mitmete näidetega, mille kokkuvõte on üks – täielikku privaatsus pole olemas ning läbi ja lõhki turvalist tehnoloogiat ei eksisteeri. Mastaapsed lunavararünded, mitmed sotsiaalmeediakeskkondade andmelekked, ulatuslikud õngitsuskirjade lained või avastatud turvanõrkused teatud arvutiprotsessorites on vaid mõned näited. Isegi kui soovime mõelda, et meid puudutav eraeluline teave kuulub ainult meile, siis paraku see nii ei ole. Kogu meie internetikasutust puudutav teave, teenuste kasutamisel sisestatud andmed, internetiavarustesse postitatu – see kõik jõuab ühel või teisel viisil ka kellegi teise käsutusse. Olgu siis isiklikuks otstarbeks või äriotsuste tegemiseks. Küsimus on, kas ja mis ulatuses saame me seda protsessi kontrolli all hoida.

Ei kehtiv ega peatselt jõustuv uus andmekaitseõigus räägi andmete omandist. Küll aga peavad inimesele kõik tema andmetega tehtavad tegevused olema läbipaistvad, arusaadavad ning selgelt esitatud. Eelmises aastaülevaates tunnustasime meie partnerasutust Riigi Infosüsteemi Ametit andmejälgija eest. Hea on tõdeda, et tänaseks lahendus töötab ja on juba rakendunud mitmetes riiklikes andmekogudes. Andmejälgija eesmärk ongi anda inimesele võimalus teada, kes, mis eesmärgil ja millises mahus tema isikuandmetega toiminguid on teinud. Tööriista rakendumine tõi kohe välja ka probleemkohad. Näiteks selgus, et mõned asutused töötlevad andmeid ulatuslikumalt kui konkreetne toiming nõuaks. Põhjuseks teatud ajalooline mugavus päringuloogika ülesehituses. Selgitasime asutustele, mis vajaks muutmist. Probleemi teadvustati ning asuti tegelema lahendustega.

Pilvandmetöötlus

Riik peab teatud käitumismudelites olema eeskujuks. Pilvandmetöötluse ajastul on lihtne eksida. Ainult üks vale otsus teenusepakkuja valikul võib tähendada hilisemaid selgitusi inspektsioonile. Halvimal juhul ka rikkumisega kaasnevaid sanktsioone. Kuna riik on oma kodanike isikuandmete osas vaieldamatult suurim andmetöötleja, soovime me olla kindlad, et meie andmed on maksimaalselt kaitstud. Teisalt, teaduse ja tehnoloogia kiire areng on viinud selleni, et isikuandmete kaitseks rakendatavate kaasaegsete turvameetmete osas toetume üha enam välistele partneritele. Seda ka andmete majutamisel pilveteenustes. Majandus- ja Kommunikatsiooniministeeriumi eestvedamisel aitasime välja töötada soovitused avaliku sektori turvaliseks andmetöötluseks avalikes pilveteenustes.

Nutisõidukid

Meie igapäevased sõiduvahendid on üha enam võrgustumas. Juba aastaid on teatud automudelitel võimekus edastada autotootjatele reaalajas teavet sõiduki tehnilisest seisundist. Või võtta vastu tarkvarauuendusi. Kuid mitte ainult. Nii on lihtne koguda andmeid ka juhi sõiduharjumustest ja maneeridest. Juba on näiteid, kus pahalastel on õnnestunud nutisõidukeid üle võrgu rünnata ja sõiduki tehnilisi omadusi muuta. Kohal on isejuhtivad sõidukid. Rahvusvaheliste ning riiklike kokkulepete ja reeglite puudumisel on väga lihtne jääda rongist maha ja asuda tegelema tagajärgedega. Olgu selle näiteks küsimus, kellele

sõiduki kasutaja andmed jõuavad või kuidas inimene ise nendele andmetele ligi pääseb. Või kas inimesel on võimalik andmetöötlusest loobuda? Läinud aasta tõi selles vallas edasimineku. Osalesime Riigikantselei algatusel ning Majandus- ja Kommunikatsiooniministeeriumi korraldatud aruteludel isejuhtivate sõidukite riskide kaardistamisel. Mõttetulemuse eesmärk on luua Eestisse rahvusvaheliselt parim keskkond liikuvusteenuste arendamiseks.

Idufirmad

Isikuandmetega tehtavate töötlemistoimingute kiiremad kasvajad on mikro-, väike- ja keskmise suurusega ettevõtted. Eelkõige raketina taevasse kihutavad idufirmad. Kiire käibenumbrite kasv ning rahaliste vahendite kaasamine on siin põhieesmärk. Uute ärimudelite väljamõtlemisel ning teenuste arendamisel jääb aga tihtilugu puudu pädevast teadmisest, kas kõik see, mida teha soovitakse, meie eraelu lubamatult ei riiva ega suisa seadusevastane ole. Olgu selle näiteks inspektsiooni kohtumised mitmete alustavate ettevõtjatega, kellele pidime selgitama, et ärimudelit ei ole kuidagi võimalik kirjeldatud viisil ellu viia. Põhjuseks elementaarsete isikuandmete kaitse põhimõtete eiramine. Seetõttu kutsusimegi iduettevõtluse kogukonna inkubaatorite ja kiirendite esindajad läinud aasta

sügisel mõttetalgutele, et inspektsiooni murekohti selgitada ja leida võimalusi olukorra parandamiseks. Kogukonna sõnul ei ole turul piisavalt andmekaitse alal tegutsevaid praktikuid. Teisalt aga ei ole olemasolevat kompetentsi osatud enda kasuks piisavalt ära kasutada. Loodetavasti saame järgmises aastakokkuvõttes raporteerida edusammudest, kuna Eesti suuremad ülikoolid on asunud usinalt tegelema andmekaitsespetsialistide koolitamisega.

Väikeettevõtted on innukad uute tehnoloogiate arendajad ning rakendajad. Olgu selleks iseõppivad algoritmid või biomeetrial põhinevad lahendused. Suurandmetöötlusena tehakse isikuandmete kaevet sotsiaalmeediast või teistest avalikest allikatest. Luuakse profiile ja tehakse inimest puudutavaid automaatotsuseid. Andmekaitse seda ei keela. Kuid tegevus peab jääma õiguslikult korrektsetesse raamidesse. Inspektsiooni üks fookusi järgmisteks aastateks saab kindlasti olema eelpool nimetatud tehnoloogiat kasutavate ettevõtete seire ja andmekaitsealaste vastavusnõuete kontroll.

Autentimislahendused

Alustasin ülevaadet viitega möödunud aasta ulatuslikele küberrünnetele. Pahalaste huviorbiidis on jätkuvalt inimeste isikuandmed – e-posti aadress, salasõnad, maksevahendite andmed. Sageli on ründevektor lihtne. Proovitakse enimlevinud salasõnade kombinatsioone. Siin aga ongi peamine murekoht – jätkuv lohakus paroolimajanduses. Seni, kuni e-teenused ei kasuta turvalise salasõna filtreid, mis nõuaks kasutajatelt piisava pikkuse ja keerukusega salasõna, olukord ei parane. Negatiivseks näiteks hiljutine juhtum Eesti juhtiva spordiklubi e-teenusega.

Eesti on eesrindlik elektroonilise identiteedi (eID) arendaja ning kasutaja. Näitena ID-kaart, Mobiil-ID või Smart ID. Riigi pakutavates avalikes e-teenustes ei tule ainult salasõnaga autentimine juba ammu kõne alla. Miks me ei võiks ka erasektori üleselt saavutada ühiskondlikku kokkulepet, et e-teenused kasutaks eelistatult eID-l põhinevaid autentimislahendusi? Euroopa Liidus on liikmesriikide elektrooniliste identiteetide vastastikuse tunnustamise õigusraamistik paigas. Kuigi see on eelkõige kohustuslik avalikule sektorile, ei keela miski ka erasektoril sellele tugineda. Ettevõtlusvaldkondade katusorganisatsioonid saaksid siin olla suunanäitajad vastavate heade tavade koostamisega. Inspektsioon on igati valmis kaasa mõtlema ja osalema.

E-õppe keskkondade seire

Viisime 2017. aasta juunis läbi omaalgatusliku seire, et saada ülevaade, milliseid e-õppe keskkondi Eesti kõrg- ja rakenduskõrgkoolid oma õppetegevuses kasutavad ning milline on isikuandmete töötlemise olukord ja õppeasutuste teadlikkus andmekaitse põhimõtetest ning nende rakendamisest e-õppe läbiviimisel.

E-õppe keskkond on elektrooniline keskkond, kus on võimalik luua ja hallata nii õppesisu (nt õppematerjalid, harjutused) kui ka õppeprotsesse (nt kodutööd, juhendamine, hindamine). E-õppe keskkondade vahendusel õppetegevuse osutaja peab arvestama võimalusega, et ta töötleb erinevaid isikuandmeid ja on isikuandmete seaduse mõistes isikuandmete vastutav töötleja.

Isikuandmeteks on näiteks õpikeskkonna kasutaja nimi, e-posti aadress ja kontaktandmed. Samuti õppijaga seotud tegevused nagu õppematerjali läbimiseks ja omandamiseks kulunud aeg, õigete ja valede vastuste osakaal või õppeasutuse hinnang õppija tulemustele.

Isikuandmete töötlemine peab olema seaduslik, eesmärgipärane ning õppijale läbipaistev. Õppeasutus kui isikuandmete vastutav töötleja peab tagama andmete kaitseks organisatsioonilised, füüsilised ja infotehnilised turvameetmed. Kui isikuandmete töötlemiseks enam õiguslikku alust pole, tuleb andmed kustutada.

Seire tulemusel selgus, et kõige levinum õpikeskkond on vabavaraline Moodle. Sõltuvalt õppeasutusest on lisaks kasutusel lahendused nagu Weebly, GoogleDrive, Google Classroom, eDidaktikum, õppematerjalide ja lõputööde varamu Eprints, e-portfooliokeskkond Mahara, õppeinfosüsteem ÕIS, Echo360, videoloengute salvestamiseks Panopto, veebisemiaride läbiviimiseks Adobe Connect Pro, veebipõhiste küsitluste läbiviimiseks Lime Survey.

Samas tõi seire välja kolm andmekaitselist kitsaskohta, millega õppeasutused õpitegevuse korraldamisel e-õppe keskkondades peavad arvestama ja parendavaid tegevusi kavandama.

1. Vähene teadlikkus oma vastutusest.
   Õppeasutus on e-õppe korraldamisel isikuandmete vastutav töötleja ning peab olema teadlik ja tagama kasutatavates vahendites andmekaitse nõuete täitmise. Seda ka nende teenuste osas, mida õppeasutus oma eesmärkide täitmiseks tellib välistelt partneritelt.

2. Infotehniliste turvameetmete parendamine
   Seire tõi välja, et salasõnade haldus mõnes e-õppe keskkonnas vajab ajakohastamist. Samuti tuleb sisse viia kord, et õppijad on kohustatud teatud perioodi möödudes (nt 6 kuud) salasõna muutma. Soovitasime õppeasutustel seadistada kaheastmeline autentimine kõikides teenustes, kus võimalik ning pigem kasutada õppijate tuvastamiseks eID lahendusi.

3. Kasutustingimuste puudumine
   Valdavalt puudusid nõuetekohased e-õppe keskkondade kasutustingimused, kus kirjas kes, mis eesmärgil ja õiguslikul alusel milliseid õppijate isikuandmeid töötleb ja kellele vajadusel edastab. Kui e-õppe keskkonna kasutamine on õppeprotsessi kohustuslik osa, võib need kirjeldada õppeasutuse sisekorras või õppekorraldust reguleerivates dokumentides. Need peavad õppijatele olema kättesaadavad ning õppeasutus peab tagama, et õppijad on nendega ka tutvunud. Kui e-õpikeskkonna kasutamine on vabatahtlik, peaksid kasutustingimused olema e-õppe keskkonna osa, millele õppija enne kasutamist oma nõusoleku annab. Nõusolek peab olema võetud vormis, mis võimaldab õppeasutusel vajadusel tõendada nõusoleku olemasolu või puudumist.

Kaamerate kasutamisest

Alvar Jõekaar, andmeturbeekspert

Tehnoloogia kiire areng avaldab selget mõju kõigis eluvaldkondades. Puutumata ei ole jäänud ka kaameravalve süsteemid, mis on muutunud kättesaadavamaks laiemale ringile tarbijatele kui kunagi varem. Nii on lisaks riigi- ja kohaliku omavalitsuse asutustele, kaubanduskeskustele ja muudele ettevõtetele hakanud oma videovalvesüsteeme üles panema ka korteriühistud ja eraisikud.

Mida tuleb silmas pidada?

Isikuandmete kaitse seaduse § 14 lõike 3 kohaselt võib isikute ja vara kaitseks kasutada jälgimisseadmestikku ainult juhul, kui sellega ei kahjustata ülemääraselt jälgitava isiku õigustatud huve ja jälgimise tulemusena saadud andmeid kasutatakse vaid nende kogumise eesmärgist lähtuvalt. Niisugusel jälgimisseadmestiku kasutamisel ei ole vaja kaamerate vaatevälja sattuvate inimeste nõusolekut, kui on piisavalt selgelt teavitatud jälgimise fakt, andmete töötleja ning tema kontaktandmed.

Inimese õigus privaatsusele ruumis, kus seda normaalselt võib eeldada, kaalub üles kaamera omaniku õiguse kaitsta oma vara võimaliku varguse või vandalismi eest. Samuti on lubamatu kasutada valvekaameraid kellegi tegevuse varjatud jälgimiseks. Niisugust tegevust võib teatud juhtudel käsitleda karistusseadustiku § 137 kohaselt kuriteona.

Valvekaamerad kaubanduskeskustes

Andmekaitse Inspektsioonile laekus 2017. aasta jooksul mitmeid selgitustaotlusi ja märgukirju, milles viidati võimalikule isikuandmete töötlemise ülemäärasusele kaubanduskeskustes. Näiteks olukord, kus kaupluse valvekaamera on seadistatud selliselt, et vaatevälja jääb ka proovikabiinis toimuv. Et kontrollida valvekaamerate kasutamise vastavust seaduses sätestatule, viisime 2017. aasta sügisel kaubanduskeskustes läbi vastavasisulise seire. Seiratavate keskuste valimisel sai lähtutud põhimõttest, et seire ei tohi olla Tallinna-keskne ning iga keskus kuuluks erinevale omanikule. Nii oli välistatud võimalus, et mõne ettevõtte sisemine töökorraldus või regioonist tulenev iseärasus moonutaks seire tulemusi. Kokkuvõtvalt meile esitatud viited ja kahtlustused kinnitust ei leidnud. Peamine kõrvalekalle valvekaamerate kasutamise nõuete täitmisel oli asjakohase teavituse puudumine.

Korteriühistute valvesüsteemid

Valvetehnika taskukohasemaks muutumine on viinud ka paljud korteriühistud mõttele oma avalikke alasid ja ruume videovalvesüsteemide abil tõhusamalt kaitsta. Paraku juhtub vahel, et valvesüsteemi vajaduse teadvustamine ning selle teadmise ühistu liikmetele edastamine kui oluline etapp süsteemi hankimisel ei pälvi piisavat tähelepanu. Nõnda võib tekkida olukord, kus ühistu liikmed, kes tunnevad, et nende arvamusega ei ole arvestatud, hakkavad aktiivselt nõudma juba paigaldatud süsteemi mahavõtmist. Seega, sama oluline kui sobivate parameetritega kaamerate hankimine, paigaldamine ning nõuetekohase teavituse ülespanek, on ühistute puhul eelnev teavitustöö ja kokkuleppe saavutamine.

Valvekaamerad eriaisikute käsutuses

Eraisikute vahelistesse vaidlustesse Andmekaitse Inspektsioon reeglina ei sekku, välja arvatud juhtudel, kui täidetud on kõik kolm korrakaitseseaduse § 4 lõikes 2 toodud tingimust:

a) kohtulikku õiguskaitset ei ole õigeaegselt võimalik saada;
b) korrakaitseorgani sekkumiseta on isikul raske või võimatu oma õigusi realiseerida ning
c) kui ohu tõrjumine on avalikes huvides.

Kuigi eraisikute puhul kehtib kaamerate kasutamisel isikliku tarbe erand, ei laiene see valvekaamerate kasutamisele. Siiski on ka siin sagenenud probleemid valvekaamerate õiguspärase kasutamisega. Enamasti on murekohaks seadusest tuleneva minimaalsuse nõude eiramine, ehk kaamerad paigaldatakse küll eesmärgiga oma varal silma peal hoida, kuid selle asukoha või asendi tõttu jääb vaatevälja ka näiteks naabri uks. Hoolimata headest kavatsustest ei pruugi niisugune olukord naabrile sugugi meeldida ning tal on seaduslik õigus nõuda kaamera eemaldamist või asendi muutmist, ehk tema isikuandmete töötlemise lõpetamist.

AVALIKU TEABE KÄTTESAADAVUS

Elve Adamson, peainspektor

Igapäevases kasutuses tähendab mõiste "avalik teave" teavet, millele pole juurdepääsupiiranguid kehtestatud. Avaliku teabe seaduse tähenduses on avalikuks teabeks, siiski teave, mis on loodud või saadud seaduses või selle alusel antud õigusaktis sätestatud avalikke ülesandeid täites. Seega kogu riigiasutuste käes olev teave, kui sellele ei ole juurdepääsupiiranguid kehtestatud, peaks olema avalikkusele vabalt juurdepääsetav.

Demokraatliku riigi ja avatud ühiskonna toimimise seisukohalt on äärmiselt oluline, et inimestel oleks võimalus riigiga suhelda ning avalike ülesannete täitmisega seotud dokumentidega tutvuda. Vabalt toimiv teabevahetus aitab kaasa avaliku võimu teostamise läbipaistvusele ning annab avalikkusele võimaluse kontrollida riigi tegevust. Samuti elavdab riigipoolne infoedastus koostööd kodanikega (osalusdemokraatia).

Ametiasutuste teabe andmise kohustus peab olema selge ja piisavalt täpne, et iga ametnik saaks aru, milline teave millisel kujul kuulub avalikustamisele ja millisele teabele tuleb juurdepääsu piirata. Kahjuks on siiski arusaam sellest asutustes erinev.

Infovabaduse põhimõtte järgimise muudab keeruliseks teabe hindamine selle avalikustamise seisukohalt. 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 omaalgatuslikult veebilehel avalikustama. See, kui seadus ei kohusta teavet võrgulehel avalikustama, ei tähenda seda, et kogu ülejäänud teave oleks piiranguga.

Praktikas valmistab probleeme teabele juurdepääsu andmise või mitteandmise otsustamine. Igaühe õigus info saamiseks avaliku võimu organite ja ametiisikute tegevuse kohta ei ole piiramatu. Juurdepääs ei laiene andmetele, mille väljaandmine on seadusega keelatud ja eranditult asutusesiseseks kasutamiseks mõeldud andmetele.

Kui enamikel juhtudel on seaduses täpselt sätestatud, millisele teabele tuleb juurdepääsu piirata, siis on seadustes ka mõningad sätted, mille puhul tuleb teabevaldajal langetada otsus piirangu kehtestamise osas kaalutlusotsuse alusel ning vajadusel ka oma otsust põhjendada. Inspektsioon ei saa teabevaldajate eest vastavaid otsuseid langetada, kuigi üsna tihti seda inspektsioonilt küsitakse.

Teabenõuetele vastamine

Kõige levinum asutustelt teabe küsimise viis on teabenõude esitamine, kui teave ei ole avalikustatud või veebilehelt leitav. Nii teabenõuete esitamisel kui ka neile vastamisel on mõlemal poolel nii õigused kui kohustused. Kuigi teabenõude esitamisel ei pea teabenõudja selgitama, miks ta konkreetset teavet soovib ega ka täpselt teadma soovitud dokumendi pealkirja või dokumendi numbrit, peab teabenõudest olema siiski arusaadav, millist teavet teabenõudja soovib. Siinkohal on seadusandja pannud teabevaldajale kohustuse teabenõudja abistamiseks ning jätnud võimaluse teabenõude täitmisest keeldumiseks, kui teabenõude täpsustamisel ei selgu, millist teavet teabenõudja soovib.

> Näitena, kus kohustused ei ole ainult teabevaldajal vaid ka teabenõudjal, võib tuua teabenõude, kus isik soovis koopiaid *asjaajamiskorrast, ametijuhenditest, käskkirjadest ja kõik otsused, mis puudega …. jne.* Kui teabevaldaja palus täpsustada, *milliseid käskkirju, otsuseid, protokolle soovitakse,* leidis vaide esitaja, et teabenõue ei vaja täpsustamist, kuna *teabenõudes on piisavalt arusaadav, millist teavet soovitakse.*
>
> Inspektsioon vaide esitajaga siiski ei nõustunud, kuna ka inspektsioonile polnud arusaadav, mis ajavahemiku kohta milliseid käskkirju, protokolle ja otsuseid soovitakse ning kas soovitakse ainult vallavalitsuse või ka volikogu ja volikogu komisjonide otsuseid ja protokolle.

Kui teabenõue on arusaadav küll teabenõudjale, kuid pole üheselt arusaadav teabevaldajale, siis pole teabenõuet võimalik täita. Ei saa eeldada, et teabevaldaja peaks oskama teabenõudja soove ära arvata, kui teabenõudja pole neid piisavalt selgelt edastanud. Ka AvTS § 23 lg 1 p 3 lubab teabevaldajal keelduda teabenõude täitmisest, kui täpsustamisel ei selgu, millist teavet teabenõudja taotleb.

Kui teabevaldaja keeldub teabenõude täitmisest, siis tuleb seda ka põhjendada, nii ütleb AvTS § 23 lg 3. Seega ei saa pidada põhjendatuks keeldumist, kui teabevaldaja keeldub teabenõude täitmisest põhjusel, et peab põhjendatuks teabe väljastamist või teabele kehtivad juurdepääsupiirangud. Selliseid keeldumisi on praktikas üsna tihti. Teabevaldajad saavad keelduda teabe väljastamisest ainult juhul, kui keeldumiseks on seadusest tulenev alus. 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*.

Samuti on jätkuvalt üheks levinumaks rikkumiseks teabenõudele tähtaegselt vastamata jätmine. Ka juhul kui kodanik on pealkirjastanud oma pöördumise teabenõudena, kuid sisult on tegemist selgitustaotlusega, tuleb 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.

Samuti oli sagedamini vaidemenetlusi seoses teabe väljastamisest keeldumisega põhjusel, et dokument sisaldab piiranguga teavet või et tegemist ei ole teabega mida AvTS § 28 kohustab veebilehel avalikustama või millele AvTS § 36 keelab piirangut kehtestada. See kui tegemist ei ole dokumendiga, mida tuleb veebilehel avalikustada või teabega, millele seadus ei luba juurdepääsu piirata, ei tähenda see seda, et sellist teavet ei pea ka teabenõude korral väljastama. Teabe väljastamisest saab keelduda siiski üksnes juhul, kui tegemist on seaduses sätestatud piiranguga teabega.

Enne teabenõuetele vastamist soovitan teabevaldajatel teabenõuded tähelepanelikult läbi lugeda, et ei jääks midagi tähelepanuta. Vaadata üle, kas dokument sisaldab piiranguga andmeid ning kas piirangud on kehtivad või lõppenud ning 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.

Omaalgatuslikud järelevalved

Kuna inspektsiooni järelevalvepädevusse kuulub järelevalve teostamine teabenõuetele vastamise, teabe avalikustamise ja AK teabe kaitsmise üle, siis võib inspektsioon järelevalve algatada, kas vaide alusel või oma algatusel. Oma algatusel alustab inspektsioon järelevalvet eelkõige nendel juhtudel, kui inspektsiooni on teavitatud teabe avalikustamisel toimunud rikkumistest või on inspektsioon veebilehtede kontrollimisel tuvastanud rikkumise.

Nii näiteks algatas Inspektsioon omaalgatusliku järelevalvemenetluse Rae valla suhtes, kus uue kasutusele võetud haridusinfosüsteemi ARNO, mille kaudu on võimalik esitada Rae vallale elektrooniliselt erinevat liiki taotlusi (sh sotsiaalabi taotlused) ning mis teostab dokumendi automaatregistreeringu valla dokumendihaldusprogrammis Amphora, oli taotluste automaatregistreerimisel tekkinud olukord, kus programm ei ole seadnud ühetaolistele taotlustele vaikimisi juurdepääsupiiranguid ning paljud taotlused, mis sisaldasid ka piiranguga andmeid, said dokumendiregistri kaudu avalikuks. Järelevalve tulemusena piiranguga dokumentidele juurdepääs suleti.

Samuti algatas inspektsioon omaalgatusliku järelevalve KEMITi metsaregistri suhtes, mis ei vastanud aasta alguses seaduses sätestatud nõuetele. Järelevalvemenetluse käigus avalikustati 11.09.2017 uuendatud metsaregister, mis võimaldab kõiki registris tehtavaid tegevusi logida ning tagada registri andmetele juurdepääsu vajaduspõhiselt. See tähendab, et kui isikul on metsaregistrile juurdepääsu õigus ei tähenda see seda, et näeb kõiki metsaregistri andmeid, vaid üksnes neid andmeid, mis tal on oma ülesannete täitmiseks vaja. Kuna täiendava kontrollimise hetkeks oli uus metsaregister olnud kasutusel väga lühikest aega, siis logide kontrolli (millest nähtuks, kas registri kasutamine on olnud õiguspärane) veel tehtud ei olnud. Selles osas tuleb teha täiendav kontroll.

Ka jäi eelmise aasta kohta silma see, et rikkumisest teavitavad kõige enam just töölt lahkunud inimesed ning volikogude ja valimisliitude liikmed, et nende asutuses ei avalikustada kõiki dokumente nõuetekohaselt. Siinkohal tahaks panna nii endistele töötajatele kui ka volikogu liikmetele südamele, et mõnikord saab kiirema lahenduse siis, kui kõigepealt teavitada teabe avalikustama jätnud asutust. Tihti ei ole tegemist tahtluse, vaid juhusliku eksimuse või tähelepanematusega. Alles siis, kui asutus viga ei paranda, tasub pöörduda inspektsiooni.

Siinkohal on asutustele soovitus, et vaadata vahel oma dokumendiregistrit ka kodaniku- ehk välisvaates. Nii on eksimused koheselt tuvastatavad. Ei tasu jääda ootama, kuni mõni kodanik või inspektsioon need kontrolli käigus avastab, sest sellisel juhul järgneb järelevalvemenetlus ning kui tegemist on piiranguga teabe avalikustamisega, siis võib järgneda ka väärteomenetlus.

AK teabe kaitse kohapealsed kontrollid

16.01.2016 jõustus avaliku teabe seaduse § 45 lg 1 p 2, mis andis inspektsioonile järelevalvepädevuse kontrollida asutusesiseks kasutamiseks mõeldud teabe kaitsmist, sh teostada ka kohapealseid kontrolle. Kontrollide läbiviimise eesmärgiks oli tutvuda kohapeal

kuidas asutuses käideldakse AK teavet, kellel on AK teabele juurdepääs ning milliseid turvameetmeid rakendatakse.

Et saada ülevaade olukorrast AK teabe kaitse osas asutustes, valiti kontrolli objektideks välja eri valdkondadest kümme asutust, mille hulgas oli nii riigiameteid, koole, omavalitsusi kui ka riigiametite maakondades asuvaid osakondi.

