Andmekaitse Inspektsiooni ettekanne

01. jaanuar 2007-31. detsember 2007

01. aprill 2008

Tallinn

Sisukord

Sisukord 3
Peadirektori pöördumine 4
Inspektsioonist 6
Valdkonna arengud 8
Arengud Euroopa Liidus 8
Siseriiklikud arengud 11
Järelevalve isikuandmete kaitse seaduse täitmise üle 14
Kodanike teadlikkuse tõstmine 14
Delikaatsete isikuandmete töötlemise registreerimine 22
Kaebuste menetlemine 23
Kaasused 26
Kohapealse kontrolli teostamine 30
Kaasused 30
Järelevalve avaliku teabe seaduse täitmise üle 37
Kodanike teadlikkuse tõstmine 37
Kaebuste menetlemine 38
Kaasused 40
Kohtukaasuse analüüs 44
Rahvusvaheline koostöö 45
Rahvusvahelised töögrupid 45
Andmekaitse Inspektsiooni plaanid järgnevaks perioodiks 52
Kokkuvõte 53
Lisad 54

Peadirektori pöördumine

Austatud Riigikogu põhiseaduskomisjoni liikmed ja õiguskantsler,

Taas on möödunud aasta, mis on Andmekaitse Inspektsiooni jaoks olnud mitmekesine ja töörohke ning käesoleva ettekande esitame Teile andmaks ülevaadet aastal 2007 tehtust ja valdkonnas toimunust.

Möödunud aruandlusperioodil seatud tegevuseesmärgid on saavutatud ja hea meel on ka selle üle, et nii mõnigi jooksvalt kerkinud murekoht on leidnud hea lahenduse.

Kui eelmisel aastal avaldasin lootust, et peagi osutub inspektsioon registreerijast järelevalveasutuseks, siis täna saab häbi tundmata aastale tagasi vaadates tõdeda, et selles suunas on toimunud oluline areng. Eelkõige annab positiivsest arengust tunnistust omaalgatuslike järelevalvete hulga kasv.

Progress, mida numbrites ei ole otstarbekas väljendada, on inimeste teadlikkuse taseme edasiareng. See on tajutav. Teavitustöö on olnud meile tähtis ja ka tulevikus plaanime just kodanikega suhtlemisele panustada rohkelt ressursse.

Möödunud kalendriaastasse jääb liikumine Siseministeeriumi haldusalast Justiitsministeeriumi haldusalasse, mis on kõigile osapooltele tähendanud uusi ja huvitavaid väljakutseid.

Perioodi üheks olulisemaks valdkonnaarenguks saab pidada 2006. aastal valminud uute isikuandmete kaitse seaduse ja avaliku teabe seaduse redaktsioonide eelnõude jõustumist, mis eelseisvaks perioodiks tähendab Andmekaitse Inspektsiooni jaoks kahe olulise õigusakti ellurakendamist.

Täna oskame eeldada, et uue isikuandmete kaitse seaduse rakendamise juures kõige suurema osakaalu saavad tööd, mis kaasnevad meediaklausli jõustumisega ning valdkond, mis on seotud isikuandmete kaitse eest vastutava isikuga. Andmekaitse ametniku instituudi sisseviimist seadusandluses tervitame rõõmuga, sest võitjateks osutuvad kõik osapooled – asutused ja ettevõtted saavad muretsemata tegeleda oma põhitegevusega ning Andmekaitse Inspektsiooni jaoks on hea sõnum selles, et valdkonna spetsialistide tööleasumise järgselt peaks isikuandmete kaitstuse tase vaid paranema.

Iga päevaga üha enam avatud maailm on tekitanud eelnevast suurema vajaduse kokkulepete järgi. Nii on andmekaitse valdkonnas suurenenud pingutuste rakendamine selle nimel, et isikuandmete kaitsega seonduv õigusraamistik oleks kõikjal sarnane osas, kus Euroopa riikide järelevalveasutustel on pädevus kaitsta kodanike õigusi. Eesmärgiks on, et Euroopa Liidus vabaliikumise õigust teostavad kodanikud saaksid kõikjal lähtuda ühtsest õiguspärasest ootusest ja õiguskindluse põhimõttest.

Andmekaitse Inspektsiooni väiksele, aga asjalikule meeskonnale, kellega ka järgneval hooajal mägesid liigutada sooviksin, suured tänud!

Lugupidamisega,

Urmas Kukk
Andmekaitse Inspektsiooni peadirektor

Inspektsioonist

Eesti Vabariigi Põhiseadus[1] annab isikuile õigused eraelu kaitsele, infovahetuse saladusele ja andmete kaitsele. Põhiseadus keelab riigisasutustel, kohalikel omavalitsustel ja nende ametiisikutel kodaniku vaba tahte vastaselt koguda ja talletada andmeid kodaniku veendumuste kohta. Samuti sätestub, et igaühel on õigus tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele. Isiku eraelu puutumatust võib piirata vaid kohtu loal, seaduses sätestatud juhtudel ja korras, kuriteo tõkestamise või kriminaalmenetluses tõe väljaselgitamise eesmärgil.

Tulenevalt põhiseadusest on riigiasutustel, kohalikel omavalitsustel ja nende ametiisikutel kohustus anda kodanikule tema nõudel informatsiooni asutuse tegevuse kohta, välja arvatud andmed, mille väljastamine on seadusega keelatud ja andmed, mis on mõeldud eranditult asutusesiseseks kasutamiseks. Seadusega sätestatud korras on Eestis elaval isikul õigus tutvuda tema kohta riigiasutustes ja kohalikes omavalitsuses ning nende asutuste arhiivides hoitavate andmetega.

Alates 1997. aastast, mil loodi Siseministeeriumi andmekaitse osakond ja 1999. aastast, kui asutati sõltumatu järelevalveasutus Andmekaitse Inspektsioon, asuti Siseministeeriumi haldusalas. Aruandlusaasta 14. veebruaril toimus haldusala vahetus, misjärgselt asub Andmekaitse Inspektsioon Justiitsministeeriumi valitsemisalas.

Andmekaitse Inspektsioon on sõltumatu riiklik järelevalveasutus, mille töö põhieesmärkideks on isikute põhiõiguste ja vabaduste tagamine isikuandmete töötlemisel ning õiguse saada vabalt üldiseks kasutamiseks levitatavat teavet, kaitsmine.
Tulenevalt eeltoodud eesmärkidest on Andmekaitse Inspektsioonile seadustega pandud ülesanneteks teostada sõltumatut järelevalvet isikuandmete töötlemise seaduslikkuse ja andmekogude pidamise üle[2] ühelt poolt ning teabe avaldamisnõuete täitmise üle teiselt poolt.

[1] Eesti Vabariigi Põhiseadus (RTI, 28.06.2007, 43, 311). Arvutivõrgus kättesaadav: https://www.riigiteataja.ee/ert/act.jsp?id=12846827
[2] Alates 1.01.2008 teostab andmekogude pidamise seaduslikkuse üle järelevalvet Majandus- ja Kommunikatsiooniministeerium

Lisaks eelnevalt kirjeldatud ülesannetele registreerib Andmekaitse Inspektsioon delikaatsete isikuandmete töötlemisi ning kohaldab oma pädevuse piires õigusaktidest (sh isikuandmete kaitse seadusest[3] ja avaliku teabe seadusest[4]) tulenevate kohustuste rikkumise korral haldussundi või väärteomenetlust. Koos Sideametiga teostab inspektsioon järelevalvet ka infoühiskonna teenuse seaduse nõuete täitmise üle.

Käesolev ettekanne esitatakse avaliku teabe seaduse (edaspidi AvTS) järelevalve kohta seitsmendat korda ja isikuandmete kaitse seaduse (edaspidi IKS) järelevalve kohta on ettekanne järjekorras viies. Ettekanne annab ülevaate ajavahemikus 2007. aasta esimesest kvartalist kuni neljanda kvartali lõpuni asetleidnud olulisematest sündmustest, faktidest ja arengutest avaliku teabe ja isikuandmete kaitse valdkonnas.

Inspektsioonile 2007. aastal eraldatud eelarveliste vahendite suurus oli 8 597 858 krooni. Teenistujate koosseis oli inspektsioonis 31. detsembri 2007. aasta seisuga 20 ametnikku; kes töötasid 18,5 ametikohal (neist kaks ametnikku 0,5 ametikohaga).

Andmekaitse Inspektsiooni struktuur jaotub lisaks peadirektori ja peadirektori asetäitja ametikohtadele kolmeks osakonnaks: kontrolliosakond, arengu- ja analüüsiosakond ning üldosakond. Kontrolliosakond koosneb registreerimis-, menetlus- ja järelevalvetalitusest. Andmekaitse Inspektsioonis on struktuurijärgselt 30 ametikohta, milledest perioodi lõpul oli täitmata 11,5 ametikohta. Käesoleva aruande esitamise hetkeks kehtiva põhimääruse, struktuuri ja koosseisu järgselt nähakse inspektsioonis ette 23 ametnikku.

Aruandlusperioodi kolmandal kvartalil edastas Andmekaitse Inspektsioon Justiitsministeeriumile ettepaneku struktuurimuudatusteks ning perioodi neljandal kvartalil leidis struktuurimuudatus aset.

1. jaanuaril 2008. aastal jõustunud Andmekaitse Inspektsiooni põhimäärus, struktuur ja koosseis[5] sätestab aruandekohustuse järgnevalt: Tulenevalt «Isikuandmete kaitse seadusest» ja «Avaliku teabe seadusest» esitab inspektsioon oma tegevusaruanded Riigikogu põhiseaduskomisjonile ja õiguskantslerile.

[3] Isikuandmete kaitse seadus (RT I 2007, 11, 53). Arvutivõrgust kättesaadav: https://www.riigiteataja.ee/ert/act.jsp?id=12788408
[4] Avaliku teabe seadus (RT I 2006, 58, 439). Arvutivõrgust kättesaadav: https://www.riigiteataja.ee/ert/act.jsp?id=12766090
[5] Andmekaitse Inspektsiooni põhimäärus, struktuur ja koosseis (RTL 2007, 17, 266). Arvutivõrgust kättesaadav: https://www.riigiteataja.ee/ert/act.jsp?id=12891072

Valdkonna arengud

Käesolevas peatükis antakse ülevaade isikuandmete kaitse ja avaliku teabe valdkondade arengust viimase aruandeperioodi jooksul. Peatükk jaguneb kaheks, esimeses osas võetakse kokku Euroopa Liidu õigusruumiga seonduv ning teises käsitletakse kokkuvõtvalt uuendusi, millel on siseriiklik kaal.

Arengud Euroopa Liidus

Andmekaitse direktiivi 95/46/EÜ harmoniseerimine liikmesriikides

Liikmesriikides osutatakse aina suuremat tähelepanu andmesubjektide õiguste ühtsetele rakendusvõimalustele liikmesriikides ja andmetetöötlemise läbipaistvusele. See eeldab andmetöötlusnõuete ühtlustamist liikmeriikides ning tuleneb ka andmekaitsedirektiivi 95/46/EC rakendamise aruandest, mille Euroopa Komisjon kinnitas 24. veebruaril 2004. aastal. Nimetatud aruandes esinevate ebakohtade kõrvaldamiseks liikmesriikides on vastu võetud tegevuskavad, mille täitmise kohta esitatakse Euroopa Komisjonile aruandeid.

Isikuandmete töötlemise nõuete ühtlustamise vajadus on tingitud ka järjest uute üleeuroopaliste andmetöötlusvõrkude loomisest - nt siseturu infosüsteemi, tarbijakaitse infosüsteemi loomine kui ka lennureisijate isikuandmete edastamisest kolmandatesse riikidesse ja tööstusettevõtete globaliseerumisest, mille tulemusena toimub isikuandmete töötlemine üle kogu maailma.

7.03.2007 on Euroopa Komisjon teinud avalikuks teatise Euroopa Parlamendile ja Nõukogule andmekaitsedirektiivi parema rakendamise tööprogrammi järelmeetmete kohta. Komisjon on leidnud, et direktiiviga ette nähtud üldine õiguslik raamistik on üldiselt asjakohane ja tehnoloogiliselt neutraalne. Euroopa Liidus kehtivad ühtlustatud eeskirjad, mis tagavad isikuandmete kõrge kaitse taseme, on toonud kaasa märkimisväärset kasu kodanikele, ettevõtjatele ja ametiasutustele. Nendega kaitstakse üksikisikuid üldise jälgimise või põhjendamatu diskrimineerimise eest teabe alusel, mida teised tema kohta omavad. /…/ Samas teatise seisab, et Euroopa Komisjon jätkab direktiivi rakendamise jälgimist, teeb kõikide sidusrühmadega koostööd, et veelgi vähendada riikide vahelisi erinevusi, ning uurib, kas on vajadust valdkondlike

õigusaktide järele, millega kohaldada andmekaitse põhimõtteid uutele tehnoloogiatele ja mis rahuldaksid avaliku julgeoleku vajadusi.

Andmekaitse Inspektsioon on aruandeperioodil käsitlenud pea kõiki olulisemaid valdkondi, mis on tõusetunud rahvusvahelisel tasandil ja kajastanud need prioriteetidena/juhistena oma kodulehel. Ka järgmisel aruandeperioodil jätkuvad tegevused nimetatud valdkondades ja täiendavalt lisandub teemavaldkond, mis käsitleb isikuandmete töötlemist krediidiasutustes. Andmekaitse Inspektsioon jätkab olulisemate valdkondade analüüsi ja tulemuste avaldamist.

Lissaboni leping

Oluliseks arenguks Euroopa Liidu suunal tuleb pidada ka Lissaboni lepingu heakskiitmist 13. detsembril 2007. aastal. Peamine muudatus isikuandmete kaitse valdkonda tuleb seoses kodanikele antavate tagatistega, mis rakenduvad tänu Euroopa Liidu põhiõiguste harta saamisest siduvaks dokumendiks. Põhiõiguste harta Artikkel II-68 sätestab, et igaühel on õigus tema isikuandmete kaitsele ning, et selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Igaühel on õigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist. Lisades, et nende täitmist kontrollib sõltumatu asutus.

Lissaboni leppe sõlmimisega lõpetati vahetegemine kolme samba vahel ja leppe artikkel 16 sätestab lisaks igaühe õigusele isikuandmete kaitsele ka selle, et Euroopa Parlament ja Nõukogu peab kehtestama reeglid isiku õiguste kaitseks andmetöötlemisel. Seega, kui peaks loodama andmekaitse raamotsus, siis kõikides Euroopa Liidu institutsioonides ja liikmesriikide valitsusasutustes, kelle tegevus tuleneb vahetult Euroopa Liidu õigusest ja keda andmekaitse direktiiv 95/46/EU oma kohaldamisalast otsesõnu ei välista, peaks andmetöötlus hakkama toimuma samadel alustel.

Õiguskaitseasutuste vaheline isikuandmete vahetamine

Viimastel aastatel on oluliseks muutunud õiguskaitseasutuste vaheline isikuandmete vahetamise temaatika. Euroopa Nõukogu otsustega, mis käsitleb piiriülese koostöö tõhustamist ehk nn Prümi lepingut, võeti 27. mail 2005. aastal Euroopa Liidu

õigusraamistikku Belgia Kuningriigi, Saksamaa Liitvabariigi, Hispaania Kuningriigi, Prantsuse Vabariigi, Luksemburgi Suurhertsogiriigi, Madalmaade Kuningriigi ja Austria Vabariigi vahelise piiriülese koostöö tõhustamist, eelkõige seoses terrorismi-, piiriülese kuritegevuse ja ebaseadusliku rände vastast võitlust käsitleva lepingu põhielemendid.
Nimetatud lepingu rakendusmeetmete vastuvõtmise protsess on olnudki üks mahukamaid tegevusi Euroopa Liidu tasandil sise- ja justiitsküsimuste valdkonnas, lisaks Schengeni õigusruumi laienemise temaatikale. Nõukogu otsusega kehtestatakse ühtsed meetmed, mis on Prümi lepingut käsitlevas Nõukogu otsuses sätestatud koostöövormide halduslikuks ja tehniliseks rakendamiseks hädavajalikud.
Prümi konventsiooniga ühinemise eelnõu on läbinud üldise kooskõlastusringi, sh on see kooskõlastatud Justiitsministeeriumiga.

