ANDMEKAITSE INSPEKTSIOON

AVALIKU TEABE SEADUSE TÄITMISEST JA ISIKUANDMETE KAITSE TAGAMISEST AASTAL 2018

Soovitused aastaks 2019

Aitäh panuse eest aastaraamatusse:

Raavo Palu, õigusdirektor
Urmo Parm, tehnoloogiadirektor
Maarja Kirss, koostöödirektor
Elve Adamson, peainspektor
Sirje Biin, juhtivinspektor
Raiko Kaur, vaneminspektor
Kaspar Uusnurm, vaneminspektor
Sergei Miller, vaneminspektor
Kristjan Küti, vaneminspektor
Kadri Levand, vaneminspektor
Helina - Aleksandra Lettens, vaneminspektor
Ain Kivistik, andmeturbeinspektor
Helve Juusu, vanemspetsialist
Triin Kask, vanemspetsialist
Signe Heiberg, avalike suhete nõunik

Print ja köide Koopia Niini & Rauam

Andmekaitse Inspektsioon 2019

Tatari 39, Tallinn

SISUKORD

AASTAST 2018 ÕIGUSDIREKTORI PILGU LÄBI

Kokkuvõte Andmekaitse Inspektsiooni tegevustest ja soovitused 2019. aastaks

2018. aasta on olnud mitmes võtmes muutuste aasta – seda nii Andmekaitse Inspektsiooni, isikuandmete töötlejate kui ka andmesubjektide jaoks. Teadupärast toimusid muudatused isikuandmete kaitse regulatsioonides, kui jõustus isikuandmete kaitse üldmäärus (Euroopa Parlamendi ja nõukogu määrus nr 2016/679). Selle kõrval tuli Euroopa Liidu liikmesriikidel üle võtta ka nn õiguskaitseasutuste direktiiv (Euroopa Parlamendi ja nõukogu direktiiv nr 2016/680) – õigusakt, millega reguleeritakse õiguskaitseasutuste tegevust süütegude tõkestamisel, avastamisel ja menetlemisel ning karistuste täideviimisel.

Regulatsioonide uuendamine tugevdas isikuandmete kaitse alaseid nõudeid. Osad kehtinud andmetöötluspõhimõtted vormistati õigusnormideks. Näiteks kehtestati eraldiseisvate nõuetena vaikimisi ja lõimitud andmekaitse põhimõtted.

Seda kõike arvestades oli raske koostada 2018. aasta kohta ülevaadet. Uusi teemasid ning tegevusi oli inspektsioonil palju ning kõikidest muudatustest ei ole võimalik selles aastaraamatus ülevaadet anda. Keskendume olulisematele, mida isikuandmete kaitse üldmäärus ning õiguskaitseasutuste direktiiv endaga kaasa tõid. Ennekõike toome välja need olukorrad, mis nüüdsest on väheke teisiti või mis meie arvates vajavad rohkem selgitamist.

Näiteks vajab käsitlemist andmekaitsealaste riskide ja mõjude hindamise teema, andmekaitsespetsialistide olemus ning vajalikkus, samuti rikkumisteate esitamine isikuandmete töötlemise rikkumise korral.

Toome välja muudatused olukordades, kui isikuandmeid soovitakse edastada kolmandatesse riikidesse. Lisaks kirjutame mõningatest probleemsematest kohtadest avaliku teabe valdkonnas. Üks osa nendest on seotud eraõiguslike avaliku teabe valdajatega, kes ei oska määratleda, mille osas on nad avaliku ülesande täitjad ning seeläbi ka teabevaldajad. Tuleb ette olukordi, kus ka avaliku sektori asutused ei oma täielikku teadmist, millist avalikku ülesannet täidab nende loodud eraõiguslik juriidiline isik. Toome välja ka probleeme teabenõuete täitmise osas ja dokumendiregistritega seotud murekohad. Teeme ülevaate omavalitsuste kontrollist – nii kohapealsetest kontrollidest kui veebilehtede seirest.

Ülevaates anname põgusalt selgitusi, kuidas elektroonilisi kontaktandmeid võib kasutada otseturustuse tegemiseks – ennekõike, kas isikuandmete kaitse üldmäärus selles osas muutis midagi või mitte.

Eraldi oleme välja toonud ülevaate mõningatest menetlustest. Näiteks täheldasime, et töösuhete valdkonnas ei ole isikuandmete töötlemise toimingud piisavalt selgelt ja läbipaistvalt korraldatud – eriti olukorras, kus tööandja ei ole kehtestanud isikuandmete töötlemise tingimusi. Samuti tegelesime mitmel korral menetlustega, kus puudusid õiguslikud alused isikuandmete avalikustamiseks või andmetele juurdepääsuks (nt tervise infosüsteemile juurdepääsu väärkasutamine). Lisaks oli ka menetlusi, kus arvati, et isikuandmete kaitse üldmäärus annab võimaluse kõik enda isikuandmed ära kustutada – ka siis, kui inimesel on rahalisi võlgnevusi.

Lisaks toome välja lühiülevaate inspektsioonile arvamuse esitamiseks antud õigusaktide eelnõudest, mis said inspektsioonilt tagasiside. Nii käesolevas aastaraamatus sisalduvad kui ka siia mitte mahtunud eelnõude puhul on näha tendentsi, et alati ei mõelda õigusakti eelnõud koostades läbi kõiki asjaolusid. See ei puuduta ainult seaduste eelnõusid, ka andmekogude põhimääruste muutmisel näeme sarnasid vigu.

Peale isikuandmete kaitse üldmääruse kehtima hakkamist saime sageli eelnõusid, kus ei olnud midagi märgitud andmekaitsealasest mõjuhinnangust. Mõjuhinnang peaks olema osa eelnõu seletuskirjast, kuid kahjuks ei olnud alati seda lisatud, kuigi selline kohustus üldmäärusest tuleneb.

Möödunud aastal arvamuse avaldamiseks saadud eelnõude põhjal võib järeldada, et riik soovib järjest enam kasutada tehnoloogilisi lahendusi oma ülesannete täitmiseks. Sageli soovitakse töödelda suuri andmemassiive – olgu see mingite otsuste tegemiseks või järelevalve teostamiseks. On arusaadav, et uued tehnoloogilised lahendused arendavad teenuseid ning on abiks otsuste tegemisel, kuid isikuandmete töötlejal ei ole lubatud tegutseda ilma, et reeglid poleks selged ja andmetöötlus läbipaistev. Näiteks on vaja võtta kasutusele asjakohased meetmed inimese õiguste, vabaduste ja õigustatud huvide kaitsmiseks, kui tehakse automaatotsuseid, sh profiilianalüüsi. Avaliku sektori jaoks peavad olema automaatotsused reguleeritud seadusandluse tasandil. See kõik tähendab, et ei tohi olla valimatut isikuandmete massilist töötlemist.

Aasta tegevuste ülevaatest leiate ka eraldi peatükid piiriülesest tööst– osalemisest rahvusvahelistes töögruppides ning koostööst teiste

järelevalveasutustega. Üldistatuna võib öelda, et inspektsiooni koostöö teiste andmekaitseliste järelevalveasutustega on suurenenud ning tendents selles osas jätkub.

Möödunud aastal tegelesime pidevalt ka isikuandmete kaitse üldmääruse nõuete tutvustamise ja selgitamisega. Selgitavad teemaartiklid isikuandmete kaitse üldmäärusest said koondatud ka isikuandmete töötleja üldjuhendisse, mille avaldasime 31.05.2018.[1] Juhend on mõeldud praktiliseks materjaliks kõigile isikuandmete töötlejatele – ettevõtetele, mittetulundusühingutele, asutustele, ametiisikutele. Üldjuhendis ei ole kitsamatele valdkondadele suunatud soovitusi. Selleks on inspektsioonil valdkondlikud juhendid, mis on uuendamisel.

Statistilised näitajad

Möödunud aastal suurenesid meie tegevusnäitajate arvud (vt nt nõuandeliini näitajaid). Selle põhjuseks peame muudatusi andmekaitseõiguses. Järgmiselt leheküljelt leiab statistilise tegevusnäitajate võrdluse viimase nelja aasta lõikes ja aastaraamatu viimasest peatükist detailsema ülevaate möödunud aasta tegevustest. Kokkuvõttes meie töömaht kasvas – seda isegi olukorras, kus me võtsime eelmisel aastal sihiks vähendada omaalgatuslike menetluste hulka.

[1] Isikuandmete töötleja üldjuhend, leitav: https://www.aki.ee/et/juhised.

Viimase nelja aasta tegevusnäitajate võrdlus

TEGEVUSNÄITAJAD	2015	**2016**	2017	**2018**
Juhendiloome, poliitikanõustamine				
juhendid (arvestamata seniste uuendamist)	4	**1**	2	**1**
arvamused õigusaktide eelnõude kohta	35	**27**	34	**42**
Teavitustöö				
selgitustaotlused, märgukirjad, nõudekirjad, teabenõuded	1369	**1417**	1520	**2384**
kõned valveametniku infotelefonile	1136	**1419**	1527	**2556**
nõustamised (ettevõtetele, asutustele)	33	**79**	148	**200**
koolitused (korraldatud või lektorina osaletud)	18	**23**	17	**23**
Järelevalvetöö				
ringkirjad (ilma järelevalvet algatamata)	5	**5**	4	**8**
sh ringkirjade adressaate	149	**34**	26	**162**
suuremahulised võrdlevad seired	14	**9**	10	**2**
sh seiratute arv	412	**148**	129	**85**
kaebused, vaided, väärteoteated (esitatud)	446	**390**	462	**462**
Kaebused, selgitustaotlused, rikkumisteated, märgukirjad, loa ja teavitusmenetlused IMI (EL infosüsteem, mille kaudu andmekaitseasutused vahetavad infot jt pöördumisi) kaudu	-	**-**	-	**479**
omaalgatuslikud järelevalveasjad (algatatud)	384	**86**	149	**15**
sh ennetavad andmekaitseauditid	24	**24**	1	**1**
kohapealsed kontrollkäigud (järelevalves)	36	**33**	45	**17**

TEGEVUSNÄITAJAD	2015	**2016**	2017	**2018**
Järelevalvetöö				
soovitused ja ettepanekud (järelevalves)	299	**56**	125	**10**
ettekirjutused (reeglina eelneb ettepanek; reeglina sisaldab sunniraha-hoiatust)	77	**59**	64	**46**
sh registreerimise alal (eelneva ettepanekuta)	28	**26**	35	**-**
väärteoasjad (lõpetatud)	16	**16**	9	**23**
trahvid (väärteokaristus), sunniraha (järelevalves)	15	**16**	4	**9**
Loa- ja erimenetlused				
registreerimistaotlused (delikaatsete andmete töötlemiseks või vastutava isiku määramiseks) – DIATR suleti 24.05.2018	540	**547**	641	**192**
andmekogude kooskõlastustaotlused (asutamiseks, kasutusele võtmiseks, andmekoosseisu muutmiseks, lõpetamiseks)	167	**139**	99	**36**
loataotlused teadusuuringuteks andmesubjektide nõusolekuta	29	**18**	54	**61**
loataotlused isikuandmete välisriiki edastamiseks	8	**18**	22	**3**
taotlused iseenda andmete suhtes Schengeni, Europoli jt piiriülestes andmekogudes	10	**10**	8	**21**
Inspektsiooni töötajate arv ja eelarve				
koosseisulisi ametikohti	18	**19**	19	**19**
aastaeelarve (tuhat eurot)	671	**700**	714	**717**

Andmekaitse Inspektsiooni tegevused 2019. aastal

Tulevikku ei ole võimalik ette ennustada, mistõttu ei ole võimalik ka kõiki tegevusi 2019. aasta osas ette näha. Seega saame välja tuua need tegevused, millega oleme kindlasti arvestanud.

- Teeme menetluslikku koostööd nii teiste andmekaitse järelevalveasutustega kui ka siseriiklike asutustega nagu Riigi Infosüsteemi Amet.
- Jätkame teavitustööga. Oma võimaluste piires tegeleme ennetuse ja teavitustegevustega, arvestades ühiskonnas levivaid suundumusi ja probleeme.
- Valmistume ette uueks järelevalveks. Inspektsioonile on pandud kohustus teostada järelevalvet avaliku sektori teabevaldajate ning eraõiguslike avaliku ülesande täitjate ehk eraõiguslike teabevaldajate veebilehtede ning mobiilirakenduste üle, et need vastaksid nn juurdepääsetavuse direktiivi (Euroopa Parlamendi ja nõukogu direktiiv nr 2016/2102) nõuetele – seetõttu tegeleme selle järelevalvetöö ettevalmistamisega.
- Kaasajastame inspektsiooni juhiseid ning näidismaterjale.
- Osaleme Euroopa Andmekaitseasutuse töös, sh sealses juhendiloomes.

Võib tekkida küsimus, millal hakkab Andmekaitse Inspektsioon määrama isikuandmete kaitse üldmäärusega tulnud „hiigeltrahve“, mida Eesti õiguse kohaselt tuleb määrata väärteomenetluse raames. Selles osas kinnitan, et Andmekaitse Inspektsioon ei muutu ka edaspidi trahvivabrikuks. Meil on olnud juba enne isikuandmete kaitse üldmääruse tulekut võimalus määrata sanktsioone. Sellekohane praktika on aastate jooksul juba paika loksunud ning põhimõttelisi muudatusi ei ole ette näha. Rikkumiste puhul on meie käitumismustriks olnud selgitamine ja hoiatamine. Karistusi ja sundi rakendame viimase abinõuna. See siiski ei tähenda, et pahatahtlikkuse või korduva tõsise rikkumise korral piirdume vaid hoiatamise ja uue võimaluse andmisega.

SOOVITUSED 2019. AASTAKS

Siinses alapeatükis annan soovitusi nii seadusloome koostajatele kui andmetöötlejatele isikuandmete kaitse regulatsioonide ning avaliku teabe alaste normide paremaks rakendamiseks.

Mitmed soovitused on oma olemuselt samad, mis olid toodud 2017. aasta ülevaates, kuid leian, et nende kordamine ning meelde tuletamine on vajalik.

Soovitused ettevõtte juhile

- **Kehtesta** selged, lihtsad ja arusaadavad andmetöötlustingimused – seda nii klientide kui oma töötajate jaoks.
- **Veendu**, et ettevõtte töötajad on saanud koolitusi, selgitusi ning (kirjalikke) juhendmaterjale, mis aitavad neil ettevõtte nimel isikuandmeid õiguspäraselt töödelda.
- **Tee vajalikud infovarade kaardistamised**, sh ka bilansi-laadne andmetöötluse register, mis annaks ennekõike ülevaate töödeldavatest isikuandmetest ning nende töötlemise õiguslikest alustest. Kui oled küberturvalisuse seaduses nimetatud teenusepakkuja, siis koosta riskianalüüs turvameetmete võtmiseks.
- **Enne kui alustad** ettevõtte jaoks sisuliselt uut laadi isikuandmete töötlemisega, vii läbi kirjalik andmekaitsealane mõjuhinnang. Kui see uut laadi isikuandmete töötlemine on seotud olukorraga, kus õigusaktide muudatuste tõttu toimub ettevõttele isikuandmete töötlemiseks lisaõiguste või võimaluste andmine, siis kontrolli, kas selles õigusakti eelnõu seletuskirjas on ka tehtud andmekaitsealane mõjuhinnang. Kui eelnõu seletuskirjas sellekohast analüüsi pole või see ei hõlma kõiki planeeritavaid isikuandmete töötlemise toiminguid, siis vii läbi andmekaitsealane mõjuhinnang.
- **Ole valmis** olukordadeks, kus andmesubjekt soovib tutvuda enda isikuandmetega, nõuab nende parandamist, kustutamist, töötlemise piiramist, soovib nende ülekandmist või soovib esitada vastuväiteid. Kui sa parandad, kustutad või piirad isikuandmete töötlemist, siis ole ka valmis nendest toimingutest teavitama vastuvõtjaid, kes on ettevõttelt isikuandmeid saanud.

- **Uuri** andmete edastamisel kolmandatesse riikidesse, kas selleks on olemas kohane õiguslik raamistik – nt on olemas Euroopa Komisjoni otsus piisava andmekaitsetaseme kohta, millal kasutatakse asjakohaseid kaitsemeetmeid, siduvaid kontsernisiseseid eeskirju või kuna edastatakse isikuandmeid erandlike tingimuste kohaselt. Arvestades hetkeolukorda, on see vajalik selgeks teha ka olukorras, kus isikuandmeid soovitakse edastada Ühendkuningriiki – eriti juhul, kui toimub leppeta-Brexit.
- **Rakenda** kohaseid ning vajalikke turvameetmeid isikuandmete kaitseks.
- **Tee varasemalt selgeks**, milliste isikuandmete töötlemise nõuete rikkumise korral pead 72 tunni jooksul teavitama Andmekaitse Inspektsiooni. Teatavates olukordades tuleb teavitada andmesubjekte ja Riigi Infosüsteemi Ametit.
- **Kehtesta** ning rakenda sisekontrolli mehhanisme, et avastada isikuandmete töötlemise nõuete rikkumisi oma ettevõtte sees.
- **Valmistu** koostööks ettevõtlusvaldkonna ühenduse või erialaliiduga praktilise hea tava ehk toimimisjuhiste loomiseks. Kui ettevõtte tegevusalal on andmekaitse osas lahtisi otsi, saab ühiselt koostada praktilise hea tava toimimisjuhise. Oma valdkonda kõige paremini tundes, saab nii materjalid, millest on kõige rohkem kasu. Inspektsiooni võimalused individuaaltasandil põhjalikumalt nõustada on kasinad, kuid sektoritasandil aitame meeleldi.
- **Tee selgeks,** kas ettevõttele on määratud mingi avalik ülesanne, mis muudab ta avaliku teabe seaduse mõistes teabevaldajaks. Selleks soovitame kontrollida vastavaid halduslepinguid, ettevõtte loomise algdokumente ja põhikirjasid ning muid ettevõtte loomise või võimaliku avaliku ülesande üle andmisega seotud dokumente. Sellest oleneb, mis ulatuses ettevõtte tegevusele kohalduvad ka avaliku teabe seaduse nõuded.
- **Vaata üle**, kas ettevõttele on antud üle avalik ülesanne. Sel juhul peavad ettevõte kui eraõigusliku teabevaldaja veebiküljed ning mobiilirakendused vastama avaliku teabe seaduse § 32 nõuetele. Sel teemal tutvu avaliku teabe seaduse §-ga 32, Euroopa Parlamendi ja nõukogu direktiiviga nr 2016/2102 ning Euroopa Komisjoni rakendusmäärusega nr 2018/1523.

- **Selgita välja**, kas ettevõttele on vaja määrata endale andmekaitsespetsialist. Kui andmekaitsespetsialist on vaja määrata, siis veendu, et tegemist on piisavalt pädeva inimesega. Samuti hoolitse selle eest, et olemas on vajalik infoturbealane oskusteave (oma personali hulgas või väljastpoolt).

Soovitused avaliku sektori asutuse juhile

- **Määra pädev** andmekaitsespetsialist ning hoolitse selle eest, et asutuses oleks ka infoturbejuht (oma personali hulgast või väljaspoolt).
- **Rakenda** kohaseid ning vajalikke turvameetmeid isikuandmete kaitseks.
- **Kehtesta** ning rakenda sisekontrolli mehhanisme, et avastada isikuandmete töötlemise nõuete ning asutusesiseseks kasutamiseks mõeldud teabe töötlemise nõuete rikkumisi oma asutuse sees.
- **Kaardista, koosta, uuenda**. Vajalik on:
    - bilansi-laadset andmetöötluse registrit, mis annaks ennekõike ülevaate töödeldavatest isikuandmetest ning nende töötlemise õiguslikest alustest;
    - küberturvalisuse seaduse kohast riskianalüüsi turvameetmete võtmiseks;
    - ülevaadet infovarade kohta vastavalt „Teenuste korraldamise ja teabehalduse aluste“ määruse §-le 12;
    - arhiivieeskirjale vastavat dokumentide liigitusskeemi.
- **Veendu,** et nii avalikkusele kui ka teenistujatele suunatud andmetöötlustingimused on uuendatud, sh piisavalt selgelt, lihtsalt ja arusaadavalt sõnastatud. Taga, et andmetöötlustingimused oleksid hõlpsasti üles leitavad asutuse veebilehelt.
- **Ole valmis** olukordadeks, kus andmesubjekt soovib tutvuda enda isikuandmetega, nõuab nende parandamist, kustutamist, töötlemise piiramist või soovib esitada vastuväiteid. Kui sa parandad, kustutad või piirad isikuandmete töötlemist, siis ole ka valmis nendest toimingutest teavitama ka neid vastuvõtjaid, kes on asutuselt isikuandmeid saanud.

- **Uuri** andmete edastamisel kolmandatesse riikidesse, kas selleks on olemas kohane õiguslik raamistik – nt on olemas Euroopa Komisjoni otsus piisava andmekaitsetaseme kohta, millal kasutatakse asjakohaseid kaitsemeetmeid või kuna edastatakse isikuandmeid erandlike tingimuste kohaselt. Arvestades hetkeolukorda, on see vajalik selgeks teha ka olukorras, kus isikuandmeid soovitakse edastada Ühendkuningriiki – eriti juhul, kui toimub leppeta-Brexit.

- **Tee varasemalt selgeks**, milliste isikuandmete töötlemise nõuete rikkumise korral pead 72 tunni jooksul teavitama Andmekaitse Inspektsiooni. Teatavates olukordades tuleb teavitada andmesubjekte ja Riigi Infosüsteemi Ametit.

- **Enne kui alustad** asutuse jaoks sisuliselt uut laadi isikuandmete töötlemisega, vii läbi kirjalik andmekaitsealane mõjuhinnang. Kui see uut laadi isikuandmete töötlemine on seotud olukorraga, kus õigusaktide muudatuste tõttu toimub asutusele isikuandmete töötlemiseks lisaõiguste või võimaluste andmine, siis kontrolli, kas selles õigusakti eelnõu seletuskirjas on ka tehtud andmekaitsealane mõjuhinnang. Kui eelnõu seletuskirjas sellekohast analüüsi pole või see ei hõlma kõiki planeeritavaid isikuandmete töötlemise toiminguid, siis vii läbi andmekaitsealane mõjuhinnang.

- **Vii läbi** kirjalik avaandmete mõjuhinnang (vt avaliku teabe seaduse § 3^1).

- **Vaata üle,** kui asutus on loonud eraõigusliku juriidilise isiku või andnud sellele üle avalikke ülesandeid, siis aita ettevõttel selgeks teha, mis osas talle võivad kohalduda avaliku teabe seaduse nõuded.

- **Veendu,** et riigi infosüsteemide haldussüsteemi kantud andmekogude andmed on kaasajastatud ning vajalikud kooskõlastused läbinud.

- **Tegele** sellega, et asutuse veebileheküljed ning mobiilirakendused oleksid juurdepääsetavad. Sel teemal tutvu avaliku teabe seaduse §-ga 32, Euroopa Parlamendi ja nõukogu direktiiviga nr 2016/2102 ning Euroopa Komisjoni rakendusmäärusega nr 2018/1523.

- **Koolita** teenistujaid, jaga selgitusi ning (kirjalikke) juhendmaterjale, mis aitavad asutuse nimel isikuandmeid õiguspäraselt töödelda.

- **Kontrolli**, et teenistujatel on teadmised dokumendihaldusest ja juurdepääsupiirangute kehtestamist – selleks on vaja teha koolitusi.

- **Võta vastutus**. Asutuse dokumendihalduse eest vastutavad isikud peaksid kontrollima oma asutuse dokumendiregistri välisvaadet, et kontrollida võimalikke eksimusi ja rikkumisi.

Soovitused seadusloome koostajatele ja ettevalmistajatele

Järgnevad soovitused on mõeldud neile, kes loovad, koostavad, valmistavad ette või annavad sisendit õigusaktidesse, mis on seotud inspektsiooni tegevusvaldkondadega.

- Enne uut tüüpi isikuandmete töötlemise võimaluse reguleerimist või olemasoleva muutmist veendu, et on ka reaalne vajadus selleks. Ära tegutse kiirustades ning kõiki asjaolusid läbi mõtlemata.
  Kehtib põhimõte – üheksa korda mõõda, üks kord lõika.
- Koosta eelnõu seletuskirja ühe osana andmekaitsealane mõjuhinnang. Selleks on abiks inspektsiooni isikuandmete töötleja üldjuhendi 5. peatükk ning üldjuhendi lisa 1.
- Soovitan eelnõu seletuskirjas analüüsida planeeritava isikuandmete töötlemise põhiseaduspärasust ehk vastavust põhiseaduse §-le 26.
- Õigusaktis muudatusi tehes veendu, et olemasolev õiguslik raamistik või planeeritavad muudatused tagavad ka andmesubjekti õiguste kaitse. Näiteks, et ei antaks asutusele õigust teostada valimatut suuremas mahus isikuandmete töötlemist andmesubjekti kohta nii, et ta sellest midagi teada ei saa – sel juhul ei ole tal ka võimalik kasutada õiguskaitsevahendeid oma õiguste kaitseks. Kui seadusandluses tehakse erand teavitamata jätmise kohta, siis see peab olema proportsionaalne ning vajalik.
- Kui teed muudatusi mõne andmekogu põhimääruses, siis vii läbi selle andmekogu andmete avaandmete mõjuhinnang, kui seda juba tehtud pole.
- Eraldi soovitan Justiitsministeeriumil tuua Eesti õiguskorda haldustrahvi võimalikkus, kuna juriidiliste isikute sanktsioneerimine tänase väärteomenetluse kaudu on ebatõhus ning kõiki osapooli koormav.

Tänuavaldus

2018 oli väga pingeline aasta, mida iseloomustas pidev muutustega kohanemine. Andmekaitseõigus uuenes ning aasta lõpus kolis inspektsioon uutesse ruumidesse Tatari 39 aadressil.

