



ANDMEKAITSE INSPEKTSIOON

# **AVALIKU TEABE SEADUSE JA ISIKUANDMETE KAITSE SEADUSE TÄITMISEST AASTAL 2014**

## **SOOVITUSED AASTAKS 2015**

## Andmekaitse Inspeksiooni aastaaruanne 2014



### Sisukord

Peadirektori kokkuvõte.....	5
I. Milleks isikuandmete kaitse? Milleks avaliku teabe kättesaadavus?.....	5
II. Mis kasu on Andmekaitse Inspeksioonist?.....	5
III. Isikuandmete kaitse ja avaliku teabe kättesaadavus ei ole üksnes inspeksiooni asi.....	6
IV. Olulisemat 2014. aastal.....	8
V. Olulisemat 2015. aastal.....	11
VI. Soovitused avaliku sektori asutustele.....	13
VII. Tänuavaldused.....	16
1. Selgitaja ja teavitaja.....	18
1.1. Selgitustaotlused.....	18
1.2. Infoliin.....	18
1.3. Konverentsid ja koolitused.....	19
1.4. Meediasuhtlus.....	20
2. Õigustavade kujundaja.....	21
2.1. Juhised.....	21

2.1.1. Juhis: Isiklikud mobiilsed seadmed töökeskkonnas.....	21
2.1.2. Juhis: Infoturve ja isikuandmete kaitse väikeettevõttes.....	21
2.1.3. Juhis: Isikuandmete kustutamine seadmetes.....	21
2.1.4. Juhis: Turvaline e-pood.....	22
2.1.5. Avaliku teabe seaduse üldjuhendi avaliku teabe masinloetava taaskasutamise osa.....	22
2.2. Rahvusvaheline koostöö.....	23
2.2.1. Euroopa andmekaitseasutuste tööühm.....	23
2.2.2. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni nõuandekomitee.....	24
2.2.3. Telekommunikatsioonialane andmekaitse tööühm.....	24
3. Poliitikanõustaja.....	25
3.1. Arvamused õigusaktide eelnõudele.....	25
3.1.1. Arvamuse avaldamine elektroonilise side seaduse ja infoühiskonna teenuse seaduse muutmise seaduse eelnõu kohta.....	25
3.1.2. Arvamuse avaldamine elektroonilise side seaduse muutmise ettepanekute kohta.....	25
3.1.3. Arvamuse avaldamine julgeoleku- ja taustakontrolli seaduse eelnõu kohta.....	26
3.1.4. Arvamuse avaldamine avaliku teabe seaduse, elektroonilise side seaduse ja isikuandmete kaitse seaduse muutmise seaduse eelnõu kohta.....	27
3.1.5. Arvamuse avaldamine kohaliku omavalitsuse korralduse seaduse § 6 täiendamise seaduse eelnõu ja selle rakendusakti kavandi kohta.....	27
3.2. Koordinaatorite võrgustik.....	28
3.3. Statistikanõukogu.....	28
4. Järelevalvaja.....	29
4.1. Isikuandmete kaitse.....	29
4.1.1. Isikuandmete kaitse töösuhetes.....	29
4.1.2. Isikuandmete töötlemine suhtluskeskkondades.....	30
4.1.3. Isikuandmete töötlemine meedias.....	30
4.1.4. Isikuandmete töötlemine rahandussektoris.....	33
4.1.5. Isikuandmete töötlemine tervishoiusektoris.....	35
4.1.6. Koolielu.....	38
4.1.7. Koostöö rahvastikuregistriga.....	39
4.1.8. Politsei infosüsteemi väärkasutamine.....	40
4.2. Avalik teave.....	40
4.3. Elektrooniliste kontaktandmete kasutamine elektroonilises otseturustuses (spämm).....	42
4.4. Tähelepanu pälvinud muud menetlused.....	43
5. Audiitor ja loaandja.....	45
5.1. Seired.....	45
5.1.1. Avaliku teabe seaduse täitmise seire.....	45
5.1.2. Kohalike omavalitsuste võrgulehtede valgusfooriseire.....	46

5.1.3. Elektroonikaseadmete utiliseerijate seire.....	47
5.1.4. Kiirlaenuandjate seire.....	48
5.1.5. Interneti rehitsemise päeva seire.....	49
5.1.6. E-lasteaedade seire.....	49
5.2. Auditid.....	50
5.2.1. Terviseandmed ja e-Tervise infosüsteem.....	50
5.2.2. Tallinna Transpordiamet.....	50
5.2.3. Tallinna Munitsipaalpolitsei Amet.....	51
5.3. Loamenetlused.....	51
5.3.1. Teadusuuringute load.....	51
5.3.2. Delikaatsete isikuandmete registreerimine.....	52
5.3.3. Andmekogude kooskõlastamismenetlused.....	52
5.3.4. Kolmandatesse riikidesse isikuandmete edastamise load.....	53
5.4. Rahvusvaheline järelevalvealane koostöö.....	53
5.4.1. Schengeni konventsiooni andmekaitse järelevalve.....	53
5.4.2. Euroopa sõrmejälgede andmebaasi (Eurodac) töögrupp.....	54
5.4.3. Tollikonventsiooni andmekaitse järelevalve.....	54
5.4.4. Europol'i konventsiooni ühine andmekaitse järelevalveasutus.....	54
5.4.5. Balti andmekaitseasutuste järelevalve koostöö.....	55

## **Peadirektori kokkuvõte**

Isikuandmete kaitse seaduse ning avaliku teabe seaduse kohaselt esitan Riigikogu põhiseaduskomisjonile ja õiguskantslerile aastaettekande mõlema seaduse täitmisest. Lisaks tagasivaatele annan ülevaate tänavusest tegevuskavast ning esitan omapoolseid soovitusi. Kasutan siinkohal võimalust soovida põhiseaduskomisjoni uuele koosseisule ning vastsele õiguskantslerile jõudu ja edu vastutusrikkas töös.

### **I. Milleks isikuandmete kaitse? Milleks avaliku teabe kättesaadavus?**

Igaühel on õigus pere- ja eraelu puutumatusel, sõnumisaladusel ning vabale eneseteostusele. Kõik need põhiõigused on ohus, kui isikuandmeid väärkasutatakse.

Väärkasutus võib ohustada samuti põhiõigust valida vabalt tegevusala, elukutset ja töökohta. Eriti siis, kui inimese kohta on teavet kogutud tema enda teadmata.

Selleks, et inimene teaks ja saaks ennast kaitsta, peab tal olema õigus pääseda tema kohta kogutud info juurde. Kuid ei see ega ükski muu isikuandmetega seotud õigustest ei ole absoluutne.

Kaitstes põhiõigusi kaitseme ühtlasi üldisi huve. Digimajanduse ja e-riigi arenguks on muuhulgas vaja usaldust. Inimesed ei usalda andmebaase ja e-teenuseid, kui nad kahtlevad, kas nende kohta kogutud teabega on seal kõik korras.

Võimuasutused koguvad-kasutavad reeglina infot ilma inimese nõusolekuta ja mõnikord ka ilma tema teadmata. Info väärkasutamine võimuasutuse poolt viib võimu väärkasutamiseni. Isikuandmete õiguspärane kasutamine avalikus sektoris on demokraatliku õigusriigi kestlikkuse üks eeldusi.

Avaliku teabe kättesaadavus on oluline konkreetset teavet vajavale üksikisikule. Kuid kogumis mõjutab see samuti tervet ühiskonda. Avaliku teabe kättesaadavus aitab tagada tõhusamat kontrolli avaliku võimu teostamise, avaliku raha kasutamise ja avalike ülesannete täitmise üle.

Avaliku teabe kättesaadavusel, sh masinloetaval kujul avaandmetena, on mõju ettevõtlusele ja innovatsioonile.

Mida enam isikuandmed kui ka (juurdepääsupiiranguga) avalik teave digitaliseeruvad, seda tähtsamaks muutub nende turvaline hoidmine

### **II. Mis kasu on Andmekaitse Inspeksioonist?**

Andmekaitse Inspeksioon valvab isikuandmete kogumise-kasutamise ja avaliku teabe kättesaadavuse üle. Nende kahe erineva tegevussuuna koondamine ühte asutusse võimaldab tasakaalustatumat lähenemist.

Isikuandmete kaitse seadus on eeskätt abstraktne üldseadus. Ta põhineb suuresti üldprintsüüpidel ning määratlemata õigusmõistetel (nt. „avalik huvi“, „ülemäärane kahjustamine“) kaalumisel.

Tänu abstraktsusele ja tehnoloogia-neutraalsusele on andmekaitserreeglid aja proovile vastu pidanud. Eesti seaduse aluseks oleva andmekaitse direktiivi 46/95/EÜ jõustumisest möödub tänavu 20 aastat.

Inspeksiooni nime kandvat asutust peetakse tavaliselt kontrolli-, sunni- ja karistusasutuseks. Tegelikult moodustavad „pehmed“ tegevused üle poole meie töömahust.

Abstraktsete õigusnormide ning määratlemata õigumõistete rakendamine koos infoühiskonna ja tehnoloogia kiire arenguga nõuavad meilt analüüsi-, ennetus- ja teavitusasutusena toimimist.

Juhendiloome on üks kesksetest ülesannetest, mille meile paneb nii isikuandmete kaitse kui ka avaliku teabe seadus.

Juhendiloome on eriti oluline Eesti keele- ja õigusruumi väiksust silmas pidades. Soovituslike selgitavate juhenditega üritame korvata privaatsus- ja IT-õiguse alase kohtupraktika ning eriala(a)kirjanduse nappust. Ühiskond vajab õiguskindlust.

Teabega seotud õigused on ajakriitilised. Mida pikem on õiguste rikkumise menetlus, seda raskem on küberruumi voolanud infot tagasi kerida. Küsitud avalik teave kaotab aga pika menetluse tõttu küsija jaoks väärtuse. Seetõttu on Andmekaitse Inspeksioonil uurimis- ja sunnivolitused järelevalveasjades ning karistamisõigus väärteoasjades.

Oma järelevalvetöös saame vajadusel kasutada Eesti Kohtuekspertiisi Instituudi ning Registrate ja Infosüsteemi Keskuse spetsiifilist oskusteavet.

Üksikrikkumistele keskendunud menetluste kõrval:

1) viime läbi võrdlevaid seireid, mis hõlmavad kümneid või sadu isikuandmete töötlejaid või avaliku teabe valdajaid. Seire tulemusena toome üldistavalt välja head ja halvad tähelepanekud ning teeme soovitusi ja ettepanekuid,

2) korraldame suurtes ja/või tundlikes organisatsioonides andmekaitseauditeid, mille põhieesmärk on probleemide ennetamine,

3) uue menetlusvormina võtsime kasutusele omaalgatuslikud ringkirjad. Kui on põhjust arvata, et mingis valdkonnas on andmekaitse või avaliku teabe alane laiem probleem, saadame kõigile ettevõtetele või asutustele, keda see võib puudutada, selgitavad ringkirjad.

Oluline roll on meie töös kommunikatsioonil – eeskätt konkreetseid sihtgrupe mõjutaval teavitustegevusel. Ka see aitab meil oma väiksust kompenseerida.

Andmekaitse Inspeksioon veab või osaleb liikme või nõustajana kümnekonnas riigisiseses koostöövõrgustikus ja ühistöörühmas. Nimetada võib näiteks valitsusasutuste avaliku teabe ja isikuandmete kaitse koordinaatorite võrgustikku, Statistikanõukogu, digitaalse teadlikkuse alaseid koostööprojekte „Targalt Internetis” ning „Nutiturva 2017”, e-tervise rakkerühma, majandusministeeriumi ava- ja linkandmete töörühma.

Inspeksiooni ühiskondlik nõukoda koosneb asjatundjaist, kellelt küsime arvamust tegevusprioriteetide ja juhendieelnõude kohta.

Kõik need meetmed ja koostöövormid võimaldavad meil tegeleda piltlikult öeldes mitte üksnes puude, vaid ka metsaga.

### **III. Isikuandmete kaitse ja avaliku teabe kättesaadavus ei ole üksnes inspeksiooni asi**

Isikuandmete kogumine-kasutamine on kõiki ühiskonnasektoreid hõlmav horisontaalne teema. Avalikule teabele ligipääs on kogu avalikku sektorit hõlmav horisontaalne teema. Mõlema horisontaalteema järelevalvega tegelevas Andmekaitse Inspeksioonis töötab 18 ametnikku. Koosseisu suuruselt oleme eelviimane valitsusasutus.

Kas niimoodi on tõesti võimalik tõhusalt tagada isikuandmete kaitstus ja avaliku teabe kättesaadavus? Kindlasti mitte, kui mõlema teemaatikaga tegeleks Andmekaitse Inspeksioon üksi ja täies ulatuses.

Isikuandmete osas on kõige olulisem inimeste eneste võimalus kontrollida, mida nende kohta on kogutud ja kuidas seda kasutatakse. Paljud avaliku sektori andmekogud ning ärisektori e-teenuste keskkonnad võimaldavad ilma eraldi küsimiseta otseligi pääsu inimese enda kohta käivale teabele.

Avaliku teabe kättesaadavuse osas on samuti oluline teabe küsijate-kasutajate endi teadlikkus ja nõudlikkus.

1.7.2014 jõustunud korraaitseeseadus loob selgemad alused järelevalveasutuse sekkumispiiride tõmbamiseks, kui asutusse pöörduakse asjus, mis on olemuselt eraisikute eratülid ning tuleks lahendada tsiviilkohtus.

Avalikus halduses on horisontaalse teemaderingi eripäraks, et sellega on sisu poolest rohkem või vähem seotud hulk teisi asutusi. Toon mõned näited isikuandmete ning avaliku teabe teematika seostest:

- 1) Riigi Infosüsteemi Amet: küberturve, andmekogude järelevalve, riigi infosüsteemi tugisüsteemid, avaliku sektori teabevärava haldamine ja avaandmete korraldamine,
- 2) Politsei- ja Piirivalveamet: isikuandmetega seonduvate süütegude uurimine, veebikonstaablid, sisekontroll politsei andmekogude ametkondliku väärkasutamise tõkestamiseks,
- 3) Terviseamet: tervishoiuteenuse osutamise, eriti selle dokumenteerimiskohustuse järelevalve,
- 4) E-Tervise Sihtasutus: e-tervise infosüsteemi teabeturve ja kasutamisseire,
- 5) ministeeriumide valitsusalasid teenindavad IT-tugiasutused: teabeturbe korraldamine,
- 6) IT-tugiasutuste seas on Hariduse Infotehnoloogia Sihtasutus ühtlasi ka digitaalse teadlikkuse edendamise vedaja,
- 7) Siseministeerium: rahvastikuregistri teabeturve ja kasutamisseire,
- 8) Välisministeerium lülitas mullu andmekaitseteema konsulaarasutuste korrapärasesse järelevalvesse.

Isikuandmete ja eraelu kaitsega seotud komponente sisaldavad ka mitmed muud järelevalvevaldkonnad, teiste seas võib välja tuua:

- 1) Tarbijakaitseamet: tarbijakaitse ja reklaamijärelevalve,
- 2) Tööinspeksioon: töölepinguseaduse järelevalve,
- 3) Finantsinspeksioon: pangandus- ja kindlustusjärelevalve,
- 4) Tehnilise Järelevalve Amet: elektroonilise side järelevalve.

Tihe seos on meil õiguskantsleri institutsiooniga. Inspeksiooni eesmärk on kaitsta teabega seotud põhiõigusi. Õiguskantsleri tööpõld hõlmab kõiki põhiõigusi, sellele lisandus tänava jätustegevuse järelevalve.

Andmekaitse Inspektsiooni peadirektoril on otsene ettekandeõigus õiguskantslerile. See võimaldab teabeõiguste kaitset paremini sidustada põhiõiguste kaitsega üldiselt. Ühtlasi annab see võimaluse vajadusel paluda, et õiguskantsler kaaluks normikontrolli teostamist.

#### **IV. Olulisemat 2014. aastal**

a) juhendiloomes ja nõustamises oli prioriteediks e-kaubandus

Inspektsioonil on tavaks seada tähelepanu ja ressursside koondamiseks üks kindel teema aasta prioriteediks. Mulluseks prioriteediks oli e-kaubandus. Uuringute kohaselt ei ole meie e-kaubanduse näitajad rahvusvahelises võrdluses esileküündivad – kontrastina näiteks e-pangandusele. E-poes ostja ja müüja teineteist ei näe, seetõttu on e-kaubanduse üheks eelduseks klientide usaldus. Kliendiandmete turvaline ja privaatsust austav töötlemine aitab usaldust luua.

E-kaubandus on alustavate ettevõtjate jaoks oluliseks segmendiks – see ei nõua suurt lähtekapitali. Väikeettevõtjate jaoks on oluline saada lihtsas keeles käepärast ametkondade-ülelt abistavat infot.

Aasta algul korraldasime koos Tarbijakaitseametiga ning majandusministeeriumiga selleteemalise ümarlaua ettevõtlusorganisatsioonidele. Saime tagasisidet, millist abi meilt tegelikult elus enim vajatakse. Selle tulemusena koostasime kaks juhendit:

- „Infoturbe ja isikuandmed väikeettevõttes”,
- „Turvaline e-pood”.

Koondasime neisse praktilised infotehnoloogilised ja juriidilised juhtnöörid. Loodetavasti on neist kasu eriti ettevõtlusega alustajail. Infoturbe osas andis koostamisel head nõu ka Riigi Infosüsteemi Amet.

Mõlema juhendi puhul pidasime silmas, et neid saaks hiljem ettevõtluse nõustamiseks kasutada laiema koolitusmaterjali kokkupanemisel.

Tutvustasime juhendeid Tarbijakaitseameti ning Eesti e-kaubanduse Liidu korraldatud koolitustel.

IKT-seadmete tavakasutajatele suunasime samuti kaks praktilist juhendmaterjali:

- „Isiklikud mobiilsed seadmed töökeskkonnas” - täienduseks töösuhetes isikuandmete töötlemise üldisele juhendile,
- „Isikuandmete kustutamine seadmetes” - elektroonikaseadmete uutiliseerimisega tegeleva 11 ettevõtte seire tulemusena.

Avaliku teabe alal olid kindlasti keskseks teemaks avaandmed ehk täpsemalt – avaliku teabe masinloetava allalaetavuse võimaldamine. Võtsime sellealased küsimused kokku avaliku teabe üldjuhendi uues peatükis. Samuti aitasime Majandus- ja Kommunikatsiooniministeeriumit avaandmete roheline raamatu koostamisel, kirjutades sinna isikuandeid ja eraelu kaitset käsitleva peatüki.

b) statistika: reageerivate tegevuste maht vähenes

Mullune statistika valmistas üllatuse. 2007. aastal toodi inspektsioon Justiitsministeeriumi haldusalasse. Sealt lugedes 5 aastaga (vahemikus 2007-2013) kasvasid inspektsiooni reageerivate tegevuste mahud 5-kordselt:

- kaebuste arv kasvas 110-lt 550-le (kasv täpselt 5 korda),
- selgitustaotluste arv kasvas samal ajal 251-lt 1370-le (kasv 5,5 korda),
- lisaks vastati 2013. aastal 1344 infotelefoni kõnele. Infotelefoni seadsime sisse aastal 2009 ning see on vähendanud selgitustaotluste ja ilmselt ka kaebuste arvu kasvu.

Kasvu jätku eeldasime ka mullu. Kuid 2014 oli esimene aasta inspektsiooni ajaloos, kus reageerivate tegevuste arvud kasvu asemel kahanesid. See puudutab kaebusi-vaideid, selgitustaotlusi, nõustamisi, infotelefoni kõnesid, väärteoasju.



Ühest ja kindlat põhjust vähenemisele ei oskagi ma välja tuua. Võimalik, et siin taga on vähemalt osaliselt inspeksiooni senise ennetustöö ja juhendilooma pikaajalisem mõju.

Delikaatsete isikuandmete töötlemise registreerimistaotluste arvu kolmandikuline kasv (602lt 902le) on seletatav tööga, et suurel osal andmetöötlejaist lõppes 5-aastane registreeringuperiood. Registreerimiskohustusega seotud ettekirjutuste arvu vähenemist (2012. a. 130lt mullu 45le) saab põhjendada inspeksiooni ennetava teavitustööga.

PEAMISED TÖÖVOOD	2012	2013	2014
<b>Selgitus- ja teavitustöö</b>			
Selgitustaotlused, märgukirjad, teabenõuded	817	1370	1144
Infotelefoni kõned	1160	1344	1141
Nõustamised	56	69	34
Koolitused ( <i>korraldatud või lektorina osaletud</i> )	18	19	24
<b>Järelevalvetöö</b>			
Võrdlevad seired ( <i>lõpetatud</i> )	4	4	6
Kaebused, vaided, väärteoteated ( <i>esitatud</i> )	404	550	413
Omaalgatuslikud järelevalveasjad ( <i>algatatud</i> )	191	171	152
Ettekirjutused järelevalveasjades	187	121	86
<i>sh. ettekirjutused registreerimiskohustuse alal</i>	130	68	45
Kohapealsed kontrollkäigud järelevalveasjades	23	15	48
Väärteoasjad ( <i>lõpetatud</i> )	43	29	11
Trahvid ( <i>väärteoasjus</i> ), sunnirahad ( <i>järelevalveasjus</i> )	39	22	8
<b>Loa- ja erimenetlused</b>			
Delikaatsete isikuandmete töötlemise või vastutavate isikute alased taotlused	608	602	902
Andmekogude kooskõlastamistaotlused ( <i>riigi infosüsteemi haldussüsteemi kaudu</i> )	84	89	115
Loataotlused teadusuuringuiks andmesubjektide nõusolekuta	13	17	13
Loataotlused isikuandmete 3. riikidesse edastamiseks	7	6	13
Andmesubjektide taotlused Schengeni, Europoli jt piiriüleste infosüsteemide asjus	4	6	6
<b>Õigustavade kujundamine, poliitikanõustamine</b>			
Juhendid	4	12	6
Arvamused õigusaktide eelnõude kohta ( <i>väljaspool</i> )	21	30	28

c) omaalgatusliku järelevalvetöö mahtu suurendasime

Reageeriva tegevuse töömahu vähenemise kompenseerimiseks suurendasime omaalgatuslike ennetustegevuste mahtu.

Kõige mahukam järelevalveprojekt on iga-aastane asutuste võrgulehtede ja dokumendiregistrite valgusfooriseire. Nimetus tuleneb sellest, et üldhinnangud seiratutele anname foorivärvides. Kui tunamullu seirasime valitsusasutusi (43 objekti), siis mullu kõiki omavalitsusi (215) ning tänavu nii omavalitsusi kui ka maavalitsusi (15).

2014. aasta omavalitsuste valgusfooriseirele järgnes läbipaisvaimate omavalitsuste konkurs. Sellel hindasime lisaks õiguslikele nõuetele ka volikogude tegevuse läbipaistvust (võrgulehel kajastamist). Konkursi võitsid suuremate voorus Põlva ja väiksemate voorus Torma vald.

Lisaks omavalitsuste seirele viisime mullu läbi veel 3 seiret:

- kiirlaenukontorite (19) seire koos Tarbijakaitseametiga,
- nutiseadmete tasuta rakenduste (30) seire andmekaitseasutuste üleilmse Interneti rehitsemise aktsiooni käigus ühtlustatud meetodika alusel,
- elektroonikaseadmete utiliseerimisega tegelevate ettevõtete (11) seire, mille põhjal koostasime juhendi „Isikuandmete kustutamine nutiseadmetes”,

Samuti viisime lõpule varem alustatud:

- asutuste dokumendiregistrite eriseire (144 asutust),
- avaliku teabe juurdepääsupiirangute õiguslike aluste seire (jättes 177 kasutusel olnud piirangust alles 86). Seire tulemusi saab Majandus- ja Kommunikatsiooniministeerium kasutada avaliku sektori dokumendihalduse arendamisel klassifikaatorina.

Eelmise ja üle-eelmise aasta võrdluses suurendasime ka kohapealsete kontrollkäikude arvu (15-lt 48-ni). Viisime läbi 5 andmekaitseauditit.

Sealhulgas ravispaaude (sanatooriumide) audit toimus Balti andmekaitseinspeksioonide ühisaktsioonina (ühise küsimustiku alusel). Eestis auditeeriti isikuandmete kaitset 12 sanatooriumis.

Tervishoiule ja hoolekandele pöörasime mullu palju tähelepanu. Lisaks sanatooriumide auditile korraldasime:

- a) andmekaitseauditid Läänemaa Haiglas ja Tallinna Lastehaiglas,
- b) delikaatsete isikuandmete töötlemise registreerimise nõuete täitmise osas korraldasime etteteatamata kontrollkäigud 10 apteegis,
- c) tervishoiu andmekvaliteedi osas saime Sotsiaalkindlustusametist lähteandmed (probleemid e-tervise infosüsteemi alusel invaliidsuse dokumendipõhise määramisel) ning osalesime Terviseameti korraldatud etteteatamata kontrollkäikudel kolme tervishoiuteenuse osutaja juures. Teiste probleemsete tervishoiuasutustega peeti kirjavahetust,
- d) samuti kontrollisime delikaatsete isikuandmete turvalise edastamise ja töötlemise nõudeid etteteatamata kontrollkäikudel 10 hooldekodus.

Maksu- ja Tolliametis kontrollisime füüsilisest isikust maksumaksjate kohta tehtavate automaatotsuste vastavust isikuandmete kaitse seadusele.

Lähemalt on mulluseid tegevusi kommenteeritud järgnevates sisupeatükkides.

## V. Olulisemat 2015. aastal

a) tervishoid ja hoolekanne: prioriteediks abivajajate kohta info liikumise juhend

Meie tänavuseks prioriteediks on praktilise juhendmaterjali koostamine meditsiini- ja hoolekandeabi vajavate inimeste kohta käiva info liikumise asjus. Sellist infot on näiteks lasteaedadel, koolidel, perearstidel, haiglatel, politseil jt.

See info ei pruugi jõuda sinna kuhu vaja – eeskätt omavalitsuse kui hoolekande-, lastekaitse- ja eestkostetasutuseni. Lünklikud on ka toetuste taotlemise põhjal üles ehitatud registrid – kui ei taotleta, siis infot ei teki.

Meditsiini- ja hoolekandeabi vajaduste kohta käiv teave on loomulikult tundlik ja seda tuleb hoolikalt hoida. Kuid sageli jääb see info seisma ega liigu edasi. Tihti tuuakse ettekäändeks kõike segav andmekaitse.

Kaardistame sellealased tüüpsituatsioonid ja -probleemid, kohtume asjaosaliste asutuste ja organisatsioonidega ning koostame selgitava juhendi.

Teiseks koostame terviseandmete piiriüleste liikumiste õigusliku analüüsi (sh õiguskaitsenkoostöös).

Samuti kontrollime kohapeal 20 perearstikeskust. Kontrolliplaani koostamisel on arvestatud ka Riigi Infosüsteemi Ameti infoturbe-alaste soovidega.