Schengeni õigusruumiga liitumine

Peamiseks läbivaks jooneks andmekaitsevaldkonnas Euroopa Liidu tasandil oli kümne liikmesriigi liitumine Schengeni õigusruumiga. Läbiti hindamismissioonid, mille tulemusena toimus 21. detsembril 2007. aastal Schengeni õigusruumi laienemine. Oluliseks eelduseks oli Schengeni uue põlvkonna infosüsteemi SIS II valmimine, millega hindamismissiooni läbinud liikmesriigid kohustusid ühinema. Raskuste tõttu SIS II valmimisel otsustas Justiits- ja Siseküsimuste nõukogu, et rakendatakse Portugali algatust SISOne4All, mis võimaldab SIS I+ kaudu integreerida liikmesriigid SIS süsteemi. Seega toimus laienemine aasta viimasel kuul.

Oktoobris 2007. aastal kuulas Brüsselis kogunenud kõigi Euroopa Liidu liikmesriikide ning Norra, Šveitsi ja Islandi esindajatest koosnev Schengeni hindamise töörühm ära ekspertgrupi aruande Eesti isikuandmete kaitse taseme kohta ning kiitis selle mööndustega heaks.
Ekspertgrupp koosnes kaheksa liikmesriigi ja Euroopa Komisjoni ekspertidest ja külastas 20.-21. märtsil ka andmekaitse taseme järelhindamiseks Justiitsministeeriumit ning Andmekaitse Inspektsiooni. Andmekaitse hindamismissiooni edukas läbimine oli oluline, sest suur osa Schengeni koostööst seisneb riikidevahelises andmete vahetamises Schengeni informatsioonisüsteemi vahendusel. Teabevahetus põhineb omakorda Eestis kehtivate isikuandmete töötlemise alastel õigusaktidel. Schengeni õigusruumiga

liitumiseks peavad andmekaitse valdkonnas esmalt olema tagatud andmekaitse järelevalveasutuse sõltumatus ning Schengeni informatsioonisüsteemis (SIS) isikuandmete töötlejate teadlikkuse tase.

On oluline, et Schengeni õigusruumiga liitumisel oleks kodanikud teadlikud oma õigustest ja nende rakendamisvõimalustest. Selleks on Euroopa Komisjon loonud ajutise töögrupi SIS teavituskampaania tarvis, kuhu on kaasatud ka Eesti andmekaitse järelevalveasutuse ametnik. Andmekaitse Inspektsioon on oma kodulehel avaldanud isikutele mõeldud dokumendi „Kodanike õigused Schengeni viisaruumiga liitumisel", mis on kättesaadavad eesti-, inglise- ja vene keeles.

Siseriiklikud arengud

Kui eelmise aruandeperioodi peamiseks valdkonna arenguks oli isikuandmete kaitse seaduse ja avaliku teabe seaduse eelnõude valmimine, siis käesoleva perioodi olulisemaks arenguks võib pidada nimetatud seaduste muudatuste vastuvõtmist ja nende osalist jõustumist. Järgmisesse aruandeperioodi jääb valdkonna kahe olulise õigusakti lõplik rakendamine.

Isikuandmete kaitse seadus

2007. aasta 15. veebruaril vastuvõetud ja täies mahus 2008. aastal rakendunud isikuandmete kaitse seaduse olulisimaks väljundiks saab pidada isikuandmete jaotuse muutmist ja delikaatsete isikuandmete laienemist biomeetriliste andmete võrra. Samuti isikuandmete töötlemise kaitstuse tõstmist, nt muudeti õiguspäraselt avalikuks kasutamiseks antavate isikuandmete töötlemise alast regulatsiooni, isikuandmete töötlemise nõudeid teadusuuringu või riikliku statistika vajadusteks ja loodi isikuandmete kaitse eest vastutava ametniku institutsioon.

Alates 01. jaanuarist 2008. aastal kadus eraeluliste isikuandmete kategooria. Isikuandmeid jaotatakse delikaatseteks isikuandmeteks ja isikuandmeteks. Koos eraeluliste isikuandmete kategooria tühistamisega muutus kehtetuks ka nimetatud isikuandmete töötlemisest teavitamise kohustus.

Delikaatsete isikuandmetena käsitletakse 2008. aasta 01. jaanuarist biomeetrilisi andmeid, eelkõige sõrmejälje, peopesajälje- ja silmaiirisekujutist ning andmed

pärilikkuse informatsiooni kohta asendatakse terminiga “geeniandmed”. Juhtimaks tähelepanu kõnealusele muudatusele ja võimalikule vajadusele delikaatsete isikuandmete töötlemine Andmekaitse Inspektsioonis registreerida, saatis inspektsioon ministeeriumitele sellesisulise märgukirja.

Ühe muudatusena näeb seadus ette, et inimesel on õigus nõuda ka õiguspäraselt avalikuks kasutamiseks antud andmete avalikustamise ja muul viisil kasutamise lõpetamist. Seega säilib isikul ka peale tema andmete avalikustamist kontroll nende edasise kasutamise üle, mida eelnev seaduse redaktsioon ei võimaldanud.

Ilmestamaks muudatust võib tuua näite, et peale seaduse jõustumist 01. jaanuaril 2008. aastal saab isik avalikku telefoniraamatusse või infotelefonile antud telefoninumbri avalikustamise igal hetkel ära keelata. Sama õigus kehtib erinevate püsikliendikaarte taotlenutele ja tarbijamängudes osalenutele - õigus nõuda, et nende andmeid töötlev ettevõtja kustutaks oma andmebaasidest tema senini avaliku olnud sidevahendi numbri ka juhul, kui ettevõtja on selle näiteks telefoniraamatust hankinud. Avalikustatud isikuandmete töötlejalt ei saa töötlemise lõpetamist nõuda juhul, kui see on tehniliselt võimatu ning toob töötlejale kaasa ebaproportsionaalselt suuri kulutusi.

Isikuandmete kaitse seadus reguleerib alates 01. jaanuarist 2008. aastal täpsemalt isikuandmete kogumist maksevõimelisuse hindamiseks. Kui siiani kehtinud normide kohaselt puudusid selliste andmete kogumisel konkreetselt sätestatud tähtaeg, siis alates 01. jaanuarist 2008. aastal võib andmeid isiku maksehäire kohta töödelda ja kolmandale isikule edastada üksnes kuni kolme aasta jooksul kohustuse rikkumisest. Seega ei tohi andmed maksehäirete registris olla vanemad kui kolm aastat. Vanemad andmed tuleb eemaldada. Erandina tuleneb krediidiasutuste seadusest, et krediidiasutus võib avaldada krediidiasutusega samasse konsolideerimisgruppi kuuluvale finantseerimisasutusele ja teistele krediidiasutusele kliendi kohustuse rikkumisega seotud isikuandmeid, kui kohustuse rikkumise lõpetamisest ei ole möödunud rohkem kui viis aastat.

Sisuliselt on seadusemuudatuse eesmärgiks tagada, et iga töötleja veenduks isikuandmete töötlemise aluses ning tagaks oma lepingute, nõusolekute ja muude dokumentide vastavuse seaduse nõuetele. Samuti muutuvad andmesubjekti nõusolekule esitatavad

nõuded. Seaduse uuest redaktsioonist tulenevate nõuete rakendamise kohustustele viidates saatis inspektsioon perioodi neljandas kvartalis märgukirja ka Pangaliidule.

Esile võib tuua ka töötlejate poolt isikuandmete töötlemise nõuete rikkumise rahaliste karistuste kümnekordset suurendamist. Seadusemuudatuse järgi võib mittenõuetekohane isikuandmete töötlemine juriidilisele isikule kaasa tuua kuni poole miljoni krooni suuruse trahvi.

Edaspidi on isikul võimalik keelata selliste andmete töötlemine, mille avaldamise ja edasise töötlemise õiguslikku alust ei ole võimalik kindlaks teha.
Isikul ei ole võimalik edasist töötlemist keelata vaid juhul, kui algne avalikustamine on toimunud ajakirjanduslikul eesmärgil (ka selle kohta on seaduses uued sätted) või seaduse alusel (näiteks riigi avalikkusele juurdepääsetavates andmekogudes).

Avaliku teabe seadus

Suurima muudatusena 15. veebruaril 2007. aastal vastuvõetud avaliku teabe seaduses on uue peatüki rakendumine 01. jaanuarist 2008. aastal, mille tulemusena kaotas andmekogude seadus kehtivuse ning andmekogusid puudutav regulatsioon rakendus avaliku teabe seaduse peatükina.

Rakenduse kõige suurem muudatus on senise riigi andmehõive poliitika muutmine andmekogupõhisest lähenemisest andmete töötlemise põhiseks lähenemiseks. 2007. aasta üheks tegevuseks oli riigi infosüsteemi haldussüsteemi (RIHA) rakendusakti väljatöötamises osalemine.

Muudatusena rakendus 01. jaanuarist 2008. aastal ka füüsilisest isikust ettevõtja lisandumine teabevaldajate nimekirja. Seda teabe osas, mis puudutab riigi või kohaliku omavalitsuse eelarvest avalike ülesannete täitmiseks või toetusena antud vahendite kasutamist.

Ülejäänud muudatuste vajadus on tulenenud praktikast ja regulatsiooni korrastavad, kuid sisulisi muudatusi võrreldes eelneva seaduse versiooniga kaasa ei too.

Järelevalve isikuandmete kaitse seaduse täitmise üle

Isikuandmete kaitse seadusest tulenevalt kontrollib Andmekaitse Inspektsioon IKS-i ja selle alusel kehtestatud õigusaktide järgimist. Samuti on vastutav töötleja kohustatud registreerima delikaatsete isikuandmete töötlemise Andmekaitse Inspektsioonis.

Kodanike teadlikkuse tõstmine

Sarnaselt eelnevatele aruandlusperioodidele on Andmekaitse Inspektsioon pidanud oluliseks tegeleda isikute teadlikkuse tõstmisega isikuandmete kaitse ja avaliku teabe kättesaadavuse valdkondades. Kuigi ka isikuandmete kaitse seadusest tuleneb Andmekaitse Inspektsioonile otsesõnu kohustus anda soovituslikke juhiseid seaduse rakendamiseks, on teavitustöö sfääri laiendatud. Lisaks soovituslike dokumentide avaldamisele on selgitatud valdkonna printsiipe ajakirjanduses[6] ning tegeletud koolitustööga nii sihtgruppidele kui ka üldisele elanikkonnale, samuti oleme näinud selgitustaotlustele vastamises tõhusat teavitustöö instrumenti.

Hea meel on olnud saadud tagasisidest, et isikuil ja ajakirjandusväljaannete esindajatel on tekkinud harjumus külastada küsimustele vastuste leidmiseks Andmekaitse Inspektsiooni kodulehekülge. Osalt just tagasisidest tulenevalt on muudetud kodulehte isikukesksemaks ja täpsemalt struktureeritumaks just huvigruppide- ja teemavaldkondadejärgselt. Eelnevast enam on koduleht täitunud ajakohaste teadetega osas, mis otseselt Andmekaitse Inspektsiooni tööd puudutab, kuid samas on koduleht muutunud valdkonna uudiste vahendamise keskuseks.

Kodulehe arendamine jätkub järgneval perioodil; lisaks eestikeelse kodulehe arendamise vajadusele, on asutud tasakaalustama inglisekeelsel kodulehel esitatava teabe mahtu ning värskelt on loodud venekeelne kodulehe osa, millel on samuti planeeritud avaldada esmane informatsioon ja juhendmaterjal Andmekaitse Inspektsiooni teemavaldkondadest.

Selleks, et edaspidise teavitustöö tõhusust oleks võimalik mõõta ja paremini planeerida teavitussuundi, tuli kaardistada olukord. Andmekaitse Inspektsioon tellis 2006. aasta

[6] „Kui praktiline on õigupoolest meie e-riik?“
Arvutivõrgust kättesaadav: http://www.epl.ee/artikkel/394209 ;
„Miks ei peaks lapsi Internetis üles lugema.“
Arvutivõrgust kättesaadav: http://www.postimees.ee/221107/tartu_postimees/arvamus/297009.php

detsembris Turu-uuringute AS-lt teadlikkuse uuringu isikuandmete kaitse valdkonnas, mille tulemused valmisid jaanuaris 2007. Uuring viidi läbi kodanike ja asutuste ametnike hulgas. Küsitluse lähteülesandeks seati kodanike teadlikkuse taseme fikseerimine isikuandmete kaitset puudutavais küsimustes.

Kuigi elanikkonna üldine teadlikkus isikuandmete kaitse vajadusest oli küllaltki hea, ei oldud eriti kursis isikuandmete kogumise ja töötlemise põhimõtetega. Vastanud ei teadnud, kes tegeleb nende isikuandmete töötlemisega; ei teadvustatud, et andmeid töödeldakse nii igapäeva-praktilistes asutustes, nagu seda on nt kaubanduskeskused, ööklubid jmt ettevõtted. Samas ligi pool vastajaskonnast oli kursis võimalusega pöörduda Andmekaitse Inspektsiooni poole juhul, kui nende andmeid valesti kasutataks. Silmapaistvalt eristus, et keskmisest halvemini oli isikuandmete kaitse ja töötlemise põhimõtetega kursis venekeelne elanikkond ning eraldi vanusegrupina paistis madalama informeeritusega välja pensioniealine elanikkond.

Järgmine samalaadne teadlikkuse uuring on planeeritud läbi viia 2009. aastal. Kogemusest tulenevalt on plaanitud mõnede küsimuste rõhuasetused teisiti püstitada, et saada täpsemat ülevaadet elanikkonna teadlikkusest – eelkõige isikuandmete töötlemise põhimõtetest, esitades küsimused selliselt, et isikuil tuleb anda vastus ilma uuringu läbiviija poolt antavate valikvastustega.

Tuginedes ülalkirjeldatud uuringu tulemustele ning arvestades Andmekaitse Inspektsiooni eelnevate perioodide koolitus- ja teavitustöö kogemust valmis dokument „Andmekaitse Inspektsiooni teavitusstrateegia aastateks 2007-2008“, milles on tulemusanalüüsi põhjal seatud vajalikud teavitustöö tegevused ning koolitussuunad.