Soovin tänada nii endisi kui praeguseid kolleege Andmekaitse Inspektsioonist, kes olid osaks protsessist ning aitasid läbi viia kõiki toiminguid ja tegevusi aastal 2018. Aitäh teile selle eest!

Lisaks tänan avaliku teabe nõukogu liikmeid, kes on aidanud andmekaitsealaseid ning avaliku teabega ümberkäimise oskusi ja teadmisi oma haldusalas edasi anda. Tänan kolleege ministeeriumitest, ametitest, omavalitsustest ning partnerorganisatsioonidest.

Raavo Palu

õigusdirektor

Andmekaitse Inspektsiooni peadirektori ülesannetes

ANDMEKAITSEÕIGUS UUENES

Euroopa Parlament ja nõukogu võtsid sarnase õiguskorra kehtestamiseks Euroopa Liidus aastal 2016 vastu kaks õigusakti, mille kohaldamine algas või vastavad sätted tuli üle võtta maiks 2018 – isikuandmete kaitse üldmäärus ning nn õiguskaitseasutuste direktiiv.

Võiks arvata, et tegemist on andmekaitseõiguse reformiga – siiski see nii ei ole, kuna põhivundament jääb samaks. Kahe õigusakti eesmärk oli sisustada osaliselt ka hetkel praktikas kasutusel olevad põhimõtted ja nõuded – nt lõimitud ning vaikimisi andmekaitse põhimõtete olemus. Samas jääda tehnoloogianeutraalseks ja seda nii toimuvate isikuandmete töötlemise toimingute kui ka kasutusele võetavate andmekaitseliste meetmete osas. Põhirõhk seati andmetöötluse riskipõhisele lähenemisele.

Sellest lähtuvalt oli Justiitsministeeriumi sooviks teha siseriiklikus õiguses muutusi nö kahes etapis – esimene oli uue isikuandmete kaitse seaduse ning teisena isikuandmete kaitse seaduse rakendamise seaduse vastu võtmise kaudu.

Möödunud ja sellele eelneval aastal andsime mitmeid kordi tagasisidet sõnastamise ja regulatsiooni loomise osas nii uuele isikuandmete kaitse seadusele kui ka selle rakendamise seadusele. Kahjuks kõiki esitatud ettepanekuid arvesse ei võetud. Esmapilgul tundub, et rakendamise seadusesse võisid lisanduda ka sellised sätted, mis oleksid meile vastuvõetamatud, kuid millede osas ei olnud meil võimalik tagasisidet anda või seda ei võetud kuulda. Kõik esitatud seisukohad on leitavad ka meie võrgulehelt.[2]

Kuigi mõlemad eelnõud olid pikka aega kooskõlastamistel ning ette valmistamisel, siis soovitud tähtajaks (25.05.2018) jäid õigusaktid vastu võtmata. Uut isikuandmete kaitse seadust jõuti Riigikogus menetleda möödunud aasta jooksul isegi kaks korda. Seadus võeti vastu 12.12.2018 ning see jõustus 15.01.2019. Isikuandmete kaitse seaduse rakendamise seadus sai Riigikogu heakskiidu alles 20.02.2019 ning jõustus 15.03.2019.

Uues isikuandmete kaitse seaduses tehti täpsustusi nende sätete kohta, mida isikuandmete kaitse üldmäärus lubab teha ning sellesse võeti üle õiguskaitseasutuste direktiivi sätted. Seaduses määrati näiteks alaealise nõusoleku võtmise õiguse alampiir talle suunatud infoühiskonna teenuse

[2] Leitavad: https://www.aki.ee/et/eraelu-kaitse/euroopa-andmekaitse-reform.

pakkumisega. Muudatus tehti samuti surnud inimeste andmete töötlemisega ning teadusuuringute jaoks lubade väljastamise tingimustes.

Isikuandmete kaitse rakendamise seadusega muudeti ühtekokku 127. seadust ning seda eesmärgiga viia kõik siseriiklikud õigusaktid vastavusse Euroopa Liidu andmekaitseõigusega. Sellele järgnevalt tehakse ka muudatused Vabariigi Valitsuse ning ministrite määrustes, kuna näiteks mitmel andmekogul toimusid muudatused vastutava töötleja osas või üldse muutus volitusnorm.

Loodan, et need muudatused on õiguskorras nii andmesubjektide, isikuandmete töötlejate ning järelevalveasutuse jaoks piisavalt selgelt ja arusaadavalt kirjeldatud – seda nii seadus(t)e enda tekstides kui ka seletuskirja(de)s.

Andmekaitseõiguse uuendamisega seonduvalt on soovitud teha muudatusi ka karistusõiguses. Muudatuste põhjuseks on isikuandmete kaitse üldmäärusest tulenevad haldustrahvid ning nende suurused. Üldmäärus võimaldab karistada maksimaalselt kuni 20 miljoni eurot või ettevõtja puhul kuni 4% tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem.

Kuna hetkel lubab karistusseadustik teha väärteokorras trahve juriidilistele isikutele kuni 400 000 eurot, siis tekkis vajadus muuta ka karistusseadustikku. Sellele lisandus veel asjaolu, et Eesti õiguskord ei tunne haldustrahvi instituuti, mistõttu isikuandmete kaitse üldmääruse põhjenduspunkti 151 kohaselt määrab inspektsioon trahve väärteomenetluse raames.

Karistusseadustikule andsime oma arvamuse juba 2017. aastal, kuid kahjuks ei jõudnud Riigikogu seda lõpuni menetleda – see langes Riigikogu menetlusest välja. Kahetsusväärselt ei võetud arvesse kõiki meie tehtud märkusi[3] selle eelnõu osas, kuid loodetavasti uuesti menetlemisel tegeletakse meie välja toodud kitsaskohtadega.

Raavo Palu

õigusdirektor

[3] Andmekaitse Inspektsiooni peadirektori 25.05.2017 seisukohad Justiitsministeeriumi koostatud kontseptsiooni asjus (vt 2. peatükk); samuti on seda seisukohta korratud Andmekaitse Inspektsiooni peadirektori memos Justiitsministeeriumi juhtkonnale (saadetud 29.05.2017). Mõlemad dokumendid on kättesaadavad: http://www.aki.ee/et/eraelu-kaitse/euroopa-andmekaitse-reform.

PRAKTIKUTE KIBEDAD PÄEVAD RISKIDE HALDAMISEL

Igasuguste reeglite rakendamiseks on vaja õigusselgust. Uues andmekaitseõiguses kahjuks ei ole selgeid vastuseid mahus, mida nii järelevalveasutus kui andmetöötleja oodanuks. Hallis udulooris orienteerumine oli nii meile kui pea kõikidele organisatsioonidele paras pähkel.

Teatavasti annab isikuandmete kaitse üldmäärus andmetöötlejatele päris palju otsustusruumi, kuidas ja mis ulatuses normi rakendada. Selle vabaduse märksõna on riskipõhine lähenemine. Mida suurema riskiga andmetöötlus, seda tugevamad peavad olema kaitsemeetmed inimeste eraeluliste õiguste tagamiseks. Näiteks sõltub riski suurusest, kas isikuandmeid töötlev organisatsioon peab enne andmetöötlusega alustamist kirjalikult vormistama põhjaliku andmekaitselise mõjude analüüsi. Või kui andmetöötluses läheb midagi valesti, siis kas peab järelevalveasutust ja inimesi sellest teavitama. Teisalt ei soovi ju keegi teha niisama mahukaid ja sageli kulukaid arendustöid.

Otsustusvabadus on hea, kuid kui ainsaks abistavaks märksõnaks on udused mõisted nagu andmetöötluse *ulatuslikkus*, *oht* või *suur oht*, paneb see esialgu nõutult õlgu kehitama. Kui tuua kõrvalepõikena näide lennundusest, siis keegi meist ei kujutaks ju ette, et lennujuhi ainsaks maandumissuuniseks kaptenile on see, et tuul on mõõdukas ja lennurada on üsna kuiv. Sinu otsus, mis suunalt ja kui kiiresti maandud! Saame ju aru, et selline soovitus võib lõppeda katastroofiga. Ka ümaralt kirjeldatud andmekaitsesuunised võivad tagajärjena inimestele olla otsest kahju põhjustavad.

> „Kui seni hindas andmetöötleja üldjuhul riske infovaradele sh andmete käideldavusele, terviklikkusele ja konfidentsiaalsusele, millel oli mõju organisatsiooni mainele, usaldusele, siis üldmääruse kohaselt tuleb lisaks hinnata ka riske isiku õigustele ja vabadustele.“

Ärgem unustagem, et tänapäevane andmetöötlus toimub valdavalt elektrooniliselt. See tähendab, et eelkõige vajavad IT süsteemide nõuetekohaseks häälestamiseks või arendamiseks andmekaitselist raamistiku IT analüütikud, arhitektid, projektijuhid, administraatorid. Just nemad ootavad organisatsiooni

õigusinimestelt selgeid suuniseid. Juristid küsivad omakorda järelevalveasutuselt, kuidas on õige.

Põhjalikumalt selgitust vajas isikuandmete kaitse üldmäärusest tuleva ohu ja suure ohu käsitlus. Selgitasime, et oma olemuselt on tegu klassikalise riskide haldamisega. See on olnud aastakümneid kasutusel näiteks IT turbes või kvaliteedijuhtimises. Mida uut tõi kaasa üldmäärus? Kui seni hindas andmetöötleja üldjuhul riske infovaradele sh andmete käideldavusele, terviklikkusele ja konfidentsiaalsusele, millel oli mõju organisatsiooni mainele, usaldusele, siis üldmääruse kohaselt tuleb lisaks hinnata ka riske isiku õigustele ja vabadustele.

Ehk, kui andmetöötluses läheb midagi valesti (toimub intsident) ja selle tulemusena võib inimene saada varalist, mittevaralist või füüsilist kahju, on tegu andmekaitselise riskiga. Sellisteks juhtudeks võivad olla näiteks, kui inimene võib saada rahalist- või mainekahju; või kaasneb riski realiseerumisega õiguslik tagajärg, mis jätab inimese ilma mõnest rahalisest toetusest või hüvitisest. Tervishoiusektoriintsidendil võib olla otsene mõju inimese tervisele või elule. Intsidendi tagajärjeks võib olla ka identiteedi vargus või pettus.

Andsime organisatsioonidele soovituse senise infoturbe intsidentide halduse kõrvale lisada ka andmekaitseline intsidendikäsitlus ja mõjuanalüüs. Intsidendikäsitlus hõlbustab otsustamist, kas füüsiliste, organisatsiooniliste või infotehniliste turvameetmete soovimatul või tahtlikul rikkumisel tuleb teavitada 72 tunni jooksul ka inspektsiooni ja/või täiendavalt intsidendist puudutatud inimesi.

Andmekaitseline mõjuanalüüs aitab aga isikuandmete töötlejal uute andmetöötlustoimingute kavandamisel läbi mõelda võimalikud andmekaitse riskid ning hinnata nende suurust.

Andsime tähenduse terminile ulatuslik andmetöötlus

Hea meel on probleemile lahenduse leidmise üle. Ühena vähestest Euroopa sõsarasutustest suutsime anda selge tähenduse koos kriteeriumitega ulatusliku andmetöötluse mõistele. See ei tulnud kergelt. Vaja oli selgeid aluseid, mida saab õigusnormiga põhjendada. Saime sellega hakkama ning andmetöötlejad tänasid. Mõiste sisustamine andis selguse samuti andmekaitsespetsialisti määramisel. Pikemalt saab selle kohta lugeda inspektsiooni isikuandmete töötleja üldjuhendi 5. peatükist.

Üks riskide haldamise meetmetest on isikuandmete kustutamine. Kui andmetöötluse eesmärk ja õiguslik alus on ära langenud, tuleb andmed kustutada

Ka inimesel endal on õigus nõuda oma isikuandmete kustutamist. Organisatsioonid said sellest esialgu aru kui absoluutsest kohustusest. Selgitasime, et nii see ei ole. Seadusandlus annab organisatsioonidele ette mitmeid aluseid, millistel juhtudel ja kui kaua tuleb või saab isikuandmeid säilitada. Näiteks personalitöös või lepingulistes suhetes, finantskohustuste täitmisel või siis õigusnõuete kaitsmise korral. Inimeste päringutele vastamisel peab andmetöötleja arusaadavalt selgitama, kas ja mis juhul ning ulatuses saab isikuandmed kustutada või kui ei saa, siis milline õiguslik alus seda piirab. Sellist vastust ei ole keeruline koostada, kui andmetöötleja on eelnevalt enda jaoks korrektselt koostanud andmetöötlustoimingute ülevaate.

„Üks riskide haldamise meetmetest on isikuandmete kustutamine.“

Paraku ei ole töö uue andmekaitseõiguse mõtestamisel lõppenud. Pean silmas biomeetriliste andmete temaatikat. Näiteks sõrmejälje või näokujutise kasutamist ruumidesse ligipääsul. Tulise arutelu põhjustaja on isikuandmete kaitse üldmääruses olev biomeetriliste andmete mõiste. Mitmed liikmesriigid tõlgendavad seda nii, et isegi kui salvestatakse ainult biomeetriast tuletatud numbriline vaste (nn räsi), mitte biomeetriline kujutis või nn *template,* on siiski tegu biomeetrilise andmetöötlusega. See aga tähendab üldmääruse poolt ette antud õiguslike aluste valmimisel kitsendusi. Näiteks ei saaks enam selliseid lahendusi kasutada lepingu täitmiseks, kui siseriiklik õigus ei näe ette erisusi. Eestis kehtiv isikuandmete kaitse seadus selliseid erisusi ei sätesta.

Siiralt loodan, et tulevased vaidlused Euroopa Andmekaitsenõukogus päädivad terve mõistuse võiduga. Ehk, kui biomeetrilised andmed on muudetud numbriliseks koodiks, on tegu juba isikuandmetega ning organisatsioonid saavad jätkata biomeetrial põhinevate ruumiligipääsude kasutamist.

Urmo Parm

tehnoloogiadirektor

ANDMEKAITSESPETSIALISTI OOTAMATU TULEK

Andmekaitsespetsialisti, lühendiga AKS-i peetakse uueks ametiks ning sageli seostatakse selle kohustuslikuks muutumist isikuandmete kaitse üldmääruse kehtima hakkamisega. Kuid delikaatsete isikuandmete töötlemise registreerimise kohustus on saanud alguse aastast 1997.
Juba siis tuli registreerimisprotsessis kirjeldada organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid.

Alates 2008. aastast loodi registreerimise kohustusele alternatiiviks võimalus teatada inspektsioonile andmekaitse eest vastutavast isikust. Seda võib pidada tänase isikuandmete kaitse üldmäärusega ettenähtud andmekaitsespetsialisti eelkäijaks, kuigi kohustuste hulk oli varasemalt väiksem. Lisaks on oluline vahe see, et andmekaitsespetsialisti määramine on praegu teatud juhtudel kohustuslik.

Õiguslik vorm	Esitatud AKS-de arv
Avalik õiguslik isik	18
Kohalik omavalitsus	328
Riigiasutus või muu riigi institutsioon	99
Mittetulundusühing	238
Sihtasutus	90
Tulundusühistu	27
Aktsiaselts	221
Euroopa äriühing	4
Füüsilisest isikust ettevõtja	24
Osaühing	1664
Täisühing	4
Usaldusühing	6
Välismaa äriühingu filiaal	21
Korteriühistu	20
Kokku	2782

Andmekaitsespetsialisti peavad määrama:

- Kõik avaliku sektori asutused (sh need eraettevõtted, kes on avaliku ülesande täitjad).
- Andmetöötlejad, kes töötlevad vähemalt 5000 inimese eriliigilisi (varasema käsitluse mõttes delikaatseid) isikuandmeid või süüteoandmeid.
- Andmetöötlejad, kes töötlevad süsteemselt ja ulatuslikult vähemalt 10 000 inimesed tundlikke isikuandmeid.
- Ettevõtted, kes töötlevad oma andmebaasis vähemalt 50 000 inimese tavalisi isikuandmeid.

Pikemalt selgitab eeltoodut inspektsiooni isikuandmete töötleja üldjuhendi kolmas peatükk.

Andmekaitsespetsialisti koolituste käivitamisest

Inspektsioon hakkas alates 2016. aastast välja töötama andmekaitsespetsialisti kui professiooni olemust. Analüüsisime samuti vastavale ametikohale vajaminevaid eeldusi ja nõudeid.

Töö käis kahel suunal –kutsestandardi loomine ning andmekaitsespetsialistide koolitamine.

Kuna kutsestandardi loomise puhul sai selgeks, et teema vajab natuke rohkem nö paika loksumist, siis ametlikult inspektsioon standardi koostamist ei alustanud. Küll aga töötasime välja põhimõtted, et kirjeldada, millised peaksid olema andmekaitsespetsialisti tööülesanded, teadmised ja oskused. Loobusime ka põgusalt arutatud ideest teostada andmekaitsespetsialistide eksamineerimist.

Kuna inspektsioonil ei olnud ressursse andmekaitsespetsialiste koolitamiseks, siis pakkusime Eesti suurematele ülikoolidele ning Tallinna Majanduskoolile välja idee lisada täiendkoolituskavadesse andmekaitsespetsialisti kursus.

Täiendkoolituskursuste läbiviimisest olid huvitatud Tallinna Tehnikaülikool, Tartu Ülikool, Tallinna Ülikool ja Tallinna Majanduskool ning alates 2017. aasta sügisest käivitusidki esimesed kursused, mis osutusid ülimalt populaarseks ning olid seda jätkuvalt ka 2018. aastal.

Määratletud roll

Andmekaitsespetsialist on ekspert andmetöötleja juures. Inspektsioon on määratlenud andmekaitsespetsialisti rolli ülesanneteks nõustamise, kontrollimise ja koostöö. Seda mitmel eri suunal ja tasandil – juhtkond, töötajad, kliendid, järelevalveasutus.

Praktikas on selgunud, et tihti tekitab segadust, kes saab olla andmekaitsespetsialist ja kuidas ta organisatsioonis paikneb. Isikuandmete kaitse üldmäärus viitab, et spetsialist peaks paiknema juhtkonna otsealluvuses ning vältida tuleb huvide konflikti. Viimane nõue tekitab probleeme. Arvestades Eesti andmetöötlejate väiksust ning ressursse on raske ette kirjutada, et alati tuleb palgata andmekaitsespetsialistiks eraldi inimene. Seega on inspektsioon lähtunud, et olulisim sellel ametikohal on teadmised ja kompetents.

Isegi kui andmetöötlejal ei ole kohustust määrata andmekaitsespetsialisti, peab ta täitma kõiki muid isikuandmete kaitse üldmäärusest, isikuandmete kaitse seadusest ning eriseadustest tulenevaid nõudeid.

Kas andmekaitsespetsialisti ülesanded antakse mõnele olemasolevale töötajale lisaülesandeks, palgatakse eraldi inimene, ostetakse teenust sisse või ametikohta

täidab näiteks mitu inimest korraga – see jääb ettevõtte või asutuse enda otsustada. Igal juhul peab andmekaitsespetsialistil olema ülevaade muuhulgas ka sisemistest tööprotsessidest, asutuse/ettevõtte infosüsteemidest, kliendisuhetest, avaliku sektoris töötades ka dokumendihaldusest. Ilma tervikpilti omamata, ei ole võimalik olla pädev andmekaitsespetsialist.

„Isegi kui andmetöötlejal ei ole kohustust määrata andmekaitsespetsialisti, peab ta täitma kõiki muid isikuandmete kaitse üldmäärusest, isikuandmete kaitse seadusest ning eriseadustest tulenevaid nõudeid."

Avasime abiliini

Alates 12. aprillist 2018 sai võimalikuks teavitada andmekaitsespetsialistist äriregistri ettevõtjaportaalis. See teavitus on mõeldud nii avalikkusele kui ka inspektsioonile. Määratud andmekaitsespetsialisti kontaktandmed avalikustati 25. maist. Samal ajal avas inspektsioon ka eraldi abiliini, et juhendada teavitamise protseduuri osas ning jagada selgitusi, millal on kohustus andmekaitsespetsialist määrata ja millal mitte. Täpsemad juhised, kuidas teavitust läbi portaali teha, on jäänud kättesaadavaks inspektsiooni kodulehel www.aki.ee.

Oluline oli andmekaitsespetsialistist teavitamise juures silmas pidada, et temast saab inspektsiooni ees oma tööandja kontaktisikuks.

Andmekaitsespetsialistide tulevik

Nagu artikli juurde kuuluvast statistikatabelist on näha, teavitati möödunud aastal kokku üle 2700 andmekaitsespetsialistist. Inspektsioon on teinud andmetöötlejate hulgas üleskutseid võimalikult palju edendada omavahelist koostööd, viidates eelkõige erialaliitude ja katuseorganisatsioonide tegevusele. Samuti oleme teinud üleskutse andmekaitsealase erialaliidu loomisele. Loodetavasti arengud selles suunas jätkuvad ning inspektsioon loodab ka tulevikus erialaliitusid tugevate koostööpartneritena näha.

Maarja Kirss

Koostöödirektor

ANDMEKAITSESPETSIALISTI AMETISSE MÄÄRAMINE

Andmekaitsespetsialisti ametisse määramisega seonduvalt vajas tihti selgitamist, kuidas on võimalik andmekaitsespetsialisti osas teavitust teha äriühingutel, kelle kõik esindusõiguslikud isikud ehk juhatuse liikmed on välismaalased ning ei ole ka e-residendid, mistõttu ei ole võimalik neil teavitusi läbi ettevõtjaportaali teha.

Selgitasime, et inspektsioon võtab vastu määramisteateid, kui sellele on digitaalselt või omakäeliselt alla kirjutanud isik, kes on ettevõtja/asutuse esindusõigusliku isikuna kantud äriregistrisse. Samuti siis, kui allkirjastaja tegutseb volituse alusel ja teatele on lisatud esindusõigusliku isiku allkirjastatud volikiri. Sealjuures ühe ettevõtja/asutuse esindusõiguslik isik ei saa ilma volituseta esitada teadet teise ettevõtte/asutuse kohta – isegi kui ta on emaettevõte või kõrgemalseisev asutus.

Sageli sooviti ka abi, kuidas sisestada ettevõtjaportaali andmekaitsespetsialisti andmeid? Inspektsiooni poole pöördus 168 ettevõtet või asutust, kes mingil põhjusel vajasid sisestamist äriregistrisse läbi inspektsiooni.

Kas andmekaitsespetsialistiks võib määrata ainult diplomiga inimese?

Küsimuste sageduse poolest võib välja tuua vastutavate töötlejate osas veel teadmatuse selles osas, et kas andmekaitsespetsialistiks võib määrata ainult diplomit omava inimese, kellel on sellealane koolitus läbitud. Sellega seonduvalt märgime, et inspektsioon on välja töötatud soovituslikud kompetentsid ning andmekaitsespetsialist võiks tunda andmekaitsealaseid õigusakte ja tavasid eksperdi tasandil ning suudab abistada ja kontrollida andmetöötlejat isikuandmete kaitse üldmääruse täitmisel. Inspektsioon nende teadmiste tagamise tõendamiseks eraldi sellekohast diplomit ei nõua – mainime ainult, et isikuandmete töötleja peaks hea seisma selle eest, et tal on pädev andmekaitsespetsialist.

ABCDE andmetöötlejale

a) Leia andmekaitsespetsialist, kes uues andmekaitseõiguses ja infoturbes orienteerub, aga tunneb ka konkreetse ettevõtte töö köögipoolt.

b) Vaata üle, et oleks olemas dokumenteeritud kujul isikuandmete töötlemisülevaade (bilansilaadne ülevaade) – inspektsioon võib selle välja nõuda, kuid omal algatusel esitama ei pea.

c) Avalda võrgulehel või tee muudmoodi kättesaadavaks oma asutuse või ettevõtte andmekaitsetingimused.

d) Ole valmis vajadusel inimesi ohustavatest andmekaitse intsidentidest inspektsioonile teavitama. Rikkumisteate vormi leiad inspektsiooni võrgulehelt.[4]

e) Veendu, et organisatsioon on valmis vastama inimestele nende endi poolt ja enda kohta tehtavatele päringutele ning teistele isikuandmetega seotud taotlustele.

Helve Juusu

vanemspetsialist

[4] Lisainfo rikkumisteate edastamisest - https://www.aki.ee/et/poordu-inspektsiooni-poole/rikkumisteate-edastamine.

UUS KOHUSTUS ANDMETÖÖTLEJATELE - RIKKUMISTEADE

Isikuandmetega toimunud rikkumiste registreerimine ja inspektsiooni teavitamine sai kõikidele vastutavatele andmetöötlejatele kohustuseks alates 25. maist. Selle tegevuse terminiks sai isikuandmete kaitse üldmäärusest tulenevalt – rikkumisteade.

Rikkumisteate esitamise kohustus tuleb siis, kui on juhtunud intsident isikuandmetega ning selle tagajärjel võib inimene saada kahju. Sellisteks olukordadeks on andmete lubamatu hävimine, kaotsiminek, muutmine, lubamatu avalikustamine või juurdepääsu võimaldamine. Teavitus rikkumisteatena tuleb inspektsioonile saata hiljemalt 72 tunni jooksul.

Uue nõude sisust oli andmetöötlejatel alguses raske aru saada. Üleval oli hirm, et kui esitada rikkumisteade, siis ollakse sihiteadlikult eksinud reeglite vastu ja järgnevad karmid sanktsioonid. Valitses teadmatus, kuidas peab käituma või millist infot andma, kui rikkumine on toimunud. Inspektsioon tegi selgitustööd, avaldades artikleid ja rääkides teemast seminaridel ja koolitustel. Avaldasime abistava vormi rikkumise asjaolude kirjeldamiseks ja esitamiseks.