Kontrollide raames vaadati

- milliseid isikutuvastamise viise kasutatakse infosüsteemidesse ja ruumides sissepääsul,
- kas ja kuidas instrueeritakse uusi töötajaid nii AK kui ka infoturbe alal,
- kes annab ja kontrollib piiranguga teavet sisaldavatele infosüsteemidele juurdepääse ning kas tegevusi kontrollitakse,
- kuidas toimub tundlike andmete edastamine,
- kuidas on riskid maandatud, kui AK teavet töödeldakse kodutööl,
- kas ja kes kontrollivad AK märgete panemist,
- kuidas on tagatud, et AK teabele ei ole juurdepääsuõigust selleks õigust mitteomavatel isikutel ning
- kuidas toimub tundliku teabe säilitamine ja hävitamine.

Kümnest läbiviidud kohapealsesse kontrollist olid kuuel juhul kaasatud eksperdid ka RIAst, kes hindasid põhjalikumalt infoturbereeglite täitmist. Kõikide läbiviidud kontrollide osas koostati ka kontrollakt, milles juhiti tähelepanu kontrolli käigus esinenud puudustele ja tehti ettepanekuid puuduste kõrvaldamiseks.

Kontrolli käigus tuvastatud puudused

Üheks puuduseks keskasutuste osakondade puhul oli see, et kohapeal puudub kompetents, kes oskaks koheselt AK teavet või infoturvet puudutavaid küsimusi lahendada. Selleks pöörduvad osakonnad keskasutuste poole, kus vastav kompetents on olemas. Tihti tunnistasid ka asutused, et korrad AK teabe kaitse ja infoturbe küsimustes on küll olemas, kuid reaalselt ei kontrollita nende täitmist (näiteks paroolide vahetamise sagedust ega ka seda, kes mis eesmärgil andmeid vaatas). Seda tehakse kaebuste või intsidentide korral. Kõigis asutustes on siiski tundlikele andmetele juurdepääs võimaldatud ainult vajaduspõhiselt, st et kõik ametnikud kõiki andmeid ei näe, vaid juurdepääsud on antud tööülesannetest lähtuvalt.

Kontrollide käigus tuvastasime ka, et kõik asutused ei vasta kodanike pöördumistele, mis on pealkirjastatud „Teabenõue“ viie tööpäeva jooksul. Enne kohapealset kontrolli kontrollisime ka asutuste dokumendiregistreid, kus esines puudusi nii piirangu aluste kui ka tähtaegade märkimisel. Samuti olid ühe asutuse dokumendiregistris üksikud dokumendid, kus olid füüsiliste isikute nimed avalikud. Kõigile nendele puudustele juhtisime kohapeal ja täiendavalt ka kontrollaktides tähelepanu.

Siinkohal tahaks asutuste juhtidele, kellel on osakonnad erinevates Eesti piirkondades, panna südamele, et igas üksuses peaks olema keegi, kes oskaks lahendada ja anda nõu AK teabe alastes küsimustes. Sellest ei piisa, kui selline kompetents on ainult keskasutuses, sest tihti vajavad sellised küsimused kiiret lahendust.

Koordinaatorite võrgustik ja avaliku teabe nõukogu

Seni on inspektsiooni juures tegutsenud koordinaatorite võrgustik, kes tegeles peamiselt isikuandmete kaitse ja avalikule teabele juurdepääsu küsimustega. Kuna aga 2018. aastal jõustuvad kolm uut õigusakti, siis küsimuste ring millega tuleb tegeleda, on laiem. Uuteks õigusaktideks on isikuandmete kaitse üldmäärus, mis on küll otsekohalduv, kuid jätab võimaluse teha siseriiklike õigusaktidega siiski teatud erisusi, õiguskaitse valdkonna direktiiv, mille osas koostatakse rakendusakti, ning küberturvalisuse seadus.

Samuti pani 2017. aasta suvel jõustunud teenuste korraldamise ja teabehalduse aluste määrus Andmekaitse Inspektsioonile kohustuse koordineerida asutusteülest teenuste arengut teabele juurdepääsu ja teabe kaitse korraldamisel. Nende ülesannete täitmiseks nägi määrus ette inspektsiooni juurde nõukogu moodustamise. Nõukogu eesmärgiks on toetada Andmekaitse Inspektsiooni tegevust teabele juurdepääsu ja teabe kaitse koordineerimisel riigiasutustes. Nõukogusse kuuluvad ministeeriumide ja Riigi Infosüsteemi Ameti esindajad.

Inspektsiooni soov oli nõukogu töösse sisse tuua ja läbi arutada peale teabele juurdepääsu ja AK teabe kaitse küsimuste ka andmekaitse määruse küsimusi laiemalt, kuna need on avaliku teabega, sh teabele juurdepääsu korraldusega, läbi põimunud. Nii kuuluvad nõukogusse nii dokumendihalduse spetsialistid kui ka asutuse infoturbega tegelevad spetsialistid, kes vahendavad nõukogus arutatut ka oma haldusala allasutustele.

Kuna nõukogu on asutusteülene, siis ei tegele nõukogu eraldi probleemidega, mis puudutavad ainult kitsalt ühte asutust. Samuti ei tegeleta nõukogu raames koolitustega. Kui mingis küsimuses on palju halli ala, mille osas ei ole kindlaid seisukohti, siis neid arutatakse, kuid see ei tähenda seda, et inspektsioon ütleks igas olukorras ette, mida tuleb teha.

Esimene uue nõukogu koosolek toimus novembris. Koosolekul anti ülevaade uue nõukogu tegevussuundadest ja uue andmekaitseõiguse rakendamisest ning ettevalmistusest andmekaitsereformiks valitsusasutustes. Samuti räägiti sellest, mida tuleb arvestada teenuste korraldamisel ja teabehalduses ning anti ülevaade küberturvalisuse seaduse eelnõust.

Kuna andmekaitse üldmäärus jõustub 2018. aasta maist, siis 2018. a esimesel poolaastal nõukogus arutatavad teemad on enamjaolt seotud just uue isikuandmete kaitse üldmääruse ja selle rakendamisega.

Vaidemenetlused

Teabenõude korras asutuse töötaja foto küsimine

Kodanik esitas Terviseametile teabenõude, milles soovis saada ühe töötaja fotot. Kuna Terviseamet kodaniku teabenõudele ei vastanud, esitas kodanik vaide. Inspektsiooni poolt tehtud järelepärimise vastuses põhjendas Terviseamet teabenõudele vastamata jätmist sellega, et peab teabenõude esitajat anonüümseks, kuna oli seisukohal, et teabenõudja esineb vale nime all ning isik ei ole tuvastatav. Seetõttu ei registreeritud ka teabenõuet.

Andmekaitse Inspektsioon Terviseameti seisukohtadega ei nõustunud, kuna avalikku teavet võib küsida igaüks ning teabevaldaja ei saa teabenõudjat ignoreerida, kuna arvab, et sellist inimest ei eksisteeri. Teabenõudele tuleb reageerida igal juhul – kas keelduda teabenõude

täitmisest või teabenõue täita. Teabenõudja isik tuleb tuvastada siis, kui küsitakse teavet, milles sisalduvad tema või kolmandate isikute juurdepääsupiiranguga isikuandmed. Kui isik taotleb juurdepääsupiiranguga isikuandmeid kolmandate isikute kohta, teatab ta teabevaldajale lisaks ka teabele juurdepääsu aluse ja eesmärgi.

Teabenõudja on küsinud ametniku isikuandmeid, mis ei ole seaduse alusel avalikud. Ametniku foto tuleb lugeda juurdepääsupiiranguga isikuandmeteks, millele juurdepääsu võimaldamine kahjustaks oluliselt andmesubjekti eraelu puutumatust. Antud olukorras ei näe inspektsioon ühtegi pädevat alust, mis annaks teabenõudjale õiguse ametniku foto välja nõuda. Seega oleks Terviseamet pidanud vastavalt AvTS 23 lg 1 punktile 1 teabenõude täitmisest keelduma, kuna taotletava teabe suhtes kehtivad juurdepääsupiirangud ja teabenõudjal ei ole taotletavale teabele juurdepääsuõigust. Inspektsioon leidis, et teabenõudele reageerimata jätmisega on Terviseamet rikkunud teabenõuete menetlemise korda.

Eksamitööde hindamisjuhendite väljastamata jätmine

Kodanik esitas SA-le Innove teabenõude, milles soovis saada matemaatika eksamitöö hindamisjuhendit oma e-posti aadressile, kuid SA Innove keeldus dokumendi väljastamisest soovitud viisil põhjusel, et hindamisjuhend on eelkõige töödokument hindajale. Seetõttu on vajalik, et hindamisjuhendis olevat selgitab asjaoludega kursis olev spetsialist, kuna muul juhul on tõenäosus eksiarvamuse tekkimiseks suur ja lõppkokkuvõttes ei saa sellest kasu ei teabe taotleja ega ka teabe valdaja.

Samas nii SA Innove kui Haridus- ja Teadusministeerium tõdesid, et hindamisjuhendi puhul on tegemist avaliku teabega, millele ei ole kehtestatud juurdepääsupiiranguid. Samuti leidis SA Innove, et teabenõude täitmise viisi valikul tuleb hinnata, mis on teabenõude sisuline eesmärk ning leiab, et antud juhul oleks teabenõudjal vajalik soovitud teabega tutvuda SA Innove ruumides koos asjaoludega kursis oleva spetsialistiga, kes saab anda selgitusi eksamitöö tulemuse ja hindamisjuhendi vahelisest seosest.

Andmekaitse Inspektsioon ei nõustunud sellise põhjendusega. Teabenõude esitamise sisulist eesmärki teab kõige paremini teabenõudja ise. Seega pole asjakohane ega põhjendatud, et teabenõude esitamise eesmärki hakkab teabevaldaja omal käel ning vastuolus teabenõudja sooviga ümber hindama. Teabevaldaja on küll AvTS § 15 lõike 2 alusel kohustatud teabenõudjat igakülgselt abistama teabenõude esitamisel ning teabenõudjale vajaliku teabe, selle asukoha ja teabenõudjale sobivamate võimalike juurdepääsuviiside väljaselgitamisel ning teabevaldaja võib küll tutvustada erinevate juurdepääsuviiside kasutegureid teabenõudjale, kuid endale sobivaima juurdepääsuviisi üle otsustab siiski lõpuks teabenõudja.

Seega oleks saanud antud olukorras lugeda põhjendatuks, et SA Innove oleks teabenõude täitmisel teabenõudja soovitud viisil tutvustanud lisaks võimalust tutvuda hindamisjuhendiga ka spetsialisti juuresolekul SA Innove ruumides, kuid mitte jätta sellel põhjusel teabenõue teabenõudja soovitud viisil täitmata.

Inspektsioon kohustas SA Innove uuesti läbi vaatama vaide esitaja teabenõude matemaatika riigieksamitöö hindamisjuhendi väljastamiseks ja väljastama nõutud teabe teabenõudja soovitud viisil, kui ei esine ühtegi seadusest tulenevat konkreetset alust teabe soovitud viisil väljastamisest keeldumiseks. SA Inniove täitis ettekirjutuse ja väljastas vaide esitajale soovitud teabe.

Kriminaaltoimiku materjalidega tutvumine

Vaide esitaja esitas inspektsioonile Lõuna Prefektuuri tegevuse peale kaebuse, mille kohaselt ei võimaldatud temal kui kannatanul tutvuda kriminaalasja toimikuga ning ühtlasi palus vaide esitaja teha kriminaaltoimikus parandusi. Kuna menetluse käigus selgus, et tegemist on poolelioleva kriminaalmenetlusega, siis tagastas inspektsioon pädevuse puudumisel vaide läbi vaatamata.

Õigus enda kohta andmeid saada ning nõuda andmete parandamist tuleneb küll isikuandmete kaitse seadusest, kuid seda juhul, kui eriseaduses ei ole ette nähtud teistsugust korda. Kui eriseaduses on teabele juurdepääsuks avaliku teabe seadusest või isikuandmete kaitse seadusest erinev kord, siis tuleb lähtuda eriseaduses sätestatud korrast. Kuna kriminaalmenetluse raames on tõendite esitamiseks, vaidlustamiseks ja dokumentidega tutvumiseks ette nähtud erikord, siis puudub inspektsioonil pädevus sekkuda menetlusse ning kontrollida esitatud andmete/tõendite õigsust või kohustada võtma mingeid dokumente menetluse juurde. Kui on tehtud ebaõige otsus, siis on seda võimalik vaidlustada menetlusseadustikus ettenähtud korras.

Kannatanu õigusi toimikuga tutvumisel kriminaalmenetluse raames reguleerib KrMS ning õiguste rikkumise korral on kaebeõigus samuti sätestatud KrMS-s ehk eriseaduses (§-d 228-230). Seega ei rakendu menetluse ajal kriminaaltoimikule juurdepääsu võimaldamisele ega teabe väljastamisele avaliku teabe seadus. Kriminaalmenetluse läbiviimise õiguspärasuse, sh esitatud andmete/tõendite õiguspärasuse ning menetlusosaliste õiguste tagamise üle teostavad kontrolli prokuratuur ja kohus. Seega puudus inspektsioonil pädevus vaide lahendamiseks ning inspektsioon tagastas vaide läbi vaatamata.

ANDMEKAITSE INSPEKTSIOONIGA SEOTUD KOHTULAHENDID

Raavo Palu, õigusdirektor

Üheks järelevalveasutuse tegevuse mõõdupuuks on ka tema tehtavate otsuste ja toimingute vastavus seadusandlusele. Meie tegevuse kontrollimiseks on võimalik esitada meile vaie, et me hindaksime oma tegevuse uuesti üle või esitada kaebus halduskohtusse. Viimast varianti on igal aastal mõnel korral kasutatud ning eelmisel aastal lõppesid mõned kohtuasjad, mis olid seotud meie tehtavate toimingute või haldusaktidega. Neist tähelepanuväärsematena tooksime välja kaks kohtuasja.

Menetluse algatamata jätmine korrakaitseseaduse § 4 lõike 2 alusel

Selle kaasuse selgitamiseks on vaja selgitada ka pisut taustalugu. Kuna see kohtuotsus ei ole leitav Riigi Teatajast kohtumenetluse kinniseks kuulutamise tõttu, siis toome ka taustainfo võimalikult üldistatult, et mitte riivata osaliste eraelu puutumatust. Leiame, et selle kohtumenetlusega seotud lõppseisukohad on aga vajalik välja tuua ennekõike ka teiste korrakaitseorganite jaoks.

Kaebaja perekonnas toimus 1990-ndatel sündmus, mis mõjutab senini nende pere-elu: üks pereliikmetest langes alaealisena kuriteo ohvriks. Viiteid sellele sündmusele kajastati neljas meediaartiklis, mis avaldati ligikaudu kümmekond aastat peale selle sündmuse toimumist ning 2016. aastal sooviti sel teemal uuesti artiklit kirjutada.

Kaebajad nõudsid meediaväljaandelt nende artiklite eemaldamist ning veel valmimata artikli avaldamata jätmist, kuid tulutult – nende soovidele ei tuldud vastu. Veel kirjutamata ning avaldamata artikli osas läksid kaebajad meediaväljaande peale kohtusse ning samal ajal esitasid ka Andmekaitse Inspektsioonile kaebuse nende nelja varasema artikli eemaldamiseks selle meediaväljaande võrgulehelt. Kõigi nende toimingute juures (suhtluses meediaväljaandega, meiega ning halduskohtuga) olid kaebajatel võetud vandeadvokaatidest esindajad.

Me jätsime oma otsusega menetluse algatamata, tuues põhjenduseks korrakaitseseaduse § 4 lõike 2 ning nende tingimuste mittetäitmise. Viidatud korrakaitseseaduse sätte kohaselt võib haldusorgan asuda riikliku järelevalve käigus eraõiguslike isikute vahelisi suhteid lahendama ainult järgmistel tingimustel:

a) inimesel ei ole kohtulikku õiguskaitset võimalik õigel ajal saada
b) ja ilma korrakaitseorgani sekkumiseta ei ole õiguse realiseerimine võimalik või on oluliselt raskendatud ning
c) kui ohu tõrjumine on avalikes huvides.

Korrakaitseseaduse eelnõu seletuskirjas on selle paragrahvi kohta selgitatud, et inimeste õiguste kaitsmine on eelkõige kohtuvõimu funktsioon. Kui täitevvõim korrakaitseorganite (milleks on ka Andmekaitse Inspektsioon) näol hakkaks lahendama eraisikute õigusi ja vabadusi puudutavaid küsimusi, konkureerides kohtuvõimuga, tooks see kaasa võimude lahususe põhimõtte rikkumise, tekiks õiguskindlusetus ja omavolioht. Korrakaitseorganid ei suuda ega peagi suutma igal juhtumil kindlaks teha isikute vahelisi tegelikke õigussuhteid,

mis eraõiguslike vaidluste lahendamisel võib olla vägagi keeruline.[5] Tsiviilkohtu volitused ja võimalused asjaolude tuvastamiseks on oluliselt ulatuslikumad kui haldusorganil.

Leidsime, et konkreetsel juhul ei olnud ühtegi asjaolu, mistõttu ei oleks kaebajatel olnud võimalik oma õigusi ise kaitsta. Üksnes kohtumenetluse kulud või keerukus iseenesest ei tähenda, et inimese õigusi peaks asuma kaitsma korrakaitseorgan. Inimesel on võimalik palgata endale õigusnõustaja või advokaat ning vajadusel taotleda riigilt abi õigusabikulude kandmiseks. Menetluse mittealgatamise hetkel oli juba tsiviilkohtus vaidlus kaebajate ja meediaväljaande vahel kavandatava uue artikli kirjutamise keelamise osas. Kaebajatel oli võimalus oma tsiviilkohtusse esitatud kaebust täiendada ka juba avaldatud artiklite eemaldamiseks. Menetluse algatamata jätmisel arvestasime, et vaidlusalused artiklid ei olnud avaldatud vahetult enne kaebuse esitamist – tegemist polnud aegkriitilise andmete avaldamise lõpetamise vajadusega. Samuti leidsime, et tsiviilkohtul on võimalik anda hinnang ka võlaõigusseaduse § 1046 kohaselt. Selle sätte kohaselt on isiku nime või kujutise õigustamatu kasutamine, eraelu puutumatuse või muu isikliku õiguse rikkumine õigusvastane, kui seadusega ei ole sätestatud teisiti. Sellise kaebuse lahendamine tähendaks ka sekkumist ajakirjandusvabadusse – toimuks kahe põhivabaduse (ajakirjandusvabadus *vs* eraelu puutumatus) konkureerimine, mille hindamine on mahukas ja põhjalik protsess. Selliste vaidluste lahendamine ja hindamine on kohasem kohtule mitte korrakaitseorganile. Seetõttu leidsime, et see vaidlus on ennekõike lahendatav tsiviilkohtus.

Kaebajad ei nõustunud menetluse algatamata jätmisega ning esitasid esmalt meile vaide menetluse algatamata jätmise teate peale. See vaie jäi rahuldamata, mistõttu kaebajad esitasid meie tegevuse peale kaebuse Tallinna Halduskohtusse. Kaebajad olid seisukohal, et Andmekaitse Inspektsioon ei saa kasutada korrakaitseseaduse § 4 lõiget 2 otsustamaks mingi menetluse algatamata jätmist. Tallinna Halduskohus kaebajatega ei nõustunud ning nõustus meie seisukohtadega.

Kohus nõustus meie seisukohaga korrakaitseseaduse § 4 lg 2 tõlgenduse osas ning et riikliku järelevalvet teostatakse eelkõige avaliku korra tagamise eesmärgil, millele viitavad korrakaitseseaduse (KorS) § 2 ja § 4 lg 2 oma koosmõjus.

> *„Vaidlust ei ole, et Andmekaitse Inspektsioon on riiklikku järelevalvet teostav korrakaitseorgan andmekaitse vallas. Kohus nõustub vastustajaga, et KorS § 4 lg 2 annab üldnormina korrakaitseasutustele võimaluse järelevalvetegevuse käigus eraõiguslike isikute vahelisi suhteid lahendada ainult selles toodud eelduste olemasolul. Andmekaitse Inspektsiooni eripädevusi või järelevalve eesmärke järelevalvemenetluse teostamisel isikuandmete kaitse seadus (edaspidi IKS) täpsemalt ei reguleeri. Põhiline [Andmekaitse Inspektsiooni] pädevus järelevalve teostamiseks on toodud IKS § 32 lg 1, mis näeb ette, et [inspektsioon] teostab IKS ja selle alusel kehtestatud õigusaktides sätestatud nõuete täitmise üle riiklikku ja haldusjärelevalvet. Kohus leiab, et selle teostamisel tuleb tal muuhulgas lähtuda KorS § 2 ja § 4 lg 2 toodust, sest IKS ei anna talle täiendavat eripädevust või ülesandeid riikliku järelevalve teostamisel isikuandmete kaitse osas eraisikute vahelistes suhetes. Kohus märgib ka, et nii kaebajad kui ka [inspektsiooni] poolt korduvalt märgitud Andmekaitse Inspektsiooni 19.11.2015 kinnitatud sekkumiskriteeriumid, on sisuliselt selgituseks, millised on need olukorrad, kui vastustaja peab võimalikuks*

[5] Korrakaitseseaduse eelnõu seletuskiri, lk 20.

> *sekkuda meedia töösse. Sisuliselt tähendab see KorS § 4 lg 2 abstraktse sõnastuse ilmestamist näidetega praktilisest elust.“*

Samuti nõustus kohus meiega, et eraõiguslikes suhtes oma õiguste maksmapanekuks on Eestis ette nähtud eelkõige tsiviilkohtusse pöördumise võimalus.

> *„Kohus märgib, et kaebajad on ise selgitanud haldusorgani poole pöördumist eelkõige menetlusökonoomia ja lootusega saada oma õigustele kaitse kiiremini, kui tsiviilnõudega kohtusse pöördumisel. Kohus märgib, et nõustub siinkohal [inspektsiooniga], et see väide ei ole muuhulgas õige ka sisulises plaanis, sest kohtusse pöördumisel oleks kaebajatel olnud võimalus taotleda ka esialgset õiguskaitset, milline taotlus lahendatakse kiireloomulisena. Samuti juhtis [inspektsioon] vaidlustatud otsuses ja vaideotsuse õigesti tähelepanu asjaolule, et kaebajatel oli võimalik juba menetletavas tsiviilasjas […] esitada täiendavad nõuded ja tsiviilkohus on oma volitustega ja võimalustega asjaolude tuvastamiseks selliste vaidluste lahendamiseks sobivam koht.“*

Kohus jõudis järeldusele, et järelevalvemenetluse algatamisel on IKS § 33 lg 5 jätnud kaalutlusruumi Andmekaitse Inspektsioonile. Ka järelevalve algatamisest keeldumise otsus on kaalutlusotsus ning kohus leidis, et kaalutlusotsused (järelevalve algatamisest keeldumise otsus ning vaideotsus) olid õiguspärased ja nende langetamisel ei ole rikutud kaalutlusõigust.

Eeltoodud kohtuotsusega nõustus kohus, et korrakaitseorganil (sh ka Andmekaitse Inspektsioonil) on riiklikus järelevalvemenetluses võimalik tugineda menetluse algatamise otsustamisel korrakaitseseaduse § 4 lõikest 2, sh et menetluse algatamiseks on vajalik kõigi selles lõikes toodud nõuete samaaegne täitmine.

Eesti Interneti SA kui teabevaldaja avaliku teabe seaduse mõistes

Järgnev juhtum annab aimu, kuivõrd segane on avaliku ülesande määratlemine, seda eriti eraõiguslike juriidiliste isikute korral ning iseäranis siis, kui riik ise on olnud osaline selle juriidilise isiku moodustamises ning osaleb selle tegevuses.

Eraisik esitas Eesti Interneti SA-le (EIS) teabenõude, millega palus talle väljastada .ee-lõpuliste domeenide nimekiri sama päeva seisuga. EIS keeldus nimekirja väljastamast, sest EIS ei ole teabevaldaja avaliku teabe seaduse mõistes ja nõutud teave ei ole avalik teave. Ükski seadus ei reguleeri domeeninimede reguleerimist ning EIS-i tegevus selle ülesande täitmisel ei rajane ühelgi õigusaktil. Selle vastusega eraisik ei nõustunud, mistõttu ta esitas meile vaide.

Jätsime oma vaideotsusega esitatud vaide rahuldamata.[6] Lõppjäreldustes märkisime, et EISi poolt .ee lõpulise domeeniregistri pidamise puhul on oma olemuselt tegemist avaliku teenuse osutamise ehk avaliku ülesande täitmisega AvTS § 5 lg 2 mõistes. See, et EIS täidab avalikke ülesandeid, on tuletatav 05.02.2009 Vabariigi Valitsuse korraldusest nr 39 ja EIS-i põhikirjast. Samas nõustusime EIS-ga selles, et domeeniregistri pidamist ei reguleeri üksi seadus ega seaduse alusel antud õigusakt. Majandus- ja Kommunikatsiooniministeerium kui EISi asutaja on avaliku ülesande delegeerinud EIS-le puuduliku regulatsiooniga ehk siis domeeniregistri pidamine EIS-le ei ole delegeeritud ei seaduse, haldusakti ega ka halduslepinguga. Kuivõrd AvTS § 5 lg 2 eeldab, et avalikud ülesanded peaksid olema delegeeritud seaduse haldusakti või lepingu alusel ning antud juhul ühtegi neist delegeerimisvormidest EISi puhul kasutatud ei ole, siis polnud meil võimalik kohustada EISi teabenõuet AvTS-i alusel täitma. Kui EISi asutaja ei ole pidanud vajalikuks domeeninimede registreerimise ja haldamise korralduslikku külge õiguslikult piisavalt reguleerida, mida Majandus- ja Kommunikatsiooniministeerium on vastuses inspektsiooni järelepärimisele ka tunnistanud, siis ei saa me järelevalveorganina asuda seadusandja asemele. Andmekaitse Inspektsioon saab üksnes kontrollida õigusaktide täitmist.

Eraisik ei olnud selle otsusega nõus ning ta esitas kaebuse halduskohtusse, kes nõustus kaebajaga, sh kohustas EIS-i täitma kaebaja teabenõue ja tühistas meie vaideotsuse. Halduskohus leidis, et EIS täidab avalikku ülesannet, sest ta osutab avalikku teenust (ehk haldab .ee domeeninimesid). Samas leidis halduskohus, et riik on vältinud vaidlusaluse teenuse reguleerimist seaduse, muu õigusakti või haldusaktiga, kuid riigi kaudsest tahteavaldusest on tuletatav, et ka riik käsitab EIS-i avaliku teenuse osutajana. Halduskohus leidis, et EIS-i asutamisotsuse tegemises ja sihtasutuse registreerimise avalduse (sh põhikirja) esitamisel osalemist tuleb käsitleda haldusaktina, millega delegeeriti domeeniregistri pidamine riigisiseselt EIS-le. Halduskohus leidis, et tegemist ei ole küll õigusselge ja selgelt äratuntava haldusaktiga, vaid hübriidaktiga, kuid et tegemist on siiski avalikku ülesannet delegeeriva haldusaktiga, mistõttu kohaldub sel juhul AvTS § 5 lg 2 ning sellest tulenevalt on inspektsioonil ka järelevalvepädevus AvTS § 45 lg 1 p 1 alusel.