Viime läbi ühe kiirabi teenuse osutaja kohapealse kontrolli (andmeliiklus kiirabi, haigla, e-tervise ning häirekeskuse vahel) ning andmekaitseauditi ühes suuremas haiglas.

b) avaliku sektori andmehaldus

Tervishoiu ja hoolekande kõrval on teiseks suuremaks tööpõlluks tänavu avaliku sektori andmehalduse teabeturve ja andmekvaliteet:

Koostame asutustele AK-teabe kaitse juhendi. Ametlik turvameetmete süsteem (infosüsteemide kolmeastmeline etalonturbe süsteem - ISKE) kehtib üksnes andmekogudele, muus osas on juhtnööriks vaid avaliku teabe seaduse säte, mis ütleb, et asutusesiseseks kasutamiseks tunnustatud teavet tuleb kaitsta (§ 43 lg 1).

Teeme järelevalvet mitmes IT-tugiasutuses, Maksu- ja Tolliametis (pääsuõiguste haldus, säilitustähtajad, piiriülene andmevahetus), Päästeametis (päästeinfosüsteem), Statistikaametis (minimaalsuspõhimõtte isikuandmete kogumisel)

Samuti kontrollime korrakaitse jälgimisseadmetiku kasutamist ning isikuandmete õiguspärasest avaldamist kohtuinfosüsteemis ja karistusregistris.

Võtsime luubi alla andmekogudes ISKE rakendamise ja andmeturbeauditite tegemise. Muuhulgas kontrollime 2020. aasta registrite põhise rahvaloenduse läbiviimise seisukohalt 40 olulisemat andmekogu.

AK-teabe kaitset kontrollime 50 õppeasutuse dokumendiregistrites. Äsja lõpetasime koolides kolme enim kasutatava õppeinfosüsteemi järelevalve.

c) isikuandmed kliendi- ja töösuhetes

Kontrollime neljas suuremas jaekaubanduskettis töölesoojijate, töötajate ja endiste töötajate isikuandmete haldamist. Valisime need ettevõtted suure personalikäibe tõttu. Läti ja Leedu andmekaitseinspeksioonid nõustusid võtma selle projekti Balti iga-aastase ühisjärelvalve teemaks. Seega toimub järelevalve kolmes riigis ühesuguse küsimustiku alusel.

Lisaks teeme järelevalvet:

- kolmes kasutatud e-seadmeid müüvas ettevõttes (et ei teeks avalikult seadme eelmise kasutaja andmeid – asjakohased soovitusel andsime mullu võrdleva seire põhjal koostatud juhendis „Isikuandmete kustutamine seadmetes”),
- viies sideettevõttes (kliendiandmete turve),
- kolmes e-poes (klientidele nõuetekohane info andmine - asjakohased soovitusel andsime mullu võrdleva seire põhjal koostatud juhendis „Turvaline e-pood”).

Inkassoettevõtete võrdleva seire käigus uurime nende andmeallikaid ja säilitustähtaegu.

Samuti viime läbi telemaatikat (täpsemalt: tööautode elektroonilist jälgimist) kasutatavate ettevõtete seire. Ilmselt saame seire tulemuste põhjal täiendada praktilist juhendmaterjali.

Samuti on kavas koostada kaasaskantavate nutiseadmete (kellad, võrud jms) privaatsusteamaline materjal. Eriti huvitab meid terviseandmete kasutamine.

Droonide (salvestus- ja jälgimisseadmetega varustatud mehitamata lennumasinade) kasutamise osas täiendame inspeksiooni 2013. aasta juhendit kaamerate kasutamise kohta. Hetkel on vastav peatükki kooskõlastamisel Lennuametis – lugeja mugavuse huvides soovime ühte materjali lülitada mõlema ametkonna soovitusel (nii isikuandmete kaitse kui lennuohutusosalased).

Samuti on vajalik kaamerajuhendit täiendada selgitustega Euroopa Kohtu 11.12.2014 eelotsusega turvakaamerate asjus <http://curia.europa.eu/juris/document/document.jsf?text=&docid=160561&pageIndex=0&doclang=ET&mode=lst&dir=&occ=first&part=1&cid=7284>

Elektrooniliste kontaktandmete otseturustuseks kasutamise osas viime läbi järelevalve 10 ettevõttes. Samuti kontrollime kindlustusseltside tüüptingimused otseturustuse ajal.

d) avaliku teabe kättesaadavus

Viime läbi omavalitsuste ning maavalitsuste võrgulehtede ja dokumendiregistrite valgusfooriseire, andes üldhinnanguid foorivärvides. Lisakriteeriumide alusel anname välja kõige läbipaistvama omavalitsuse auhinna. Seire küsimustikku arutasime omavalitsuste katusorganisatsioonidega.

Samuti viime läbi seire, hindamaks, kuidas asutused täidavad seaduse nõudeid ning avaliku teabe üldjuhendi ning avaandmete rohelise raamatu soovitusi avaliku teabe masinloetava allalaetavuse alal.

Avaliku teabe üldjuhendit täiendame kahe uue peatükiga, mis käsitlevad Euroopa Liidu tõukefondide kasutamise ning riigihangete avalikkust.

e) rahvusvaheline koostöö

Andmekaitsealase rahvusvahelise koostöö keskne teema on jätkuvalt 2012. a. jaanuaris väljakäidud Euroopa Liidu andmekaitseõiguse reformikava. Korraldasime Õiguskantsleri Kantselei abiga reformi mõjude arutamiseks 23.01.2015 asjatundjate foorumi.

Eesti Andmekaitse Inspeksioon panustab Euroopa andmekaitseasutuste töörühmas praktilise piiriülese koostöö teematikale.

Eesti, Läti ja Leedu andmekaitseinspeksiooni koostöö on olnud järjepidev. Igal aastal oleme läbi viinud ühise küsimustikuga järelevalved, et tagada ühtlast andmekaitsetaset kolme Balti riigi majandusel.

## VI. Soovitused avaliku sektori asutustele

### a) avaliku sektori infoturbe vajab tugevamat ohjamist

Avaliku sektori teabeturbe vallas näikse väliselt asjad korras olevat:

- seadused kohustavad asutusi kaitsma isikuandmeid ja muud juurdepääsupiiranguga teavet (haldusmenetluse seaduse [§ 7 lõiked 3 ja 4](#), isikuandmete kaitse seaduse [§-d 24-26](#), avaliku teabe seaduse [§ 43](#)),
- valitsus on määrusega kohustanud valitsusasutusi rakendama ühtlustatud teabeturbe meetmeid („Infoturbe juhtimise süsteem“)
- avaliku sektori andmekogudele kehtib valitsuse määruse alusel põhjalik turvameetmete süsteem ([infosüsteemide kolmeastmeline etalonturbe süsteem – ISKE](#)),
- uued andmekogud läbivad kooskõlastusmenetluse [riigi infosüsteemi haldussüsteemis](#), selle käigus saab võimalikke puudusi välja sõeluda,
- teabeturbe järelevalvet teeb lausa kaks asutust:

Riigi Infosüsteemi Amet valvab niihästi andmekogude pidamise üle kui ka kõigi elutähtsate teenuste elektroonilise turvalisuse üle ja täidab üldisi küberturbeasutuse ülesandeid;

Andmekaitse Inspeksioon valvab niihästi isikuandmete kaitstuse üle kui ka avaliku teabe kättesaadavuse üle, viimane sisaldab ka juurdepääsupiirangute rakendamise järelevalvet.

Inspeksiooni hinnangul ei vasta tegelikkus päriselt välisele fassaadile. Lihtne näide: suur osa asutusi on andmekogude pidamisel eiranud korrapärase andmeturbeauditi tellimise kohustust. Riigi infosüsteemi haldussüsteemi ei tehta auditeerimise kohta ettenähtud märkeid, mis raskendab ülevaate saamist.

Suurte ja keeruliste infosüsteemide puhul ei saa asutuse juhtkond ilma erapooletu välise hindamiseta tagada, et infoturbelised ja andmekaitsetised riskid – eeskätt omaenda personalirisk – on maandatud.

Tuletan kõigile asutuste juhtidele meelde, et digiajastul on vilets teabeturbe sama ohtlik kui kehvalt valvatud riigipiir, katkine ukسلukk või ripakil rahakott. Asutuse juht vastutab teabeturbe tagamise eest samapalju kui näiteks asutuse raamatupidamise korraldamise eest.

Ootan Riigi Infosüsteemi Ametilt tõhusat panust ja koostööd:

- andmekogude kooskõlastusnõude täitmise asjus,
- andmekogude kohta riigi infosüsteemi haldussüsteemi kantud andmete õigsuse ja täielikkuse asjus,
- ISKE ning valitsusasutustes infoturbe juhtimise süsteemi rakendamise järelevalve alal, sealhulgas andmekogude auditeerimiskohustuse täitmise üle.

Järelevalvest üksi ei piisa – kooskõlastamata ja auditeerimata andmekogud tuleb mitte üksnes jätta ilma Euroopa Liidu tõukefondidest jagatavaist investeeringuist, vaid süstemaatiliselt eemaldada ka andmekogude andmevahetuskihi („x-tee“) teenustest kui riskiallikad.

Andmekogude kooskõlastamise kohta käiv määrus on tegelikkusest liiga kaugemale hälbinud ja vajab kiiret kohendamist. Tegelikus elus on kooskõlastatavate objektide liikide arv muutunud oluliselt laiemaks kui määruses kirjas. Isegi kooskõlastusi andvate asutuste ring on laiem kui määruses kirjas. Inspeksioon esitas oma ettepanekud Majandus- ja Kommunikatsiooniministriumile [18.11.2013 kirjaga nr 1.2.-2/13/2001](#).

Võtan avaliku sektori teabeturbe korrastamise isiklikuks prioriteediks ning kavatsen selles ilmutada järjekindlat rangust. Alates sellest aastast võttis inspeksioon teravdatud tähelepanu alla nii ISKE rakendatuse kui andmekogude auditeerimiskohustuse täitmise. Samuti koostame juurdepääsupiiranguga teabe kaitse juhendmaterjali (ISKE kehtib vaid andmekogudele), projekt on hetkel arvamuse avaldamiseks Riigi Infosüsteemi Ametis.

## **b) avaliku teabe avaandmetena kättesaadavaks tegemine**

Alates 1.1.2015 peavad kõik avaliku sektori andmekogud olema Eesti teabevärava kaudu masinloetavalt allalaetavad (avaliku teabe seaduse § 29 lõiked 3 ja 4 ning § 58.2).

Hindan nende seadusesätete elluviimist ebarahuldavaks, sest hetkeseisuga on teabevärava kaudu otse vastavas andmevaramus masinloetavaks kasutamiseks avaldatud kõigest 23 andmekogu.

Kuid mul on raske on andmekogude pidajatest asutuste suhtes kriitikat teha, sest:

- masinloetava avalikustamise kui suhteliselt komplitseeritud muudatuse läbiviimiseks vajalik juhendmaterjal – avaliku teabe masinloetava avalikustamise rohelise raamatu lõppversioon – valmis mitte enne seadusesätete vastuvõtmist, vaid kaks aastat hiljem ja kõigest kuu aega enne nende täielikku rakendamistähtaega.
- avaandmete varamu avati andmekogude pidajatele oma andmestike avamiseks alles peale avaandmete seadusesätete täielikku jõustumist ehk 2015. aasta jaanuaris.

Sisuliselt õnneks olukord nii halb ei ole. Kasutajatele olulisemad andmekogud – näiteks kohturegistrid, Maa-ameti ja Maanteeameti andmekogud – on masinloetavaks kasutamiseks avatud olnud juba palju varem, osalt isegi möödunud sajandi lõpuaastaist.

Seda suurem risk inimeste eraelule võib tuleneda neist isikuandmeid sisaldavaist andmekogudest, mida pidavad asutused ei ole varem avaandmete temaatikaga kokku puutunud.

Kordan tungivat soovitusi kõigile andmekogusid pidavatele asutustele – viige masinloetava allalaetavuse asjus läbi inventuur – mõjude hindamine. See aitab:

- hinnata teie infovarade olulisust avaandmetena,
- üle vaadata masinloetavuse tagamise tehnilise külje,
- kaardistada eraelu riive tõsiduse ning teha vajalikud muudatused. Terve andmekogu täielik allalaetavus koos võimalusega panna saadud teave kokku muudest allikaist pärit andmestikega loob oluliselt suurema inimeste profileerimise võimaluse kui üksikpäringute-teabenõuete ajal osati arvata.

Sellega seoses panen kõigile asutuste juhtidele südamele: asutuse dokumendiregistri avalikus osas peab eraisikutega peetava kirjavahetuse andmestik enne masinloetavuse võimaldamist olema umbisikustatud (initsiaalstatud).

## **c) ametliku e-posti laiem juurutamine**

Isikute kohta asutustesse ja andmekogudesse kogutud kontaktandmestiku ebarahuldavale kvaliteedile olen tähelepanu juhtinud nii 2008., 2011. kui 2013. a. ettekannetes.

Avalik sektor peaks isikutega suhtlemisel kasutama kontaktandmetena rahvastikuregistri andmeid. Mistahes avaliku sektori asutusega suhtlemisel peaksid andmeuudendused jõudma rahvastikuregistrisse. Asutused ei peaks koguma dubleerivalt kontaktandmeid.

Paraku näeme, et need põhimõtted ei ole ikka rakendunud, muuhulgas rahvastikuregistri seaduse ja menetlusseaduste haakumatuse tõttu. Füüsiliste ja ka juriidiliste isikute kontaktandmeid kogutakse haldus- ja kohtumenetlustes valdavalt igas asutuses eraldi ja tihti lausa igaks menetluseks eraldi. Tulemuseks on kehv andmekvaliteet (kontaktandmed on kiiresti muutuv teave) ning pidevad menetlusviivitused dokumentide kättetoimetamisel.

Samas on riik loonud kõigile füüsilistele ja juriidilistele isikutele ametliku e-posti aadressi (...@eesti.ee) ning sisse logides isikustatud ligipääsu nii kesksesse teabeväravasse ([www.eesti.ee](http://www.eesti.ee)) kui ka ametkondlikesse portaalidesse.

Tegin mullust aastaettekannet tutvustades soovitusena muuta asutuste ja isikute vaheliseks eelistatud suhtluskanaliks ametlik e-post ning elektrooniline kättetoimetamine. Nii saaksime üle avaliku sektori käes oleva isikute kontaktandmestiku kehvast kvaliteedist. Samuti saaksime muuta asjaajamist kiiremaks ja odavamaks.

Asjassepuutuvad ametkonnad avaldasid ettepanekule toetust. Ettepaneku rakendamiseks kutsusin kokku töörühma, milles osalevad Justiitsministeerium, Majandus- ja Kommunikatsiooniministeerium, Siseministeerium ning Riigi Infosüsteemi Amet.

Töörühmas arutasime läbi, mida saaks esmalt teha seadusi muutmata:

- isikuile teadete saatmiseks kasutada ametlikku e-posti aadressi [isikukood@eesti.ee](mailto:isikukood@eesti.ee) või [registrikood@eesti.ee](mailto:registrikood@eesti.ee);
- menetlusdokumendi kätte toimetamiseks sisaldab teade vastavat linki,
- lingi avamiseks tuleb oma isikut tuvastades sisse logida vastavale vörgulehele (Eesti teabevärvavas [www.eesti.ee](http://www.eesti.ee) loodav „Minu postkasti” teenus, e-maksuamet, e-toimik vms portaal),
- haldusmenetlusseadus nõuab elektrooniliseks kättetoimetamiseks isiku nõusolekut, kuid ei välista üldise etteulatava nõusoleku andmist. Seetõttu koostasime seadusele vastava, kuid lihtsas keeles üldise nõusoleku teksti (eraldi füüsilisele ja juriidilisele isikule),
- nõusolek sobib nii neile, kes veel ei ole oma ametliku e-posti aadressi seadistanud, kui ka neile, kes on seda juba teinud (senised [www.eesti.ee](http://www.eesti.ee) kasutustingimused ei vasta seadusega nõutud elektroonilise kättetoimetamise nõusolekule),
- lingitud dokumendi avamisel (selleks peab isik end sisse logides tuvastama) loetakse menetlusdokument kätte toimetatuks, avamisest jääb alles digitaalne jälg,
- et isiku- või registrikoodi põhised ametlikku e-posti aadressid ei väärkasutataks, lubatakse selle kaudu saata üksnes ametlikke menetlusdokumente, Riigi Infosüsteemi Amet filtreerib tehniliselt saatjate ringi.

Praegu käib tehniline ettevalmistustöö Riigi Infosüsteemi Ametis. Nõusoleku andmise fakt konkreetse isiku kohta peab asutustele, kes isikule teadet või menetlusdokumenti saadavad, olema nähtav. Kättetoimetatava dokumendi avamisest tekkiv digitaalne jälg – kui see ei jää vastavasse portaali (nt e-maksuametisse) – peab Eesti teabevärvava kaudu jõudma dokumendi saatnud asutuse asjaajamissüsteemi. Kaasabi ootame ka Sise- ja Justiitsministeeriumilt (ametliku e-posti seadistamise fakti kajastamine füüsilise või juriidilise isiku kohta vastavalt rahvastiku- või äriregistris).

Et asutused ei jätkaks inertsist paberposti või menetluse käigus eraldi avaldatud e-posti aadresside eelistamist, on vajalik, et Majandus- ja Kommunikatsiooniministeerium teeks vastavad täiendused „Asjaajamiskorra ühtsetesse alustesse”. Kasulik oleks ka menetlusõiguslike seadusesätete ülevaatamine, iseäranis väärteomenetluses on ülemäärast lembetunnet paberi suhtes.

Samuti tuleb teha teavitustööd nii avalikkusele (et ametlikke e-posti aadresse seadistataks) kui ametnikele (et seda hakatakse kasutama esimese valikuna).

Tulevikus ootame Justiitsministeeriumilt seadusemuudatusi, mis vähemalt äriühingutele muudaksid ametliku e-posti kaudu avaliku sektoriga suhtlemise kohustuslikuks.

Kuna ametlik e-posti aadress on kõigil olemas, siis ei nõua see isikult täiendavaid kulutusi. Küll aga teeb see haldus-, kohtu-, täitemenetlused kiiremaks ning säästab raha postikulude pealt. See võimaldab ka üle saada avaliku sektori käes oleva kontaktandmestiku kehvast andmekvaliteedist.

Kutsun ettevalmistustöös osalevaid partnerasutusi üles projekti jätkuvalt panustama. Kutsun projekti teostumisel kõiki asutusi seda kasutama. Kutsun kõiki kodanikke, elanikke, e-residente ja juriidilisi

isikuid üles oma ametlikku e-posti aadressi seadistama, et muuta avaliku sektoriga suhtlemist mugavamaks ja kiiremaks.

#### **d) ühtsete veebipöördumiste vormide juurutamine**

Majandus- ja Kommunikatsiooniministeeriumi ning Andmekaitse Inspektsiooni ühise algatuse tulemusena on rakendusjärgus inspektsioonis väljatöötatud veebipöördumiste ühtsed vormid. Sellel algatusel on loodetavasti avaliku sektori ülene mõju.

Algidee järgi saab igaüks neid kasutada inspektsiooni poole pöördumisel, et esitada selgitustaotlust, märgukirja, teabenõuet, kaebust või vaiet. Selleks tuleb logida Eesti teabevärasse ning täita vastav vorm.

Andmeväljad, mida saab automaat- või eeltäita, on seal juba täidetud. Vabatekstiliste andmeväljade täitmise kohta kuvatakse selgitusi.

Lisaks saab pöörduja Eesti teabevära vahendusel näha, mida tema pöördumisega tehakse (menetlusinfo pöördumise vastuvõtmise, läbivaatamise ja vastamise kohta).

Inspektsioon ei pea veebipöördumise vastuvõtmise kohta käsitsi topelt-sisestustööd tegema – meie asjaajamissüsteem võtab need andmed automaatselt Eesti teabeväravast.

Täna on nii asutuste võrgulehtedel kui Eesti teabeväras sadu erinevaid dokumendivorme asutuste poole pöördumiseks. Paljud neist on ebamugavad (nt pdf-vormingus, mis tuleb täitmiseks välja trükkida).

Väga paljud arvutivõrgus avaldatud pöördumisvormid on dubleerivad. Teabenõudele, selgitustaotlusele ja märgukirjale kehtiv samad nõuded sõltumata sellest, kas see esitatakse näiteks valla-, linna- või maavalitsusele, ametile, inspektsioonile või ministeeriumile. Seega saavad Andmekaitse Inspektsiooni veebipöördumiste vorme kasutada ka kõik teised asutused.

Tänaseks 64 riiki koondava Avatud Valitsemise Partnerluses osalemiseks Vabariigi Valitsuse kinnitatud [2014-2016. aastate tegevuskavas](#) on eraldi välja toodud Andmekaitse Inspektsiooni ühtsete veebipöördumiste koostamine. Praegusel hetkel on inspektsioon väljatöötatud materjalid Majandus- ja Kommunikatsiooniministeeriumile üle andnud.

Mugavama, kiirema ja odavama asjaajamist huvides soovitan Majandus- ja Kommunikatsiooniministeeriumile järgmiste sammudena:

- a) muuta ühtsete veebipöördumiste vormid peale praktikas järgiproovimist riigiasutustele soovituslikust kohustuslikuks – tehes vastava täienduse „Asjaajamiskorra ühtsetesse alustesse”,
- b) võtta kasutusele ka muid pöördumisvorme – eeskätt omavalitsustasandil (näiteks ehitusalaste taotluste vormid), leppides kokku haldaja määramises,
- c) edaspidi keskselt arendada ka asutustest väljaminevaid veebipõhiseid dokumendivorme. Nende suur eelis on juurdepääsupiirangute ja säilitamise automaathaldus. Ametnik saab juba dokumenti luues eristada vaba juurdepääsuga dokumendiosad ning piiranguga kaetud dokumendiosad. Piirangutähtaegu saaks edaspidi hallata infosüsteem, dokumendihalduses väheneks käsitsitöö.

## **VII. Tänuavaldused**

Mullusele tegevusaastale tagasi vaadates on mul põhjust südamest tänada töökaaslasi Andmekaitse Inspektsioonist, kodu- ja välismaiseid koostööpartnereid ning inspektsiooni ühiskondliku nõukoja



liikmeid. Tänu teile võib möödunud aastat lugeda kordaläinuks nii eraelu kaitstuse kui avaliku teabe kättesaadavuse valdkonnas.

Olen tänulik eelmisele õiguskantslerile Indrek Tederile – kuue ja poole aasta jooksul tundsin Eesti riigi peajuristi heatahtlikku toetust.

Austusega

Viljar Peep

## 1. Selgitaja ja teavitaja

Selgitamine ja teavitamine hõlmab igasuguse informatsiooni jagamist nii individuaalselt selgitustaotlustele, teabenõuetele, märgukirjadele ja infotelefonile vastamisel kui ka avalikkuse informeerimist ulatuslikumalt, näiteks koolituste korraldamist või teavitamist meedia vahendusel. Selgitus- ja teavitustöö kaasneb nii isikuandmete kaitse, elektroonilise side kui ka avaliku teabe valdkonnaga. Teabe levitamisse on kaasatud sealjuures nii isikuandmete töötajad, andmesubjektid, teabenõudjad, teabevaldajad kui ka teised isikud – eesmärgiga suunata informatsioon kõigi asjaosalisteni.

Kuna selgitus- ja teavitustöö eesmärk on ennetada praktilisi probleeme ning vähendada järelevalvetegevuse ja karistusmeetmete kohaldamise mahtu, on see toonud kaasa vajaduse panustada ka inspeksiooni kui **poliitikanõustaja** ja **õigustavade kujundaja** ülesannetesse. Poliitikanõustaja ülesanne seisneb peamiselt konsultatsioonides eesmärgiga täiustada ja täpsustada õigusakte ning korraldada andmekogude loomist ja toimimist.

Õigustavade kujundaja eesmärk on juhendmaterjali koostamine ehk nn pehme õiguse loomine, mis on selgitus- ja teavitustöö oluline osa. Juhendmaterjalidel on soovituslik iseloom ja eesmärk analüüsida seaduses sätestatud üldaspekte just mingi konkreetse valdkonna probleemidest lähtuvalt. Kogu juhendmaterjal on kätte saadav inspeksiooni võrgulehel, samuti kaasneb juhendite valmimisega nende tutvustamine ja levitamine vastavates sihtgruppides, aga ka meedias, sh sotsiaalmeedias.

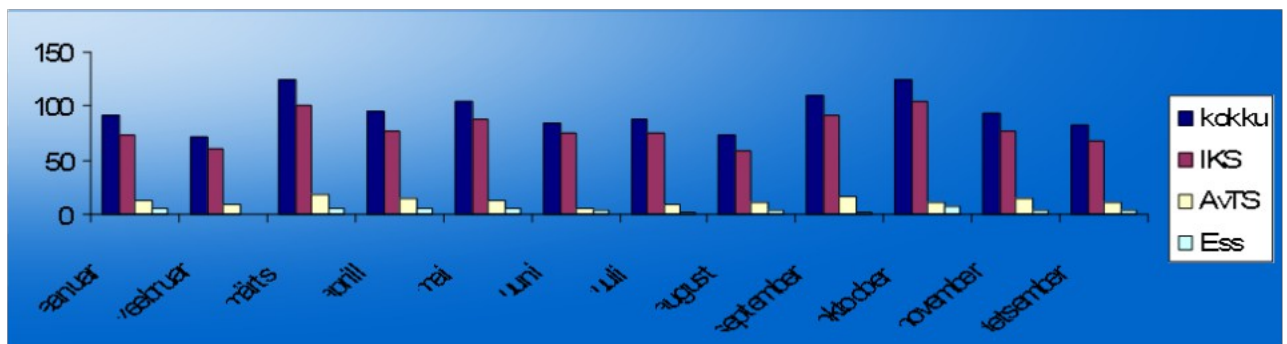
### 1.1. Selgitustaotlused

2014. aastal registreeriti Andmekaitse Inspeksioonis kokku 1144 selgitustaotlust, märgu- ja nõudekirja ning teabenõuet. See teeb 226 pöördumist vähem kui 2013. aastal, mil neid registreeriti 1370.

### 1.2. Infoliin

Alates 1. jaanuarist kuni 31. detsembrini 2014 helistati Andmekaitse Inspeksiooni infoliinile 1141 korral. Neist 1141st kõnest 947 olid seotud isikuandmete kaitse seadusega, 147 seotud avaliku teabe seadusega ja 47 helistajal oli probleeme elektroonilise side seaduse järgimisega.

Võrreldes eelmisel aastal tehtud kõnedega vähenes kõnede koguhulk 15%. Isikuandmete kaitse seaduse osakaal vähenes 19% ja avaliku teabe seadusega seotud kõnede osakaal vähenes 18%. Elektroonilise side seadusega seoses tehti 47 kõne, mis moodustab 4% kõikidest infoliini kõnedest.



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

- muud kõned – 168 kõnet (kõik muud teemad, mille lahterdamine oleks ebamõistlik),
- delikaatsete isikuandmete töötlemise register – 149 kõnet (vähenes 28 võrreldes 2013),

- c) isikuandmete avalikustamine – 148 kõnet (vähenes 36 võrreldes 2013),
- d) isikuandmed töösuhetes – 94 kõnet (vähenes 26 võrreldes 2013),
- e) salvestusseadmete kasutamine (video/foto) – 72 kõnet (vähenes 22 võrra võrreldes 2013ga),
- f) nõusoleku küsimine/andmine – 43 kõnet (vähenes 25 võrreldes 2013),
- g) võlasuhe – 40 kõnet (vähenes 11 võrreldes 2013),
- h) delikaatsete isikuandmetega seotud probleemid – 36 kõnet,
- i) andmeturbega seotud küsimused – 18 kõnet (2014 aasta II pool).