„Andmekaitsealase rikkumise sisuline hindamine tähendab klassikalist riskihaldust.“

Näiteks vajas selgitamist, et enne teavituse tegemist peab andmetöötleja esmalt juhtumi tuvastama ja dokumenteerima. Seejärel tuleb hinnata juhtumi võimalikke negatiivseid tagajärgi inimestele ning alles siis otsustada, kas tuleb inspektsiooni juhtunust teavitada. Rikkumisteate esitamine sõltub sellest, kui mitut inimest või kui suuri andmemahte oht puudutab. Teavitada tuleb juhtumistest, millega tuleb kaasa reaalne oht isikuandmete kuritarvitamisele. Kui

rikkumisega ei tule kaasa ohtu inimeste jaoks, siis inspektsioonile rikkumisteadet esitada ei ole vaja.

Andmekaitsealase rikkumise sisuline hindamine tähendab klassikalist riskihaldust. Seda puudutasime aastaülevaate eelpool toodud peatükis. Õiguslikult tugevad vastutava-volitatud töötleja lepingud ning koostööpartnerite koolitamine tagavad edukuse intsidentide haldamisel. Kui andmetöötluses läheb midagi valesti partnerettevõtte eksimusel, tuleb järelevalveasutusele anda aru vastutaval töötlejal.

Perioodil 25 mai kuni 31 detsember esitati inspektsioonile 64 rikkumisteadet. Rikkumisteated andsid aluse väärteomenetluse algatamiseks kolmel korral ja haldusjärelvalve menetluseks ühel korral. Valdkondlikult toimus rikkumisi nii avalikus kui erasektoris. Intsidente registreeriti veebiteenuste, tervishoiuteenuste, pangandus/finantsteenuste ja transporditeenuste pakkujate hulgast. Samuti andmetöötlejatelt side-, tootmise - ja haridusvaldkonnast.

„Perioodil 25 mai kuni 31 detsember esitati inspektsioonile 64 rikkumisteadet.“

Põhjuseid oli erinevaid – nii inimlikku eksimust, hoolimatust kui teadmatust. Kahjuks ka teadlikult vääriti käitumist. Intsidendid puudutasid olukordi, kus infosüsteemides oli tarkvara uuendamata, versiooniuuendused vigased või turvaaugud lappimata. Töötaja tegi uudishimupäringuid või edastati andmeid valele isikule. Juhtus ka olukordi, kus iseteeninduses said nähtavaks teise inimese andmed. Rakendusi testiti pärisandmetega, riigiametnik ei olnud hoolas kaitsemeetmete rakendamisel piiratud juurdepääsuga teabele. Andmetöötlejad teavitasid ka pahatahtlikest rünnetest infosüsteemidele ja selle tagajärjel toimunud isikuandmete leketest.

Rikkumistest teada andmine võimaldab inspektsioonil analüüsida korduvaid mustreid ning anda soovitusi võimalike negatiivsete tagajärgede ennetamiseks. Olen tänulik Riigi Infosüsteemi Ameti CERT meeskonnale, kellega perioodiliselt toimunud teabevahetus aitas mitmelgi korral päästa andmetöötlejaid kõige hullemast.

Urmo Parm

tehnoloogiadirektor

PRAKTIKUTE TÖÖLAUALT

Aastat 2018 jääb meenutama inspektsiooni menetlejate ühine panus uuenenud andmekaitseõiguse mõtestamisse, selgitamisse ja praktikas parimal moel rakendamisse.

Selles peatükis toob aastaraamat lugejani seitsme inspektsiooni kolleegi tagasivaated käsitletud juhtumitele ning seda kas isikuandmete õigusaktide või avaliku teabe seaduse üle järelevalve teostamisel. Ülevaadetes on kesksel kohal probleemid ja tegevused tulenevalt uuenenud andmekaitseõigusest, kuid käsitletakse samuti eelnevatel aastatel üles kerkinud tähelepanuväärsemaid küsimusi või korduvaid probleeme.

Andmekaitse Inspektsioon tänab kõiki menetlejad, kes andsid oma panuse uuenenud andmekaitseõigusesse ja tegid oma tööd südamega.

TÖÖSUHETESSE ON VAJA ROHKEM LÄBIPAISTVUST

Andmetöötlus töösuhetes oli 2018. aastal enimkäsitletud teemade hulgas. Töösuhete raames pöörduti inspektsiooni kõige rohkem kaamerate kasutamise ja nimelise e-posti aadressi sulgemisega seotud küsimuste või probleemidega.

Olulise uue teemana tõstatus aga inimese õigus saada enda kohta käivaid andmeid, milleks on ka kaamera - ja kõnesalvestised.

Inspektsioonil oli mitu menetlust, mis puudutasid isikule endale tema kohta käiva salvestise väljastamist. Kui kaamerasalvestiste puhul võib salvestis kajastada kolmandate isikute andmeid (nt teiste klientide), siis kõnesalvestise puhul on reeglina kaks osapoolt, ehk asutuse/ettevõtte esindaja (töötaja) ja klient. Menetlused puudutasid nii kõnesalvestiste kui kaamerasalvestiste väljastamist. Viimase osas tegi inspektsioon ka ettekirjutuse ASC Motors OÜ-le.

2018. aastal kehtinud isikuandmete kaitse seaduse (kehtis kuni 14.01.2019) § 19 lõike 3 ning isikuandmete kaitse üldmääruse artikkel 15 alusel on isikuandmete töötleja kohustatud väljastama inimesele tema enda kohta käivaid isikuandmed või põhjendama andmete väljastamisest või teabe andmisest keeldumist. Olukorras, kus andmete väljastamisest keeldumiseks alust ei ole, tuleb inimese soovil talle teatavaks teha tema isikuandmed.

Kõnesalvestise välja andmisest

Tööandjal tuleb arvestada, et olukorras, kus kasutatakse salvestusseadmeid, on isikuandmete töötlejal nii õigusi kui kohustusi. Tihtipeale asutakse seisukohale, et juhul, kui salvestusseadmete kasutamiseks on õiguslik alus, siis kuuluvad salvestised üksnes isikuandmete töötlejale endale. Siiski nii see ei ole.

Kõigepealt toome esile, et tööalased telefonikõned (sh salvestised) ei ole töötaja eraelu kaitsealas. Isegi juhul, kui leitakse, et salvestise edastamine kahjustaks töötaja huve (nt õigust privaatsusele), ei ole võimalik selle alusel keelduda salvestise väljastamisest. Sellisel juhul tuleks töötaja andmed muuta salvestisel lihtsalt tuvastamatuks.

Oluline on enne väljastamist hinnata vestluse sisu, kas tegemist on tööalase kõnega või erasuhtlusega. Kui tegemist on puhtalt tööalase kõnega, tuleb kõnesalvestise väljastamise keeldumise otsustamisel hinnata üksnes seda, kas vestluse sisu võib kahjustada teiste isikute õigusi. Kui vestluse sisu puudutab näiteks üksnes ettevõtte üldist hinnapoliitikat või kliendi enda tasumata arveid, siis reeglina ei ole otsest alust salvestiste väljastamata jätmiseks. Kui aga

kõnesalvestise üks osa võib kahjustada teiste isikute õigusi, tuleb isikule väljastada see osa teabest, mis teiste isikute õigusi ei kahjusta.

Toimingute läbipaistmatus

Kõige rohkem tekitas töösuhetes jätkuvalt probleeme andmetöötluse läbipaistmatus. Tihtipeale puuduvad töökorralduse reeglid, mis käsitlevad isikuandmete töötlemist, sh kaamerate ja e-postkasti kasutamist (sh kustutamist). Kui puuduvad konkreetsed reeglid, ei ole tööandja tõenäoliselt ka analüüsinud, millisel õiguslikul alusel ja eesmärkidel on lubatud näiteks kaameraid kasutada ning kuidas saab vähendada töötaja e-posti aadressi kaudu toimuva kirjavahetuse kasutamisega seotud riske, et ära hoida võimalikku riivet töötaja ja kolmandate isikute eraelu puutumatusele ja sõnumisaladusele.

Soovitus tööandjatele: Panustage andmetöötluse läbipaistvusesse, et töötajate isikuandmete töötlemisega seonduvad reeglid ja kommunikatsioon oleks lihtsasti mõistetav ja kergesti kättesaadav.

Töötajale tekitab reeglite puudumine omakorda teadmatust, miks ja millisel eesmärgil näiteks kaameraid kasutatakse, töötaja kasutatavat e-posti aadressi vaadatakse ning millal kustutatakse e-posti aadress peale töölt lahkumist.

Oluliseks suunaks oli teavitustegevus

26.09.2018 toimus inspektsioonis ümarlaud, kuhu olid kutsustud Eesti Ametiühingute Keskliit, Eesti Tööandjate Keskliit, Eesti Kaubandus-Tööstuskoda, Eesti Väike-. ja Keskmiste Ettevõtjate Assotsiatsioon, Tööinspektsioon, Eesti Haiglate Liit.

Ühise laua taga arutati olulisemate muudatuste ja probleemsemate kohtade üle töösuhetes isikuandmete kaitse üldmääruse rakendamisel. Lahti räägiti andmetöötluse läbipaistvuse olulisus nii klientide kui ka töötajate vaatest.

Ümarlaua kokkuvõttena valmis oktoobris 2018 ka tööandjate infoleht, mis andis ülevaate andmetöötluse nõuetest.

Raiko Kaur

vaneminspektor

HARIDUS-JA KULTUURISEKTORIS ON TEKKINUD UUED ANDMEKAITSEALASED MUREKOHAD

Seoses enamkäsitletud kärgperede teemaga on inspektsioon saanud küsimusi e-keskkondades (e-päevik, e-kool) vanema soovil lapse andmetele ligipääsu võimaldamise kohta kolmandatele isikutele (nt uuele kasuvanemale). Inspektsioon on selgitanud, et lapse andmete töötlemise üle saavad otsustada tema seaduslikud esindajad kuni 18-aastaseks saamiseni. Erandiks on vaid lapse õigus anda oma nõusolek infoühiskonna teenuse saamiseks alates 13. eluaastast. Juhul kui kohus ei ole kummagi vanema esindusõigusi piiranud, siis on neil võrdselt õigus otsustada, kellele anda õigus oma lapse isikuandmete töötlemiseks. Samamoodi on neil mõlemal igal ajal õigus see nõusolek tagasi võtta. Seetõttu soovitas inspektsioon sellises olukorras teavitada teist vanemat ja anda vastav ligipääs kolmandale isikule nii, et teine vanem oleks asjast teadlik enne ja sellega nõus.

Võlglaste andmete avalikustamine võrgulehel ja stendidel on alati olnud aktuaalne teema. Sellist varianti proovis teha ka üks raamatukogu juhataja, kes sätestas võlglaste andmete avaldamise raamatukogu sisekorraeeskirjades. Paraku ei ole see lubatud. Kui võlglaste nimede avalikustamine ei tulene seadusest, siis muul alusel, kui inimese nõusolek seda teha ei saa. Nõusoleku alusel andmete töötlemine selles olukorras tähendab kohati kõige ebastabiilsemat õiguslikku alust, sest nõusolekut saab alati tagasi võtta ning kindlasti ei ole võlglastel huvi enda andmete avalikustamiseks.

> „Kui võlglaste nimede avalikustamine ei tulene seadusest, siis muul alusel, kui isiku nõusolekul seda teha ei saa.“

Dokumendiregistrite pidamine on olnud juba aastaid Andmekaitse Inspektsiooni tähelepanu all, seda avalikus sektoris terviklikult. Vaatamata sellele tuli 2018. aastal päevavalgele, et koolide infosüsteemi EKIS kaudu on lekkinud arvukalt asutusesiseseks kasutamiseks (AK) mõeldud dokumente.

Algatasime menetluse Haridus – ja Teadusministeeriumi infosüsteemi EKIS haldaja (standardlahenduse vastutav töötleja) suhtes. Menetlustulemused jäävad 2019. aastasse.

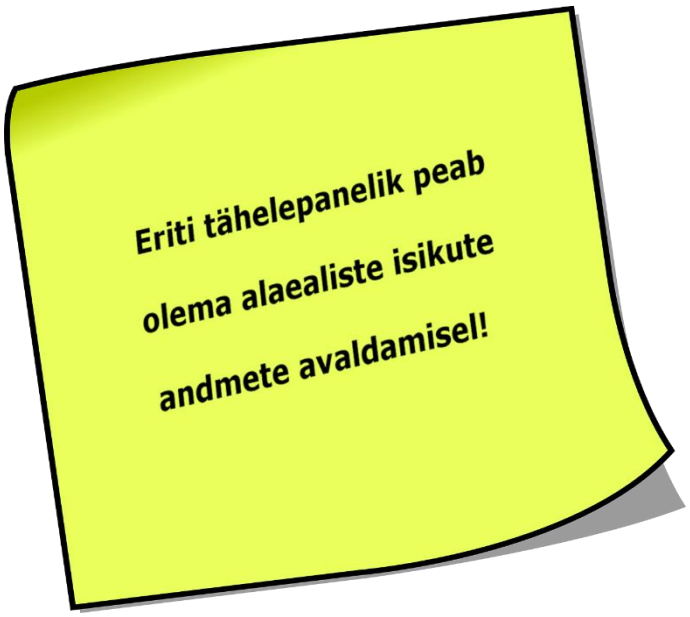
Kadri Levand
vaneminspektor

NIMEDE AVALDAMISEKS ON VAJA ÕIGUSLIKKU ALUST

Aastal 2018 tegelesime meedia ja mittetulundusühingute valdkonnas õigusvahemehena, teavitajana ja karistajana sama intensiivselt kui eelnevatel aastatel. Aastaraamatusse toome mõned kaasused, mis said kas enim käsitlust või olid võrreldes varasemate aastatega uudsemad.

Enimkäsitletud juhtumite hulka kuulub isikuandmete avaldamine võrgulehel.

- MTÜ Eesti Tennise Liit sai ettepaneku lõpetada võrgulehel oma liidusiseste otsuste avalikustamine isikustatud kujul.. Oluline on märkida, et mitmed isikud, kelle kohta taolist informatsiooni avaldati, olid alaealised. MTÜ-l ei tulene ühestki seadusest taoliste otsuste avalikustamise kohustust. Kuna otsustes olid kirjas isikute nimed koos nende eraelu kahjustava informatsiooniga, milleks on näiteks võistluskeeld halva käitumise pärast, stipendiumi mittemaksmise põhjused vms. Selliste otsustega seotud informatsioon on oluline vaid liidusiseseks tegevuseks, kuid avalikustades selle oma võrgulehel, muutuvad avaldatud isikud leitavaks ka otsingumootorite kaudu ning info võib põhjendamatult kahjustada isikuid väljaspool liidu tegevust. Eriti tähelepanelik peab olema alaealiste isikute andmete avaldamisel. Iga töötleja peab olema alati veel kaalutlevam ja ettevaatlikum, kuna alaealistel isikutel ei ole õigust enda andmete avaldamisel kaasa rääkida ning nende eest otsustavad nende seaduslikud esindajad.



- MTÜ Mumm sai ettepaneku lõpetada oma võrgulehel ühe oma erivajadustega liikme piltide avalikustamine. Kuna see mõjutas temasse kolleegide suhtumist, oli riive õigustele olemas. Puuetega inimeste andmete avalikustamisse peaks suhtuma erilise hoolikusega, isegi kui nad on ise oma andmete avaldamisega nõus.

„Puuetega inimeste andmete avalikustamisse peaks suhtuma erilise hoolikusega, isegi kui nad on ise oma andmete avaldamisega nõus“.

- Sekkusime kodaniku märgukirja peale Postimees AS ja Kanal 2 saate Radari tegevusse. Leidsime, et tegijad peavad efektiivsemalt valima meetodeid, et isikud ei oleks ka kaudselt tuvastatavad, kui selleks puudub õiguslik alus. Antud juhul näidati videos ja ka artikli juures olevatel piltidel dokumente, kus isikute nimed olid musta markeriga ära kaetud, küll aga oli võimalik ekraanipildi helendamisega nimesid tuvastada ja seda ka üks kodanik tegi. Kõnealusel juhul oli arusaadav, et töötlejal ei olnud alust ja ka soovi oma loos kajastatud isikute andmete avaldamiseks ning seetõttu soovitas inspektsioon edaspidi kasutada nii avaldatud loo kui edaspidiste lugude juures vahendeid, mis ei annaks võimalust sellisel viisil isikute tuvastamiseks.
- Uuema kaasusena toome välja juhtumi, kus väikesed lapsed on loonud endale kogemata või ilma vanema nõusolekuta konto või laadinud sotsiaalmeedia keskkonda üles oma andmeid. Youtube´i postitas 7-aastane tüdruk endast kogemata video ja ema ei saanud seda kuidagi maha. Teises sarnases juhtumis tegi 7-aastane poiss omale Facebooki konto, aga kasutas väljamõeldud telefoninumbrit ja e-maili, mistõttu ei olnud võimalik kontot kustutada. Selliste sekkumistaotluste arv 2018. aastal kasvas.
- Eesti Iseseisvuspartei sai ettekirjutus - hoiatuse lõpetada kaebaja isikuandmete töötlemine, sh avalikustamine äriregistris erakonna liikmena. Kaebaja ei ole olnud kunagi erakonna liige. Erakonnal ei olnud esitada isiku erakonnaliikmeks olemise kohta vastavaid tõendeid, sealhulgas ka liitumisavaldust. Tol hetkel kehtinud isikuandmete kaitse seaduse § 12 lõikest 2 tulenevalt pidi nõusolek olema reeglina kirjalikku taasesitamist võimaldavas vormis. Nõusoleku tõendamise kohustus on töötlejal.

Aasta lõpus toimus Vabariigi Valimiskomisjoni koolituse raames kohtumine erakondade esindajatega, kelle jaoks olime ette valmistanud meelespea isikuandmete töötlemise kohta valimistel.

Kadri Levand

vaneminspektor

SELGITUSTÖÖ AASTA TERVISHOIUS JA SOTSIAALIS

Andmetöötlejatele tervishoiusektoris tuli juurde uusi kohustusi ja aastaid töötanud isikuandmete töötlejate ja isikuandmete kaitse eest vastutavate isikute register (DIATR) suleti, kuna delikaatsete isikuandmete töötlemise registreerimiskohustus kehtis möödunud aasta 24. maini.

Pärast DIATR registri sulgemist pidid avalikku teenust osutavad vastutavad ja volitatud töötlejad määrama ametisse andmekaitsespetsialisti (AKS).

Tervishoiu ja sotsiaalhoolekande teenust osutavatele ettevõtetele tuli selgitada AKS-i määramise kohustus vajadust. Kõik haiglad, perearstid ja kiirabiteenuse pakkujad on avaliku ülesande täitjad ning seega kohustatud määrama andmekaitsespetsialisti. Kõigi muude tervishoiuteenuse osutajate puhul on ulatusliku andmetöötlusega tegu siis, kui andmetöötleja andmebaasis on 5000 või enama inimese eriliiki isikuandmed.

Leidsime, et samuti rehabilitatsiooniasutustel, kes riigi tellimusel osutavad avalikku teenust, on vaja määrata AKS teenuste osas, mida rahastab riik. Lisaks leidsime, et eriliiki isikuandmeid töötlevad rehabilitatsiooniasutused peavad teatud andmete töötlemise mahust alates tegema mõjuhinnangu. Kohustus tuleb töötlejatele, kelle andmebaasis on 5000 või enama kliendi eriliiki isikuandmed.

Töötukassa ja tervise infosüsteem tõi palju küsimusi

2018. aastal saime küsimusi töötute kohta info otsimise õiguse osas, mida teostab Töötukassa. Leidsime, et tööturuteenuste osutamine ja tööturutoetuste maksmine käib teatud tingimustel ja kuigi töötule on pandud kohustus teavitada Töötukassat asjaoludest, mis toovad kaasa tööturuteenuste ja -toetuste saamise õiguse lõppemise, ei tähenda see seda, et Töötukassa ise ei võiks nimetatud asjaolusid kontrollida.

Kuna Töötukassal on õigus valeandmete esitamise, samuti tööturutoetuse või teenuse saamist mõjutavatest asjaoludest teatamata jätmise korral õigus tagasi nõuda alusetult makstud summad, siis peab Töötukassal olema ka õigus iseseisvalt tõendeid koguda. See, kuidas ja milliseid allikaid kasutades andmeid kogutakse, on Töötukassa kaalutlusotsus.

2018. aastal kerkis eriti teravalt üles küsimus töötervishoiuarstide õigusest kasutada tervise infosüsteemis olevaid andmeid. Peale Sotsiaalministeeriumiga konsulteerimist leidsime, et kuna töötervishoiuarst on tervishoiuteenuste

korraldamise seaduse mõistes tervishoiutöötaja, siis järgib ta tervisekontrolli läbiviimisel muuhulgas ka tervishoiuteenuste korraldamise seaduse nõudeid. Töötervishoiuarsti läbiviidava tervisekontrolli eesmärk on hinnata töötaja terviseseisundit ning töökeskkonna või töökorralduse sobivust töötajale, eesmärgiga säilitada töötaja töövõime ja ennetada tööga seotud tervisekahjustusi, samuti diagnoosida tööst põhjustatud haigestumist ja kutsehaigestumist ning korraldada töötaja taastusravi.

Töötervishoiuarstide ligipääs tervise infosüsteemi andmetele on vajalik tervishoiuteenuse osutamise lepingu täitmiseks ning see võimaldab pakkuda kvaliteetsemat teenust töötajate tervise kaitse eesmärgil. Tervishoiuteenuste korraldamise seadus paneb tervishoiuteenuse osutajale kohustuse tervishoiuteenuse osutamine dokumenteerida ning nimetatud dokumendid tervise infosüsteemi edastada.

Tervise infosüsteem tõi inspektsioonile jätkuvalt palju kaebusi selle kohta, et arstid on vaadanud inimeste terviseandmeid tervise infosüsteemis väljaspool aktiivset ravisuhet. Terviseandmete kohta tehtud päringutega seonduvatest kaebustest koorus välja 6 juhtumit, kus terviseandmete vaatamiseks puudus õiguslik alus, ehk tervishoiutöötaja vaatas andmeid väljaspool ravisuhet. Kõik isikud on riikliku järelevalvemenetluse käigus oma eksimust ka tunnistanud ning sellele järgneb alati väärteo korras karistamine.

> „Terviseandmete kohta tehtud päringutega seonduvatest kaebustest koorus välja 6 juhtumit, kus terviseandmete vaatamiseks puudus õiguslik alus, ehk tervishoiutöötaja vaatas andmeid väljaspool ravisuhet.“

2018. aastal avaldas Kaitseressursside Amet nördimust selle üle, et arstlikul komisjonil on tervise infosüsteemis terviseandmetele juurdepääs üksnes isiku nõusolekul. Väidetavalt on selline lahendus takistuseks arstliku komisjoni igapäeva töö tegemisel, kuna inimestel on võimalik nõusoleku andmisest keelduda ja teatud terviseandmeid varjata.

Selgitasime, et Eesti on valinud tervise infosüsteemi puhul *opt-out* mudeli, mis tähendab, et andmete edastus tervise infosüsteemi toimub seaduse alusel. Patsiendilt ei küsita nõusolekut tema kohta käivate terviseandmete

edastamiseks tervise infosüsteemi, kuid tal on võimalus enda kohta käivate andmete töötlemist soovi korral piirata, nt sulgedes juurdepääsu enda andmetele.

Sellise regulatsiooni eeliseks on see, et kui patsient otsustab hiljem, et ta soovib siiski, et tervishoiuteenuse osutajad pääseksid tema kohta käivatele andmetele ligi, siis on andmed tervise infosüsteemis olemas. *Opt-in* süsteemi puhul annaks isik oma andmetele ligipääsu ja nõusoleku edasiseks töötlemiseks vastavalt nõusolekus toodud tingimustele. Kui *opt-in* süsteem oleks kasutuses, siis võimaldataks juurdepääs ka süsteemist väljaspool asuvatele teenusepakkujatele.

2018. aastal võimaldati tervise infosüsteemi kantud andmetele juurdepääsu ainult tervishoiuteenuse osutajatele ning üksnes tervishoiuteenuse osutamise lepingu sõlmimiseks ja täitmiseks. Muudele isikutele (sh ametiasutused avalike ülesannete täitmiseks) oli võimalik saada juurdepääsu tervise infosüsteemi kantud andmetele ainult isiku nõusoleku alusel või seaduses sätestatud konkreetse erandi alusel.

Kaitseressursside Ametile ei ole küll seadusega sätestatud konkreetset erandit ette nähtud, kuid on antud alternatiivne võimalus nõuda vajalike andmete esitamist paberil, kui isik ei anna nõusolekut oma tervise infosüsteemi kantud terviseandmete kasutamiseks või tervise infosüsteemis puuduvad tema andmed või kui need on ebapiisavad.

Ringkiri isikuandmete kaitse üldmääruse täitmiseks

Aastal 2018 saatsime ringkirju kaheksal korral ning ühe ringkirja saajateks olid Eesti haiglad. Selgitasime, et andmetöötlustoimingutest tuvastatavate jälgede, logide tekitamine ja nende haldamine on üks lõimitud andmekaitse rakendamise kesksemaid aspekte. Kõik organisatsioonid, kes oma tegevuse käigus isikuandmetega kokku puutuvad, on kohustatud tagama, et nende juures töödeldakse isikuandmeid turvaliselt. See tähendab muu hulgas, et infosüsteemides olevaid isikuandmeid kasutatakse ainult sel eesmärgil, mille

jaoks need on kogutud ning keegi ei pääse andmetele ligi uudishimust või omakasupüüdlikel ning pahatahtlikel eesmärkidel.

Selleks, et ära hoida isikuandmete väärkasutamist ning tagada, et tagantjärele oleks võimalik kindlaks teha, kes, millal ja miks infosüsteemis on andmeid vaadanud või kasutanud, peabki elektroonilise andmetöötluse puhul pidama logikirjeid isikuandmete töötlemise kohta.

Logide pidamise alus tuleneb isikuandmete kaitse üldmääruse artiklite 5 ja 32 koosmõjust ning haiglate puhul ka küberturvalisuse seadusest. Isikuandmete töötlemisel peab tagama andmete käideldavuse, terviklikkuse ning konfidentsiaalsuse. Selleks peab andmetöötleja rakendama asjakohaseid organisatsioonilisi, infotehnilisi ja füüsilisi turvameetmeid, et kaitsta andmeid loata või ebaseadusliku töötlemise eest.