[6] AKI 15.04.2015 vaideotsus nr 2.1-3/15/421

EIS ei nõustunud Tallinna Halduskohtu otsusega ning esitas apellatsioonikaebuse Tallinna Ringkonnakohtule. Ringkonnakohus leidis, et EIS-i apellatsioonkaebus on põhjendatud ning rahuldas selle.[7] Ringkonnakohus leidis, et halduskohus on avaliku ülesande täitmist AvTS § 3 lg 1 ja § 5 lg 2 tähenduses sisustanud põhjendamatult avaralt.

> *„Avaliku ülesande mõistet ei ole seadustes defineeritud. Riigikohus on samuti teabenõude täitmist puudutavas asjas märkinud, et avalikud ülesanded on vahetult seadusega või seaduse alusel riigile, kohalikule omavalitsusele või muule avalik-õiguslikule juriidilisele isikule pandud ülesanded, olenemata sellest, millises vormis neid täidetakse. Seevastu ei muuda teenuse osutamist iseenesest avalikuks ülesandeks see, et vastava teenuse suhtes esineb avalik huvi, vaid avalikuks ülesandeks muutub teenus siis, kui seda osutatakse avalik-õigusliku isiku seadusest tuleneva kohustuse täitmiseks (vt Riigikohtu 19.06.2014 otsus nr 3-3-1-19-14, p-d 11-14). Varasemas praktikas on viidatud, et haldusinstitutsioonidele pandud avalikud ülesanded võivad olla ka õigusnormidest tõlgendamise teel tuletatud (nt Riigikohtu 14.12.2011 otsus nr 3-3-1-72-11, p 8; 16.02.2010 määrus nr 3-3-4-1-10, p 5). Kokkuvõtlikult peab avalik ülesanne seega olema ette nähtud vahetult seadusega või seaduse alusel või vähemasti õigusnormist tõlgendamise teel tuletatav (vt ka Riigikohtu 11.12.2015 otsus nr 3-1-1-98-15, p-d 60-62).“*

Ringkonnakohus leidis, et Eesti maatunnusega domeeninimede haldamist ei ole alust pidada ülesandeks, mida peaks olemuslikult täitma avalik võim. Samuti ei saa seda käsitada osana otsuse tegemise hetkel kehtinud hädaolukorra seaduse (HOS) § 34 lg 2 p-s 14 märgitud andmesidevõrgu toimimisest või alates 01.07.2017 jõustunud uue HOS § 36 lg 1 p-s 7 märgitud andmesideteenusest kui elutähtsast teenusest (mis on kehtiva HOS § 37 lg-s 1 ja tulevase HOS § 38 lg-s 1 selgelt määratletud avaliku halduse ülesandena), mille toimepidevuse korraldamine on MKMi ülesandeks. Seda põhjusel, et andmeside on võimalik (kuigi ebamugav) ka ilma domeeninimede süsteemita, mis aitab üksnes hõlpsamalt leida õigeid IP-aadresse (st domeeninimede süsteem on sisuliselt midagi interneti telefoniraamatu sarnast). Halduskohtu viidatud avalik teenus on samas märksa avaram mõiste kui avalik ülesanne. Teenust, mille suhtes eksisteerib avalik huvi või mis teenib üldist heaolu, tuleb pidada küll avalikuks teenuseks, kuid see ei tähenda tingimata, et tegemist peaks olema avaliku ülesandega ning seda ka juhul, kui teenuse osutaja on monopoolses seisundis ettevõtja (vt N. Parrest. Segadus mõistetes seoses avaliku võimu ülesannetega. Juridica, 2014, nr 10, lk 732–739).

Ringkonnakohus ei nõustu käsitusega, et kui mingi teenuse olemasolu suhtes esineb tungiv avalik huvi, siis kaasneb sellega automaatselt riigi positiivne kohustus astuda samme vastava teenuse tagamiseks ka juhul, kui teenuse osutamine on riigi hinnangul niigi piisavalt tagatud. Kui tegemist pole riigi tuumikfunktsioonidega ega avaliku võimu teostamisega, siis on riigil õigus endal otsustada, millist teenust ta peab avalikuks ülesandeks ja millist mitte.

EIS on riigi osalusel asutatud sihtasutus (RVS § 3 lg 1 p 9) ning kahtlust ei saa olla, et riik on olnud huvitatud sellest, et .ee-tippdomeeni haldamisega tegeleks just riigi osalusel asutatud EIS, mis annaks riigile tema asutajaõigustest tulenevalt teenuseosutaja tegevuse suhtes teatud kontrollivõimaluse (nt RVS § 79 lg 1 p-d 2–7; § 81 lg 1 p 1; § 87 p 1; § 89).

[7] Tallinna Ringkonnakohtu 06.04.2017 otsus nr 3-15-1050; otsuse peale esitati ka kassatsioonkaebus, kuid Riigikohus ei võtnud oma 03.08.2017 määrusega nr 3-15-1050 kohtuasja menetlusse.

Ringkonnakohus ei nõustunud halduskohtu seisukohaga, mille kohaselt delegeeritigi domeeniregistri pidamine kui avalik ülesanne riigisiseselt EIS-le riigi poolt sihtasutuse asutamisotsuse tegemises ja sihtasutuse registreerimise avalduse (sh põhikirja) esitamisel osalemisega, mida tuleb käsitada haldusaktina. Eelkõige tuleb praegusel juhul pidada määravaks, et riik ei ole ilmselgelt soovinud käsitada .ee-tippdomeeni haldamist avaliku ülesandena AvTS § 3 lg 1 tähenduses, sest puudub õigusnorm, mis sellise avaliku ülesande sätestaks või millest see oleks tõlgendamise teel tuvastatav. Halduskohus on ka ise viidanud, et MKM kaalus enne EIS-i asutamist, kas luua täiendav avalik-õiguslik regulatsioon või osutada teenust eraõiguslikus vormis (vt Vabariigi Valitsuse 05.02.2009 korralduse nr 39 seletuskiri; samuti Vabariigi Valitsuse 20.11.2008 kabinetiistungil heakskiidetud „Eesti .ee lõpuliste teise taseme domeenimede haldamise ja registreerimise korralduse parandamise kontseptsioon“, p 3.2), langetades täiesti teadlikult valiku just viimase variandi kasuks. Kui tegemist ei ole üldse avaliku ülesandega, siis ei ole võimalik rääkida ka avaliku ülesande delegeerimisest (AvTS § 5 lg 2) EIS-i asutamisotsustuste või muude dokumentidega.

Lõppkokkuvõttes leidis ringkonnakohus, et EIS ei täida .ee domeeni haldamise ja Eesti maatunnusega domeeninimede registri pidamisel avalikku ülesannet, mistõttu ei olnud kaebaja soovitud teabe näol tegemist avaliku teabega AvTS § 3 lg 1 ja § 5 lg 2 tähenduses. Seega EIS keeldus vastava teabe väljastamisest õiguspäraselt ning me jätsime oma vaideotsusega kaebaja vaide rahuldamata samuti õiguspäraselt.

TERVISHOID JA SOTSIAALVALDKOND

Helina-Aleksandra Lettens, vaneminspektor

Seoses andmejälgija projekti käivitamisega saabus meile suurel hulgal küsimusi, miks üks või teine asutus või isik on inimese andmete kohta päringu teinud. Tuli korduvalt selgitada, et vastavalt isikuandmete kaitse seaduse paragrahvile 19 on inimesel õigus küsida enda kohta käivat teavet andmete töötlejalt. Sealhulgas ka teavet selle kohta, millistel põhjustel on tema kohta päringuid tehtud. Andmekaitse Inspektsioon ei saa asuda inimese asemele isikuandmete kaitse seaduses sätestatud õiguste realiseerimisel.

Terviseandmete kohta tehtud päringutega seonduvatest kaebustest koorus välja neli juhtumit, kus terviseandmete vaatamiseks puudus õiguslik alus ehk tervishoiutöötaja vaatas andmeid väljaspool ravisuhet. Kõik neli isikut on riikliku järelevalvemenetluse käigus oma eksimust ka tunnistanud ning sellele järgneb kindlasti väärteokorras karistamine.

Esindusõigus

Endiselt kütab kirgi advokaatide õigus andmete saamisel. Tuli selgitada, et advokaadi puhul on tegemist kliendi esindajaga, kellel on samad õigused, mis on tema esindataval. Kui kliendil on õigus kolmanda isiku andmeid saada (nt tegemist on seadusliku esindajaga, eestkostjaga või isikuandmete kaitse seaduse paragrahvis 13 toodud isikutega), siis on sama õigus ka advokaadil. Kui kliendil puudub õigus kolmandate isikute andmete saamiseks, ei ole sellist õigust ka advokaadil. Andmete küsimisel peab advokaat oma esindusõigust tõendama, kas eraldi volitusega andmete saamiseks või muu dokumendiga, millest nähtub esindusõigus.

Terviseandmete kasutamine hariduslikel eesmärkidel

Arutelu all on pikalt olnud teema, kas tervishoiuteenuste korraldamise seaduse § 4^1 saab olla aluseks patsientide isikuandmete töötlemiseks hariduslikel eesmärkidel (näiteks residentide õpetamiseks). Meie oleme leidnud, et tervishoiuteenuse osutajal on seadusest tulenev saladuse hoidmise kohustus ning tal on õigus inimese nõusolekuta töödelda tervishoiuteenuse osutamiseks vajalikke isikuandmeid, sealhulgas delikaatseid isikuandmeid. Selle eelduseks on aga ravisuhte olemasolu patsiendi ja tervishoiutöötaja vahel, mis tähendab, et juurdepääs delikaatsetele isikuandmetele (ka suletud haigusloo avamine) on mõeldud üksnes tervishoiuteenuse osutamiseks.

Residentide õpetamiseks näeb tervishoiuteenuste korraldamise seadus ette tervishoiuteenuse osutamisel osalemise. Peale haigusloo sulgemist selle hilisem kasutamine hariduslikel eesmärkidel saab toimuda üksnes patsiendi eelneval nõusolekul. Nõusolek peab olema kirjalikku taasesitamist võimaldavas vormis ja vastama isikuandmete kaitse seaduse paragrahvis 12 toodud nõuetele.

Samuti on mitmed haiglad küsinud, et kuidas on siis võimalik kliinilisi juhtumeid arutada või kvaliteedi auditeid läbi viia, kui juurdepääs terviseandmetele on mõeldud üksnes tervishoiuteenuse osutamiseks. Siinkohal oleme selgitanud, et tervishoiuteenuse kvaliteedi tagamine, kliiniliste auditite ja kliiniliste konverentside läbiviimine on tervishoiuteenuse

osutajale seadusega pandud ülesanne. Tervishoiuteenuste korraldamise seaduse alusel kehtestatud määrus „Tervishoiuteenuste kvaliteedi tagamise nõuded“ annab tervishoiuteenuse osutajale õiguse töödelda isikuandmeid hilisema analüüsi, järelduste tegemise ja tervishoiuteenuste kvaliteeti parandamise eesmärgil.

Laste andmetega seotud probleemid

Laialt levinud probleemiks on, et tervishoiutöötajad satuvad tahtmatult lapse hooldusõiguse vaidlustesse. Paljud lapsevanemad keelavad arstidel lapse terviseandmete väljastamise teisele lapsevanemale, samas teine lapsevanem väidab, et tal on samuti hooldusõigus. Oleme leidnud, et tavaolukorras, kus mõlemal vanemal on hooldusõigus, ei ole ühel ega teisel vanemal õigust keelata lapse terviseandmete väljastamist teisele vanemale. Kui üks vanem väidab, et tal on lapse suhtes ainuhooldusõigus, siis tuleb seda väidet ka tõendada. Kui teine osapool väidab, et tal siiski on õigus lapse terviseandmete saamiseks, siis tuleb ka seda tõendada. Tuleb nentida, et see on kahetsusväärne, kui tervishoiuteenuse osutajad kistakse olukordadesse, kus lapsevanemad üritavad lapse terviseandmeid teineteise eest varjata. Selliste segaste asjaolude korral on alati parem terviseandmete väljastamata jätmine kui väljastamine.

Meieni jõudsid möödunud aastal ka mitmed lastekaitsega seotud juhtumid. Kohalikud omavalitsused tegelevad lastekaitsealaste juhtumimenetlustega ning lapsevanem nõuab neilt isikuandmete kaitse seaduse paragrahvi 19 alusel välja kõik tema enda ja lapse kohta käivad dokumendid. Kuna lastekaitse juhtumi menetluses kogunenud teave on äärmiselt

tundlik ning võib kahjustada lapse huve, siis on kohalikud omavalitsused keeldunud väljastamast dokumente, mis sisaldavad lapse kohta käivat teavet.

Meie seisukoht antud küsimuses on järgmine. Isikuandmete kaitse seaduse paragrahvis 19 toodud andmete saamise õigus ei saa olla lapsevanema jaoks absoluutne. Laps on siiski eraldiseisev indiviid, kellel on õigus eraelu puutumatusele ning seaduse kaitsele. Vastavalt lapse õiguste konventsioonile ja lastekaitse seadusele tuleb igasugustes lapsi puudutavates ettevõtmistes riiklike või erasotsiaalhoolekandeasutuste, kohtute, täidesaatvate või seadusandlike organite poolt esikohale seada lapse huvid.

Kui lapse sotsiaalne, füüsiline, psühholoogiline, emotsionaalne ja hariduslik heaolu võib olla ohus, siis on ülimalt oluline tagada ennekõike lapse õigused ja heaolu. Igal lapsel on õigus iseseisvaks seisukohavõtuks kõigis teda puudutavates küsimustes ning õigus väljendada oma vaateid. Nimetatud õiguste tagamine oleks raskendatud, kui anda lapsevanemale absoluutne voli last puudutava informatsiooni suhtes. Lapsevanemale piiramatu juurdepääsu andmisega kõikidele dokumentidele, mis sisaldavad lapse ütlusi või tähelepanekuid lapse käitumise kohta, antakse talle ühtlasi ka vahend lapse edasiseks mõjutamiseks ja olukorra manipuleerimiseks.

Mitmeid kordi on meie poole pöördutud, kui kohtus on menetluses lapse hooldusõiguse määramine ning vastaspool on esitanud kohtule tõendeid, mille puhul kaebaja leiab, et sellega rikutakse tema õigusi. Oleme selgitanud, et tõendamine ja tõendite esitamine kohtule on tsiviilkohtumenetluse seadustikus eraldi reguleeritud. Tõendite hindamine on kohtu pädevuses. Kohus hindab seadusest juhindudes kõiki tõendeid igakülgselt, täielikult ja objektiivselt ning otsustab oma siseveendumuse kohaselt, kas menetlusosalise esitatud väide on tõendatud või mitte, arvestades muu hulgas poolte kokkuleppeid tõendamise kohta. Ühelgi tõendil ei ole kohtu jaoks ette kindlaksmääratud jõudu, kui pooled ei ole kokku leppinud teisiti.

Oleme leidnud, et Andmekaitse Inspektsioon ei saa sekkuda kohtumenetlusse ning piirata menetlusosaliste õigusi tõendite esitamisel. See oleks täitevvõimu lubamatu sekkumine kohtupidamisse, kuna põhiseaduse kohaselt peab kohtupidamine olema täitevvõimust sõltumatu.

Isikuandmete kaitse üldmäärusest tulenevad kohustused

Kohtusime Eesti Perearstide Seltsiga ja Tallinna Perearstide Seltsiga, kus arutasime perearstide põhilisi kohustusi seoses 25.05.2018 jõustuva andmekaitse üldmäärusega. Perearstidele valmistab kõige suuremat muret mõjuhinnangu tegemise kohustus ja andmekaitsespetsialisti määramise kohustus.

Nende kahe kohustusega seonduvalt sai selgitatud, et sisuliselt teevad kõik andmetöötlejad mingis vormis mõjuhinnangu. Mis tähendab, et perearst mõtleb läbi, mis andmed tal on, kuidas ta neid töötleb, millised on riskid ja kuidas ta neid riske maandab. Teisiti ei saaks ju asjakohaseid meetmeid rakendada. Üldmäärus nõuab mõjuhinnangu dokumenteerimist, kui andmetöötlusega kaasneb ühekorraga nii suur oht kui ka ulatuslik töötlemine. Mõjuhinnang tuleb teha andmetöötluse kohta, millega alustatakse või mis oluliselt muutub pärast üldmääruse jõustumist.

Terviseandmete töötlemisega kaasneb alati suur oht. Haigla on meie hinnangul ulatuslik andmetöötleja ja haigla jaoks on mõjuhinnang kohustuslik. Üksik perearst (sõltumata oma

abiarstide, õdede jt palgaliste arvust) seevastu ei ole ulatuslik andmetöötleja, tal ei ole mõjuhinnangu dokumenteerimine kohustuslik. Mitu perearsti üheskoos aga tähendab ulatuslikku andmetöötlust ja mõjuhinnangu kohustust, kui nende andmetöötlus on ühine (ühine registratuur, arvutivõrk, arhiiv jne). Seda sõltumata sellest, kas ühe katuse all tegutsevad perearstid on kõik ühes äriühingus või on igaüks eraldiseisev FIE ja/või äriühing. Loeb see, kas andmetöötlus on ühine või on see igal perearstil eraldi.

Andmekaitsespetsialisti määramise kohta selgitasime, et kõik perearstid on kohustatud määrama andmekaitsespetsialisti, kuna perearstid täidavad ühelt poolt avalikku ülesannet ja teisalt töötlevad eriliigilisi (ehk delikaatseid) isikuandmeid. Andmekaitse Inspektsiooni jaoks ei ole oluline andmekaitsespetsialisti sõltumatus, kuna andmete seaduspärase töötlemise eest vastutab niikuinii perearst ise. Teenust võib sisse osta, kuid hoiduda tuleks inimestest, kes perearsti tööd ei tunne. Mitme perearsti peale võib olla ka üks spetsialist.

Tervise ja Heaolu Infosüsteemide Keskuse audit

Andrus Altmeri, andmeturbeinspektor

Perioodil 22.09.2017-01.11.2017 viis Andmekaitse Inspektsioon läbi omaalgatusliku auditi Tervise ja Heaolu Infosüsteemide Keskuses. Audit viidi läbi vastavalt isikuandmete kaitse seaduse (edaspidi IKS) § 32[1] ja Andmekaitse Inspektsiooni auditi juhendile.

Auditi eesmärk oli kontrollida isikuandmete ja asutusesiseseks kasutamiseks mõeldud teabe kaitset, selleks rakendatavaid infoturbemeetmeid ning teisi teabe kaitsega seonduvaid organisatoorseid, füüsilisi ja infotehnoloogilisi meetmeid Tervise ja Heaolu Infosüsteemide Keskuses (TEHIK). TEHIK haldab volitatud töötlejana Sotsiaalministeeriumi haldusala infosüsteeme ja andmekogusid, mis töötlevad keskselt ja eriti suures mahus Eesti elanike delikaatseid tervise- ja eraelulisi andmeid.

Vastavusauditi osas tutvusid inspektsiooni ametnikud TEHIKu saadetud dokumentatsiooniga (22 dokumenti). 18.10.2017 viidi läbi valmidusaudit kohapealse kontrollkäiguna, mille käigus kontrolliti TEHIKu ruumides alljärgnevat:

- dokumentatsiooni ja sisereeglistiku rakendamine reaalsuses,
- asutusesisene teave, selle kaitse ja haldus asutuse igapäevatöös vastavalt avaliku teabe seadusele,
- isikuandmete väljastamine teadusuuringute tarbeks,
- kehtivate seaduste (IKS, AvTS) rakendamine ja valmistumine andmekaitse üldmääruseks,
- andmekaitse kontroll kohapeal vastavalt IKS § 25,
- turvaintsidentidega tegelemine ja asutuse sisekontroll,
- infosüsteemi päringulogid, enda andmetele juurdepääs IKS § 19 kohaselt ja logide haldus.

Andmekaitse Inspektsiooni hinnangul vastavad TEHIKu rakendatud organisatsioonilised, füüsilised ja infotehnoloogilised meetmed isikuandmete kaitse seaduses toodud nõuetele, mistõttu menetlus lõpetati 01.11.2017.

Auditi järeldusena toob inspektsioon välja TEHIKu kui Sotsiaalministeeriumi valitsusalas asuva delikaatset teavet koondava keskse infotöötluse ja infoturbeasutuse rolli, mille tõttu

on sealne isikuandmete töötlemine inspektsiooni hinnangul kõrgendatud riski allikas. Seetõttu vajab TEHIK inspektsiooni hinnangul kindlasti täiendavaid infoturbealaseid ressursse, et paremini maandada nii Sotsiaalministeeriumi valitsusala üleseid kui ka oma asutuses esineda võivaid isikuandmete kaitse alaseid riske.

ISIKUANDMED ÄRI- JA TÖÖELUS

Raiko Kaur, vaneminspektor

Avalikustatud andmete kasutamine

Tihtipeale ollakse seisukohal, et kõiki isikuandmeid, mis on avalikest allikatest leitavad, võib vabalt kasutada. Siiski see nii ei ole. Andmekaitse Inspektsioon tegi 2017. aastal ka ühe ettekirjutuse, mis puudutas avalikest allikatest saadud isikuandmete töötlemist eesmärgil, mis ei olnud andmete avalikustamise esialgse eesmärgiga kooskõlas.

Avalikes allikates inimese enda avaldatud kontaktandmeid võib kasutada üksnes sel eesmärgil, milleks nad avaldati. Näiteks kui kontaktandmed on avaldatud konkreetse eseme müügikuulutuse juures, võib ühendust võtta üksnes selle konkreetse eseme osas tehingu tegemise eesmärgil. Samuti võib seaduse alusel avalikustatud isikuandmeid kasutada üksnes sel eesmärgil, milleks nad on avalikustatud. Näiteks äriregistrisse kantud ettevõtte kontaktandmeid võib kasutada ettevõttega seotult, kuid mitte ettevõttes tegutsevate inimestega (juhatuse liikmed, osanikud jt) suhtlemiseks nende inimeste eraelulistel teemadel.

Andmete avalikustamise eesmärgist muul eesmärgil isikuandmete töötlemiseks peab olema õiguslik alus. Seejuures ei ole IKS § 11 lõige 1 Riigikohtu praktika kohaselt iseseisev õiguslik alus isikuandmete töötlemiseks. Nimelt on Riigikohus asjas nr 3-3-1-85-15 otsustanud (otsuse punkt 18) järgnevat:

> *„IKS § 11 lg 1 piirab teiste sama seaduse sätete kohaldamist, mitte ei ole iseseisev alus andmete töötlemiseks. Ka ei tulene seaduse sättest, et juba avalikustatud isikuandmete uueks töötlemiseks ei pea olema seaduslikku alust.“*

Sama on Riigikohus kinnitanud asjas nr 3-3-1-3-12, p 23 ja asjas nr 3-2-1-159-14, p 14.

Infoportaalide seire

Kuna sarnaselt varasematele aastatele oli ka 2017. aastal üheks peamiseks kaebuste allikaks ettevõttega seotud äri– ja isikuandmete avalikustamine infoportaalides, alustasime omaalgatusliku järelevalvemenetluse, et kaardistada isikuandmete töötlemise olukord infoportaalides. Läbiviidava seire eesmärgiks on eelkõige välja selgitada, millisel õiguslikul alusel ning milliseid isikuandmeid infoportaalides kogutakse ja (taas)avaldatakse.

Infoportaali pidajad peavad arvestama sellega, et oma teenuse osutamise raames töötlevad nad isikuandmeid. Isikuandmete kaitse seaduse kaitsealasse kuuluvad muuhulgas ka endiste äriühinguga seotud isikute (esindajate) andmed (nt nimi, isikukood). Reeglina ainuüksi kehtivate äriühingu esindajate nimed isikuandmete kaitse seaduse kaitsealasse ei kuulu. Küll aga kuulub äriühingu esindaja nimi isikuandmete kaitse seaduse kaitsealasse

juhul, kui lisaks nimele on muid seoseid eraelulise informatsiooniga (nt füüsilise isiku maksehäired, seotud kinnisvara, meediakajastused, ametlike teadaannete andmed, maksuvõlad). Isikuandmete kaitse seaduse kaitsealasse ei kuulu juriidilise isiku maksehäired, kinnisvara jne.

Isikuandmete töötlemine peab olema seaduslik, eesmärgipärane ning inimesele läbipaistev. Kui isikuandmete töötlemiseks õiguslikku alust ei ole, on isikuandmete töötlemine keelatud (sh tuleb olemasolevad andmed viivitamata kustutada).

Läbiviidav seire on näidanud, et kõik seires osalevad infoportaalid töötlevad vähemal või rohkemal määral isikuandmeid. Küll aga jääb osale infoportaalidest arusaamatuks, kas ja millises ulatuses nad isikuandmeid töötlevad. Seetõttu vastatakse ka inimestele tuginedes Andmekaitse Inspektsiooni maksehäirete avaldamise juhendile, milles on märgitud järgnev:

> *„Juriidilisel isikul kui seaduse alusel loodud abstraktsel moodustisel eraelu ei ole ja sellega seonduvad andmed, sh ka juhatuse liikmete nimed isikuandmete kaitse seaduse kaitsealasse ei kuulu, sest tegemist pole eraeluliste, vaid majandustegevusega seonduvate andmetega, mis on kõigile kättesaadavad äriregistris*".

Sellele punktile saab tugineda aga üksnes juhul, kui füüsiline isik on sel ajal juriidilise isiku majandustegevust võimeline mõjutama[8] ja puuduvad muud seosed eraelulise informatsiooniga. Juhul kui üks eelnevatest punktidest ei ole täidetud, ei saa automaatselt väita, et isiku nime avaldamine ei kuulu isikuandmete kaitse seaduse kohaldamisalasse. Kuigi seire veel jätkub, juhtis inspektsioon infoportaalidele tähelepanu, et oma võrgulehel avaldatud füüsiliste isikute andmete puhul tuleb hinnata, kas isik on võimeline konkreetse ettevõtte majandustegevust mõjutama ning kas puuduvad muud seosed eraelulise informatsiooniga. Inimeste vastuväidetele/kaebustele tuleb vastata viie tööpäeva jooksul lähtuvalt hindamise tulemustest ja asjaoludest, sh tuleb vajadusel (õigusliku aluse puudumisel) isikuandmed kustutada (sh võrgulehelt eemaldada).

Seire jätkub 2018. aastal, arvestades seejuures ka alates 25. maist 2018. a kohaldatava andmekaitse üldmäärusega.

Metsaomanike isikuandmete töötlemine

2017. aastal oli olulisel kohal ka metsaomanike isikuandmete töötlemise kontrollimine, ajendatuna eelkõige inspektsioonile tehtud pöördumistest seoses metsaomanike andmete müügiga. Inspektsioon suunas 2017. aastal oma tegevuse peamiselt andmete võimalikele lähteallikatele.

Augustis ja septembris viisime läbi omaalgatusliku seire, mille eesmärk oli kontrollida valitud ettevõtete vastavust isikuandmete kaitse nõuetele klientide ja potentsiaalsete klientide, eelkõige metsa ostjate/müüjate, isikuandmete töötlemisel. Muuhulgas oli eesmärgiks tuvastada ka lähteallikad, kust metsaomanike andmeid saadakse.