Avaliku teabe seadusega seotud arupärimiste hulgas olid kõige populaarsemad järgnevad valdkonnad:

- a) juurdepääsupiirangud – 72 kõnet (vähenes 2 kõne võrra võrreldes 2013ga),
- b) teabenõude täitmine/mitte täitmine – 51 kõnet (vähenes 22 võrra võrreldes 2013ga),
- c) kõik muu, mis puudutas AvTSi – 24 kõnet (vähenes 9 võrra võrreldes 2013ga).

Elektroonilise side seadusega seotud kõnesid tehti 47 korral ning eranditult olid kõik kõned seotud elektroonilise otsepostitusega (spämm).

Kokkuvõttes kajastatud andmete põhjal arvatati välja ka järgmised tõenäosused:

- a) infoliini kõne puudub isikuandmete kaitse küsimust – tõenäosus 83% (AvTSi tõenäosus on 13% ja ESS 4%),
- b) infoliini valveametnikule tehakse tööpäevas keskmiselt 4,5 kõnet, millest 3,74 on isikuandmete kaitse teemalised, 0,59 avaliku teabe teemalised ja 0,17 seotud elektroonilise side seadusega,
- c) kõige vähem infoliini kõnesid tehakse reedeti: 1 kõne,
- d) enim infoliini kõnesid tehakse tavaliselt esmaspäeviti ja kolmapäeviti,
- e) läinud aastal oli ühel päeval (teisipäeval) tehtud infoliini kõnede maksimumhulk 13 kõne.

### 1.3. Konverentsid ja koolitused

7. oktoobril korraldas Andmekaitse Inspeksioon Sokos Hotell Viru konverentsisaalis avaliku teabe teemalise konverentsi kohalikele omavalitsustele. Konverentsil keskenduti andmekogude määratlusele ja avaliku teabe masinloetavale taaskasutusele, teenuste kirjeldamisele asutuste võrgulehtedel, aga ka võrguvormidele ja mobiilsele internetile. Eraldi leidsid kajastamist läinud aastal inspeksiooni poolt läbi viidud kohalike omavalitsuste võrgulehtede nn valgusfooriseire tulemused. Konverentsil esinesid ettekannetega Andmekaitse Inspeksiooni peadirektor Viljar Peep, IT-nõunik Urmo Parm, Majandus- ja Kommunikatsiooniministeeriumi infoühiskonna teenuste arendamise osakonna juhataja Janek Rozov ning inspeksiooni peainspektor Elve Adamson. Konverents päädis parimate võrgulehtede haldajate tunnustamisega. Avaliku teabe konverentsiga tähistatakse traditsiooniliselt rahvusvahelist avaliku teabe päeva (*International Right To Know Day*).

2014. aasta teises pooles algasid ettevalmistused jaanuaris tähistatavale isikuandmete kaitse päevale pühendatud ürituse läbiviimiseks, mille tulemusena toimus 23. jaanuaril Riigikogu konverentsisaalis andmekaitse valdkonna asjatundjate foorum. Riigikogu põhiseaduskomisjoni esimehe patronaazi all toimunud foorumil käsitleti isikuandmete kaitse küsimusi Euroopa Liidu andmekaitse reformi kontekstis. Arutati eraelu kaitstuse ja ühiskonna turvalisuse sõlmküsimusi Euroopa Parlamendi

kriminaalvaldkonna andmekaitsedirektiivi valguses, otsekohalduvat Euroopa Liidu määrust, eraelu kaitse ja infotehnoloogilist innovatsiooni ning meedias avaldatud isikuandmete säilitamise ja kustutamise seotud probleeme. Teiste seas esinesid ettekannetega Euroopa Parlamendi liige Marju Lauristin, Justiitsministeeriumi nõunik Merili Oja, Majandus- ja Kommunikatsiooniministeeriumi asekantsler Taavi Kotka ning ajakirjanik, Tallinna Ülikooli lektor Priit Hõbemägi. Lisaks kuulati ohtralt lühisõnavõtte erinevates valdkondades isikuandmete kaitsega kokku puutuvatelt ametnikelt. Modereeris Viljar Peep.

#### **1.4. Meediasuhtlus**

2014. aasta jooksul saatis inspeksioon meediaväljaannetele kokku 36 pressiteadet, neist 12 eelteavitust, mis jõudsid meediasse valitsusasutuste nädala eelinfo paketi kaudu. Ajakirjanike kirjalikud küsimused said vastuse rohkem kui 30 korral. Erinevates väljaannetes ja meediakanalites leidis andmekaitse valdkond inspeksiooni saadetud pressiteadete või küsimustele saadetud vastuste abil kajastust 26 korral, sageli samal päeval mitmes eri väljaandes.

Lisaks on inspeksiooni ametnikud andnud pidevalt intervjuusid erinevatele tele- ja raadiokanalitele.

Läinud aasta lõpul alustas inspeksioon teavitamist olulisematest menetluslikest otsustest, mis on leitavad inspeksiooni veebilehel menetlusuudiste rubriigis (<http://www.aki.ee/et/uudised/menetlusuudised>) ja millest on juba alguse saanud nii mõnigi teemakajastus nii üleriigilises kui kohalikus meedias.

Sotsiaalmeedia kanalitest kasutab inspeksioon aktiivselt Facebooki, kus tänase seisuga on inspeksiooni konto pidevaid jälgijaid 956 (Euroopa suurimal, 360 töötajaga Briti andmekaitse asutusel *The Information Commissioner's Office*'il on FBs 1739 jälgijat), arvesse võttes tõsiasja, et Facebook kuvab postitusi konto meeldivaks tunnistanutele oma suva järgi ja kõigi inspeksiooni konto jälgijateni meie postitused ei jõua. Edukaimat postitust, mis hoiatas inimesi isikuandmeid sisaldavate dokumentide fotode jagamise eest sotsiaalmeedias, vaadati 28192 korral, jagati 364 korral.

Korraldaja või lektorina osales inspeksioon kokku 24 koolitusüritusel, millest 13 käsitlesid isikuandmete kaitse seaduse, 10 avaliku teabe seaduse ning 1 elektroonilise side seaduse valdkonda jäävaid teemasid.

## **2. Õigustavade kujundaja**

### **2.1. Juhised**

2014. aastal koostas Andmekaitse Inspeksioon neli uut juhist ning nelja varasemalt valminud juhisesse viidi sisse olulisi täiendusi.

Jaanuaris tähistas Andmekaitse Inspeksioon kaheksandat rahvusvahelist isikuandmete kaitse päeva e-äri ümarlause korraldamisega. Koostöös Tarbijakaitseameti ning Majandus- ja Kommunikatsiooniministeeriumiga läbi viidud arutelul käsitleti e-ettevõtlusega seotud teemasid: andmekaitset, infoturvet, kontaktandmete kasutamist ja tarbijakaitset. Arutus osalesid e-Kaubanduse Liit, Teenusmajanduse Koda, Pangaliit, Kaubandus-tööstuskoda, Kaupmeeste Liit, Infotehnoloogia ja Telekommunikatsiooni Liit jt. Ümarlause eesmärk oli kaardistada valdkonnas esinevad probleemid ning leppida kokku edasised ühistegevused.

Inspeksioon koolitas 2014 aastal e-kaubandusega tegelevaid ettevõtjaid kahel Tarbijakaitseameti seminaril „Suunanäitaja” ning Eesti e-kaubanduse Liidu seminaril „Kvaliteetse ja turvalise e-poe ABC”. Lisaks avaldas inspeksioon e-kaupmeestele suunatud juhendi „Turvaline e-pood”.

#### **2.1.1. Juhis: Isiklikud mobiilsed seadmed töökeskkonnas**

Juunis avaldas inspeksioon juhise „Isikliku mobiilse seadme kasutamine töökeskkonnas” soovitusetega tööandjatele ja töötajatele.

Selliste seadmete nagu nutitelefonide ja tahvelarvutite kasutamine on muutunud väga populaarseks. Seadmete pakutavad võimalused ja nende suutlikkus on märgatavalt suurenenud. Tööandjad puutuvad üha rohkem kokku nii tööle asuvate kui olemasolevate töötajate sooviga kasutada isiklikus omanduses olevaid seadmeid töökeskkonnas igapäevatöö tegemiseks sh tööandja teabele juurdepääsuks, selle salvestamiseks kui ka töötlemiseks. Kui tööandja lubab isiklike seadmetega töödelda organisatsioonis hoitavaid isikuandmeid, tekib mitmeid küsimusi, mida tööandjal kui isikuandmete vastutaval töötajal tuleb lahendada. Vastutavale töötajale peab alati jääma kontrolli tema vastutuse alla kuuluvate isikuandmete üle, olenemata isikuandmete töötlemisel kasutatava seadme omanikust.

Juhis aitab nii tööandjatel kui töötajatel mõista oma kohustusi ja edendada häid tavasid. Juhis annab selgitusi ja soovitusi, mida tuleb arvestada, kui tööandja lubab töötajatel kasutada isiklike seadmeid organisatsiooni vastutusalasse kuuluvate isikuandmete töötlemisel.

#### **2.1.2. Juhis: Infoturbe ja isikuandmete kaitse väikeettevõttes**

Augustis avaldatud juhise „Infoturbe ja isikuandmete kaitse väikeettevõttes” on mõeldud väikeettevõtjate teadlikkuse tõstmiseks. Ettevõtte andmehalduse ja infosüsteemide turvalisuse tagamine nõuab aega, ressursse ja eriteadmisi. Olgu andmed kas laua- või sülearvutis, võrguserveris, pilves, mobiilses seadmes (nutitelefon, tahvelarvuti), võrgulehel, e-posti serveris või paber kandjal – kõiki neid andmeid on vaja kaitsta. Kui ettevõtte töötleb isikuandmeid, siis vastutab ettevõtte lisaks ka nende inimeste ees, kelle andmed tal on. Isikuandmete korral peab ettevõtte teadma seadusest tulenevaid nõudeid.

Juhisega anname ettevõtte juhtidele, infoturbe- ja IT-spetsialistidele abistavaid soovitusi isikuandmete kaitse ja infoturbe korraldamiseks ning tegevuste planeerimiseks.

#### **2.1.3. Juhis: Isikuandmete kustutamine seadmetes**

Tänapäeval on igapäevaelu lahutamatuks kaaslasteks erinevad seadmed, mis sisaldavad hulgaliselt andmeid meie eraelu kohta. Olgu selleks kas laua- või sülearvuti, nutiseadmed (nutitelefon, tahvelarvuti, navigatsiooniseade, „käed-vabad” autoseade) või fotokaamera. Kõik need seadmed kannavad endas vähemal või suuremal määral meie isikuandmeid.

Tehnoloogia kiire areng tähendab lisaks arvukatele seadmetele ka seda, et me vahetame neid seadmeid välja kiiremini kui kunagi varem. Kui kasutaja soovib oma seadet müüa või taaskasutusse

anda, on ülimalt oluline tagada, et uuele omanikule ei läheks seadmega kaasa eelmise omaniku eraelulised andmed nagu e-kirjad, kontaktid, sõnumid, pildid või kõnelogid.

Oktoobris avaldatud juhisega „Isikuandmete kustutamine seadmetes” annab inspeksioon soovitusi seadmete igapäevakasutajatele. Milliseid toiminguid peaks seadme omanik andmete sh isikuandmete kustutamiseks enne seadme müümist või taaskasutusse andmist tegema.

#### **2.1.4. Juhis: Turvaline e-pood**

Eelmisel aastal oli inspeksiooni fookuses e-äri ja väikeettevõtlus. Jaanuaris toimunud e-äri ümarlaua järeltegevusena avaldasime novembris e-kaubandusega tegelevatele ettevõtjatele juhise „Turvaline e-pood”.

Inspeksioon senine praktika on näidanud, et e-kaupmehed eelistavad hinna tõttu pigem valmis IT-lahendusi ja nn karbitooteid kui kallimaid erilahendusi. Valmis lahenduse puhul pole aga alati kindlust, kas see vastab e-poe vajadustele ning tagab isikuandmete töötlemisel seaduse nõuete täitmise.

Juhisega anname selgitusi, milliseid seadustest tulenevaid nõudeid peab e-kaupmees järgima turvaliseks isikuandmete töötlemiseks e-poes tarbijaga seotud ostutoimingul.

#### **2.1.5. Avaliku teabe seaduse üldjuhendi avaliku teabe masinloetava taaskasutamise osa**

Andmekaitse Inspeksioon koostas 2010. aastal avaliku teabe seaduse üldjuhendi, mille eesmärgiks on aidata selgitada avaliku teabe seadusest tulenevaid nõudeid. Kuna aega-ajalt muutuvad nii seadused kui halduspraktika, siis on eelnimetatud juhendi näol tegemist nn elava dokumendiga, mida inspeksioon on püüdnud hoida ajakohasena ning vajadusel lisanud juhisesse uusi peatükke. Nii täiendati 2014. aastal juhendit peatükiga "Avaliku teabe masinloetav taaskasutamine".

Nimetatud peatüki lisamise vajadus tekkis asjaolust, et alates 01.01.2015 hakkas kehtima avaliku teabe seaduse säte, mis kohustas teabevaldajaid võimaldama nende valduses oleva teabe taaskasutamist ja allalaadimist tervikliku andmekogumina masinloetaval kujul. Masinloetava taaskasutuse mõisted ja nõuded on avaliku teabe seadusesse (AvTS) üle võetud avaliku sektori valduses oleva teabe taaskasutamise direktiivist 2003/98/EÜ (koos täiendusega 2013/37/EL).

Juhisesse lisatud peatükis on välja toodud olulisemad punktid, millele tuleks tähelepanu pöörata enne, kui anda mingid andmed masinloetaval kujul taaskasutusse. Samuti on eelnimetatud peatükis selgitatud, kust saab täiendavaid tehnilisi juhiseid ning millisel juhul võib masinloetavusest kõrvale kalduda. Ühtlasi on juhitud teabevaldajate tähelepanu ka asjaolule, et enne teabe masinloetavasse taaskasutusse andmist tuleb arvestada ka isikuandmete töötlemise nõuetega.

Juhises soovitab inspeksioon teabevaldajatel enne isikuandmeid sisaldada võiva teabe masinloetavat avalikustamist läbi viia eraelu riive mõjude hindamine. Seda nii seniste andmete kättesaadavaks tegemisel kui uute infosüsteemide loomisel ja e-teenuste kavandamisel. Juhises on inspeksioon leidnud, et riskide hindamisel ei saa arvestada tavapärase taaskasutamise (näiteks teabe väljastamisel teabenõude korral või formaadis mis ei võimalda masinloetavat taaskasutust). Mõjude hindamise tuleb üle vaadata nii isikuandmete töötlemise õiguslik alus, kui ka see, kas avalikustamine vastab isikuandmete minimaalsuse põhimõtetele. Seda nii sisulise kui ajalise ulatuse osas. Teavet, mis on vananenud või mille avalikustamistähtaeg on ületatud, ei tohi enam kättesaadavana hoida – eriti isikuandmeid. Vajadusel tuleb ka säilitus- ja avalikustamistähtajad üle vaadata.

Lisaks avaliku teabe seaduse üldjuhendile täiendati veel Andmekaitse Inspeksiooni menetluskorda riigi infosüsteemi haldussüsteemis (RIHA), juhust isikuandmete edastamise kohta välisriiki ning juhust isikuandmete töötlemise kohta töösuhetes.

## 2.2. Rahvusvaheline koostöö

### 2.2.1. Euroopa andmekaitseasutuste töörühm

Andmekaitse direktiivi 46/95/EÜ artikli 29 alusel moodustatud [Euroopa andmekaitseasutuste töörühm](#) koosneb liikmesriikide andmekaitseasutuste juhtidest või nende esindajaist, Euroopa Liidu institutsioonide andmekaitsega tegelevast Euroopa andmekaitseinspektorist ning Euroopa Komisjoni esindajaist. Sõnaõigusega osalevad veel 7 Euroopa riigi andmekaitsejuhid. Töörühm koguneb täiskogu tasemel 5 korda aastas, teemasid valmistavad ette liikmesasutuste ekspertidest alamtöörühmad. Euroopa Komisjoni andmekaitseüksus täidab töörühma sekretariaadi ülesandeid.

Keskne tegevus, mis meie hinnangul ületab 90% töörühma töömahust, on juhendiloomine. Olulisemate 2014. aastal vastuvõetud ühisarvamustena võib välja tuua:

- põhjalik [töödokument elektroonilise side jälgimise kohta luure ja riikliku julgeoleku eesmärgil \(ingl. k\)](#), samuti samas asjas eelnevalt koostatud [arvamus 04/2014 \(eesti k\)](#),
- [juhised Google'i Hispaania tütarühingu ning Hispaania andmekaitseasutuse ja Mario Costeja Gonzalezi kohtuasjas tehtud Euroopa Liidu Kohtu otsuse täitmise kohta \(ingl. k\)](#),
- [arvamus 09/2014 direktiivi 2002/58/EÜ kohaldamisest seadmete tekitatud jälgede kohta \[device fingerprinting\] \(ingl. k\)](#),
- [arvamus 08/2014 värsketest arengutest asjade internetis \[värkvõrgus\] \(ingl. k\)](#),
- [arvamus 05/2014 anonüümimistehnikate kohta \(eesti k\)](#),
- [arvamus 03/2014 isikuandmetega seotud rikkumistest teatamise kohta \(eesti k\)](#),
- [arvamus 01/2014 vajalikkuse ja proportsionaalsuse põhimõtete kohaldamise ja isikuandmete kaitse kohta õiguskaitse sektoris \(eesti k\)](#).

2013. a. oktoobris toimunud töörühma täiskogul tegi Eesti andmekaitse inspeksiooni peadirektor ettepaneku lisaks juhendiloomele tuua püsivalt täiskogu päevakorda praktiline koostöö temaatika.

Juhendiloomele keskendunud tegevus meenutab poolparlamentlikku tegevust ning töörühma tase „pehme õigusloome” on kõrgelt hinnatud. Selle kõrval peaksid korrapäraselt kohtuvad asutuste juhid pöörama tähelepanu ka praktilisele piiriülesele koostööle.

Paraku on praktiline koostöö – kui ad hoc reageerimised kõrvale jätta – seni jäänud kas töörühma tasemest allapoole (nt naaberriikide vaheline koostöö, sh Balti ühisauditid) või ülespoole (sh nt Globaalse Eraelu Kaitse Võrgustikku ühinenud andmekaitseasutuste järelevalve-alane infoplatvorm, igakevadised „Interneti luudamise päevad” ning koostöö-alased telefonikonverentsid).

Piiriülese koostöö praktilised [soovitused](#) ja ametiabi taotlemise vormi on välja töötanud küll Majandusarengu- ja Koostöö Organisatsioon (OECD), kuid mitte pea 20 aastat ühise õigusraamistiku (andmekaitse direktiivi) põhjal tegutsenud Euroopa andmekaitseasutuste töörühm.

2013. aasta lõpus Eesti ja Ühendkuningriigi andmekaitseasutuse läbiviidud küsitluse põhjal tutvustati töörühmas 2014. aastal kogutud võrdlevat ülevaadet ja häid praktikaid andmekaitseasutuste tegevuse korraldamisel:

- omaalgatusliku tegevuse osakaalu ning rikkumistele reageerimiste paindlikkust,
- riigisisest koostööd teiste asutustega,
- piiriülest koostööd andmekaitseasutuste vahel.

Järgnevalt soovitas Eesti andmekaitseasutus tegeleda andmekaitseasutuste pädevuste, tegevuste ja statistika täiealatusliku võrdleva kaardistamisega. Kuigi andmekaitse õigusraamistik on kõigile üks (direktiiv), on menetlusõigus ja andmekaitseasutuste menetluslik „tööriistakast” liikmesriigiti väga erinev.

Tihti märgitakse üht ja sama tegevust erineva sõnaga, mõnikord tähistab sama termin täiesti erinevaid tegevusi, vahel takerdub piiriülene koostöö esmapilgul ebaolulistesse piasjasjadesse (mõnes riigis on andmekaitseauditi tulemused avalikud, mõnes võib neid avaldada vaid auditeeritava nõusolekul). Komisjoni kogutav tööühma statistika on oma sisult väärtusetu.

Koostöö planeerimiseks on vaja võrreldavat ülevaadet. Eesti andmekaitseasutus koostas [oma võrgulehel 2014. a. avaldatud küsitluse](#) abil andmekaitseasutuste pädevuste, tegevuste ja statistika tüpologia. Selle arutamine ja võimaliku võrdlusstandardina kaalumise jätkus 2015. aastal.

### **2.2.2. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni nõuandekomitee**

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.

Konventsiooni nõuandva komitee 31. täiskogu istung peeti Strasbourgis, 2.-4. juunil 2014. Toimus eelnõu soovitus liikmesriikidele tööhõiveotstarbel kasutatavate isikuandmete kaitse kohta teine lugemine. Sekretariaati volitati andma eelnõu üle meedia ja infoühiskonna Juhtkomiteele eesmärgiga see edastada Ministrite Komiteele vastuvõtmiseks.

### **2.2.3. Telekommunikatsioonialane andmekaitse tööühm**

Telekommunikatsioonialane rahvusvaheline andmekaitse tööühm (IWGDPT) tegutseb isikuandmete töötlemise põhimõtete analüüsi ja selgitustööga telekommunikatsiooni ning tehnoloogia valdkonnas. Aastas korraldatakse kaks töökohtumist. 2014 kevadisel tööühma koosolekul võeti vastu töödokument *Working Paper on Big data and privacy, Privacy principles under pressure in the age of Big Data analytics*. Dokument kirjeldab nn suurandmete (*big data*) olemust ning seda, kes ning millistel alustel tohib neid andmeid töödelda. Mida silmas pidada, et andmete töötlemisel oleks tagatud eraelu puutumatus.

Sügisel tööühma kohtumisel võeti vastu dokument *Working Paper on Privacy and Security Risks with the Use of „Own Devices” in Corporate Networks*. Tänapäeval puutuvad tööandjad üha rohkem kokku nii tööle asuvate kui olemasolevate töötajate sooviga kasutada isiklikus omanduses olevaid seadmeid töökeskkonnas igapäevatöö tegemiseks sh tööandja teabele juurdepääsuks, selle salvestamiseks kui ka töötlemiseks. Kui tööandja lubab isiklike seadmetega töödelda organisatsiooni hoitavaid isikuandmeid, tekib mitmeid küsimusi, mida tööandjal kui isikuandmete vastutaval töötlejal tuleb lahendada, et täita isikuandmete kaitse nõudeid. Vastutavale töötlejale peab alati jääma kontroll tema vastutuse alla kuuluvate isikuandmete üle, olenemata isikuandmete töötlemisel kasutatava seadme omanikust. Tööühm annab dokumendiga rida soovitusi, mis aitavad ettevõtjal infosüsteemide ja äriteabe turvalisust paremini tagada, kui andmetöötluseks lubatakse kasutada töötajate isiklike nutiseadmeid.



### 3. Poliitikanõustaja

#### 3.1. Arvamused õigusaktide eelnõudele

Arvamuste avaldamine õigusaktide eelnõudele moodustab olulise osa poliitikanõustaja tegevustest. 2014. aastal avaldasime arvamust erinevate õigusaktide eelnõudele 28 korral, millest 14 juhul oli tegemist isikuandmete kaitse valdkonnaga ning sama palju avaliku teabe valdkonnaga.

Õigusaktide eelnõude vastavust nõuetele analüüsib inspeksioon ühtlasi riigi andmekogude kooskõlastamismenetluse raames. Andmekogude kooskõlastamist käsitletakse lähemalt loamenetluste peatükis.

Alljärgnevalt peatume Andmekaitse Inspeksiooni hinnangul enim tähelepanu väärinud eelnõudel, mille osas inspeksioon arvamust avaldas.

##### 3.1.1. Arvamuse avaldamine [elektroonilise side seaduse ja infoühiskonna teenuse seaduse muutmise seaduse eelnõu kohta](#)

Eelnõu kohaselt nähti ette eelneva nõusoleku küsimise nõue teabe saamiseks või juurdepääsu loomiseks teenuse kasutaja terminalseadmesse juba salvestatud teabele.

Leidsime, et küpsiste kasutamiseks vajaliku isikuandmete kaitse seaduse § 12 kohase nõusoleku kehtestamine toob isikute eraelu puutumatus kaitsmise asemel kaasa hoopis selle põhiõiguse intensiivsema riive. Teenuse kasutaja külastab enamiku ajast erinevaid võrgulehti sisuliselt anonüümselt. Teenuse osutajal puudub üldjuhul teadmine, kes konkreetselt on see kasutaja, kes seadet veebilehitsemiseks kasutab. Tõsi, teenuse osutajale saavad teatavaks teatud andmed teenuse osutamisest tingituna, kuid teenuse osutaja ei tuvasta üldjuhul konkreetset isikut, kes parasjagu võrgulehte külastab.<sup>1</sup> Olukorras, kus teenuse kasutaja peaks taolisel juhul võtma kasutajalt isikuandmete kaitse seaduse § 12 kohase nõusoleku, toob see kasutaja eraelu puutumatus kaitsmise asemel kaasa täiendava riive: teenuse osutaja peab hakkama tuvastama neid kasutajaid, kes võrgulehti külastavad. Arvestades, et iga võrgulehe külastada nõusolek peab olema kirjalikku taasesitamist võimaldavas vormis ja vajadust nõusolekuid säilitada, et vaidluse korral nõusoleku olemasolu tõendada, toovad niisugused nõuded kaasa ka ulatusliku sekkumise teenuse osutaja õigustesse. On küsitav, kas teenuse osutajatel on tegelik valmisolek ja ressursid nende tingimuste täitmiseks olemas.

Alternatiivselt palusime kaaluda nõusoleku nõude kehtestamise asemel kasutajate piisava teavitamise meetet või teabe kogumisest keeldumise avaldamise lihtsamat meetet, kus kasutaja tuvastamine isikuandmete kaitse seaduse mõttes ei oleks vajalik.

Tulemus – eelnõu jäi algatamata.

##### 3.1.2. Arvamuse avaldamine elektroonilise side seaduse muutmise ettepanekute kohta

Eelnõu eesmärk oli piirata soovimatuid otseturustuse huvides tehtavaid telefonikõnesid ja võimaldada isikul otsustada, kas ta soovib otseturustuslikke kõnesid saada või mitte ning vastava teabe kandmine riiklikusse numbrini broneerimise andmekogusse (NBA).