Küberturvalisuse seaduse alusel kehtestatud määrusest „Võrgu- ja infosüsteemide riskianalüüsi nõuded ning turvameetmete kirjeldus“ tuleneb ka nõue seirata ja ajakohastada turvameetmeid (sh ka logisid), et tagada infosüsteemi riskide haldamine. See tähendab, et haiglad peavad regulaarselt seirama ja analüüsima oma infosüsteemi logisid, et omada operatiivselt ülevaadet nendes kajastuvate sündmuste ja tegevuste kohta.

Isikuandmete kaitse üldmääruse osas selgitasime ka kõikide teiste nõuete olemasolu. Tervishoiuasutused kui vastutavad töötlejad peavad koostama töötlustoimingute registri, milles tuleb kajastada nii põhitegevusega kui ka personaliga seonduvad andmetöötlustoimingud.

Samuti on andmetöötlejatel mõjuhinnangu kohustus. Mõjuhinnangu tegemise käigus tuleb hinnata ja analüüsida, milliseid isikuandmeid ja milliste vahenditega oma tegevuse eesmärkide täitmiseks töödeldakse ning kas ja milliseid organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid rakendatakse. Mõjude hindamine tuleb läbi viia enne isikuandmete töötlemise alustamist, siis kui hakatakse kasutama mõnda (uut) tehnoloogiat või rakendust, millega varasemat kokkupuudet ei ole olnud.

Samuti peavad vastutavad töötlejad arvestama sellega, et Andmekaitse Inspektsioonile tuleb hakata esitama rikkumisteateid. Isikuandmete töötlemise käigus võib paraku esineda turvanõuete rikkumisi, mis võivad põhjustada edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku hävitamise, kaotsimineku, muutmise, loata avalikustamise või juurepääsu

võimaldamise. Sellist turvanõuete rikkumist käsitleb isikuandmete kaitse üldmäärus isikuandmetega seotud rikkumisena.

Andmetöötlejal tuleb arvestada ka sellega, et isikuandmete kaitse üldmäärus rõhutab läbipaistvuse ja selguse olulisust isikuandmete töötlemisel. See tähendab, et inimesele tuleb lihtsalt ja arusaadavalt selgitada, milliseid andmeid tema kohta kogutakse ja mis eesmärkidel neid kasutatakse. Neist nõuetest tuleb lähtuda ka ettevõtte andmekaitsetingimuste (ehk nn privaatsuspoliitika) koostamisel.

Helina - Aleksandra Lettens

vaneminspektor

ETTEKIRJUTUS ANDMETE MITTEVÄLJASTAMISE KOHTA

Tartu Ülikool Genoomika Instituut (Eesti Geenivaramu) sai ettekirjutuse, sest ei väljastanud inimesele tema kohta kogutud andmeid.

Leidsime, et Geenivaramu on isikuandmeid kogunud juba pea 20 aastat ning isikuandmete kaitse seadus koos õigusega saada enda kohta käivat teavet jõustus Eestis 22 aastat tagasi. Seetõttu ei saa olla enam aktsepteeritavad põhjendused, et puuduvad protseduuri reeglid ja tehnilised vahendid andmete väljastamiseks. Nii isikuandmete kaitse seadus kui isikuandmete kaitse üldmäärus näevad ette, et andmesubjektil peab olema võimalik kasutada õigust tutvuda kõikide teda käsitlevate andmetega. Nimetatud õigusaktid ei võimalda andmete väljastamisest keelduda seetõttu, et andmed võivad olla eksitavad, vastutaval töötlejal puuduvad andmete väljastamiseks reeglid või tehniline võimekus. Ettekirjutuse hetkel kehtinud õiguse kohaselt võis isiku õigust saada teavet ja enda kohta käivaid isikuandmeid piirata üksnes siis, kui see võib kahjustada teise isiku õigusi ja vabadusi, ohustada lapse põlvnemise saladuse kaitset, takistada kuriteo tõkestamist või kurjategija tabamist või raskendada kriminaalmenetluses tõe väljaselgitamist.

Helina - Aleksandra Lettens

vaneminspektor

MAKSEHÄIRETE KUSTUTAMISEST NING ANDMETE VÄLJASTAMISEST

Isikuandmete kaitse üldmäärusest ei saanud maksehäirete kustutaja

Inimesed, kes oma võlgadega olid sattunud maksehäireregistrisse, lootsid isikuandmete kaitse üldmääruse artiklile 17 rõhudes avalikustamisest pääseda. On ju sellel sättel muuhulgas paljulubav pealkiri – „õigus olla unustatud". Kahjuks ei süvenetud alati selle artikli sisusse. Kõigepealt saab nõuda andmete kustutamist ainult teatud tingimustel (nt eesmärk on saavutatud, nõusolek võetakse tagasi, töötlemine on ebaseaduslik) ning teiseks on samas artiklis loetletud olukorrad, mil andmeid ei kustutata, sest neid on vaja näiteks sõna- ja teabevabaduse õiguse teostamiseks, juriidilise kohustuse täitmiseks, avaliku ülesande täitmiseks jne. Seega ei osutunud isikuandmete kaitse üldmäärus selles vallas imerohuks. Ka enne isikuandmete kaitse üldmäärust oli isikuandmete kaitse seaduse alusel võimalik nõuda oma andmete kustutamist, kui selleks oli alust.

Jätkuvalt oli suur nende inimeste hulk, kes esitasid kaebusi aegunud võlgade avalikustamise tõttu. Tihti jättis inimene tähele panemata või ei soovinudki aru saada, et võla aegumine ja õigus maksehäiret avalikustada on kaks eri asja – üks annab võlgnikule võimaluse maksmisest loobuda, teine aga annab võimalikele võlausaldajatele teavet inimese krediidivõimelisusest.

Mida saab võlaandmete edastajatele ette heita, on see, et võlgnikega ühenduse saamiseks kasutatakse meetodeid, mis ei lähe kokku isikuandmete töötlemise põhimõtetega – võlateateid saadetakse valimatult sugulastele, tuttavatele ja tööandjatele igasuguse õigusliku aluseta ja võlgniku teadmata. Päris süüta ei ole ka võlgnikud ise, sest inspektsioonilt abi otsides tunnistavad nad, et ei taha ise inkassofirmaga suhelda, sest siis saavad need tema e-postiaadressi või telefoninumbri teada.

Kirgi küttis DataMe OÜ tegevus isikuandmete kogumisel volikirja alusel

Paljud asutused ja ettevõtted pöördusid Andmekaitse Inspektsiooni selgituste saamiseks küsimusega, et kui õiguspärane on DataMe OÜ tegevus volikirja alusel andmesubjekti isikuandmete pärimisel ning kas andmeid peab väljastama nende soovitud viisil.

DataMe OÜ suhtes läbi viidud järelevalve käigus kontrollisime inimeste esindamiseks kasutatava volikirja ja andmete jagamise platvormi kasutustingimuste vastavust tol hetkel kehtinud isikuandmete kaitse seadusele. Järelevalve käigus võttis DataMe OÜ arvesse inspektsiooni märkusi ning tegi kasutustingimustes muudatusi seadusega kooskõlla viimiseks ning kliendi jaoks suurema läbipaistvuse saavutamiseks.

Olukorras, kus on tegemist haldusmenetlusega, kohaldatakse isikuandmete väljastamise otsustamisel haldusmenetluse seadust. Selle seaduse § 13 lõike 1 kohaselt on menetlusosalisel õigus kasutada haldusmenetluses esindajat, kes võib esindada menetlusosalist kõigis menetlustoimingutes, mida seadusest tulenevalt ei pea menetlusosaline tegema isiklikult. Esindusõigus antakse haldusmenetluses kirjaliku volitusega ning esindusele kohaldatakse tsiviilseadustiku üldosa seaduse sätteid.

> „Seega peab inimene andmete töötlejalt saama enda isikuandmeid seaduses sätestatud mahus nii neid ise küsides kui ka esindaja abil välja nõudes.“

Isikuandmete kaitse seadusest ei tulenenud, et andmesubjekt peaks isiklikult teostama õigust saada isikuandmete töötlejalt enda kohta käivaid isikuandmeid. Seega peab inimene andmete töötlejalt saama enda isikuandmeid seaduses sätestatud mahus nii neid ise küsides kui ka esindaja abil välja nõudes. See kehtib nii avalikule kui ka erasektorile ning see on kohaldav ka isikuandmete kaitse üldmääruse kehtima hakkamise järgselt. .

Andmete väljastamisest volituse alusel

Eraõiguslikes suhetes saavad ettevõtted ja kliendid kokku leppida mis iganes suhtluskanalite kasutamises ja teadete vorminõuetes. Küll aga ei tohiks inimesele, kes oma andmeid küsides (sh esindaja vahendusel) realiseerib õigust oma andmeid küsida, peale suruda ebamõistlikke piiranguid. Kuna andmete küsimiseks esindusõiguse andmiseks piisab kirjalikust volitusest, ei ole põhjendatud nõuda näiteks notariaalset tõestatud volikirja. Andmete väljastaja peab tuvastama andmete saaja, volituse digitaalne allkiri võimaldab andmesubjekti tuvastada.

Isikuandmeid väljastatakse võimalusel andmesubjekti soovitud viisil. Juhul kui ei ole võimalik andmeid väljastada soovitud viisil või see oleks isikuandmete

töötleja jaoks ebaproportsionaalselt koormav, valib andmete väljastamise viisi töötleja. Seejuures peab isikuandmete töötleja valima andmesubjekti jaoks võimalikult mugava viisi, et andmetega tutvumine oleks lihtne, kiire ja mõistlike kuludega. See ei tähenda, et isikuandmete töötleja peaks asuma oma infosüsteeme andmesubjekti mugavusest lähtudes ümber ehitama. Seadusest ei tulene, et väljastatavad andmed peaksid olema masinloetaval kujul või muul andmesubjekti või tema esindaja jaoks soovitud tehnilises vormingus. Andmeid peab andmesubjektile või tema esindajale väljastama lähtudes olemasolevatest võimalustest.

Andmetöötlejale on liigselt koormavate päringute puhul abiks isikuandmete kaitse üldmääruse säte, mis võimaldab nõuda tasu andmesubjekti põhjendamatute või ülemääraste taotluste eest, võttes arvesse kaasnevat halduskulu.

Sirje Biin

juhtivinspektor

NÕUSOLEKUST OTSETURUSTUSES ENNE JA PÄRAST ISIKUANDMETE KAITSE ÜLDMÄÄRUST

2018. aastal jätkusid sekkumistaotlused olukordadesse, kus inimesed leidsid, et e-posti aadressile on saadetud reklaam ilma, et oleks küsitud ja antud saatjale eelnev nõusolek.

Seega ei olnud elektroonilise otseturustuse valdkonnas peamise teema osas midagi kardinaalselt uut. Kuid isikuandmete kaitse üldmääruse kehtima hakkamisel kerkis nõusoleku küsimuse teema aktuaalsemaks ja seda kahes aspektis. Esmalt, otseturustuspakkumiste saajad said teadlikumaks eelneva nõusoleku vajalikkusest ning asusid uurima, kas see on pakkumiste saatjatel olemas. Kui ei olnud, tehti inspektsiooni kaebus või saadeti märgukiri. Teiseks, otseturustajad ei teadnud, kas nad peavad nõusolekut uuendama.

Reklaamisaajate teadlikkus kasvas

Inspektsioonil tuli teha läbi selgituskirjade ja avalike pöördumiste põhjalikku teavitustööd. Rõhutasime esmalt, et füüsilisest isikust kliendi elektrooniliste kontaktandmete kasutamine otseturustuseks on lubatud üksnes kliendi eelneval nõusolekul ning selle olemasolu tõendamise kohustus on isikul, kelle nimel otseturustust edastatakse. Juhul, kui otseturustuseks kasutatakse juriidilise isiku kontaktandmeid, siis eelneva nõusoleku omamise kohustust ei ole, kuid talle peab andma võimaluse keelata oma kontaktandmete edasine kasutamine.

> „Otseturustuspakkumistest keeldumine ei tohi olla kliendi jaoks keerulisem, kui on nõusoleku andmine.“

Sealjuures peab iga saadetav pakkumine sisaldama selget ja arusaadavat võimalust võimaldada tasuta ning lihtsal viisil keelata oma kontaktandmete sellekohane kasutamine.

Muuhulgas tuleb arvestada, et otseturustuspakkumistest keeldumine ei tohi olla kliendi jaoks keerulisem, kui on nõusoleku andmine.

Reklaamisaatjad kimpus andmebaasidega

2018 aasta näitas veel, et suuri andmebaase omavad ettevõtted ei suuda sageli tagada, et peale nõusoleku tagasivõtmist ei saadeta otseturustuspakkumisi kliendi aadressile. Säärastes olukordades ei viidanud ettevõtete põhjendused

pahatahtlikule spämmimisele, vaid keeruliste andmebaasidega töötamisel tehtud eksimustele.

Tuginedes menetluspraktikale ning juhindudes elektroonilise side seaduse §-st 103^1 rõhutab inspektsioon, et juhul, kui andmetöötleja tehnilised võimalused või muu asjaolud ei võimalda nõuetekohaselt täita selle seaduse nõudeid elektroonilise otseturustuse tegemisel, tuleb andmetöötlejal isiku elektrooniliste kontaktandmete töötlemine koheselt lõpetada.

Oli selgitustöö aasta

Kogu aasta vältel tegime põhjalikku selgitustööd nõuandeliini kaudu ning osaledes nõustajana erinevatel kohtumistel.

Märgime eraldi ära, et üks olulistest kohtumistest toimus 12.03.2018 Eesti e-kaubanduse liidu esindajaga, kus tegime vajalikku selgitustööd. Isikuandmete töötleja üldjuhendi valmimisel (31.05.2018) varustasime liitu abistava juhendmaterjaliga, mis tehti kättesaadavaks liidu liikmetele.

Lisaks toome välja olulise selgitustöö osana 28.06.2018 avalikkusele ja e-turustusettevõtetele väljasaadetud pressiteate selgitamaks õiguslikke aluseid isikuandmete töötlemiseks otseturunduse tegemisel. Selgitasime, et levimas on vale arusaam, et alates isikuandmete kaitse üldmääruse jõustumisest oleks justkui lubatud saata otseturustuslikke teateid, kui teate saatjal on selleks õigustatud huvi. Nagu eelnevalt märgitud, tohib füüsilisele isikule teateid saata ennekõike tema eelneval nõusolekul. Selle pressiteate tagajärjel käsitlesid mitmed ajakirjandusväljaanded isikuandmete kasutamise teemat otseturustuses.

Vaneminspektorid Sergei Miller ja Kaspar Uusnurm

ISIKUANDMETE EDASTAMINE KOLMANDATESSE RIIKIDESSE

Andmekaitse valdkonnas tekivad tihti küsimused, mis saab siis, kui mul on andmeid vaja saata väljaspool Eestit asuvale ettevõttele, asutusele või organisatsioonile?

Üldjoontes käib andmete edastamine välisriiki nii enne isikuandmete kaitse üldmääruse kehtima hakkamist kui ka peale seda sarnase põhimõtte järgi. Kui edastamine toimub Euroopa Liidu siseselt, siis peab olema küll õiguslik alus, nagu seda on vaja igaks andmetöötluse toiminguks, kuid täiendavaid meetmeid (nt inspektsioonilt luba taotleda) rakendama ei pea. Kui aga edastamine toimub kolmandasse riiki, siis tuleb uurida, millisele andmekaitsetasemele riik vastab ja järgida teatud nõudeid.

Variante on neli.

- Edastamine Euroopa Majanduspiirkonna (Norra, Island, Liechtenstein) riikidesse on võrdsustatud piisava andmekaitse tasemega riikidega ehk edastamise kord on analoogne Euroopa Liidu sisese edastusega.
- Edastamine riikidesse, mis on saanud Euroopa Komisjonilt andmekaitse taseme piisavuse otsuse, on protsess analoogne Euroopa Liidu sisese edastusega. Riikide nimekiri on saadaval Euroopa Komisjoni kodulehelt[5], sinna on muuhulgas arvatud näiteks Argentiina, Kanada (ainult erasektor), Šveits, 2019 lisandub Jaapan jne.
- Edastamine Ameerika Ühendriikidesse, kui ühendriikides asuv ettevõte on liitunud *Privacy Shield* programmiga, on loetud piisava andmekaitse tasemega edastuseks (ehk siis analoogne liidu sisese edastusega).
- Edastamist ülejäänud riikidesse, mis ei ole ülalpool loetletud, on andmete edastamine mittepiisava andmekaitsetasemega riiki ning edastamisel tuleb rakendada lisakaitsemeetmeid või see võib toimuda erandolukordades (rakendades vastavalt isikuandmete kaitse üldmääruse artikleid 46-49).

Enne isikuandmete kaitse üldmääruse kehtima hakkamist reguleeris andmete edastamist nö vana isikuandmete kaitse seadus, mis nägi ette, et mittepiisava andmekaitsetasemega riikidesse edastamisel tuleb selleks taotleda inspektsioonilt vastav luba. Luba väljastades hindas inspektsioon andmeeksportija ja andmeimportija vahel sõlmitud andmeedastuslepinguid

[5] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

(enamasti kasutati selleks Euroopa Komisjoni loodud standardseid andmekaitseklausleid – *Standard Contractual Clauses*). Lisaks kasutasid suurkorporatsioonid siduvaid kontsernisiseseid eeskirju (*Binding Corporate Rules*), mille hindamine toimus andmekaitseasutuste vahel vastastikuse tunnustamise põhimõttel (nö emakontori riigis asuv juhtiv järelevalveasutus koos kaasatud asutustega hindas eeskirju, ülejäänud asjassepuutuvad järelevalveasutused tunnustasid juhitva asutuse tehtud otsust).

Isikuandmete kaitse üldmääruse tulemisega on toimunud mõningane muudatus just loataotlemise kohustuse osas. Kui edastamine toimub kasutades artikli 46 lõikes 2 ettenähtud kaitsemeetmeid (nt standardse andmekaitseklauslid, toimimisjuhendid, sertifitseerimine, siduvad kontsernisisesed eeskirjad (kuigi nende puhul on säilinud järelevalveasutuste vaheline tunnustamise protseduur)) ei ole vaja inspektsioonilt enam andmete edastamise luba taotleda. Seega võib öelda, et isikuandmete kaitse üldmäärusega on andmete töötlejatele pandud kohustus ise tagada täielik kaitsemeetmete vastavus kehtivale õigusele ning neid inspektsioon eraldi ei hinda.

„Üldmääruse kehtima hakkamine on vähendanud inspektsioonilt loa taotlemise vajadust. Andmetöötlejatel on rohkem võimalusi andmete edastamise aluste valiku osas.“

Erandiks, mil peab luba taotlema, on olukord, kui edastamine toimub andmeeksportija ja -importija vahel sõlmitud üldise lepingu alusel või avaliku sektori asutuste vahelise halduskokkuleppe alusel. Sellistel juhtudel tuleb inspektsioonilt taotleda luba ning enne otsuse tegemist peab inspektsioon läbi viima järjepidevuse mehhanismiga seotud protseduurid (esitama lepingud ja otsuse Euroopa Andmekaitsenõukogu liikmetele heakskiitmiseks).

Üldmääruse artikkel 49 loetleb erandid, mil võib mittepiisava andmekaitsetasemega riiki edastada andmeid ilma inspektsiooni loata või artiklis 46 loetletud kaitsemeetmeid rakendamata. Sellisteks erandjuhtumiteks on näiteks isiku nõusolek (selgesõnaline nõusolek edastamise lubamiseks), isiku ja andmetöötleja vaheline leping, avalik huvi jms.

Seega võib kokku võtta, et isikuandmete kaitse üldmääruse kehtima hakkamine on vähendanud inspektsioonilt loa taotlemise vajadust. Andmetöötlejatel on rohkem võimalusi andmete edastamise aluste valiku osas (võrreldes varasemalt

kehtinud korraga) – näiteks on võimalus kasutada toimimisjuhendeid, sertifitseerimist ja ka erandite kasutamine on võrreldes varasemaga laiem.

Kontsernisisesed eeskirjad

Töövoogudest rääkides, siis aastal 2017 väljastas inspektsioon 22 otsust andmete edastamiseks välisriiki. Antud number on põhjendatav isikuandmete kaitse üldmääruse jõustumisega, kuna andmetöötlejad soovisid enne õigusakti tulekut oma dokumentatsiooni korrastada. Nimelt varasemalt antud load jäid kehtima ka peale isikuandmete kaitse üldmääruse kehtima hakkamist. Aastal 2018 esitati inspektsioonile 3 loataotlust, millest ühele väljastati luba. Küll aga oli sel perioodil inspektsioon esmakordselt kaasatud siduvate kontsernisiseste eeskirjade läbivaatamise protseduuri kui kaasläbivaataja. Sellest kogemusest võib öelda, et tegemist on aja- ja ressursimahuka protseduuriga, mille puhul tavaliselt 3 andmekaitseasutust korraga hindavad korporatsiooni andmetöötlusega seonduvat dokumentatsiooni. Lisaks esimesele läbivaatusele, järgneb ka järelläbivaatus ning eeskirjade osas tehtud otsus esitatakse kõikidele teistele asjassepuutuvatele järelevalveasutustele vastuväidete esitamiseks. Kui vastuväiteid ei ole, võetakse otsus vastu ehk siis siduvad kontsernisisesed eeskirjad kiidetakse heaks. Ajaliselt võtab kogu protseduur aega minimaalselt pool aastat kuni aasta.

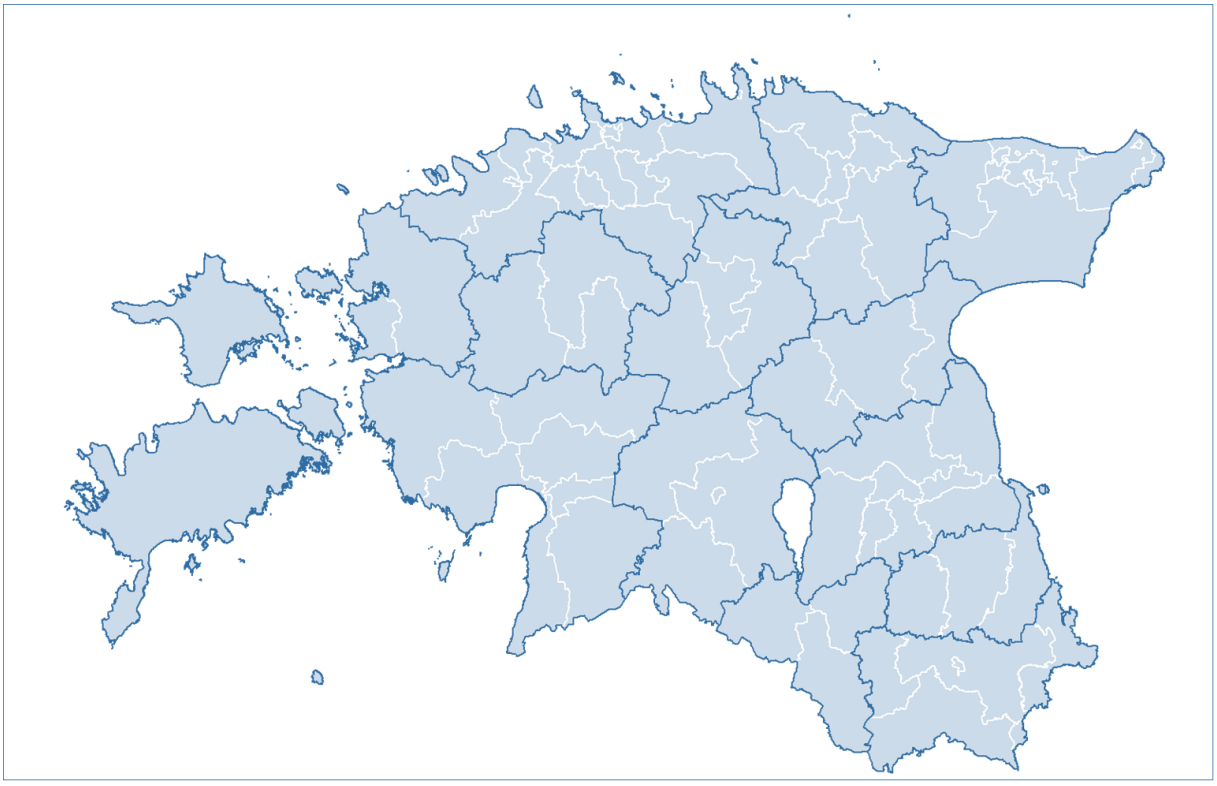
Maarja Kirss

koostöödirektor

AVALIKU TEABE SEADUSE TÄITMISEST

Vaatamata sellele, et avaliku teabe seadus on kehtinud juba alates 2001. aastast, tekitavad mõisted veel segadust. Näiteks fraasid „avalikud ülesanded" ja „avalike ülesannete täitmist puudutav teave" on avaliku teabe väljaselgitamisel tekitanud omajagu palju segadust. On üsna tavaline, et riigi äriühingud või sihtasutused ei tea, kas ja milliseid avalikke ülesandeid nad täidavad. On juhuseid, kus äriühingu või sihtasutuse asutanud avaliku sektori asutus ei oska vastata, kas ja milliseid avalikke ülesandeid tema äriühing või sihtasutus täidab. Sellisel juhul on tulnud inspektsioonil välja selgitada, kas ja mis ulatuses konkreetne eraõiguslik isik täidab avalikke ülesandeid, kuigi seda peaks iga eraõiguslik juriidiline isik ise teadma. Samuti peaks seda teadma ka avaliku sektori asutus, kes on eraõigusliku juriidilise isiku asutanud - kas ja millised ülesanded on asutus eraõiguslikule juriidilisele isikule üle andnud, mille eest lõppvastutajaks on avaliku sektori asutus. Olukorra parandamiseks on Andmekaitse Inspektsioon avalikustanud oma veebilehel mitmeid juhiseid nii teabevaldajatele kui ka laiemale üldsusele.[6]

Eesti kohalike omavalitsuste haldusjaotus 2018



Allikas: wikimedia.org

[6] Andmekaitse Inspektsiooni juhendid on leitavad: https://www.aki.ee/et/juhised.