Selgus, et metsaomanike andmeid saadakse peamiselt kinnisvaraportaalidest, ajalehtedest, Maa-ameti enampakkumistest ning muudelt Google'i otsingumootori kaudu leitavatelt võrgulehtedelt, kus inimesed avaldavad soovi kinnisvara või metsaga tehinguid teha.

[8] Vt näiteks Riigikohtu otsust asjas nr 3-2-1-67-10

Samuti tuvastasime veebipõhise andmebaasi, mille eesmärgiks oli koguda metsaomanike andmeid, et neile ostupakkumisi teha. Inimeste nimed olid võetud telefoniraamatust ning nimede alusel tehti igal öösel automaatpäringuid kinnistusraamatusse, kust saadi vaste sellele, kas sellele konkreetsele nimele vastab mõni maatulundusmaa. Telefoninumber nime juurde saadi kas 1182.ee-st või Google'i otsingumootorit kasutades. Eeltoodust lähtudes tegi inspektsioon Registrite ja Infosüsteemide Keskusele olukorra parandamiseks ettepaneku piirata kinnistusraamatust ees- ja perekonnanime järgi otsides masspäringute tegemise võimalust.

Isikuandmed töösuhetes

Töösuhete raames isikuandmete töötlemisega seonduvalt pöörduti 2017. aastal inspektsiooni enim kaamerate kasutamise ja nimelise e-posti aadressi sulgemisega seotud küsimuste ning probleemidega.

Kõige rohkem tekitab töösuhetes probleeme andmetöötluse läbipaistmatus. Tihtipeale puuduvad reeglid, mis käsitleksid isikuandmete töötlemist, sh kaamerate ja e-postkasti kasutamise reeglid. Reeglite puudumine tekitab aga probleeme nii töötajale kui ka tööandjale. Kui puuduvad konkreetsed reeglid, siis tõenäoliselt ei ole ka tööandja analüüsinud, millisel õiguslikul alusel ja millistel eesmärkidel on lubatud näiteks kaameraid üleüldse kasutada ning kuidas vähendada e-postkastis olevate kirjadega seotud riske seoses töötaja ja kolmandate isikute eraelu ja sõnumisaladuse võimaliku rikkumisega. Töötajale tekitab reeglite puudumine omakorda teadmatust, miks ja millisel eesmärgil näiteks kaameraid kasutatakse, töötaja kasutatavat e-postkasti vaadatakse ning millal lahkuva töötaja e-posti aadress kustutatakse.

Andmekaitse Inspektsioon soovitab tööandjatel panustada andmetöötluse läbipaistvusesse. Eelkõige on oluline, et töötajate isikuandmete töötlemisega seotud teave ja sõnumid on lihtsasti kättesaadavad, arusaadavad ning selgelt ja lihtsalt sõnastatud.

Võlaandmed

Sirje Biin, vaneminspektor

Maksehäirete avaldamise probleemid on üldjoontes samad, mis eelnevatel aastatel. Võlgnik peab parimaks probleemi lahenduseks pea liiva alla peitmist, aegumise kui imerohu uskumist ja võlausaldaja peale kaebamist (olgu siis põhjusega või põhjuseta). Võlgnikele tuleb tihti selgitada, et esimesed sammud oma murede lahendamiseks peavad nad ise astuma – IKS § 19 annab õiguse küsida andmete töötlejalt teavet andmete allika, töötlemise eesmärgi ja andmete edastamise kohta. Tihti jäetakse see tegemata lootuses, et seda peab nende eest tegema inspektsioon.

Võlgnikud ei saa jätkuvalt aru, et aegumine ei rakendu automaatselt, see ei tähenda võla kustumist ning Andmekaitse Inspektsiooni pädevuses ei ole selle üle otsustada. Aegumist saab nõuda võlgnik, kuid enamasti peetakse kohtu kaudu oma õiguste maksmapanekut keeruliseks, aeganõudvaks ja kalliks. Jäädakse lootma, et võlausaldaja esitab hagi (st tasub ka riigilõivu ja esitab tõendid) või et inspektsioon käsib avalikustamise lõpetada. Kuid ka võlausaldaja ei kiirusta kohtuteega, vaid püüab võlgnikku tasumisele survestada, vaatamata sellele, et nõue on ilmselgelt aegunud. Inspektsioon saab üksnes selgitada oma seisukohta, miks tasumata võlgade puhul tuleb arvestada 13-aastase avalikustamise tähtajaga.

Võlgniku sugulastega kontakti võtmine pole lubatud

Võlgniku survestamisel ei peeta paljuks otsida üles sugulased, tuttavad ja tööandjad. Sellesisulised kaebused on kasvutrendis. Mitte alati ei ole sugulaste-tuttavate kontaktandmed saadud seaduslikul teel (nt suhete otsimine rahvastikuregistrist õigustamata päringutega) ning võlaandmete edastamiseks puudub võlgniku nõusolek või seaduslik alus.

Ka kontakti otsimise sildi all ei peaks inkassofirma tüütama kolmandaid isikuid – õhku jääb küsimus, kust on kontaktandmed saadud ja mis alusel neid kasutatakse. Hea võimaluse kolmandate isikutega suhtlemiseks on võlausaldaja leidnud Facebooki näol. Inspektsioon ei näe probleemi selles, kui võlausaldaja suhtleb sotsiaalvõrgustike või *online*-suhtluskeskkondade kaudu otse võlgnikuga (olles siiski veendunud, et tegemist on õige inimesega). Küll aga ei saa aktsepteerida võlgniku Facebooki kontaktide teavitamist tema maksehäiretest.

Parkimise leppetrahv

Inkassoettevõtjate peale kaebavad ka parkimise leppetrahvi teateid saavad inimesed. On neid, kes ei arvesta, et parkimisettevõtjal on õigus mobiilsel parkimisel (lepingu sõlmimisel) antud telefoninumbrit säilitada raamatupidamise seaduse alusel 7 aastat ja kasutada seda järgmise parkimiskorra rikkumisel sama autoga. On aga ka parkimise korraldaja poolseid rikkumisi – ei kontrollita andmete õigsust enne inkassoettevõtjale üleandmist või ei täideta taotlusi andmeid parandada, näiteks olukorras, kus autoomanik on vahetunud.

RAHANDUSSEKTOR

Merit Valgjärv, juhtivinspektor

Pankade ja kindlustusandjatega on sel aastal koostöö toimunud andmekaitse üldmääruse ettevalmistuste võtmes. Toimunud on teabevahetus Pangaliiduga ja Eesti Kindlustusandjate seltsiga. Igapäevatöös on nii pankade kui ka kindlustusandjate puhul olnud enim kaebusi seoses andmesubjekti õigusega saada iseenda kohta käivaid andmeid ning samuti on rohkelt olnud andmete edastamisega seonduvaid pöördumisi.

Mobiilirakenduste kasutamine pangandussektoris

Andmekaitse Inspektsioon viis läbi seire, mille käigus kontrolliti pankade mobiilirakendusi. Täpsemalt keskendus seire sellele, millistele andmetele pank rakenduse kaudu ligipääsu saab. Tänan seires osalenud pankasid panuse eest valdkonna kaardistamisel.

Andmekaitsealane seadusandlus on tehnoloogianeutraalne. Tulenevalt sellest ei takista õigusnormid erinevatel infotehnoloogilistel viisidel andmete töötlemist, tingimusel, et järgitakse isikute eraelu kaitseks kehtestatud õigusraamistikku.

Isikuandmete töötlemiseks loetakse kõiki nende andmetega tehtavaid toiminguid, sealhulgas lisaks kogumisele ja salvestamisele näiteks ka juurdepääsu võimaldamist isikuandmetele, päringute teostamist ja erinevate andmete ühendamist. Lähtuvalt isikuandmete kaitse seaduse § 6 sätestatud eesmärgikohasuse ja minimaalsuse põhimõttest võib andmeid töödelda üksnes mahus, mis on eesmärgi saavutamiseks vajalik. Kui andmete töötlemine toimub lepingu täitmiseks, siis saab isik anda nõusoleku vaid enda andmete töötlemiseks. Kolmandate isikute eest reeglina nõusolekut anda ei saa.

Telefonis olevate andmete kasutamine rakendusesiseselt, näiteks kui see aitab kasutajal mingisuguseid välju automaatselt eeltäita, on lubatud. Samuti ei ole midagi halba selles, kui

töödeldakse klientide andmeid, kes on rakenduse kasutusele võtnud, aru saanud, mil viisil ja mis eesmärgil nende andmeid töödeldakse ning ise sellega nõustunud. Ehk siis klientide vahel, kes ise teenust kasutavad ja oma andmete edastamisega nõus on, võib ka omavahel andmeid vahetada. Seires osales kaheksa panka. Neist seitse kas ei oma juurdepääsu või ei töötle kliendi aadressraamatus olevate teiste isikute andmeid. AS SEB pank on suutnud organisatsiooniliste ja tehnoloogiliste turvameetmete abil tagada selle, et andmetöötlus vastaks isikuandmete kaitse seaduses sätestatule.

Kindlustused

Liikluskindlustusfondis toimus kohapealne kontroll, mille fookus keskendus logide olemasolule ja asja- ning ajakohasusele. Puudusi ei tuvastatud.

Kohtumisel kindlustusseltside liidus kindlustusandjate esindajatega andmekaitse üldmääruse küsimustes olid arutusel üldmääruses sätestatud uued mõisted ja kohustused. Kindlustusandjad suhtuvad vägagi tõsiselt üldmääruse art 13 ja 14 sätestatud teavitamiskohustuse täiendamise vajadusse. Samuti on paljud määranud andmekaitsespetsialisti juba praegu. Kindlustusseltside liidu eestvedamisel täiendatakse ka isikuandmete töötlemise sektoripõhiseid juhendmaterjale üldmäärusest tulenevate nõuete osas.

Maksundus

Maksu- ja Tolliametiga on toimunud mitmeid kohtumisi, mille käigus on arutatud allhankijate töötajate keskmise töötasu tõendite väljastamist hankijatele ning eesmärgikohasuse ja minimaalsuse põhimõtete täitmist sellise andmetöötluse puhul. Lahendusena, mis kaitseks palga konfidentsiaalsust ning maksusaladust, esitab hankija ise MTA-le hankes osalevate töötajate nimed. MTA edastab hankijale vastuse ilma nimedeta, kinnitades kas töötajate palk on vähemalt 70% valdkonna keskmisest või ei ole. Seniks kuni pole muudetud siseriiklikku õigust, ei ole lubatud nimeliselt töötajate palku avaldada.

Isikukoodide avaldamine maksuvõlgade masspäringus

MTA võrgulehel kuvatav maksuvõlgade otsingu päring on vastavuses andmekaitse nõuetega – päringu tegijale on juba isikukood teada. Masspäringus väljastab MTA suurel hulgal isikukoode, iga päringuga võib isikukoode lisanduda. Samas ei pruugi isikukoodi omanikul enam järgmise päringu ajal maksuvõlga olla. Sellisel moel saadud isikukoode on võimalik sisestada andmekogudesse, kus andmeid kasutatakse juba muudel eesmärkidel, kui maksuvõla teadasaamine.

Teistel eesmärkidel, kui neid esialgselt avalikustati võib andmeid kasutada ainult juhul, kui need andmed on tunnistatud avaandmeteks (AvTS § 3^1). Füüsiliste isikute andmeid avaandmeteks enamasti ei loeta – riskiks profileerimine, eraelu riive. Avaandmete loetelu peab olema soovituslikult kinnitatud peadirektori käskkirjaga ja selleks tuleb eelnevalt läbi viia analüüs, millisel põhjendusel konkreetsed füüsilise isiku andmed avaandmed on/ei ole.

Andmekaitse nõuetest lähtuvalt ei ole füüsiliste isikute maksuvõlgade avaldamine masspäringuga aktsepteeritav. Maksuvõla masspäringu teenusest on soovitus füüsiliste isikute andmed välja jätta.

JUSTIITSSÜSTEEM

Merit Valgjärv, juhtivinspektor

2017. aastal on justiitssüsteemis tegeletud mitmete valdkondadega keskendudes eelkõige neile, millega kaasneb suuremamahuline andmete töötlemine.

Karistusregister

Karistusregister on tegelenud tõsiselt andmekvaliteedi parandamise probleemistikuga. Eesmärgi saavutamiseks tegeletakse andmeandjatega, mis tähendab karistuste sisestamisega seotud täiendusi. Selle tulemusena väheneb olulisel määral vigaste karistusandmete tekkimine. Samuti on käesoleval aastal tehtud arendusi, et vigaste andmete parandamine ning identifitseerimine karistusregistri haldaja poolt oleks lihtsam ning kiirem.

Kinnistusraamatu ligipääsud ja masspäringud

Selgus, et osad kinnistusraamatu lepingulised kliendid ei kasutanud XML-otsingut eesmärgipäraselt. Registrite ja Infosüsteemide Keskus analüüsis, kuidas muuta päring selliseks, et masinliidese kaudu ei oleks võimalik kinnistu omandi andmeid massiliselt tasuta pumbata. Kuigi teenus töötab tehniliselt korrektselt, siis teatud juhtudel, nagu mahtude ja andmete kombineerimisel on võimalik süsteemist massiliselt pumbata andmeid, mida kombineerides on võimalik tuletada kinnistu omanike nimesid.

Andmekaitse Inspektsioon tegi Registrite ja Infosüsteemide Keskusele ettepaneku isikute ja eraelu puutumatuse kaitseks piirata kinnistusraamatust ees- ja perekonnanime järgi otsides masspäringute tegemise võimalust. Registrite ja Infosüsteemide Keskus märkis, et masspäringute tegemist võimaldas tasuta XML-teenus. Samuti leidsid, et piiramaks masspäringute tegemist kinnistu omaniku ees- ja perekonnanime järgi, st tagada olukord, kus päringuid tehakse põhjendatud kaalutlustel ja vajadustest lähtuvalt, asendatakse tasuta teenus tasulise teenusega. Alates 01.12.2017 tuleb iga isiku järgi päringu tegemisel tasuda 1 euro iga talle kuuluva kinnistu kohta (info kinnistu olemasolu ja omaniku seose kohta). Päringutasu 1 euro on piisav mõjutusvahend vältimaks edaspidi teenuse kuritarvitamist. Uue tasulise teenuse kasutamist jälgitakse ja juhul kui ilmneb, et seatud päringutasu ei ole piisav piirang, analüüsitakse täiendavate meetmete kasutuselevõttu.

Äriregistris FIE-de kontaktandmete avalikustamine

Inspektsioon on ka varasemalt tähelepanu juhtinud kustutatud füüsilisest isikust ettevõtjate sideandmete avalikustamise problemaatikale. Selle tulemusel on äriregistri avalikust vaatest 2016. aasta lõpuks eemaldatud tegevuskoha aadressid. Samas on jätkuvalt nähtavad kustutatud FIE-de telefoninumbrid ja e-posti aadressid, mille avalikustamine riivab isikuid sageli isegi rohkem kui postiaadressi avalikustamine. Vastavalt 10.04.2017 toimunud Justiitsministeeriumi, Registrite ja Infosüsteemide Keskuse ja Andmekaitse Inspektsiooni kohtumisel otsustatule, eemaldati masspäringu vastustest kustutatud FIE-de kontaktandmed (e-posti aadress ja telefoninumber).

Pilootprojekt

Justiitsministeerium on 2017. aastal alustanud projekti andmekaitse üldmääruseks ettevalmistumiseks. See on kaasa toonud kuus ettevalmistavat kohtumist, mille käigus arutasime määruses sätestatud nõuete ja sellega kaasnevate reaalsete tegevuste üle. Projekti käigus on kaardistatud juba tehtud andmeturbega seotud tegevused ning selgitatud välja millised tegevused on vajalikud, et olla valmis otsekohalduva määruse jõustumiseks 25.05.2018. Projekti esitlused ja teabe jagamine teistele ministeeriumidele on toimunud avaliku teabe nõukogu koosolekutel alates novembrist 2017.

Rahvastikuregister

Rahvastikuregistriga on olnud meeldiv koostöö seoses andmejälgija projekti käivitumisega ning sellega, et rahvastikuregister oli esimeste seas, kes projektiga liitus. Projekti käigus ilmnes vajadus lisada selgitusi päringuvastuste juurde. Näiteks automaatpäringud andmete ajakohasena hoidmiseks andmete kvaliteedi põhimõtte täitmiseks tekitasid palju küsimusi. Tänaseks on selle päringu juurde lisatud selgitus.

Samuti on projekti käivitumine toonud kaasa selle, et andmetöötlejad on paremini läbi mõelnud, milliseid andmeid nad rahvastikuregistrilt oma töö jaoks täpselt vajavad ja hakanud paremini täitma eesmärgikohasuse ja minimaalsuse põhimõtteid andmetöötluses.

Oleme osalenud Siseministeeriumi rahvastikutoimingute osakonna, Notarite Koja ja Kohtutäiturite Koja koosolekutel, kus arutati rahvastikuregistrisse tehtavate päringute korrastamist eesmärgipärasuse ja minimaalsuse põhimõtte täitmiseks. Tulemuseks on see, et päringute andmekoosseise analüüsitakse ja vajadusel muudetakse vältimaks nn mugavuspäringuid, mille tulemusel nähakse ka andmeid, millel andmetöötluse eesmärgiga seost ei ole.

Näiteks päring seotud isikute kohta on sõltuvalt andmetöötluse eesmärgist võimalik teha nii, et näha oleks vaid ülenejad sugulased või nii, et näha oleks vaid alanejad sugulased. Rahvastikuregister on andmetöötlejatele päringute vastuste minimeerimisel osutanud suurt abi. Samuti on tõusnud teadlikkus selles osas, et eelistatud on päringute tegemine isikukoodi kasutades, sest see annab päringu vastuseks konkreetse isikukoodi omaniku andmed. On juhuseid, kus isikukood ei ole teada ja tuleb teha nimepäring, kuid sel juhul peab andmete töötleja suutma isikutele selgitada, miks selline päring oli vältimatu.

Andmejälgija projekti käivitamine on kaasa toonud individuaalse osalemise suurenemise andmetöötluses. Inimestel on suur huvi vaadata oma andmete kasutamist ning nõuda IKS § 19 alusel nii erasektorilt kui ka avalikult sektorilt teavet, kes ja mis eesmärgil on tema andmeid töödelnud. Andmesubjektide kontroll andmekasutuse üle on positiivselt kaasa toonud selle, et andmetöötlejad on (mõnikord küll inspektsiooni kaasabil) teadvustanud kohustust anda selgitusi andmete töötlemise kohta.

Päringute korrastamine on pikaajalisem protsess, kuid lõpptulemus on see, et andmete kasutamine muutub ökonoomsemaks ja eesmärgistatumaks.

AJAKIRJANDUS JA ÜHISMEEDIA

Sirje Biin, vaneminspektor

2017. aastal oli ligi kümnendik inspektsiooni nõuandetelefonile tehtud kõnedest ajendatud sellest, et helistaja leidis oma andmed ajakirjandusest või suhtlusportaalidest. Meedias andmete avalikustamise kohta saime ka hulgaliselt kirjalikke pöördumisi (selgitustaotlusi, märgukirju ja kaebusi).

Kuna enamasti on tegemist olukorraga, kus konflikt tekib kahe eraõigusliku isiku huvide vahel (sõnavabadus *versus* privaatsus), ei sekku inspektsioon sellesse korrakaitseseaduse normidest lähtudes. Seda, et inspektsioonil on õigus menetluse algatamise otsustamisel lähtuda korrakaitseseaduse reeglitest, kinnitab Tallinna halduskohtu otsus, millest saab lähemalt lugeda kohtulahendite peatükist.

Inimene saab ja peab kõigepealt ise panustama oma õiguste kaitsesse. Pealegi viidatakse suuremas osas pöördumistes, et avaldatu on vale, halvustav ning tekitab kahju. Sellele saab aga hinnangu anda kohus, mitte inspektsioon. Vaatamata sellele, et inspektsioon ei sekku, selgitame inimestele, kuidas nad ise oma õigusi kõige kiiremini ja efektiivsemalt kaitsta saavad. Vastavad juhendmaterjalid oleme kättesaadavaks teinud ka oma võrgulehel.

Püüame inimesi julgustada oma õiguste eest seisma ka siis, kui vastas on telesaate meeskond kaameraga. Ühelt poolt ei pea inimene oma elu kõigiga televisiooni vahendusel jagama ning teiselt poolt ei tohi saatetegija eetika ja taktitundeta üle sõita inimesest üksnes vaatajanumbrite tõusu nimel (skandaal, surm ja seks müüvad hästi). Paraku on sellised juhtumid aga viimase aasta jooksul sagenenud.

Isikuandmed sotsiaalmeedias

Üha igapäevasem on oma elu eksponeerimine sotsiaalmeedias. Seda, et osa teabest ja piltidest vajaks võõraste pilkude eest kaitset, taibatakse tihti alles siis, kui avaldatut on kuritarvitatatud. Keegi ei ole päriselt kaitstud nutikate kurjategijate eest, kuid oma kontode kaitsmine turvaliste paroolidega, privaatsussätete üle vaatamine ja tundlikuma sisu hoidmine ainult usaldusväärsete inimestega jagamiseks on iga inimese võimuses.

Peale oma isiklike õiguste peaks sotsiaalmeedia kasutaja arvestama ka teiste inimeste õigustega. Lihtsalt vihast, kättemaksuks või omakohtuks koostatud petturite vms nimekirjad võivad tuua sekeldusi täiesti süütutele inimestele. Õigust mõistab siiski kohus.

Suhtlusportaalides, erinevates foorumites ja blogides isikuandmete töötlemist käsitleme sama mõõdupuuga, nagu muus meedias töötlemist. See tähendab, et ka siin kaalume, kas inimene saab oma õigusi kaitsta ilma inspektsioonita ega sekku, kui selleks hädavajadust pole.

Kunstiline ja kirjanduslik eneseväljendus

Kui isikuandmete kaitse seaduses on praegu eraldi reguleeritud isikuandmete töötlemine ajakirjanduslikul eesmärgil, siis üldmääruse jõustumisel lisandub iseseisva normina isikuandmete töötlemine kunstilise ja kirjandusliku eneseväljenduse tarbeks. Regulatsioon on vajalik raamatute, filmide ja kujutava kunsti teoste jaoks, mis ei kvalifitseeru ajakirjandusena. Järjest rohkem avaldatakse elulooraamatuid ja vändatakse reaalsetel sündmustel põhinevaid filme, mis annavad põhjust vaidlustada isikuandmete avaldamise õiguspärasust. Nagu ajakirjandusliku eesmärgi korral, ei ole ka isikuandmete kasutamisel kunstilise ja kirjandusliku eneseväljenduse tarbeks vaja inimese nõusolekut. Küll aga ei tohi see ülemääraselt kahjustada andmesubjekti õigusi. Kuidas uus norm rakendust leiab ning milliseks kujuneb praktika, saame rääkida juba järgmisel aastal.

HARIDUS

Liisa Ojangu, vaneminspektor

Dokumendiregistrite seire

Seirasin 2017. aasta kolmandas kvartalis 20 erineva suurusega üldhariduskooli ja avaliku ülikooli dokumendiregistreid eesmärgiga kontrollida, kas need vastavad avaliku teabe seaduses sätestatud nõuetele. Eelkõige kontrollisin, kas register on avalikustatud, kas selles olevad avalikud dokumendid on lihtsalt kättesaadavad ning kas juurdepääsupiirangut vajav teave on kaitstud.

Seire tulemusel selgus, et ainult ühel koolil oli dokumendiregistriga seonduv täielikult nõuetekohane. Dokumendiregister ei olnud leitav kooli kodulehel ega Eesti koolide haldamise infosüsteemi (EKIS-e) kaudu kaheksal koolil. Kaheksal koolil oli dokumendiregister leitav ainult EKIS-es ilma, et kooli kodulehel oleks sellele viidatud. Kahel koolil oli dokumendiregister leitav kooli kodulehel, kuid mitte nn ühe kliki kaugusel ehk dokumendiregistri asukohta pidi veebilehe kaudu pikemalt otsima. Ühel koolil oli dokumendiregister küll kodulehel leitav, kuid sisenemiseks oli vaja kasutajanime ja parooli. Leidus koole, kellel oli dokumendiregister EKIS-es olemas, kuid dokumente ei õnnestunud tehnilise veateate tõttu kuvada.

Koolidele, kelle kodulehe kaudu ei olnud dokumendiregister lihtsasti leitav, tegin soovituse dokumendiregister lihtsamini leitavaks teha. Koolide suhtes, kelle dokumendiregister ei olnud leitav ühestki allikast, juurdepääs oli piiratud kasutajanime ja parooliga või kus dokumendiregistri metaandmetes sisaldusid eraisikute nimed, alustasin järelevalvemenetluse.

Aasta lõpuks olid kõik järelepärimise saanud koolid dokumendiregistri probleemide tagamaid selgitanud ning dokumendiregistri nõuetekohaselt avalikustanud või seadnud konkreetse kuupäeva, millal register nõuetekohaselt avalikuks tehakse. Kontrollin kindlasti, kas seatud tähtaegadest peetakse kinni ja uurin, kas ettevalmistustöödega tegeletakse.

Dokumendiregistrite avalikustamata jätmise põhjusteks oli tihti asjaolu, et koolide dokumendiregistrid on sageli seotud kohaliku omavalitsuse dokumendiregistriga, kuid valdade ühinemine tekitas liidetavate valdade koolide dokumendiregistrite osas segadust ja viivitusi.

Õpilaste nimekirjade ja piltide avalikustamine

Andmekaitse Inspektsioonile esitavad haridusasutused tihti selgitustaotlusi, milles soovitakse teada, milliseid õpilaste andmeid võib kooli kodulehel avalikustada. Õpilaste nimekirjade ja piltide avalikustamise osas on inspektsioon seisukoha kujundanud juhendites õpilaste ja vilistlaste nimekirjade avalikustamise ning kaamerate kasutamise kohta. Õpilaste nimekirja võib avalikustada vaid õpilase (või alaealise puhul tema vanema) nõusolekul.

Kooli või lasteasutuse enda tehtud fotode avalikustamise osas kooli kodulehel või Facebookis soovitab Andmekaitse Inspektsioon väga hoolikalt kaaluda, kas on vajalik avalikustada kõikide koolis käivate laste fotod, iseäranis koos nimedega. Selline avalikustamine võib ohustada laste turvalisust. Kindlasti ei tohi õpilaste nimekirjad ega laste fotod olla otsingumootoritele avatud.

Andmekaitse Inspektsioon soovitab tungivalt kehtestada kooli või lasteasutuse territooriumil filmimise ja pildistamise kord, lähtudes eelkõige laste turvalisuse tagamisest. Selles korras tuleks ära reguleerida filmimine ja pildistamine ning kooli territooriumil või kooliüritustel tehtud piltide-filmide internetti üles riputamise reeglid nii lastele, lapsevanematele, kooli personalile kui ka kõigile kolmandatele isikutele, sh meediale selle kõige laiemas tähenduses.

SISETURVALISUS

Kristjan Küti, vaneminspektor

2017 alustasime omaalgatusliku järelevalvega Schengeni infosüsteemi (SIS II) siseriikliku osa üle. Järelevalvekohustus tuleneb Euroopa Parlamendi ja Nõukogu 20.12.2006 määruse (EÜ) nr 1987/2006 art 44 lõikest 1 ja 2 ning Nõukogu 12.06.2007. aasta otsuse 2007/533/JSK art 60 lõikest 1 ja 2.