28. jaanuaril 2007. aastal pidas Euroopa esmakordselt Rahvusvahelist Andmekaitse päeva (*Data Protection Day*). Tähtpäeva pidamise initsiatiiv tuli Euroopa Nõukogult ja lisaks Eestile tähistati päeva kõigis Euroopa Liidu ja ka teistes riikides, kes on ratifitseerinud isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni. [7]

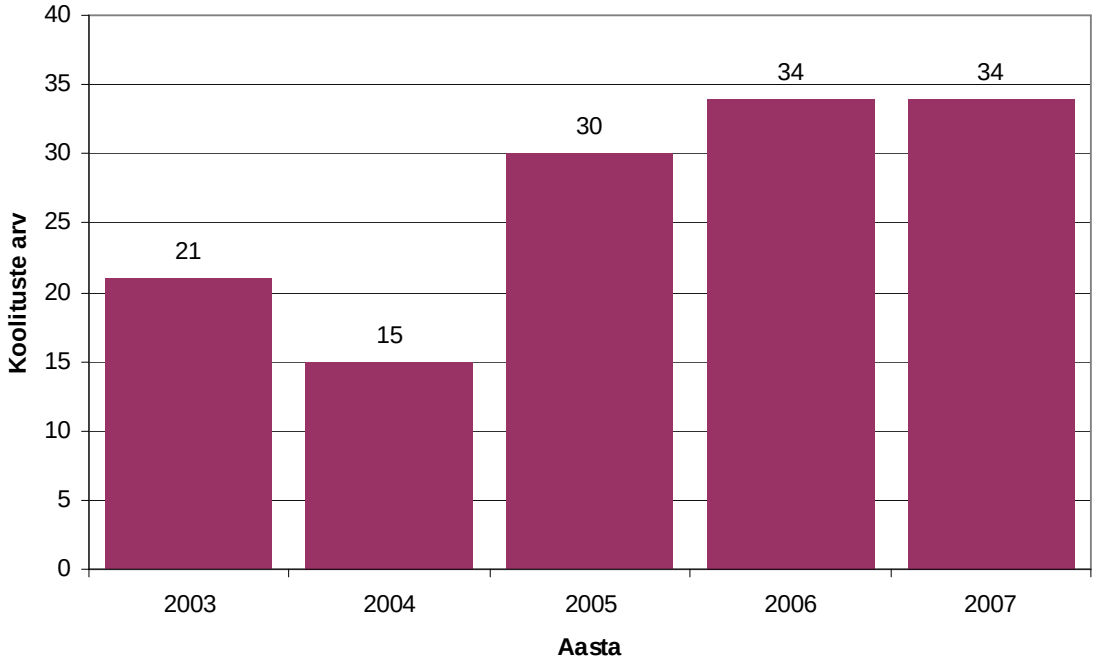
[7] konventsioon on isikuandmete töötlemise valdkonna põhidokument, mis allkirjastati 28. jaanuaril 1981. aastal Strasbourgis ja seetõttu on tähtpäev valitud just konventsioonileppe allkirjastamise kuupäevale.

Esimese Andmekaitse päeva juhtmõtteks oli avalikkuse teadlikkuse tõstmine andmekaitse valdkonnas. Andmekaitse Inspektsiooni konverentsil „Isikuandmete kaitse ja E-riik“ seoti teemadena omavahel isikuandmete kaitse ja E-ühiskond. Põhjus teemavalikuks eelkõige see, et kiireloomulise tehnoloogia arengu ajastul, mil luuakse järjest enam e-lahendustel baseeruvaid süsteeme ja andmebaase, tekib rohkelt küsimusi isikuandmete töötlemise nõuetekohase täitmisega ning seetõttu sooviti algatada diskussiooni andmetöötlejatega neil teemadel.

Perioodi lõpul alustati ka 2008 aasta Andmekaitsepäeva konverentsi korraldamist. Seekordne teemavalik oli seotud isikuandmete kaitse seadusesse lisandunud meediaklausliga ja kandis pealkirja „Isikuandmete kaitse ja meedia“.

Detsembris koordineeris Andmekaitse Inspektsioon TAIEX´ (Technical Assistance Information Exchange Unit) poolt korraldatavat koolitust Eesti riigiasutustes töötavatele ametnikele, kes on ametialaselt seotud isikuandmete kaitse ja andmete edastamisega kolmandatesse riikidesse. Koolituspäeval tutvustasid teemat Soome andmekaitse ombudsman Reijo Aarnio ja Andmekaitse Inspektsiooni peadirektor Urmas Kukk.

Andmekaitse Inspektsiooni ametnikud on jätkanud koolitusürituste läbiviimisega, mille eesmärk on tõsta üldist teadlikkuse taset isikuandmete kaitse ja kodaniku privaatsusõigust puudutavais valdkondades (vaata joonis 1). Kindlasti jätkatakse Rahvusvahelise Andmekaitse päeva tähistamist ja valdkonna konverentsi korraldamise traditsiooni, sest nii olnud konverents kui ka teised koolituse- või seminarivormis peetud üritused annavad tunnistust sellest, et ühelt poolt on üldine teadlikkus valdkonnas ebapiisav ja teemal rääkimine on vajalik, kuid teisalt võib tõdeda, et teadlikkuse tõus on tekitanud olukorra, kus üha enam pöördutakse Andmekaitse Inspektsiooni poole koolitussoovidega, seega mõistetakse isikuandmete kaitse ja avaliku teabe valdkondade laiahaardelisust ja puutumust üha rohkemate elualadega.



Joonis 1. Andmekaitse Inspektsiooni ametnike poolt läbi viidud koolitused aastate lõikes.

Tegevusprioriteedid aastal 2007 ja antud arvamustest

Esmakordselt sel perioodil sõnastas Andmekaitse Inspektsioon aasta omaalgatuslikud järelevalve tegevusprioriteedid. Teemavaldkondi, millega sel korral põhjalikumalt tegeleti, sai valitud seitse ja igal neist avaldas inspektsioon oma kodulehel, meedias või huvigrupile kättesaadava kanali kaudu arvamus- või juhenddokumendi. Tegemist on algatusega just organisatsiooni seest ja valituks prioriteetide hulka said need teemad, mille inspektsiooni ametnikud leidsid isikuandmete kaitse ja avaliku teabe valdkondades kõige enam probleemsed või raskesti tõlgendatavad olevat. Mõne huvisuuna puhul oli valikukriteeriumiks see, et isegi kui valdkond veel ei ole aktuaalne Eesti mastaabis, siis teistes Euroopa riikides või mujal maailmas on teema põhjustanud probleeme või mitmetimõistetavusi ning võib lähitulevikus osutuda potentsiaalseks probleemkohaks ka meil. Teemapõhiselt viidi läbi analüüs ja vajadusel järelevalve ning tulemustest lähtuvalt koostati juhised/juhendmaterjal, mis on avaldatud Andmekaitse Inspektsiooni kodulehel.

Valitud tegevusprioriteedid käesoleval perioodil olid järgmised: Isikuandmete edastamine kolmandatesse riikidesse; Ohud ehk võimalused veebiotsingu maailmas; Telefonikõnede lindistamise lubatavusest; Isikuandmete avalikustamine kohalike omavalitsuste aktides;

Isikuandmete töötlemine ID-pileti projekti raames; Laps ja tema õigused isikuandmete töötlemisel ning viimasena Isikuandmete koosseis kliendikaardi väljastamisel.

Prioriteet: **Isikuandmete edastamine välisriiki.**

Andmekaitse Inspektsioon oma ülevaatlikus juhendis "Isikuandmete edastamine välisriiki" toob välja nõuded ja nende erinevused, mis on vajalikud ja esinevad, kui isikuandmeid edastatakse riiki, mille puhul Euroopa Komisjon on andmekaitse taseme hinnanud piisavaks või mille puhul nimetatud positiivset hinnangut ei ole. Andmekaitse piisava taseme saavutamise eelduseks on siseriikliku andmekaitse seadusandluse ühtlustamine andmekaitse direktiivi (direktiiv 95/46/EÜ) nõuetega andmete edastamise küsimuses. Riike, mille puhul andmekaitse taset ei ole hinnatud piisavaks, nimetatakse andmete edastamise kontekstis kolmandateks riikideks.

Isikuandmete kaitse seaduse kohaselt võib isikuandmeid välisriiki, kus ei ole tagatud piisav andmekaitse tase, edastada üksnes Andmekaitse Inspektsiooni loal. [8] (vt Lisa 1)

Prioriteet: **Ohud ehk võimalused veebiotsingu maailmas.**

Sellise pealkirjaga dokumendi koostamise eesmärk oli anda ülevaade Interneti otsingusüsteemide kasutamisega kaasnevatest ohtudest, millele Andmekaitse Inspektsiooni arvamuse kohaselt on, võrreldes valdkonna eelistega, liialt vähe tähelepanu pööratud.

Arvamuses on tähelepanu suunatud probleemidele, mis on seotud isikuandmete kaitse ja andmeturbega. Välja on toodud kolm erinevat ohu liiki, millega peaks arvestama või millest vähemalt tuleks olla teadlik Interneti avarustes viibides.

Ohud, millest on dokumendis pikemalt räägitud saab võtta kokku järgnevate nimetajatega: oht andmesubjekti privaatsusele; oht veebis lehitseja privaatsusele ja oht veebiväljundiga infosüsteemi andmetele.

Kõikide nende ohtude vastu on olemas üsna toimivad vastumeetmed, kui asjaosalised neid ohte vaid teadvustavad ning suudavad vastavalt tegutseda.[9](vt Lisa 2)

[8] http://www.dp.gov.ee/document.php?id=166
[9] http://www.dp.gov.ee/document.php?id=232

Prioriteet: **Telefonikõnede lindistamise lubatavusest.**

Dokument „Telefonikõnede lindistamise lubatavus" loodi sooviga juhtida tähelepanu eraelu kaitse parandamise vajadusele telefonikõnede lindistamisel. Dokumendis on võetud arvesse Andmekaitse Inspektsiooni poolt teostatud järelevalvetoimingute tulemeid asutustesse, kus klienditeeninduse telefonikõned salvestatakse. Soovituslikus juhendis on antud ülevaade eraelu kaitse parandamise vajaduse sisust, samuti on vaadeldud eraldi nende isikute õigusi, kes ettevõttes telefoniga töötavad ja isikuid, kes on nende asutuse kliendid.

Toetudes õiguslikele alustele ja valdkonna kaardistatusele on Andmekaitse Inspektsioon asunud seisukohale, et isikute eraelu kaitse paremaks rakendamiseks on tingimata vajalik isiku nõusoleku võtmine telefonikõne lindistamiseks. Siinjuures on nõusoleku võtmine vajalik nii klientidelt kui ka kõigilt töötajatelt, kes telefoniga töötavad. Nõusolek peab olema võetud enne lindistamise algust ja töötajate puhul enne tööle asumist. Soovitav on võtta nõusolek töötajatelt kirjalikult, sest vaidluse korral eeldatakse, et nõusolekut ei ole antud ja sel juhul on asutusel kohustus tõendada, et nõusolek oli olemas.

Juhul, kui telefonikõnede lindistamine toimub seaduses ettenähtud kohustuste täitmiseks, piisab töötajate teavitamisest, mis peaks sisaldama vähemalt teavet lindistamise eesmärkide ja andmete säilitamise aja kohta.[10](vt Lisa 3)

Prioriteet: **Isikuandmete töötlemine ID-pileti projekti raames.**

Vastavalt isikut tõendavate dokumentide seadusele on Eestis esmane ja ainus kohustuslik isikutunnistus ID-kaart. Andmekaitse Inspektsiooni avaldatud dokument "Isikuandmete töötlemine ID-pileti projekti raames" vaatleb ID-kaardi kasutamist teenuse ostmist tõendava dokumendina Tallinnas kehtiva ID-pileti süsteemi näitel, juhtides eelkõige tähelepanu isikuandmete töötlemisega seonduvale taolistes süsteemides.

Juhend on mõeldud eelkõige avalik- ja eraõiguslikele organisatsioonidele, kes soovivad luua infosüsteeme, mis kasutavad teenuse või toote saamise õigust tõendava dokumendina ID-kaarti.

[10] http://www.dp.gov.ee/document.php?id=292

Andmekaitse Inspektsioon annab dokumendis juhendeid süsteemi rakendamiseks lähtuvalt isikuandmete kaitse ja andmetöötlemise põhimõtetest. [11](vt Lisa 4)

Prioriteet: **Laps ja tema õigused isikuandmete töötlemisel.**

Andmekaitse Inspektsioon analüüsis laste isikuandmete töötlemist erinevates igapäevaelu valdkondades. Avaldatu aluseks võeti peamised rahvusvahelisel tasandil laste õigusi käsitlevad õigusaktid, siseriiklikud vastavate valdkondade normid, läbiviidud järelevalvetulemid ja praktikas kasutatavad käitumisharjumused erinevates keskkondades. Lastekaitse seaduse kohaselt peetakse lapseks kuni 18-aastasi inimesi.

Dokumendis on esitatud argumentatsioon, mis puudutab lapse isikuandmete töötlemist ja õigust eraelu puutumatusele. Lapsel on õigus isiklikule elule, suhtlus- ja sõprusringile ning lapse õigust eraelule ei tohi kahjustada meelevaldse või ebaseadusliku sekkumisega.

Lisaks järeldub esitatud argumentatsioonist, et kuigi alla 18 aastase inimese kohta õiguslikke järelmeid kaasatoovaid otsuseid teevad lapse vanemad või seaduslikud hooldajad, tuleb lapse isikuandmete töötlemisel lähtuda samuti isikuandmete kaitse seaduses sätestatud põhimõtetest.

Eraldi alalõigus on analüüsitud küsimusteringi, mis seondub veebikaameratega koolides. Tehnoloogia võimaldab lapsevanemal jälgida oma lapse tegemisi 24 tundi ööpäevas ja videojärelevalve vajadust on põhjendatud turvalisuse kaalutlustele tuginedes. Samas aga mõjutab igasugune andmete videolindile salvestamine isiku põhiõigusi.

Inspektsioon on andnud dokumendis soovituse, et lapse tegevuse üle teostatav kontroll peab olema proportsioonis ühelt poolt lapse õigusega privaatsusele ning teisest küljest üldhuvidest lähtuvalt nagu näiteks turvalisusega kuritegude ennetamisega jne.

Lisaks on avaldatud dokumendis analüüsitud valdkondi, mis räägivad lapse hinnete avalikustamisest, lapse andmete avaldamisest Internetis ning pikemalt on peatutud lapse meedias eksponeerimise teemal.

Kokkuvõtvalt on asutud seisukohale, et laste privaatsuse kaitsel tuleb lähtuda kahest aspektist: vastutus ja teadlikkus. [12] (vt Lisa 6)

[11] http://www.dp.gov.ee/document.php?id=374
[12] http://www.dp.gov.ee/document.php?id=572

Prioriteet: **Isikuandmete koosseis kliendikaardi väljastamisel.**

Sellise nimetusega soovitus on mõeldud isikutele, kes on mõne kaubandusettevõtte või teenuseosutaja püsiklient ehk kliendikaardi omanik (klient) või soovib selleks saada. Soovituse eesmärgiks oli anda ülevaade sellest, mida kujutavad endast kliendikaardid isikuandmete töötlemise seisukohalt ning kliendi õigustest antud vallas.

Ostu sooritades ning selle käigus kliendikaarti kasutades jääb enamikel juhtudel maha jälg: kas ainult ostusumma suurus või ka konkreetne soetatud kaupade/teenuste nimekiri, mida on võimalik siduda kliendikaardi omanikuga. Olemasoleva isikuandmete hulgaga, sh sooritatud ostud, avaneb ettevõttel võimalus profileerida oma kliente, saada teada nende käitumisharjumusi ja ostueelistusi ning seeläbi edastada klientidele suunatud reklaame, mis lähtuvad konkreetsest kliendist.

Isikuandmete kaitse seisukohast on oluline, et klient teaks, et tema andmed kuuluvad talle ja kui klient on otsustanud soetada mõne ettevõtte kliendikaardi, siis tuleb arvestada, et sellega loobub ta väikesest osast oma eraelu puutumatusest.

Andmekaitse Inspektsiooni soovitused kliendile sellisel tegevusel on eelkõige sellised, et kliendikaardi taotlusele tuleks märkida minimaalsel hulgal isikuandmeid, mis on eelduseks kaardi saamisel; kliendikaarti taotledes kaaluda sooduspakkumiste ja kampaaniate informatsiooni kasutamise võimalust või sellest loobumist ning soovitus küsida ettevõttelt teavet isikuandmete töötlemise kohta.[13] (vt Lisa 7)

Dokument „Isikuandmete avalikustamine kohaliku omavalitsuse õigusaktis" on tutvustatud osas, mis käsitleb kodanike teadlikkuse tõstmist avaliku teabe seaduse valdkonnas.