TAGASIVAADE AVALIKU TEABE SEADUSE TÄITMISELE

Mida rohkem on teavet võrgulehtedel aktiivselt avalikustatud, seda vähem tuleb teabenõuetele vastata, kuid praktikas on paljude asutuste puhul olukord vastupidine. Seda tingib sageli puudulik oskus hindamaks, kas dokument vajab juurdepääsupiirangut või ei. Mõningatel juhtudel kehtestatakse juurdepääsupiirang igaks juhuks, mis eemaldatakse alles teabenõude korral või oodatakse, mida inspektsioon vaidemenetluses ütleb.

Teabenõuded

Teabenõuetele vastamisel eksivad teabevaldajad kõige rohkem selles, et ei vastata teabenõuetele seaduses sätestatud tähtaja jooksul. Ka juhul, kui isik on edastanud asutusele pöördumise, mis on pealkirjastatud teabenõudena, kuid on oma olemuselt selgitustaotlus, tuleb 5 tööpäeva jooksul teabenõudjat teavitada, et tema teabenõue loetakse selgitustaotluseks. Seda nõuab avaliku teabe seaduse § 23 lg 2 p 5. Isik ei pea teabenõuet esitades alati teadma, kas tema pöördumisele vastamiseks on võimalik väljastada mõnest dokumendist koopia või tuleb teavet erinevates dokumentidest alles koguda, küll aga on see teada teabevaldajale.

> „Teabenõuetele vastamisel eksivad teabevaldajad kõige rohkem selles, et ei vastata teabenõuetele seaduses sätestatud tähtaja jooksul.“

Aasta aastalt on üha rohkem ka selliseid teabenõudjaid, kes kasutavad oma õigust teabenõudeid esitada pahatahtlikult, suurendades sellega oluliselt asutuste halduskoormust. Kui eelnevatel aastatel koormasid asutusi teabenõuetega peamiselt kinnipeetavad, siis eelmisel aastal oli ka mitmeid eraisikud, kes võisid ennekõike kontrollida, kui korrektselt asutused teabenõudeid täidavad. Oli ka kodanikke, kes igal nädalal esitasid asutustele mitmeid hulgaliselt dokumente küsivaid teabenõudeid, (näiteks 10-20 dokumenti), mis ilmselgelt ei ole teabenõuete esitamise mõttega kooskõlas.

Asutuste dokumendiregistrid erineva tasemega

Asutuse dokumendiregistrit võib pidada nii mõneski mõttes asutuse peegelpildiks, kust on võimalik saada teavet asutuse tegevuse kohta. Nii on erinevate asutuste dokumendiregistrites dokumentidele juurdepääsu võimaldamine erinev. Kui mõnede asutuste dokumendiregistrites on

avalikustatud võimalikult palju teavet, siis mõne teise asutuse puhul on pea kogu teave asutusesiseseks kasutamiseks.

Kuna ametnike teadmised dokumendihaldusest ja juurdepääsupiirangute kehtestamisest on väga erinevad, siis on kerged tulema ka eksimused. Et eksimusi vältida, tuleks asutustel aeg-ajalt teha oma ametnikele töötajatele täiendkoolitusi. Samuti oleks mõistlik asutuse dokumendihalduse eest vastutavatel isikutel kontrollida oma asutuse dokumendiregistrit välisvaatest, sest nii on eksimused kiiresti tuvastatavad.

Dokumendiregistri lekete puhul on asutused teinud etteheiteid ka Andmekaitse Inspektsioonile, et miks inspektsioon ei ole suutnud välja selgitada ja kiirelt avastada puudusi dokumendiregistris. Kindlasti inspektsioon monitoorib jõudumööda asutuste dokumendiregistrid ning puuduste avastamisel reageerib nendele, kuid eelkõige on see siiski teabevaldajate kohustus tagada, et dokumendiregistrid vastaksid nõuetele ning ei avalikustataks piiranguga teavet. Inspektsioon ei saa siin asutada teabevaldajate asemele ning vastutada nende eest, et dokumendid oleksid registreeritud ja avalikustatud nõuetekohaselt. Inspektsioon saab järelevalveasutusena tegeleda ainult rikkumiste tuvastamisel nende tagajärgedega.

Kohapealsed kontrollid omavalitsustesse

2018.aastal viisid inspektorid läbi 5 kontrolli. Seekord oli eesmärgiks vaadata, kuidas on peale ühinemist korraldatud kohalikes omavalitsustes asutusesiseks kasutamiseks mõeldud teabe (AK teabe) kaitse.

> „Kõige enam esines puudusi IT valdkonnas, kuna süsteemid on vananenud ning valdades on raske leida IT valdkonda tundvaid spetsialiste.“

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

Kõige enam esines puudusi IT valdkonnas, kuna tihti on süsteemid vananenud ning valdades on raske leida IT valdkonda tundvaid spetsialiste. Tihti puudusid ka ajakohased korrad ja juhendid. Näiteks oli ühes vallas dokumendiregistrile võimaldatud juurdepääs ka vallavalitsuse liikmele, kes ei olnud enam vallaametnik ning ka praktikandile, kuid konfidentsiaalsuskokkulepet nendega ei olnud sõlmitud. Kuna kontrollid toimusid aasta algul, mil ühinenud vallad alles alustasid ühe omavalitsusena tööd, siis 2018. aasta kontrolli tulemused veel terviklikku ülevaadet valdadest ei andnud. Küll aga on inspektsioonil kavas selliseid kontrolle jätkata ka edaspidi.

Avaliku teabe nõukogu

Kui aastaid on inspektsioon korraldanud teabepäevi isikutele, kelle korraldada on asutuses isikuandmete kaitse ja teabe avalikustamine, ehk koordinaatorile, siis 2018. aastal alustas tegutsemist avaliku teabe nõukogu.

Avaliku teabe nõukogusse kuuluvad peale dokumendihalduse spetsialistide ka riigiasutuste IT valdkonda kuuluvad spetsialistid. Seega on avaliku teabe nõukogu laiemapõhjalisem ning hõlmab tegevusi nii isikuandmete kaitsel ja teabe avalikustamisel. Kuna 2018. aastal jõustus uus Euroopa Liidu isikuandmete kaitse üldmäärus, siis avaliku teabe nõukogu kohtumistel olid peamised arutlusteemad seotud just üldmääruse jõustumisega, et ühtlustada tegevusi ja leida paremaid praktikaid nõuete täitmiseks. Avaliku teabe nõukogu kohtumiste kokkuvõtted on leitavad meie võrgulehelt.[7]

Järgneval aastal kavatseme pöörata suuremat tähelepanu avaliku teabe seaduse täitmisele.

Elve Adamson

peainspektor

[7] https://www.aki.ee/et/avalik-teave/avaliku-teabe-noukogu.

OMAVALITSUSTE VEEBIKÜLGEDE SEIREST

Seirasime 2018. aastal haldusreformi järgsete kohalike omavalitsuste veebilehti. Seire üheks eesmärgiks oli saada ülevaade, kuidas on ühinenud omavalitsused suutnud täita teabe avalikustamise nõudeid.

Millal, mida ja kuidas seirati?

Omavalitsuste võrgulehekülgede seireid on läbi viidud erinevalt. Mõnel varasemal aastal on eelnevalt omavalitsusi teavitatud seire kaudu väljaselgitatavast eesmärgist. 2018. aastal seda ei tehtud. Vaatasime veebilehti tavakodaniku pilguga, sh seda kas ja kui lihtsalt on teave leitav. Seire viidi läbi augustis ja septembris, mille käigus vaadati üle 79 asutuse võrguleht.

Seire eesmärk

Peale haldusreformi on liitumise tulemusel moodustatud uusi omavalitsusi. Seire eesmärgiks oli kontrollida, kuidas uute omavalitsuste võrgulehtedel on teave avalikustatud ja kas teabe avalikustamine vastab seaduses sätestatud nõuetele ning hinnata teabe leidmise lihtsust ja asutuse tegevuse läbipaistvust.

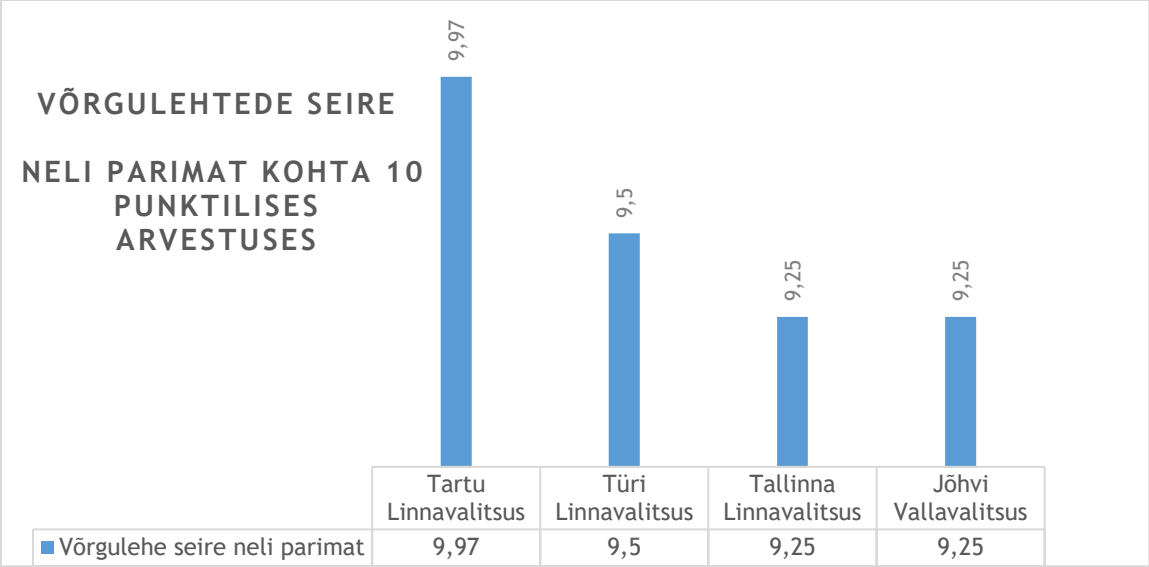
Seire kriteeriumite koostamisel lähtuti 25. mail jõustunud isikuandmete kaitse üldmäärusest, mis tõi teabe avalikustamise osas täiendavaid kohustusi. Üks nendest on avaliku sektori asutuse jaoks andmekaitsespetsialisti määramine. Andmekaitsespetsialisti andmed tuleb asutusel avalikustada ning teavitada sellest ka Andmekaitse Inspektsiooni. Samuti sai seire kriteeriumite valimisel määravaks see, mille osas on inspektsioonile saabunud kodanikelt kaebusi ja märgukirju ning üks nendest on teabe mitteleidmine veebilehelt.

Tähelepanekutest

Isikuandmete kaitse üldmääruse artikkel 37 kohustab avaliku sektori asutusi määrama andmekaitsespetsialisti ning avalikustama andmekaitsespetsialisti kontaktid. Samuti teavitama sellest järelevalveasutust. Kuna tegemist on üsna uue kohustusega, siis on andmekaitsespetsialistide kontaktandmete avalikustamine asutuste lõikes üsna erinev ning paljude omavalitsustel teave üldse puudub. Probleeme oli ka andmekaitsetingimuste kättesaadavaks tegemisel. 14 omavalitsuse veebilehelt ei õnnestunud andmekaitsetingimusi leida ja 20-l omavalitsusel olid andmekaitsetingimused uuendamata. Suurematest probleemidest nimetame veel eksimused dokumentidele ligipääsu

võimaldamisel dokumendiregistris ning samuti tehti vigu e-kirjade avalikes vaadetes eraisikute andmete avaldamisega.

Kokkuvõte



Kõige rohkem punkte - 9,75 sai võrgulehe eest Tartu Linnavalitsus. Järgnes Türi Vallavalitsus 9,5 punktiga ning 9,25 punkti said võrdselt Tallinna Linnavalitsus ja Jõhvi Vallavalitsus.

Elve Adamson

peainspektor

VAIETE MENETLUSTEST

Vaie teabe väljastamisest keeldumise kohta ärisaladuse ja suure mahu tõttu

Eesti Ekspress esitas Maanteeametile teabenõude, milles soovis tutvuda Kose-Aruvalla tee-ehituse kohta peetud koosolekute ja arutelude esimese kümne protokolliga. Maanteeamet keeldus soovitud teabe väljastamisest põhjusel, et dokumendid sisaldavad Maanteeameti lepingupartneri ärisaladust ning tegemist on suure mahuga. Maanteeamet leidis, et teabenõude täitmise mahukus seisneb eelkõige protokollide ükshaaval välja otsimises ja sisulises läbi töötamises, seoses võimalike ärisaladustega. Kogu täitedokumentatsioon on paberkandjal, mistõttu tuleb ärisaladust ja isikuandmeid sisaldav osa enne digitaliseerimist kinni katta. Samuti eeldab teabenõude spetsiifika, et teabenõude otsene täitja mõistab tehnilise dokumentatsiooni sisu. Antud olukorras ei pidanud Maanteeamet mõistlikuks vabastada inseneri kutsega töötaja avalike ülesannete täitmisest, seoses suuremahulise teabenõude täitmisega, mistõttu lähtudes avaliku teabe seaduse § 23 lg 2 p 3, keeldus teabenõude täitmist küsitud mahus.

Kuna teabenõudja soovis ainult 10-t esimest protokolli, siis Andmekaitse Inspektsioon Maanteeameti selgitustega ei nõustunud. Inspektsioon leidis, et 10 protokolli väljastamise puhul (arvestades, et protokollid on orienteeruvalt ca 3 lehekülge), mida on orienteeruvalt 30 lehekülge, ei saa kuidagi pidada suureks mahuks. Seda enam, et kuni 21 lehe väljastamine on seaduse kohaselt tasuta.

Teabenõuetele vastamine on Maanteeameti jaoks avaliku teabe seadusest tulenev kohustus. Kui Maanteeamet leiab, et teabe väljaotsimine nõuab tal asutuse töökorralduse muutmist, siis inspektsiooni hinnangul võib sellisel juhul tegemist olla Maanteeameti dokumentide haldamise (arvestuse) puudustega, mis ei saa aga olla teabenõude täitmisest keeldumise aluseks.

Ka ei nõustunud inspektsioon sellega , et protokollid on täies ulatuses ärisaladus, kuna menetluse käigus inspektsioonile näidisena saadetud protokolli nr 10 puhul jäi inspektsioonile arusaamatuks, mis selles protokollis on ärisaladus ning kuidas sellise teabe väljastamine kahjustaks Nordecon AS-i ärihuve. Ka juhul, kui mõni

protokoll sisaldabki piiranguga teavet, sh ärisaladust, mida ei saa välistada, siis ei anna see võimalust jätta dokumente tervikuna väljastamata. Sellisel juhul tuleb väljastada see osa teabest või dokumendist, millele piirang ei laiene (avaliku teabe seadus § 38 lg 2).

Eeltoodust tulenevalt tegi Andmekaitse Inspektsioon Maanteeametile ettekirjutuse - vaadata uuesti läbi vaide esitaja teabenõude punkt 2 ning väljastada vaide esitajale Kose-Aruvalla tee-ehituse kohta peetud koosolekute ja arutelude kümme esimest protokolli ulatuses, mis ei sisalda piiranguga teavet. Kui mõni protokoll jäetakse mingis osas väljastamata põhjusel, et see sisaldab Nordeconi AS ärisaladust, siis tuleb põhjendada, milles seisneb konkreetse teabe väljastamisel ärihuvide kahjustamine, küsides selleks vajadusel selgitusi Nordeconilt AS-lt.

Vaie kahju hüvitamise lepingu küsimisel

Kodanik soovis teabenõude korras saada TS Laevad OÜ-lt kompromisslepingut, mis oli sõlmitud TS Laevad ja reisija vahel seoses üleveol vigastada saanud mootorrattaga. TS Laevad keeldus lepingu väljastamisest põhjusel, et küsitud teave ei ole avalik teave ning TS Laevad ei ole küsitud teabe osas teabevaldjaks. TS Laevad oli seisukohal, et ta täidab küll avalikke ülesandeid, kuid need piirduvad ainult üleveo teenuse osutamisega ning see ei laiene reisija ja laevafirma vahel sõlmitud kompromisslepingule kahju hüvitamiseks.

Andmekaitse Inspektsioon nõustus TS Laevad OÜ seisukohaga, kuna TS Laevad OÜ puhul on tegemist eraõigusliku juriidilise isikuga, siis ei laiene talle teabevaldaja kohustused kogu tema valduses oleva teabe osas, vaid ainult teabe osas, mis puudutab üleveo teenuse osutamist.

Avalike ülesannete puhul reguleerib avalik õigus tihti soorituse tegemise kohustust, kuid sooritus ise võib alluda eraõiguslikule regulatsioonile. Nii on see ka ühistranspordi puhul – ühistranspordi (sh reisiparvlaevaga liiniteenuse) korraldamine on avalik ülesanne, mille täitmiseks sõlmitakse vedaja ning kohustust omava asutuse vahel avaliku teenindamise leping, kuid sõitja ja laevafirma vahel tekib eraõiguslik veoleping. Sellest aga tuleneb, et niisugusel juhul ei ole võlaõigusliku lepingu poolte vaheline infovahetus avalik teave. Nii on küll üleveo teenust puudutav teave avalik teave, kuid avalik teave ei ole teave konkreetsele sõitjale osutatud ühistransporditeenuse info ega info reisija ja laevafirma vahel sõlmitud lepingute osas.

Eeltoodust tulenevalt on avalik teave, millistel aegadel, tingimustel ja hinnaga osutatakse üleveo teenust ning seda saab küsida teabenõude korras. Avalikuks teabeks ei ole aga reisija ja laevafirma vahel sõlmitud lepingud. Kuna antud juhul ei puudutanud vaide esitaja teabenõudes küsitud teave avalikku teavet, siis leidis inspektsioon, et TS Laevad OÜ on keeldunud õiguspäraselt teabenõude täitmisest ja jättis vaide rahuldamata.

Vaie - Tallinna Sadam kui monopol

Vaide esitaja esitas AS-le Talllinna Sadam kui olulist vahendit omavale ettevõtjale teabenõude Muuga sadamas ja Paldiski Lõunasadamas operaatoritele pakutavate sadama infrastruktuuri kasutamise tingimuste kohta.

Teabevaldaja keeldus teabenõude täitmisest ja põhjendas seda sellega, et ta ei ole soovitud informatsiooni osas teabevaldaja avaliku teabe seaduse § 5 lõike 3 p 1 mõttes, kuna teabevaldaja ei ole turgu valitsevas seisundis ettevõtja. Teabevaldaja on seisukohal, et tal ei ole võimalik esitada teabenõudes küsitud dokumente ka seetõttu, et teabevaldaja kohustub hoidma lepingupartneritega sõlmitud lepingu sisu konfidentsiaalsena.

Teabenõudja ei nõustunud eeltoodud seisukohaga ning leidis, et teabevaldaja on turgu valitsevas seisundis ettevõtja ning seega avaliku teabe kohustatud subjekt avaliku teabe seaduse § 5 lõike 3 p 1 mõttes, järelikult ei ole teabenõudest keeldumine õiguspärane.

Vaide esitaja leidis, et teabenõudjal on teabevaldajaga sõlmitud hoonestusõiguse leping (nimetatud lepinguga omandas teabenõudja viljaterminali teabevaldajale kuuluval kinnistul) ja koostööleping Muuga sadama infrastruktuuri kasutamiseks. Viljaterminali opereerimisel kasutab teabenõudja üksnes teabevaldajale kuuluvat Muuga sadama infrastruktuuri. Teiste sadamate infrastruktuuri kasutamine ei ole võimalik juba ainuüksi seetõttu, et hoonestusõiguse leping ja koostööleping on omavahel seotud. Koostööleping lõppeb hoonestusõiguse lepingu lõppemise või lõpetamisega. Koostöölepingut on võimalik lõpetada üksnes juhul, kui infrastruktuuri kasutamine Muuga sadamas ei ole võimalik ja see võimatus kehtib vähemalt 6 kuud. Seega, sisuliselt kaasneb viljaterminali hoonestusõigusega kohustus kasutada Muuga sadama infrastruktuuri.

Arvestades, et teistel ettevõtjatel ei ole võimalik Muuga sadama infrastruktuuri dubleerida või isegi kui see oleks võimalik, ei ole see majanduslikult otstarbekas, siis omab teabevaldaja Muuga sadamas loomulikku monopoli.

Eeltoodud menetluse käigus küsis inspektsioon seisukohta ka Konkurentsiametilt.

Konkurentsiameti hinnangul ei ole esitatud andmed ja selgitused piisavad, mille tulemusel saaks kinnitada, et AS Tallinna Sadam omab nimetatud kaubaturul turgu valitsevat seisundit konkurentsiseaduse § 13 tähenduses või loomulikku monopoli konkurentsiseaduse § 15 tähenduses. Turgu valitseva seisundi kindlakstegemiseks on kõigepealt vaja piiritleda asjaomane kaubaturg, kuna Konkurentsiamet ei ole uurinud AS-i Tallinna Sadam tegevust antud valdkonnas, siis ei ole ametil endal käesoleval hetkel piisavalt andmeid kaubaturu piiritlemiseks. Tavapäraselt piiritleb Konkurentsiamet kaubaturu ja määrab ettevõtjate positsiooni konkreetse juhtumi menetluse raames, kui on ilmnenud mõni konkurentsi õiguslik probleem.

Konkurentsiamet märkis, et kui vaide esitaja leiab, et AS Tallinna Sadama on turgu valitsev ettevõtja konkurentsiseaduse tähenduses ning vaide esitajale on kehtestatud kõrgemad hinnad kui tema konkurentidele, on tal õigus pöörduda Konkurentsiametisse, kes kontrollib nimetatud väidete paikapidavust ja vastavust konkurentsiseaduses sätestatud nõuetele ning rikkumise tuvastamisel võtab kasutusele vastavad meetmed

Andmekaitse Inspektsioon leidis, et kuna Konkurentsiamet ei ole hinnanud, kas Tallinna Sadam on vaidlusalusel kaubaturul valitsevas seisus, omab eri- või ainuõigust või loomulikku monopoli, siis ei saa inspektsioon asuda seisukohale, et Tallinna Sadam on teabevaldajaks avaliku teabe seaduse § 5 lg 3 p 1 mõistes. Samuti oli vaide esitaja täiendavalt pöördunud ka juba kohtu poole andmete välja nõudmiseks. Samas asjas oli paralleelselt juba käimas ka kohtumenetlus, millisel juhul puudub inspektsioonil pädevus menetluse jätkamiseks, kuna kohtul tuleb sisuliselt lahendada sama küsimus. Eeltoodust tulenevalt jättis inspektsioon vaide rahuldamata.

Elve Adamson

peainspektor

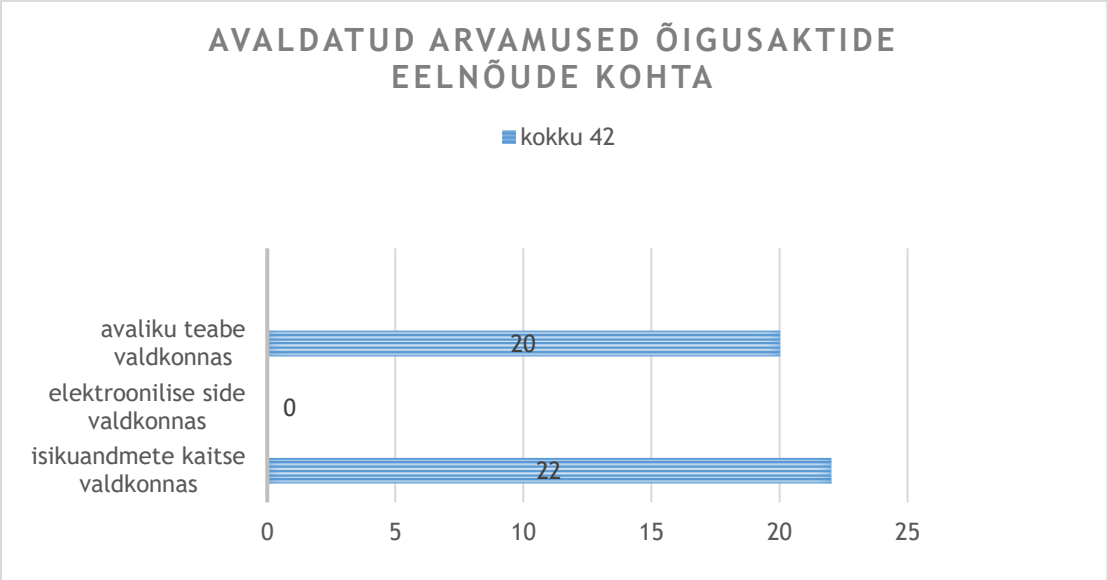
ÕIGUSLOOME ARENGUTEST JA KOHTULAHENDID

Möödunud aasta oli õigusloomes väga tegus ning tõi Andmekaitse Inspektsiooni lauale palju eelnõusid, milledele küsiti inspektsiooni arvamust. Kokku andis inspektsioon tagasisidet 42 õigusakti eelnõu kohta.

Mitmed eelnõud ei olnud selgelt läbi mõeldud või tehtud kohati kiirustades. Paljuski oli see kiirustamine seotud ka isikuandmete kaitse üldmääruse jõustumisega ning nende muudatustega, mis oli vaja teha Eesti õiguskorras, et muuta eriseadusi ning omakorda ka andmekogude põhimäärusi. Järgnevatel lehekülgedel on oluline teha ülevaade nendest inspektsioonile kooskõlastamiseks esitatud ja tagasiside saanud eelnõudest, mis tõid kaasa andmetöötluses suuremaid muutusi. Aastaraamatus käsitleme samuti üldisemaid tähelepanekud probleemidele või tendentsidele, mida oleme õigusaktide eelnõudes korduvalt välja toonud seoses inimeste eraelu kaitse tagamisega ja ligipääsuga avalikule teabele.