SIS II pidamist reguleerib Euroopa Liidu tasandil:

- Euroopa Parlamendi ja Nõukogu 20.12.2006 määrus (EÜ) nr 1987/2006, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist,
- Nõukogu otsus 2007/533/JSK, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist,
- Euroopa Parlamendi ja Nõukogu 20.12.2006 määruse (EÜ) nr 1986/2006, mis käsitleb liikmesriikides sõidukite registreerimistunnistusi väljaandvate teenistuste juurdepääsu teise põlvkonna Schengeni infosüsteemile (SIS II) ning
- Komisjoni 4.05.2010 aasta otsus 2010/261/EL keskse SIS II ja sideinfrastruktuuri turvakava kohta.

SIS II siseriiklik osa on loodud siseministri 22. detsembri 2009. a määruse nr 93 „Schengeni infosüsteemi riikliku registri pidamise põhimäärus" alusel.

Omaalgatuslik järelevalve käsitleb järgmisi valdkondi: andmete kogumine, töötlemine ja säilitamine; andmesubjekti õigused; juurdepääs Schengeni infosüsteemi riiklik registrile (edaspidi ESIS); logimine; kontrolli teostamine; ning infoturve. Eesmärk on teha kindlaks, kas isikuandmete töötlemisel järgitakse kehtestatud nõudeid. Järelevalve jätkub 2018. aastal.

RIIKLIK STATISTIKA

Liisa Ojangu, vaneminspektor

Statistikanõukogu on riikliku statistika tegijaid (Statistikaametit ja Eesti Panka) ning Rahandusministeeriumi nõustav organ, mille moodustab riikliku statistika seaduse alusel Vabariigi Valitsus.

Statistikanõukogu eesmärk on tagada nõustades ja arvamust avaldades riikliku statistika süsteemi toimimine. Statistikanõukogus on 13 liiget: Statistikaameti, Eesti Panga ja Andmekaitse Inspektsiooni esindaja ning veel kümme riikliku statistika tarbijate ja andmeesitajate esindajat ning eksperti. Statistikanõukogusse ekspertide määramisel on lähtutud põhimõttest, et esindatud oleksid statistika, rahvastiku, sotsiaalvaldkonna, keskkonna, majanduse ja põllumajanduse asjatundjad. 2017. Statistikanõukogu koosolekute protokollid on kättesaadavad siin.

REGISTREERIMIS- JA LOAMENETLUSED

Delikaatsete isikuandmete töötlemine

Helve Juusu, vanemspetsialist

Peamiseks arenguperspektiiviks on andmekaitsereform ning ka delikaatsete isikuandmete töötlemisega seonduvalt valmistutakse isikuandmete kaitse üldmääruse kohaldamiseks. Muudatused puudutavad ka delikaatsete isikuandmete töötlemise registrit, mis senisel kujul kaob. Esile kerkib uus mõiste, milleks on andmekaitseametnik ehk andmekaitsespetsialist.

Alates 25.05.2018 muutub kehtetuks 1995. aastast pärinev andmekaitsedirektiiv 95/46 ja sellel põhinev isikuandmete kaitse seadus ning see on tekitanud delikaatsete isikuandmete töötlejate hulgas poleemikat. Delikaatsete isikuandmete töötlemise registreerimise kohta esitati 2017. aastal palju küsimusi, kuid statistikat telefonikõnede arvu kohta seoses registreerimismenetlustega hakkasime loendama alles aasta viimastel kuudel. Perioodi viimase nelja kuu jooksul tuli selliseid kõnesid inspektsioonile kokku 234 korral.

2017. aastal olid peamised takistused ja mured delikaatsete isikuandmete töötlemise registreerimisel järgmised:

1) asjaolu, et taotluse muutmise ajal ei ole vastutava töötleja staatus avalikustatud registridokumentides kodanikule nähtav;
2) ei olnud selge vastutavate ja volitatud töötlejate suhe – vastutav töötleja annab volitatud töötlejatele kohustuslikke juhiseid isikuandmete töötlemiseks ja vastutab selle eest, et volitatud töötleja täidab isikuandmete töötlemise nõudeid;
3) kui andmeid hoiustatakse kodeeritud kujul (statistika eesmärgil, ilma isiku tuvastamiseks vajaminevate detailideta nagu nimi, aadress, meiliaadress ja isikukood), siis kas on kohustus registreerida ettevõte delikaatsete isikuandmete töötlejana.

Sagedasemad küsimused puudutasid ka DIAT-registri veebikeskkonna kasutamist ning registreerimistoiminguid.

Registreeringu kehtivus peale ettevõtete ühinemist

Inspektsioonilt paluti seisukohta seoses ettevõtte kehtiva delikaatsete isikuandmete töötlemise registreeringuga pärast piiriülest ühinemist. Inspektsioonis delikaatsete isikuandmete töötlejana registreeritud vastutav töötleja on sõlminud piiriülese ühinemise lepingu Soomes registreeritud emaettevõttega ning ühinemisel lähevad kõik õigused ja kohustused üle ühendavale ühingule ehk emaettevõttele. Eestis jätkab tegutsemist filiaal muudetud ettevõtte nimega ja uue registrikoodiga. Tõstatus küsimus, kas kehtiv delikaatsete isikuandmete töötlemise registreering jääb pärast ühinemist Eesti filiaali suhtes kehtima ning kas uut registreerimistaotlust ei ole vaja esitada. Kuna on asutatud uue ärinimega ja registrikoodiga filiaal, siis tuleb Andmekaitse Inspektsioonile esitada uus delikaatsete isikuandmete töötlemise registreerimise taotlus või määrata isikuandmete kaitse eest vastutav isik ettevõttes.

Tõrge koolide ja lasteaedade taotluste esitamisel

Aasta lõpus saabusid inspektsioonile teated lasteaedadelt, koolidelt (avalik-õiguslikud asutused), kes soovisid sisestada delikaatsete isikuandmete töötlemise taotlust või teatist isikuandmete kaitse eest vastutava isiku määramiseks, kuid esitamine registris oli takistatud ning digitaalselt registrisse sisenemisel kuvas veateadet. Nüüdseks on see probleem lahendatud.

Uued mõisted: andmekaitsespetsialist ja eriliigilised isikuandmed

Alates 2018. aasta 25. maist, kui hakatakse kohaldama uut isikuandmete kaitse üldmäärust, lõpeb delikaatsete isikuandmete töötlemise registreerimine senisel kujul. Delikaatsete isikuandmete töötlemise registreerimise kohustus kehtib kuni 24.05.2018. Kuni selle kuupäevani saab DIAT-registris esitada töötlemise taotlusi ja teatisi isikuandmete kaitse eest vastutavate isikute määramisest. Alates 25. maist registreerimise kohustus kaob, uusi taotlusi enam esitada ei saa ning register arhiveeritakse.

Üldmääruse jõustumisega kaotab kehtivuse ka isikuandmete kaitse seaduse § 4 lõige 2, mis sätestas, millised on delikaatsed isikuandmed. Üldmääruse mõistes nimetatakse neid edaspidi eriliigilisteks isikuandmeteks. Isikuandmete kaitse üldmäärus toob kaas veel ühe uue mõiste: „andmekaitsespetsialist“. Määruse artikkel 37^1 sätestab, millised isikuandmete töötlejad peavad andmekaitsespetsialisti määrama. Nendeks on

- avaliku sektori asutus või organ,
- andmetöötlejad, kelle põhitegevuseks on ulatuslik andmesubjektide korrapärane ja süstemaatiline jälgimine,
- andmetöötlejad, kelle põhitegevuseks on andmete eriliikide ulatuslik töötlemine või süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete ulatuslik töötlemine.

Kui teie asutusel või ettevõttel on üldmääruse kohaselt vaja määrata andmekaitsespetsialist, peate spetsialisti määramisest teavitama Andmekaitse Inspektsiooni. Seda saate teha alates 2018. aasta aprilli lõpust ettevõtjaportaali kaudu. Täiendav info lisatakse inspektsiooni võrgulehele www.aki.ee.

Isikuandmete töötlemine teadusuuringutes

Liisa Ojangu, vaneminspektor

Nagu igasuguseks isikuandmete töötlemiseks, on ka teadusuuringu läbiviimiseks vaja õiguslikku alust. Laias laastus saab õiguslikuks aluseks olla kas isiku nõusolek või seaduses ettenähtud kohustuse täitmine. Isikuandmete kaitse seadus lubab töödelda isikuandmeid teadusuuringu jaoks, sõltumata sellest, millisel eesmärgil need andmed algselt kogutud on. Juhul kui isikuandmete kasutamine kodeerituna ei ole võimalik, siis tuleb Andmekaitse Inspektsioonilt taotleda luba, mille väljastamisega luuakse õiguslik alus isikustatud kujul andmete töötlemiseks.

Kohustus jälgida õigusliku aluse olemasolu on igal andmetöötlejal. Seega peaksid need andmetöötlejad, kes väljastavad teadusuuringute tarbeks andmeid isikustatud kujul, alati küsima juurde ka inspektsiooni väljastatud loaotsust (muidugi on siin erandiks eelmainitud isiku nõusolek).

Koostöö eetikakomiteedega

Andmekaitse Inspektsioonile esitati 2017. aastal 56 loataotlust või loaotsuse muudatuse taotlust teadusuuringus isikuandmete töötlemiseks. 2016. aastal esitati 18 taotlust. Taotluste hulga suurenemine näitab teadusuurijate teadlikkuse tõusu andmekaitse valdkonnas. Sellele on kindlasti kaasa aidanud Andmekaitse Inspektsiooni ning Tallinna ja Tartu meditsiinieetika komiteede 2016. aastal käivitatud koostöö, mille raames suunavad eetikakomiteed teadusuurijaid teadustöös isikustatud andmete kasutamisel ka inspektsiooni juurde luba taotlema.

2017. kolmandas kvartalis viisin läbi seire, milles palusin Tallinna ja Tartu meditsiinieetika komiteedelt ning Tervise infosüsteemi eetikakomiteelt nimekirja teadusuuringutele antud kooskõlastustest. Tallinna eetikakomitee on 2017. aasta oktoobri seisuga välja andnud 83 kooskõlastust, Tartu eetikakomitee 119 kooskõlastust ning Tervise infosüsteemi eetikakomitee 4 kooskõlastust. Inspektsioon oli novembri lõpu seisuga andnud 37 luba. Seega on inspektsiooni loa taotlenud kuni 20% eetikakomiteedes kooskõlastuse taotlenutest. Täpsema ülevaate saamiseks esitasin eetikakomiteedele täiendava päringu asutuste kohta, kes inspektsiooni luba kordagi taotlenud pole või uuringute pealkirja alusel, kus ilmselgelt isikuandmeid töödeldakse. Nende osas toimub täiendav järelevalvemenetlus.

Et teadusuuringute taotluste arv on kasvamas ning vähemalt meditsiiniuuringute valdkonnas tegutsevad juba praegu professionaalsed eetikakomiteed, on AKI teinud Justiitsministeeriumile ja Sotsiaalministeeriumile ettepaneku kaaluda teadusuurijate halduskoormuse vähendamist nii, et seaduse alusel loodud eetikakomiteelt saadud kooskõlastuse puhul ei ole täiendavalt vaja taotleda inspektsiooni luba. See eeldab seniste eetikakomiteede töökorralduse üle vaatamist ja andmekaitsealase kompetentsi tõstmist, millega Sotsiaalministeerium on lubanud tegelema asuda.

Uued suunad: poliitika kujundamise uuringud ning algoritmide väljatöötamine

Siiski esitatakse inspektsioonile järjest rohkem teadusuuringu taotlusi ka muudest kui meditsiiniuuringute valdkondadest. Eelkõige tehnika arendamise valdkondadest, näiteks transkriptsioonitarkvara arendamiseks ja erinevate algoritmide väljatöötamiseks. Samuti on kasvanud ministeeriumite esitatud poliitika kujundamise uuringute taotlused. Et kehtiv isikuandmete kaitse seadus reguleerib vaid teadusasutuste poolt tehtud uuringuid, on inspektsioon teinud ettepaneku uue andmekaitse üldmääruse siseriiklikus rakenduseseaduses reguleerida ka poliitika kujundamise uuringutega seonduv.

Tihti soovitakse poliitika kujundamise uuringutes kasutada andmeid väga mitmetest erineva ministeeriumi haldusalas olevatest andmekogudest ning sageli on uuringu teema delikaatseid isikuandmeid puudutav. Selliste mahukate uuringute puhul on kindlasti eelnev inspektsioonilt loa taotlemine vajalik, et vältida läbimõtlemata andmete töötlemisest tulenevaid ohte. Eelkõige hindabki inspektsioon teadusuuringule luba andes seda, et

vastutav töötleja on kõik andmete töötlemisega seotud etapid läbi mõelnud ning võimalikud ohud kaardistanud ja nende maandamiseks abinõud rakendanud.

2017. aasta mahukamad ja kõige rohkem delikaatseid isikuandmeid puudutanud uuringutaotlused tulid just Sotsiaalministeeriumilt. Näiteks: „Puuetega laste perede toimetuleku ja vajaduste uuring“ ja „Aastatel 2006–2015 enesetapu sooritanute epidemioloogiline ülevaade“.

Nimetamist väärib ka Tallinna Tehnikaülikooli taotlus uuringuks, millega soovitakse välja töötada algoritm, mis suudaks ennustada, millal on üliõpilane väljalangemise ohtu sattumas. Selleks soovitakse töödelda viimase viie aasta kõikide üliõpilaste väga ulatuslikke andmeid alates ülikooli erinevate ruumide külastamisest kuni kooli e-posti kontrollimise sageduseni, rääkimata üliõpilase sotsiaalse tausta andmetest. Andmekaitse Inspektsioon ei ole taotlust rahuldanud, sest esineb tugev kahtlus, kas valitud meede on soovitud tulemuse saavutamiseks proportsionaalne. Inspektsioon on küsinud ka oma Euroopa kolleegide kogemuste kohta sarnaste algoritmide osas isikuandmete töötlemiseks ning seniste vastuste põhjal näib, et ükski andmekaitseasutus ei ole sellise andmetöötlusega seni kokku puutunud.

Isikuandmete edastamine mittepiisava andmekaitse tasemega riikidesse

Maarja Kirss, koostöödirektor

Isikuandmete kaitse seaduse kohaselt võib isikuandmeid edastada kolmandatesse riikidesse Andmekaitse Inspektsiooni loal või isikuandmete kaitse seaduse § 18 lõikes 5 ettenähtud erandjuhtudel. Kolmandate riikide all peetakse silmas riike, mis ei ole Euroopa Liidu liikmesriigid ega ole liitunud Euroopa Majanduspiirkonna lepinguga (Norra, Island). Viimati mainitud välisriikidesse võib isikuandmeid edastada samadel tingimustel, kui edastamine toimuks Eesti siseselt. Kolmandaid riike nimetatakse ka mittepiisava andmekaitse tasemega riikideks.

Kolmandate riikide puhul on lisaks Euroopa Komisjon ettenäinud ka erandeid, kellele võib isikuandmeid ilma inspektsiooni loata edastada – need on riigid, mille andmekaitse taset on

eraldi analüüsitud ja hinnatud piisavaks (selliste riikide nimekirja leiab Euroopa Komisjoni kodulehelt andmekaitse rubriigist). Muuhulgas on loetud piisava andmekaitse tasemega andmete edastamiseks edastamist Ameerika Ühendriikidesse kasutades Eraelukaitse Kilbi andmekaitseraamistikku (*Privacy Shield*). Kuigi üldisena Ameerika Ühendriike ei loeta piisava andmekaitse tasemega riigiks.

Seega tuleb teatud juhtudel Inspektsioonile esitada loataotlus isikuandmete edastamiseks kolmandasse riiki. Taotluses selgitatakse andmete edastamise eesmärke, andmete koosseisu, isikute kategooriaid, kelle andmeid edastatakse ja loomulikult nimetatakse need mittepiisava andmekaitse tasemega riigis asuvad andmetöötlejad, kellele isikuandmed edastatakse. Andmete edastamise loa taotlemine põhineb andmetöötlejate vahelistel kokkulepetel või lepingutel – siduvad korporatsiooni eeskirjad (*binding corporate rules*), tüüplepingud (*standard contractual clauses*) või *ad-hoc* lepingud.

Viimastel aastatel toimunud vaidlused andmete edastamise osas Ameerika Ühendriikidesse (*Safe Harbour* programmi tühistamine 2015. aastal ning *Privacy Shield'i* kehtestamine 2016. aastal) on kaasa toonud ka suurema tähelepanu loa taotlemise vajadusele. Aasta-aastalt on kasvanud inspektsioonile esitatud loataotluste hulk (2015. aastal oli neid 8, 2016. aastal 18 ja 2017. aastal laekus 22 loataotlust). Enamik 2017. aastal laekunud taotlustest puudutavad personali- ja kliendiandmete edastamist ülemaailmse korporatsiooni siseselt ühtsesse infosüsteemi.

Laekunud 22 taotlusest rahuldas inspektsioon 20 ning jäeti läbi vaatamata kaks loataotlust. Huvitavaima kaasusena võib välja tuua ühe suurhaigla taotluse statistiliste raviandmete edastamiseks Ameerika Ühendriikides asuvale andmeimportijale (TriNetX Inc.) ravimi- ja teadusuuringute läbiviimise eesmärgil. Andmed oli viidud otsest tuvastamist välistavale kujule, kuid taotleja hinnangul säilis isikuandmete kaudse tuvastamise võimalus. Kuna Ameerika Ühendriikides asuv andmeimportija on liitunud Eraelukaitse Kilbi programmiga, siis jättis inspektsioon nimetatud loa läbi vaatamata. Taoliseks andmete edastamiseks ei ole tule inspektsioonilt luba taotleda, küll aga peab arvestama, et isikuandmete edastamiseks peab alati olema õiguslik alus (ei ole vahet kas edastatakse siseriiklikult või välisriiki) ning see on eraldiseisev edastamise loa andmisest.

Vastastikuse tunnustamise protseduur

Aruandeperioodi lõpus oli inspektsioon esmakordselt kaasatud siduvate korporatsiooni eeskirjade (BCR) heakskiitmise protseduuri kui kaasläbivaataja. Nimelt on Euroopa andmekaitseasutused omavahel sõlminud kokkuleppe, et andmete edastamisel kolmandasse riiki, mis toimub siduvate korporatsiooni eeskirjade alusel, moodustatakse iga korporatsiooni eeskirjade läbivaatamiseks kolmeliikmeline andmekaitseasutuste grupp (juhtiv läbivaataja ja kaks kaasläbivaatajat). Töögrupi liikmed analüüsivad korporatsiooni poolt esitatud materjalid detailideni läbi, esitavad täiendavaid nõudmisi ja parandusi ning lõpptulemusena, kui eeskirjad on viidud vastavusse Euroopa andmekaitsenõuetega, siis kiidavad need eeskirjad heaks.

Taoline menetlus hõlbustab ülejäänud andmekaitseasutuste tööd, kes tunnustavad töögrupi poolt tehtud otsust ning seeläbi on neil võimalik kiiremini jõuda loataotluse saabumisel andmete edastamise loa otsuseni. Kirjeldatud protseduuri nimetatakse vastastikuse

tunnustamise (*mutual recognition*) protseduuriks. Taoline protseduur on ajaliselt väga pikk, enamasti kestab see aasta ja enam. Nagu eelnevalt mainitud, alustasime kaasläbivaatamise protseduuri 2017. aastal, kuid lõpliku tunnustamiseni läheb veel aega.

Eesootavad muudatused

Teadaolevalt on 2018. aasta andmekaitsereformi aasta. Muudatusi tuleb ka välisriiki edastamiste loataotlemistes, sellest saab lugeda inspektsiooni kodulehe vastavast rubriigist. Oluline on teada, et seni väljastatud load jäävad kehtima, välja arvatud juhul, kui neis on vaja teha andmetöötlemise protseduuride ja tingimuste ajakohastamist.

E-residentide pilootprojekt Lõuna Koreas

Raavo Palu, õigusdirektor

Eelmisel aastal algatas Politsei- ja Piirivalveamet (PPA) pilootprojekti e-residentidele digitaalse isikutunnistuse (digi-ID) väljastamiseks Eestist väljaspool asuva partneri poolt. E-residentsuse digi-ID-sid on seni väljastatud ainult PPA teenindustes ja Eesti Vabariigi välisesindustes. Pilootprojekti valiti Lõuna-Korea ning nüüdseks saavad Aasia e-residendid oma digitaalse isikutunnistuse kätte Souli kesklinnas asuvast viisakeskusest. Kuna Lõuna-Korea on Euroopa õigusruumi mõistes kolmas riik, siis pole ta ka piisava andmekaitsetasemega riik. Seetõttu on vajalik selliseks projektiks ka luba Andmekaitse Inspektsioonilt – seda siis isikuandmete edastamiseks Eestist Lõuna-Koreasse.

Andsime 24.11.2017 otsusega nr 2.2-4/17/22 PPA-le loa isikuandmete edastamiseks ebapiisava andmekaitse tasemega riigis asuvale andmete importijale perioodiks 12.12.2017-12.12.2020. Sellele eelnevalt kontrollisime poolte vahel sõlmitavat lepingut, mis sisaldab Euroopa Komisjoni 05.02.2010 otsuses nr 2010/87/EL toodud lepingu tüüptingimusi.

ANDMEKOGUDE PIDAMINE

Avaliku sektori andmekogude kooskõlastamine

Raavo Palu, õigusdirektor

Kui 2016. aasta kohta koostatud aastaettekandes tõime suurima probleemina välja andmekogudes olevad säilitamistähtajad, siis tuleb tõdeda, et ka eelmisel aastal oli see jätkuv probleem andmekogude kooskõlastamisel riigi infosüsteemide haldussüsteemis ehk RIHA-s. Täiendavalt pöörasime kooskõlastamistel ka rohkem tähelepanu andmekogus tehtavate toimingute logimise temaatikale ning vaatasime kuivõrd on kooskõlas andmekogu põhimääruses toodud teave ning RIHA-sse kantud teave.

Eeltoodule tuleb eriti tähelepanu pöörata andmekaitse üldmääruse ning teatavatel juhtudel ka õiguskaitseasutuste direktiivi alusel vastu võetud sätete rakendamise tõttu – mõlemad õigusaktid nõuavad sisuliselt, et isikuandmete töötlemine oleks läbipaistvam ja inimese jaoks selgem. Üheks selliseks väljundiks on andmekogude pidamist reguleerivates sätetes veel selgemalt reguleerida andmekogus säilitavate andmete säilitamistähtajad, juurdepääs kogutavatele andmetele ning kontrolli teostamine tehtavate andmetöötluste osas. Kontrolli teostamise osas mõtleme, et ka andmekogude vastutav töötleja teeks ise kontrolli, kes ning mis eesmärgil tema andmekogu andmeid kasutab.

Siseministeeriumi ning Politsei- ja Piirivalveameti andmekogud

Eelneval aastal sai mitme ministeeriumi ning asutuse tähelepanu juhtida säilitamis-tähtaegade ja -eesmärkide probleemile andmekogudes. Näiteks on Siseministeeriumi haldusalas, sh ennekõike enamustes Politsei- ja Piirivalveameti andmekogudes olevatele andmetele määratud alatine säilitamistähtaeg.[9] Samuti olid mõne andmekogu osas andmete säilitamise tähtajad üldse teadmata. Lisaks ei olnud selgelt reguleeritud neis andmekogudes andmete pikema säilitamise eesmärk ning tagatud andmekogude juurdepääsuregulatsiooni kooskõla säilitamise eesmärgiga.

Näiteks Eesti kodakondsuse saanud, taastanud või kaotanud isikute andmekogu pidamise eesmärk on *„töödelda andmeid kodakondsuse seaduses sätestatud menetluste läbiviimiseks ning pidada arvestust Eesti kodakondsuse saanud, taastanud või kaotanud isikute ja nende taotluste üle“*. See eesmärk ei hõlma kuidagi andmete pikaajalist säilitamist näiteks terrorismiga võitlemiseks või avaliku korra tagamiseks. Riikliku rahvusvahelise kaitse andmise registri pidamise eesmärk põhimääruse sõnastuses on „andmete töötlemine“. Välismaalase lühiajalise Eestis töötamise registreerimise andmekogu, Eestis seadusliku aluseta viibivate ja viibinud välismaalaste andmekogu, elamislubade ja töölubade registri ning viisaregistri pidamise eesmärk on „tagada avalik kord ja riigi julgeolek“. Isikut tõendavate dokumentide andmekogu peetakse riigi sisejulgeoleku tagamiseks.

[9] Siseministeeriumile ning Politsei- ja Piirivalveametile saadeti seisukoht 09.01.2017 kirjaga nr 2.2.-8/16/1604 – kättesaadav: http://adr.rik.ee/aki/dokument/4945713.

Selline säilitamise korraldus ei ole kuidagi kooskõlas andmekaitse põhimõtetega, mida kinnitavad ka Euroopa Kohtu kaks elektrooniliste kontaktandmete kohta tehtud lahendit.[10] Neis lahendites tunnustab Euroopa Kohus igati võitlust terrorismi ja raske kuritegevuse vastu avaliku julgeoleku tagamiseks kui üldist huvi pakkuvat EL-i eesmärki. Kohtulahendid selgitavad, et ka sel eesmärgil ei ole õigustatud isikuandmete valimatu ja üldine säilitamine. Põhiõiguste piirangud peavad olema rangelt vajalikud ning õigusakt peab andma selged ja täpsed reeglid ja garantiid. Palusime Siseministeeriumil kõnealustes andmekogudes säilitamise eesmärgid, tähtajad ja juurdepääsud üle vaadata, kusjuures regulatsiooni läbivaatamisel tuleks:

- selgelt määratleda andmete algsest kogumise eesmärgist (nt taotluse alusel loa väljastamine) erinev eesmärk (riigi julgeolek, rasked kuriteod, terrorism *vs* igasugune avaliku korra kaitse, arvestades korrakaitseseaduse avaliku korra ülilaia sisu ja korrakaitseorganite paljusust);[11]
- üle vaadata surnud või eeldatavalt surnud inimeste andmete säilitamise põhjendatus (saab määrata säilitamistähtaja tulenevalt eeldatavast maksimaalsest elueast) – surnud inimene ise ei saa enam kujutada ohtu avalikule korrale;
- õigusakti tasandil reguleerida pikema säilitamise eesmärgil andmete aktiivsest andmebaasist selgelt piiritletud juurdepääsuga arhiivi kandmine ja juurdepääsud;
- vähendada andmekoosseis vastavaks pikema säilitamise eesmärgile (kõiki algselt kogutud andmeid ei pruugi pikema säilitamise eesmärgil vaja olla ning osad andmed ilmselgelt aeguvad pikas perspektiivis).

Maksu- ja Tolliameti andmekogud

Probleemid säilitamistähtaja reguleerimisel on ka Maksu- ja Tolliameti maksukohustuslaste registril. Andmekogu kooskõlastamisel selgus, et maksukohustuslaste registri andmetele on Maksu- ja Tolliamet määranud alatise säilitamistähtaja. Samas maksukorralduse seadus ega selle andmekogu põhimäärus säilitamistähtaega ei reguleeri. MTA teavitas kooskõlastamisel, et asub neid säilitamistähtaegasid üle vaatama, kuid senini pole seda tehtud.