[13] http://www.dp.gov.ee/document.php?id=592

Delikaatsete isikuandmete töötlemise registreerimine

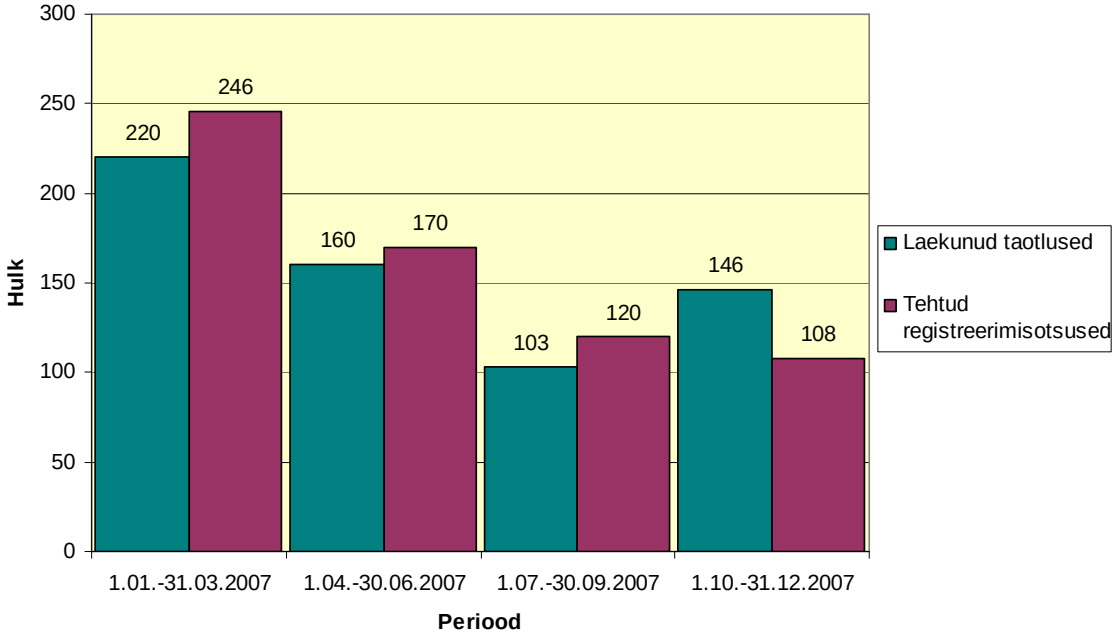
Perioodil 1. jaanuar 2007 – 31. detsember 2007. aastal laekus Andmekaitse Inspektsioonile 629 registreerimistaotlust, milledest 218 olid esmakordsed ning 305 korduvad. Muudatuste taotlusi laekus 106.

Antud perioodil rahuldati 644 registreerimistaotlust. Käesoleval perioodil delikaatsete isikuandmete töötlemise registreerimisest keeldumisi ei esinenud, samuti ei jäetud ühtegi registreerimistaotlust rahuldamata (vaata joonist 2). Saabunud taotluste hulga ja registreeringute näitajate erinevus tuleneb sellest, et taotlus on menetlusse võetud vaadeldava perioodi eel, kuid töötlemise registreerimine on toimunud aruande perioodi jooksul.

Põhjus, miks käesoleval perioodil on registreerimistaotluste ja antud registreeringute hulk märgatavalt suurem võrreldes eelmise aruande perioodiga, on selles, et 1. oktoobril 2006. aastal kaotasid kehtivuse delikaatsete isikuandmete töötlemise registreeringud neil, kes olid delikaatsete isikuandmete töötlemise registreerinud enne 2003. aastat. Nimetatud delikaatsete isikuandmete töötlejatel oli kohustus taotleda korduv registreering. Tähtaeg tulenes 2003. aastal jõustunud isikuandmete kaitse seaduse rakendussätetest. Delikaatsete isikuandmete töötlemise registreerituse tähtaja lõppemistest on jooksvalt töötlejaid meilivahendusel teavitatud, samuti on meeldetuletusartikleid avaldatud meditsiinivaldkonna ajakirjades.

Sellise laialdase teavitustöö tulemusena olid aktiivsemad delikaatsete isikuandmete töötlemise registreerijad apteegiteenuse pakkujad. Positiivse poole pealt võib tuua esile maavalitsuste aktiivset tegutsemist töötlemiste registreerimisel, sest peale märgukirjade saatmist maavalitsustele, oli esimese kvartali lõpuks delikaatsete isikuandmete töötlemine registreeritud kõikides maavalitsustes.

Aasta neljandas kvartalis alustati mittereageerinud isikuandmete töötlejatele ettekirjutuste tegemisega. Inspektsioon koostas perioodil 1. jaanuar 2007 – 30. detsember 2007. aastal delikaatsete isikuandmete töötlejaile 56 ettekirjutust.



Joonis 2. Saabunud taotluste hulk ja registreeritud delikaatsete isikuandmete töötlemised.

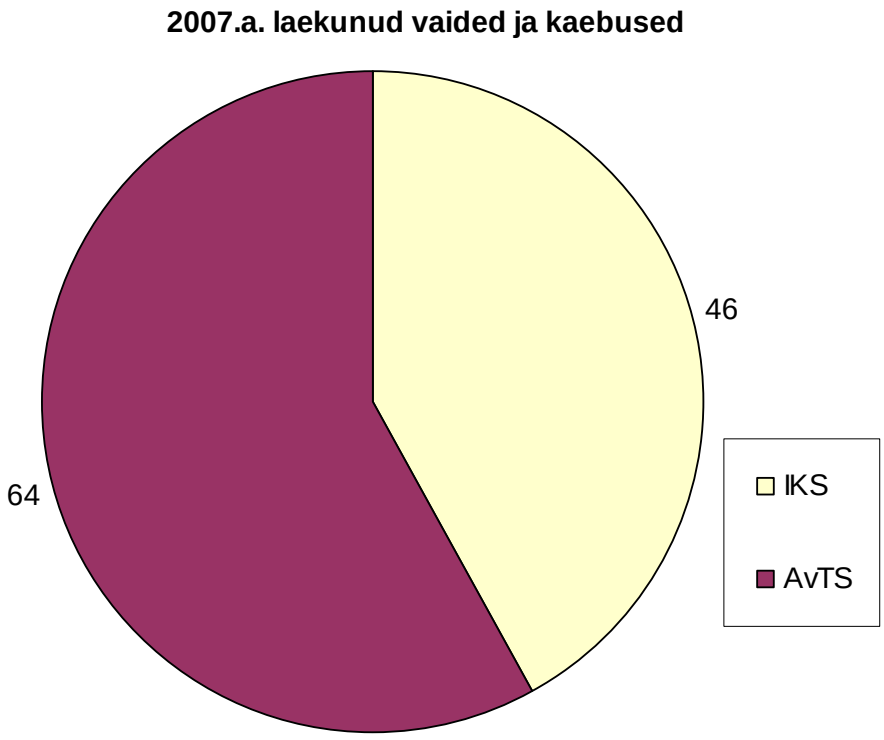
Eelmise aruandeperioodi lõpus alanud koostöö Ravimiametiga, mille tulemusel korraldati mitmeid infopäevi apteegiteenuse pakkujatele, tutvustamaks delikaatsete isikuandmete töötlemise kohustust, jätkus ka käesoleval perioodil. Eri piirkondade apteegiteenuse osutajatele korraldati isikuandmete töötlemisega seotud koolitusi kokku neljal korral, mil Andmekaitse Inspektsiooni ametnik andis ülevaate valdkonna probleemkohtadest ja vastas tekkinud küsimustele. Kirjeldatud loenguseeria tulemusel ja praktikale toetudes koostati näidisjuhis „Registreerimistaotluse esitamise juhend apteegiteenuse osutajale", mis avaldati Andmekaitse Inspektsiooni kodulehel abistamaks delikaatsete isikuandmete töötlemise registreerimistaotluse esitajaid.

Lisandus analoogne abimaterjal „Registreerimistaotluse esitamise juhend tervishoiuteenuse osutajale", mis samuti avaldati inspektsiooni kodulehel andmetöötlejaile mõeldud alajaotises.

Kaebuste menetlemine

Aruandeperioodil laekus Andmekaitse Inspektsioonile 110 kaebust ja vaiet, millest 46 kaebust/vaiet puudutas IKS-i kohaldamisala (vaata joonist 3). Laekus 251 selgitustaotlust ja märgukirja, millest IKS-i kohaldamisalaga oli puutumus 177 korral. Teostatud

menetluste käigus tuvastati rikkumine 26 korral, millest puutumus IKS-iga 6 korral, 130 korral rikkumist ei tuvastatud, millest 71 korral puudutas see IKS-i alusel teostatud kontrolli. Tuvastatud rikkumiste puhul tehti ettekirjutus 36 korral kokku ning sellest 5 korral tehti ettekirjutus IKS-i alusel. Kokku viidi väärteomenetlusi läbi 4 korral, kuid IKS-i puudutavas osas väärteomenetlusi ei esinenud. Aruandeperioodil viis Andmekaitse Inspektsiooni menetlustalitus läbi 41 omaalgatuslikku järelevalvemenetlust, millest 13 korral teostati menetlus IKS kohaldamisalas. Sunniraha ja trahviotsuste rakendamist tuli ette 2 korral, summas 8400 krooni (perearstipoolne delikaatsete isikuandmete töötlemise registreerimata jätmine; perearstikeskuse poolt patsientidele valimisreklaami edastamine).



Joonis 3. Inspektsioonile laekunud vaided ja kaebused seaduste lõikes aruandlusperioodil.

Probleem: meditsiinilise dokumentatsiooni säilitamine pärast teenuseosutaja tegevuse lõpetamist

Esilekerkinud probleem puudutab eriarstide loodud meditsiinidokumentatsiooni säilitamisega seonduvat olukorras, kus vastava teenuse osutaja lõpetab tegevuse.

Tervishoiuteenuste osutamist tõendavate dokumentide loetelu ja vormid ning tervishoiuteenuste dokumenteerimise kord on kinnitatud sotsiaalministri 6. mai 2002.aasta määrusega nr 76 (edaspidi määrus). Määruse § 3 lg 3 kohaselt säilitatakse määrusega kehtestatud dokumendid kui avalikud arhivaalid kehtestatud tähtaja jooksul arhiiviseaduses sätestatud nõuete kohaselt. Määrusega kehtestatakse tervisekaardi ja hambaravikaardi säilitamisajaks 110 aastat arvates patsiendi sünnist.

Arhiiviseaduse § 34 lg 7 kohaselt annavad eraõiguslikud juriidilised isikud neile kuuluvad avalikud arhivaalid, mille säilitamistähtaeg ei ole möödunud üle avalikku arhiivi, kui arhivaalid on hävimisohus või eraõiguslik juriidiline isik on likvideerimisel.

Nimetatud määratlus ei anna piisavalt selgust olukordades, kus avaliku arhivaali omanikuks olnud füüsilisest isikust ettevõtja sureb, eraõiguslik juriidiline isik lõpetab tegevuse meditsiinivaldkonnas vms.

Andmekaitse Inspektsiooni poole on peaasjalikult pöördunud tervishoiuteenuse osutajad (eriarstiabi) või nende lähedased küsimusega, kuidas käituda õiguspäraselt olukorras, kus soovitakse lõpetada tervishoiuteenuse osutamist või on tervishoiuteenuse osutamine lõppenud seoses tervishoiuteenuse osutaja surmaga. Nimetatud isikutelt saadud informatsiooni kohaselt on kõnealuste teabekandjate üleandmine avalikku arhiivi olnud komplitseeritud.

Lisaks dokumentide valdajatepoolsele probleemitõstatusele, puudutab kõnealune küsimus väga teravalt ka andmesubjektide, nende huve ning õigusi. Tegevuse lõpetanud tervishoiuteenuse osutaja valduses olnud teave võib teatud juhtudel olla andmesubjektile elulise tähtsusega ning nimetatud teabele juurdepääsu puudumine võib tekitada andmesubjektile olulist kahju. Olukorras, kus puudub selgus nimetatud teabekandjate asukoha ning nende eest vastutava isiku kohta, ei ole andmesubjektil võimalik realiseerida oma õigust teabe saamisele.

Andmekaitse Inspektsioon on pöördunud kõnealuses küsimuses Sotsiaalministeeriumi, Tervishoiuameti ning riigiarhivaari poole. Sotsiaalministeerium ning Tervishoiuamet möönavad probleemi olemasolu ning avaldavad lootust, et küsimus saab lahenduse loodava E-tervise raames.

Sarnaselt eelnimetatutele möönab ka riigiarhivaar probleemi olemasolu, kuid läheneb probleemile sisuliselt. Riigiarhivaari hinnangul ei lahendaks olukorda kõnealuste dokumentide üleandmine avalikku arhiivi ning jõuab tõdemusele, et kehtiva regulatsiooni tingimustes ei ole võimalik rahuldavale lahendusele jõuda. Riigiarhivaari hinnangul on määrus kehtival kujul lünklik, ega sisalda töötavat lahendust.

Kaasused

K-Rautakesko

Andmekaitse Inspektsiooni saabus märgukiri, mille kohaselt M.M. külastas mais K-Rautakesko kauplust ja ostis murutraktori, lubades traktorile järgi tulla nädala jooksul. Rohkem temalt infot ei küsitud.
M.M.-i isa läks traktorile järele paar päeva hiljem. Traktor tõsteti järelkärule, kui selgus, et kuna maksekviitungil on teine nimi, siis isale traktorit ei väljastata. (Maksmisel ei mainitud, et kaubale tuleb järele teine isik, peab kauplust sellest informeerima ja kviitungile vastava nime kandma.) Isa helistas M.M.-le ja rääkis tekkinud olukorrast. Samal ajal võttis laotöötaja isa käest passi, otsis midagi arvutist ja ütles isale, et kõik on korras, registrist olevat näha, et tema on tõesti M.M. isa.

Kuna M.M.-l on juba ca 20 aastat isast erinev perekonnanimi, tekkis tal huvi, milline andmebaas seob vanemaid täiskasvanud lastega. Kontrollis X-tee kaudu tema kohta tehtud päringuid, kuid selgus, et peale tema enda ei ole keegi isiku vastu huvi tundnud.
Et kauplus jättis väljastamata garantiitalongi, siis läks M.M. kauplusest läbi ja küsis ühtlasi andmeid registri kohta. Infolaua töötaja ehmus M.M. juttu kuuldes ja päris isiku nime järele ning lisas, et ainult infolauas on õigus registrit vaadata. M.M. kordas küsimust, kuid kaupluse töötaja helistas lattu ja vesteldes telefonitsi laotöötajaga rõhutas korduvalt, et ainult infolauas on õigus registrit vaadata. Kõne lõppedes küsis M.M. uuesti, millise registriga tegemist on. Kaupluse töötaja väitis, et laotöötaja tegi nalja ja

saab karistada, kuid registri kohta jäi jutt kliendi jaoks segaseks ning konkreetset vastust ei saanud.

Samal päeval helistas M.M.-le laotöötaja ja vabandas inetu käitumise eest. Klient vastas, et teenindus on olnud äärmiselt sõbralik ja viisakas, keegi pole teda halvasti kohelnud ning inetust käitumisest on kohatu rääkida. Arusaamatuks jäi vabanduse põhjus, kuid kliendil jäi huvi seoses kasutatud registriga. Helistaja kinnitas, et mingit registrit asutuses ei ole. Klient väitis end sellist juttu mitteuskuvat ning viitas infolaua töötaja sõnadele, et ainult nendel on õigus registrit kasutada.

Andmekaitse Inspektsiooni poolt algatati riiklik järelevalvemenetlus, mille käigus kontrolliti K-Rautakesko töötajate tegevust seoses kliendi kirjas märgitud asjaoludega.