Keskne probleem oli järelevalvemeetmete rakendamine. Alustades sellest, kuidas tõendada otseturustuslikku komponenti häälkõne teel edastatud teabe puhul, sest regulatsioon puudutab kontaktandmete kasutamist just otseturustuslikul eesmärgil. Seega peab järelevalveasutusel olema

---

<sup>1</sup> Välja arvatud näiteks autentimise küpsised, mis võimaldavad võrgulehel meeles pidada kasutaja tehtud valikuid (näiteks nimi, keel või piirkond). Neid küpsiseid kasutavad võrgulehed näiteks sisse logitud kasutaja identifitseerimiseks (internetipanganduse võrgulehel), kasutajad saavad end järjestikuste võrgulehtede külastuste käigus autentida ning ligi pääseda sisule, nagu konto saldo, ülekanded jne. Autentimise küpsised on enamasti ajutised küpsised.

võimalus kontrollida, millist liiki teavet sidevahendi kaudu edastati. Kui ettevõtja reklaamib oma tooteid e-posti teel, jääb saadetud otseturustuslikust teatest maha jälg. Otseturustusliku teate edastamist tõendab isiku e-postkasti saabunud e-kiri, mille otseturustuslikku olemust (kas teade on suunatud edendama toodete või teenuste pakkumist) saab järelevalveasutus hinnata. Kui aga otseturustust tehakse telefoni teel, ei ole võimalik tagantjärele tõendada, millest helistaja rääkis.

Problemaatiline on ka helistaja kindlakstegemine. Seda põhjusel, et helistaja ei pruugi esitada kliendile täpseid andmeid ettevõtja kohta, kelle nimel otseturustust tehakse. Samuti, kuna otseturustuslik kõne võib saabuda ootamatult, ei pruugi klient isegi kaebust kirjutama hakates mäletada, kust talle helistati. Isegi, kui kliendil on telefoni kõnelogide all alles telefoni number, kust talle helistati, ei anna see garantiid, et järelevalveasutusel õnnestub jõuda tegeliku otseturustajani. Telefonikõnesid on võimalik teha ka päris anonüümselt helistaja numbrit näitamata.

Palusime enne muudatuste planeerimist seadusandluses kaaluda, kas muudatuste tegemine on ilmingimata vajalik. Õiguslik regulatsioon peab olema vajalik ja inimestele arusaadav, nende alusel toimuv menetlus peab olema omakorda teostatav. Ülereguleerimine ähmastab õigusselgust. Ebapraktiline regulatsioon suurendab põhjendamatult järelevalveasutuse halduskulusid ja ei suuda samas vastata ühiskonna tegelikele ootustele.

Avaldasime arvamust, et soovimatuid otseturustuslikke häälkõnesid aitaks eelkõige vähendada asjakohase hea tava välja töötamine ning nende aktsepteerimine otseturustuslike telefonikõnede tegijate endi poolt.

Tulemus – eelnõu jäi algatamata.

### **3.1.3. Arvamuse avaldamine [julgeoleku- ja taustakontrolli seaduse eelnõu](#) kohta**

Eelnõu eesmärk oli tagada riigi julgeoleku ja riigisaladuse ning salastatud välisteabe kaitse ja isikute põhiõiguste ning vabaduste kaitse taustakontrolli ja julgeolekukontrolli menetluses selle aluste ning korra sätestamise kaudu.

Andmekaitse Inspektsioon esitas hulganisti erinevaid märkusi.

Oluliseks ebakõlaks pidasime lisaks seaduse alusel toimuvale isikuandmete töötlemisele nõusolekupõhise isikuandmete töötlemise õiguse kehtestamist. Kusjuures meie hinnangul ei vastanud eelnõus kirjeldatud nõusolek isikuandmete kaitse seaduse § 12 kohase nõusoleku (eelkõige vabatahtlikkuse printsiibi) tingimustele, kuna sellest sõltub isiku teenistusse võtmine või teenistusest vabastamine. Avaliku ülesande täitmiseks peab isikuandmete töötlemine olema võimalik sõltumata andmesubjekti tahtest.

Ühtlasi jäi arusaamatuks, milliseid konkreetseid isikuid võib taustakontrollile allutada, sest õigus teostada taustakontrolli põhjendatud vajaduse korral on liiga ebamäärane kirjeldus. Avara tõlgendamise korral saaks eeldada taustakontrolli läbiviimise lubatavust iga ametiasutuse ametniku või töötaja suhtes. Palusime õigusselguse põhimõttele tuginedes täpsemalt välja tuua, kes on need andmesubjektid, kelle õigusi võidakse riivata ning millised konkreetsete kaalutlused selleks peavad esinema. Ühtlasi olime kahtlevad, kas kõik andmed, mida isikute kohta soovitakse koguda, on eesmärgi saavutamiseks vajalikud ning kas samade andmete kogumine on põhjendatud kõigi isikute suhtes. Leidsime, et alluvate delikaatsete isikuandmete töötlemiseks peab esinema ümberlükkamatu põhjus ja reaalne vajadus.

Eelnõuga nähti ette taustakontrolli teostamise õigus laiale asutuste ringile. Leidsime, et ei ole põhjendatud olukord, kus erinevalt erasektorist võib ametiasutus koguda alluvate kohta hulganisti tundlikke andmeid. Ühest küljest riivab taoliste andmete avaldamine asutuse personaliosakonnale tugevalt andmesubjekti privaatsust, kuid teisalt võib taoline protseduuri ülesehitus tingida valeandmete esitamise vaid ainuüksi seetõttu, et ametiisik ei soovi oma delikaatseid andmeid

personalispetsialistile usaldada. See omakorda toob kaasa kogutud andmete kvaliteediprobleemi, sest need ei vasta tegelikkusele. Palusime vähemalt piiritleda isikute ringi, kes võivad andmetega kokku puutuda. Meie arvates on ka küsitav, kas iga valitsusasutus on pädev iseseisvalt ohtu riigi julgeolekule adekvaatselt hindama.

Tulemus – eelnõu jäi algatamata, osad sätted tõsteti ümber kaitseväeteenistuse seaduse muutmise seadusesse.

#### **3.1.4. Arvamuse avaldamine [avaliku teabe seaduse, elektroonilise side seaduse ja isikuandmete kaitse seaduse muutmise seaduse eelnõu kohta](#)**

Eelnõu eesmärk oli reguleerida avaliku teabe taaskasutamise nõuded ning lahendada praktilised kitsaskohad, mis on avaliku teabe seaduse, elektroonilise side seaduse ja isikuandmete kaitse seaduse nõuete täitmise üle järelevalve teostamisel esile kerkinud. Eelnõu valmis Justiitsministeeriumil koostöös Andmekaitse Inspektsiooniga.

Eelnõu sisaldab muudatusi, mille kohaselt ei saa haldusorgan olla teabenõudjaks. Avaliku teabe saamise õigus on tuletatud Eesti Vabariigi põhiseaduse §-s 44 sätestatud üldisest informatsiooniõigusest. Nii nagu mitmed teisedki põhiõigused, on ka informatsiooniõigus igapäevane õigus, subjektiivne põhiõigus, mille kandjaks võib olla nii füüsiline kui juriidiline isik. Põhiõiguste kaitse ei laiene aga riigile ega muudele avalik-õiguslikele juriidilistele isikutele. Seni on ette tulnud juhtumeid, kus asutused on end ekslikult pidanud teabenõudjaks.

Täiendavalt juhtisime tähelepanu, et karistusseadustiku § 279 tuleks täiendada ja näha ette selle kohaldamise võimalus ka haldusjärelevalve menetluse puhul. Kuigi riikliku järelevalvemenetluse korral on asutusel võimalik menetluse läbiviimist takistavat isikut korrale kutsuda mitmete haldus- või järelevalve meetmete kaudu, esineb juhtumeid, kus need meetmed ei ole enam tõhusad – nt kui järelevalve teostamise käigus järelevalveks vajalikud dokumendid nende kontrollimise vältimiseks hävitatakse. Kui dokumendid olid sellised, mida ei saa taastada, ei ole enam abi ka ettekirjutusest vm haldussunnist. Seetõttu tuleks niisugusteks eriolukordadeks ette näha väärtekoosseis ka haldusjärelevalve takistamise eest, mis lubaks karistada teo toime pannud füüsilist isikut, kes vastavate nõuete täitmise eest haldusorganis vastutab.

Tulemus - eelnõu sai valmis, kuid jäi Riigikogu valmiste tõttu algatamata.

#### **3.1.5. Arvamuse avaldamine [kohaliku omavalitsuse korralduse seaduse § 6 täiendamise seaduse eelnõu ja selle rakendusakti kavandi kohta](#)**

Eelnõuga sooviti sätestada kohalikele omavalitsustele senisest selgem volitusnorm andmekogude asutamiseks.

Andmekaitse Inspektsioon esitas hulganisti sisulisi ja formaalseid ettepanekuid. Eelnõus ei olnud selge, milliseid ülesandeid on õigus täita kohalikul omavalitsusel ja milliseid ülesandeid on õigus täita regionaalministril. Leidsime, et kohaliku omavalitsuse korralduse seaduse § 6 lg-s 1 sätestatud avalikke ülesandeid on õigus täita üksnes omavalitsusel endal ja regionaalministrile saab jääda toetav funktsioon.

Ühtlasi märkisime, et kui kohalik omavalitsus täidab riigi poolt pandud avalikku ülesannet, peaks ülesande täitmiseks vajaliku andmekogu asutamine olema samuti ette nähtud seaduses. Kui aga omavalitsus tegeleb kohaliku elu küsimusega, siis sõltub andmekogu asutamise volitusnormi vajalikkus sellest, kas andmekogu loomine toob kaasa põhiõiguste riive või mitte. Arvestades, et andmekogud sisaldavad enamikel juhtudel isikuandmeid, mis toob kaasa privaatsusõiguse riive, eeldab andmekogu asutamine reeglina vastavat volitusnormi seaduse tasemel. Kusjuures andmekogu asutamise eesmärk peab volitusnormis olema piisavalt konkreetne.

Tulemus – eelnõu arutelu lõpetati, eelnõu langes Riigikogu menetlusest välja. Siseministeerium lahendas asja inspektsiooni soovitude kohaselt standard-tarkvaralahendusena.

### **3.2. Koordinaatorite võrgustik**

Isikuandmete kaitse ja teabe avalikustamise koordinaator on riigiasutuses see inimene, kes korraldab asutuse olevate dokumentide avalikustamist ja neis dokumentides sisalduvate isikuandmete kaitset. Kohustus selline inimene määrata tuleneb Vabariigi Valitsuse määrusest „Asjaajamiskorra ühtsed alused”.

Omavalitsuses täidab koordinaatori kohustusi sisuliselt valla- või linnasekretär. Kui eelnevatel aastatel on inspeksioon pööranud suuremat tähelepanu just riigiasutuste koordinaatoritele, siis 2014. aastal otsustati üks üritus teha ka valla- ja linnasekretäridele.

2014. aastal valla- ja linnasekretäridele korraldatud ürituse ühitasime omavalitsute seire tulemuste avalikustamisega, mis andis võimaluse ka läbi rääkida seires leitud puudused ja millele teabe avalikustamisel võrgulehel tuleks rohkem tähelepanu pöörata. Valla- ja linnasekretäridelt saadud positiivsest tagasisidest nähtub, et selliste ürituste korraldamine on küll vajalik, kuid mis ei ole just lihtne, kuna omavalitsuste arv on suur.

Ka koordinaatoritelt saadud tagasisidest nähtub, et selliste ürituste korraldamine on vajalik, kuna selle käigus juhitakse tähelepanu kitsaskohtadele, saab esitada küsimusi ja arutada probleeme kolleegidega ning vahetada kogemusi. Järjest on kasvanud ka huvi nendel üritustel osalemise vastu.

### **3.3. Statistikanõukogu**

Statistikanõukogu läinud aasta üheks olulisimaks teemavaldkonnaks, millele suurt tähelepanu pöörati, oli 2020.aasta registritepõhise rahva ja eluruumide loenduse projekt. Ühe probleemina käsitleti registritesse kantud elukoha andmete sagedast mitte vastavust tegelikule elukohale. Samuti tuleb Statistikaametil jätkata tööd, et loenduse andmetele tuginedes saaks koostada aegridu nende andmete põhjal, mida on küsitud kõikidel rahvaloendustel. Kindlasti tuleks kaasata andmekogude täienduste või uuenduste prioretiseerimisel Statistikaameti spetsialiste ja tähtsustada nii Statistikaameti statistikatööde kui ka teiste asutuste registriandmete digitaalsete andmete arhiveerimist kujul, mis võimaldab nende töötlemise ka aastate pärast.

## 4. Järelevalvaja

### 4.1. Isikuandmete kaitse

Enamik inspektsiooni jõudvatest kaebustest ja väärteoteadetest kuuluvad isikuandmete kaitse valdkonda. Valdavalt on pöördujaks isik, kelle õigusi isikuandmete töötlemisel on rikutud. Olenevalt pöördumiste eesmärkidest ja kaasuste asjaoludest, valib inspeksioon välja optimaalse ja põhjendatud reageerimismeetodi, kas rakendada järelevalve või väärteomenetlust, kusjuures üks ei välista teist. Avaliku menetlushuvi puudumisel jätab inspektsioon menetluse algatamata.

#### 4.1.1. Isikuandmete kaitse töösuhetes

Töösuhete osas on kaebuste arv vähenenud pärast inspektsiooni koostatud mahukat juhendit isikuandmete töötlemisest töösuhetes. Kaebuste peamiseks põhjuseks on endiste töötajate isikunimeliste aadresside jätkuv kasutamine pärast töösuhte lõppemist. Isikuandmete kaitse seadusest lähtuvalt peab töötaja e-posti pärast töösuhte lõppemist järgmisest päevast koheselt sulgema, kui isik just ise ei anna nõusolekut teha seda hiljem. Praktikast see aga nii korrektselt ei toimi.

Inspektsioon tegi näiteks Instigo Arsenal OÜle ettekirjutuse endise töötaja kontaktandmete võrgulehelt eemaldamiseks, isikunimelise Skype'i konto töötlemise lõpetamiseks ja isikunimelise e-postiaadressi sulgemiseks. Sarnane ettekirjutus tehti ka ISS Eesti AS-ile. Samas teemas lõpetati pärast inspektsiooni sekkumist endiste töötajate e-posti aadresside töötlemine Megaron-E AS-is ja Nordcity Center OÜs.

Nimetatud menetluste raames pöördus inspektsioon ka RIKi poole, et selgitada välja, kas elektronposti aadressi saab samaaegselt sulgeda ja kasutada nt ise loodavad automaatteavitust, mis postiaadressilt saatjale tagasi saadetakse. RIKi vastuse kohaselt sõltub administraatorist, kas kiri säilitatakse või mitte. Sellest tulenevalt muutis inspektsioon oma tööõiguslikku juhist, kuna soovitus genereerida ise vormindatud vastus ei ole praegusel hetkel toimiv lahendus ja suue tõenäosusega ei saa sellega garanteerida, et aadress on kustutatud.

Andmekaitse Inspektsioon kontrollis saadud vihjete alusel turvakaamerate kasutamise eesmärgikohasuse, minimaalsuse ja kasutuse piiramise rakendamist Trans Chemicals OÜ-s (pakke-, kate- ja termokilet ning kilekotte tootev ettevõtte) ja Saint-Gobain Glass Estonia SE Tartu tehases (klaaspakette tootev ettevõtte).

Inspektsioon kontrollis kumbagi ettevõtet kohapeal. Uuriti, kuidas teavitatakse videovalve kasutamisest, kuidas on kaamerad paigutatud, mis eesmärgil neid kasutatakse, kuidas on see reguleeritud töökorralduse reeglites jm dokumentides ning kuidas tagatakse isikuandmete turvaline hoidmine.

Trans Chemicals OÜ-s olid kaamerad paigutatud tootmisruumidesse, territooriumi valveks alles planeeriti nende paigaldamist. Videovalve kasutamisest teavitasid ruumidesse sisenejaid ustel olevad sildid, millel oli ka viide kaamerate omanikule, vastutava isiku nimi ja telefoninumber. Kaamerate kasutamine oli reguleeritud töö sisekorraeskirjades, millega võib tutvuda tootmisruumi seinal oleval stendil. Jälgimissüsteemi kasutamise faktist, kohast ja eesmärgist teavitatakse töötajaid töölepingus ja selle lisaks olevas ametijuhendis. Kaamerate kasutamise eesmärgiks on isikute ja vara kaitse, tööohutuse, tööprotsessi katkematus ja tööaja optimaalse kasutamise jälgimine. Ligipääs salvestistele on kaitstud paroolidega ning salvestisi säilitatakse serveriteenust pakkuvas ettevõttes. Kuna salvestiste hoidmise tähtaega ei olnud üheski dokumendis reguleeritud, soovitas inspektsioon analüüsida, kui kaua on neid eesmärkide saavutamiseks vaja säilitada ning kehtestada konkreetsed tähtajad.

Kuna ettevõttes ei tuvastatud isikuandmete kaitse seaduse nõuete rikkumist, lõpetas inspektsioon riikliku järelevalvemenetluse.

Saint-Gobain Glass Estonia SE Tartu tehases olid tootmisruumidesse ja territooriumile kaamerad paigutatud eesmärgiga jälgida tööprotsessi isikute ja vara kaitseks. Kaamerad kuulusid ettevõttele,

serveriteenus ostetakse sisse. Kaamerate kasutamine oli reguleeritud töökorralduse eeskirjades, mida tutvustati töötajatele tööle asumisel. Lisaks sellele oli isikuandmete töötlemine reguleeritud töölepingu lisaks olevas isikuandmete töötlemise infolehes ja töötaja nõusolekus. Hoonesse sisenejat teavitas videojärelevalvest vastav silt uksele.

Kaamerapilti ei jälgitud reaajas, salvestisi vaadati ainult vajaduse tekkimisel (toodangu purunemise või õnnetuse põhjuste selgitamiseks). Salvestisi hoitakse serveris umbes kaks nädalat, misjärel need kirjutatakse uuesti üle.

Kuna ettevõttes ei tuvastatud isikuandmete kaitse seaduse nõuete rikkumist, lõpetas inspeksioon riikliku järelevalvemenetluse.

#### **4.1.2. Isikuandmete töötlemine suhtluskeskkondades**

Enamik kaebusi puudutas Facebooki keskkonnas avaldatavat laimu. Neist umbes pooled suunas inspeksioon tsiviilvaidlusteks kohtusse.

Näiteid:

Kodanik kaebas, et Facebookis on tehtud tema fotodega suvalist nime kasutades libakonto. Kaebaja kahtlustas, et konto on teinud ja fotod avalikustanud endine abikaasa. Inspeksioon alustas riiklikku järelevalvemenetlust, mille käigus tegi endisele abikaasale järelepärimised, millele ei vastatud. Edasine avalikustamine siiski lõpetati, mistõttu sai menetluse lõpetada.

Kodanik kaebas blogis (<http://tonusamuel.blogspot.com/>) avaldatu peale. Kaebus jäeti rahuldamata, kuna isiku kohta on samad andmed leitavad mujal meedias ja pooltel tuleks vaidlust jätkata tsiviilkohtus. Võtsime arvesse asjaolu, et antud blogi pidaja on juba kohtus käinud ja võitnud, mistõttu on sama õigus ka kõnealusel kodanikul.

Mitmete isikute kontaktandmed on avaldatud portaalis Livejournal.com. Portaali on registreeritud USA-s ja inspeksioonil puuduvad võimalused koostööks. Küll aga saatsime portaali pöördumise ja juhtisime antud probleemile tähelepanu. Samas kaebajat otseselt aidata ei ole võimalik.

Lõpuni jõudis veebilehe pidu.eu vastu algatatud massiline kaebuste saaga, kus portaali haldav isik lõpuks eemaldas kaebajate kontod ning lisan võrgulehele teabe, kuidas inimesed saavad ise lehe poole pöörduda ([www.pidu.eu/kkk](http://www.pidu.eu/kkk)). Kasutajakontod loodi tagaselja Facebooki kontodest, mis olid rakendustele avatud.

Ühe juhtumi puhul külastas isik kaebuse esitanud kodaniku alaealise poja Facebooki kontot ning kopeeris endale seal pildi, millel oli kujutatud kaebaja koos oma alaealise tütreaga. Pilt kopeeriti mitte seotud inimese Facebooki seinale avalikuks näitamiseks. Kaebuse kohaselt ei olnud poeg oma Facebooki kontot piisavalt turvanud, mistõttu oli see kõigile kättesaadav. Kaebaja soovis AKI sekkumist, kuna pildi avaldamine väidetavalt kahjustas tema mainet. Menetlust ei alustatud, kuna leidsime, et inimesel on võimalik pöörduda pildi avaldaja poole nõudega nimetatud pildi eemaldamiseks. Samuti on tal võimalik pöörduda Facebooki poole ning teavitada ebasobiva pildi levitamisest võõraste isikute poolt. Arvestati ka asjaoluga, et tegemist oli juba varasemalt avaldatud andmete taasesitamisega – vaidlusi tekitanud pilt oli avalik ning kõigile kättesaadav.

#### **4.1.3. Isikuandmete töötlemine meedias**

Kodanike teadlikkus oma õiguste osas on oluliselt kasvanud, kuid seda on ka meediaväljaannete oma. Inspeksioonini jõuab järjest vähem kaebusi ja pooled saavad omavahel palju kaasusi juba lahendatud. Muutused on tõenäoliselt seotud asjaoluga, et avalikkuse huvi on ajan muutuv mõiste ning järjest enam artikleid on internetis kõigile lihtsalt leitavad ja kättesaadavad.

Kaks kaebust Äripäeva edetabelites avaldavate isikute kohta jõudsid ka kohtuvaidlusteni.

Seoses isikuandmete kasutamisega meedias tegi inspeksioon rea ettekirjutusi ja ettepanekuid: ettekirjutus BMA Estonia OÜle (MKE Estonia) võrguartiklis isikuandmete tuvastamatuks muutmise kohta; ettepanek kaebuse peale Delfi artiklist foto eemaldamiseks, mis täideti; ettepanek kaebuse peale Õhtulehest isiku perekonnanime eelmadamiseks, mis täideti.

Inspeksioon algatas menetluse ühe abielupaari kaebuse asjus, kus paar leidis, et artiklis kajastatud fakt, et tegemist on abielupaariga, kahjustab ülemääraselt nende õigusi, kuna see viitab nende seksuaalsetele eelistustele. Menetlus lõpetati, kuna kaebajad ei suutnud esitada objektiivset põhjendust või reaalselt näidet, kuidas fakti, et nad on abielus, mainimine nende eraelu puutumatus on ülemääraselt kahjustanud. Ajakirjandusväljaanne suutis põhjendada, miks selle fakti avaldamine oli artiklile uudisväärtust andev.

Kaebuse peale algatati menetlus ka Võrumaa Teataja osas digiarhiivis isikuandmete avaldamise lõpetamiseks. Pärast menetluse algatamist lõpetas ka väljaanne kõnealuste isikuandmete avaldamise digiarhiivis.

Ringkonnakohtusse jõudis juhtum, kus kodanik protesteeris oma isikuandmete (nime) avaldamise vastu nn rikaste edetabelis Äripäevas. Kaebus oli esitatud selle vastu, et inspeksioon keeldus ettekirjutust tegemast. Ringkonnakohus leidis, et apellatsioonkaebus ei ole põhjendatud ja tuleb jätta rahuldamata. Kohus nõustus inspeksiooniga, et isiku ettevõtlusega seotud info avaldamine ei kujuta endast ülemääraselt eraelu puutumatus riivet. Ettevõtlus on väljapoole, avalikkusele suunatud tegevus. Seadusandja on leidnud, et avalikkusel on õigus teada ettevõtete omanike ja juhtorganite liikmete andmeid ning ka ettevõtete majandustulemusi ning seetõttu on see info äriregistris tehtud avalikult kättesaadavaks. Ringkonnakohus nõustus, et ettevõtlustulu ja varaga seotud andmete avaldamine on realselt edendanud ühiskonnas vajalikku debatti paljude erinevate majandusega seotud oluliste teemade üle. Kõnealused edetabelid on avaldatud ajakirjanduslikul eesmärgil, st ei ole koostatud üksnes sensatsiooni ja meelelahutuse huvides ega ole mõeldud kellegi solvamiseks.

Ringkonnakohus leidis, et kaebaja on isik, kelle puhul saab eeldada teatud majandusliku võimu olemasolu ning kes seetõttu vastab avaliku elu tegelase tunnustele. Kolmas isik avaldas, et kaebaja võib olla oma abikaasa firma tegelik suunaja ning kaebaja sellele väitele käesolevas asjas vastu ei vaielnud.

Kohus leidis, et kaebaja on Eestis tuntud kui ärimees, kes on pikka aega aktiivselt tegelenud ettevõtlusega ning seostanud ennast tuntud isikutega, samuti on tema tegevust korduvalt kajastatud meedias. Asjaolu, et isik on aastaid Eestist eemal viibinud, ei välista tema suhtes avaliku huvi esinemist, kui tegemist on jätkuvalt avaliku elu tegelase määratlusele vastava isikuga.

Ringkonnakohus leidis, et kaebaja, kes oma endise nime avaldamise tõttu oma õiguste ülemääraselt kahjustamist väidab, oleks pidanud välja tooma need kahjulikud tagajärjed, mida tema endise nime avaldamine ajakirjanduses temale on tekitanud ning põhistama oma väiteid viisil, et neid saaks lugeda usutavaks. Sellisel juhul oleks inspeksioon saanud andmesubjekti õiguste ülemääraselt kahjustamist hinnata, teostades erinevate põhiseadusega kaitstud hüvede ja huvide võrdlevat kaalumist. Antud juhul ei toonud kaebaja välja neid kahjulikke tagajärgi, mida tema varasema nime avalikustamine talle põhjustas. Asjaolu, et isiku varasema nime kajastamine on tema jaoks ebameeldiv, ei ole andmesubjekti õiguste ülemäärase kahjustamise sedastamiseks piisav.

Riigikohtus antud kaasust menetlusse ei võetud.

Teise kohtusse jõudnud juhtumi puhul kaebas kodanik halduskohtusse inspeksiooni järelevalve menetluse lõpetamise teate. 2014. aastal avaldas ajaleht Äripäev edetabeli „Eesti börsinvestorite TOP 50“, kus esines ka kaebuse esitanu nimi ning selle kõrval börsinvesteeringute suurus eurodes 2013 ja 2014. Nimekirjas avaldatu esitas Andmekaitse Inspeksioonile kaebuse tuvastamiseks, kas Äripäev AS on rikkunud tema isikuandmete töötlemise ja avaldamisega tema põhiõigusi ja -vabadusi. Rikkumise tuvastamise korral palus kodanik Andmekaitse Inspeksioonil teha Äripäev ASile ettekirjutus lõpetada tema isikuandmete töötlemine ja avaldamine nii olevikus kui tulevikus ning kustutada ja/või sulgeda tema kohta kogutud isikuandmed.



Kohus nõustus inspeksiooni ja Äripäeva seisukohaga, et menetluse lõpetamise teate näol ei olnud tegemist haldusaktiga, mistõttu selles puudub ka vaidlustamisviide. Sellist teadet võib halduskohtus vaidlustada toiminguna, taotledes selle õigusvastasuse tuvastamist.

Inspeksioon lõpetas menetluse ühe kodaniku kaebuse asjus, kus kodanik kaebas Äripäeva paberversioonis 2014. aasta augustis ilmunud artiklis isiku pangakonto numbri avaldamise peale - inspeksioon ei saa muuta paberandjal avaldatut. Samas asus inspeksioon seisukohale, et artiklis isiku pangakonto numbri väljatoomine võis olla tõepoolest ülemäärane andmete avaldamine, mis ei andnud artiklile uudisväärtust juurde. Äripäev nõustus antud arvamusega ka ise.