Eelmise aasta juulist jõustus uus tolliseadus, mis annab ka aluse mitme andmekogu loomiseks. Senini ei ole kehtestatud e-tolli andmekogu põhimäärust, kuigi MTA soovis sellele andmekogule juba enne tolliseaduse kehtima hakkamist saada asutamise kooskõlastamist RIHA kaudu. Toona jäeti kooskõlastus tegemata, kuna tol hetkel ei olnud tolliseadus jõustunud ning puudus lõplik ning jõustunud põhimäärus. Tolliseaduse alusel on võimalik asutada ka reisijate nimekirjade töötlussüsteemi andmekogu, läbivalgustuse piltide andmekogu ning tolli automaatse numbrituvastussüsteemi andmekogu, kuid ka need andmekogud ei ole läbinud RIHA kooskõlastust. Neist esimesele andmekogule sooviti samuti enne tolliseaduse kehtima hakkamist saada asutamise kooskõlastust, kuid toona oli selle andmekogu osas mitmeid puudusi, mistõttu jäeti see kooskõlastamata.

[10] 21.12.2016 liidetud kohtuasjades C-203/15 ja C-698/15 ja 8.04.2014 liidetud kohtuasjades C-293/12 ja C-594/12
[11] Seejuures arvestades, et KoRS § 4 lg 2 annab eriti avara tõlgendamisruumi eraõiguslike suhete avaliku korra alla kuuluvuse osas.

Sotsiaalministeeriumi haldusala andmekogud

Kuna Sotsiaalministeeriumi haldusalas on valdavalt enim teavet, mis on käsitletav delikaatsete isikuandmetena (andmekaitse üldmääruse mõistes eriliigilsite isikuandmetena), siis selle haldusala andmekogude osas peab isikuandmete töötlus olema veelgi selgem ja läbipaistvam. Näiteks ilmnes kooskõlastamistest, et vähi sõleuuringute registri andmeid sooviti säilitada tähtajatult. Samas Rahvusarhiiv oli RIHA kooskõlastuses märkinud, et nende andmete osas arhiiviväärtus puudub.

Probleem alatise säilitamistähtaja osas on ka Terviseameti peetava mürgistusteabe andmekogul. Rahvusarhiiv oli enda kooskõlastuste juures märkinud, et nendel andmetel puudub arhiiviväärtus. Samas andmekogu põhimääruses oli märgitud, et enamikke andmeid säilitatakse tähtajatult.

Samuti on jätkuvalt alatise säilitamistähtajaga ka kollektiivlepingute andmekogus olevad andmed. Möödunud aastal sooviti selle andmekogu põhimäärust muuta, kuid siis ei soovitud teha muudatusi andmete säilitamistähtaja osas. Lisaks sellele on suurem probleem andmekogu volitusnormiga, kuna seaduses puudub volitusnorm, millega lubatakse kollektiivlepingute andmekogus isikuandmeid töödelda.

Töövõime hindamiste ja toetuste andmekogu (TETRIS) käis 2016. a asutamise kooskõlastamisel ning selgus, et Töötukassa e-teeninduses on töövõime hindamise taotlus lahendatud selliselt, et ilma tervise infosüsteemi kasutamiseks nõusoleku andmiseta ei ole taotluse esitamine võimalik (ilmub veateade, et kohustuslikud nõusolekud on andmata). Samuti ei olnud taotluse pabervormil võimalik eraldi märkida nõusoleku andmist tervise infosüsteemi päringute tegemiseks. Selgitasime, et selline olukord ei vasta Sotsiaalministeeriumi poolt välja töötatud ja vastu võetud töövõimetoetuse seadusele, mis annab taotlejale õiguse otsustada, kas ta annab Töötukassa ekspertarstile juurdepääsu tervise infosüsteemi kantud andmetele või mitte. Nõusoleku mitteandmisega ei kaasneks mitte taotluse rahuldamata jätmine, vaid inimene peaks andmed sellisel juhul ise tervishoiuteenuse osutajatelt kokku koguma ning Töötukassale esitama. Sotsiaalministeerium asus 2016. a suvel seisukohale, et vastuolu seadusega tuleb kõrvaldada.

2017. a aprillis kontrollisime, kas vastuolu on kõrvaldatud. Selgus, et olukord oli täpselt sama, mis 2016. a suvel. Töötukassa asus seisukohale, et muuta tuleks seadust, mitte infosüsteemi ega taotlemise vorme. Samas ei ole senini vastavaid muudatusi tehtud – ei õigusaktides, ega taotluste vormides. Samas võeti töövõimetoetuse seadus (TVTS) vastu 19.11.2014 ning jõustus 01.07.2016, sh samal ajal jõustus ka praeguse sõnastusega TVTS § 6. Seega oli Töötukassale juba varakult teada, kuidas toimub juurdepääs isiku terviseandmetele. Kehtiv seadusandlus kohustab võtma isikult nõusoleku, kuid infotehnoloogilise probleemi tõttu ei ole isikul võimalik ise otsustada, kas ta üldse annaks seda nõusolekut või mitte. Asjaolu, et infotehnoloogiliselt ei ole süsteem välja arendatud, ei saa olla ainuke ettekääne seadusandluse muutmiseks. Sel juhul oleks pidanud juba infosüsteemi loomise protsessis sedasorti probleemid ära lahendama. Samuti pole TETRIS senini läbinud kasutusele võtmise kooskõlastust.

Justiitsministeeriumi haldusala andmekogud

Tööstusomandi õiguskaitse valdkonna registrite pidamist reguleerib tööstusomandi õiguskorralduse aluste seadus. Meile on kooskõlastamistest teatavaks saanud, et selles seaduses kirjeldatud registrite ülesehitus ei haaku infosüsteemi tegeliku ülesehitusega. Seniste infosüsteemide puhul oli keeruline aru saada, kuidas seaduses kirjeldatud kannete ja märgete süsteem ning andmekoosseisud infosüsteemiga reaalselt haakuvad. Kuna meile teadaolevalt on kõigi tööstusomandi õiguskaitse valdkonna registrite osas arendamisel uus menetlustarkvara, siis soovime, et uue süsteemi arendamisel tagatakse infosüsteemi toimimise loogika kooskõlas seaduses kirjeldatud registri loogikaga.

Välisministeeriumi haldusala andmekogud

Välisministeerium soovis saada konsulaarametnike ametitoimingute raamatu osas kasutusele võtmise kooskõlastust, kuid ka selle andmekogu osas olid probleemid säilitamistähtaegadega (lisaks muudele probleemidele). Toona oli RIHA andmetel selle andmekogu andmete säilitamistähtajaks alatine säilitamistähtaeg. Samas Rahvusarhiiv märkis oma kooskõlastamise osas, et andmeid pole arhiivinduslikult hinnatud, kuid eelduslikult puudub arhiiviväärtus (ehk puudub vajadus alatiselt säilitada).

Välisministeerium soovis saada välisriikide ja rahvusvaheliste organisatsioonide esinduste, rahvusvaheliste organisatsioonide ja rahvusvahelise kokkuleppega loodud institutsioonide ning nende isikkoosseisu andmekogu andmete koosseisu muutmise kooskõlastamist, kuid ka selle andmekogu osas oli mh probleem andmete alatise säilitamisega. Seetõttu me ei andnud vastavat kooskõlastust.

Keskkonnaministeeriumi haldusala andmekogud

Keskkonnaministeerium soovis vastu võtta keskkonnaotsuste infosüsteemi põhimäärust, sh määrata andmetele alatine säilitustähtaeg, kui õigusaktist ei tulene teisiti. Seletuskirjas märgiti, et *„kuna andmekogusse sisestatakse andmeid, millele kohaldatakse nõudeid paljudest eri õigusaktidest, on otstarbekas jätta sätte sõnastus paindlikuks.“* Samas sõnastuses võeti eelnõu ka vastu ning see oli ka üks põhjustest, miks ei antud andmekogule kooskõlastust. Samas senini ei ole sellekohaseid muudatusi andmekogu põhimääruses tehtud. Ka Rahvusarhiiv leidis oma kooskõlastuses, et eelduslikult puudub sellesse andmekogusse kantud andmetele arhiiviväärtus ehk vajadus andmeid alatiselt säilitada.

Uuendused RIHA kooskõlastuses

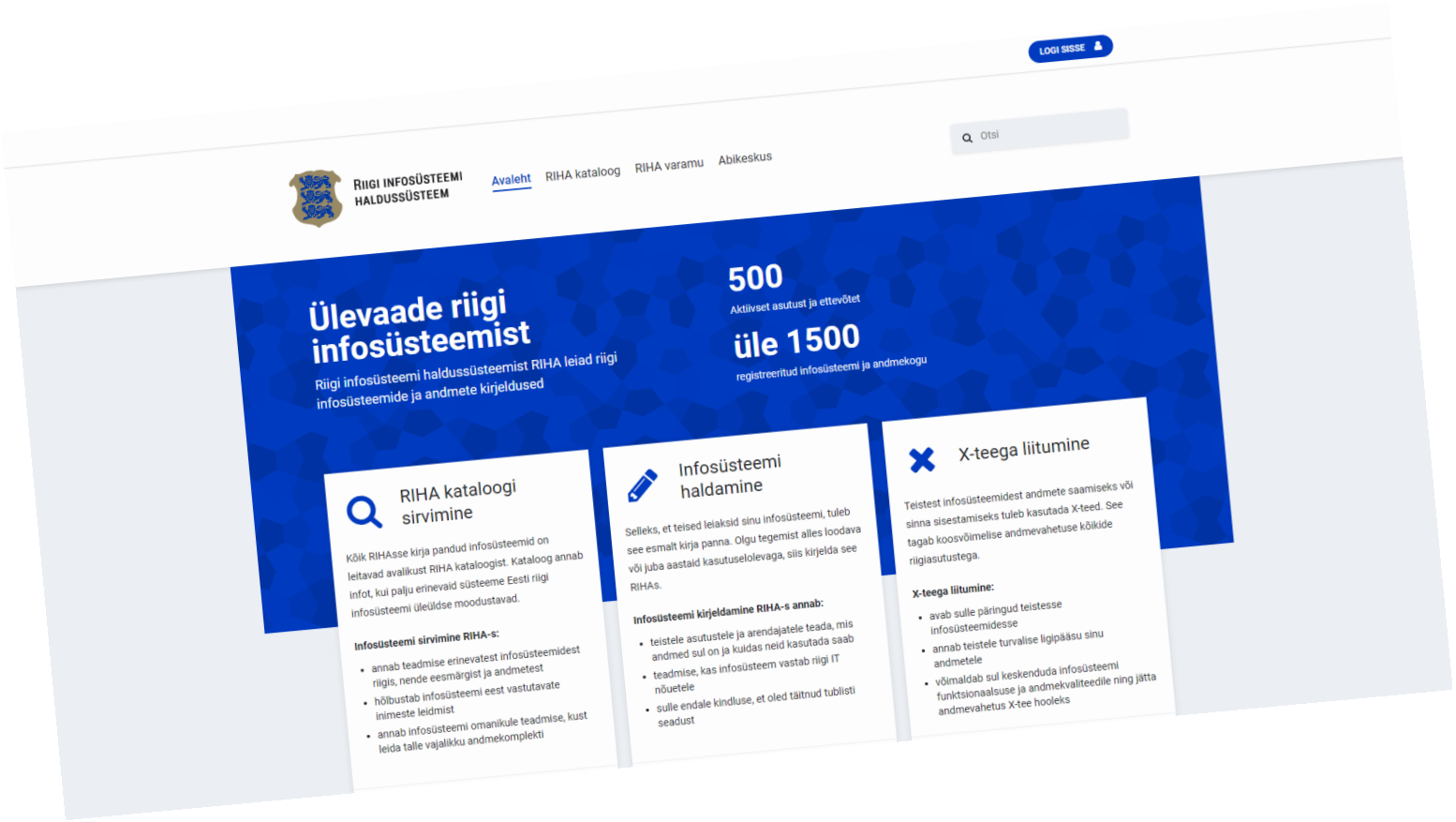
Alates 01.11.2017 on kasutusele võetud uus RIHA, kuid uue lahenduse kasutusele võtuga muutus ka oma olemuselt RIHA ülesehitus ja sellega seotud andmete koosseis. Vähemalt esialgu ei ole lubatud RIHA-sse üles laadida juurdepääsupiirangulist teavet sisaldavaid dokumente. See muudatus sundis meid muutma meie menetlusprotseduure, kuna me ei saanud oma kooskõlastuste tegemiseks vajaliku informatsiooni täies mahus RIHA-st kätte.

Ainsa lahendusena leidsime, et hakkame meile vajalikku teavet küsima nõudekirjaga RIHA-väliselt otse andmekogu kooskõlastamisele esitajalt (enamasti andmekogu vastutavalt töötlejalt). On arusaadav, et selline tegevus viib meid mõne sammu tagasi ning on ka

andmekogude vastutavatele töötlejatele lisakoormuseks, kuid vastasel juhul puudub meil võimalus anda kooskõlastus andmekogu asutamisel, kasutusele võtmisel, andmekoosseisu muutmisel või lõpetamisel.

Avaldasime oma võrgulehel selle teabe, mida andmekogude kooskõlastamisel küsime. Ühe täiendava lisandusena võrreldes nö tavapärasega küsime edaspidiselt ka andmekaitselist mõjuhinnangut, kui isikuandmete töötlemine hakkab toimuma peale 25.05.2018. Kui tegemist on avaliku sektori andmekogudega, siis eeldame, et andmekaitseline mõjuhinnang on koostatud vastava andmekogu põhimääruse või selle põhimääruse muudatuse seletuskirjas – sel juhul eraldi sellist dokumenti ei ole vaja luua. Andmekogu põhimääruse seletuskiri võib, aga ei pruugi katta andmekaitselist mõjuhinnangut – reaalsuses pannakse tegelikud andmetöötluse asjaolud (ja nendega seotud ohud) paika isikuandmete töötlemise käigus. Kui on vähegi uus kohustus, mis hõlmab ka uut tehnoloogiat, siis peaks andmetöötleja ka need mõjud üle vaatama – kas eelnõu koostamisel või hiljemalt rakendamise käigus.

Eeltoodud menetluskord kehtib Andmekaitse Inspektsioonis seni, kuni me saame kogu meile vajamineva teabe uuesti RIHA kaudu.



RIHA kooskõlastamisega seotud soovitused

Arutelud eelnevalt välja toodud ning ka teiste andmekogude pidamise, sh säilitamistähtaegade temaatika osas kestavad senini edasi. Eeldatavasti soovitakse neist enamus lahendada andmekaitse üldmäärusega seotud ning õiguskaitseasutuste direktiivi

ülevõtmisega seotud rakendusseaduste sätetes. Seetõttu soovitame andmekogude vastutavatel töötlejatel RIHA kooskõlastuste sujuvama läbiviimise jaoks andmekogude osas:

- vastavalt olukorrale viia läbi andmekaitseline mõjuhinnang;
- määratleda andmekogu reguleerivas õigusaktis ja/või põhimääruses kohased andmete säilitamistähtajad;
- kontrollida andmekogudes olevatele andmete juurdepääsude vajalikkust ja ulatust, sh kas põhimääruses toodu vastab ka reaalsusele;
- mõelda läbi logide pidamine, haldamine ning nende kontrollimine;
- viia läbi andmekogus olevate andmete osas avaandmete hindamine – nt teha seda põhimääruse seletuskirjas, kui toimuvad muudatused andmekogu pidamises.

Andmekogude järelevalvest

Andrus Altmeri, andmeturbeinspektor

Olukord 2017. aasta jaanuaris

RIHAsse on sisestatud 492 andmekogu/infosüsteemi. Andmekogudest/infosüsteemidest on staatuses „Kasutusel“ 277, lisaks on 53 andmekogu/infosüsteemi staatuses „Lõpetatud“ ja 14 märkega „Ei asutata“. 148 andmekogu/infosüsteemi on muus staatuses („Asutamine sisestamisel“, „Asutamine kooskõlastamisel“, „Asutamine kooskõlastatud“, „Kasutusele võtmine kooskõlastamisel“, „Kasutusele võtmine registreerimisel“).

ISKE rakendamise ja auditeerimise kohta on inspektsioonil infot 143 andmekogu/infosüsteemi puhul. Vastavalt RIAga sõlmitud koostööleppele ei tegele inspektsioon järelevalve korras enam peamise ülesandena riiklike andmekogude/infosüsteemide ISKE rakendamise ja auditeerimise kontrolliga, seetõttu ei näita ISKE info kindlasti tõelist ja täielikku seisu. Täpsemat ülevaadet ISKE kui riikliku infoturbestandardi rakendamise olukorra kohta kogub Riigi Infosüsteemi Amet.

Esmasesse järelevalvevalimisse kaasatud andmekogudega on 2017. aasta alguses olukord järgmine:

- Haridus- ja Teadusministeeriumi valitsusala 12 probleemsest andmekogust on tänaseks korrastatud 9, ülejäänute puhul on plaan info korrastada 2017. aasta I kvartalis;
- Justiitsministeeriumi 30 probleemsest andmekogust on tänaseks korrastatud 24, ülejäänute puhul on tähtajaks 2017. aasta II kvartal;
- Sotsiaalministeeriumi 17 probleemsest andmekogust on tänaseks korrastatud 9, ülejäänute puhul on tähtajaks 2017. aasta II kvartal;
- Siseministeeriumi andmekogude puhul on tänaseks kokku lepitud ISKE auditite kava, millega SMITi ISKE auditid tehakse ära ajavahemikus 2017-2018;
- Keskkonnaministeeriumi 50 andmekogust on nende endi hinnangul probleeme 22 andmekoguga, ministeeriumi esitatud kava kohaselt korrastatakse need kõik 2017. aasta lõpuks.

Olukord 2017. aasta aprilli lõpuks

RIHAsse oli sisestatud 802 infosüsteemi/andmekogu. Neist 33 oli staatuses „Ei asutata“ ja 61 staatuses „Lõpetatud“ või „Lõpetamise kooskõlastamisel“. „Kasutusel“ oli 539 infosüsteemi/andmekogu ja muus staatuses 169 („Asutamine sisestamisel“, „Asutamine kooskõlastamisel“, „Asutamine kooskõlastatud“, „Kasutusele võtmine kooskõlastamisel“, „Kasutusele võtmine registreerimisel“).

Järelevalvevalimisse kaasatud andmekogudega on 2017. aasta esimese trimestri lõpuks olukord järgmine:

- Haridus- ja Teadusministeeriumi valitsusala 12 probleemsest andmekogust oli korrastatud 10, kaks viimasena puudustega andmekogu oli läbinud asutamise kooskõlastamise;
- Justiitsministeeriumi 30 probleemsest andmekogust oli korrastatud 29, ainuke veel puudustega register IS003544 vajas kasutuselevõtu kooskõlastuse läbimiseks õigusliku segaduse klaarimist (AKI hinnangul on tegu topeltregistriga, pidaja arvates on kinnipeetavate andmete mitmes registris töötlemine õigustatud);
- Sotsiaalministeeriumi 17 probleemsest andmekogust oli korrastatud 10, ülejäänute puhul oli osaliselt täiendatud RIHA andmestikku, jõutud staatusest „Asutamine sisestamisel“ staatusesse „Asutamine kooskõlastamisel“ või teatatud inspektsioonile kirjalikult põhjustest, miks registri kasutuselevõtt RIHAs venib. Esitatud kava kohaselt likvideeritakse puudused 2017. aasta II kvartali lõpuks;
- Siseministeeriumi andmekogude puhul jätkub kokkulepitud ISKE auditite kava elluviimine, millega SMITi ISKE auditid tehakse ära ajavahemikus 2017-2018;
- Keskkonnaministeeriumi 50 andmekogust oli nende endi hinnangul probleeme 22 andmekoguga, ministeeriumi esitatud kava kohaselt korrastatakse need kõik 2017. aasta lõpuks.

Olukord 2017. aasta augustis

RIHAsse on sisestatud 1045 andmekogu/infosüsteemi. Nende seas on hulgaliselt ka x-tee alamsüsteeme ning muidu liidestusi, mis inspektsiooni seisukohalt ei ole andmekogud, kuid mille registreerimist soovib Riigi Infosüsteemi Amet. Andmekogudest/infosüsteemidest on staatuses „Kasutusel“ 765, lisaks on 62 andmekogu/infosüsteemi staatuses „Lõpetatud“ ja 3 märkega „Ei asutata“. 215 on muus staatuses („Asutamine sisestamisel“, „Asutamine kooskõlastamisel“, „Asutamine kooskõlastatud“, „Kasutusele võtmine kooskõlastamisel“, „Kasutusele võtmine registreerimisel“).

2016. aastal järelevalvevalimisse kaasatud andmekogudega on 2017. aasta teise trimestri lõpuks olukord järgmine:

- Haridus- ja Teadusministeeriumi valitsusala 12 probleemsest andmekogust oli korrastatud 10, kaks viimast riigi seisukohalt vähetähtsat andmekogu oli läbinud asutamise kooskõlastamise. Otsustasin järelevalve lõpetada ja anda kahe viimase andmekogu kasutuselevõtu kooskõlastamiseks aega aasta lõpuni. Probleemide jätkumisel algatan uue järelevalve;

- Justiitsministeeriumi 30 probleemsest andmekogust oli korrastatud 29, ainukese veel puudustega registri teemal palus ministeerium taaskord ajapikendust (register peaks praeguse plaani järgi asendama kahte inspektsiooni hinnangul topeltandmekoosseisuga registrit ja koondama kinnipeetavate andmed ühte andmekogusse). Uus tähtaeg on 2018. a I poolaasta;
- Sotsiaalministeeriumi valitsusala 17 probleemsest andmekogust on endiselt küsitavusi viie puhul, ülejäänute puhul oli osaliselt täiendatud RIHA andmestikku, jõutud staatusest „Asutamine sisestamisel“ staatusesse „Asutamine kooskõlastamisel“ või teatatud AKIle kirjalikult põhjustest miks registri kasutuselevõtt RIHAs venib. Esitatud uue kava kohaselt likvideeritakse puudused 2018. aastal;
- Siseministeeriumi andmekogude puhul on tänaseks kokku lepitud ISKE auditite kava, millega SMITi ISKE auditid tehakse ära ajavahemikus 2017-2018;
- Keskkonnaministeeriumi 50 andmekogust on nende endi hinnangul probleeme 22 andmekoguga, korrastamine jätkub 2018.

Kokkuvõte

Minu hinnangul on oluliselt täienenud infosüsteemide/andmekogude andmestik RIHAs, mistõttu on paranenud ülevaade riigi infosüsteemi olukorrast ning riigi töödeldavatest andmetest. 2016. aasta esmasesse järelevalvevalimisse kaasatud andmekogude info RIHAs on samuti paranenud, enamus puudusi on likvideeritud ning aastaid ebamäärases staatuses olnud andmekogud on läbinud korrektsed kooskõlastusprotsessid. Järelevalve otstarbekuse huvides otsustasin lõpetada Haridus- ja Teadusministeeriumi andmekogude järelevalve, kuna kõik skoopi kuulunud andmekogud on läbinud vähemalt asutamise kooskõlastamiseringid ning kaks veel kasutusele võtmata andmekogu on riigi infosüsteemi seisukohalt vähetähtsa andmestikuga (õppevara infosüsteem ja Eesti Kirjandusmuuseumi infosüsteem).

Andmekogude pidajad on erinevatel põhjustel palunud ajapikendusi inspektsioonile esitatud tähtaegadest kinnipidamisel. On tõenäoline, et enamus puuduseid likvideeritakse 2018. esimesel poolaastal. Erandiks SoMi andmekogud, mille korrastamine liigutati plaanitult 2018. aastasse ja SMITi hallatud andmekogud, kus „H“ ISKE turvatasemega andmekogude auditid on plaanis teha ära 2017. lõpuks ja muud 2018. aasta lõpuks.

Seoses 2017. aasta lõpus aset leidnud RIHA arendustöödega, oli Andmekaitse Inspektsioon sunnitud oma andmekogude kooskõlastusprotsessid üle vaatama, et jätkuvalt täita avaliku teabe seaduses toodud ülesandeid. Kõige küsitavam uuendus muutunud RIHAs oli AK-teabe välistamine. Senine kooskõlastusprotsess aga hõlmas suuremal või vähemal määral alati ka AK-teavet sisaldava dokumentatsiooni läbivaatamist. Seoses sellega otsustas inspektsiooni kooskõlastusmeeskond tulevikus vajaliku info välja küsida otse andmekogu pidajalt/teabevaldajalt nõudekirjaga, viies kooskõlastusprotsessiks vajaliku teabe RIHAst inspektsiooni dokumendihaldussüsteemi.

ÕIGUSAKTIDE EELNÕUD

Raavo Palu, õigusdirektor

Eelnev aasta oli õigusloomeliselt mitmel moel seotud ka tänavusega – ennekõike andmekaitse õiguse muutumisega. Samuti esitati kooskõlastustele ka mitmeid eelnõusid, mis otseselt ei ole seotud andmekaitse õiguse uuenemisega, kuid on läbivalt seotud isikuandmete töötlemisega – iseasi, kas see toimub mõnes andmekogus või mõne õigusakti alusel toimuva toimingu käigus.

Eelmisel aastal inspektsioonile kooskõlastamiseks esitatud eelnõude osas tooksin välja mõningad eelnõud ning neile antud tagasisidet. Võib kohe öelda, et mitte kõigi kavatsuste osas ei olnud eelnõude koostajad kõike andmesubjekti ning tema õiguste kaitsmise vaatenurgast läbi mõelnud.

Andmekaitseõigus uueneb

Euroopa Parlament ja nõukogu võtsid 2016. aasta aprillis vastu kaks õigusakti, mille kohaldamine ning ülevõtmine on vajalikud Euroopa Liidu tasemel sarnase õiguskorra kehtestamiseks. Nendeks õigusaktideks on:

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

Võiks arvata, et tegemist on andmekaitseõiguse reformiga – siiski see nii ei ole, kuna põhivundament jääb samaks. Selle „reformi" tulemusena sisustatakse osaliselt ka hetkel praktikas kasutusel olevad põhimõtted ja nõuded, nt lõimitud andmekaitse ning vaikimisi andmekaitse põhimõtete olemuse. Samas jäädakse ka edaspidi tehnoloogianeutraalseks – seda ennekõike toimuvate isikuandmete töötlemise toimingute kui ka kasutusele võetavate andmekaitseliste meetmete osas. Põhirõhk on riskipõhisel lähenemisel andmetöötlusele.

Isikuandmete kaitse üldmäärusest kui ka õiguskaitseasutuste direktiivist (vastavalt artikli 36 lõikest 4 ning artikli 28 lõikest 2) tuleneb ka üks eraldiseisev õigusloomeline nõue – selle kohaselt peab riik konsulteerima Andmekaitse Inspektsiooniga, kui koostamisel on Riigikogus vastu võetava õigusliku meetme ettepanek või sellisel õiguslikul meetmel põhinev reguleeriv meede, mis seondub isikuandmete töötlemisega.

Eelnevalt märgitud EL-i õigusaktide sisustamiseks koostas Justiitsministeerium esmalt isikuandmete kaitse uue õigusliku raamistiku kontseptsiooni 18.04.2017 ning alles 24.11.2017 esitati kooskõlastusele uue isikuandmete kaitse seaduse eelnõu. Selle eelnõu ning ka muude asjaolude osas oleme andnud ka mitmeid sisendeid ja tagasisidet. Kõik sellekohane teave on kättesaadav meie võrgulehelt.