Kontrolli käigus selgus, et isikuandmeid andmebaasidest ei vaadatud ning peale kliendiandmebaasi teisi isikuandmeid sisaldavaid andmekogusid K-Rautakesko kassiiri arvutis ei ole. Arvutites on müügiprogramm, kus isikuandmeid põlvnemise kohta ei töödelda.

Vestluses kaupluse juhataja ning kauba väljastanud kassiiriga selgus, et tegemist oli kohatu naljaga kliendi aadressil. Tulenevalt eeltoodud asjaoludest järelevalvemenetlus lõpetati.

SA Tartu Ülikooli Kliinikum

Oktoobris 2007. aastal kontrolliti delikaatsete isikuandmete töötlemist SA Tartu Ülikooli Kliinikumi poolt pildi arhiveerimise ja kommunikatsiooni süsteemis (edaspidi PAKS). Kontrollimisel pöörati tähelepanu isikute ringile, kes omavad ligipääsu PAKS-le, sh millises ulatuses on neil infosüsteemis võimalik delikaatseid isikuandmeid töödelda. Samuti täpsustati PAKS infosüsteemis kasutatavaid infotehnilisi turvameetmeid.

PAKS kasutajateks on suurklientidena haiglad ja perearstid. SA Tartu Ülikooli Kliinikum töötaja sõnul kasutab infosüsteemi 24 haiglat ning ligi 95% perearstidest ning haiglatel oli ligipääs kõigile PAKS-s olevatele delikaatsetele isikuandmetele. Samas loovad haiglad oma infosüsteemi tasemel delikaatsete isikuandmete töötlemisel piiranguid ja annavad vastavad juurdepääsuõigused. PAKS-s tehtavad toimingud delikaatsete isikuandmetega salvestatakse. Kui haiglatel on PAKS-s juurdepääs kõigile delikaatsetele isikuandmetele, siis perearstidel on ligipääs ainult oma patsientide terviseseisundit

kirjeldavatele andmetele. Järelevalvemenetluse käigus SA Tartu Ülikooli Kliinikumi PAKS infosüsteemis puudusi ei tuvastatud.

Töötajate videojälgimine: Eesti Vedurimeeste Ametiühing

Andmekaitse Inspektsioonile edastati Eesti Vedurimeeste Ametiühingu avaldus, mis esmalt esitati õiguskantslerile. Avalduse kohaselt rikkus AS Eesti Raudtee vedurimeeste õigusi, neid vedurite juhikabiinides jälgides ja nende vestlusi pealt kuulates. Andmekaitse Inspektsioon kontrollis isikuandmete töötlemist Spacecom AS töötlemiskohtades.

Kontrollimise käigus selgusid järgmised asjaolud:

AS Spacecomi poolt rendile antavatesse veduritesse oli paigaldatud videojälgimissüsteem, mis koosneb kaheksast kaamerast.

Vedurijuhi kabiinis oleva videokaamera kõrval oli teatis selle kohta, et veduris on nii video kui audio jälgimissüsteem.

Juurdepääs videosalvestistele on antud ainult AS Spacecom töötajale, kes on määratud juhtkonna käskkirjaga vastutavaks andmete töötlemise ja talletamise eest. Salvestisi vaadatakse ainult juhul kui on kahtlus, et veduri meeskond on rikkunud veduri ekspluatatsiooni eeskirju, raudteeohutuse eeskirju (eiranud punast foori tuld), on juhtunud õnnetus või veduri tehnilised parameetrid näitavad kõrvalekaldeid, mis on seotud kütusega. Kui raudteeveeremi koosseisuga ei ole toimunud mingeid intsidente ega olnud kõrvalekaldeid tehnilistest parameetritest, siis ei võeta salvestist kõvakettalt ega vaadata läbi. Seega igapäevast lauskontrolli ei toimunud.

Menetluse käigus selgus, et AS-ile Spacecom kuuluvatele veduritele paigaldatud seadmed ei ole vedurimeeste jälgimise ja pealtkuulamise seadmed, vaid tegemist on veduri tehnilise seisukorra automaatse kaugkontrollisüsteemi ja videoaudiovalvekontrolli süsteemiga.

Analoogsed seadmed on kasutusel ka teistes Euroopa Liidu liikmesriikides. Seadmete eesmärk on eelkõige seotud liiklusohutuse tagamisega ja nende poolt salvestatavat informatsiooni loetakse juhul, kui tekib vajadus veduri tehnilise seisukorra kontrollimiseks tagasiulatuvalt.

AS Eesti Raudtee selgitas, et AS Spacecom´ilt renditud vedureid kasutatakse Lõuna - Eestis, kuna Vene Föderatsioon ei luba teisi vedureid üle piiri. Samuti edastas AS Eesti Raudtee materjali koos lisalehtedega, kus selgus, et juhendiga on tutvunud nii vedurijuhid kui ka nende abid.

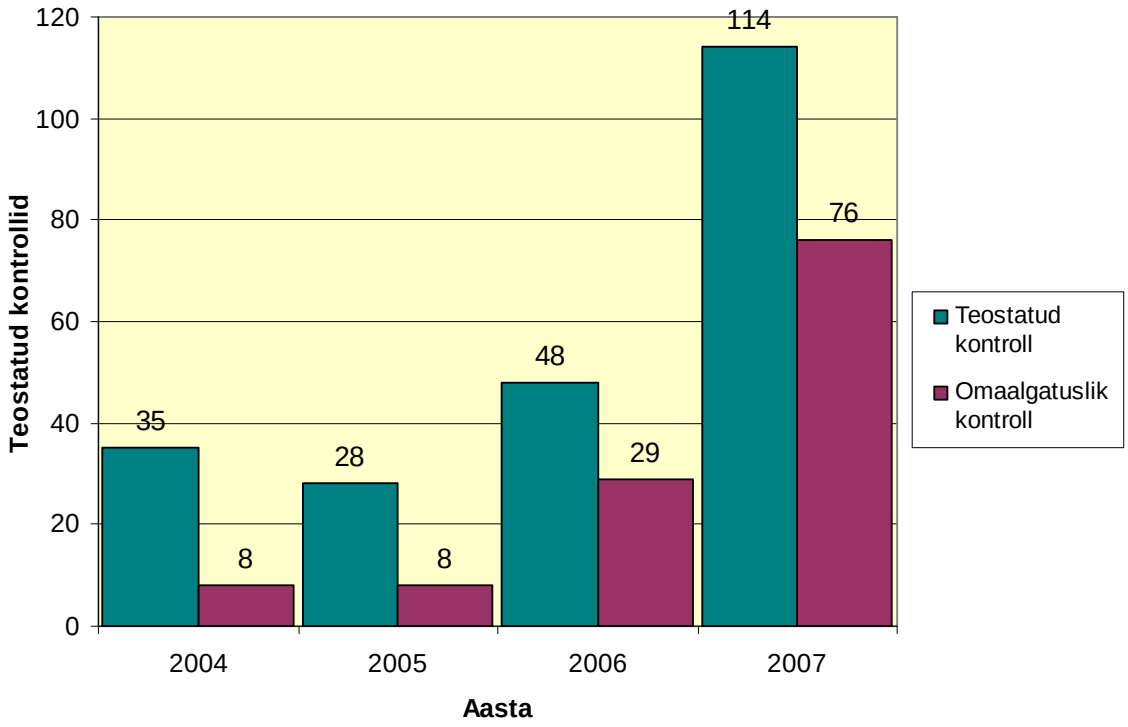
Lähtudes eelnevast oli Andmekaitse Inspektsioon seisukohal, et turvakaamerate paigaldamise eesmärgiks ei olnud vedurimeeste jälgimine (reaalajas jälgimist ei toimunud), vaid ohutuse tagamine ja avariide ennetamine.

Kuna antud juhul oli veduri juhikabiinis video- ja helisalvestiste kasutamise eesmärgiks tagada ohutus raudtee infrastruktuuril, siis ei saanud vastava tehnika kasutuselevõtt olla kuidagi sõltuvuses vedurimeeste nõusolekust. Tööandjal on õigus vajadusel kontrollida tööülesannete täitmist ja vara kasutamist. AS Eesti Raudtee oli tutvustanud allkirja vastu lõuna ekspluatatsiooni vedurijuhtidele ning abidele eelpoolnimetatud süsteemi. Samuti oli vedurikabiinis kaamera juures teave, et toimub salvestamine.

Seega oli tegemist teavitatud andmetöötlusega, mille eesmärgiks ei olnud jälgida mitte vedurimehi, vaid eesmärgiks oli eelkõige raudteeliiklusohutuse ja turvalisuse tagamine.

Kohapealse kontrolli teostamine

Aruandeperioodil teostas Andmekaitse Inspektsiooni järelevalvetalitus 114 korral kohapealset kontrolli isikuandmete kaitse seaduse täitmise üle. Omaalgatuslikku järelevalvet teostati 76 korral, millest puudused tuvastati 48 korral (vaata joonist 4). Andmekaitse Inspektsiooni järelevalvetalitus osaleb delikaatsete isikuandmete töötlemise registreerimistaotluste ning andmete muutmise või täiendamise menetlemisel. Aruandeperioodil on registreerimistalitusele antud arvamusi delikaatsete isikuandmete töötlemise valmisolekuks 741 korral.



Joonis 4. Järelevalvetalituse poolt läbi viidud kontrollkäigud ja teostatud omaalgatuslikud kontrollid

Kaasused

EURODAC-süsteem

Käesoleval perioodil lõpetati järelevalvemenetlus Eurodac-süsteemi siseriikliku osa üle (Kodakondsus- ja Migratsiooniamet (edaspidi KMA) teostatud päringute seaduslikkuse

kontroll ja Euroopa Liidu Nõukogu määruse nr 2725/2000 artiklis 14 sätestatud nõuete täitmine).

Teostatud järelevalvetoimingute käigus koostati kontrollakt: KMA teavitas, et kontrollaktis fikseeritud puudused on kõrvaldatud. Teostati järelkontroll, kas kasutatava serveri uuest versioonist on võimalik vaadata Eestist EURODAC-i süsteemi tehtud päringute ja Eesti poolt EURODAC-i süsteemis sisestatud andmete logisid ja tuvastati puudused turvameetmetes. Kuu aega hiljem teavitas KMA, et kontrollaktis fikseeritud puudused on kõrvaldatud. Järgnes uus järelkontroll. Kontrolliti, kas kasutatava serveri uuest versioonist on võimalik vaadata Eestist EURODAC-i süsteemi tehtud päringute ja Eesti poolt EURODAC-i süsteemis sisestatud andmete logisid. Kuna järelevalvemenetluse lõppeesmärk, milleks oli õiguspärase olukorra taastamine, oli saavutatud ning tulenevalt sellest puudus alus järelevalvemenetluse jätkamiseks, siis haldusorgani initsiatiivil algatatud haldusmenetlus lõpetati.

Schengeni infosüsteem (SIS)

Keskkriminaalpolitsei (edaspidi KKP) esitas Andmekaitse Inspektsioonile taotluse delikaatsete isikuandmete töötlemise registreerimiseks Schengeni infosüsteemi riiklikus registris (edaspidi SIS). Registreerimismenetluse käigus kogutud informatsiooni alusel ning tulenevalt SIS-is töödeldavate isikuandmete hulgast, delikaatsusest ja rahvusvahelisusest, otsustas Andmekaitse Inspektsioon kontrollida registreerimismenetluse käigus delikaatsete isikuandmete töötlemist KKP kriminaalteabeosakonna esimeses talituses.

Kontrolli eesmärgiks oli hinnata valmidust tagada 19. juuli 1990. aasta konventsiooni, millega rakendatakse 14. juuni 1985. aasta Schengeni lepingut Beneluxi Majandusliidu riikide, Saksamaa Liitvabariigi ja Prantsuse Vabariigi valitsuste vahel nende ühispiiridel kontrolli järkjärgulise kaotamise kohta (edaspidi Schengeni konventsioon) artiklis 118 sätestatud nõuete täitmine. Eelpool kirjeldatud kontrolli eesmärk valiti, kuna registreerimismenetluse raames KKP poolt esitatud dokumentatsioon ei käsitlenud Andmekaitse Inspektsiooni hinnangul Schengeni konventsiooni artiklis 118 sätestatu täitmist SIRENE büroos piisava põhjalikkusega.

KKP-s läbiviidava kontrolli ettevalmistamiseks kasutasid Andmekaitse Inspektsiooni

ametnikud lisaks Schengeni konventsioonile alusmaterjalidena ka Ühise Järelevalveasutuse poolt 1999. aastal väljatöötatud küsimustikku ning teisi teemasse puutuvaid Soomes Schengeni infosüsteemis isikuandmete töötlemist käsitleval TAIEX-i koolitusel saadud materjale.

Registreerimismenetluse käigus kogutud informatsiooni ja SIRENE büroos läbi viidud kohapealse kontrolli tulemusena leidis Andmekaitse Inspektsioon, et KKP poolt on isikuandmete kaitseks rakendatud piisavalt meetmeid ning registreeris isikuandmete töötlemise Schengeni infosüsteemi riiklikus registris.

Kontrollkäik: Maavalitsused

Maavalitsused töötlevad delikaatseid isikuandmeid neile seadusega pandud ülesannete täitmisel, sotsiaalhoolekande, tervishoiu ja haridusega seonduvates küsimustes. 2007. aasta alguseks oli valdaval osal maavalitsustest täitmata isikuandmete kaitse seadusest tulenev nõue, mille kohaselt peab delikaatsete isikuandmete töötleja registreerima delikaatsete isikuandmete töötlemise Andmekaitse Inspektsioonis. Vaatamata asjaolule, et 2006. aastal viis Andmekaitse Inspektsioon läbi teabepäeva maavalitsustele, kus selgitati isikuandmete kaitse seadusest tulenevaid nõudeid ning kohustusi, oli 2007. aasta jaanuari seisuga täitnud registreerimiskohustuse 2 maavalitsust viieteistkümnest.
Aasta alguses pöördus Andmekaitse Inspektsioon kirjalikult kõikide maavalitsuste poole ning juhtis veelkord nende tähelepanu asjaolule, et seadusest tulenev kohustus on täitmata. Nimetatud pöördumise tulemusena esitasid kõik maavalitsused delikaatsete isikuandmete töötlemise registreerimistaotlused ning I kvartali lõpuks on delikaatsete isikuandmete töötlemine kõikides maavalitsustes registreeritud.

Vaadeldava aasta esimeses kvartalis kontrolliti Andmekaitse Inspektsiooni järelevalvetalituse poolt kohapeal üheksat maavalitsust, milleks olid: Tartu Maavalitsus, Jõgeva Maavalitsus, Saare Maavalitsus, Võru Maavalitsus, Valga Maavalitsus, Lääne-Viru Maavalitsus, Ida-Viru Maavalitsus, Viljandi Maavalitsus ja Pärnu Maavalitsus.

Üheks esimeseks kontrollitavaks maavalitsuseks oli Ida-Viru Maavalitsus. Nimetatud maavalitsuse üle algatatud riiklik järelevalvemenetlus vältas kõige pikemalt – ligi kaks kuud.