Kaks kaebajat soovisid, et OÜ Filmimees lõpetaks neist filmitud videode, nende telefonikõnede ja muude andmete töötlemise ja avalikustamise. Kaebuse kohaselt puudus kaebajate nõusolek nende isikuandmete avalikustamiseks. Kaebajatele teadaolevalt ei ole materjali mujal avaldatud, kuid saatelõik oli kättesaadav AS TV3 vörguleheküljel [www.tv3play.ee](http://www.tv3play.ee) (rubriigis Kaua Võib).

Inspeksiooni ettepanekul kustutati ka nõ must materjal (sh telefonikõnede salvestused) ära. Saates avaldati kaebaja ning saatejuhi vahel tehtud intervjuu, kuid selles kaebajaid ei identifitseeritud – ei avaldatud kaebajate ega nende perekonnaliikmete nimesid, moonutati häält ning hägustati maja, et isikuid ei oleks võimalik tuvastada ka ümbritseva kaudu. Saatelõigus mainiti ainult kaebaja eesnime, kuid selle alusel ei ole võimalik konkreetset isikut tuvastada. Sellest tulenevalt nõustus inspeksioon OÜ Filmimees selgitustega ning leidis, et TV3Play.ee vörguleheküljel olevas saatelõigus ei ole toimunud isikuandmete töötlemist IKS § 4 lõike 1 ja § 11 mõttes.

Kodanik edastas allkirjastamata kaebuse vörgulehe [www.ee.pokernews.com](http://www.ee.pokernews.com) suhtes. Kaebuse kohaselt sooviti enda nime ning pildi eemaldamist nimetatud vörgulehekülje artiklist. Kaebaja väitel oli ta oma aastatetaguse teo eest karistada saanud ning mingit õigust tema tulevast elu neil rikkuda ei ole. Inspeksioon tõdes, et avaldatud artikkel ei rikkunud ülemääraselt tema õigusi, sest sama artikliga vahendati ajalehe Sakala vörgulehel olnud artiklit, mille kohaselt mõistis kohus kokkuleppemenetluses kaebaja mai keskel süüdi ehk karistus oli kehtiv. *Pokernews*i artiklis oli toodud välja kohtuotsuse põhisisu ning muid eraelulisi andmeid tema kohta ei avaldatud.

Kodanik edastas kaebuse, millega soovis enda isikuandmete eemaldamist Delfis ilmunud artiklist. Varasemalt oli ta esitanud avalduse ASile Delfi enda andmete, sh erakondliku kuuluvuse kohta, eemaldamiseks ning inspeksioon lisatud kirja koopias saajate hulka. Inspeksioon kontrollis vaidlusalust artiklit ning selles sisalduvaid kommentaare, aga ei tuvastanud, et selles oleks avaldatud kaebaja ees- või perekonnanimi ning vanus ehk isikuandmed, mille kaudu on teda võimalik üheselt tuvastada. Ainult erakonda kuuluvuse ning erakonnas viibimise aja järgi ei ole võimalik isikut üheselt tuvastada. Seda enam, äriregistris toodud erakonda kuuluvuse otsingut on võimalik kasutada ainult isiku nime kaudu otsides, kuid erakonda astumise või sellest väljumise aja järgi ei ole võimalik konkreetset isikut otsida. Kuna avaldatav artikkel ei sisaldanud isikuandmeid, mille kaudu oleks isikut võimalik otseselt tuvastada, siis ei peetud vajalikuks sekkuda ajakirjandusvabadusse ning nõuda kogu artikli koos kommentaaridega eemaldamist. Samuti ei leitud vaidlusalust Delfi artiklit tema nime järgi Google'ist otsides.

Kodanik vs kodanik kaebuste osas on enamiku puhul tegemist laimuga ning nende osas inspeksioon reeglina menetlust ei alusta, vaid soovib pöörduda kohtusse.

Nt süüdistas üks kodanik teist teda laimava ja alusetult süüdistava videoklipi meedias tahtliku avaldamise eest, mis kaebaja mainet kahjustab. (Video puudutas avalikul üritusel lauale ununenud mobiiltelefoni omastamise fakti, mis jäi turvakaamera salvestisele ning mis avaldati Youtube's).

Kodanikud esitasid kaebuse veebilehekülgedel [rameshwar.wordpress.com](http://rameshwar.wordpress.com) ja [lhv.delfi.ee/foorum/free/121811](http://lhv.delfi.ee/foorum/free/121811) nimede ja isikukoodide avaldamise kohta ilma asjaosaliste nõusolekuta. Antud juhul tuginesid eelnimetatud vörgulehtedel avaldatud kommentaarid Eesti Ekspressi artiklile ning saates „Mõtleme taas” kaebaja enda avaldatud seisukohtadele. Nii telesaates



kui ajaleheartiklis avaldatu töid kaasa suure avalikkuse huvi ning soovi avaldada esitatu suhtes ka arvamust. Inspeksioon tegi kindlaks, et isikuandmete töötlemiseks ajakirjanduslikul eesmärgil oli seaduslik alus, mistõttu järelevalvemenetlust ei algatatud.

#### 4.1.4. Isikuandmete töötlemine rahandussektoris

##### a) kindlustusandjad

Kaebused/selgitustaotlused 2014 aastal olid valdavalt seotud küsimustega, millisel õiguslikul alusel võib kindlustusandja lepingu sõlmimisel ja kindlustusjuhtumi toimumisel kolmandatelt isikutelt andmeid küsida. Lisandunud on pöördumised seoses sellega, et inimestel on tekkinud kahtlus oma andmete töötlemisel minimaalsuse põhimõtte täitmise osas.

Andmete saamise õigust puudutavad kaasused liikluskindlustusjuhtumitega seoses

Vastavalt isikuandmete kaitse seaduse (IKS) § 14 lg 2 on isikuandmetele juurdepääsu lubamine või isikuandmete edastamine lubatud, kui isik, kes andmeid soovib, töötleb neid seadusega ettenähtud kohustuse täitmiseks. Selliseks seaduseks on näiteks kindlustustegevuse seaduse (KTS) § 14<sup>2</sup> lg 9, mille kohaselt on kindlustusandjal õigus nõuda kolmandalt isikult isikuandmeid või juurdepääsu võimaldamist isikuandmetele, mis on vajalikud kindlustuslepingu täitmise kohustuse või selle täitmise ulatuse kindlaks tegemiseks. Kolmas isik on kohustatud kindlustusandja nõudel viivitamata edastama isikuandmed või võimaldama nendele juurdepääsu. Nimetatud eesmärgil ei ole kindlustusandjale andmete edastamine või juurdepääsu võimaldamine lubatud, kui tegemist on delikaatsete isikuandmetega, välja arvatud juhul, kui kindlustusandja vajab delikaatseid isikuandmeid sama paragrahvi lõigetes 5 ja 6 nimetatud juhtudel. Lisaks toetab andmete saamise õigust liikluskindlustuse seaduse (LKindIS) § 43 lg 1, mille kohaselt peab kindlustatu vastu esitatud nõude saanud kindlustusandja juhtumit käsitlema ja tegema otsuse kahju hüvitamise või sellest keeldumise kohta. LKindIS § 43 lg 7 p 1 järgi on nõuete käsitleja kohustatud koguma nõude kohta vajalikku teavet ning vajaduse korral pidama läbirääkimisi vaidluse lahendamiseks.

Tegemist on nn üldvolitusnormidega, seega tuleb kindlustusandjal päringut koostades lähtuda IKS § 6 sätestatud põhimõtetest (eelkõige seaduslikkuse põhimõtte, eesmärgikohasuse põhimõtte ja minimaalsuse põhimõtte). Päringu saajal peab olema selge, millisel õiguslikul alusel andmeid soovitakse sh andmete saamise eesmärk (miks need on konkreetsel juhul vajalikud), soovivate andmete koosseis jms. Kuna andmete vastutav töötleja vastutab andmete väljastamise eest, siis on ka temal kohustus lähtuda andmeid väljastades samadest põhimõtetest, mis eeldab iga pöördumise puhul nn kaalutusotsuse tegemist (päringu sisu sh õigusliku aluse, eesmärgi ja andmekoosseisu hindamist). Seega võib nõustuda sellega, et kui andmete vastutaval töötlejal puudub kindlus andmete õigsuse osas (pole kindel, kas tegemist on just selle isikuga seotud andmetega), on andmete väljastamisest keeldumine õigustatud. Muudel juhtudel (tegemist on delikaatsete isikuandmetega või eraeluliste isikuandmetega) keelduda ei tohiks, kui on olemas KTS § 14<sup>2</sup> lg 9 sätestatud alus ning koostatud põhjendatud taotlus andmete saamiseks.

Tulenevalt eeltoodust ei ole terviseandmete töötlemine kindlustussektoris keelatud. Isiku nõusolek ei ole juhul, kui andmeid töödeldakse seaduse alusel, vajalik, vaid hoopis eksitav ja andmesubjekti positsiooni nõrgestav. Tegemist on nn üldvolitusnormidega, seega tuleb kindlustusandjal lähtuda IKS § 6 sätestatud põhimõtetest (eelkõige seaduslikkuse põhimõtte, eesmärgikohasuse põhimõtte ja minimaalsuse põhimõtte). Antud juhul ei ole leidnud kinnitust minimaalsuse põhimõtte rikkumine.

Kindlustussektoriga seoses oli 2014 menetluses ka kaebus, mille sisuks oli kindlustusandja töötaja tegevus. Nimelt saatis töötaja endale tööalaseid dokumente. Kindlustusandja oli kehtestanud ettevõttesisesed reeglid, mis sellise tegevuse keelasid. Kuna ettevõttesisene regulatsioon oli olemas ja töötajale tutvustatud, oli õigustatud ka Andmekaitse Inspeksiooni ettepanek andmete kustutamiseks, mis töötaja poolt täideti.

Eesti Kindlustusmaaklerite Liidule on edastatud kindlustusmaaklerite tegevusega seotud isikuandmete töötlemise probleemid komplekselt. Teemad võib tinglikult jagada kolmeks.

Isikuandmete töötlemine enne lepingu sõlmimist. Andmekaitse Inspeksioon juhtis lisaks varasematele seisukohtadele Eesti Kindlustusmaaklerite Liidu tähelepanu juhtudele, mil kasutatakse nn hulgimaaklerlust (KTS sellist võimalust ei välista, samuti on hulgimaaklerluse võimalikust kasutamisest juttu Finantsinspektsiooni vastavasisulises märgukirjas). Finantsinspektsioon ei ole oma märgukirjas pööranud tähelepanu isikuandmete kaitsele hulgimaaklerluse puhul. Kuna tegemist ei ole mingi eraldiseisvana reguleeritud isikuandmete töötlemise viisiga, siis laienevad sel juhul isikuandmete kaitse seaduses sätestatud üldreeglid. Isikuandmete töötlemisel on oluline, et andmetöötlusprotsess oleks läbipaistev ja isikul oleks ülevaade oma andmete töötlemisest. Seetõttu peab inimene olema teadlik sellest, et tema andmeid võidakse edastada kolmandatele isikutele, samuti sellest, millised need kolmandad isikud on. Seega peab isikut teavitama sellisest andmete töötlemisest juba lepingu sõlmimisel. Isikuandmete töötlemine lepingu täitmiseks ja lepingu täitmise tagamiseks (IKS § 14 lg 1 p 4). Isikuandmete kaitse seaduse kohaselt võib kindlustusmaakler kliendisuhete ajal isikuandmeid töödelda isikuandmete kaitse seaduse (IKS) § 14 lg 1 p 4 alusel lepingu täitmiseks ja lepingu täitmise tagamiseks ja/või isiku nõusoleku alusel IKS § 12 sätestatud tingimustel. Praktikas ei ole välistatud, et mõnel andmetöötluse juhul võib üheaegselt kohaldada mitut õiguslikku alust, tingimusel, et neid aluseid kasutatakse õiges kontekstis. Kindlustusvahenduses toimub isikuandmete töötlemine nii seaduse alusel (IKS § 14 lg 1 p 4 kui ka nõusoleku alusel (elektroonilise side seadus (ESS) § 103, § 103', § 133 lõige 2', § 184'').

Andmete säilitamine peale lepingu lõpetamist

Kindlustustegevuse seaduse § 142 lõike 7 sätestab, et kindlustusandjal on õigus lepingu täitmise tagamiseks säilitada isikuandmeid kuni lepingust tuleneva nõude aegumistähtaaja möödumiseni. Kui seadus ei sätestata teisiti, laieneb see säte ka maakleritele vastavalt KTS §le 136 lg 1.

#### **b) koostöö Maksu- ja Tolliametiga IKS §is 17 sätestatud automaatsetest otsustest teavitamisel**

Automaatseid otsuseid tehakse MTAs füüsilistele isikutele tulumaksu tagastamise kohta. Teavituse tegevusest lisatakse iga isiku deklaratsiooni teavituselehele e-maksuametis ja see läheb kasutusse 2015.a. kevadel. Isiku õigus automaatne otsus vaidlustada on samuti teavituse osaks. MTA privaatsuspoliitikasse on lisatud peatükk „Automaatsed otsused”, mis selgitab inimestele millise andmetöötlusega on tegemist.

#### **c) maksehäired**

Maksehäireandmete töötlemisega seonduvalt oli ka 2014. aastal hulgaliselt kaebusi. Põhiliste probleemidena sai välja tuua kreditoride poolt inimeste andmete vaatamise maksehäireregistri peale seda, kui võlgnevus oli tasutud ja lepinguline suhe lõppenud.

Inspektsiooni hinnangul on selline tegevus vastuolus isikuandmete kaitse seaduses toodud eesmärgikohasuse põhimõttega. Selle kohaselt võib isikuandmeid töödelda ainult määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkidega kooskõlas. Samuti ei anna isikuandmete kaitse seaduse § 14 lg 1 punkt 4 volitust isiku nõusolekuta tema andmetega tutvumiseks, kui võlgnevus on tasutud, kuna ei ole enam lepingut, mille täitmist tagada.

Teise probleemina paistis silma inkassoettevõtjate poolne tegevus inimeste maksehäireandmete edastamisel. Nimelt edastati inimeste maksekäitumist kirjeldavat infot nende tööandjatele, sugulastele ja tuttavatele. Samuti otsiti võimalusi kasutada selleks sotsiaalmeedias levinud suhtlusvõrgustikke.

Siinkohal leidis Andmekaitse Inspeksioon, et kuna isiku tööandja, sugulane või tuttav ei töötle võlaandmeid seadusega pandud ülesannete täitmiseks, siis ei saa selline edastamine toimuda inimese nõusolekuta temaga sõlmitud lepingu täitmise tagamiseks, kuna läbi kõnealuste isikute ei ole võimalik lepingu täitmist tagada. Samuti kahjustab selline maksehäireandmete edastamine ülemääraselt isiku

eraelu puutumatus, kuna tööandjad, sugulased ja tuttavad on võlgniku suhtes kolmandad isikud, kellel puudub õigustatud huvi võlaandmetega tutvumiseks.

Sageli on jäänud inimestele arusaamatuks, millistest allikatest saavad inkassoettevõtted nende kodused aadressid. Siinkohal on inspeksioon selgitanud, et inkassoteenuse osutajatele on antud juurdepääs rahvastikuregistri andmetele rahvastikuregistri seaduse § 71 lõike 1 alusel andmete saamiseks õigustatud huvi korral.

Jätakuvalt pöördusid inspeksiooni poole juriidiliste isikute juhatuse liikmed, kelle isikuandmed olid avalikustatud koos ettevõtte võlgnevustega. Sellistel puhkudel selgitati neile, et juriidilistest isikutest võlglaste andmete avalikustamist koos juhatuse liikmete kui seotud isikute nimedega ei saa pidada vastuolus olevaks seadusest tuleneva keeluga, esmajoones isikuandmete kaitse seadusega, sest selliste andmete puhul ei ole tegemist eraeluliste, vaid majandustegevusega seonduvate andmetega.

2014. aastal viis Andmekaitse Inspeksioon koostöös Tarbijakaitseametiga ka läbi kiirlaenuandjate seire, vt aruandes p 5.1 Seired, 5.1.4 kiirlaenuandjate seire.

#### **4.1.5. Isikuandmete töötlemine tervishoiusektoris**

##### **Kontrollid ning auditid**

2014.aastal viidi läbi kohapealne kontroll apteekides seoses isikuandmete kaitse eest vastutavate isikute poolt peetavate andmetöötlusregistritega. Kontrollitavaid ette ei teavitatud, kuna inspeksioon soovis saada ülevaadet hetkeolukorrast, kas üldse ning kuidas andmetöötlemise registrit peetakse. Kontrolliti kokku kümnet apteeki. Üldpilt oli rahuldav: kui registris esines puudusi (sh kui register üldse puudus), kõrvaldati need suhteliselt kiiresti.

Kolmele apteegile, kelle puhul tuvastati, et andmetöötlemise register puudus, anti tähtaeg registri esitamiseks, mis õigeaegselt täideti.

Neli apteeki ei suutnud kohapealse kontrolli käigus andmetöötlemise registrit esitada, kuid väitsid, et eelduslikult oli register olemas.

Üks apteek palus korduvalt inspeksiooni abi registri koostamisel, mistõttu esitati register paar päeva hiljem ning selles puudusi ei tuvastatud.

Kahe apteegi puhul oli mingis osas kirjeldatud andmeid, mis peavad registris olema ning üks apteek esitas registri kohapeal.

Ühe puhul eksisteeris dokument, milles oli valdavas osas välja toodud registris vajalikud andmed. Dokument oli koostatud 2008. aastal, kuid edaspidised sissekanded puudusid. Uuendatud registris puudusi ei tuvastatud.

Kõik apteegid, kelle registripidamises avastati puudjääke, likvideerisid need inspeksiooni nõudmisel kiiresti.

Inspeksioon auditeeris ka kaht haiglat, vt p 5.2.1

##### **Näited kaebustest ja järelevalvemenetlustest**

Kodanik kaebas, et tema andmeid on vaadanud arst, kellel polnud selleks õigust. Kaebuse kohaselt toimus isikuandmetega tutvumine arsti poolt 2012. aasta märtsis. Arsti esmaste selgituste kohaselt ei ole tal olnud kokkupuuteid kaebaja nimelise isikuga ning leidis, et tegemist oli eksitusega. Täiendavate selgituste kohaselt ei olnud juurdepääsu e-tervise infosüsteemile tema ID-kaarti kasutades ka kõrvalistel isikutel. Samas märkis, et teoreetiliselt oli võimalik, et ta sattus kaebaja nimele ekslikult, töödeldes sarnase perekonnanimega patsiendi andmeid.

Arstil on õigus ilma nõusolekuta isikuandmeid töödelda ainult tervishoiuteenuse osutamiseks. Samuti ei tohi ta kasutada nimetatud juurdepääsu isikliku uudishimu rahuldamiseks. Arsti selgitused ei andnud konkreetseid vastuseid kaebaja isikuandmete töötlemise osas. Järelevalvemenetlus lõpetati,

kuna järelevalvemenetluse abinõud olid ammendunud. Samas ei olnud tol hetkel võimalik isikut väärteokorras vastutusele võtta, kuna menetlus lõppedes oli väärtegu aegunud.

Inspeksioon algatas järelevalvemenetluse kaebuse osas, kus süüdistati arsti E-tervise infosüsteemis korduvas isikuandmete, sh delikaatsete isikuandmete vaatamises. Logifailidest nähtus, et arst teostas 9 kuu jooksul ühe kaebaja suhtes 130 päringut ning teise suhtes 128 päringut. Selgituste kohaselt puudus kaebajatel ravisuhe nimetatud arstiga, nad ei kuulu tema perearstinimistusse ning viimane kokkupuude nimetatud arstiga oli neil 2007. aastal.

Arsti selgituste kohaselt olid kaebajad tema endised patsiendid. Selgituste kohaselt tutvus arst kaebajate tavaretseptide ning ambulatoorsete epikriisidega e-tervise infosüsteemis, kuna soovis tutvuda ravimitega ja uuringutega, mida eriarstid kasutavad erinevate haiguseisundite korral. Enamus faile E-tervise Infosüsteemis ei avanenud või logimine ebaõnnestus, sest kaebajad ei kuulunud arsti nimistusse – sellest ka suur logifailide arv. Päringute tegemine ei olnud seotud arsti ning kaebajate vahelise ravisuhtega ega tervishoiuteenuse osutamisega kaebajatele. Arst märkis, et ei olnud teadlik, et arstina puudub tal õigus kasutada e-tervise infosüsteemi taolisel eesmärgil. Järelevalvemenetlus lõpetati, väärteo menetlus on pooleli.

Maksu- ja Tolliamet (EMTA) edastas inspeksioonile märgukirja, mille kohaselt sai EMTAle kontrolli käigus teatavaks, et eraisikust Soome kodanik on müünud Optiprof Estonia OÜle Soome kodanike silmauuringute andmeid. Ettevõtte poolt EMTAle antud selgituste kohaselt on võimalik andmekogus sisalduvate andmete põhjal analüüsida glaukoomi tekkimise tõenäosust, teavitada isikut glaukoomi ohust ning kutsuda isik täiendavale uuringule. Mainitud Soome kodanikul on arstilitsents nii Eestis kui ka Soomes ning ta oli Optiprof Estonia OÜ juhatuse liige.

Menetlusest selgus, et patsiente võeti vastu Soome Vabariigis ning nende silmarõhu ja refraktsiooni näidud kantakse kodeeritud andmebaasi patsientide nõusoleku alusel. Nimetatud andmebaasi kasutati teadusuuringu läbiviimiseks Soome Vabariigis ehk nii isikuandmete kodeerimine kui ka teadustöö toimusid Soomes. Samuti selgus, et Optiprof Estonia OÜl kodeeritud andmebaasi polnud ning ettevõttele piisas ainult uuringu tulemustest. Seega andmebaasi lahti kodeerimist ei toimunud ning inspeksioonile edastatud näidisandmebaasis ei olnud isikud üheselt tuvastatavad.

Kuna isikuandmete töötlemine isikustatud kujul toimus Soomes, puudus inspeksioonil järelevalvepädevus. Eesti Vabariigi territooriumil kõnealuse andmebaasiga seonduvalt isikuandmete töötlust ei toimunud ning Optiprof Estonia OÜ-le edastati ainult teadusuuringu tulemused. Seetõttu menetlus lõpetati.

Inspeksioon sai ka märgukirju, kus ettevõtted ise teavitasid endapoolsest rikkumisest. Nt Kaarli Hambapolikliinik OÜ andis teada, et rikkus delikaatsete isikuandmete töötlemise nõudeid. Märgukirja kohaselt soovis üks polikliiniku patsientidest saada seoses raviarsti vahetusega ettevõtte andmebaasist enda röntgenpilte aastast 2008, kuid selgus, et neid pilte pole võimalik näha ega ole ka võimalik tuvastada nende piltide asukohta fotopangas. Ettevõttes toimus sisejuurdlus, mille käigus tuvastati, et „tõenäoliselt on nimetatud pildid kustunud 2011. aasta novembris, mil toimus uue tarkvara kasutuselevõtmine.“ Pildimaterjali hävimine toimus välisele kõvakettale ümberkopeerimise käigus ning tegemist oli riistvaralise probleemiga, mida ümberkopeerimise hetkel ei õnnestunud tuvastada. Selgituste kohaselt puudus kolmandatel isikutel juurdepääs piltidele.

Ettevõtte tähelepanu juhiti asjaolule, et polikliinikul on kohustus tagada, et isikuandmete töötlemisel on täidetud isikuandmete kaitse seadusest tulenevad nõuded (sh tagatud isikuandmete terviklikkus ning nende turvaline käitlemine).

Koostöös Terviseametiga kontrolliti kohapeal mõningaid tervishoiuteenust pakkuvaid perearste. Tuvastati puudujääke paberkandjal olevate tervisedokumentide hoiustamisel – need olid kätte saadavad kõrvalistele isikutele. Ettevõtjatele tehti ettepanek täiendada selles osas turvameetmeid isikuandmete kaitseks.

Kaebaja soovis ühest perearstikeskusest saada oma surnud vanemat puudutavaid andmeid. Pöördumise kohaselt anti talle ainult osad andmed, mille hulgas ei olnud teavet perearsti visiitide, eriarsti juurde suunamise ja tehtud uuringute kohta. Menetluse käigus selgus, et kaebaja oli korduvalt pöördunud perearstikeskuse poole sooviga saada oma surnud vanema ravidokumente. 2014. aasta jaanuaris väljastati perearstikeskuse poolt kaebajale kogu olemasolev dokumentatsioon, kuid kaebaja nõudis erinevaid dokumente korduvalt uuesti. Perearstikeskus kinnitas, et muid dokumente neil antud isiku kohta pole. Inspeksioon leidis, et kuna kaebajale väljastati varasemalt kõik dokumendid, puudus vajadus koostada ettekirjutust soovitud andmete väljastamiseks.

### **Nõudekirjad, selgituste andmised, nõu andmine**

Andmekaitse Inspeksioon osales läinud aastal regulaarselt Eesti e-tervise õiguse ja eetika eksperdirühmas, mille eesmärk on kujundada riikliku strateegiat.

Inspeksioon valmistas ette sisendi seoses Sotsiaalministeeriumist saadetud nõudekirjaga, mis puudutas Euroopa Komisjoni poolt välja töötatud m-tervise (mobiilne tervishoid) rohelist raamatut ja selles sisalduvaid küsimusi. Sisendi koostamisel juhtiti tähelepanu Euroopa andmekaitseasutuste töörühma arvamusele nutiseadmete rakenduste kohta, Euroopa Võrgu- ja Infoturbeameti (ENISA) avaldatud suunistele mobiilirakenduste turvalisuse osas ning suurandmete töötlemisele pilves, samuti töörühma arvamusele pilveandmetöötluse ning sellega seonduvate riskide, õigusraamistiku kohta. Üks osa rohelisest raamatust käsitles ka m-tervise lahendusi ning positsioneerimist, mistõttu juhtiti tähelepanu töörühma arvamusele nutiseadmetes kasutatava asukoha kindlaksmääramise teenuse, sh sellega seonduvate riskide, õigusliku raamistiku, andmekaitsealaste kohustuste, järelduste ning soovitude kohta.

Innovaatik OÜ soovis selgitusi seoses delikaatsete isikuandmete varundamise asukoha osas. Konkreetsemalt sooviti teada saada, kas meditsiiniandmeid võib varuda näiteks *Amazon Cloud Storage* liirima süsteemis.

Terviseandmed on delikaatsed isikuandmed, mistõttu tuleb nende töötlemisel rakendada täiendavaid turvameetmeid, et tagada andmete terviklus, käideldavus ja konfidentsiaalsus. Kui terviseandmeid soovitakse säilitada andmepilves, siis tuleb eelkõige arvestada asjaoluga, kas ning millises ulatuses on võetud kasutusele piisavad turvameetmed isikuandmete kaitseks. Kui isikuandmeid hoitakse teise riigi serverites, siis puudub patsiendil ning tervishoiuteenuse osutajal (vastutaval töötlejal) füüsiline kontroll isikuandmete käitlemise üle. Kuna tegemist on delikaatsete isikuandmetega, siis soovitab inspeksioon leida alternatiivseid lahendusi delikaatsete isikuandmete säilitamisele andmepilves.