Justiitsministeeriumi soov on teha muudatusi kahes etapis – esimene on n-ö kehtestamine ning teine on n-ö teiste seaduste muutmise pakett. Kui esimeses seaduses kehtestatakse ennekõike neid täpsustusi, mida isikuandmete kaitse üldmäärus lubab teha, sh võetakse üle ka nn õiguskaitseasutuste direktiivi sätted, siis teise muudatustepaketi raames muudetakse ülejäänud Eesti õigusruumi, et viia see uue õiguskorraga vastavusse. Samas on kahetsusväärne, et suhteliselt keerukas ning sisuliselt kõiki isikuid mõjutavad muudatused tehakse vägagi kiirustatult ning piltlikult öeldes viimasel tunnil. Siiski võiks loota, et need muudatused on õiguskorras andmesubjektide, isikuandmete töötlejate ning järelevalveasutuse jaoks piisavalt selgelt ja arusaadavalt kirjeldatud – seda nii seadus(t)e enda tekstides kui ka seletuskirja(de)s.

Lisaks isikuandmete kaitse üldmäärusele kavatsetakse eriregulatsioonina kohaldama ka Euroopa Liidu e-privaatsuse määrust. See hakkab e-privaatsusdirektiivi 2002/58 ning elektroonilise side seaduse asemel normima andmekaitse erinõudeid elektroonilise side valdkonnas, sh otseturustust (rämpspost, soovimatud müügikõned). Algselt sooviti seda määrust jõustada koos isikuandmete kaitse üldmäärusega, kuid on selge, et seda ei ole hetkel võimalik saavutada.

Karistusseadustiku jt seaduste muutmise seaduse eelnõu

Andmekaitseõiguse uuenemisega on seotud ka süüteomenetluste uurimisega seotud muudatused. Reformitakse väärtegude toimepanemisele järgnevaid õiguslikke tagajärgi ning luuakse võimalus Euroopa Liidu õiguses sätestatud haldustrahvide kohaldamiseks väärteomenetluses, eestkätt finantssektoris ning andmekaitse valdkonnas.

Selle eelnõule tagasisidet andes leidsime, et EL haldustrahvide temaatikat on parem sisustada haldusõiguses, mitte väärteomenetlusõiguses. Sellele seisukohale oleme korduvalt Justiitsministeeriumi tähelepanu ka juhtinud, kuid tulutult.[12] Selle eelnõu osas juhtisime eelnõu koostaja tähelepanu ka kahtlusele, et pakutud sõnastus ei olnud ilmselt kooskõlas isikuandmete kaitse üldmääruse artikkel 83 lõigetega 4 ja 5. Algselt välja pakutud sõnastusest võis anda eksitavat teavet võimaliku rakendatava rahatrahvi suuruse arvutamise osas.

Samuti oleme seisukohal, et andmekaitsealaste väärtegude keerukust arvestades, tuleks pikendada nende väärtegude aegumistähtaegasid. Vähemalt seni on andmekaitsealased väärteod olnud menetluslikult (sh kohtute jaoks) keerulised, sest väärteokoosseisud on sõnastatud väga üldsõnaliselt. Suurte trahvisummadega väärteomenetlustes suureneb kindlasti ka vaidlustamine, kaasatakse esindajaid, kes püüavad menetlust venitada istungite edasilükkamise jms abil. See kõik pärsib läbiviidavat väärteomenetlust ning lõpp-kokkuvõttes ei ole trahvid tõhusad, proportsionaalsed ja heidutavad.

Küberturvalisuse seadus

Lisaks andmekaitseõiguse uuenemisega toimub paralleelselt ka uuenemine küberturvalisuse valdkonnas. Eelnõuga võetakse üle Euroopa võrgu ja infoturbe direktiiv ning soov on see jõustada samuti mais 2018. Riigisiseselt kehtestatakse turvameetmete

[12] Andmekaitse Inspektsiooni peadirektori 25.05.2017 seisukohad Justiitsministeeriumi koostatud kontseptsiooni asjus (vt 2. peatükk); samuti on seda seisukohta korratud Andmekaitse Inspektsiooni peadirektori memos Justiitsministeeriumi juhtkonnale (saadetud 29.05.2017). Mõlemad dokumendid on kättesaadavad inspektsiooni võrgulehel.

rakendamise ja küberintsidentidest teavitamise nõuded olulise teenuse ja digitaalse teenuse osutajatele. Samuti täpsustatakse riikliku järelevalveasutuse (Riigi Infosüsteemide Amet ehk RIA) ülesandeid küberturvalisuse tagamise koordineerimisel ja piiriülese koostöö korraldamisel.

Selle eelnõu osas tekitasid meile enim küsitavusi RIA-le antavate (järelevalve)meetmete kvalifitseerimine. Teadupärast toimub Eestis järelevalvemenetlus kas korrakaitseseaduse (riiklik järelevalvemenetlus) või Vabariigi Valitsuse seaduse (haldusjärelevalvemenetlus) alusel. Seega erinevad menetlustoimingud, mis on oma olemuselt seotud järelevalvete ning sellega seotud meetmega, peavad olema seotud ka vastava menetlusliigiga. Konkreetse eelnõuga jäi selgusetuks, kuidas suhestuvad selles eelnõus toodud meetmed riikliku-või haldusjärelevalve menetluse läbiviimisega – mitmed eelnõus loetletud meetmed olid justkui riikliku- või haldusjärelevalve menetluse välised „meetmed“.

Eelnõuga sooviti RIA-le anda ka õigus küsida sideettevõtjalt teatud sideseansi andmeid (sh ka IP-aadressi). Kuna sideseansi andmetele juurdepääsu osas on tehtud Euroopa Kohtu otsused Tele2 Sverige[13] ja Digital Rights Ireland[14], siis nendes kohtuotsustes on toodud nõuded, kellele ning millistel tingimustel on sideettevõtjal lubatud sideseansi andmeid väljastada. Samas tundus, et eelnõu seletuskirjas ei ole neid aspekte üldse analüüsitud.

Samuti oli meil selle eelnõu osas üldisem soovitus järelevalvetöö tõhusama korraldamise kohta – järelevalveasutuste tööjaotuse ja koostöö kohta. Küberturvalisuse alal tegutseb kaks horisontaalset ehk valdkonnaülest järelevalveasutust: põhiliselt RIA, kuid tema kõrval ka meie (isikuandmete töötlemise turvalisus ja AK-teabe kaitse). Samas on eelnõus käsitletud mitut valdkonda, kus teenuseosutajad on vertikaalse regulaatori järelevalve all. Arusaadavalt ei saa vertikaalsetele regulaatoritele panna ülesandeid, mis nõuavad spetsiifilisi küberturbealaseid võimekusi või mõjutavad laiemat võrguturvalisust – see on RIA vastutusala. Samuti ei saa teistele regulaatoritele panna ülesandeid, mille EL andmekaitseõigusõigus paneb meile. Kuid tõsiselt tuleks kaaluda valdkondlike järelevalveasutuste kaasamist küberturbealase nn baashügieeni kontrolli. Seda nii tegevusloa andmisel kui hilisemalt, kohapealsete kontrollide korral.

Rahapesu ja terrorismi rahastamise tõkestamise seaduse eelnõu

Eelnõu eesmärk oli üle võtta uus rahapesu direktiiv. Palusime eelnõus täpsustada kohustatud isiku kontaktisikute taustakontrolliks andmekogudest andmete kogumist. Eelnõu jättis selleks rahapesu andmebüroole sisustamata õiguse – mis teavet ja mis andmekogudest võib koguda. Samuti palusime eelnõus seadustada ammu kasutusel oleva rahapesu andmebüroo andmekogu asutamine koos põhimääruse kehtestamise volitusega.

Tagasisides leidsime, et kinnisvaratehingute monitoorimisel seatud hinnapiir (15 000 eurot) on ebaproportsionaalselt madal ja toob sisuliselt kaasa kõigi kinnisvaratehingute jälgimise. Samuti ei peaks kinnisvaratehingute puhul maakler ja notar dubleerivalt hoolsusmeetmeid rakendama ja selleks andmeid koguma ning säilitama.

[13] Euroopa Kohtu otsus 21.12.2016, liidetud kohtuasjad C-203/15 ja C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others.
[14] Euroopa Kohtu otsus 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Seitlinger and Others.

Täpsustamist vajas eelnõus ka kohustatud isikute teabevahetus ning kliendi rikkumise päritolu kohta täiendava teabe kogumise kohustus.

Taustakontrolli seaduse eelnõu

Eelnõus on võrreldes väljatöötamiskavatsusega küll positiivseid arenguid, kuid taustakontrolli ulatus on endiselt konkreetselt piiritlemata ning arusaamatuks jääb laiendatud taustakontrolli vajadus ja kohaldamise alused.

Seletuskirjast jääb mulje, nagu sätestaks taustakontrolli seadus selgelt taustakontrolli maksimaalse ulatuse. Tõsi, eelnõus on küll loetelu andmetest, mida taustakontrolli adressaadilt nõutakse, kuid hilisemad sätted andmekogude kasutamise ning mujalt allikatest andmete hankimise kohta muudavad selle loetelu sisutuks. Arusaamatuks jääb loetletud andmekogude (kinnistusraamat, kohtute infosüsteem ja e-toimik, abieluvararegister, laevakinnistusraamat, tervise infosüsteem jt) andmekogude seos ankeedis nõutud andmete ning usaldusvääruse mõistega. Täiesti lubamatu on taustakontrolli teostaja juurdepääs e-tervisele ning elektroonilise side nn liiklusandmete kasutusala laiendamine olukorras, kus nende säilitamist ette nägevad sätted on Euroopa Kohus tunnistanud lubamatuks.

Lisaks on ka paljud taustakontrolli ankeedis nõutud andmed arusaamatud ning seletuskiri ei sisalda põhjendusi iga andmeühiku kaupa. Näitena võib tuua ankeedis nõutud kinnituse majandusraskuste puudumise kohta. Esiteks on tegemist täiesti määratlemata mõistega ning teiseks ei ole kuidagi arusaadav, miks majanduslik seis peaks usaldusväärsuse kahtluse alla seadma.

Eelnõu kohaselt hõlmab usaldusväärsus isiku kõlbelisi, sotsiaalseid ja majanduslikke asjaolusid, mistõttu jääb arusaamatuks, kuidas on tervisekontrolli seotud isiku usaldusväärsusega. Oleme jätkuvalt seisukohal, et nõuded terviseseisundile (kui vaba eneseteostuse õiguse e põhiõiguse riive) tuleb sätestada seaduse tasandil ega saa jääda (meditsiiniteadmisteta) haldusorgani suvaks.

Kuigi eelnõus on sätestatud taustakontrolli teostaja võimalus määrata kontrolli vajaduse ja ulatuse üle, siis seletuskirjast ilmneb, et taustakontrollist loobumine või selle ulatuse piiramine on haldusorganile pigem riskantne otsus, mida peab igatpidi põhjendama ning mis võib kaasa tuua värbamise tühisuse. Põhjendamiskohustus peaks olema seatud hoopis vastupidiselt – taustakontrolli teostaja peaks põhjendama taustakontrolli vajalikkust ning selle ulatust, mitte selle vähendamist.

Eelnõuga sooviti ka piirata inimese juurdepääsu tema kohta taustakontrolli käigus kogutud andmetele, mis on juurdepääsupiiranguga. Selgitame, et alused andmesubjektile tema kohta kogutud (töödeldud) andmete väljastamisest keeldumiseks saavad tuleneda üksnes IKS §-st 20, mitte AvTSist. St inimesele ei saa keelduda tema kohta käivate andmete väljastamisest viitega mõnele AvTS § 35 punktile. Arusaamatuks jäi ka eelnõus toodud tingimus, et taustakontrolli teostanud haldusorgan võib keelduda taustakontrolli arvamuse põhjendamisest, kui taustakontrolli adressaadil ei ole õigustatud huvi tema enda kohta tehtud arvamuse põhjenduste saamise vastu. Kuidas saab inimesel selles olukorras mitte olla õigustatud huvi?

Selle eelnõuga soovitakse küll selgemaks teha taustakontrolli teostamine, kuid tuleb arvestada, et see kõik toimub inimeste privaatsust riivates. Seetõttu ongi vajalik, et sellised

sekkumised oleksid piisavalt selgelt, arusaadavalt ja põhjalikult reguleeritud, sh ei tohi jääda ruumi mitmeti tõlgendatavuse jaoks.

Töövõimetoetuse seaduse muutmise seaduse väljatöötamiskavatsus

Hetkel kehtiv töövõimetoetuse seadus (TVTS) annab isikule võimaluse otsustada, kas ta annab nõusoleku Töötukassas olevale arstiharidusega isikule juurdepääsu enda terviseandmetele tervise infosüsteemis või tuua vajalikud dokumendid paberkandjal.

Sotsiaalministeerium koostas seaduseelnõu väljatöötamiskavatsuse, millega sooviti muuta mh ka TVTS-i. Selle raames soovib Töötukassa muuta ka TVTS-st nii, et isikult eelnevalt kirjeldatud nõusolekut terviseandmetele tervise infosüsteemis ei võeta – Töötukassa leidis, et see on õigustatud TVTS § 5 lõikega 2: „töövõime hindamisel võetakse arvesse isiku terviseseisundit ning sellest tulenevaid tegutsemise ja osalemise piiranguid, nende prognoosi ja eeldatavat kestust.“

Siin tuleb eristada kahte asjaolu: TVTS § 5 lõige 2 määratleb ära, mida võetakse arvesse töövõime hindamisel, kuid see ei määratle ära, kuidas terviseandmetele juurdepääs saadakse – seda reguleerib TVTS § 6 lõige 1 ehk toimub nõusoleku alusel. Saame nõustuda sellega. et töövõimet on võimalik ennekõike isiku terviseandmete põhjal hinnata, kuid see ei tähenda, et selleks peaks koheselt andma sisuliselt otsejuurdepääsu tervise infosüsteemile. Isikule peaks andma võimaluse ise otsustada, kumba varianti ta soovib – kas annab nõusoleku või toob ise oma tervisealased dokumendid töövõime hindaja juurde.

TVTS võeti vastu 19.11.2014 ning jõustus 01.07.2016, sh samal ajal jõustus ka praeguse sõnastusega TVTS § 6. Seega oli Töötukassale juba varakult teada, kuidas toimub juurdepääs isiku terviseandmetele. Kehtiva seaduse kohaselt peab inimeselt võtma nõusoleku, kuid infotehnoloogilise probleemi tõttu ei ole isikul võimalik ise otsustada, kas ta üldse annaks seda nõusolekut või mitte. Asjaolu, et infotehnoloogiliselt ei ole süsteem välja arendatud, ei saa olla ainuke ettekääne seadusandluse muutmiseks. Sel juhul oleks pidanud juba infosüsteemi loomise protsessis sedasorti probleemid ära lahendama. Samuti ei olnud selge, kuidas tagatakse isikuandmete töötlemisel minimaalsuse põhimõtte järgimine ehk juurdepääs saadakse ainult nendele terviseandmetele, mis on vajalikud töövõime hindamise otsustamiseks – kõik terviseandmed ei ole ilmselt vajalikud, et hinnata isiku töövõimet. Samuti ei olnud selles osas tehtud ka põhjalikku andmekaitselist mõjuhinnangut.

Haldusmenetluse seaduse muutmise eelnõu

Justiitsministeerium esitas kooskõlastamisele kaua oodatud haldusmenetluse seaduse muudatused, millega reformitakse haldusmenetluse dokumentide saatmise reegleid.

Haldusmenetluses seaduses, erinevalt ülejäänud menetlusseadustikest, on jäänukina sees elektroonilise suhtluse algusaegadest pärinev nõue, et isikule e-postiga millegi saatmiseks peab olema isiku eelnev nõusolek. Eelnõu jäi selles osas siiski poolele teele pidama ning nõusoleku nõuet ei kaotanud, vaid üksnes leevendas osaliselt.

Ei ole ühtegi mõistlikku põhjust, miks haldusmenetluses peaks sellise arhailise eelneva nõusoleku nõude erinevalt ühiskonna kogu ülejäänud suhtlusmallist alles jätma. Seda enam, et kättetoimetatuks loetakse dokument jätkuvalt üksnes pärast inimese aktiivset tegevust –

kas kättesaamiskinnituse saatmist või dokumendi asukohaks olevasse elektroonilisse keskkonda sisse logimist. Sestap tegime ettepaneku elektrooniliseks saatmiseks eelneva nõusoleku nõue seadusest täielikult välja jätta.

Lisaks leidsime, et seadus peaks selgelt eelistama elektroonilist suhtlust ning suhtlus riigiga peaks käima inimese ametlike kontaktandmete (ametlik e-post ja rahvastikuregistrisse kantud kontaktandmed) kaudu. Põhjendatud juhul peab muidugi olema inimesel võimalik suhelda ka teise kontaktandmete kaudu, kuid see ei peaks olema reegel, et iga asutus peab inimese kohta dubleerivalt oma kontaktandmebaasi.

Makseasutuste ja e-raha asutuste seaduse muutmine

Selles osas, milles isikuandmeid töödeldakse makseteenuse osutamiseks (tsiviilõigusliku lepingulise suhte raames lepingu eesmärgi saavutamiseks) ei või kliendilt küsida nõusolekut isikuandmete töötlemiseks. Nõusoleku küsimine olukorras, kus andmeid tuleb lepingu täitmiseks möödapääsmatult töödelda, on eksitav, sest nõusoleku peaks seaduse järgi saama igal ajal tagasi võtta.

Massprofileerilisest riigi andmekogudes

Juba eelmises Andmekaitse Inspektsiooni ettekandes kirjutasime probleemist teemal riigi andmekogudes isikuandmete massanalüüs. Sellest ajendatuna esitasime ka oma murekohad Justiitsministeeriumile.

Erinevate andmekogude andmete ühendamise ja massanalüüsi soovi on meile tutvustanud vähemalt Maksu- ja Tolliamet, Politsei- ja Piirivalveamet ning Maanteeamet. Kõik need asutused on oma sellekohase tegevusega riiklikku järelevalvet teostavad korrakaitseorganid, kes soovivad erinevate andmekogude isikustatud andmete kombineerimise ja massanalüüsi kaudu koostada ohuprognoose, riskianalüüse ning tuvastada õigusrikkujad (näiteks vara võõrandamisest saadud tulu deklareerimata jätmine, ebakvaliteetne tehnoülevaatus või liiklusõpetus, kõikvõimalike kuritegude ja kurjategijate avastamine ning tabamine).

Tõsi, ka EL ise nõuab terrorismi tõkestamise eesmärgil täiendavaid massandmetöötlusi (nt broneeringuinfo direktiiv), kuid reeglina on sellised töötlused piiratud konkreetsete tingimustega (töötlemine on lubatud üksnes raskete kuritegude avastamiseks ja menetlemiseks, andmete esmane massanalüüs toimub väga lühikese aja, nt 24 tunni jooksul, edasisele säilitamisele kuuluvad üksnes positiivsed leiud jms). Ka Euroopa Kohus on elektroonilise side andmete teemal tehtud kahes lahendis (viidatud ülalpool) tänaseks selgelt nõudnud, et igasugune taoline massandmetöötlus peab piirduma rangelt vajalikuga ning olema väga piiratud.

Seega lausjälgimist võib teatud piiratud juhtudel siiski teha, kuid selle raamid peavad olema selged ja proportsionaalsed. Niihästi korrakaitse-, väärteo- kui kriminaalõigus, samuti eriseadused lubavad asutustel teha inimeste kohta üksikpäringuid. Seda niihästi juba toimunu uurimiseks kui ka ennetuseks. Kuid olemasolevate, üksikpäringuid silmas pidades sõnastatud, menetlussätete kasutamine kogu elanikkonda hõlmavaks massandmeanalüüsiks, olgu seda siis ühe või mitme andmekogu andmete baasil, ei ole vastuvõetav.

Korrakaitseseadus (KorS) räägib andmekogude kasutamisest üksnes kaude – KoRS § 5 lg 7 kohaselt on ohu ennetamine muu hulgas teabe kogumine, vahetamine ja analüüs; KoRS § 30 lõike 5 kohaselt ei või isikut küsitleda ning temalt dokumente nõuda, kui teave on võimalik saada andmekogust. KorS § 5 lõige 7 ei ole siiski käsitletav üldise õigusliku alusena kõigi andmekogude kõikvõimalikuks järelevalve otstarbeliseks massandmetöötluseks - sellekohane norm on korrakaitseseadusest lihtsalt puudu.

Andmete kogumine korrakaitseliseks (sh „maksuõigusrikkumiste riskihindamise“) massanalüüsiks ning andmekogude kombineeritud massanalüüs vajab täpsemaid tingimusi, kuid sellekohased sätted ei tohiks tekkida iga asutuse parema äranägemise järgi igaüks omas sõnastuses ning arusaamatus seoses korrakaitseseadusega. Eelmises aastaettekandes tõimegi välja minimaalse loetelu küsimustest, millele selline regulatsioon peaks vastuse andma.[15]

Sealhulgas vajab ülevaatamist sideandmete laussäilitamine (vastuolus Euroopa Liidu Kohtu otsustega) ning paradoksaalne olukord elektroonilise side sõnumi metaandmete ja sisu kasutamise võimalustes.[16] Tähelepanu tuleks pöörata ka EL üleselt ette nähtud andmete kogumise siseriiklikult kehtestatud tingimustele (eeskätt samade andmete Eesti siseriiklikus andmekogus säilitamise tihti ülipikale või alatisele tähtajale ja avaralt sõnastatud kasutamise eesmärgile, nt „avaliku korra kaitseks“).[17] Need aspektid on senini relevantsed ka praegu kui ka tulevikus isikuandmete töötlemisega seotud muudatuste korral.

E-riigi harta

E-riigi harta koostati Riigikontroll aastal 2008 auditi „Avaliku teenuse kvaliteet infoühiskonnas“ järelmina. Hartas on kirjas ka mõõdetavad kriteeriumid, millele peaksid vastama riigi pakutavad e-teenused. Riigikontroll ja Õiguskantsler koostasid esialgse e-harta Hollandi e-kodaniku harta eeskujul ning nüüd on soov hartat uuendada.

Selle harta juhtisime tähelepanu, et kui inimeste nõustamisel soovitakse kasutada videokonverentsi, siis tuleb ka läbi mõelda, kas ning milliste teenuste jaoks on vajalik isiku tuvastamine – nt kui nõustamine on sellist laadi, kus antakse üldisi selgitusi mingi valdkonna osas, siis ei ole ilmtingimata vajalik tuvastada isikut. Samas kui mingit teenust soovitakse osutada videokonverentsi abil ning on vajalik tuvastada teenuse saaja isik, siis võiks e-hartas olla ka sellekohased selgitused/täpsustused/nõuded, mida tuleb arvestada, kui tekib vajadus teenust sel moel osutada. Proaktiivsete teenuste osas oli harta tekst sõnastatud justkui asutused vahetavad omavahel informatsiooni, et pakkuda inimesele teenuseid, sh pakutakse neid teenuseid ka enda algatusel. Harta sooviks on, et asutused osutaksid teenuseid isiku eeldatava tahte kohaselt riigi andmekogude andmete alusel. Juhime tähelepanu, et sellise tegevuse osas peab alati arvestama ka põhiseadusega.

Põhiseaduse §-s 26 on ära määratletud, millal riik (st riigiasutus, kohalik omavalitsus ja nende ametiisikud) saab sekkuda füüsilise isiku eraellu ning iga asutuse peab seda oma proaktiivse teenuse väljatöötamisel arvestama. Proaktiivne teenus ei saa tekkida ainult

[15] Andmekaitse Inspektsiooni 2016. a aastaettekande õigusaktide eelnõude peatükis.
[16] Täpsemalt selgitatud Andmekaitse Inspektsiooni 2016 a aastaettekande õigusaktide eelnõude peatükis lk 62, „Elektrooniline side ja liiklusandmed“.
[17] Andmekaitse Inspektsiooni peadirektori 09.01.2017 kiri 2.2.-8/16/1604 Siseministeeriumile ja Politsei- ja Piirivalveametile.

andmekogudest jt andmeallikatest kokkupandava teabe tulemusena, kuna selliseks isikuandmete töötluseks (andmete kogumiseks, välja sõelumiseks ehk profileerimiseks ning isiku teavitamiseks pakutavast teenusest) peab olema õiguslik alus, mis omakorda peab olema kooskõlas põhiseadusega. Seetõttu ei tohi jääda ka sellist muljet, et riigil on alati võimalik isikuandmeid töödelda, et tulevikus mingit proaktiivset teenust isikule osutada.

Vabariigi Valitsuse ning ministrite määrused

Vabariigi Valitsuse ning ministrite määruste muudatused olid ennekõike seotud andmekogude põhimääruste muutmisega. Nendeks andmekogudeks olid Schengegi infosüsteemi riiklik register, eeltäidetud viisataotluste andmekogu, viisaregister, e-toll, vangistusregister, päästeinfosüsteem, hädaabiteadete infosüsteem, raseduse infosüsteem, sotsiaalkaitse infosüsteem ning sotsiaalteenuste ja –toetuste andmeregister.

Olulisemad märkused

Eelnõude ülevaatamistest võib välja tuua põhilisemate puudustena/märkustena:

- andmekoosseisude ammendav määratlemine – need pole põhimääruses ja/või selle lisas piisavalt konkreetselt ja selgelt määratletud;
- varasemalt koguti teatud tüüpi andmeid, kuid muudatuste tulemusena enam neid andmeid ei koguta – samas eelnõust ei selgu, mis nende andmetega edasi tehakse (kustutatakse ära, viiakse umbisikustatud kujule või arhiivi vms);
- andmekogude vaheline teabevahetus ei toimu üle X-tee (põhimääruses on nt märgitud, et „muu elektrooniline kanal“) - AvTS § 43^9 lõike 5 kohaselt andmevahetus riigi infosüsteemi kuuluvate andmekogudega ja riigi infosüsteemi kuuluvate andmekogude vahel toimub läbi riigi infosüsteemi andmevahetuskihi ehk X-tee;
- säilitamistähtajad nii andmete kui ka andmekogu logide osas ei ole kehtestatud või puudub piisavalt veenev põhjendus selle säilitamistähtaja pikkuse osas;
- andmekogule ja/või selle alamandmekogudele juurdepääsude andmine – isikuandmete töötlemise põhimõtete ning nendega seotud nõuete eesmärkideks on, et andmete töötlemine oleks võimalikult läbipaistev ning eesmärgipärane, mistõttu tasub andmekogule juurdepääsud reguleerida kas seaduse (ennekõike tundlikumate andmete osas – nt terviseandmed) või põhimäärus tasandil; samuti tuleb läbi mõelda, kas see juurdepääs on püsijuurdepääs või nö päringupõhine;
- andmete allikate määratlemine - see nõue tuleneb sisuliselt AvTS § 43^5 lõikest 1, mille kohaselt on vajalik ära määratleda andmeandjad; samuti tagab see ka parema andmetöötluse läbipaistvuse, kui nt on ära määratletud, millistest andmekogudest ning milliseid andmeid saadakse; see omakorda aitab selgeks teha, millised andmed on mõne andmekogu põhiandmed;
- soovitus lisada andmekogudele andmejälgija teenus – selle teenuse kasutamine muudab läbipaistvamaks ning selgemaks, mida andmesubjektide andmetega tehakse, sh kes neid andmeid töötleb;
- andmekogu vastutav töötleja teostaks enda andmekogu üle järelevalvet – kuna andmekogu vastutav töötleja vastutab ennekõike enda andmekogus toimuv andmetöötluse eest, siis on vajalik teha ka järelevalvet selle andmekogus tehtud toimingute osas ning andmekogu andmete väärkasutuse korral (nt tehes uudishimust päringuid) teavitada sellest ka Andmekaitse Inspektsiooni;

- andmekogule juurdepääsu andmine õppe eesmärgil[18] – andmekogudesse kantud andmeid on võimalik kasutada ennekõike kooskõlas IKS § 10 lõikega 2 ehk avaliku ülesande täitmiseks; kui õppurile soovitakse anda andmekogu andmetele juurdepääs seetõttu, et nt justiitsvaldkonna või sisekaitse valdkonna õppejõud on ette näinud, et ülesande täitmiseks võib/peaks kasutama mõnda andmekogu, siis selline tegevus ei ole kohe kindlasti seotud selle õppuri (kes võib samal ajal olla praktikal vms) tööülesannete täitmisega; selle asemel tuleks luua vastavad õppekeskkonnad, kui soovitakse õpetada selle andmekogu kasutamist.