Allikas: Pixabay

ÕIGUSLOOME ARENGUTEST



Avaliku teabe seaduse muutmine seoses direktiiviga nr 2016/2102

Möödunud aastal võeti avaliku teabe seadusesse üle Euroopa Parlamendi ja nõukogu direktiiv (EL) nr 2016/2102, mis käsitleb avaliku sektori asutuste veebisaitide ja mobiilirakenduste juurdepääsetavust, arvestades erivajadusi, sealhulgas nägemis-, kuulmis-, taju-, kõne- ja keelepuudeid, õpiraskusi ning füüsilisi ja neuroloogilisi puudeid. Selle muudatuste tulemusena lisandub inspektsioonile kohustus teostada avaliku sektori asutuste veebilehtede ja mobiilirakenduste osas järelevalvet, et need vastaksid juurdepääsetavuse nõuetele. Lisaks peame esitama ka järelevalve raames kogutud seire aruandeid Euroopa Komisjonile.

Algne inspektsioonile kooskõlastusele saadetud eelnõu oleks laiendanud ülevõetava direktiivi nõuded kõigile teabevaldajatele, sh ka eraõiguslikule juriidilisele isikule ja füüsilisele isikule, kui ta täidab avalikku ülesannet avaliku teabe seaduse § 5 lõike 2 mõttes või kui ta on teabevaldajaga võrdsustatud sama seaduse § 5 lõike 3 kohaselt.

Leidsime oma arvamuses, et kooskõlastamisele saadetud avaliku teabe seaduse muutmise eelnõus ei olnud piisavalt analüüsitud mõju nendele eraõiguslikele teabevaldajatele. Eelnõu seletuskirjas oli peamiselt keskendutud nn avaliku sektori teabevaldajate mõjudele, sh oli toodud arvud ja kulud võimalike veebilehtede ning mobiilirakenduste arvu kohta – eelnõu seletuskirjas puudusid sellekohased näitajaid ning analüüsid nn erasektori teabevaldajate osas.

Samuti leidsime, et meelevaldselt on sooviti esialgse eelnõuga laiendada kavandatud avaliku teabe seaduse § 31 lõike 1 nõudeid ka sama seaduse § 5 lõigete 2 ja 3 mõistes teabevaldajatele.

> „Küsimusena ning probleemina jääb üles asjaolu, et reaalsuses on nn eraõiguslikel teabevaldajatel raskusi aru saada, kas ning mis teabe osas on nad üldse teabevaldajad, sh kuidas määratleda avalikku ülesannet.“

Enne Riigikogule eelnõu esitamist lisati eelnõusse säte, et juurdepääsetavuse nõuded ei kohaldata avaliku teabe seaduse § 5 lõikes 3 nimetatud teabevaldajaga võrdsustatud isikule. See tähendab, et juurdepääsetavuse nõuded on avaliku teabe seaduse § 5 lõikes 2 toodud avalikku ülesannet täitvatel eraõiguslikel juriidilistel ning füüsilistel isikutel. Seega ei ole kõik need nn eraõiguslikud teabevaldajad nende nõuete täitmisest vabastatud. Küsimusena ning probleemina jääb üles asjaolu, et reaalsuses on nn eraõiguslikel teabevaldajatel raskusi aru saada, kas ning mis teabe osas on nad üldse teabevaldajad, sh kuidas määratleda avalikku ülesannet.

Eraõiguslikel teabevaldajatel puhul saab olla ainult üks võimalus, kuidas ligipääsetavuse nõuded neile ei kehti – avaliku teabe seaduse § 32 lg 1 p 6 võimaldab juurdepääsetavuse nõudeid mitte täita, kui see nõuab ebaproportsionaalselt suuri pingutusi. See pingutus on sama paragrahvi lõike 4 kohaselt suur, kui teabevaldaja suurust, ressurssi ja tüüpi ning veebilehe või mobiilirakenduse kasutamise sagedust ja kestust arvestades toob veebilehe või mobiilirakenduse ligipääsetavaks tegemine kaasa ebamõistlikud kulud.

Riikliku statistika seaduse väljatöötamiskavatsus

Väljatöötamiskavatsuse vajadus tulenevat olukorrast, kus andmekogudest olevad andmeid ei ole piisava kvaliteediga, et nende põhjal teha riiklikku statistikat. Väljatöötamiskavatsuses märgitakse, et statistika tegemiseks saadavad andmed ei pruugi olla õiged või need ei ole täielikud ning seetõttu ei saa nende alusel teha riikliku ja rahvusvahelistele kvaliteedinõuetele vastavat statistikat nõutava kvaliteediga. Erinevate andmekogude andmeid ei ole võimalik omavahel siduda selliselt, et teha statistikat üksnes nende põhjal.

Selle probleemi lahendamiseks sooviti Eestis määrata ühene andmekogude sisuline andmehalduse koordineerimine. Selleks tehti muudatusi nii riikliku statistika seaduses kui ka avaliku teabe seaduses. Nõustusime, et riiklikes

andmekogudes kogutavate ja kasutatavate isikuandmete ning muude andmete kvaliteeti tuleb tõsta. Samas tuleb arvestada, et tegemist on pikaajalise protsessiga, mis vajab selget läbi mõtlemist ning teostust. Seetõttu tooksin välja ainult mõned esitatud tagasisides tõstatatud murekohad.

Oma tagasisides leidsime, et Statistikaametil oli juba enne nende muudatuste tegemist mõningad meetmed, mida nad saaksid kasutada – nt andmekogude kooskõlastamiste raames riigi infosüsteemi haldussüsteemis. Seda seetõttu, et Statistikaametil oli ka varasemalt võimalik statistikaseaduse alusel teha „ettepanekuid andmekogudes olevate andmete koosseisu ja kasutatavate klassifikaatorite muutmiseks, kui andmete kaetus ning andmekogus olevate andmete koosseis, detailsus ja kvaliteet ei võimalda teha riikliku statistika kvaliteedikriteeriumidele vastavat riiklikku statistikat.".

Tagasisides tõime ka välja, et esmalt on vaja enne andmekogude tehnilist sidumist vaja selgeks teha, kas neid andmekogusid on võimalik üldse õiguslikult siduda – ennekõike, kas ühel eesmärgil kogutud (isiku)andmeid on lubatud kanda teise andmekogusse ja/või ühendada kaks või enam andmekogu. Samuti peab arvestama asjaoluga, et avaliku teabe seaduse § 3^1 reguleerib avaliku teabe taaskasutamist, mille lõike 1 viimane lause ütleb selgelt: „Teabevaldajate vahel teabe vahetamine oma avalike ülesannete täitmiseks ei ole teabe taaskasutamine". Poliitika kujundamiseks andmete töötlemine on oma olemuselt avalik ülesanne.

Lisaks tekitas meile ka küsitavusi väljatöötamiskavatsuses märgitud üldvolitus, mis lubaks Statistikaametil koguda kõiki andmeid sh et ei saaks keelduda andmete väljastamisest mõnes eriseaduses toodud saladuse hoidmise kohustuse tõttu (nt maksu- või pangasaladuse osas). Erandina leitakse, et see oleks õigustatud „ulatusliku privaatsusriivega seotud" andmete töötlemise korral, kuid väljatöötamiskavatsusest ei selgunud, mis oleksid sellekohased näited ning kuidas seda mõeldakse ära reguleerida. Juhtisime tähelepanu asjaolule, et isikuandmete töötlemise üks läbivaid põhimõtteid on läbipaistev andmete töötlemine. Kui Statistikaametile tekib nn üldvolitus kõigilt ja kõiki andmeid koguda, siis võib riiklike andmekogude vastutavatel töötlejatel ning sisuliselt ka erasektori isikuandmete töötlejatel tekkida raskusi andmesubjektide ees läbipaistvuse tagamisel, kui ka nende enda toimingute korral. Näiteks olukorras, kus Statistikaamet sooviks saada terviseandmeid.

Väljatöötamiskavatsuses pakuti ka välja soov, et reguleeritakse andmejagamisteenuse olemus – seda kasutataks riikliku statistikatööde määratlusest välja jäävate tööde puhul. Selle teenuse sisu oleks riiklike „andmete

kogumine ja taaskasutamine andmeanalüüsi kaudu statistilistel ja ühiskonnale kasulikel eesmärkidel. Kusjuures oluline on, et andmeid on võimalik koguda ja kasutada mitte ainult riikliku statistika tegemiseks, vaid ka andmete vaheliste seoste, nende peidetud tähenduste sh andmekaeve jms ülesannete lahendamiseks ning nende alusel statistika tegemiseks. Selliselt tehtud statistika ja osutatud andmejagamisteenus edastatakse konkreetsele rühmale või tellijale. Täiendada tuleks [riikliku statistika seaduse] paragrahvi 35, mis käsitleb konfidentsiaalsete andmete levitamist ning lubada riikliku statistika tegijal levitada isiku nõusolekuta statistilise üksuse otsest või kaudset tuvastamist võimaldavaid andmeid riikliku poliitika kujundamise eesmärgil, kuid välistades isikute suhtes kohustavate haldusaktide andmist nimetatud andmetele tuginedes."

Selle teenuse osas märkisime tagasisides, et riiklike andmete taaskasutamine on seotud avaliku teabe seaduses reguleeritud avaandmete temaatikaga ning selle kohaselt ei ole lubatud avaliku sektori sees avaandmete vahetamist ametiülesannete raames. Avaliku teabe seaduses sätestatu, et avaandmete hinnangu viib läbi teabevaldaja ning sama seaduse kohaselt, ei ole avaandmete hulka arvatud isikuandmed (statistilises mõttes statistilised üksust otseselt või kaudselt tuvastatavad andmed). Nõustusime sellega, et andmejagamisteenuse raames edastatud andmeid ei tohi kasutada isikute suhtes kohustatavate haldusaktide andmiseks. Samas ei olnud väljatöötamiskavatsuses täpsemat teavet, kuidas tagatakse, et selle nõude vastu ei eksita, sh kuidas toimub kontrollimehhanism.

Tagasisides märkisime lisaks, et väljatöötamiskavatsuses ei olnud teavet, millise põhiseaduse §-s 26 toodud seadusereservatsiooni alusel õigustatakse konkreetsel juhul privaatsusõiguse riivet.

Väljatöötamiskavatsuses ei olnud ka üldse mainitud, et mõjutatud on ka isikuandmete reaalsed omanikud ehk andmesubjektid. Väljatöötamiskavatsuses oli märgitud, et andmejagamisteenuse kasutamisel on kaudne mõju üksikisikutele, kuid rohkem teavet selle kohta ei kirjeldatud. Kui arvestada, et Statistikaamet teostab sisuliselt massandmetöötlust statistika tegemiseks, siis on andmesubjektidele vastavad mõjud kohe kindlalt olemas. Samuti ei olnud väljatöötamiskavatsuses teostatud andmekaitsealast mõjuanalüüsi.

Väljatöötamiskavatsuse järgselt koostati riikliku statistika seaduse ning avaliku teabe seaduse muutmise seaduse eelnõu, mis võeti vastu 20.02.2019 ning see jõustub 01.04.2019. Kahetsusväärselt ei esitatud seda eelnõu meile ametliku arvamuse avaldamiseks.

Massprofileerimisest riigi andmekogudes

2018. aastat resümeerides saab kirjutada, et (isiku)andmete töötlemise algatusi soovitakse edasi arendada. Riigi andmekogudes olevate isikuandmete massanalüüsist kui probleemsest teemast oleme ka 2016. aasta kui ka 2017. aasta ettekannetes kirjutanud.[8]

Oleme seisukohal, et suuremas mahus (isiku)andmete töötlemine tohib toimuda ainult üksnes piiratud ja konkreetsetel tingimustel – nt ainult raskete kuritegude avastamiseks ja menetlemiseks, andmete esmane massanalüüs toimub väga lühikese aja, nt 24 tunni jooksul, edasisele säilitamisele kuuluvad üksnes positiivsed leiud jms.

> „Lausjälgimist võib teatud piiratud juhtudel siiski teha, kuid selle raamid peavad olema selged ja proportsionaalsed.“

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

Oleme jätkuvalt seisukohal ka selles osas, et korrakaitseseaduse alusel ei saa mitmetest andmekogudest koguda andmeid kokku, et teostada järelevalvelist massandmetöötlust - sellekohane norm on korrakaitseseadusest lihtsalt puudu.

Lisaks tuleb arvestada, et nii isikuandmete kaitse üldmääruse artikkel 22 kui ka isikuandmete kaitse seaduse § 21 keelab teha üksnes automatiseeritud töötlusel põhinevat otsust, sh profiilianalüüsi, kui see toob andmesubjektile kaasa teda puudutavaid kahjulikke tagajärgi või avaldab talle muud märkimisväärset mõju. Selline tegevus on ainult siis lubatud, kui sellise otsuse tegemine on lubatud liidu või liikmesriigi õigusega (ennekõike seadusega), milles on sätestatud

[8] Vt meie 2017. aastal koostatud aastaraamatut 2016. aasta kohta, konkreetsemalt lk 11, 62 – kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/aastaraamat_2016.pdf. Lisaks ka meie 12.08.2016 kiri nr 1.2.-4/16/932 Justiitsministeeriumile (http://adr.rik.ee/aki/dokument/4789810).

asjakohased meetmed andmesubjektide õiguste ja vabaduste ning õigustatud huvide kaitseks.

Soolise võrdõiguslikkuse seaduse jt seaduste muutmine

Meil oli võimalik sellele eelnõule oma arvamus esitada kahel korral – nii Sotsiaalministeeriumile kui ka Riigikogu põhiseaduskomisjonile. Sisuliselt mõlemal juhul olid esitatud samad seisukohad, kuna esialgselt antud tagasisidet ei olnud arvestatud. Siiski ei jõudnud Riigikogu seda eelnõu lõpuni arutada (Riigikogu kolmanda lugemiseni ei jõutud) ning see langes Riigikogu menetlusest välja.

Selle eelnõuga sooviti sisuliselt muuta avalikus sektoris läbipaistvamaks nii ametnikele kui töötajatele erinevate makstavate tasude osas. Kuigi selline initsiatiiv on tervitatav, leidsime planeeritud lahenduse osas mitmeid puudujääke.

Soolise võrdõiguslikkuse seaduse (SoVS) jt seaduse muutmise eelnõu kohaselt soovitakse ametnikele ja töötajatele anda üldistatud ning statistilist teavet erinevate makstud tasude kohta, sh võrdlust ametigruppide kaupa. Samas, kui organisatsioon ei ole töökohti ametigruppidesse jaotanud, siis esitatakse informatsioon ametikohtade kaupa.

Juhtisime tähelepanu, et kui personali koosseisu kohta kogutakse teavet organisatsiooni eri tasanditel ja ametigruppides, siis võib juhtuda nii, et kui ühe tasandi või grupi moodustab sisuliselt üks inimene, siis võib olla tegemist isikuandmetega, kuna inimene võib olla kaudselt tuvastatav. Näiteks, kui on kaks sama tasandi inimest, kes on eri soost, kuid eelnõu kohaselt on soov neid andmeid koguda soopõhiselt. Seega on kaudse tuvastamise risk olemas.

Eelnõuga sooviti Tööinspektsioonile anda ülesanne teha üks kord aastas automatiseerituna töökeskkonna andmekogus esmase palgaandmete analüüs. Seletuskirjas märgiti, et *„[Tööinspektsioon] hindab esmase palgaandmete analüüsi raames organisatsiooni töötasu andmeid riigi infosüsteemides olemas olevate andmete alusel ehk teeb sisuliselt tööandjaga kontakteerumata eelhinnangu ehk korrakaitseseaduse tähenduses ohuprognoosi. Kui ohuprognoosi tulemusel tekib kahtlus, et tööandja tegevus on diskrimineeriv vastavalt SoVS § 6 lõike 2 punktile 3, võib [Tööinspektsioon] sekkuda ja teha keskmiselt kümne ja enama töötajaga avaliku sektori tööandajale ettekirjutuse naiste ja meeste võrdse palga auditi läbiviimiseks (palgaaudit).“*

Kordasime seisukohana uuesti üle, et korrakaitseseadus ei luba teostada massandmetöötlust – sellele asjaolule oleme ka avalikkuse ees mitmel korral

kirjutanud (vt eelmise alapeatüki teemat). Seetõttu me ei pooldanud käsitlust, kus esmane palgaandmete analüüs toimuks korrakaitseseaduse alusel, tehes massandmetöötlust andmekogude põhjal. Sel juhul tekib ka küsitavus, et kui korrakaitseseaduse aluselt toimub massandmetöötlus kavandatud SoVS § 3 lg 2 punktis 3 märgitud „riigi ja kohaliku omavalitsuse osalusega äriühingu, riigi ja kohaliku omavalitsuse asutatud sihtasutuse ja mittetulundusühingu" suhtes, siis tekitas veel suuremat küsitavust, kuidas õigustatakse muude, nö puhtalt avaliku sektori asutuste osas toimuvat massandmetöötlust. Sel juhul toimub Vabariigi Valitsuse seaduse alusel haldusjärelevalvemenetlus, mitte korrakaitseseaduse alusel „ohuprognoosi koostamine".

Samuti tekitas ka küsitavust, milliseid tagatisi on andmesubjektidele antud seoses kavandatava „massandmetöötlusega", mille olemus on sarnane automaatsete otsuse, sh profiilianalüüsi tegemisega. Isikuandmete kaitse üldmääruse art 22 (2) punkti b kohaselt peavad olema seadusandluses ka asjakohased meetmed andmesubjekti õiguste ja vabaduste ning õigustatud huvide kaitseks.

Kavandatud SoVS § 11^1 lg 5 kohaselt oleks pidanud avaliku sektori tööandja avalikustama oma kodulehel soopõhise võrdluse ehk organisatsiooni soolise palgalõhe. Samas eelnõust ega seletuskirjast ei olnud arusaadav, mis on soopõhise võrdluse tulem, mis tuleb avalikustada. Seletuskirjas oli küll märgitud, et tegemist on „keskmise soolise palgalõhega" ning et tööandja ei avalikusta oma töötajate palka isikustatult ega nimeliselt. Leidsime, et selle kohustuse täitmisega seonduvalt võib tekkida probleem olukorras, kui inimene on kaudselt tuvastatav nende andmete alusel – samas ei ole eelnõus selgitatud, mida sel puhul tuleks ette võtta.

Selle eelnõu puhul oli esialgu kooskõlastamisele saadetud eelnõu seletuskirjast puudu ka andmekaitsealane mõjuhinnang ehk puudus riskide analüüs andmesubjekti ning teda mõjutatavate tegevuste osas. Riigikogule esitatud eelnõus oli mingis osas andmekaitsealane mõjuhinnang tehtud, kuid leidsime, et kõiki asjaolusid ei olnud selles arvestatud – jätkuvalt oli oht, et alusandmed Tööinspektsiooni teostatava palgaandmete soopõhise võrdluse tegemiseks võivad tekitada ohu, et konkreetne inimene on kaudselt tuvastatav.

Tähelepanekud Vabariigi Valitsuse ning ministrite määruste osas

Vabariigi Valitsuse ning ministrite määruste muudatused olid ennekõike seotud andmekogude põhimääruste muutmisega. Paljudel juhtudel olid need seotud isikuandmete kaitse üldmääruse jõustumisega ning sisaldasid sellega

kohaldumiseks vajalikke muudatusi, kuid nendes esines ka probleeme, milledele oleme juba varasemalt tähelepanu juhtinud. Toon välja mõned põhilisemad neist:

- Andmekoosseisude ammendav määratlemine – need pole põhimääruses ja/või selle lisas piisavalt konkreetselt ja selgelt määratletud. Kui andmete koosseis on väga mahukas, võib loetelu esitada põhimääruse lisana, nt menetluste/andmekogud osade kaupa. Olgu mainitud, et isikuandmete töötlemine peab olema inimese jaoks piisavalt läbipaistev ning omakorda ka seaduslik: seda nõuavad nii isikuandmete kaitse üldmääruse artikkel 5 lg 1 punkt a, direktiivi 2016/680 (nn õiguskaitseasutuste direktiiv) põhjenduspunkt 26 kui ka avaliku teabe seaduse § 43^5 lõige 1. Tuleb arvestada, et avalik sektor tohib ainult neid andmeid koguda, mis talle seadusandlus lubab ning kui kogutavad (isiku)andmed ei ole piisavalt ammendavalt paika pandud, ei ole võimalik läbipaistavalt ja seaduslikult kogutavate andmetega toimetada.
- Mõningate põhimääruste muudatuste puhul selgus, et mõningaid (isiku)andmeid edaspidiselt ei koguta ega töödelda, kuid eelnõudest endast ei olnud otseselt selge, mida nende (isiku)andmetega tehakse. Kui eelnõude muudatuste tulemusena neid (isiku)andmeid enam ei koguta ning ei ole ka teavet, mida juba kogutud (isiku)andmetega tehakse, siis tuleb need andmed kustutada, sest puudub õiguslik alus nende hoidmiseks ja säilitamiseks.
- Väga sageli on andmekogude põhimäärustes sees nn stampsäte, et andmekogus võidakse teha päringuid ka teistesse andmekogudesse – see säte ei anna täit selgust andmete algsetest allikatest ehk andmeandjatest. Ka avaliku teabe seaduse § 43^5 lõige 1 sätestab nõude, et andmekogu põhimääruses pannakse paika andmeandjad ehk selline tegevus peab olema läbipaistev.
- Ei ole selgelt välja toodud (isiku)andmetele juurdepääsu saajad – nt ei ole sageli püsijuurdepääsu saavad asutused ja isikud põhimäärustes ära loetletud või ei ole ära määratletud, kuidas see juurdepääsukorraldus toimub.
- Mõningate andmekogude põhimäärustes oli ka märgitud, et kui andmekogule antakse juurdepääs, siis „vajaduse korral sõlmitakse“ selle andmete saajaga selle juurdepääsu kohta leping – leiame, et sedasorti juurdepääsu sõlmitav lepingu peab kindlasti sõlmima, mitte jätta ainult „vajaduse“ põhiseks. See on ka eriti oluline olukorras, kus andmekogu vastutav töötleja annab mingi ülesande üle volitatud töötlejale – sel juhul on vajalik sedasorti leping sõlmida ka isikuandmete kaitse üldmääruse

artiklist 28 ning isikuandmete kaitse seaduse §-st 30 tulenevate nõuete tõttu.

- Mida tundlikumad andmeid kogutakse, seda suurem on vajadus sätestada ennekõike seaduse tasandil lisatagatised inimestele, et tema kohta kogutud andmetele ei antaks juurdepääsu selleks mittesobivatel eesmärkidel
- Järjest rohkem on soovitud juba loodud andmekogu juurde luua või luua eraldi andmeladu, et kogutud (isiku)andmeid analüüsida erinevatel eesmärkidel. Sedasorti suuremahuliste andmete kogumite puhul tekivad ka uued riskid ja probleemid, eriti kui andmelaos toimuvad andmete töötlemised võivad mõjuda negatiivselt inimesele – nt teda profileeritakse nende andmete alusel. Seetõttu tulekski meie arvates ennekõike seadusandluses ära reguleerida, millistel eesmärkidel võib neid andmeid kasutada, sh et neil ei oleks negatiivseid mõjutusi inimesele – nt reguleeritakse ära, kes ning millistel tingimustel võib nendele andmetele juurdepääsu saada, rakendatakse kohe andmete saamise alguses isikuandmete isikustamata kujule viimist jne. Sisuliselt on vajalik, et kohe algusest peale rakendatakse lõimitud ja vaikimisi andmekaitset selle andmelao puhul.
- Järjest enam soovib riik automatiseerida oma otsuste tegemist ehk teha automaatseid otsuseid. Tegelikkuses on üldreegel, et lihtsalt niisama sedasorti automaatset otsust teha ei tohi – selleks peavad olema seadusandluses sätestatud asjakohased meetmed inimeste õiguste ja vabaduste ning õigustatud huvide kaitseks. Seda nõuavad nii isikuandmete kaitse üldmääruse artikkel 22 kui ka isikuandmete kaitse seaduse § 21.
- Andmete säilitamistähtajad tuleb konkreetselt selgeks määrata, olema proportsionaalsed ning seletuskirjas ära põhjendatud – väga sageli ei ole andmete säilitamistähtaegade pikkused piisavalt selgelt ja arusaadavalt määratletud ning on ülemäära pikad.
- Mitmes andmekogu põhimääruses oli ka reguleeritud, et teatud aja pärast kantakse (isiku)andmed andmekogu arhiivi, kuid ei ole piisavalt selgelt reguleeritud, kes, millistel tingimustel ja eesmärkidel nendele juurdepääsu saavad. Arhiiviga on paljuski seotud ka säilitamistähtajad, kuna ka arhiivis toimub (isiku)andmete säilitamine ning ka see tuleb piisavalt selgelt ja eesmärgipäraselt ära määratleda ning seadusandluses paika panna.
- Avaliku teabe seaduse § 43^9 lõike 5 kohaselt toimub andmevahetus riigi infosüsteemi kuuluvate andmekogudega ja riigi infosüsteemi kuuluvate

andmekogude vahel läbi riigi infosüsteemi andmevahetuskihi ehk X-tee. Mõningate eelnõude puhul oli soovitud reguleerida, et andmekoguga ei toimu andmevahetus üle X-tee (nt „muul kokkulepitud elektroonset teabevahetust võimaldaval viisil"), kuid nagu öeldud, ei ole see lubatud.