SA Narva Haigla esitas selgitustaotluse, mille kohaselt soovis Vene Föderatsiooni justiitsasutus saada kriminaalmenetluse raames teavet ühe Narva elaniku ravi ja diagnoosi kohta. Haigla soovis teavet, kas tervishoiuasutus on kohustatud teise riigi võimuinstitsioonile välja andma patsiendi delikaatseid isikuandmeid.

Eesti Vabariigi ja Vene Föderatsiooni vahel on sõlmitud leping õigusabi ja õigussuhete kohta tsiviil-, perekonna- ja kriminaalasjades. Nimetatud lepingu kohaselt suhtlevad õigusabi andmisel lepingupoolte asutused üksteisega Eesti Vabariigi Justiitsministeeriumi, Eesti Vabariigi Prokuratuuri ning Vene Föderatsiooni Justiitsministeeriumi ja Vene Föderatsiooni Peaprokuratuuri kaudu. Seetõttu ei ole Vene Föderatsiooni asutustel õigust otse kriminaalmenetluse tarbeks Eesti kodanike kohta teavet saada ning tervishoiuasutusel ei ole lubatud neid andmeid küsijale otse väljastada.

Inspeksioonilt palus teavet AS Medicum, kes küsis delikaatsete isikuandmete USAsse edastamise turvalisuse kohta. Tegemist oli meditsiiniuasutuse endise välismaalasest patsiendiga, kes esitas e-kirja teel soovi oma digitaalse haigusloo saatmiseks praegusesse asukohariiki. AS Medicum soovis teada saada, kas neil on õigus edastada patsiendile väljavõtted digitaalsest haigusloost ja saata need tähtid postiga või krüpteeritult e-kirjaga USA-sse, samuti seda, kas ettevõttel on kohustus tõlkida haigusloo väljavõtte inglise keelde.

Inspeksioon selgitas, et isikul on õigus küsida enda kohta andmeid isikuandmete kaitse seaduse alusel. Isikuandmete töötaja peab aga olema kindel, et isikuandmeid küsib sama isik, kelle andmeid on töödeldud. Isikuandmete edastamise viisi valimisel tuleb arvestada asjaoluga, kas edastamise viisi valik on piisavalt turvaline, et vältida kõrvaliste isikute juurdepääsu isikuandmetele – eriti kui tegemist on delikaatsete isikuandmetega. Tähtis postiga edastamise korral peab olema tagatud see, et kirjasaadetise võtab vastu õigustatud isik ning krüpteerimisel tuleb arvestada ka asjaoluga, kas aadressaadil on võimalik temale edastatud andmed lahti krüpteerida.

Haigusloo väljavõtte tõlkimise osas märkis inspeksioon, et isikuandmete kaitse seaduse kohaselt väljastatakse isikuandmed võimaluse korral isiku soovitud viisil, otsene kohustus haigusloo väljavõtte tõlkimiseks puudub.

## **Väärteomenetlused**

Väärteomenetlused puudutasid kaht omavahel abielus olnud arsti, kes vaatasid õigusliku aluseta poja elukaaslase isikuandmeid e-tervise infosüsteemis, et saada ülevaade nimetatud isiku tervisega seotud probleemidest. Ühe arsti puhul puudus inspeksioonile kaebuse esitanud kodaniku ja arsti vahel igasugune ravisuhe: isik ei olnud antud arsti vastuvõtul kunagi käinud ning arst ei olnud ka tema perearst. Arst tutvus andmetega peale seda, kui avaldaja oli oma perearsti vahetanud. Teise arsti puhul oli kaebaja küll tema kui perearsti nimistus, kuid menetlusest selgus, et kaebuse esitaja ei olnud kunagi arsti poole pöördunud seoses tervishoiuteenuse osutamisega. Kumbagi arsti karistati kiirmenetluse korras trahviga.

### **4.1.6. Koolielu**

2014.aastal kontrollis inspeksioon turvakaamerate kasutamisel eesmärgikohasuse, minimaalsuse ning kasutuse piiramise põhimõtete järgimist kahes tootmisettevõttes ja ühes koolis.

Kontrollitud tootmisettevõtetes ei olnud kaamerate kasutamisel eesmärgikohasuse, minimaalsuse ja kasutuse piiramise põhimõtete rikkumisi, mis võimaldas menetlused lõpetada. Küll aga ei olnud seadusepärane videojälgimissüsteemi kasutamine Laagri Koolis, kus kaamerad olid kõikidesse klassidesse paigutatud juba ehitamise käigus ning need olid pidevas töös.

Põhikooli- ja gümnaasiumiseaduse (PGS) § 44 lõike 5 kohaselt võib videovalvet kasutada kooli territooriumil õpilaste ja koolitöötajate turvalisust ohustava olukorra ennetamiseks ning olukorrale reageerimiseks.

Kuigi seadus lubab (inimese eelneva nõusolekuta) isikuandmete töötlemise turvalisust ohustava olukorra ennetamiseks ning olukorrale reageerimiseks, ei tähenda see, et jälgimisseadmestikku võiks kasutada kõikjal ning erinevatel eesmärkidel. Jälgimisseadmetike kasutamine on lubatud vaid juhtudel, kui muudel viisidel ei ole võimalik turvalisust tagada. Jälgimisseadmetiku kasutamine peab olema kooskõlas isikuandmete töötlemise minimaalsuse põhimõttega ning ei või kahjustada ülemäärast jälgimisseadmetiku vaatevälja jäävate isikute õigusi.

Kooli ümbruses, fuajees ja koridorides võib olla videovalve kasutamine põhjendatud, sest seal võivad liikuda ka muud isikud, mitte ainult õpilaskond.

Küll aga on Andmekaitse Inspeksioon seisukohal, et videovalve kasutamine klassiruumides ei ole põhjendatud, kuna klassiruumis toimuva üle on kontrolli võimalik teostada õpetajal. Õpetajapoolse kontrolli kasutamine on videovalvega võrreldes märksa vähem isikute (nii õppurite kui ka õpetaja enda) eraelu puutumatust riivav abinõu. Kui alternatiivsete abinõudega on võimalik saavutada sama eesmärk (turvaline koolikeskkond), tuleb eelistada sellist andmetöötlust, mille kasutamine riivab isiku eraelu puutumatust vähimal määral. Klassiruumides on õpilaste (samuti õpetajate ja teiste koolitöötajate) õigus eraelu puutumatusele ja õpetamise vabadus kaalukamad kui vajadus pideva jälgimise järele. Klassiruumides segab videovalve mitte ainult õpilaste kõne- ja õppimisvabadust, vaid samuti õpetamisvabadust.

Kool jättis inspeksiooni esialgse ettepaneku klassidest kaamerate väljalülitamiseks täitmata, kuna pidas neid väga efektiivseteks distsipliini tagamise vahenditeks. Alles pärast inspeksiooni samasisulise ettekirjutus-hoiatuse saamist teatas kool kaamerate kasutamise lõpetamisest.



Andmekaitse Inspeksioon menetles kaebust Tallinna Arte Gümnaasiumi tegevuse peale laste isikuandmete töötlemisel. Kaebuse kohaselt oli Tallinna Arte Gümnaasium töödeldud kaebaja laste isikuandmeid, sh delikaatseid isikuandmeid, ilma õigusliku aluseta. Väidetavalt vestles kooli sotsiaalpedagoog lapsega tema pikaajalisest haigusest, mis oli kantud e-kooli süsteemi. Vastavalt isikuandmete kaitse seaduse (IKS) § 10 võib isikuandmeid töödelda kas seaduse või nõusoleku alusel. Üheks seaduses sätestatud aluseks on ka lastekaitse seaduse § 58. Õiguskantsler on oma juhendis „Abivajavast lapsest teatamine ja andmekaitse“ leidnud, et abivajava lapse puhul ei ole tagatud tema turvatunne, areng ja heaolu. Lapse abivajadus võib tuleneda tema võimalikust väärkohtlemisest (sh vägivallast ja hooletusse jätmisest), aga ka tema sotsiaalsest või hariduslikust erivajadusest, pere toimetulekuraskustest jne. Lapse abistamiseks ja kaitseks suunatud tegevused hõlmavad lastekaitsetööd kõige laiemas tähenduses, sh sotsiaalteenuseid ja -toetusi ning koostööd lapse, tema pere ja lapsega kokkupuutuvate võrgustikuliikmete vahel. Seega on tegemist kaalutusotsusega, mille tegija peab suutma põhjendada, millistele argumentidele tuginedes on ta leidnud, et ohus on lapse turvatunne, areng ja heaolu. Antud juhul oli kool põhjendanud sotsiaalpedagoogi otsust lapsega vestelda: oli võimalik oht lapse arengule, heaolule ja turvatundele.

Kaebuses oli õigesti märgitud, et probleemide korral tuleb kõigepealt võtta ühendust lapsevanema, kui lapse seadusliku esindajaga. Kool oli püüdnud probleemide lahendamise kaasata ka lapsevanemat, kuid see ei lõppenud konstruktiivselt, kuna lapsevanem tuli kooli vaid ühel korral, mil vestlus lõppes edutult ja edasisi kutsumisi ta eiras.

Kooli sotsiaalpedagoogi otsus vestelda lapsega, et selgitada välja, kas puudub sekkumisvajadus lapse heaolu huvides lastekaitse seaduse § 59 tähenduses, oli antud juhul põhjendatud.

#### **4.1.7. Koostöö rahvastikuregistriga**

Siseministeeriumi järelevalveaktide alusel on menetletud 2 väärtegu ja tehtud väärtetoetus 2013 alustatud üldmenetluses. Nimetatud üldmenetluses oli isik ilma õigusliku aluseta teinud enam kui 1000 päringut. Väärtegade arvu vähenemine näitab nii vastutavate töötajate, kui ka kasutajate teadlikkuse tõusu.

23.03.2014 ja 18.11.2014 toimusid Siseministeeriumis Andmekaitse Inspeksiooni (AKI) ja Siseministeeriumi rahvastiku toimingute osakonna (RTO) osalusel koosolekud, kus ühe läbiva teemana oli arutusel minimaalsuse põhimõtte rakendamine rahvastikuregistrist andmete väljastamise teenustes pärast RRWeb-ilt X-tee põhisele juurdepääsule üleminekut.

Õigusliku aluse hindamine toimub igakordselt ka edaspidi kaalutusotsusena, mille tegemisel võetakse arvesse juurdepääsu taotlemise eesmärki, IKS § 6 sätestatud põhimõtteid. Samuti lähtub praktika RRS § 72 lg 4 sätestatud põhimõttest, et üksikandmete väljastamise otsustusprotsessi kaasatakse teatud juhul (taotlus ei ole piisavalt põhjendatud, andmesubjekti huvide kahjustus) ka inimene ise. RTO teostab ka pidevat kontrolli AS Andmevara poolt õigusliku aluse hindamisele ning annab omalt poolt ka vastavaid juhiseid.

18.11.2014 toimunud kohtumisel oli testkeskkonnas võimalik tutvuda minimaalsuse põhimõtte parema tagamisega X-tee põhiste ligipääsude puhul.

Andmekaitse Inspeksioonil oli võimalus veenduda, et X-tee põhised ligipääsud tagavad praktikas paremini minimaalsuse põhimõtte täitmise, sest:

- kasutajaõigusi on võimalik varasemast detailsemalt jagada, et tagada tõepoolest vaid selle teabe nägemine, mis on vajalik konkreetse isiku tööülesannete täitmiseks;
- päringuvorme on võrreldes varasemaga rohkem.

Päringute vastused ei anna ülemäärast teavet, nt teovõime päringu puhul ei ole enam võimalik näha ka dokumenti, vaid teovõime piiramise fakti, esindaja tehtavaid toiminguid ja teovõime piiramise tähtaega.

Muutub see, et kasutajatele antakse kõik asutuse jaoks vajalikud ligipääsud ja asutused ise peavad olema võimelised jagama kasutajaõigusi nii, et iga ametnik näeks vaid enda tööks vajalikku. See paneb töötajatele suurema vastutuse, kui seni.

#### 4.1.8. Politsei infosüsteemi väärkasutamine

Politseiametnike poolt igapäevatööks Politsei infosüsteemi POLIS kasutamine on olnud juba viimased neli aastat inspeksiooni teravama tähelepanu all. Seda eelkõige seepärast, et tegemist on väga suure ja tundliku infosüsteemiga, mille kasutajate hulk on suur. Kuigi juurdepääsud ja andmete töötlemine on väga detailselt reguleeritud ja järelevalvatud, tuleb siiski ette ka hooletust ja pahatahtlikkust. Ühine pingutus koostöös Politsei- ja Piirivalveametiga aitab märksa tõhusamalt kaitsta üksikisiku õigusi tundlikus valdkonnas. Seda illustreerib fakt, et 2014. aastal olime sunnitud väärteokorras karistama andmekogu väärkasutamise eest vaid üht politseiametnikku. Rikkumiskahtluste korral teavitavad AKI ja PPA teineteist; koostöö korras nõustatakse nii juriidiliste kui infotehnoloogiliste probleemide lahendamisel.

#### 4.2. Avalik teave

Avaliku teabe seaduse eesmärgiks on avaliku võimu läbipaistvuse tagamine, mis võimaldab avalikkusel kontrollida avalike ülesannete täitmist. Samuti on avaliku teabe seaduse eesmärgiks võimaldada igähele teabe operatiivne kättesaadavus oma õiguste ja kohustuste realiseerimiseks.

AvTS § 3 lg 1 sätestab, et avalik teave on mis tahes viisil ja mis tahes teabekandjale jäädvustatud ja dokumenteeritud teave, mis on saadud või loodud avalikke ülesandeid täites. Seega ei ole avalikuks teabeks üksnes dokumendid, vaid avalikus teabeks võib olla ka infosüsteemides olev teave, helisalvestised, videod jms. Avalikule teabele võimaldatakse juurdepääs kas teabevaldja poolt omaalgatuslikult asutuse võrgulehe kaudu või vastates isikute/asutuste teabenõuetele.

Admekaitse Inspeksiooni üheks ülesandeks on järelevalve teostamine avaliku teabe seaduses sätestatud nõuete täitmise üle. Oma ülesannete täitmisel kontrollib inspeksioon teabevaldajate poolt seaduse täitmist nii omaalgatuslikult (eelkõige seirete näol) kui ka märgukirjade ja vaiete lahendamise käigus. Samuti annab inspeksioon vajadusel juhised AvTSi tõlgendamisel ja rakendamisel.

Kõige suurema osa AvTSi järelevalvest hõlmab selgitustaotlustele ja märgukirjadele vastamine ning vaiete lahendamine. Läbi aastate esitatakse kõige enam vaideid teabenõuetele vastamata jätmise ja teabenõuete täitmisest keeldumise osas ning kõige rohkem selgitustaotlusi on teabele juurdepääsupiirangute kehtestamise osa. Siinkohal peame vajalikuks märkida, et Andmekaitse Inspeksioon saab anda küll selgitusi, mida tuleb arvestada ja millest lähtuda dokumentidel juurdepääsupiirangute kehtestamisel, kuid inspeksioon ei saa järelevalveasutusena teabevaldajate eest nende valduses olevatele dokumentidele juurdepääsupiiranguid kehtestada.

Kui teabe avalikustamise olukorda võrgulehtedel on inspeksioon püüdnud parandada ennetava tegevusega seirete näol, juhtides asutuste tähelepanu võrgulehel olevatele puudustustele, siis teabe väljastamise vigadest teabenõuete korral on räägitud koordinaatorite võrgustiku kohtumisel. Kahjuks ei hõlma aga koordinaatorite võrgustik kõiki teabevaldajaid.

Üheks oluliseks eksimuseks teabenõuetele vastamisel on see, kui teabenõudja on esitanud asutusele pöördumise, mis on pealkirjastatud „teabenõue“, aga sisult on pöördumine käsitletav selgitustaotlusena, siis teabevaldajad ei teavita teabenõudjat, et käsitlevad tema pöördumist selgitustaotlusena, kuigi seadus seda nõuab.

Näitena võib välja tuua kaasuse, kus kinnipeetav esitas vanglale pöördumise, mis oli pealkirjastatud „Teabenõue“ ning milles kinnipeetav soovis vanglalt teavet, kui suur on aprillikuus iga päeva lõunasöökide lihasisaldus grammides ühe kinnipeetava kohta. Vangla registreeris pöördumise selgitustaotlusena ning vastas 30 päeva jooksul. Samas aga ei teavitanud vangla kinnipeetavat sellest, et käsitleb tema teabenõuet selgitustaotlusena. Kuna vaideotsuse tegemise ajaks oli vangla juba selgitustaotlusele vastanud, siis antud juhul inspeksioon vanglale ettekirjutust küll ei teinud, kuid juhtis vaideotsuses vangla tähelepanu asjaolule, et kui teabenõudja on oma pöördumise



pealkirjastanud teabenõudena, mis aga oma olemuselt on selgitustaotlus, siis tuleb sellele vastata viie tööpäeva jooksul, selgitades, et teabenõudja pöördumist käsitletakse selgitustaotlusena ning sellele vastatakse 30 päeva jooksul.

Teiseks oluliseks eksimuseks on olukord, kus teavet küsitakse asutuselt või asutuse struktuuriüksuselt, kes ei ole seda ise loonud, vaid saanud teiselt asutuselt. Sellises olukorras püütakse teabenõude täitmisest keelduda ja suunata teabenõudja teavet küsima asutuselt (või siis ka asutuse siseselt teiselt struktuuriüksuselt/osakonnalt), kes soovitud dokumendi on koostanud või kelle valduses soovitud dokumendid asuvad.

Näitena võib välja tuua kaasuse, kus Äripäeva ajakirjanik edastas Tallinna Linnakantselei struktuuri kuuluvale ajalehele Raepress ja linnakantselei avalike suhete teenistuse direktorile teabenõude, milles soovis tutvuda Tallinna linnapea ja abilinnapeade välislähetuste käskkirjade, lähetustulemuste aruannete ja lähetuskulude õienditega.

Raepress keeldus teabenõude täitmisest põhjendusega, et teabevaldaja poolt soovitud dokumendid asuvad erinevates struktuuriüksustes, seega on teabenõudjat ammendava ja rahuldava vastuse koostamine komplitseeritud ning ületab Raepressi pädevuse ja võimekuse. Teabega on võimalik tutvuda teabevaldaja juures, kuid see eeldab aega, püsivust ning tugiteenust. Päringuga seotud materjalid asuvad erinevates struktuuriüksustes - käskkirjad personaliteenistuses, lähetusaruanded välissuhete osakonnas ja lähetuskulude õiendid ökonomikaosakonnas. Eeltoodust jäi arusaamatuks kas Raepress keeldus teabenõude täitmisest või soovitas küsida teavet iga dokumendi liigi kohta eraldi erinevatelt struktuuriüksustelt.

Inspektsioonile antud selgitustes leidis Raepress, et antud juhul ei ole olemas sellist dokumenti, kus oleks kirjas linnapea ja abilinnapeade välislähetused ajavahemikus 1. jaanuarist 2012 kuni 17. märtsini 2014, nende välislähetuste aruanded ja iga konkreetse lähetuse kulud. AvTS § 23 lg 2 punkti 5 mõttes on tegemist selgitustaotlusega, millele ei pea vastama, kui selgitustaotlusele vastamine nõuab teabe suure mahu tõttu asutuse või organisatsiooni töökorralduse muutmist, takistab talle pandud avalike ülesannete täitmist või nõuab põhjendamatult suuri kulutusi. Samuti leidis Raepress, et avaliku teabe seaduse mõistes ei ole ajakirjaniku soovitud dokumenti Raepressi poolt loodud ning teabenõuete esitamiseks on linnakantseleis välja töötatud kord teabenõuete esitamiseks ning selleks on võrgulehel vastav vorm.

Andmekaitse Inspektsioon eeltoodud seisukohtadega ei nõustunud ja leidis, et tegemist on teabenõudega, kuna Äripäev soovis tutvuda konkreetsete dokumentidega. Juhul kui Raepress ei olnud pädev teabenõudele vastama, oli Raepressi kui Tallinna Linnakantselei struktuuriüksuse kohustus edastada teabenõue pädevale struktuuriüksusele. Inspektsioon leidis ka, et teabevaldaja valduses oleva teabe koondamine ja juurdepääsu aegade pakkumine on teabevaldaja kohustus ning teabevaldajal pole õigust nõuda erinevate dokumendiliikide osas eraldi teabenõuete esitamist.

Ka leidis Andmekaitse Inspektsioon, et juhul kui teabenõude vastusest eeldada, et teabenõudjal paluti endal erinevate struktuuriüksustega aeg kokku leppida, mida küll teabenõude vastusest kuidagi välja ei lugenud, siis puuduvad andmed, kelle poole oleks tulnud pöörduda. Seega ei saanud teabenõudele vastamist pidada korrektseks, kuna jäeti täitmata AvTS § 15 lõigetest 1 ja 3 tulenev teabenõudja abistamiskohustus. Tulenevalt eelnevast tegi Andmekaitse Inspektsioon Tallinna Linnakantseleile ettekirjutuse vaadata uuesti läbi Äripäeva ajakirjaniku poolt 25.04.2014 Raepressile edastatud teabenõue ning teavitada teabenõudjat, millal ja kus tal on võimalik tema poolt soovitud dokumentidega tutvuda. Teabenõude täitmisest keeldumise korral viidata keeldumisele alusele ja põhjendada keeldumist.

Esineb ka olukordi, kus teabenõude täitmisel ei süüvita teabenõudja poolt soovitud dokumentide sisse, kas need sisaldavad piiranguga teavet või ei ning lähtutakse sarjadele kehtestatud piirangutest, kuigi konkreetne dokument ise piiranguga teavet ei sisalda. Sellise kaasusena võib välja

tuua Eesti Ajalehed ASi esitatud teabenõude Riigikogu Kantseleile, kus teabenõudja soovis Riigikogu liikme välislähetuse kohta vormistatud dokumentide koopaid.

Riigikogu Kantselei keeldus dokumentide väljastamisest põhjusel, et kõik lähetusega seotud dokumendid on tunnistatud ametialaseks kasutamiseks ning täiendava info saamiseks soovitati pöörduda konkreetse Riigikogu liikme poole. Vastuseks teabenõudja täiendavale pöördumisele selgitati, et vastavalt Riigikogu ja Riigikogu Kantselei dokumentide loetelule kehtivad dokumentide sarja „Riigikogu liikmete lähetused lisadega” dokumentidele piirangud järgmistel alustel AvTS § 35 lg 1 punktid 3,11 ja 12 ning lg 2 punktid 2 ja Andmekaitse Inspeksioon leidis, et teabenõude täitmisest keeldumise korral tuleb lähtuda konkreetsele dokumendile kehtestatud piirangutest ning eeltoodud alustel keeldumine ei ole põhjendatud ja tegi Riigikogu Kantseleile järelepärimise. Menetluse käigus dokumentide ülevaatamisel ja hindamisel leidis teabevaldaja ka ise, et eeltoodud piirangud kehtisid sarjale, mitte teabenõudja poolt soovitud dokumentidele, ning väljastas teabenõudjale tema poolt soovitud dokumendid.

### **4.3. Elektrooniliste kontaktandmete kasutamine elektroonilises otseturustuses (spämm)**

Valdav osa elektrooniliste kontaktandmete kasutamisega seotud kaebustest olid seotud otseturustajatega, kes kasutasid otseturustust enda toodete ja teenuste levitamiseks ise või toimus otseturustus otseturustusteenust pakkuva ettevõtte vahendusel. Saabunud kaebuste puhul oli märgata tendentsi, et üldreeglina eemaldas otseturustaja kaebajate elektroonilised kontaktandmed kohe pärast inspeksiooni sellekohast pöördumist. Näiteks oli menetluses juhtum, kus isik oli varasemalt keelanud enda elektronpostiaadressi kasutamise otseturunduslikul ning tarbijaharjumuste uurimise eesmärgil Elektrilevi OÜ suhtes. Ettevõtte selgituste kohaselt saadeti kiri infosüsteemides toimunud muudatuste tõttu, kuid kuna edaspidiselt arvestati kaebaja soovi infokirjast loobumise osas, siis menetlus lõpetati.

Esines ka juhtum, kus inspeksioon tegi seadusliku olukorra taastamiseks otseturustajale kohustusliku ettekirjutuse elektrooniliste kontaktandmete kasutamise lõpetamiseks kommertsteadete saatmiseks. Menetluse käigus tehti Interheat OÜle äriregistris olevaid kontaktandmeid kasutades korduvalt ettepanekuid kommertsteadete saatmise lõpetamiseks. Kui ettepanekutele ei reageeritud, määrati ettevõttele ettekirjutus koos sunniraha hoiatusega.

Elektroonilise side seaduse kohaselt on füüsilisele isikule otseturustusliku teate edastamisel nõusoleku tõendamise kohustus isikul, kelle nimel otseturustust tehakse. Praktikas esines juhtum, kus puudus isik, keda oleks saanud vastutusele võtta: päev enne otseturustusliku teate saatmist oli juriidiline isik äriregistrist kustutatud.

Inspeksioon viis omaalgatuslikult kahe ettevõtte juures läbi järelevalvemenetlused, et kontrollida elektroonilise side seaduse ja isikuandmete kaitse seaduse nõuete täitmist. Shoppa OÜ puhul kontrolliti, kuidas toimub enne kommertstedaannete saatmist nõusolekute võtmine, postiloenditest eemaldamine ja ka nn musta nimekirja pidamine. Nimetatud ettevõttel mingeid erilisi rikkumisi ei esinenud. Lisaks kontrolliti kohapeal Cherry Media OÜ kommertstedaannete saatmist. Ka selle ettevõtte puhul suuri puudusi ei tuvastatud ning ettevõtte selgituste kohaselt viiakse läbi muudatusi uudiskirjadega liitumise osas.

Inspeksiooni poole pöördus 5 eraisikut, kellele Tallinn Arena edastas 31.07.2014 otseturustusliku teate ilma nende eelneva nõusolekuta. Selle teabe alusel algatas inspeksioon omaalgatusliku järelevalvemenetluse. Menetlusest selgus, et kontaktandmeid küsiti personaalselt ning eesmärgiks oli kutse saatmine Tondiraba Jäähalli avamisele - sellest olevat isikuid ka kontaktide kogumise ajal teavitatud. Samas ei olnud võimalik täpselt kindlaks teha, millal ning millisel viisil konkreetse isiku elektronposti aadress teada saadi, sest nõusolekuid ei dokumenteeritud. Samas on märkimisväärne asjaolu, et Tondiraba Spordikeskuse puhul on tegemist Tallinna linna ametiasutuse (Tallinna Spordi- ja

Noorsooameti) hallatava asutusega. Sellest tulenevalt võib Tondiraba Spordikeskus isikuandmeid töödelda ilma nõusolekuta ainult oma ülesannete täitmiseks. Käesoleval juhul ei olnud tegemist Tondiraba Spordikeskusele pandud avaliku ülesande täitmisega. Kui ametiasutus soovib isikute elektroonilisi kontaktandmeid kasutada kommertsteate saatmiseks (sh otseturustuseks), peab see avaliku ülesande puudumise korral toimuma isikuandmete vastavalt kaitse seadusele füüsilise isiku nõusoleku alusel. Menetlusest selgus, et kogutud isikuandmeid ei säilitatud, mistõttu puudus vajadus ettekirjutuse tegemiseks.