Soovitused ja märkused õigusloome valdkonna osas

Eeltoodud teemade pinnalt esitame mõningad soovitused ja märkused õigusloome valdkonna osas, millega tuleb meie järelevalvepädevusega seotud valdkondades edaspidiselt arvestada või ära teha:

- isikuandmete kaitse üldmääruse kui ka õiguskaitseasutuste direktiivi kohaselt peab riik konsulteerima Andmekaitse Inspektsiooniga, kui koostamisel on Riigikogus vastu võetava õigusliku meetme ettepanek või sellisel õiguslikul meetmel põhinev reguleeriv meede, mis seondub isikuandmete töötlemisega;
- kui on soov teostada uusi andmetöötlustoiminguid peale isikuandmete kaitse üldmääruse jõustumist (st luua vastav õiguslik alus andmete töötlemiseks), siis tuleks sellekohaste riskide analüüs (andmekaitseline mõjuhinnang) ära teha vastava õigusakti eelnõus; selle kõige eelduseks on muidugi, et selline andmetöötlus on üldse kohane põhiseaduse § 26 kohaselt ehk ka eelnõus on seda aspekti analüüsitud – ennekõike eriliigiliste isikuandmete ja teiste tundlike isikuandmetega (nt teave sotsiaalabi maksmise kohta; side- või finantsandmed) seotud andmetöötluste korral;
- avaandmete mõjuhinnang – alates 2016. aasta jaanuarist on AvTS-s teabevaldajatel kohustus avaldada enda juures kogutud avalikud andmed, mis on mõeldud avalikuks taaskasutamiseks (avaandmed) ning selle tegemiseks on vajalik teha eelnev avaandmete mõjuhinnang; ka selle analüüsi soovitame ära teha õigusakti eelnõu seletuskirja juures – nt tehes seda andmekogu põhimääruses muutmise korral ning märkida andmekogu põhimääruses kohe eraldi sättena, mis teave on avaandmed AvTS-i mõistes;
- soovitame ka edaspidiselt andmekogude põhimääruste koostamisel või nende muutmisel võimalikult selgelt ning lihtsalt ära kirjeldada, milliseid andmetöötlustoiminguid konkreetses andmekogus tehakse, sh ka andmekogu korraldusliku poole pealt nt ära reguleerida andmete koosseisud, andmeandjad ehk andmete allikad, kes andmetele juurdepääsu saavad (asutused vms), andmete säilitamistähtajad ning muud andmekogu pidamisega seotud korralduslikud küsimused[19]; sellekohane selge teave aitab nii ka andmesubjekti kui ka andmekogu vastutavat- ja volitatud töötlejat nende õiguste ja kohustuste täitmisel;
- sideandmete korraldus – arvestades eelpool viidatud Euroopa Kohtu otsuseid, tuleb Eesti õiguskorras võtta seisukoht, kas ning kuidas muudetakse elektroonilise side seaduses reguleeritud sideandmete säilitamist ning nende andmete töötlemist, sh ennekõike kes ning millistel tingimustel nendele andmetele juurdepääsu saab.

[18] Märkus: siin ei ole mõeldud juurdepääsude andmist teadusuuringute kontekstis – sel juhul on juurdepääsukorraldus teistel alustel.
[19] Andmekogu põhimäärusega seotud nõuded on toodud AvTS § 43[5] lõikes 1 ning täpsemalt oleme seda aspekti kirjeldanud ka andmekogude juhendi peatükis 3.2.

RAHVUSVAHELISED TÖÖRÜHMAD

Euroopa andmekaitseasutuste töörühm

Maarja Kirss, koostöödirektor

Andmekaitse Inspektsioon on Euroopa andmekaitseasutuste töörühma liige olnud 2004. aastast alates (enne seda osaleti vaatleja rollis). Euroopa andmekaitseasutuste töögrupp, mida kutsutakse ka Artikkel 29 töögrupiks, on loodud andmekaitsedirektiivis 95/46/EÜ artikli 29 alusel. Töörühma liikmeskond koosneb Euroopa andmekaitseasutuste juhtidest (või nende määratud asendusliikmetest), Euroopa andmekaitse inspektorist ning Euroopa Komisjoni esindajatest (kes täidavad ka sekretariaadi kohustusi). Lisaks on sõnaõigus ka Euroopa Majanduspiirkonda kuuluvatel riikidel. Töörühma töökorraldus näeb ette alatöörühmade tegutsemist ning viis korda aastas toimuvat põhitöörühma kohtumist.

Seoses andmekaitsereformiga on ka töörühmas murrangulised aastad – enamus töömahust on pühendatud andmekaitsemäärusele, selle artiklite ning mõistete tõlgendamisele. Samuti kujuneb andmekaitsetöörühm 2018. aasta mais ümber Euroopa Andmekaitsenõukoguks. Töörühma juhendiloome valmistatakse ette alarühmades ning lõplikult kiidetakse juhendid heaks põhitöörühmas.

Esialgselt vastuvõetud juhendid pannakse avalikule arutelule, mille käigus on kõigil võimalus arvamust esitada. Pärast avaliku konsultatsiooni lõppemist ning kommnetaaridega arvestamist, kinnitatakse juhend töörühmas lõplikult. Kuna andmekaitsereform toob palju uut ka andmekaitseasutuste töökorraldusele (nt seoses ühtse *one-stop-shop* põhimõttega), siis on töörühm koostanud ka n-ö sisemisi juhiseid, mis puudutavad andmekaitseasutuste edaspidist töökorraldust. Sellised juhendid läbivad enne lõpliku vastuvõtmist ka praktilise kaasuste testimise.

Andmekaitse Inspektsioon osaleb aktiivselt nii põhitöörühma kui ka üheksa alarühma töös – privaatsuse tuleviku, tehnoloogia, koostöö, võtmesätete, menetlustöö, rahanduse, e-riigi, piiriüleste edastamiste ning piiride, reisijate ja korrakaitse alarühmades. Alljärgnevalt on ülevaade tegevusest olulisemate alarühmade kaupa.

Tehnoloogia alarühm

Alarühma eesmärk on toetada Euroopa andmekaitseasutuste töörühma tööd. Möödunud aastal toimus viis alarühma kohtumist. Põhitähelepanu oli andmekaitse üldmääruse alasel juhendiloomel. Valmisid juhendid teemadel nagu andmete ülekantavus ja andmekaitsealane mõjuhinnang. 2018. aasta esimesel poolel lisanduvad rikkumisteadete ning sertifitseerimise ja akrediteerimise juhendid. Lisaks avaldas alarühm mahuka arvamuse Euroopa Komisjoni määrusettepanekule (e-privaatsusmäärus) andmekaitse erinõuete kohaldamiseks elektroonilise side valdkonnas. Uuendati arvamust, mis käsitleb isikuandmete töötlemist töökeskkonnas.

Võtmesätete alarühm

Võtmesätete alagrupp koostas 2016. aastal suunised andmekaitseametnike kohta ning suunised, kuidas määrata juhtivat andmekaitseasutust. Need võeti esmakordselt vastu detsembris 2016. Peale seda järgnes avalik konsultatsiooniperiood, mille jooksul sai avalikkus anda oma kommentaarid, sisendid ja probleemküsimused nende juhendite kohta. Saadud sisendi pinnalt vaadati suunised uuesti üle ning lõplikult kinnitati mõlemad suunised aprillis 2017. Andmekaitseametnike suuniste lõplik versioon on saadaval ka inspektsiooni kodulehel. Eelmisel aastal oli alatöögrupi tööplaanis kolme kolm juhendmaterjali koostamine:

- juhend automaatotsuste ja profileerimise kohta – seotud andmekaitse üldmääruse art 4 punktiga 4 ning artikliga 22,
- juhend nõusoleku kohta – seotud ennekõike andmekaitse üldmääruse art 4 p 11,
- juhend andmetöötluse läbipaistvuse kohta – seotud ennekõike andmekaitse üldmääruse põhjenduspunktiga 39, art 5 (1) punktiga a ning artiklitega 12-14.

Juhend automaatotsuste ja profileerimise kohta võeti vastu oktoobris 2017 ning juhendid nõusoleku ja läbipaistvuse kohta võeti vastu novembris 2017 – peale seda järgnesid kõigi juhendite osas avalikud konsultatsioonid. Juhend automaatotsuste ja profileerimise kohta võeti vastu selle aasta veebruaris. Teiste juhendite osas tehakse tööd edasi.

Koostöö alarühm

Koostöö alarühma peamiseks tegevussuunaks on just eelnevalt mainitud n-ö sisemiste juhendmaterjalide koostamine. Andmekaitsereformiks ettevalmistamisel valmisid esimeste juhenditena juhendid üldmääruse artiklite 60, 61 ja 62 kohta (ehk siis koostöö, vastastikune abi ning ühisoperatsioonide toimumine *one-stop-shop* põhimõtetel) ning artikli 56 (juhtiva järelevalveasutuse määramine ja pädevus).

One-stop-shop juhendite pakett läbis enne lõplikku vastuvõttu menetluse alarühma testimise, millega püüti maksimaalselt välja selgitada praktilisi probleeme, mis võivad eelnimetatud juhendite rakendamisel tekkida. Lõpptulemusena valmis praktilised abivahendid andmekaitseasutuste töötajatele ülepiiriliste kaasuste menetlemisel. Alarühma töö ülepiiriliste menetluste osas endiselt jätkub, kuna lahendamist vajavad nii mitmedki küsimused andmekaitsenõukogus vaidluste lahendamiste osas, samuti peaks enne 2018. aasta maikuud valmima ühtne infosüsteem, mis hõlbustab ülepiiriliste juhtumite menetlemist.

Juhtiva järelevalveasutuste pädevus ja määramise juhend kiideti lõplikult heaks aprillis 2017 ning teemajätkuna on koostamisel andmetöötlejatele vabatahtlikult täidetav ankeet juhtiva järelevalve asutuse kindlaksmääramiseks. Ankeet peaks valmima 2018. aasta jooksul.

Enim vaidlusi tekitas alarühmas haldustrahvide juhendi koostamine. Peamine vaidluskoht oli trahvide määramise vajalikkus kui selline, kuna on liikmesriike, kus trahvimine on igapäevane karistusmeede ning on liikmesriike (nagu Eesti), kus andmekaitsealaste rikkumiste eest trahvimine on äärmuslik ja harva kasutatav meede. Ühtse seisukoha leidmine osutus etteennustatavalt keeruliseks ülesandeks. Lõpptulemuseks oli juhendi tekst nii neutraalne, kui antud olukorras oli võimalik – trahvimist esmase meetmena juhend ette ei näe. Kuna tegemist on siiski järjepideva teemaga otsustati menetluse alarühma juurde

luua alatine trahvide töögrupp, mis tegeleb järjepidevalt antud teema monitoorimisega ka peale üldmääruse jõustumist.

Menetlustöö alarühm ja trahvide rakkerühm

Menetlustöö alarühmas arutati 2017. a eelkõige Euroopa andmekaitseasutuste piiriülest koostööd puudutavat ning testiti koostöö alarühma koostatud juhiseid piiriülese menetluse kohta. 2017. a teises pooles loodi alarühma juurde eraldi trahvide rakkerühm, mille ülesandeks on leida võimalusi ja juhiseid, et ühtlustada liikmesriikide trahvimise praktikat.

Privaatsuse tuleviku alarühm

Privaatsuse tuleviku alarühm üldiselt ise juhendeid ei koosta. Võib öelda, et tegemist on pigem n-ö puhvriga alarühmade ning põhitöörühma vahel, kus arutatakse alarühmades tekkinud küsimusi enne põhitöörühma arutelusid. Lisaks jooksvate küsimuste arutamisele tegeles alarühm tulevase andmekaitsenõukogu töökorralduslike küsimustega, eelkõige protseduurireeglite koostamisega. Nimelt hakkab Euroopa andmekaitse inspektori kontor pakkuma tulevasele andmekaitse nõukogule sekretariaadi teenust.

Inspektsioon on alati olnud aktiivne osaline töörühma töökorralduslikes aruteludes, et tagada toimivad töötingimused. Näiteks on inspektsioon põhitöörühmas ning privaatsuse tuleviku alarühmas juhtinud korduvalt tähelepanu praktilistele probleemidele – töörühmas arutelule tulevate materjalide edastamine ning piisav aeg teemade ettevalmistamiseks. Tegemist on eelkõige väiksemate andmekaitseasutuste murega, kus personali on vähe ning kus tekib oht, et ettevalmistamine koosolekuks on raskendatud, kuna materjalid saabuvad liiga väikese ajavaruga. Teine murekoht on töögrupi juhendite tõlkimine. Tõlkekiirused ja mahud on aastaid olnud vaidlusteemaks, kuid uue andmekaitsenõukogu tegevusega kaasneb veel rohkem materjale (lisaks juhenditele ka näiteks vaidluste lahendamise käigus koostatud otsused jms), mis tuleks kindlasti tõlkida kõikidesse liikmesriikide keeltesse, kuna see mõjutab otseselt asutuste ja andmetöötlejate tegevust.

Telekommunikatsioonialane andmekaitse töörühm

Urmo Parm, tehnoloogiadirektor

Telekommunikatsioonialane rahvusvaheline andmekaitse töörühm (IWGDPT) tegutseb isikuandmete töötlemise põhimõtete analüüsi ja selgitustööga telekommunikatsiooni ning tehnoloogia valdkonnas. Aastas korraldatakse kaks töökohtumist.

2017. aasta kevadiselt töörühma kohtumiselt märgiksin vastu võetud dokumenti Working Paper on E-Learning Platforms. Dokument kirjeldab andmekaitsealaseid põhimõtteid, millega e-õppe platvormide kasutajad peavad arvestama. Õppeasutused on üha enam hakanud kasutama veebipõhiseid õpikeskkondi. Õpilased logivad nendesse sisse ja lahendavad erinevaid ülesandeid ja loevad tekste. Õpiplatvormid logivad kõik tegevused, sh õiged-valed vastused, ülesannete sooritamise aja jms. Võimalik on saada detailne ülevaade ühe või teise õpilase võimekusest. Põhilised murekohad on paljuski samad, mis paljastusid

inspektsiooni e-õppe keskkondade seires. Samuti juhitakse ka andmekaitseasutuste tähelepanu vajadusele õppeasutuste teadlikkuse suurendamiseks.

Sügisel toimunud töörühma kohtumisel töötasime eelkõige kahe kaaluka dokumendiga, mille vastuvõtmine ja avaldamine kavandatakse 2018. aasta esimesse poolde:

1. *Firmware updates for IoT devices*
   Püsivara (*firmware*) uuenduste temaatika asjade interneti (*Internet of Things ehk IoT*) seadmetes on ülimalt asjakohane, kuna tavakasutajal puudub siin reeglina võimalus ise sekkuda ja seetõttu on vastutus eelkõige vidinate tootjatel. Dokument selgitab, mis on püsivara ning miks seda peab uuendama. Antakse soovitusi õigusloome ning regulaatorasutustele. Seadmete tootjatele ning kasutajatele.
2. *Working Paper on Privacy and Data Protection Issues with Regard to Registrant data and the WHOIS Directory at ICANN*
   Rahvusvaheline andmekaitsekogukond tunneb muret, et ICANN'i (*Internet Corporation for Assigned Names and Numbers*) lepingutingimused domeeniregistrite pidajatega ei võimalda piirata ligipääsu registreerija isikuandmetele ja nende avaldamisele WHOIS (*who is responsible for this domain name*) registrites. Sellest tulenevalt on töörühm Kanada Toronto Ülikooli eestvedamisel koostamas dokumenti mahukate soovitustega.

Rahvusvaheline järelevalvealane koostöö

Kristjan Küti, vaneminspektor

Schengeni konventsiooni andmekaitse järelevalve

Teise põlvkonna Schengeni infosüsteem (SIS II) on andmebaas, mis sisaldab informatsiooni tagaotsitavate või kadunud isikute kohta, salajase jälgimise all olevate isikute kohta, kolmandate riikide kodanike kohta, kellele on Schengeni territooriumile sisenemine keelatud, samuti andmeid varastatud või kadunud sõidukite, kadunud dokumentide, sõidukite registreerimistunnistuste ja numbrimärkide kohta.

Andmekaitse inspektsioon on siseriiklik järelevalveasutus, kes valvab, et isikuandmete töötlemine SIS II-s ei rikuks isiku õigusi. Järelevalvetegevuse koordineerimiseks kohtuvad siseriiklikud andmekaitseasutused ja EDPS mitu korda aastas (SIS II järelevalve koordineerimisgrupp).

Viisainfosüsteemiga seotud järelevalve

Viisainfosüsteem (VIS) on andmebaas, mille pidamise eesmärgiks on parandada ühise viisapoliitika rakendamist, konsulaarkoostööd ning viisasid väljastavate keskasutuste vahelist konsulteerimist, lihtsustades taotlusi ja nende suhtes tehtud otsuseid käsitleva teabe vahetamist liikmesriikide vahel. VIS sisaldab ka lühiajalisi Schengeni viisasid.

Andmekaitse inspektsioon kontrollib andmete töötlemist siseriiklike ametiasutuste poolt ja nende andmete edastamist keskküksusele. VIS järelevalve koordineerimisgrupp vastutab

ühiste järelevalvetegevuste eest, et tagada VIS-i määruse ja viisaeeskirja andmekaitse sätete täitmine ning annab soovitusi liikmesriikidele ja kesküksusele.

Tollikonventsiooni andmekaitse järelevalve

Infotehnoloogia tollialase kasutamise konventsiooni eesmärgiks on liikmesriikide tolliametite vahelise koostöö tugevdamine menetluste kehtestamise abil, mille kohaselt võivad tolliametid tegutseda ühiselt ja vahetada salakaubaveoga seotud isikuandmeid ning muid andmeid nende andmete haldamise ja edastamise uut tehnoloogiat kasutades. Selle ülesande täitmiseks loodi liikmesriikide tolliametite tollialaseks kasutamiseks ühine automatiseeritud infosüsteem ehk tolliinfosüsteem (CIS), mille eesmärgiks on infotehnoloogia tollialase kasutamise konventsiooni sätete kohaselt olla abiks siseriiklike õigusaktide rikkumise ärahoidmisel, uurimisel ja karistamisel, suurendades kiirema teabelevi abil liikmesriikide tolliametite koostöö- ja kontrollimenetluste tõhusust.

Osaleme tolliinfosüsteemi ühise järelevalveasutuse töös. See infotehnoloogia tollialane ühine järelevalveasutus on pädev järgima tolliinfosüsteemi tööd, läbi vaatama selle tööga seotud rakendamis- või tõlgendamisküsimusi, uurima probleeme, mis tekivad liikmesriikide siseriiklikel järelevalveasutustel sõltumatu järelevalve teostamisel või üksikisikutel süsteemile juurdepääsu õiguse kasutamisel, samuti koostama ettepanekuid probleemide ühiseks lahendamiseks.

Siseriiklikult kontrollime, et CIS-is hoitavate andmete töötlus ja kasutamine ei rikuks kellegi õigusi. Sellega seonduvalt on loodud ka eraldi töörühm (*Customs SCG*), mis koordineerib sellega seotud järelevalvetööd.

Euroopa sõrmejälgede andmebaasi (Eurodac) järelevalve

Euroopa varjupaigataotlejate tuvastamise infosüsteem Eurodac on loodud varjupaigataotlejate ja ebaseaduslike immigrantide sõrmejälgede võrdlemiseks ning on kasutusel kõigis Euroopa Liidu liikmesriikides ja seotud kolmandates riikides.

Andmekaitse inspektsioon kontrollib andmete töötlemist siseriiklike ametiasutuste poolt ja nende andmete edastamist kesküksusele. Eurodaci järelevalve koordineerimisgrupp vastutab ühiste järelevalvetegevuste eest, et tagada Eurodaci määruse andmekaitse sätete täitmine ning annab soovitusi liikmesriikidele ja kesküksusele.

Europoli koostöönõukogu

1. mail 2017 jõustus uus Europoli määrus, millega EDPS võttis Europoli ühiselt järelvalveasutuselt üle Europoli järelevalve. EDPS kohustused on jälgida ja tagada Europoli andmekaitse sätete kohaldamine Europoli poolt ning Europoli ja liikmesriikide nõustamine isikuandmete töötlemisega seotud küsimustes.

Riikide andmekaitseasutustel on oluline osa Europoli koostöönõukogus. Koostöönõukogul on nõuandev funktsioon ja ta võib välja anda arvamusi, suuniseid, soovitusi ja parimaid tavasid.

Ülemaailmne eraelu kaitse võrgustik (GPEN)

Raavo Palu, õigusdirektor

Interneti rehitsemise seire 2017 (*GPEN Sweep*)

Andmekaitse Inspektsiooni viis koostöös Üleilmse Andmekaitseasutuste Võrgustikuga GPEN (*Global Privacy Enforcement Network*) läbi seire teemal, kuidas inimestel on kontroll oma isikuandmete üle. Tegemist on viienda privaatusõigusega seotud seirega, mis on GPEN-i eestvedamisel läbi viidud.

Seire viidi läbi üle maailma mitmetes sektorites ja tegevusvaldkondades. Andmekaitse Inspektsioon keskendus selle aasta seires Eestis asuvate e-poodidele, mis pakuvad inimestele ehitusalaseid kaupasid (e-ehituspood). Valimis oli 21 e-ehituspoodi. Seire läbiviimisel kontrolliti, kuidas ning millist inimestele antakse teavet nende isikuandmete töötlemisest – nt kellele võidakse tema isikuandmeid avaldada või edastada. Selleks uuriti e-ehituspoe kodulehel olevat teavet, et saada aimu, kuidas toimub konkreetses e-ehituspoes isikuandmete kogumine, mida nendega edasi tehakse ning kuivõrd läbipaistev ja turvaline on e-ehituspoe tegevus isikuandmete kaitse vaatest.

Eestis kehtiv isikuandmete kaitse seadus on oma loomult tehnoloogianeutraalne, kuna ta ei sisusta konkreetselt, milliseid konkreetseid meetmeid tuleb rakendada isikuandmete kaitseks. Ka mais jõustuv andmekaitse üldmäärus toetab tehnoloogianeutraalsust. Seetõttu peab ka ajas muutuv isikuandmete töötlemine arvestama ohtude ja nende ohtude maandamiseks kasutatavate tehnoloogiate arenguga.

Üheks elementaarseimaks sisuks on läbipaistvuse tagamine. Inimestel peab olema selge ja arusaadav ülevaade, mis tema isikuandmetega tehakse – ennekõike, mida tema kohta kogutakse, kellele võidakse tema isikuandmeid edastada või avaldada, kuivõrd turvaliselt tema isikuandmeid töödeldakse jne. Selles osas on abiks piisavalt selge ja konkreetse isikuandmete töötlemise põhimõtete ja -tingimuste kirja panek. Selle tulemusena muutub e-ehituspoes toimuv tegevus ka inimese jaoks läbipaistvamaks ja selgemaks. Sellise teabe esitamine mõjutab ka e-ehituspoe avalikku kuvandit ja usaldusväärsust.

Vastutus isikuandmete kaitse osas lasub isikuandmete töötlejal, kes peab rakendama kohaseid meetmeid, et veebileht, mille kaudu isikuandmeid kogutakse ning edaspidi kasutatakse oleks turvaline. Selleks kasutatavad meetmed võivad olla ka sellised meetmed, mis tunduvad elementaarsed olevat, kuid miskil põhjusel ei ole neid rakendatud. Näiteks on üheks lihtsaimaks meetmeks kasutada oma e-ehituspoe veebilehel turvalist ühendust (veebiaadressi alguses on *https*, mitte *http*).

Nendele asjaoludele on kasulik mõelda ka selle aasta maist jõustuva isikuandmete kaitse üldmääruse valguses, kuna järjest enam nõutakse isikuandmete töötlemise osas läbipaistvust ning selgust. Seetõttu soovitame nii e-ehituspoodidel kui ka teistel e-poodidel juba praegu tegelda oma e-poe platvormi tegevuspõhimõtete ülevaatamisega, kaardistada oma andmetöötlusprotsessid ning anda piisavalt selgelt inimestele teavet nende isikuandmete töötlemisest.

Konkreetsemalt on seire Eesti lõpptulemused üldistatud kujul kättesaadavad inspektsiooni kodulehelt ning GPEN-i enda üldtulemused kättesaadavad GPEN-i võrgulehelt. Seirega

seonduvalt soovitame e-poodidel tutvuda ka inspektsiooni turvalise e-poe juhendmaterjaliga.

GPENi praktikute töötuba

Eelmisel aasta juunis toimus Manchesteris, Inglismaal esimene GPEN-ga seotud praktikute töötuba, mis tehti jätkuüritusena Euroopa kaasuste lahendamise töötoale (European Case Handling Workshop). Töötoas osalesid 70 esindajat 32. asutusest üle maailma ning ka eksperdid tarbijakaitselistest asutustest ja telekommunikatsiooni sektorist. Töötoa eesmärgiks oli arutada privaatsuse kaitse ja andmekaitse asutuste praktilist koostööd ning jagada parimat praktilist kogemust.

Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni nõuandekomitee

Kaja Puusepp, arendusdirektor

Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon avati allkirjastamiseks Strasbourgis 28. jaanuaril 1981, Eesti ratifitseeris selle 14. novembril 2001. Konventsiooni lisaprotokoll avati allkirjastamiseks 8. novembril 2001 ning selle ratifitseeris Eesti 28. juulil 2009.

2017. aasta täiskogu istungitel olid arutusel Ministrite Nõukogule esitatavate soovituste eelnõud terviseandmete kaitse ning isikuandmete kaitse kohta politseitöös. Arutelud nende soovituste osas jätkuvad 2018. aastal. Euroopa Nõukogus on algatatud konventsiooni uuendamise protsess, arutamisel on küsimustiku eelnõu, mille abil hinnata riikide vastavust uue konventsiooni nõuetele. 2017. aastal avaldati nõuandekomitees valminud juhend isikuandmete kaitseks suurandmete maailmas.

Andmekaitse Inspektsioon
2018