Kontrolltoimingute käigus Ida-Viru Maavalituses ilmnesid puudused isikuandmete kaitseks rakendatavate infotehniliste turvameetmete osas. Digitaalsel kujul töödeldakse maavalitsustes delikaatseid isikuandmeid riigi osalusega abivahendi soetamise andmebaasis. Andmebaasi sisestatakse abivahendite müügiga tegelevate ettevõtete poolt saadetud andmeid. Kohapealse kontrolli käigus selgus, et abivahendite müügiga tegelevad ettevõtted edastavad Ida-Viru Maavalitsusele andmeid lisaks paberkandjatele ka elektronposti vahendusel. Isikuandmete töötlemise nõuete täitmise kohta Andmekaitse Inspektsiooni ametnike poolt koostatud kontrollaktis fikseeris maavalitsuse ametnik, et andmete edastamine elektronposti vahendusel andmebaasi korraldatakse turvalisuse tagamiseks ümber ning teavitatakse sellest ka järelevalveasutust. Peatselt pärast kontrollkäiku edastaski Ida-Viru Maavalitsus Andmekaitse Inspektsioonile kirja, kus teatati, et andmevahetus toimub kogu riigis samadel alustel ning seda korraldab Sotsiaalministeerium. Samas märgiti, et kuna andmevahetus toimib kogu riigis ühtsetel põhimõtetel, siis ei ole maavalitsusel võimalik iseseisvalt andmevahetust ümber korraldada. Lisaks andis maavalitus teada oma pöördumisest Sotsiaalministeeriumi poole, mille tulemusena selgus, et probleem on laiem ning puudutab kogu andmebaasi aruandlust tervikuna üle Eesti ning probleemile lahenduse leidmisega tegeleb Sotsiaalministeerium.

Pärast Ida-Viru Maavalitsuse täpsustavate selgituste andmist esitas Andmekaitse Inspektsioon maavalitsusele täiendavad seisukohad kasutuseloleva andmebaasi tarbeks e-posti teel delikaatsete isikuandmete edastamise kohta. Kirjas juhiti muuhulgas tähelepanu Sotsiaalministri määruse nr 79 „Tehniliste abivahendite taotlemise ja soodustingimustel eraldamise tingimused ja kord“ § 11 lõikes 3 sätestatud võimalusele korraldada abivahendite andmete elektrooniline edastamine kasutades füüsilist andmekandjat, mis välistaks krüpteerimata delikaatsete isikuandmete sattumist avalikku võrku. Samuti juhiti maavalitsuse tähelepanu võimalusele kasutada delikaatsete isikuandmete krüpteerimiseks ID-kaardi infrastruktuuri. Maavalitsusel paluti esitada täiendavaid selgitused ja seisukohad delikaatsete isikuandmete edastamiseks e-posti kasutamise osas.

Vastuskirjas järelevalveasutuse kirjale teatas Ida-Viru Maavalitsus, et kõiki abivahendite müüjaid on vajalikest muudatustest teavitatud ning neile on edastatud maavalitsuse ja ettevõtete vaheliste lepingute muudatuste lisad, milles on sätestatud, et maavalitsusele edastatakse abivahendi müüjate poolt abivahendi saanud isikute ning eraldatud abivahendite kohta kvartaalselt aruanded e-posti teel krüpteeritult.

Aruandeperioodil jätkatud kontrollide käigus pöörasid Andmekaitse Inspektsiooni ametnikud jätkuvalt tähelepanu ka sellele, millisel viisil abivahendite müügiga tegelevad ettevõtted maavalitsustele andmeid edastavad. Teistele kontrollitud maavalitsustele edastasid ettevõtted andmeid elektronposti teel krüpteeritud kujul ja tähitud kirjaga.

Kontrollkäik: Apteegid

Apteegiteenuse osutamisega kaasneb delikaatsete isikuandmete töötlemine. Apteegiteenuse osutaja kogub ja säilitab teenuse osutamisel ravimiretsepte, kuhu on märgitud nii isikut tuvastavad andmed kui ka isikule määratud diagnoosi kood, kontrollib vajadusel retseptile kantud andmete õigsust, osaleb müügiloata ravimi erandkorras sisseveoloa menetluses ning menetleb ravimi kohta esitatud kaebusi.

2006. aasta alguse seisuga ei olnud ükski apteegiteenuse osutaja delikaatsete isikuandmete töötlemist Andmekaitse Inspektsioonis registreerinud. Andmekaitse Inspektsiooni töötajad osalesid 2006.aasta lõpul apteegiteenuse osutajatele suunatud teabepäevadel ning selgitasid isikuandmete kaitse seadusest tulenevaid nõudeid ning kohustusi seoses isikuandmete töötlemisega.

Teavitamistöö tulemusena on registreerimiskohustuse vabatahtlikult täitnud umbes pooled apteegiteenuse osutajaist. Apteegiteenuse osutajate suhtes, kellel on 2008. aastaks jätkuvalt täitmata delikaatsete isikuandmete töötlemise registreerimiskohustus, alustab Andmekaitse Inspektsioon vajadusel haldussunni rakendamist. Ettekande koostamise ajaks on alustatud mittereageerinud apteegiteenuse osutajatele ettekirjutuste tegemist.

Vastavalt IKS-i § 36 lõike 1 punktile 1 on Andmekaitse Inspektsiooni ülesandeks kontrollida samas seaduses sätestatud nõuete täitmist.

Perioodil 01.01.2007 kuni 31.12.2007 kontrolliti omaalgatuslikult kohapeal kaheksat apteegiteenuse osutajat. Enamikes kontrollitud apteekides vastas isikuandmete töötlemine seaduses sätestatud nõuetele. Siiski esines ka mõnes apteegis isikuandmete kaitseks rakendatud füüsiliste ja infotehniliste turvameetmete osas puudusi. Puudused kõrvaldati kõikidel juhtudel paari-kolme nädala jooksul arvestades kohapealse kontrolli toimumise päevast.

Lisaks kaheksale apteegile, kontrollisid Andmekaitse Inspektsiooni ametnikud aruandeperioodil isikuandmete töötlemist AG Eesti Filiaalis ja Apteekide Infosüsteemide OÜ-s.

IMS AG Eesti Filiaal (edaspidi IMS) kogub lepingu alusel apteekidest andmeid, mille põhjal koostatakse isikustamata ravimimüügi statistika, mida müüakse edasi ravimite müügiga tegelevatele ettevõtetele. Andmekaitse Inspektsiooni ja IMS-i vahel järelevalvemenetluse käigus toimunud koostöö tulemusel võeti IMS-i poolt kasutusele täiendavad lahendused vähendamaks volitamata isikute poolt kodeeritud andmete tagasi isikustamise jääkriski.

Apteekide Infotehnoloogia OÜ tegeleb järgnevate valdkondadega: AS Astronoomilised Kassasüsteemid poolt arendatava tarkvara edasimüümisega apteekidele; tarkvara kasutatavatelt apteekidelt ravimi müügiga seonduvate andmete ostmisega; apteekidelt ostetud andmete töötlemisega ravimimüügi-alase statistika koostamise eesmärgil. Lisaks teostab Apteekide Infotehnoloogia OÜ lepingute ja väljakutsete alusel apteekide infosüsteemide hooldamist. Järelevalvemenetluse käigus Apteekide Infotehnoloogia OÜ-s puudusi ei tuvastatud.

Kontrollkäik: Ferratum Estonia OÜ

19.12.2007 kontrollis Andmekaitse Inspektsioon Ferratum Estonia OÜ (edaspidi OÜ) tegevust, et välja selgitada, kuidas ja milliseid isikuandmeid kogutakse väikelaenude (sms-laenude) andmise käigus ning kas see vastab isikuandmete kaitse seaduse nõuetele.
Teostatud järelevalve käigus selgus, et laenutaotluses edastatakse OÜ-le lühisõnumi või Interneti teel isiku ees- ja perekonnanimi, isikukood, elukoha aadress ja pangakonto number. Laenutaotluses olevad andmed sisestatakse automaatselt OÜ kasutuses olevasse andmebaasi. Andmebaasile omavad juurdepääsuõigust kõik OÜ töötajad ning neile on

välja antud personaalsed kasutajanimed ning paroolid. Samuti selgus, et kõigil kasutajatel on õigus vaadata, muuta ja kustutada andmebaasis olevaid isikuandmeid.

Veenduti, et OÜ töötaja poolt tehtud laenutaotluse aktsepteerimise või mitte aktsepteerimise otsus fikseeritakse andmebaasis kuupäeva ja kellaajalise täpsusega, seega kõikidest andmebaasis tehtud päringutest jäävad järgi logid.

IKS § 19 lg 2 p 2, 3[14] järgi on vastutav ja volitatud töötleja kohustatud isikuandmete töötlemisel ära hoidma andmete omavolilist lugemist, kopeerimist ja muutmist andmetöötlussüsteemis ning tagama, et tagantjärele oleks võimalik kindlaks teha, millal, kelle poolt ja milliseid isikuandmeid salvestati, muudeti või kustutati. Kasutusel olev tehniline lahendus vastab Andmekaitse Inspektsiooni hinnangul isikuandmete kaitse seaduse eelnimetatud sättele.

Lisaks eelnevale selgus, et OÜ säilitab laenutaotluste käigus kogutud andmeid tähtajatult ning ei teavita andmesubjekti andmete säilitamise tähtajast. Kuna OÜ ei ole piiritlenud tema poolt kogutud isikuandmete säilitamise tähtaega, siis ei ole OÜ isikuandmete töötlemine IKS-iga kooskõlas ning selline töötlemine ei ole AKI poolt aktsepteeritav. OÜ lubas isikuandmete töötlemise viia kooskõlla IKS-iga ning informeerida vastuvõetud otsusest ka inspektsiooni. Ettekande esitamise hetkeks on inspektsiooni teavitatud puuduste kõrvaldamisest.

[14] Kuni 2007.a lõpuni kehtinud isikuandmete kaitse seaduse redaktsioon. Kättesaadav arvutivõrgust: https://www.riigiteataja.ee/ert/act.jsp?id=12788408

Järelevalve avaliku teabe seaduse täitmise üle

Tulenevalt avaliku teabe seadusest teostab Andmekaitse Inspektsioon oma pädevuse piires järelevalvet AvTS-i nõuete täitmise üle. Samuti teostatakse riiklikku järelevalvet teabevaldajate üle nende poolt teabenõuete täitmisel ja teabe avalikustamisel.

Kodanike teadlikkuse tõstmine

Kui isikuandmete kaitse seadusest tuleneb Andmekaitse Inspektsioonile kohustus anda soovituslikke juhiseid seaduse paremaks rakendamiseks, siis samasisulist tegevust AvTS ette ei näe. Vaatamata sellele on Andmekaitse Inspektsioon, lisaks seadusest selgesõnaliselt tulenevatele kohustustele, võtnud eesmärgi tegeleda teavitustööga kogu järelevalve valdkonna raames - nii ka avalikku teavet- ja informatsiooni kättesaadavust puudutavas osas.

Perioodil peeti oluliseks tutvustada valdkonna põhimõtteid nii meedias kui kodanike ja ametnike gruppide hulgas, kellel võiks olla tõenäoliselt suurem huvi või puutumus üldiseks kasutamiseks mõeldud informatsiooni valdkonnaga seoses.

Eelpool tutvustatud teadlikkuse uuringust tulenevalt oli võimalik saada ülevaade sellest, milline on kodanike teadlikkus osas, mis puudutab asutustelt informatsiooni küsimist. Paraku on levinud eksiarvamus, et teiste isikute kohta on asutustelt õigus küsida mitmesuguseid andmeid, eeldatakse, et teave inimese töökoha ja karistatuse kohta on avalik.

Vaadeldaval perioodil on tuvastatud suuri puudusi riigi- ja kohalike omavalitsusasutuste dokumendiregistrites, millest võib järeldada, et just üldine kodanike teadlikkuse nõrk tase on võimaldanud neil puudustel siiani eksisteerida.

Andmekaitse Inspektsioon on loonud ja avaldas soovitusliku dokumendi (vaata allpool prioriteet: „Isikuandmete avalikustamine kohaliku omavalitsuse õigusaktis”), mis on sisult seotud isikuandmete kaitsega, kuid probleemkoht, ehk nende dokumentide avaldamiskohustus, tuleneb algselt just avaliku teabe seaduse reguleerimisalast.

Kuivõrd 2008. aastal jõustus uus avaliku teabe seaduse redaktsioon, siis vaadeldaval perioodil on Andmekaitse Inspektsiooni ametnikud viinud läbi koolitussoovidest tulenevaid seminare ja teabepäevi, millel on antud ülevaade nii uuendustest kui ka üldiselt printsiipidest avaliku teabe kättesaadavuse valdkonnas.
Oluliseks sihtgrupiks on peetud noori kodanikke, kellele on kodanikuõpetuse tunni raames käidud selgitamas avaliku teabe olemust, kodanike õigust esitada teabenõudeid neid huvitavate dokumentide ja informatsiooni suhtes.

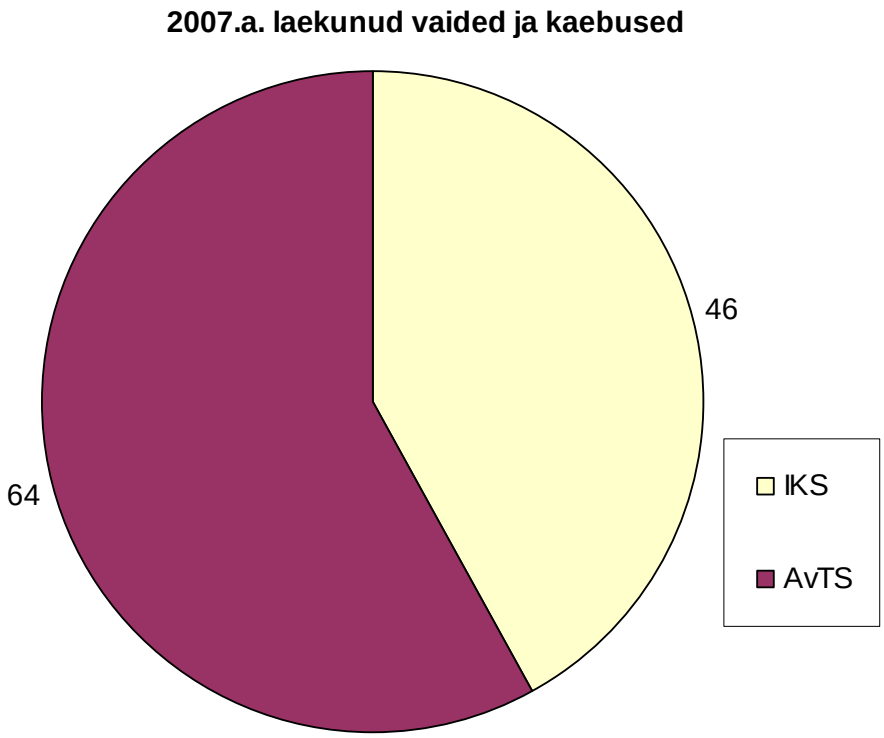
Prioriteet: **Isikuandmete avalikustamine kohaliku omavalitsuse õigusaktis**.
Avaldatud dokument kannab pealkirja "Juhendmaterjal KOV[15]-ide isikuandmeid sisaldavate õigusaktide avalikustamiseks"(vt Lisa 5) ja on mõeldud eelkõige valla- või linnasekretäridele, kes kohaliku omavalitsuse korralduse seaduse (KOKS) kohaselt korraldavad valitsuse õigusaktide avaldamist ja töö avalikustamist, osalevad valitsuse istungite ettevalmistamisel ja korraldavad istungite protokollimist, samuti annavad valla- või linnakantselei sisemise töö korraldamise käskkirju.

Dokumendi eesmärk on aidata leida kohalikel omavalitsustel tasakaal kahe olulise põhimõtte vahel, millel kohalik omavalitsus seadusejärgselt rajaneb – igaühe seaduslike õiguste ja vabaduste kohustuslik tagamine, sealhulgas informatsioonilise enesemääramisõiguse tagamine ning teiselt poolt oma tegevuse avalikkuse tagamine.[16]

Kaebuste menetlemine

Ajavahemikul 1. jaanuar kuni 31. detsember 2007. aastal laekus Andmekaitse Inspektsioonile 251 selgitustaotlust ja märgukirja, millest 74 korral oli puutumus AvTS-ga. Kaebuseid ja vaideid laekus inspektsioonile 110 korral, millest 64 korral puudutasid need AvTS-i kohaldamisala (vaata joonist 5).