Inspeksioon menetles kaebust Scandinavian Marketing OÜ suhtes, kelle käest ning vahendusel sai kaebaja otseturustuslikke teateid. Samas ei suutnud ettevõtte kaebajale selgitada, kustkohast on tema elektronposti aadress saadud. Ka inspeksioonil oli menetluse alguses raskusi selgituste saamisega, kuna ettevõtte ei asunud äriregistris märgitud aadressil, sh ei olnud võimalik ka kontakteeruda äriregistris asuvate elektrooniliste kontaktandmete kaudu. Menetlusest selgus, et ettevõtte poolt kasutatavad elektronposti aadressid on pärit keskkonnast [www.inforegister.ee](http://www.inforegister.ee). Menetluse jooksul kontrolliti ka ettevõtte andmebaasi kaebaja elektronposti aadressi osas, kuid kaebaja elektronposti aadressi nimetatud andmebaasis ei suudetud tuvastada. Ettevõtte juhatause liige ei osanud ka selgitada, kustkohast pärinevad kaebaja elektroonilised kontaktandmed. Kuna elektronposti aadressi enam ettevõtte andmebaasis polnud, siis lõpetati menetlus.

Inspeksioon viis läbi vääртеomenetluse MK Äriühendused OÜ suhtes. Vääртеomenetlusele eelnes 2013. aastal ettevõttele tehtud ettekirjutus, millega kohustati ettevõtet lõpetama ühe füüsilise isiku isikuandmete töötlemine, sh tema elektronposti aadressile kommertsteadete saatmine. Ettekirjutus jõustus ning seda ei vaidlustatud. 2013. aasta lõpus hakkas sama isik uuesti saama MK Äriühendused OÜ vahendusel otseturustuslikke teateid, mistõttu esitati ettevõttele vääртеoteade. Isik oli ka kasutanud edasistest teadetest loobumise võimalust (nn loobumislinki), kuid see ei andnud tulemusi. Vääртеomenetlusest selgus, et algselt asusid elektronposti aadresside andmebaasid vähemalt kolmes eraldi serveris ning kui ühele serverile saadeti loobumise taotlus, siis teistes serverites jäid andmebaasid muutmata. Alates juulist 2014 on kogu andmebaas ühes serveris ning kui isik kasutab loobumise võimalust, siis väidetavalt otseturustust tema suhtes ei rakendata. Vastavalt elektroonilise side seadusele on elektrooniliste kontaktandmete kasutamine otseturustuseks keelatud, kui: edastatud teave ei sisalda juhendit või teavet, mis võimaldab sideteenuse kasutajal, kliendil või ostjal oma õigust keeldumisele realiseerida või sideteenuse kasutaja, klient või ostja on keelanud oma elektrooniliste kontaktandmete kasutamise otseturustuseks. Inspeksiooni koostatud ettekirjutusega keelati MK Äriühendused OÜ avaldaja elektronposti aadressi kasutamine otseturustuses.

Alates 1. jaanuarist 2015 puudub inspeksioonil pädevus elektroonilise side seaduses § 184<sup>2</sup> sätestatud elektrooniliste kontaktandmete kasutamisele kehtestatud nõuete rikkumise eest sama seaduse § 188 lõike 6 alusel algatada vääртеomenetlust. Seega saab inspeksioon alates 1. jaanuarist saabunud kaebusi menetleda vaid järelevalvemenetluse raames.

#### **4.4. Tähelepanu pälvinud muud menetlused**

Kodanik esitas kaebuse turvalahendusi pakkuva firma G4S osas. Kaebaja oli G4S iseteenindust kasutades avastanud, et tema kontaktisikuteks oli märgitud ka isikud, kes olid juba surnud või polnud üldse temaga seotud. Menetlusest selgus, et kontaktisikute nimekirja uuendati andmebaaside korrastamise käigus. Kaebaja kontaktisikute nimekirja sattusid surnud inimeste nimed ja kontaktandmed ekslikult, kuna andmebaasis oli kaks samanimelist klienti. Menetluse jooksul ajakohastati kaebaja kontaktandmed G4Si e-teeninduses ning ettevõtte selgituste kohaselt on uue e-teeninduse rakendamise alates kõikidel kontaktisikutel unikaalne tunnus, mis välistab kliendilepingute andmebaasis kliendi kontaktisikute eksliku valimise. Inspeksioon juhtis G4Si tähelepanu asjaolule, et firma peab kasutusele võtma kohased meetmed, et kaebuses toodud asjaolud ei korduks, sh et e-teeninduses olevad andmed peaksid olema ajakohased ning tõesed.

Kodanik esitas vaide Järva Maavalitsuse osas. Vaide esitaja pöördus maavalitsuse kolme ametniku poole, kuna soovis saada koopiat teise isiku sünnitunnistusest, millel oli märgitud vaide esitaja sünnitunnistusel oleva isiku isana. Järva Maavalitsus keeldus telefoni vahendusel teabenõuet täitmast, kuna telefonivestlusest selgus, et vaide esitaja oli andnud nõusoleku oma lapse lapsendamiseks endise abikaasa uuele mehele ning tema sugulussuhe lapsega on lõppenud.

Teabevaldajal on abistamiskohustus, mis hõlmab kohustust selgitada teabenõudjale teabele juurdepääsu korda, tingimusi ja viise. Inspeksioon leidis, et kõik ametnikud täitsid kaasaaitamise kohustust, sh selgitati kirjaliku teabenõude esitamise võimalust. Maavalitsuse puhul on tegemist nii teabevaldaja kui ka isikuandmete töötlejaga, mistõttu on tal võimalik kasutada nii isikuandmete kaitse seadusest kui ka avaliku teabe seadusest tulenevaid keeldumise aluseid. Inspeksioon nõustus, et kuna vaide esitaja oli andnud lapse lapsendada, siis lõppes tal sellega ka õigus saada enda bioloogilise lapse kohta isikuandmeid. Teabenõudes soovitud teabe (algse sünnitunnistuse) väljastamine võib kahjustada teise isiku õigusi ja vabadusi ning ohustada lapse põlvnemise saladuse kaitset. Kuna teabevaldaja täitis AvTS § 15 lõikes 1 sätestatud kaasaaitamiskohustust ning vaide esitajal puudus õiguslik alus soovitud teabe saamiseks, siis puudus inspeksioonil alus ettekirjutuse tegemiseks ning vaide jäi rahuldamata.

## 5. Audiitor ja loaandja

### 5.1. Seired

#### 5.1.1 Avaliku teabe seaduse täitmise seire

Andmekaitse Inspektsioon viis 2010-2014 aastal läbi avaliku teabe täitmise seire, mille käigus hinnati ministeeriumide, nende hallatavate riigiasutuste ja avalik-õiguslike juriidiliste isikute dokumendiregistrite pidamise vastavust avaliku teabe seaduse nõuetele. Dokumendiregistrite, mis on oluline töövahend tagamaks asutuste tegevuse avalikkus ja ligipääs avalikule teabele, võrgulehele paigutamise kohustus tuleneb avaliku teabe seaduse § 28 lg 1 punktist 31. Nõuded dokumendiregistrile sätestab avaliku teabe seadus § 12.

Kontrolliti järgnevate nõuete täitmist:

- \*dokumendiregistri olemasolu;
- \*dokumendiregistri mitte leitavust interneti otsingumootorite abil;
- \*kasutusjuhendi olemasolu;
- \*dokumendiregistri avalikku vaadet katva üldtekstiotsingu olemasolu;
- \*kirjavahetuse dokumentide kuvamist säilitustähtajaga sama aja vältel;
- \*käskkirjade kandmine dokumendiregistrisse;
- \*juurdepääsupiiranguga dokumentide pealkirjade korrektne sõnastus, mis ei võimaldaks dokumentide sisu aimata;
- \*sarjapiirangu korral AK-märke juures või dokumendiregistri kasutusjuhendis selgituse olemasolu, et märke ei sega teabenõude esitamist;
- \*lepingute, mille sisule on kehtestatud juurdepääsupiirang nt ärisaladuse tõttu, olemasolu.

Seiratud asutused

Majandus- ja Kommunikatsiooniministeerium, Konkurentsiamet, Lennuamet, Maanteeamet, Patendiamet, Tehnilise Järelevalve Amet, Tarbijakaitseamet, Veeteede Amet, Patendiinfo Keskus, Riigi Infosüsteemide Arenduskeskus, Kultuuriministeerium, Eesti Rahvusringhääling, Eesti Kultuurkapital, Eesti Rahvusraamatukogu, Palamuse O. Lutsu Kihelkonnamuuseum, Eesti Filmi SA, Teater Vanemuine, Eesti Riiklik Nukuteater, Teater Vanalinnastuudio, Eesti Kontsert, Eesti Riiklik Sümfooniaorkester, Eesti Filharmoonia Kammerkoor, Eesti Lastekirjanduse Keskus, Eesti Hoiuraamatukogu, Rahvusooper Estonia, Ennistuskoda Kanut, Rahvakultuuri Arendus- ja Koolituskeskus, Võru Instituut, Põllumajandusministeerium, Põllumajandusamet, Veterinaar- ja Toiduamet, Põllumajanduse Registre ja Informatsiooni Amet, Põllumajandusuuringute Keskus, Jõudluskontrolli Keskus, Veterinaar- ja Toidulaboratoorium, Maamajanduse Infokeskus, Eesti Maaviljeluse Instituut, Eesti Piimandusmuuseum, C.R. Jakobsoni Talumuuseum, Jõgeva Sordiareture Instituut, Eesti Põllumajandusmuuseum, Haridus- ja Teadusministeerium, Riiklik Eksami- ja Kvalifikatsioonikeskus, Keeleinspektsioon, Eesti Hariduse ja Teaduse Andmesidevõrk EE Neti, Eesti Noorsootöö Keskus, Astangu Kutserehabilitatsiooni Keskus, Tervise Arengu Instituut, Illuka Varjupaigataotluste Vastuvõtukeskus, Raviamet, Sotsiaalkindlustusamet, Terviseamet, Tööinspektsioon, Sotsiaalministeerium, Muinsuskaitseamet, Eesti Nuku- ja Noorsooteater, Pärnu Teater Endla, Eesti Arhitektuurimuuseum, Eesti Ajaloomuuseum, Eesti Meremuuseum, Eesti Kunstimuuseum, Eesti Spordimuuseum, Eesti Rahva Muuseum, Harjumaa Muuseum, Hiiumaa Muuseum, Iisaku Muuseum, Järvamaa Muuseum, Läänemaa Muuseum, Eesti Tarbekunsti- ja Disainimuuseum, Dr. Fr. R. Kreutzwaldi Memoriaalmuuseum, Tartu Kunstimuuseum, Eesti Tervishoiu Muuseum, Eesti Teatri- ja Muusikamuuseum, Eesti Vabaõhumuuseum, Rannarootsi muuseum, Viljani Muuseum, Valga Muuseum, Tartumaa Muuseum, Saaremaa Muuseum, Pärnu Muuseum, Põlva Talurahvamuuseum, Mahtra Talurahvamuuseum, Martna Vallavalitsus, Kõrgessaare Vallavalitsus, Vormsi Vallavalitsus, Lohusuu Vallavalitsus, Avinurme Vallavalitsus, Aseri Vallavalitsus, Alajõe Vallavalitsus, Oru Vallavalitsus, Nõva Vallavalitsus, Noarootsi Vallavalitsus, Viiratsi Vallavalitsus, Suur-Jaani Vallavalitsus, Seerepeedi Vallavalitsus, Kõo Vallavalitsus, Kolga-Jaani Vallavalitsus, Keskkonnateabe Keskus,

Keskonnaamet, Keskkonnainspeksioon, Maa-amet, Keskkonnaministeerium, Tallinna Tehnikaülikool, Eesti Maaülikool, Tallinna Ülikool, Narva Linnavalitsus, Narva-Jõesuu Linnavalitsus, Vaivara Linnavalitsus, Sillamäe Linnavalitsus, Toila Vallavalitsus, Jõhvi Linnavalitsus, Kohtla-Järve Linnavalitsus, Püssi Linnavalitsus, Kiviõli Linnavalitsus, Tudulinna Vallavalitsus, Eesti Keele Instituut, Eesti Biokeskus, Eesti Lennuakadeemia, Eesti Kunstiakadeemia, Eesti Muusika- ja Teatriakadeemia, Tartu Ülikool, Eesti Mereakadeemia, Tallinna Tehnikakõrgkool, Tartu Observatoorium, Tallinna Pedagoogiline Seminar, Ida-Viru Maavalitsus, Kaitseliit, Murru Vangla, Registrate ja Infosüsteemide Keskus, Siseministeeriumi Infotehnoloogia ja Arenduskeskus, Misso Vallavalitsus, Meremäe Vallavalitsus, Laheda Vallavalitsus, Kõlleste Vallavalitsus, Mooste Vallavalitsus, Alatskivi Vallavalitsus, Alatskivi Vallavalitsus, Anija Vallavalitsus, Jõelähtme Vallavalitsus, Kiili Vallavalitsus, Eesti Kirjandusmuuseum, Põlula Kalakasvatusteskeskus, Meteoroloogia ja Hüdroloogia Instituut, Eesti Loodusmuuseum.

Seire algas 09.08.2010 ja lõppes 11.12.2014 ehk kestis kokku 4 aastat 4 kuud ja 2 päeva.

Seire andmed

Kokku seirati 144 asutust, 144st asutusest kahele saadeti ainult 1 kiri, mis sisaldas arvamust, et asutuse dokumendiregister vastab täielikult avaliku teabe seaduses sätestatud nõuetele. Nendeks asutusteks olid Eesti Filmi Sihtasutus ja Eesti Riiklik Nukuteater.

85 asutusele tuli saata 2 kirja dokumendiregistri avaliku teabe seaduse nõuetega vastavusse viimiseks.

34 asutusele tuli inspeksioonil saata 3 korduvat arupärimist dokumendiregistri seaduslikkuse kohta.

15 asutuse puhul pidi inspeksioon pöörduma nende poole 4 korral, mille tulemusena suudeti dokumendiregister korrastada.

6 asutuse puhul pidi inspeksioon saatma välja 5 järelepärimist, ühe puhul 6 ning ühe asutuse puhul kokku 7 järelepärimist. Kõige rohkem kirju saatis inspeksioon Eesti Kultuurkapitalile ja Eesti Kirjandusmuuseumile.

Põhilised vead: dokumendiregistri avaliku vaate täielik puudumine, juurdepääsupiirangute puudumine dokumendiregistris olevatel kirjadel, käskkirjade puudumine dokumendiregistrist ning lepingute puudumine dokumendiregistrist.

Kokkuvõte

Pärast suuremahulise seire läbi viimist on kõikidel kontrollitutel toimiv dokumendiregister, mis vastab avaliku teabe seadusele.

### **5.1.2. Kohalike omavalitsuste võrgulehtede valgusfooriseire**

Seire eesmärgiks oli kontrollida omavalitsuste võrgulehtedel teabe avalikustamist vastavalt avaliku teabe seaduses sätestatud nõuetele ning kas võrgulehel on avalikustatud ka teavet, mida kodanikud võivad küll vajada, kuid mille avalikustamise kohustust otseselt seadusest ei tulene (näiteks asutuse tööaeg). Lisaks hinnati ka teabe leidmise lihtsust ning asutuse tegevuse läbipaistvust.

Kui kahel eelneval aastal viis inspeksioon võrgulehtedel teabe avalikustamise osas seire läbi riigiasutustes, siis 2014. aastal otsustati seirata kohalike omavalitsuste võrgulehti. Et seire läbiviimine ei tuleks omavalitsustele üllatusena, siis edastas inspeksioon 2014. aasta suve hakul kõigile 215le omavalitsustele teate, milles teavitati omavalitsusi, et augustis ja septembris viiakse läbi omavalitsuste võrgulehtede seire. Teatele lisati ka 15 punkti, mida võrgulehel vaadeldakse. Seire käigus vaadeldi omavalitsustele edastatud 15st punktist 10t.

Kuigi omavalitsustel oli teada, millal ja mida seire käigus hinnatakse ja vaadeldakse, esines siiski üllatavalt palju puudusi. Kõige enam puudusi oli piiranguta e-kirjadele dokumendiregistri kaudu juurdepääsu võimaldamisel.

AvTS § 14 lg 41 sätestab, et dokumendiregistris registreeritud ja dokumendihaldussüsteemis sisalduvatele elektroonilistele dokumentidele, millele ei ole kehtestatud juurdepääsupiirangut, tagatakse juurdepääs dokumendiregistri kaudu. Seire käigus tuvastati, et osad omavalitsused ei võimalda ühelegi elektroonilisele dokumendile oma dokumendiregistri kaudu juurdepääsu. Samuti võimaldasid osad omavalitsused piiranguta elektroonilistele dokumentidele juurdepääsu osaliselt.

Samuti olid seire ajal mitmel omavalitsusel viimased dokumendid registreeritud kuu või rohkem tagasi. Ajakohase dokumendiregistri puudumist põhjendati mitmel korral sellega, et sekretär oli puhkusel. Siiski esines ka juhuseid, kus tegemist oli tehnilise veaga, millisel juhul ametniku vaates olid dokumendid kõik korrektselt registreeritud ja nähtavad, kuid süsteem ei kuvanud neid välisvaatesse. 215st kontrollitud omavalitsusel esines eeltoodu osas puudusi 173l.

Teiseks suuremaks puuduseks oli omavalitsuste võrgulehtedel puuduv teave, kuidas asutuses töödeldakse kodanike isikuandmeid, kui kodanik pöördub asutuse poole. Selline teave puudus 153 omavalitsuse võrgulehel.

Veel oli enim puudusi võrgulehel teabe avalikustamisega riigihangete kohta. Seire käigus ilmnes, et kõik omavalitsused ei avalikusta oma võrgulehel kõiki riigihankeid. Kui võrrelda võrgulehel avalikustatud riigihankeid Riigihangete registris olevate andmetega, siis ilmneb, et Riigihangete registris on rohkem hankeid kui asutus on oma võrgulehel avalikustanud, ehk siis võrgulehel ei ole avalikustatud teavet kõigi hangete kohta.

Oli ka omavalitsusi, kus võrgulehel oli avalikustatud ainult hankeplaan, millest tegelikult ei nähtu, millised hanked on toimunud või millised käimas. Samuti oli võrgulehti, kus puudus igasugune teave hangete kohta või oli teave vananenud. Muude kontrollitud punktide osas oli rikkumisi vähem.

Peale seire läbi viimist edastas inspeksioon kõigile omavalitsustele ettepaneku avaliku teabe seaduse paremaks rakendamiseks, milles märkisime ära omavalitsuse võrgulehel seire käigus tuvastatud puudused ning palusime need kõrvaldada. Omavalitsustelt saadud tagasisidest selgus, et paljud omavalitsused oli oma võrgulehete uuendamas ning seetõttu ei kogu teave nõuetekohaselt avalikustatud. Samuti on omavalitsused teavitanud, et on asunud võrgulehel esinenud puudusi kõrvaldama.

Samuti selgus ka tagasisidest, et nii mõnelgi korral oli teave, mida inspeksioon seire käigus ei leidnud, asutuse võrgulehel siiski olemas, kui see oli raskesti leitav. Sellisel juhul on andnud inspeksioon soovitusi, kuidas teavet avalikustada, et see oleks lihtsamini leitav. Antud menetluse käigus saatis inspeksioon välja kokku 425 kirja.

Et parandada teabe kättesaadavust võrgulehtede kaudu ning asutuste läbipaistvust, on inspeksioonil kavas jätkata ka edaspidi asutuste võrgulehtede seiret.

### **5.1.3. Elektroonikaseadmete utiliseerijate seire**

Viisime juunis läbi seire, et saada ülevaade isikuandmete töötlemise olukorrast elektroonikaseadmete ja elektroonikaromude utiliseerimise teenust osutavates ettevõtetes.

Saatsime 10-le jäätmekäitlusteenust osutavale ettevõttele küsimustiku, millele vastas 7 ettevõtet. Vaatluse all olid andmete (sh isikuandmete) salvestamist ja taasesitamist võimaldavad seadmed, nagu laua- ja sülearvutid, tahvelarvutid, nutitelefonid, välised mäluseadmed (CD-ROM, mälupulk, väline kõvaketas), salvestamist võimaldavad kaamerad, navigeerimisseadmed jms. Mainitud seadmed



võivad olla isikuandmeid sisaldavateks teabekandjateks. Seega võib utiliseerimine kaasa tuua ka isikuandmete töötlemise, kui enne utiliseerimist ei ole teabekandjal olevaid isikuandmeid kustutatud. Isikuandmeteks on nii elektroonilistes dokumentides olevad isikut tuvastada võimaldavad andmed, aga ka fotod, millele on konkreetne inimene jäädvustatud. Isikuandmeid võivad sisaldada ka helisalvestised jm failid.

Inspektsioon jäi seire tulemustega üldjoontes rahule. Samas tuvastasime mõningased probleemid jäätmekäitleja ja jäätmevaldaja vahelistes lepingutes, kus ei ole alati fikseeritud jäätmekäitleja konfidentsiaalsuskohustus.

Seire kokkuvõttes soovitasime jäätmekäitlejatel mõelda elektroonikaseadmete valdaja informeerimise vajadusele, mis suunaks neid enne elektroonikaseadme üleandmist sealt eelnevalt kõik andmed kustutama.

#### **5.1.4. Kiirlaenuandjate seire**

Andmekaitse Inspektsioon viis 2014. aastal koostöös Tarbijakaitseametiga läbi kiirlaenuandjate seire. Inspektsioon soovis saada ülevaadet kiirlaenuandjate poolt klientide isikuandmete töötlemisest. Täpsemalt kogutavate isikuandmete koosseisust, isikuandmete allikatest, andmete töötlemise eesmärkidest, isikute kategooriatest, kelle andmeid töödeldakse ja andmete säilitamistähtaegadest. Tarbijakaitseameti sooviks oli saada ülevaade lepingute sõlmimiseks kogutava teabe mahust ja sisust, samuti selgitada välja, kuidas ja milliste dokumentide alusel hinnatakse tarbijate maksevõimet

Andmekaitse Inspektsiooni seires osales 19 ettevõtet, millest üheksat ettevõtet seirati koos Tarbijakaitseametiga. Koos ametiga käidi kohapeal kontrollimas kolme ettevõtet.

Kokkuvõtvalt sai öelda, et rahule võis jääda kogutavate andmete koosseisuga, kasutatavate allikatega ja isikute kategooriatega, kelle andmeid töödeldi - kõik see vastas kenasti andmete töötlemise eesmärkidele. Midagi üleliigset ja kellegi üleliigse kohta andmeid ei kogutud. Olukord ei olnud rahuldav osas, mis puudutas kogutud andmete säilitamistähtaegasid, paljud ettevõtted ei olnud selle peale üldse mõelnud või olid säilitamistähtajad lühemad, kui seadus ette nägi.

Andmete säilitamise osas tegi inspektsioon enamusele seiratavatele soovitus isikuandmete kaitse seaduse paremaks rakendamiseks. Nimelt leidis inspektsioon, et lepingulisi kohustusi korralikult täitvate klientide puhul tuleb lähtuda raamatupidamise seadusest, mille kohaselt peab raamatupidamiskohustuslane raamatupidamise algdokumente säilitama seitse aastat, alates selle majandusaasta lõpust, mil algdokument raamatupidamises kajastati.

Mis puudutas lepingulisi kohustusi eiravaid kliente, soovitas inspektsioon andmete säilitamisel lähtuda nõude aegumise tähtaegadest. Tsiviilseadustiku üldosa seaduse § 146 lõige 1 sätestab, et tehingust tuleneva nõude aegumistähtaeg on kolm aastat. Sama paragrahvi lõike 4 kohaselt on nõuete aegumistähtaeg kümme aastat, kui kohustatud isik rikkus oma kohustusi tahtlikult. Inspektsioon ei saa anda hinnangut, kas isikute võlanõuded võlausaldaja ees olid tekkinud õiguspäraselt või kas isikud olid kohustusi võlausaldaja ees rikkunud tahtlikult.

Arvestades võimalusega, et kohustusi võib olla rikutud tahtlikult, lähtub inspektsioon täitmata kohustuste puhul 10-aastasest aegumistähtajast. Et mitte asetada kohustuse täitnud isikuid ebavõrdsesse olukorda (kuivõrd isikuandmete kaitse seaduse § 11 lg 7 punkt 4 lubab nõude täitmisest veel 3 aasta jooksul andmeid avaldada), lähtub inspektsioon olukorras, kus kohustus on täitmata kuid aegunud, proportsionaalsuse põhimõtet arvestava avaldamise maksimaalse tähtaja määramisel 13 aastast arvates nõude sissenõutavaks muutumisest.

Nõuete kohtu kaudu sissenõudmisel algab nõude aegumistähtaeg kohtuotsuse jõustumisest. Tulenevalt tsiviilseadustiku üldosa seaduse §st 157 on jõustunud kohtuotsusega tunnustatud nõude aegumistähtaeg 10 aastat, mis algab kohtuotsuse jõustumisest või muu täitedokumendi väljaandmisest, kuid mitte enne nõude sissenõutavaks muutumist.

Andmete säilitamistähtajad vastasid seaduses toodud nõuetele üksnes kahel ettevõttel – SNEL Grupp OÜ ja Trimo Investments OÜ.

Seire käigus vaadeldi järgmisi ettevõtteid: BB Finance OÜ, Credit Invest OÜ, Express Credit AS, Ferratum Estonia OÜ, Folkia AS Eesti filiaal, HALL Laenud OÜ, OÜ Investhaus Pluss, isePankur AS, KiirLaenud OÜ, MCB Finance Estonia OÜ, AS MiniCredit, Omalaen OÜ, Omaraha OÜ, Placet Group OÜ, Raha24 OÜ, SMS Laen AS, SNEL Grupp OÜ, Ziip OÜ, OÜ Trimo Investments.

### **5.1.5. Interneti rehitsemise päeva seire**

Käesoleva aasta mais seiras Andmekaitse Inspeksioon Eesti kasutajatele mõeldud erinevate nutiseadmete rakendusi eesmärgiga saada laiaulatuslik ülevaade tingimustest ja praktikatest, millistele andmetele nutirakendused juurdepääsu küsivad ja kuidas saadud andmeid hiljem kasutatakse. Samuti pööras inspeksioon seire käigus tähelepanu andmete hulgale, millele juurdepääsu küsitakse ning hindas, kas juurdepääsu küsimine on põhjendatud ja vastavuses reguleeritud korraga.

Seire tulemusena sai esile tuua rea rakendusi, kus isikuandmete töötlemine on reguleeritud arusaadavalt ja töötlemise kord hõlpsasti leitav. Tunnustust väärtsid näiteks Elektriäpp, Taxify, Weekdone, Anna teada, Sportlyzer GPS Sports Tracker ja Bluesec Wifi Bluetooth Unlocker.