- Mitme andmekogu põhimääruse muutmise eelnõus ei olnud üldse või oli puudulikult läbi viidud riskide analüüs ehk andmekaitsealane mõjuhinnang. Selle kõige eelduseks on muidugi, et selline andmetöötlus on üldse kohane põhiseaduse § 26 kohaselt ehk ka eelnõus on seda aspekti analüüsitud – ennekõike eriliigiliste isikuandmete ja teiste tundlike isikuandmetega (nt teave sotsiaalabi maksmise kohta; side- või finantsandmed) seotud andmetöötluste korral.
- Kui soovitakse andmekogu andmeid anda avaandmeteks, siis tuleb teha eraldi avaandmete mõjuhinnang. – soovitatavalt näiteks andmekogu muutvas eelnõu seletuskirjas. Kui tegemist on andmekogu avaandmetega, siis avaliku teabe seaduse § 29 lõike 6 kohaselt tuleb sellekohased avaandmed avalikustada Eesti teabevärava (www.eesti.ee) kaudu – kuigi praktikas tehakse seda Eesti Avaandmete portaalis (https://opendata.riik.ee/).
- Eelnõudele kooskõlastusi andes andsime soovituse lisada andmekogudele andmejälgija teenus[9] – selle teenuse kasutamine muudab läbipaistvamaks ning selgemaks, mida andmesubjektide andmetega tehakse, sh kes neid andmeid töötleb.
- Juhtisime tähelepanu asjaolule, et andmekogu reaalsete andmetega (*live-andmetega*) testimine ei ole lubatud.[10]

Raavo Palu

õigusdirektor

[9] Andmejälgija selgitus: https://www.ria.ee/et/riigi-infosusteem/x-tee/andmejalgija.html.

[10] Oleme varasemalt avaldanud ringkirja reaalandmetega testimise kohta: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ringkiri%20201503%20-%20testimine%20reaalandmetega.pdf.

ANDMEKAITSE INSPEKTSIOONIGA SEOTUD KOHTUASJAD

Üheks järelevalveasutuse tegevuse mõõdupuuks on tema otsuste ja toimingute vastavus seadusandlusele. Andmekaitse Inspektsiooni tegevuse kontrollimiseks on võimalik esitada inspektsioonile vaie, et saame hinnata oma tegevuse uuesti üle või esitada kaebuse halduskohtusse.

Viimast varianti on igal aastal kasutatud ning eelmisel aastal lõppesid mõned kohtuasjad, mis olid seotud inspektsiooni tehtavate toimingute või haldusaktidega. Neist tähelepanuväärsematena toome välja kolm kohtuasja.

Kohaliku omavalitsuse töötajate palgaandmete avalikkus

Üks eraisik esitas Tartu Vallale teabenõude, milles soovis saada koopiaid mitmetest käskkirjadest. Soovitud teave sisaldas käskkirjasid, milles määrati Tartu Vallale ja tema hallatavate asutuste töötajatele erinevaid tasusid või tegemist oli mõne töötaja tööle vormistamise või lähetusse saatmise käskkirjaga. Vald väljastas osa teabest, mida ta pidas avalikuks teabeks, kuid jättis mõningad dokumendid väljastamata. Selle peale esitati vaie Andmekaitse Inspektsioonile.

Leidsime vaideotsuse ja ettekirjutus-hoiatusega nr 2.1-3/15/2139 (edaspidi: vaideotsus), et vaie rahuldatakse täielikult ning tegime ettekirjutuse, millega kohustasime valda väljastama soovitud teave kooskõlas avaliku teabe seaduse § 36 lg 1 p 9 sätestatuga (koos tasudega).

Lühidalt kokkuvõttes märkisime vaideotsuse põhjendustes, et teabe avalikustamises tuleb arvestada kahte avalikustamise viisi: aktiivne avalikustamine (asutus ise aktiivselt avalikustab oma võrgulehel avalikku teavet ilma, et oleks vaja teabenõuet esitada; nt avaliku teenistuse seaduse alusel ametnike palgaandmete avalikustamine, mis ei hõlma töölepinguga töötavaid isikuid) ning passiivne avalikustamine (teavet ei avalikustata omaalgatuslikult, vaid see piirdub teabenõuetele vastamisega). Leidsime, et avaliku sektori palgaandmed peaksid olema avalikud, sh on see seisukoht jäänud püsima ka tööõiguse ja avaliku teenistuse reformide korral. Avaliku teenistuse seadus ei välista avaliku sektori palgaandmete küsimist teabenõude korras. Samuti keelab avaliku teabe seaduse § 36 lg 1 p 9 tunnistada asutusesiseseks kasutamiseks dokumente avalik õigusliku isiku eelarvevahendite kasutamise ja eelarvest makstud tasude ja hüvitiste kohta. Ehk kui teabele piirangut kehtestada ei saa või ei tohi, siis tuleb teave väljastada täies ulatuses. Riigikohtu halduskolleegium on leidnud oma otsuses 3-3-1-19-14 punktis 19 et avaliku teabe seaduse kohaldamisel

ei ole tähtsust isegi mitte sellel, millisest allikast pärineb raha kulude kandmiseks.

Vaideotsuses märkisime samuti: kui avaliku teabe seaduse § 28 lg 1 p 25 alusel umbisikuline palgaandmete avaldamine üldjuhul küsimusi ei tekita, kuid kui palgaandmeid küsitakse teabenõude korras ja nimeliselt, leitakse tihti, et see on vastuolus üldise tööõigusliku põhimõttega, mille kohaselt tööandja avaldab palgaandmeid kolmandatele osapooltele üksnes töötaja nõusolekul (töölepingu seaduse § 28 lg 2 p 13). Sama norm aga lubab avaldada palgaandmeid ka töötaja nõusolekuta, kui avaldamise aluseks on seadus. Antud juhul on selleks seaduseks, mis keelab eelarvest makstud tasudele piirangut kehtestada just avaliku teabe seaduse § 36 lg 1 p 9, mille kohaselt on tegemist passiivselt avaliku teabega, mis väljastatakse teabenõude korras. Avaliku teabe seaduse § 36 lg 1 p 9 on võrreldes töölepingu seaduse § 28 lg 2 p 13 erinorm, mis sätestab, et eelarvest maksutud tasud sh makstud palk on väljaküsitavad teabenõude korras. Kuna töölepingu seaduse § 28 lg 2 p 13 sätestab, et töötasude andmeid võib ilma töötaja nõusolekuta avaldada seaduse alusel, oleme seisukohal, et avaliku teabe seaduses sätestatu on samasugune erand nagu kohtumenetluse seadustikud või maksukorralduse seadus.

„Töötaja töötasu ei tule aktiivselt avalikustada veebilehel, kuid see omakorda ei anna vastust olukorrale, kus teavet küsitakse teabenõude korral."

Kohtuasi nr 3-15-3228.

Leidsime, et seadusandja tahe teabe väljastamisel eelarvest makstud tasude kohta avaliku teabe seaduse § 36 lg 1 p 9 alusel on tagada avaliku sektori läbipaistvus ja see ei riiva ülemääraselt isiku eraelu. Teistsugune on olukord siis, kui makstakse näiteks toimetuleku toetusi, millest on järeldatav isiku majanduslik seisukord. Sellisel juhul on toetuse saajate nimedele piirangute kehtestamine põhjendatud. Ka tol hetkel kehtinud isikuandmete kaitse seaduse (kehtis kuni 14.01.2019) § 11 lg 1 lubas isikuandmete avalikustamist, kui avalikustamine toimub seaduse alusel. Antud juhul sätestabki avaliku teabe seaduse § 36 lg 1 p 9 passiivse avalikustamise kohustuse.

Vald esitas koostatud vaideotsuse ja ettekirjutus-hoiatuse peale kaebuse halduskohtusse ning soovis esialgse õiguskaitse kohaldamist. Halduskohus esialgse õiguskaitse taotlus osaliselt ning peatas eelnevalt märgitud vaideotsuse ja ettekirjutus-hoiatuse osaliselt nii, et vallavalitsusel tuli teabenõudjale tema

nõutud käskkirjad väljastada, kattes neis kinni töölepingu alusel töötasu saavate isikute töötasud. Tallinna Halduskohus rahuldas oma otsusega Tartu valla kaebuse ning tühistas inspektsiooni vaideotsuse. Esitasime apellatsioonikaebuse, millega taotlesime tühistada halduskohtu otsuse ja teha asjas uus otsus, millega jäetaks kaebus rahuldamata. Tallinna Ringkonnakohus jättis oma otsusega apellatsioonikaebuse rahuldamata ja Tallinna Halduskohtu otsuse muutmata. Mh leidis ringkonnakohus, et isikutele makstud tasude väljastamata jätmise asemel tulnuks vallal jätta avaliku teabe seaduse § 4 lg 3 ja § 36 lg 1 p 9 alusel väljastamata hoopis isikute nimed.

Me ei nõustunud ringkonnakohtu lahendiga ning esitasime kassatsioonikaebuse. Kassatsioonikaebuses märkisime mh, et kui isik on töösuhtes avaliku sektori asutusega, on ta suurema avalikkuse tähelepanu ja kontrolli all. Avalikkusel on õigus teada, mille eest ja kellele avaliku raha arvel preemiaid makstakse. Samuti ei näita ühekordne preemia või muutuvpalga maksmine kuidagi isikute tegelikke sissetulekuid ega majanduslikku seisu või olukorda, mis võiks oluliselt kellegi eraelu riivata. Juurdepääsupiirangu korral tuleb ennekõike kinni katta isikuandmed, mille kaudu on otseselt või kaudselt võimalik tuvastada eelarvest makstud tasude ja hüvitiste saaja. Ringkonnakohus ei ole esitanud põhjendusi kõigi apellatsioonkaebuse väidete kohta, nt ei võetud seisukohta, mis oleks praegusel juhul väljastamata jäetud teabe puhul juurdepääsupiirangu aluseks.

Riigikohus rahuldas kassatsioonikaebuse ning tühistas halduskohtu ja ringkonnakohtu otsused. Otsuse punktis 12 on märgitud „Kolleegiumi hinnangul ei ole seadusandja seisukoht töötasude avalikkuse kohta üheselt tuvastatav AvTS-i, PalS-i ja ATS-i eelnõude menetlemise materjalidest. Lisaks on eri aegadel olnud erinevaid lähenemisi, kelle töötasu on avalik.“ Samas punktis toodi ka välja mõningad näiteid, kuidas aja jooksul on terminid „ametiisik“ ja „töötaja“ ning erinevad tõlgendusviisid ei anna ka selget vastust vaidlusaluse küsimuse kohta. Siiski leiti, et töötaja töötasu ei tule aktiivselt avalikustada veebilehel, kuid see omakorda ei anna vastust olukorrale, kus teavet küsitakse teabenõude korral.

„Kolleegium leidis (otsuse punkt 20), et põhiseadus võimaldab „avaldada kohaliku omavalitsuse töötajate töötasu nii isikustatud kui ka isikustamata kujul.“

Kohtuasi nr 3-15-3228.

Kolleegium analüüsis erinevaid põhjendusi, mis toetavad ning lükkaksid ümber üksnes kohaliku omavalitsuse töötajate töötasu avaldamist teabenõude korras. Kolleegium leidis (otsuse punkt 20), et põhiseadus võimaldab „avaldada kohaliku omavalitsuse töötajate töötasu nii isikustatud kui ka isikustamata kujul. Arvestades eeltoodud argumente kogumis, tuleb AvTS-i ja TLS-i siiski tõlgendada viisil, mille järgi AvTS § 36 lg 1 p 9 on erinorm TLS § 28 lg 2 p 13 suhtes. Viidatud AvTS-i säte kohustab kohalikku omavalitsust teabenõude saamisel andma kohaliku omavalitsuse töötajale arvutatud, makstud või maksmisele kuuluva töötasu kohta andmeid isikustatud kujul ning seda sõltumata töökohast. Sellist kohustust avaldada kohaliku omavalitsuse töötajate töötasu ei väära ka AvTS-i eraelu puutumatust kaitsvad normid (nt AvTS § 4 lg 3, § 35 lg 1 p 12). Kohustus teabenõude korras töötasu kohta teavet väljastada ei tähenda teabe aktiivset avalikustamiskohustust.“

Tuleb ära märkida, et eeltoodu seisukoht on kohtuotsuse kohaselt seotud ainult olukorraga, kus toimub kohaliku omavalitsuse töötajate töötasu avaldamine teabenõude korras.

Eraõiguslik juriidiline isik teabevaldajana

Järgnevas kohtuasja selgitatakse, millisest seadusest lähtudes tuleb sisustada juriidilise isiku mõistet, kui tegemist on eraõiguslikust juriidilisest isikust teabevaldajaga.

Nelja Energia AS esitas Eesti Energia AS-le 20.04.2017 teabenõude, mis sisaldas mh ka soovi saada: koopia Tootsi tuulepargi võrguga liitmiseks Eesti Energia ja Elering AS vahel sõlmitud liitumislepingust; ning koopiad kuludokumentidest, mis kajastavad Eesti Energia poolt seoses Tootsi tuulepargi arendamisega kantud kulutusi ja nende suurust. Kuna seda teavet ei väljastatud, siis esitas Nelja Energia Eesti Energia tegevuse peale vaide.

Vaideotsusega nr 2.1-3/17/1036 jätsime vaide rahuldamata, kuna leidsime, et soovitud dokumendid ei puuduta avalike ülesannete täitmist ega eelarvevahendite kasutamist ehk Eesti Energia ei olnud soovitud teabe osas teabevaldaja avaliku teabe seaduse mõistes.

Nelja Energia sellega ei nõustunud, mistõttu kandus see vaidlus halduskohtusse. Nelja Energia leidis, et Eesti Energiale on pandud elutähtsa teenuse osutamise kohustused, kuna väidetavalt on tema elektrijaama netovõimsus suurem kui 200 MW, mis muudaks ka elutähtsa teenuse osutajaks. Olgu märgitud, et kui eraõiguslik juriidiline isik on elutähtsa teenuse osutaja, siis ta on ka avaliku ülesande täitja ning ta on teabevaldaja ainult selle ülesande täitmisega seotud

teabe osas. Tegelikkuses kuulusid kõnealused elektrijaamad Eesti Energia tütarettevõtetele Enefit Energiatootmine AS ning Eesti Energial endal puudusid elektrijaamad, millede netovõimsus on suurem kui 200 MW.

Nelja Energia oli seisukohal, et eraõiguslikust juriidilisest isikust teabevaldaja määratlemise puhul ei oma tähendust asjaolu, et elektritootmise varud ei kuulu Eesti Energiale vaid tema tütarettevõttele, kuna need tootmisvarad on Eesti Energia kontrolli all. Samuti leidis ta, et Eesti Energia on teabevaldaja ka teabe osas, mis on tema tütarettevõtete valduses. Nelja Energia leidis, et konkurentsiseaduse § 2 lg 3 kohaselt loetakse Eesti Energia AS ja Enefit Energiatootmine AS üheks ettevõtjaks. Raamatupidamise seaduse kohaselt moodustavad need äriühingud konsolideerimisgrupi.

„AvTS §-s 5 sätestatud eraõigusliku teabevaldaja mõiste sisustamisel on asjakohane lähtuda ÄS § 2 lg-s 1 sätestatud äriühingu mõistest."

Kohtuasi nr 3-17-1514.

Kohtus esitasime seisukohad, et avaliku teabe seaduse § 9 lg 1 kohaselt on teabevaldaja kohustatud võimaldama juurdepääsu tema valduses olevale teabele seaduses sätestatud korras. Seega ei saa teabenõude korras nõuda dokumente, mis asuvad teise juriidilise isiku, sh tütarettevõtte, valduses. Kui mõni Eesti Energia AS-i tütarettevõtetest täidab avalikke ülesandeid, on teabevaldajaks konkreetne tütarettevõte kui eraldiseisev juriidiline isik. Avaliku teabe seadus ei võimalda ettevõtja määratlemisel lähtuda konkurentsiseaduse § 2 lg-st 3. Äriühingu mõiste sisustamisel tuleb lähtuda äriseadustikust. Asjakohatu on viidata raamatupidamise seadusele, kuna see ei reguleeri teabenõuetele vastamist.

Tallinna Halduskohus nõustus meiega ning leidis, et Nelja Energia kaebust ei rahuldata – tema puhul pole tegemist elutähtsa teenuse osutajaga ning talle pole mh üle antud sedasorti avalikku ülesannet, mille tulemusena oleks pidanud soovitud teabe väljastama. Kohus märkis mh: „Eesti Energia AS ei saa olla teabevaldajaks andmete osas, mille on saanud või mida valdavad tema tütarettevõtted. Tütarettevõtete näol on tegemist eraldiseisvate juriidiliste isikutega, kellel on eraldiseisvad kohustused, sh AvTS-st tulenevad kohustused. Kuna eraõiguslikule juriidilisele isikule AvTS-st tulenevad kohustused on

piiratud teabega, mis saadakse avaliku ülesande täitmisel või avalikke vahendeid kasutades, tuleb ka äriühingu mõistet sisustada lähtudes ÄS-st, mitte KonkS-st või RPS-st. Kaebaja laiendav tõlgendus tähendaks, et Eesti Energia AS peaks avalikustama kõik elektrienergia tootmise ja müügiga seotud dokumendid, sh lepingud, mis ei oleks aga AvTS mõttega kooskõlas."

Nelja Energia esitas kohtuotsuse peale apellatsiooni, kuid ka ringkonnakohus leidis, et halduskohtu otsus on õige. Täiendavalt märkis ringkonnakohus järgnevat (otsuse punkt 18):

„AvTS §-s 5 sätestatud eraõigusliku teabevaldaja mõiste sisustamisel on asjakohane lähtuda ÄS § 2 lg-s 1 sätestatud äriühingu mõistest. Kuigi KonkS § 2 lg 3 järgi võib Eesti Energia AS-i ja elektrijaamade omaniku Enefit Energiatootmine AS-i lugeda üheks ettevõtjaks, on ettevõtja tavamõistest erinev sisustamine põhjendatud, lähtuvalt KonkS eesmärgist reguleerida vaba ettevõtluse huvidest lähtuva konkurentsi kaitsmist ja ära hoida konkurentsi kahjustamist (KonkS § 1 lg 1). RPS §-de 27 ja 28 alusel moodustavad Eesti Energia AS ja Enefit Energiatootmine AS ka konsolideerimisgrupi, mis koostab ühise majandusaasta aruande, kuid selle eesmärk on tagada rahvusvahelistest põhimõtetest lähtuva raamatupidamise ja finantsaruandluse korraldamine (RPS § 1). AvTS eesmärk on tagada üldiseks kasutamiseks mõeldud teabele avalikkuse ja igaühe juurdepääsu võimalus ning luua võimalused avalikkuse kontrolliks avalike ülesannete täitmise üle (AvTS § 1 lg 1). Selle eesmärgi täitmiseks ei ole äriühingu tavamõistest laiem sisustamine vajalik ega põhjendatud, sest nii ema- kui ka tütarettevõtjaks olevad äriühingud eraldi võetuna saavad olla AvTS-s ettenähtud tingimustel teabevaldajad."

Vangistusseadusest tulenev kohustuslik kohtueelne menetlus

Üks kinnipeetav esitas vanglale teabenõude, millega soovis erinevaid dokumente. Vangla keeldus dokumente väljastamast, kuna tegemist oli kolmandatele isikutele koostatud vastustega, milledele oli sätestatud juurdepääsupiirang avaliku teabe seaduse § 35 lg 1 punkti 12 alusel. Vaideotsusega nr 2.1.-3/17/1764 leidsime, et vaie jääb rahuldamata. Vaides juhtisime ka vaide esitaja tähelepanu asjaolule, et vangistusseaduse § 1^1 lg 5 kohaselt peab „kinnipeetav enne kohustamisnõude esitamist olema eelnevalt esitanud vangla keeldumisele mingit toimingut teha (antud juhul teabenõude täimisest keeldumine) vaide vanglateenistusele või Justiitsministeeriumile ning vanglateenistus või Justiitsministeerium peab olema vaide tagastanud, osaliselt rahuldanud, rahuldamata või tähtaegselt lahendamata jätnud. Asja materjalidest

nähtub, et vaide esitaja ei ole esitanud vanglale vastavasisulist vaiet [haldusmenetluse seaduses] sätestatud tingimustel ja korras.“

Kinnipeetav sellega ei nõustunud ning esitas kaebuse halduskohtusse ning soovis mh vaideotsuse tühistamist ning kohustada vanglat täitma esitatud teabenõuet. Tallinna Halduskohus tagastas määrusega esitatud kaebuse kohustamisnõudes kohustusliku kohtueelse menetluse läbimata jätmise tõttu ning ülejäänud nõuete osas kaebeõiguse puudumise tõttu. Kinnipeetav ei olnud ka sellega nõus ning esitas apellatsiooni Tartu ringkonnakohtusse, kuid ringkonnakohus jättis määruskaebuse rahuldamata. Ringkonnakohus täiendas halduskohtu määruse põhjendusi enda määruse põhjendustega.

Ringkonnakohtu lahendis on halduskohtu põhjenduste osas mh märgitud: „Halduskohus märkis, et tal ei ole iseenesest põhjust kahelda kaebaja poolt nõutud dokumentidele vangla poolt seatud juurdepääsupiirangu õigsuses, kuid samas ei ole halduskohtul õigust seda ka käesolevas asjas sisuliselt kontrollida, sest kaebaja ei ole läbinud VangS-st tulenevat kohustuslikku kohtueelset menetlust. Asjaolu, et kaebaja otsustas pöörduda vaidega AKI poole, oli kaebaja valik ja lubatav AvTS kohaselt, kuid kinnipeetavast kaebajana kohaldub kaebaja suhtes vangistusseadusest tulenev eriregulatsioon kohustusliku kohtueelse menetluse näol. Kinnipeetava poolt vabatahtlikku vaidemenetluse läbimist ei saa lugeda täidetud eelduseks kohustamiskaebusega kohtusse pöördumiseks.“.

„Kui kinnipeetav soovib vaidlustada vangla tegevust teabenõude täitmisega seonduvalt, peab ta esitama vaide vangistusseaduse kohaselt vanglale.“

Ringkonnakohus on enda põhjenduste osas mh märkinud järgnevat: „Ringkonnakohus nõustub halduskohtu vaidlustatud määruse põhjendava osa p-des 9 ja 13 välja tooduga, et kohustamisnõude osas (kohustada Tallinna Vanglat täitma 13.08.2017. a teabenõuet) on kaebajal läbimata VangS § 1^1 lg-st 5 tulenev kohustuslik kohtueelne kord, mistõttu kohustamisnõude osas tuleb kaebus tagastada HKMS § 121 lg 1 p 4 alusel (kuigi konkreetselt sellele sättele halduskohus oma määruses ei viita). Sellele, et AKI menetlust ei saa samastada VangS § 1^1 lg-s 5 nõutud kohustusliku kohtueelse menetlusega ja asjaolule, et kui kinnipeetav ei ole vangla keeldumise, s.h teabenõude täitmisest keeldumise, peale esitanud vaiet vanglateenistusele, puudub tal alus halduskohtusse kohustamiskaebusega pöördumiseks, viitas ringkonnakohus ka oma varasemas määruses haldusasjas nr 3-17-1781.“.

Seega, kui kinnipeetav soovib vaidlustada vangla tegevust teabenõude täitmisega seonduvalt, peab ta esitama vaide vangistusseaduse kohaselt vanglale – tegemist on kohustusliku kohtueelse menetlusega. Seda vaideotsust on tal võimalik vaidlustada halduskohtus, sh nõuda kohustamiskaebusega teabenõude täitmist. Kui kinnipeetav esitab oma vaide kohustusliku kohtueelse menetluse asemel Andmekaitse Inspektsioonile (mis on ka lubatav) ning inspektsioon teeb tema kahjuks vaideotsuse (jätame vaide rahuldamata), siis ei ole kinnipeetaval õigust meie vaideotsuse peale esitada halduskohtusse kohustamiskaebust teabenõude täitmiseks.

Raavo Palu

õigusdirektor

RAHVUSVAHELINE KOOSTÖÖ OLI TOIMEKAS

Aasta 2018 oli andmekaitse järelevalveasutuste töös murranguline aasta. Isikuandmete kaitse üldmäärus tõi kaasa mitmeid olulisi muudatusi nii igapäevases töös kui menetlusprotseduurides. Esmalt käsitleme koostööd Euroopa institutsioonide ja andmekaitseasutustega.

MURRANGULINE AASTA ÜLEPIIRILISES KOOSTÖÖS

Minnes ajas tagasi, siis Euroopa Liidu liikmesriikide ja lisaks ka Euroopa Majanduspiirkonna riikide andmekaitseasutused on aastaid teinud tihedat koostööd. Andmekaitsedirektiivi 95/46/EÜ alusel oli loodud juba paar aastakümmet tagasi andmekaitseasutuste töögrupp, mille ametlikuks liikmeks on olnud ka Andmekaitse Inspektsioon alates 2004. aastast. Seda töögruppi tunti nime all „Artikkel 29 töögrupp“. Töögrupp kohtus regulaarselt ning selles osalemine ja ka töögrupi alagruppides osalemine oli osa inspektsiooni igapäevasest tööst. Peamisteks ülesanneteks oli ühiselt välja anda suuniseid ja arvamusi erinevates andmekaitset puudutavates küsimustes.

Euroopa Andmekaitsenõukogu laiendas tegevust

Isikuandmete kaitse üldmäärus tegi muutusi töögrupis ning liikmesriikide järelevalveasutustest ja Euroopa Andmekaitseinspektorist moodustati uus organ – Euroopa Andmekaitsenõukogu, mis küll jätkab eelkäija tegevust anda välja suuniseid ja arvamusi, kuid lisaks sellele tegeletakse näiteks andmekaitseasutuste vaheliste vaidluste lahendamise ning järjepidevuse mehhanismiga.

Järjepidevuse mehhanismi näitena on vaja teatud teemades liikmesriigi järelevalveasutusel saada otsuse vastu võtmiseks Euroopa Andmekaitsenõukogu arvamust. Näiteks kui liikmeriigi järelevalveasutus tahab taotluse alusel aktsepteerida toimimisjuhised või väljastada luba sertifitseerimiseks isikule, kes

töötleb andmeid piiriüleselt, näeb protseduur enne loa väljastamist ette arvamuse küsimist Euroopa Andmekaitsenõukogult.