[15] KOV- Kohalik omavalitsus
[16] http://www.dp.gov.ee/document.php?id=218



Joonis 5. Inspektsioonile laekunud vaided ja kaebused aruandlusperioodil.

Enamus käesoleval perioodil Andmekaitse Inspektsioonile laekunud vaietest esitati riigiasutuste ja kohalike omavalitsuste veebilehtede pidamise nõuete rikkumise suhtes.

Samuti oli perioodi läbivaks teemaks vaided teabevaldaja poolt teabenõuete mittetäitmisega või mittenõuetekohase täitmisega seotult. Esines olukordi, kus teabevaldaja ei pidanud vajalikuks teabenõudjat informeerida, millist teavet saab teabenõudega nõuda ja millist mitte. Samuti ei teavitatud teabenõudjat teabenõude täitmise tähtaja pikendamisest, jäeti teabenõuded registreerimata või keelduti teabenõude täitmisest valedel alustel.

Suure osa vaiete läbivaatamisel selgus, et tegemist ei olnud teabenõuetega AvTS-i mõistes, vaid selgitustaotluse või märgukirjaga, milledele vastamisel tuleb lähtuda märgukirjale- või selgitustaotlusele vastamise seadusest. Seejuures hea haldustava järgimisel pidanuks teabevaldajad isikut, kes nende poole vastavasisulise taotlusega pöördus, informeerima sellest, et esitatu näol ei olnud tegemist teabenõudega.

Veebilehtede pidamise nõuete rikkumiste valdava osa moodustas dokumendiregistrite puudulikkus või hoopis registri puudumine (dokumendiregistrit ei täidetud korrapäraselt, registrist ei olnud näha, millised dokumendid on juurdepääsupiiranguga ning millised mitte). Dokumendiregistritega seonduv on enim probleemiks kohalikes omavalitsustes.

Lähtuvalt eeltoodust pööras Andmekaitse Inspektsioon ka omaalgatusliku riikliku järelevalvemenetluse teostamisel eelkõige tähelepanu veebilehe pidamise nõuete täitmisele ning seal kajastatava teabe korrektsusele ja ajakohasusele.

Esitati kaebusi väärteomaterjalide ja kriminaalmenetluse käigus kogutud materjalide avaldamise kohta pärast vastavate menetluste lõpetamist kuna teabevaldajad ei arvestanud asjaoluga, et peale kriminaal- või väärteomenetluse lõppemist ning asjades tehtud otsuste jõustumist rakendub kogutud materjalide avaldamisel avaliku teabe seadus.

Esines olukordi, kui dokumendid olid tunnistatud asutusesiseseks kasutamiseks, kuid juurdepääsupiirang oli seatud ebaseaduslikult.

Kaasused

Kontroll: Tallinna Linnavalitsus[17]

Andmekaitse Inspektsiooni poole pöördus selgitustaotlusega eraisik V.A. ning palus selgitada, millisel õiguslikul alusel on Tallinna Linnavalitsuse õigusaktide registris linnavalitsuse korraldus, millele on võimaldatud avalik juurdepääs, avaldatud tema lapse nimi. V.A. leiab, et dokumendis on avaldatud isikuandmed, millele peaks kolmandate isikute juurdepääs olema piiratud.
Andmekaitse Inspektsioon pöördus nimetatud küsimusega Tallinna Linnavalitsuse poole ning selgitas Tallinna Linnavalitsuse ametnikele oma seisukohti isikuandmete avalikustamisel veebilehel.

Andmekaitse Inspektsioon esitas oma kirjaliku seisukoha isikuandmete avaldamise kohta Tallinna Linnavalitsuse õigusaktides ning lähtuvalt V.A. kaebusest palus kustutada,

[17] Kontrolli järelmina tehtud ettekirjutus on küll tulem isikuandmete kaitse seaduse alusel teostatud järelevalvest, kuid asutuste koduleheküglegedel dokumendiregistri avaldamise alus pärineb avaliku teabe seadusest, seetõttu on kaasus kajastatud avaliku teabe seaduse järelevalvet puudutavas peatükis.

Tallinna Linnavalitsuse veebilehel avalikustatud õigusaktide registrist V.A. lapse nime. Tallinna Linnavalitsus ettenähtud tähtajaks lapse nime ei kustutanud ega esitanud ka vastuväiteid.

Tulenevalt kohaliku omavalitsuse korralduse seaduse (KOKS) § 31 lõikest 1 avalikustatakse valla- ja linnavalitsuse õigusaktid ning need peavad olema kättesaadavad kõigile isikutele seaduses ja valla või linna põhimääruses sätestatud korras. Kui valla või linna põhimääruses ei ole sätestatud teisiti, avalikustatakse valitsuse määrus väljapanekuga valla- või linnakantseleis. Sama paragrahvi lõike 2 kohaselt ei avalikustata andmeid, mille väljastamine on seadusega keelatud või mõeldud üksnes valla või linna ametiasutuse siseseks kasutamiseks.

Tulenevalt IKS-i §-st 1 on isikuandmete kaitse seaduse eesmärgiks isikuandmete töötlemisel füüsilise isiku põhiõiguste ja põhivabaduste kaitsmine kooskõlas avalike huvidega. Isikuandmete töötlemisel on vastutav ja volitatud töötleja kohustatud isikuandmete töötlemisel lähtuma eesmärgikohasuse ja minimaalsuse põhimõttest (IKS § 6 p 3) ning eraelu puutumatusest. Kui isiku nimi iseenesest ei kuulu eraeluliste isikuandmete hulka, siis koosmõjus muu informatsiooniga võib ka isiku nimi olla eraelulisteks isikuandmeteks. Põhiõiguste kaitse seisukohalt on äärmiselt oluline, et isikuandmeid töödeldakse võimalikult vähesel määral konkreetset, eelnevalt kindlaksmääratud eesmärkide saavutamiseks.

AvTS-i § 4 lõike 1 kohaselt on teabevaldajad kohustatud demokraatliku riigikorralduse tagamiseks ning avaliku huvi ja igaühe õiguste, vabaduste ja kohustuste täitmise võimaldamiseks tagama juurdepääsu nende valduses olevale teabele seaduses sätestatud tingimustel ja korras. Kui teabele juurdepääsu võimaldamine võib põhjustada juurdepääsupiiranguga teabe avalikuks tulemise, siis tagatakse juurdepääs üksnes sellele osale teabest või dokumendist, mille kohta juurdepääsupiirangud ei kehti (AvTS § 38 lg 2).

Vastavalt Euroopa andmekaitse direktiivi 95/46/EÜ artikli 1 lõike 1 ja preambula punkti 10 eeskujule on ka IKS-i eelnõus eesmärgi määratlemisel rõhutatud vajadust kaitsta inimeste põhiõigusi ja vabadusi, eelkõige õigust eraelu puutumatusele. See ei tähenda siiski isikuandmete kaitse ja eraelu puutumatuse õiguse absolutiseerimist, vaid see üksnes rõhutab, et isikuandmete töötlemise nõuete sisustamisel tuleb piiripealsetel juhtudel alati

eelistada tõlgendust, mis kaitseb tugevamini eraelu puutumatust, mitte ei sea esiplaanile võimalikke avalikke huve.

Eraelu kaitse ja teabe avalikustamise vajaduse vastuolu tuleb kõige selgemini esile Internetis avaldatud teabe korral. AvTS § 35 lõike 2 punktid 10 ja 11 ning § 39 koosmõjus isikuandmete kaitse seaduse §-ga 14 sätestavad, et eraelulisi ja delikaatseid isikuandmeid avalikustada on keelatud (va seaduses ettenähtud juhud). Mittedelikaatseid isikuandmeid võib avalikustada huvide kaalumise põhimõttel: kui avalikustamine kahjustaks andmesubjekti eraelu puutumatust, ei tohi ka mittedelikaatseid isikuandmeid avalikkusele kättesaadavaks muuta. Siinjuures on oluline märkida, et piirangud kehtivad vaid laiemale üldsusele avalikustamise kohta.

Lähtudes eelnevast leidis Andmekaitse Inspektsioon, et Tallinna Linnavalitsus rikub isikuandmete töötlemisel minimaalsuse ja eesmärgikohasuse põhimõtet, milles andmete avalikustamine Internetis ei ole proportsionaalne seatud eesmärgiga ning riivab eraelu puutumatust. Seega on Tallinna Linnavalitsus rikkunud IKS § 6 punktist 2 ja 3 tulenevaid nõudeid.

Isikuandmete kaitse seaduse § 40 lõike 1 alusel tegi Andmekaitse Inspektsioon Tallinna Linnavalitsusele kohustusliku ettekirjutuse kustutada Tallinna Linnavalitsuse veebilehel avalikustatud õigusaktide registris V.A. lapse nimi. Tallinna Linnavalitsus täitis ettekirjutuse kohaselt.

Kontroll: ministeeriumide dokumendiregistrid

Oktoobris kontrollis Andmekaitse Inspektsioon ministeeriumite dokumendiregistreid. Kontrollimise käigus tuvastati, et Kaitseministeeriumil puudus dokumendiregister ning Keskkonnaministeeriumi poolt peetav dokumendiregister ei olnud ajakohane, viimased kanded dokumendiregistris pärinesid aprillist 2007. a. Samuti pärinesid Majandus- ja Kommunikatsiooniministeeriumi dokumendiregistri viimased kanded augustist 2007. a. Justiitsministeeriumi dokumendiregistri kasutusjuhendis teavitati asjaolust, et dokumendi mitteleidmisel palutakse pöörduda teabenõudega ministeeriumi poole, kuna dokument võib puududa avalikust dokumendiregistrist seoses delikaatsete isikuandmete sisaldumisega dokumendis.

Menetluse käigus kõrvaldasid Keskkonnaministeerium ja Majandus- ja Kommunikatsiooniministeerium oma dokumendiregistrites esinevad puudused ning

seetõttu ettekirjutust ei järgnenud. Ettekirjutus avalikustada dokumendiregister tehti Kaitseministeeriumile. Justiitsministeeriumile tehti ettekirjutus registreerida veebilehel olevas avalikus dokumendiregistris ka juurdepääsupiiranguga (delikaatseid andmeid sisaldavad) dokumendid. Eelnevalt on kaebuse alusel algatatud järelevalvemenetlus ja tehtud ettekirjutus ka Välisministeeriumile, kellel puudus samuti dokumendiregister. Ettekande avaldamise ajaks on kõik ministeeriumid osundautud puudused kõrvaldanud.

Kontroll: Saaremaa vallavalitsused

Perioodi neljandal kvartalil kontrollis Andmekaitse Inspektsioon omaalgatuslikult Saaremaal asuvate valdade vallavalitsuste veebilehti, täpsemalt vastavust avaliku teabe seaduses sätestatud nõuetele, mis seonduvad dokumendiregistri pidamise kohustusega. Kuueteistkümnest Saaremaa vallast kümne vallavalitsuse puhul tuvastati järelevalve käigus puudusi veebilehe pidamise nõuete täitmisel. Nimetatud hulgale vallavalitsustest tehti Andmekaitse Inspektsiooni poolt sellekohane ettekirjutus kohustuslikuks täitmiseks. Üheksa Saaremaa vallavalitust on viinud veebilehel asuva dokumendiregistri avaliku teabe seadusest tulenevate nõuetega vastavusse ning üks vallavalitus on taotlenud ettekirjutuse tähtaja täitmise pikendamist tehnilistel põhjustel.

Kohtukaasuse analüüs

Eraisik H.R. ja Hansapanga vahel oli sõlmitud Ego järelmaksukaardi kasutamise leping, mille kohaselt sai H.R. kasutada krediiti, samuti võttis ta kohustuse antud krediit lepingu tingimuste kohaselt Hansapangale tagasi maksta igakuise püsimaksena. H.R. ei täitnud endale lepinguga võetud tagasimaksukohustust.

Seejärel sõlmiti Hansapanga ja H.R. vahel Ego järelmaksukaardi kasutamise lepingust tuleneva võlgnevuse tagasimaksmiseks täiendavalt võlaleping. Ka viimati nimetatud lepinguga endale võetud võlasumma tagasimakse kohustust H.R. korduvalt ei täitnud.

Lähtudes krediidiasutuste seaduse § 88 lõike 2 punktist 4 ja Ego järelmaksukaardi kasutamise lepingust ning võlalepingust avalikustas Hansapank H.R.-i võlgnevused AS-i Krediidiinfo veebilehel.

H.R. tasus 2006. aastal oma võla AS-i Hansapank ees ning soovis oma andmete kustutamist maksehäireregistrist. Hansapank keeldus andmete kustutamisest.
Peale seda pöördus H.R. kaebusega Andmekaitse Inspektsiooni poole. Andmekaitse Inspektsioon tegi Hansapangale ettekirjutuse: andmesubjekti kaebuse kohaselt ei andnud ta nõusolekut oma isikuandmete avalikustamiseks AS Krediidiinfo veebilehel. Kuna AS Hansapank ei määratlenud H.R. isikuandmete töötlemise eesmärke lepingus ega ka Andmekaitse Inspektsioonile teadaolevalt muudes andmesubjektiga seotud dokumentides, siis tulenevalt põhimõttest, et vaidluse korral eeldatakse, et andmesubjekt ei ole oma isikuandmete töötlemiseks nõusolekut andnud (IKS § 12 lg 5), loeti AS Hansapank poolt H.R. isikuandmete avalikustamine andmesubjekti nõusolekuta isikuandmete töötlemiseks.
Ettekirjutusega kohustati panka lõpetama H.R. isikuandmete ebaseaduslik avalikustamine. Ettekirjutuse AS Hansapank täitis, kuid saatis Andmekaitse Inspektsioonile vaide nimetatud ettekirjutuse kohta. Andmekaitse Inspektsioon ei rahuldanud vaiet ja Hansapank edastas materjalid kohtusse.
Tallinna Halduskohus leidis oma 17.04.2007. aasta otsuses, et ettekirjutus oli sisuliselt põhjendatud ja oma lõppjäreldustes õiguspärane.
14.05.2007.aastal esitas AS Hansapank Tallinna Ringkonnakohtule apellatsioonikaebuse ja käesoleval ajal on kohtuistung määratud 9.04.2008. aastal.

Rahvusvaheline koostöö

Isikuandmete kaitse seadusest tulenevalt teeb Andmekaitse Inspektsioon koostööd rahvusvaheliste andmekaitse järelevalve organisatsioonidega ja välisriikide andmekaitse järelevalve asutuste ning välisriikide muude pädevate asutuste või isikutega. Eelpooltoodud seadusest tulenevale kohustuse täitmisel ja olles Euroopa Liidu liige ning tulenevalt valdkonna iseloomust pole Andmekaitse Inspektsiooni pädevus seotud riigipiiridega. Valdkonna probleemid on piiriülesed ja ühetaolised kõikjal ning arvestades näiteks elektrooniline isikuandmete töötlemise iseloomu, ei ole riigipiir oluline.

Ka käesoleval perioodil on inspektsiooni ametnikud võtnud osa mitmetest iga-aastastest ja ka ühekordselt toimuvatest rahvusvahelistest konverentsidest ja töökohtumistest, kus on teemaks püsivas arengus olevad küsimused kui ka uudissuunad isikuandmete kaitse valdkonnas. Allpool antakse ülevaade olulisematest üritustest ja teemadest, samuti töögruppidest, mille liikmetena Andmekaitse Inspektsiooni ametnikud kaasatud on, tehtavast tööst.