Enamlevinud probleemid, millega inspeksioon kokku puutus, olid isikuandmete töötlemise korra puudumine, korra raske leitavus või ei olnud isikuandmete töötlemise kord mõeldud ainult rakendusele, vaid reguleeris kogu ettevõtte isikuandmete töötlemist. Rakenduste puhul, mis koguvad palju isikuandmeid või tahavad paljudele andmetele juurdepääsu, peaks olema isikuandmete töötlemise kord olemas rakendustepoes, rakenduses endas ja/või viitega ettevõtte kodulehel. Kõikide rakenduste puhul ei ole isikuandmete töötlemise kord nõutav, näiteks kui rakendus kasutab andmeid ainult funktsioneerimiseks nagu kiiruskaamerate rakendus.

Seire toimus andmekaitse järelevalveasutuste ülemaailmses koostöös ühiselt tähistatava Interneti rehitsemise päeva (*Internet Sweep Day*) raames. Rehitsemise päeva korraldaja oli ülemaailmne eraelukaitse võrgustik GPEN (*Global Privacy Enforcement Network*). Seiret koordineerivaks asutuseks oli Kanada andmekaitseasutus.

Seire käigus tehti koostööd konkursi „Eesti parim mobiilirakendus 2014“ korraldaja, Riigi Infosüsteemi Ameti ning avaliku- ja erasektori organisatsioonide koondava algatusega „Nutikaitse 2017“. Seire viidi läbi IOSi ja Androidi platvormidel ning seiratud rakendused olid Elektriäpp, Piletilevi, RMK, Bluesec Wifi Bluetooth Unlocker, Taxify, Pargi.ee, KV Üürivad, Swedbank, DigiDoc 3 Android, EMHI Weather, Weekdone, M-Tartu, Anna teada, Starman, TRAFI Eesti, Eesti spordiregister, LHV, Like a Local, Kiiruskaamerad, Stortlyzer GPS Sports Tracker, Rahvuskalender, Kes käis?, DigiDoc, Hall ilm, Elmo kiirLaadimine, EMT Live, Auto24.ee, Bluetec Wifi Bluetooth Unlocker, Seb Eesti ja Estonia Radio Player.

### **5.1.6. E-lasteaedade seire**

Läinud aasta oktoobris-novembris viis Andmekaitse Inspeksioon läbi e-lasteaedade järelevalve, mille käigus saadi ülevaade Eesti e-lasteaedade infosüsteemide üldistest andmeturbe põhimõtetest ja rakendatavatest turvameetmetest.

Inspeksioon hindas üldise teadlikkuse vajalikest andmeturbemeetmetest heaks. Kõik kolm kontrollitud ettevõtet olid vastavalt isikuandmete kaitse seadusest tulenevale nõudele ennast registreerinud Andmekaitse Inspeksiooni delikaatsete isikuandmete töötlemise registris. Viimase 12 kuu jooksul olid e-lasteaiad panustanud regulaarselt oma infosüsteemide turvalisusse ja täiustanud turvameetmeid, samuti analüütsid võimalikke turvariske ning kohaldati vastavalt sellele ka infosüsteemid.

Järjest rohkem Eesti lasteaedu kasutab igapäevaseks tööks ja lastevanematega suhtlemiseks mõnda infosüsteemi ehk nn e-lasteaeda. Enamasti on tegu teenusepakkujatega ehk lasteaiad ise nimetatud infosüsteeme ei oma ega halda nagu ka põhikoolide ja gümnaasiumite puhul (e-kool). See toob kaasa olukorra, kus nimetatud valdkonnas tegutsevate eraettevõtete kätte koondub järjest rohkem laste isikuandmeid, mistõttu on see pälvunud ka Andmekaitse Inspektsiooni erilise tähelepanu.

## **5.2. Auditid**

### **5.2.1. Terviseandmed ja e-Tervise infosüsteem**

Inspektsioon kontrollis kaht haiglat seoses seal kasutatavate infosüsteemidega ning infosüsteemide vastavusega isikuandmete kaitse seadusest (IKS) tulenevatele nõuetele. Auditi käigus kontrolliti, kuidas toimis logide süsteem, kuidas oli reguleeritud juurdepääs andmetele, kuidas oli korraldatud andmete (ka paberandjal) säilitamine, sh varundamine, kuidas korraldati andmete hävitamine, kas andmeid krüpteeriti ja edastati ehk kas andmetöötlus oli liidestatud e-tervise infosüsteemiga. Auditeeriti SA Läänemaa Haiglat (SALMH) ning SA Tallinna Lastehaiglat (TLH).

SALMHis on kasutusel haigla infosüsteemina ESTER ning auditeerimise käigus tuvastati järgnev:

- \*kõigi pöördumiste kohta andmekogusse jäi jälj ehk logi ning kõik pöördumised haigla infosüsteemi poole oli võimalik tuvastada;
- \*juurdepääs infosüsteemi andmetele sõltus kasutajale antud õigustest ehk oli vastavuses teenistuja rolliga (ametikoht) haiglas;
- \*kasutaja identifitseerimiseks ja autentimiseks kasutati kasutajanime ja parooli lahendust;
- \*SALMH tagas isiku (andmesubjekti) õiguse saada enda kohta käivaid andmeid, samuti toimis andmete varundamine ja hävitamine vastavalt isikuandmete kaitse seadusele;
- \*SALMHi infosüsteem ESTER oli liidestatud e-Tervise infosüsteemiga.

Inspektsioon järeldas auditis, et SALMHis rakendatavad turvameetmed hoiavad ära andmete kaotsi mineku või isikuandmete omavolilise kasutamise ehk isikuandmete kaitse seaduse turvanõuete üldpõhimõtted on täidetud.

Samal eesmärgil auditeeriti ka Sihtasutust Tallinna Lastehaigla (TLH), mis kasutab andmete töötlemiseks haigla infosüsteemi LIISA. Analoogselt ESTERi lahendustele on ka LIISA puhul kõik TLH poolt püstitatud andmetöötlamise eesmärgid täidetud. Erinevus ESTERiga seisneb sisselogija autentimisel ehk LIISAsse on võimalik siseneda ainult ID-kaardi abil. Kasutajatele lubatud tegevused on määratud rollide ja õiguste süsteemiga. LIISA on oma ülesehituselt teenuse põhine infosüsteem, mis on kasutajate jaoks loogiline ning lihtsasti mõistetav ja kasutatav. LIISA on liidestatud täies mahus e-Tervise lahendustega ning Eesti Haigekassa retseptikeskusega.

Inspektsiooni seisukoht oli, et lastehaiglas rakendatavad turvameetmed on piisavad selleks, et kaitsta isikuandmete kaotsi minekut või nende omavolilist kasutamist.

### **5.2.2. Tallinna Transpordiamet**

Veebruaris 2014 viis Andmekaitse Inspektsioon omaalgatuslikult läbi auditi isikuandmete kaitse meetmete kontrollimiseks Tallinna Transpordiametis (edaspidi TTA).

Auditi eesmärk oli teha kindlaks, kas isikuandmete töötlemisega seotud tegevused TTA-s on vastavuses organisatsiooni isikuandmete kaitse poliitika ja protseduuridega ning kas isikuandmete töötlemine vastab isikuandmete kaitse seaduse nõuetele ning kas TTA päringud sõiduki omaniku ja sõiduki vastutava kasutaja kohta Maanteeameti liiklusregistrisse on eesmärgipõhised ning kas järgitakse minimaalsuse põhimõtet.

Inspektsiooni seisukoht oli, et Tallinna Transpordiametis rakendatavad turvameetmed on piisavad isikuandmete turvaliseks hoidmiseks ning takistavad isikuandmete omavolilist kasutamist – isikuandmete kaitse seaduse turvanõuete üldpõhimõtted olid täidetud.

Süsteemi parendamiseks soovitas inspeksioon TTAI sõlmida Maanteeametiga liiklusregistri andmete automaatse töötlemise lepingu ning fikseerida Maanteeameti ja TTA õigused ja kohustused.

Asutuse tähelepanu juhiti asjaolule, et TTA kui teabevaldaja peab lähtuma avaliku teabe seaduse nõuetest ning tagama, et teabele turvasüsteemide, turvaorganisatsiooni või turvameetmete kirjelduse kohta kehtib juurdepääsupiirangu nõue.

### **5.2.3. Tallinna Munitsipaalpolitsei Amet**

Omaalgatusliku auditi korras kontrolliti ka Tallinna Munitsipaalpolitsei Ametit (edaspidi MUPO). Eesmärgid olid analoogsed TTAga.

Auditi käigus selgus, et ka MUPOs rakendatavad turvameetmed tõkestavad isikuandmete kaotsi minekut ning nende omavolilist kasutamist, st isikuandmete kaitse seaduse turvanõuete üldpõhimõtted olid täidetud.

Süsteemi parendamiseks soovitas inspeksioon MUPOI uuendada Tallinna väärteoasjade registri (VTR) põhimäärust, mis kajastaks ja reguleeriks kõiki andmetöötlemise aspekte. Põhimääruses tuleks kirjeldada kõik registrisse kantavad andmekoosseisud; andmete säilitamistajad nii registris aktiivselt sisalduvate andmete kui arhiivandmete puhul; registrisse kandmise aluseks olevad dokumendid; registre ja andmebaaside loetelud koos konkreetsete andmekoosseisudega, mis kantakse VTR-i ning andmete registrist kustutamise või sulgemise aeg ja kord.

## **5.3. Loamenetlused**

### **5.3.1. Teadusuuringute load**

Isikuandmete kaitse seaduse § 16 reguleerib isikuandmete töötlemist teadusuuringu või riikliku statistika vajaduseks. Teadusuuringuid, mis kasutavad isikuandmeid, võib läbi viia kodeeritud kujul või inimese nõusolekul ning on ka võimalus nõusolekuteta uuringuks isikuandmetele juurdepääsuks taotleda luba Andmekaitse Inspeksioonilt. Loataotlus peab vastama seaduses sätestatud tingimustele, milleks on näiteks ülekaalukas avalik huvi, piisavad turvameetmed ja adekvaatne põhjendus, miks eesmärgi saavutamine oleks ebamõistlikult raske kasutades ainult isikustamata andmeid. Kui teadusuuring hõlmab delikaatseid isikuandmeid, peab taotleja end registreerima ka delikaatsete isikuandmete töötlemise registris.

2014. aastal menetles inspeksioon kokku kolmteist loataotlust. Inspeksioon andis 7 korral loa teadusuuringu teostamiseks ning 6 korral jättis taotluse läbi vaatamata. 5 korral 13-st saatis inspeksioon taotluse tagasi puuduste kõrvaldamiseks, millest 2 asutust kõrvaldasid puudused õigeaegselt ning 3 jätsid puudused õigeaegselt kõrvaldamata. Sellest hoolimata, et taotlusi ei rahuldatud, võis taotleja esitada uue taotluse, milles olid eelnevalt mainitud puudused kõrvaldatud. 5 korral 13-st oli taotlus isikuandmete töötlemiseks teadusuuringus vormistatud korrektset ning 3 korral 13-st jäeti taotlus läbi vaatamata koheselt, kuna taotluse esitajal ei olnud inspeksiooni luba vaja.

Asutused, kes 2014. aastal said loa teadusuuringute läbiviimiseks, olid sihtasutus Tartu Ülikooli Kliinikum (3 teadusuuringut), Tartu Ülikool, Tartu Ülikooli tervishoiu instituut, Tallinna Tehnikaülikool ja Sisekaitseakadeemia. Teadusuuringute teemade üldised kategooriad puudutasid viiel korral terviseandmeid ja meditsiini, 1 korral sooviti teadusuuringu läbiviimiseks juurdepääsu karistusregistri andmetele ning 1 korral sooviti uuringu läbiviimiseks haridusandmeid ning andmeid investeerimistehingute kohta väärtpaberi ja kinnisvaraturul.

### **5.3.2. Delikaatsete isikuandmete registreerimine**

Delikaatsete isikuandmete töötlemise registreerimine ja isikuandmete kaitse eest vastutavate isikute määramine toimub digitaalselt inspeksiooni võrgulehel oleva registri kaudu. Kuna valdava osa

delikaatsete isikuandmete töötajatest moodustavad erinevad tervishoiuteenuse osutajad, kasutavad infoliinilise nõustamise võimalust eeskätt just tervishoiutöötajad, kes registri kohta küsimusi esitavad. Põhiliselt tuntakse huvi registreerimismenetluse ja elektroonilise taotluse esitamise vastu ning kuidas kontrollida registreeringute olemasolu.

<b>Delikaatsete isikuandmete töötlemise (DIAT) registreerimine, haldussund ja karistused</b>	
DIAT registreerimine	534
DIAT muudatuse registreerimine	105
DIAT lõpetamise registreerimine	18
Vastutava isiku registreerimine	195
Vastutava isiku muudatuse registreerimine, sh ühe isiku teisega vahetamine	11
Vastutava isiku tagasikutsumine koos DIAT lõpetamisega	5
DIATR taotluste rahuldamata v. läbivaatamata jätmine	12
Ettekirjutus(-hoiatus) DIATR kohustuse asjus	45

### **5.3.3. Andmekogude kooskõlastamismenetlused**

Andmekaitse Inspeksioon kooskõlastab AvTS § 43<sup>3</sup> lõike 3 alusel avaliku sektori andmekogusid andmekogu asutamise, kasutusele võtmise, andmekogusse kogutavate andmete koosseisu muutmise või andmekogu lõpetamise puhul. Kooskõlastamine toimub ühises võrgupõhises kooskõlastamissüsteemis - riigi infosüsteemi haldussüsteemis (RIHA).

2014. aastal esitati RIHA-s kooskõlastamisele 115 andmekogu. Andmekogude asutamise kooskõlastasime 36 korral ja andmekogu kasutusele võtmise 38 korral.

Eelmisel aastal esile tõstetud probleem, et andmekogus töödeldavate andmete koosseisude kirjeldamisel kasutatakse liigset üldsõnalisust, mis ei võimalda teha kindlaks, milliseid andmeobjekte tegelikult töödeldakse, on olnud ka 2014. aastal aktuaalne. Samas tuli korduvalt selgitada täiendavalt ka andmetöötlemise kohta logide pidamise nõudeid. Isikuandmete kaitse seaduse § 25 lg 2 punktide 3 ja 5 tuleneb nõue, mille kohaselt peab isikuandmete töötaja tagama, et tagantjärele oleks võimalik kindlaks teha, millal, kelle poolt ja milliseid isikuandmeid salvestati, muudeti või kustutati või millal, kelle poolt ja millistele isikuandmetele andmetöötlussüsteemis juurdepääs saadi; samuti peab isikuandmete töötaja tagama andmete olemasolu isikuandmete edastamise kohta: millal, kellele ja millised isikuandmed edastati, samuti selliste andmete muutusteta säilimise. Üllatust on valmistanud tõsiasi, et ka andmete vaatamine tuleb logida.

2014. a selgitas Andmekaitse Inspeksioon andmekogude kooskõlastamismenetlusega seonduvat avaliku teabe koordinaatorite kohtumisel. Tutvustati andmekogude kooskõlastamismenetluse korda üldiselt ja lahati kitsaskohti.

1. Asutamise kavatsuse kooskõlastamine	36
2. Asutamise kavatsuse kooskõlastamata jätmine	6
3. Kasutusele võtmise kooskõlastamine	38
4. Kasutusele võtmise kooskõlastamata jätmine	9
5. Andmekooseisu muutmise kooskõlastamine	17
6. Andmekooseisu muutmise kooskõlastamata jätmine	3
7. Lõpetamise kooskõlastamine	3
8. Lõpetamise kooskõlastamata jätmine	3

### 5.3.4. Kolmandatesse riikidesse isikuandmete edastamise load

Isikuandmete kaitse seaduse § 18 annab Andmekaitse Inspeksioonile õiguse väljastada lube isikuandmete edastamiseks kolmandatesse riikidesse, mille andmekaitse taset ei ole Euroopa Komisjon hinnanud piisavaks. Luba taotledes peab taotleja inspeksioonile esitama dokumentatsiooni, mis garanteerib isikute õiguste ja vabaduste kaitse kolmandas riigis. Isikuandmete saatmise eelduseks saavad olla Euroopa Komisjoni kinnitatud lepingu tüüptingimused, kontserni siseeskirjad või pooltevahelised asjakohased andmekaitselepingud.

2014. aastal vaatas inspeksiooni läbi 13 taotlust isikuandmete edastamiseks ebapiisava andmekaitse tasemega riiki, neist 12 olid positiivsed load ning 1 korral jäeti taotlus läbi vaatamata. 9 korral 13-st oli esitatud taotlus vormistatud nõuetekohaselt, 4 korral 13-st saatis inspeksioon taotluse tagasi puuduste kõrvaldamiseks, millest 3 asutust kõrvaldasid puudused õigeaegselt ning 1 jättis puudused õigeaegselt kõrvaldamata.

Loa said UADDBB Aon Baltic Eesti filiaal, Riskikonsultatsioonide OÜ, Federal Express Corporation Eesti filiaal, General Electric Inc Eesti filiaal, GE Healthcare Estonia OÜ, Sandoz d.d. Eesti filiaal, Arvato Services Estonia OÜ (2 korda), IBM Eesti OÜ, Danfoss AS, FLIR Systems Estonia OÜ, Danske Bank A/S Eesti filiaal.

Kolmandad riigid, kuhu loa saanud isikuandmete töötledajad isikuandmeid tahtsid edastada, olid Ameerika Ühendriigid, India Vabariik, Hiina Rahvavabariik ning Vene Föderatsioon.

### 5.4. Rahvusvaheline järelvalvealane koostöö

Andmekaitse Inspeksioon osaleb mitmes vormis Euroopa ja üleilmse haardega rahvusvahelises järelvalvealases koostöös. Töörühmade ja koostöövormide ühisnimetajaks võib pidada õigustavade ühtlustamist.

#### 5.4.1. Schengeni konventsiooni andmekaitse järelvalve

Ühine järelvalveasutus (*Schengen Joint Supervisory Authority* ehk Schengen JSA) vastutab Schengeni konventsiooni kohaselt loodud Schengeni infosüsteemi - SISI tehnilise abi üksuse järelvalve eest.

Samuti on Schengeni ühine järelvalveasutus pädev läbi vaatama Schengeni infosüsteemi tegevusega seotud rakendamise- või tõlgendamisküsimusi, uurima probleeme, mis konventsiooniosalistel siseriiklikel järelvalveasutustel sõltumatu järelvalve teostamisel või süsteemile juurdepääsu õiguse kasutamisel võivad tekkida ning koostama ühtlustatud ettepanekuid olemasolevate probleemide ühiseks lahendamiseks.

Ühe huvitava ja avalikkust enim puudutava aruteluna võib välja tuua Saksa andmekaitseasutuse püstitatud probleemi sõidukiandmete osas Schengeni infosüsteemis.

Saksa politseiasutus pöördus andmekaitseasutuse poole juriidilise küsimusega teatud sõidukiandmete kustutamise kohta Schengeni infosüsteemist.

Saksa politseile laekub suurel hulgal juhtumeid, kus sõiduk on kuulutatud teises liikmesriigis varastatuks ja sisestatud seetõttu Schengeni infosüsteemi. Sõiduk aga müüakse Saksamaal eraisikule, kes soetab selle heas usus. Kui uus omanik aga püüab sõidukit arvele võtta või teatatakse talle vahetult pärast tehingu toimumist politsei poolt, et selle sõiduki suhtes on sisestatud SIS II süsteemi märged ja seetõttu sõiduk konfiskeeritakse. Märke seadnud liimesriiki teavitatakse õiguslikest tagajärgedest ja võimalustest sõiduk tagasi saada teatud aja jooksul. Kui sellele ei järgne tegevusi, antakse sõiduk ostjale tagasi. Ostjat aga teavitatakse, et märged jääb endiselt kehtima ja sõiduki müügi soovist tuleb teavitada kohaliku politseid. Kuna probleem puudutab üksikisikute vabadusi vägagi vahetult, on äärmiselt oluline, et andmekaitseasutused ja politseiasutused leiaksid kiire lahenduse, kuidas omavahelise koostöö tõhustamise kaudu probleem lahendada.

#### **5.4.2. Euroopa sõrmejälgede andmebaasi (Eurodac) töögrupp**

Töögrupis jätkus arutelu uue Eurodaci määruse osas ja õiguskaitseorganite ligipääsu osas Eurodaci infosüsteemile. Töögrupis lepiti kokku nelja aasta tegevusplaan, mis on seotud tihedalt ka uue ülesandega, mis puudutab õiguskaitse organite ligipääsu Eurodaci andmebaasis olevatele sõrmejäljeandmetele. Ligipääs hõlmab ka Europoli.

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

Eestis on ainsaks asutuseks, kes omab juurdepääsu Eurodaci keskandmebaasi salvestatud andmetele, Politsei- ja Piirivalveamet.

Nii nagu Schengeni teise põlvkonna infosüsteemi ja Euroopa Viisainfosüsteemi (VIS) puhul, nii ka Eurodac'i puhul teostab infosüsteemi juhtimist EU-Lisa ehk Euroopa IT-Agentuur ning järelevalvet Euroopa andmekaitseinspektor.

#### **5.4.3. Tollikonventsiooni andmekaitse järelevalve**

Infotehnoloogia tollialane ühine järelevalveasutus on asutus, mis on pädev järgima tolliinfosüsteemi tööd, läbi vaatama selle tööga seotud rakendamise- või tõlgendamisküsimusi, uurima probleeme, mis tekivad liikmesriikide siseriiklikel järelevalveasutustel sõltumatu järelevalve teostamisel või üksikisikutel süsteemile juurdepääsu õiguse kasutamisel, samuti koostama ettepanekuid probleemide ühiseks lahendamiseks.

Tollinfosüsteemi puhul võib kõige teravamaks probleemiks lugeda selle kasutamisstatistikat. Sisult head tööriista ei ole laialdaselt kasutusele võetud ja numbrid näitavad, et enamikul juhtudel leitakse muid viise infovahetuseks. Selle küsimusega tegeletakse aktiivselt, et välja selgitada taolise tendentsi põhjused ning otsustada, kas piisab muudatustest või tuleb see süsteem sulgeda.

#### **5.4.4. Europoli konventsiooni ühine andmekaitse järelevalveasutus**

Andmekaitse Inspeksioon osaleb Europoli (Euroopa politseiameti) konventsiooni artikkel 24 kohase ühise järelevalveasutuse töös. Europoli ühise järelevalveasutuse eesmärk on kooskõlas Europoli konventsiooniga jälgida Europoli tegevust tagamaks üksikisiku õigused andmete talletamisel, töötlemisel ja kasutamisel. Ühise järelevalve kompetentsi kuulub Europoli isikuandmete töötlemise ja kasutamise seotud toimingute täiendamise ja tõlgendamise seotud küsimuste läbivaatamine, liikmesriikide järelevalve organite poolt iseseisvalt läbi viidud kontrollidega seotud küsimuste läbivaatamine, informatsiooni saamise õigusega seotud küsimuste läbivaatamine ning esilekerkivatele probleemidele lahenduste leidmine ning nende põhjal seisukohtade avaldamine.



Nii nagu igal aastal, viidi ka 2014. aastal läbi mahukas Europol keskasutuse ja selle infosüsteemi kontroll. Kontrolliti nii eelmiste aastate kontrollidel tehtud märkuste täitmist kui ka uusi asjaolusid. Endiselt tekitab probleeme Europolile varasemate puudujääkide kohane täitmine. Järelevalveasutus püüab otsepöördumistega ning vastavates komiteedes probleemidele tähelepanu juhtimisega siiski nõudeid kehtestada.

Tegeleti muuhulgas ka huvitava küsimusega, mis puudutas Europol soovi luua „*Europol Most Wanted List*” ehk tagaotsitavate isikute pingerida Europol kodulehele. Takistuseks osutus aga põhimõte, et liikmesriigiti on selliste andmete avalikustamine küll lubatud, kuid Euroopa tasemel mitte.

Samuti kohtuti kolmandate riikide esindajatega (Lichtenstein, Monaco, Makedoonia, Šveits, Austria, Kanada, Ameerika Ühendriigid), et selgitada koostöö võimalusi ning anda ülevaade riiklike andmekaitseasutuste tegevustest.

Europol ühise järelevalveasutuse juurde on loodud ka apellatsioonikomitee, mille eesmärk on lahendada kodanike kaebusi nendele Europol konventsiooniga tagatud andmetele juurdepääsu õiguse kaitseks.

Komitee otsused on lõplikud ja pooltele siduvad ning need avaldatakse ühise järelevalveasutuse kodulehel: <http://europoljsb.consilium.europa.eu/appeals-committee/tasks.aspx?lang=et>

#### **5.4.5. Balti andmekaitseasutuste järelevalve koostöö**

Alates 2011. aastat käivitus isikuandmete kaitse alane koostöö Läti kolleegidega ja 2012. aastast alates liitus tegevusega ka Leedu andmekaitseasutus, mistõttu saab koostööd nimetada Balti koostööks. Vajadus Balti regionaalse koostöö järele oli ilmne: Põhja- ja Baltimaade majandussektor on järjest enam põimumas ja et erinevates riikides tagada isikuandmete kaitse ühtne tase, tuleb järelevalveid läbi viia ühetaolise meetodi alusel ja süstemaatiliselt samades sektorites.

Ühisjärelvalve läbiviimiseks valitakse konkreetse sektori põhiselt ettevõtjad, kes on esindatud igas riigis, ühiselt sõnastatakse eesmärgid ja määratletakse fookus.

2014. a auditeeriti kõigis kolmes riigis tegutsevaid ravispaasid isikuandmete kaitseks kehtestatud infoturbe nõuete täitmise osas. Auditi läbiviimise aluseks oli ühiselt koostatud 42st küsimusest koosnev küsimustik.

Ühisauditi detailsemat ülevaadet saab lugeda AKI veebilehelt:

[https://www.waki.rik.ee/sites/www.waki.ee/files/elfinder/article\\_files/20150302%20Balti%20ravispaade%20audit.pdf](https://www.waki.rik.ee/sites/www.waki.ee/files/elfinder/article_files/20150302%20Balti%20ravispaade%20audit.pdf)

Ettekande koostas: Margit Liivoja, avalike suhete nõunik  
Peadirektori kokkuvõtte kirjutas Viljar Peep.

Valdkonnapõhise sisendi andsid:

Andres Ojaver, järelvalvedirektor

Kaja Puusepp, arendusdirektor

Elve Adamson, peainspektor

Kristiina Laanest, juhtivinspektor (endine õigusnõunik)

Merit Valgjärv, juhtivinspektor

Raavo Palu, vaneminspektor

Helina-Aleksandra Lettens, vaneminspektor

Kadri Levand, vaneminspektor

Kuldar Võsar, vaneminspektor (endine)

Urmo Parm, IT-nõunik

Andrus Altmeri, andmeturbeekspert

Boris põldre, andmeturbeekspert

Silver Sarapuu, nõunik (endine)

Helve Juusu, vanemspetsialist

Eret Kobin, vanemspetsialist

### **Andmekaitse Inspeksioon**

Väike-Ameerika 19, 10129 Tallinn

[www.aki.ee](http://www.aki.ee)

[info@aki.ee](mailto:info@aki.ee)

telefon 627 4135

fax 627 4137