Lisaks eelnevale teevad Euroopa Liidu andmekaitse järelevalveasutused omavahel menetlusalast koostööd. Näiteks, kui Andmekaitse Inspektsioonile esitatakse Eesti elanikult kaebus mõne väljaspool Eestit asuva andmetöötleja peale, siis juhtumi lahendamist alustatakse sellest, et kaebuse saanud Andmekaitse Inspektsioon võtab ühendust vastava riigi järelevalveasutusega, kus asub andmetöötleja, kelle tegevuse peale on kaevatud. Seejärel tuleb määratleda, kes on juhtiv järelevalveasutus ning millised riigid on veel kaasatud ning lõpuks, kes kaebust menetleb. Alles siis hakkab reaalne juhtumi menetlemine pihta. Kui järelevalveasutus on kaebuse osas otsust tegemas, siis otsuse eelnõu tuleb samuti kooskõlastada kõigi kaasatud järelevalveasutustega. Selliste protseduuride lihtsustamiseks on andmekaitseasutused liitunud siseturu infosüsteemiga (IMI), mis võimaldab igapäevast menetlusalast suhtlemist ja teabevahetust.

Andmekaitsenõukogu sisulise töö osas on oluline välja tuua see, et nõukogu põhiplenaari juurde on moodustatud mitmeid alagruppe, mis tegelevad valdkonniti arvamuste ja suuniste välja töötamisega, mis võetakse Andmekaitsenõukogus vastu. Andmekaitse Inspektsioon on võtnud Andmekaitsenõukogu töös oma prioriteediks osalemise nii strateegilise nõustamise, tehnoloogia, koostöö, menetlustöö kui trahvimise alagruppide kohapealses töös. Kuid lisaks oleme aktiivsed ka võtmeküsimuste, finants, sotsiaalmeedia ja andmete edastamise alagrupis. Allpool on toodud ainult mõningate nendes alagruppides arutatud teemad ja tegevused.

„Ülepiirilise koostöö olulisemaiks saavutuseks ja seda ühtlasi järjepidevuse mehhanismi protseduuride täideviimise osas võib pidada Eesti algatust ülepiiriliste mõjuhinnangute nimekirjade koostamiseks.“

Andmekaitsenõukogu andis 2018. aastal välja hulk arvamusi ja suuniseid, mis on (osaliselt eesti keelde tõlgituna) saadaval nõukogu kodulehel https://edpb.europa.eu/. Aasta teises pooles avalikustati arvamused sertifitseerimise ja andmete edastamise osas kolmandatesse riikidesse artikkel 49 alusel. Lisaks kinnitas nõukogu isikuandmete kaitse üldmääruse jõustumisega seonduvad juhendmaterjalid, mis küll koostati juba varasemalt

Artikkel 29 töögrupi nimel. Nende hulgast väärib esile toomist nõusoleku ja läbipaistvuse juhend, profileerimise juhend, rikkumisteadete juhend, andmekaitsespetsialisti juhend, andmete ülekantavuse juhend jne. Materjalid töötati välja abimaterjalina andmetöötlejatele ja seda oma tegevuse vastavusse viimisel isikuandmete kaitse üldmäärusega. Juhendid osutusid heaks alusmaterjaliks inspektsiooni koostatud isikuandmete töötleja üldjuhendi koostamisel.

Ülepiirilise koostöö olulisemaiks saavutuseks ja seda ühtlasi järjepidevuse mehhanismi protseduuride täideviimise osas võib pidada Eesti algatust ülepiiriliste mõjuhinnangute nimekirjade koostamiseks.

Maarja Kirss

koostöödirektor

ÜLEVAADE OSALEMISEST RAHVUSVAHELISTES TÖÖRÜHMADES

Osalemine telekommunikatsioonialases andmekaitse töörühmas

Telekommunikatsioonialane rahvusvaheline andmekaitse töörühm kohtub aastas kaks korda.

2018 kevadiselt töörühma kohtumiselt väärib märkimist vastu võetud dokumenti *Working Paper on Connected Vehicles*.[11]

Kaasaegsed sõiduvahendid on juba täna varustatud erinevate telemaatikaseadmete ja sensoritega. Määrata saab sõiduki asukohta, vaadata distantsilt sõiduki tehnilisi andmeid kuni varguse korral sõiduk sõidukõlbmatuks muutmisel. Ühelt poolt võimaldab kasutatav tehnoloogia tõsta juhtimise turvalisust ja parandada sõidukvaliteeti. Teisalt aga toimub juhi käitumise ja sõiduharjumuse jälgimine läbi kogutavate andmete. Kui juhi isik ja andmed on võimalik kokku panna, on tegemist isikuandmete töötlemisega.

Dokumendis analüüsitakse erinevaid juhtusid, milliste andmete kogumine sõidukis toimub, kus ja kuidas neid andmeid salvestatakse ning kellele edastatakse. Samuti millised sõiduki juhte puudutavad privaatsusriskid võivad sellega kaasneda. Antakse soovitusi sõiduvahendite tootjatele, teenusepakkujatele, standardiorganisatsioonidele, seaduse loojatele, kuidas üleskerkivaid andmekaitselisi riske tõhusalt hallata.

Lisaks on töörühmas valmimas privaatsusriskide analüüsid koos rakendussoovitustega masinõppe, veebijälgimise, blokiahela ning lastele suunatud nutikate mänguasjade osas. Dokumentide avaldamist on oodata 2019 aastal.

Osalemine Euroopa Andmekaitsenõukogu tehnoloogia alagrupis

Artikkel 29 töögrupi õigusjärglase Euroopa Andmekaitsenõukogu mandaadi alusel jätkasid tööd senised valdkonnapõhised alagrupid.

Tehnoloogia alagrupis möödunud aasta põhitähelepanu läks isikuandmete kaitse üldmääruse rakendusjuhiste koostamisele. Valmisid juhendid, mis käsitlevad isikuandmetega seotud rikkumisi, andmetöötlejate sertifitseerimist ning sertifitseerimisettevõtete akrediteerimist.

[11] https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper

Töös on ning 2019 aastal valmivad abistavad materjalid videojälgimise, vaikimisi- ning lõimitud andmekaitse, blokiahela ning nutisõidukite osas.

Samuti valmistas alagrupp ette lähtekohad liikmesriikide kohustusele koostada ning esitada Andmekaitsenõukogule arvamuse andmiseks nimekirjad nendest piiriülestest andmetöötlustoimingutest, mis nõuavad andmekaitselist mõjude hindamist. Et tegu oli esmakogemusega nõukogu tasemel selliste otsuste tegemisel, oli teekond konarlik ja tuliseid vaidlusi tekitav. Sellele vaatamata on valdav osa andmekaitseasutusi oma nimekirjad esitanud ja tänaseks ka andmekaitsenõukogu otsuse saanud.[12]

Osalemine Euroopa Andmekaitsenõukogu võtmesätete alagrupis

Mitmete selle alagrupiga seotud juhendite loomisele eelnenud tegevus algas juba enne 2018. aastat. Paljud juhenditest võeti esmakordselt vastu 2017. aastal, mille järel esitati need avalikule konsultatsioonile. Avaliku konsultatsiooni järel tegeleti saadud tagasiside läbi töötamisega ning lõpptulemusena lõplikult kinnitati mitmed suunised 2018. aastal. Materjalid on kättesaadavad meie võrgulehelt.[13]

Eelmisel aastal tegeles alagrupp konkreetselt allolevate teemadega:

- Suunised automatiseeritud töötlusel põhinevate üksikotsuste tegemise ja profiilianalüüsi kohta (vastu võetud ning esitatud avalikule konsultatsioonile 03.10.2017; lõplikult muudetud ja kinnitatud 06.02.2018).
- Suunised määruse (EL) 2016/679 kohase nõusoleku kohta (vastu võetud ning esitatud avalikule konsultatsioonile 28.11.2017, lõplikult muudetud ning kinnitatud 10.04.2018).
- Suunised määruse 2016/679 kohase läbipaistvuse kohta (vastu võetud ning esitatud avalikule konsultatsioonile 29.11.2017, lõplikult muudetud ning kinnitatud 11.04.2018).
- Valmistati ette suunist isikuandmete kaitse üldmääruse artikkel 3 ehk territoriaalse kohaldamisala kohta.
- Valmistati ette suunist isikuandmete kaitse üldmääruse artikkel 6 lg 1 punkti b kohta *online* teenuste kontekstis.
- Valmistati ette seisukoht isikuandmete kaitse üldmääruse art 30 lõike 5 osas.

[12] Otsused leitavad: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

[13] https://www.aki.ee/et/andmekaitse-reform/juhendmaterjalid.

Osalemine Euroopa Andmekaitsenõukogu piiride, reisijate ja korrakaitse alagrupis

2018. aastal tegeleti aruteludega, kuidas hakkab edaspidiselt toimima järelevalve ja koostöö alagrupiga seotud valdkonna teemades, arvestades asjaolu, et teatav osa ühisest järelevalvest justiits- ja sisevaldkonnaga (JHA) seotud andmetöötlustest läheb Euroopa Andmekaitsenõukogu juurde. Alagrupis tegeleti aga ka nende teemadega:

- Eraelukaitse Kilbi andmekaitseraamistiku üle vaatamine.
- Jaapani andmekaitselise adekvaatsusotsuse ettevalmistamine õiguskaitsega seotud aspektide osas.
- Arvamus Euroopa Komisjoni välja pakutud e-tõendite (e-evidence) regulatsioonile.

Järelevalvekoostöö Euroopa piiriüleste infosüsteemide alal

Osaleme mitmes järelevalvealases koostöös, mis on ennekõike seotud riikidevaheliste infosüsteemide pidamisega. Koostöö ning andmekaitse järelevalves kasutatava teabe ühtlustamiseks on Euroopa Andmekaitseinspektori juurde loodud järelevalve koordinatsiooni töögrupid (SCG), mis koosnevad liikmesriikide ning Euroopa Andmekaitseinspektori esindajatest. Nimetatud töögrupid on loodud Schengeni infosüsteemi, Viisa infosüsteemi, Eurodaci infosüsteemi ning Tolliinfosüsteemiga seonduvalt. Ka Europoliga seotud järelevalve jaoks on loodud eraldi koostöönõukogu. Töörühmade ja koostöövormide ühisnimetajaks võib pidada õigustavade ühtlustamist. Kui infosüsteemi kesksüsteemi osas teostab järelevalvet Euroopa Andmekaitseinspektor, siis meie teostame järelevalvet siseriikliku osas ehk me kontrollime, kas nende infosüsteemide siseriiklik kasutamine toimub isikute õigusi rikkumata.

Schengeni infosüsteemiga seotud järelevalve

Teise põlvkonna Schengeni infosüsteem (SIS II) on suuremahuline andmebaas, mis sisaldab informatsiooni tagaotsitavate või kadunud isikute kohta, salajase jälgimise all olevate isikute kohta, kolmandate riikide kodanike kohta, kellele on Schengeni territooriumile sisenemine keelatud, samuti andmeid varastatud või kadunud sõidukite, kadunud dokumentide, sõidukite registreerimistunnistuste ja numbrimärkide kohta. Andmebaasi peamiseks eesmärgiks on tagada turvalisus Schengeni alal, kus sisepiiridel puudub piirikontroll. Seda kompenseeritakse

pädevate piirivalve- ja politseiasutuste infovahetusega Schengeni infosüsteemi kaudu.

2018. aastal kohtus ühine töögrupp kaks korda ning tegeleti järgmiste teemadega:

- Võeti vastu raport logimise kohta SIS II kohta liikmesriikide tasandil.[14]
- Võeti koos Viisa infosüsteemi ja Eurodaci infosüsteemi järelevalve koordinatsiooni töögruppidega koos vastu kiri Euroopa Komisjoni ettepanekule, mille sisuks oli EL-i suuremahuliste infosüsteemide ristkasutuse/ühendamine.[15]
- Võeti vastu töögrupi tegevusraporti aastate 2016-2017 kohta.[16]
- Tegeleti 2019-2021 tööprogrammi koostamisega ja suuniste ülevaatamisega, mis selgitavad inimeste õigusi, kui neil on soov saada juurdepääs enda isikuandmetele Schengeni infosüsteemis.

Viisa infosüsteemiga seotud järelevalve

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

2018. aastal kohtus ühine töögrupp kaks korda ning tegeleti järgmiste teemadega:

- Võeti vastu VIS määruse artikkel 41 rakendamisega seotud raporti (seotud andmekaitseasutuste teostavate auditite ga liikmesriikides).
- Võeti vastu raport, milles analüüsiti väliste teenuse osutajatele kehtivaid andmekaitsenorme.
- Tegeleti 2019-2021 tööprogrammi koostamise ettevalmistamisega.
- Arutati Euroopa Komisjoni ettepanekut, mis muudab VIS-i tegevust reguleerivat Euroopa Parlamendi määrust.

Euroopa sõrmejälgede andmebaasi (Eurodac) järelevalve

Euroopa varjupaigataotlejate tuvastamise infosüsteem Eurodac on loodud varjupaigataotlejate ja ebaseaduslike immigrantide teatud rühmade

[14] Leitav: https://edps.europa.eu/sites/edp/files/publication/18-06-12_sis_report_national_level_en.pdf.

[15] Leitav: https://edps.europa.eu/sites/edp/files/publication/18-06-22_letter_on_interoperability_scgs_ep_en.pdf.

[16] Tegevusraport on leitav: https://edps.europa.eu/sites/edp/files/publication/19-01-09_sis_ii_scg_activity_report_2016-2017_final_en.pdf.

sõrmejälgede võrdlemiseks ning on kasutusel kõigis Euroopa Liidu liikmesriikides ja seotud kolmandates riikides.

2018. aastal kohtus ühine töögrupp kaks korda ning tegeleti järgmiste teemadega:

- Võeti vastu töögrupi tegevusraporti aastate 2016-2017 kohta.[17]
- Tegeleti raportiga, milles analüüsiti inimese õigusi seoses Eurodaci infosüsteemiga – sellega seotud tegevused liikusid 2019. aastasse.
- Tegeleti 2019-2021 tööprogrammi koostamise ettevalmistamisega.
- Arutati Euroopa Komisjoni ettepanekut, mis muudab Eurodaci tegevust reguleerivat Euroopa Parlamendi määrust.

Tollikonventsiooni andmekaitse järelevalve

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

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

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

2018. aastal kohtus see töörühm kaks korda ning tegeleti mh järgmiste teemadega:

---

[17] Leitav: https://edps.europa.eu/sites/edp/files/publication/19-01-07_eurodac_supervision_coordination_group_activity_report_2016-2017_en.pdf.

- Võeti vastu töörühma tegevusraport aastate 2016-2017 kohta.
- Võeti vastu ühine järelevalvemetoodika järelevalveasutustele CIS-i järelevalve osas.
- Tegeleti varasemalt vastu võetud CIS-i juurdepääsu juhendi uuendamise ettevalmistamisega.

Europoli määrusega seotud järelevalve

Europoli määruse (Euroopa Parlamendi ja Nõukogu määrus nr 2016/794) kohaselt teostab Europoli osas järelevalvet Euroopa Andmekaitseinspektor, kuid liikmesriikides asuvate Europoli riiklikes üksustes toimuva isikuandmete töötlemise osas teostavad järelevalvet liikmesriikide andmekaitselised järelevalveasutused. 2017. aastal moodustati Europoli määruse alusel andmekaitseasutustest ning Euroopa Andmekaitseinspektori esindajast koostöönõukogu (Europol Cooperation Board), mille ülesandeks on arutada Europoli üle andmekaitsealase järelevalve teostamise üldpõhimõtteid ja strateegiat ning liikmesriikide poolt Europolile isikuandmete edastamise, nendest väljavõtete tegemise ja nendest teatamise lubatavust.

2018. aastal toimus kaks koostöönõukogu kohtumist, kus mh arutati koostöönõukogu tööprogrammi aastateks 2018-2020. See tööprogramm sisaldab peamiselt koostöönõukogu eelkäija, Europoli ühise järelevalveasutuse (Europol Joint Supervisory Body), töö jätkamist ning selle varasemate tegevuste ja seisukohtade üle vaatamist ning uuendamist. Näiteks uuendatakse „tunne oma õigusi“ infolehte, mis selgitab Europolis toimuvat isikuandmete töötlemist ning tegeleti selgituste koostamisega, mis selgitavad, kuidas inimene saaks tutvuda enda isikuandmetega, mis asuvad Europolis.

GPEN

2018. aasta juunis toimus Tel Avivis teine Üleilmse Eraelu Kaitse Võrgustikuga ehk GPEN-ga (*Global Privacy Enforcement Network*) seotud praktikute töötuba. Töötoa teemaks oli „Praktilised lahendused järelevalveks globaalselt digitaalses maailmas“. Töötoas osales üle 40 menetleja Põhja-Ameerikast, Euroopast, Aasiast, Aafrikast ning Austraaliast, kes tegelevad eraelu kaitse ning muudest sektoritest. Andmekaitse Inspektsiooni esindaja osales ka selles töötoas.

2018. aasta septembris toimus GPEN-i seire teemal vastutus eraelu puutumatuse eest. Seires uuriti, kuidas andmetöötlejad on enda sisemistesse protseduuridesse ning andmetöötluse tingimustesse eraelu kaitse aspektid sisustanud. Tulemustest selgus, et kuigi andmetöötlejad on nõuetest teadlikud, esineb üsna

palju puudusi teadmiste praktiseerimisel. Tegemist on kuuenda privaatsusõigusega seotud seirega, mis on GPEN-i eestvedamisel läbi viidud.

Inspektsioon on osaline GPEN-i töös, kuid möödunud aastal ei olnud meil võimalik seires osaleda. Möödunud aasta kohta tehtud seire tulemused on leitavad GPEN-i võrgulehelt.[18]

[18] GPEN-i pressiteade: https://www.privacyenforcement.net/content/gpen-sweep-2018-international-investigation-finds-organisations-should-be-doing-more-achieve.

STATISTIKA JA NÕUANDELIIN

AASTA 2018 ARVUDES

Tegevusnäitajad	aasta tulemus kokku	IKS/üld-määrus	ESS	AvTS
Juhised (avaldatud kodulehel)	1	1	0	0
Arvamused õigusaktide eelnõudest	42	22		20
Teavitustöö				
Selgitustaotlused, märgu- ja nõudekirjad, teabenõuded	2384	1856	305	223
Kõned valveametnikule (kogu arv sisaldab väljapoole järelevalve ala olevaid küsimusi)	2556	2117	72	212
Nõustamised	200	170	1	29
Koolitused (korraldatud või lektorina osaletud)	23	21	1	1
Järelevalvetöö				
Ringkirjad (ilma järelevalvet algatamata)	8	6	0	2
sh ringkirjade adressaate	162	0	0	0
Võrdlevad seired	2	1	0	1
sh seiratute arv	85	6	0	79
Vaided, kaebused, väärteoteated (esitatud)	462	274	17	171
Kaubused, selgitustaotlused, rikkumisteated, märgukirjad, loa ja teavitusmenetlus IMI* kaudu	479	0	0	0
Omaalgatuslikud järelevalved (lõpetatud)	15	8	0	7
sh ennetavad andmekaitseauditid	1			
Kontrollkäigud (järelevalves)	17	10	0	7
Soovitused ja ettepanekud (järelevalves)	10	3	0	7
Ettekirjutused	46	9	1	36
sh registreerimiskohustuse ettekirjutused				
Väärteomenetlused (lõpetatud)	23	20	0	3
Sunnirahad ja trahvid (määratud)	9	8	0	1
Loa- ja erimenetlused				
Registreerimismenetlused (esitatud taotlused)	192			
Andmekogude kooskõlastusmenetlused RIHA-s	36			
Loataotlused teadusuuringuks andmesubjekti nõusolekuta	61			
Loataotlused isikuandmete edastamiseks ebapiisava andmekaitsetasemega riikidesse	3			
Taotlused iseenda andmete suhtes Schengeni, Europoli jt piiriülestes andmekogudes	21			
Rikkumisteated	64			
Osavõtt rahvusvahelistest töökohtumistest (kohtumiste loetelu, lähetuskäsk	23			

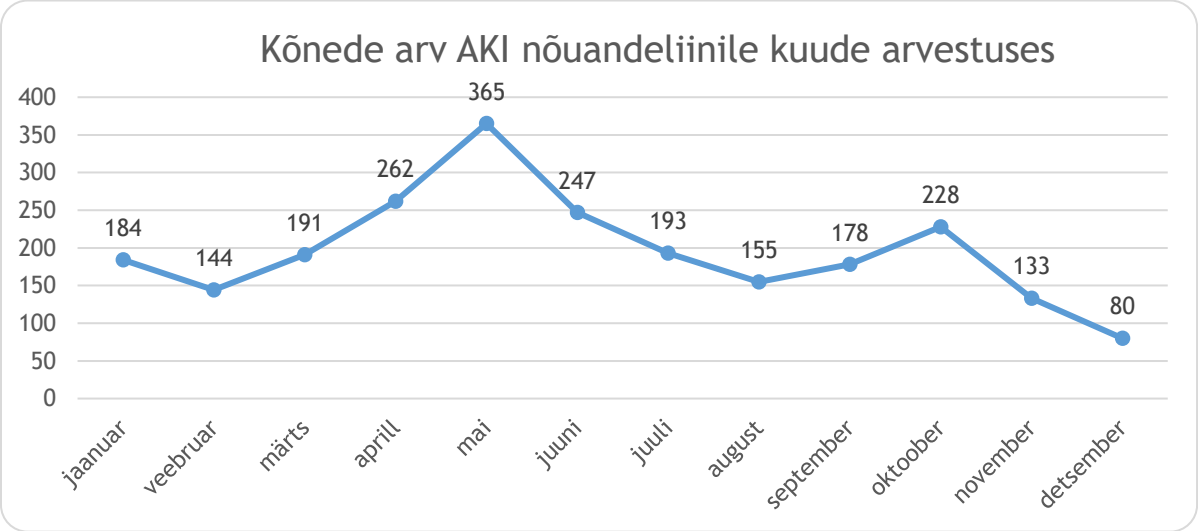
*IMI on Euroopa Liidu siseturu infosüsteem, mille kaudu vahetavad andmekaitseasutused infot ning mille kaudu esitakse kaebusi, selgitustaotlusi, rikkumisteateid ja märgukirju.

KÕNEDE ARV KASVAS MÄRGATAVALT

82% kõnedest, mis infoliinile tehakse puudutavad isikuandmete kaitse seadust ning isikuandmete kaitse üldmäärust.

Keskmiselt tehti 2018. aastal päevas ligikaudu 10 kõnet. Võrreldes varasemate perioodidega oli kõnede arvu kasv märgatav, sest eelnevatel aastatel on olnud keskmine 5 kuni 6 kõnet päevas.

Kõige rohkem tehti kõnesid maikuu eelviimasel nädalal, vahetult enne isikuandmete kaitse üldmääruse kehtima hakkamist ja selle järel. Siis jõuti infoliinis vastu võtta töönädala jooksul 122 kõnet. Helistamise päevarekord on 30 kõnet päevas.



Nõuandeliinile tehtud kõnede kokkuvõte

Vahemikus 1. jaanuar kuni 31. detsember 2018. aasta helistati Andmekaitse Inspektsiooni infotelefonile 2556 korda. Üle-eelmise aasta samal perioodil tehti 1665 kõnet. Seega on aastal 2018 infotelefoni kõnede maht kasvanud 35% võrreldes aastaga 2017. Põhjuseks on loomulikult Euroopa isikuandmete kaitse üldmääruse jõustumine. Allpool anname detailsema ülevaate infoliinis esitatud valdkondadest ning küsimustest.

Enim küsiti küsimusi, mida saab liigitada isikuandmete kaitse alla käivateks – kokku 2117 kõnet. Taolised kõned moodustasid 82% kõigist infoliinile laekunud

kõnedest. Avaliku teabe seaduse kohaldamise kohta küsiti 212 korda, elektroonilise side seaduse ehk elektroonilise otseturustuse kohta 72 korda.

Muudel teemadel, mida ei olnud võimalik liigitada AKI järelevalvealasse, oli kokku 155 kõnet.

Isikuandmete kaitse seadusega seotud küsimuste hulgas olid kõige populaarsemad järgnevad valdkonnad.

1) Töösuhetega seotud küsimused – 259 kõnet (22%). Enim küsiti töökohtadel kaamerate kasutamise kohta (kokku 47 kõnet) ning asjaolu osas, kas töölt lahkudes tuleb tööandjal sulgeda töötaja tööalane e-posti aadress.
2) Andmekaitsespetsialisti määramine – 231 (20%)kõnet.
3) Andmete avalikustamine – 205 kõnet (18%). Pea kõikidel juhtudel oli mureks andmete (nime, isikukood, foto jms) avalikustamine internetis või meedias.
4) Salvestusseadmete kasutamine - 133 kõnet (11%). Küsimused kaamerate kasutamise lubatavuse kohta avalikes kohtades ning eramajade küljes.
5) Uuringute läbiviimine – 79 kõnet (7%). Küsiti isikuandmete kasutamise võimalikkust nii teadusuuringutes kui ka muudes küsitlustes.
6) Nõusoleku küsimine – 78 kõnet (7%). Seoses uue isikuandmete kaitse üldmäärusega huvitas helistajaid, mis saab vanadest nõusolekutest ning kas ja kuidas isikuandmete kaitse üldmääruse järgi küsida nõusolekuid.
7) Võlgnevused, kohtutäiturid ja inkasso – 73 kõnet (6%). Võlgnevustega seonduvate probleemide puhul küsiti enim inkasso ja kohtutäiturite poolt võlaandmete avaldamise kohta (nt kas inkasso võib tööandjat teavitada võlgnevusest).
8) Korteriühistutega seonduvate probleemide osas helistati 61 korda (5%) (põhiliselt oli mureks kaamerate kasutamine ühistu territooriumil ja ühistusisese andmevahetuse kohta);
9) Andmete edastamisega kolmandatesse riikidesse pöörduti 42 korral (5%).

Maarja Kirss

koostöödirektor