Rahvusvahelised töögrupid

Iga-aastase Euroopa andmekaitse järelevalveasutuste kevadkonverentsi (Küpros) põhiteemadeks oli küsimustering, mis puudutab elektroonilisi terviseandmete süsteeme ning valdkond, mis seob teemasid isikuandmete kaitse ja meedia. Andmekaitse Inspektsiooni peadirektor tegi ülevaatliku ettekande teemal „Isikuandmete avaldamisest meedias”.

Kesk- ja Ida-Euroopa isikuandmete kaitse volinike konverentsil (Zadar) arutleti Schengeni viisaruumiga liitumisega seotud andmekaitse kriteeriumite ja Euroopa Liidu õiguskorra rakendamise üle, isikuandmete kaitsest sise- ja justiitsküsimustega seonduvates asutustes, andmekaitse ja riigi läbipaistvuse teemadel, arengutest e-tervisekaartide valdkonnas ning uute tehniliste võimaluste üle, mis võimaldavad andmetöötlust ja mille võimalused ei ole valdkonnas veel ammendavalt reguleeritud.

Igal aastal kaks korda toimuval otseselt järelevalvega tegelevate ametnike töökohtumisel (*Case Handling Workshop*) käivad koos andmekaitse järelevalve asutuste kaebustega tegelevad ametnikud (kaebuste menetlejad). Sügiskonverentsil Ateenas arutleti kaasuste

üle, mis puudutasid videojärelevalvet, sideandmeid, dokumentidest koopiate tegemist, samuti panganduse valdkonnas krediidivõimelisuse hindamiseks kasutatavate andmetega seonduvat. Arutleti e-teenuste arendamise võimalusi riigi- ja kohalike omavalitsuste koduleheküIgedel seonduvalt isikuandmete kaitsega.

Sama üritusesarja kevadine töökohtumine Helsingis kandis endas järgnevaid aruteluteemasid: isikuandmete kaitse ja Internet, otsepostitus 21. sajandil, videojärelevalve üldise järelevalveühiskonna kontekstis, terviseandmed, privaatsus ja ligipääs avalikele dokumentidele, biomeetria ning sõrmejälgede temaatika ning arutelu oli pühendatud andmekaitse järelevalveasutuste pädevus-võimekusele – millised on ennetavad ja reaktiivsed meetmed.

Käesoleva perioodi telekommunikatsioonialase rahvusvahelise andmekaitse töögrupi (IWGDPT), mille tegutsemise rõhuasetus on seatud isikuandmete töötlemisele läbi telekommunikatsiooni ning tehnoloogia arengu. Seekordse kohtumise raames toimus telekommunikatsioonialane mess, millel peeti rahvusvaheline sümpoosium „Eraelu puutumatus digitaaltelevisioonis" („Privacy in Digital Television"). Kokkuvõtlikult jõuti sümpoosiumil järeldusele, et digitaaltelevisiooni tehnoloogia võimaldab vaatajale personaalset lähenemist, mis on vastuolus Telekommunikatsiooni direktiivi artikliga 10. Samuti on nõrgalt kaitstud vähemuste huvid ja tuleb näha ette erimeetmeid laste kaitseks. Vastu võeti 2 soovituslikku dokumenti: *„E-Ticketing in Public Transport"*[18] ja *„Privacy Issues in the Distribution of Digital Media Content and Digital Television"*[19].

Jätkuvalt on Andmekaitse Inspektsioon tegev mitmetes Euroopa Liidu töögruppides. Olulisemad neist on Direktiivi 95/46/EÜ artikkel 29 alusel loodud andmekaitse töögrupp, Europoli konventsiooni artikkel 24 alusel loodud ühine järelevalveasutus (Europol JSB), Schengeni konventsiooni artikkel 115 alusel loodud ühine järelevalve asutus (Schengen JSA) ning infotehnoloogia tollialase kasutamise konventsiooni artikkel 18 alusel loodud ühine järelevalveasutus (Custom JSA).

[18] E-piletid ühiskondlikku transpordivahendit kasutades
[19] Eraelu puutumatuse küsimused digitaalses meedias sh digitaalses televisioonis töödeldava teabe osas

Artikkel 29 andmekaitse töögrupp

Artikkel 29 Andmekaitse Töögrupp on Euroopa Komisjoni juures tegutsev andmekaitse töögrupp, mille eesmärk on anda soovituslikke andmekaitsealaseid juhendeid ja seisukohti. Töögrupi liikmeteks on kõik Euroopa Liidu liikmesriikide andmekaitse asutused, Euroopa andmekaitseinspektor ning samuti võtavad kohtumistest osa ka teiste Euroopa riikide andmekaitseasutused. Töögrupp kohtub regulaarselt viis korda aastas. 2007. aastal on töögrupis olnud arutlusel jätkuvalt PNR (*Passenger Name Record*)[20], SWIFT[21] (SWIFT võrgus isikuandmete töötlemine), BCR (*Binding Corporate Rules*)[22]. Lisaks on vaatluse alla võetud laste õigused andmekaitse aspektist, isikuandmete defineerimine erinevates valdkondades, elektroonilised terviseandmed, tervisekindlustusseltsid seotult isikuandmete kaitsega.

Europoli Ühine Järelevalveasutus

Europoli ühise järelevalveasutuse (*Europol Joint Supervisory Body* ehk *Europol JSB*) eesmärgiks on kooskõlas Europoli konventsiooniga jälgida Europoli tegevust, tagamaks üksikisiku õigusi andmete talletamisel, töötlemisel ja kasutamisel.

2007. aasta märtsis viis Europoli ühine järelevalveasutuse inspekteerimisrühm läbi Europoli keskküksuse iga-aastase järelevalve, mille kohta koostati ka inspekteerimisraport.

Aruandeperioodil avaldas Europoli ühine järelevalveasutus oma kolmanda tegevusaruande, mis annab ülevaate ühise järelevalveasutuse tegevusest ajavahemikul november 2004 kuni oktoober 2006.aasta.

Tollikonventsiooni Ühine järelevalveasutus

Andmekaitse Inspektsioon osaleb infotehnoloogia tollialase kasutamise konventsiooni ühise järelevalveasutuse (*Customs Joint Supervisory Authority* ehk *Customs JSA*) töös. Tollikonventsiooni ühine järelevalveasutus on pädev teostama järelevalvet infotehnoloogia tollialase kasutamise konventsiooni täitmise üle, läbi vaatama konventsiooniga seotud rakendamis- või tõlgendamisküsimusi, uurima probleeme, mis tekivad liikmesriikide siseriiklikel järelevalveasutustel sõltumatu järelevalve teostamisel

[20] Lennureisijate nimekiri
[21] Society for Worldwide Interbank Financial Telecommunication
[22] Korporatsiooni sisene reeglistik

või üksikisikutel süsteemile juurdepääsu õiguse kasutamisel, ning koostama ettepanekuid probleemide ühiseks lahendamiseks.

Vaatamata asjaolule, et turvameetmete osas suuri probleeme ei täheldatud, erinevad rakendatud turvameetmed liikmesriigiti suuresti, seega soovitab tollikonventsiooni ühine järelevalveasutus kõigil liikmesriikide pädevatel asutustel võtta üle AFIS Security Policy

Schengeni Ühine Järelevalveasutus

Andmekaitse Inspektsioon osales aruandeperioodil küll veel vaatlejana, kuid järgmisest aastast juba täieõigusliku liikmena, Schengeni konventsiooni ühise järelevalveasutuse (*Schengen Joint Supervisory Authority* ehk *Schengen JSA*) töös. Ühine järelevalveasutus vastutab Schengeni konventsiooni kohaselt loodud Schengeni infosüsteemi – SIS-i, tehnilise abi üksuse järelevalve eest. Samuti on Schengeni ühine järelevalveasutus pädev läbi vaatama Schengeni infosüsteemi tegevusega seotud rakendamis- või tõlgendamisküsimusi, uurima probleeme, mis konventsiooniosalistel siseriiklikel järelevalveasutustel sõltumatu järelevalve teostamisel või süsteemile juurdepääsu õiguse kasutamisel võivad tekkida, ning koostama ühtlustatud ettepanekuid olemasolevate probleemide ühiseks lahendamiseks.

Aruandeperioodil jätkas Schengeni konventsiooni Ühine Järelevalveasutus 2006. aasta juunis alustatud Schengeni konventsiooni artikkel 99 kohaste SIS-i sisestatud teadete ühisinspekteerimist.

Ühisinspkteerimise tulemusel valmis raport, mille kohaselt on konventsiooniosaliste praktika artikkel 99 teadete kasutamisel väga erinev, osad konventsiooniosalised on SIS-i sisestanud mitmeid tuhandeid artikkel 99 teateid, samas kui teised mitte ühtegi. Raporti põhjal leidis ühine järelevalveasutus, et konventsioonis viidatud “äärmiselt rasked õigusrikkumised” tuleb täpsemalt määratleda, näiteks tuleks määratlus siduda Euroopa vahistamismääruse kohaldamisalasse kuuluvate kuritegudega.
Raportis keskenduti ka küsimusele, millistel liikmesriikide siseriiklikel andmekaitse järelevalveasutustel on üldse pädevus riigi julgeoleku eest vastutavaid asutusi kontrollida. Prantsuse ja Portugali siseriiklikel andmekaitse järelevalveasutustel selline pädevus puudub. Vastavate juurdepääsulubade olemasolu korral saavad riigi julgeoleku eest

vastutavaid asutusi kontrollida Belgia, Soome, Rootsi, Šveitsi ja föderaaltasandil ka Saksa siseriiklikud andmekaitse järelevalveasutused.

Teine Schengeni konventsiooni artikkel, mille tõlgendamisele, siseriiklikule rakendamisele ja praktikale Schengeni konventsiooni ühine järelevalveasutus aruandeperioodil keskendus oli konventsiooni artikkel 111.

2006. aasta oktoobris esitas Schengeni konventsiooni ühine järelevalveasutus konventsiooniosalistele küsimustiku, milles sooviti teada millised on need siseriikliku õiguse alusel pädevad asutused. Esitatud vastuste põhjal koostati artikkel 111 vaatlusraport. Schengeni konventsiooni ühine järelevalveasutus leidis raportis, et kooskõlas konventsiooni artiklis 106 sätestatud nn „omaniku printsiibiga" peavad konventsiooni artikkel 111 viidatud kohtute või siseriikliku õiguse alusel pädevate asutuste tehtud lõplike otsuste alusel SIS-is sisalduvad teated parandama, kustutama või selle kohta teavet või kompensatsiooni andma ikkagi teate esitanud konventsiooniosalised. Samas ei pruugi teate esitanud konventsiooniosalised kohtute või siseriikliku õiguse alusel pädevate asutuste tehtud lõplikest otsustest üleüldse teadlikud olla. Seega tuleks konventsiooniosaliste siseriiklikku õigust muuta selliselt, et siseriiklikud andmekaitse järelevalveasutused, juhul, kui nad ei ole ise eelmainitud pädevad asutused, oleksid kohtute või muude pädevate asutuste artikkel. 111 kohastest otsustest teadlikud. Seega peaks siseriiklikus õiguses eksisteerima selline teavitamiskohustus. Samuti peaks eksisteerima teate sisestanud konventsiooniosalise kaasamise kohustus.

Lisaks eeltoodule andis Schengeni konventsiooni ühine järelevalveasutus aruandeperioodil mitmeid arvamusi uue Schengeni infosüsteemi ehk SIS II rakendusmeetmete ja uue SIRENE manuaali eelnõude kohta ning lahendas mitmeid teisi konventsiooniga seotud rakendamis- või tõlgendamisküsimusi.

Euroopa Liidu andmekaitse järelevalveasutuste töörühm politsei ja justiitsküsimustes (Working Party on Police and Justice ehk WPPJ)

Kuna Euroopa Liidu sise- ja justiitsküsimuste valdkonnas on viimasel ajal tehtud mitmeid isikuandmete töötlemist puudutavaid ja isikute põhiõigusi ja vabadusi, eelkõige õigust era- ja perekonnaelu puutumatusele, piiravaid algatusi ning sise- ja justiitsküsimuste

puhul puudub iseseisev ja sõltumatu nõuandev organ, kes tegeleks andmete ja eraelu kaitsega, nagu seda I samba puhul on direktiivi 95/46/EC art. 29 alusel moodustatud töörühm, siis otsustasid siseriiklike andmekaitse järelevalveasutuste juhid 2007. aasta mais toimunud Küprose konverentsil luua siseriiklike andmekaitse järelevalveasutuste esindajatest koosneva Euroopa Liidu andmekaitse järelevalveasutuste politsei töörühma (*Police Working Party*) baasil, iseseisev ja sõltumatu nõuandev organ - Euroopa Liidu andmekaitse järelevalveasutuste töörühm politsei ja justiitsküsimustes (*Working Party on Police and Justice* ehk *WPPJ*).

Töörühma ülesandeks on monitoorida Euroopa Liidu sise- ja justiitsküsimuste valdkonnas toimuvaid arenguid ja algatusi, mis võivad riivata isikute põhiõigust era- ja perekonnaelu puutumatusele ning pöörata tähelepanu, et algatuste raames võetud meetmed võtaksid arvesse kõiki olulisi privaatsuse ja andmekaitse reegleid ja garantiisid, mida pakub Euroopa andmekaitsealane õiguslik raamistik, Euroopa Nõukogu Euroopa inimõiguste ja põhivabaduste kaitse konventsioon, isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (konventsioon 108), Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta ning Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris ning kindlasti ka Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni teatud tingimusi täpsustavat Euroopa Nõukogu ministrite komitee 17. septembri 1987. aasta soovitus R (87) 15, mis reguleerib isikuandmete kasutamist politsei valdkonnas.

Euroopa Liidu andmekaitse järelevalveasutuste töörühma politsei ja justiitsküsimustes esimeseks ülesandeks oli vastu võtta töörühma protseduurireeglid, mida ka tehti.

Aruandeperioodil keskendus töörühm eelkõige kahele põhiteemale - Euroopa Nõukogu raamotsuse eelnõule politseikoostöö ja kriminaalasjade õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta (COM 2005 475) ning Euroopa Nõukogu otsuse eelnõule ning hilisemale otsusele, mis käsitleb piiriülese koostöö tõhustamist, eelkõige seoses terrorismi ja piiriülese kuritegevusega. Prümi konventsiooni Euroopa Liidu õigusesse inkorporeerimist puudutavat Euroopa Nõukogu otsuse eelnõud.

Euroopa Nõukogu otsuse eelnõu ning hilisema otsuse, mis käsitleb piiriülese koostöö

tõhustamist, eelkõige seoses terrorismi ja piiriülese kuritegevusega, kohaselt inkorporeeriti Euroopa Liidu õigusesse Prümi konventsiooni põhielemendid. 27. mail 2005.aastal sõlmiti Belgia Kuningriigi, Saksamaa Liitvabariigi, Hispaania Kuningriigi, Prantsuse Vabariigi, Luksemburgi Suurhertsogiriigi, Madalmaade Kuningriigi ja Austria Vabariigi vahel Prümi konventsioon piiriülese koostöö tõhustamiseks eelkõige seoses terrorismi-, piiriülese kuritegevuse ja ebaseadusliku rände vastase võitlusega, mis kohustas konventsiooniosalisi tagama võrdlusandmete kättesaadavuse teistele konventsiooniosalistele oma riiklikest DNA, sõrmejälgede, sõidukite registreerimisandmete ja ka muudest registritest. Eelmainitud seitse algset konventsiooniosalist esitasid ettepaneku võtta Prüm Euroopa Liidu III samba õigusesse üle, Euroopa parlament andis sellele mittesiduva arvamuse ning Nõukogu võttis otsuse vastu.

Aruandeperioodil koostas töörühm arvamuse eelmainitud otsuse eelnõu ja ka hilisema otsuse alusel koostatud rakendusotsuse eelnõu kohta.

Andmekaitse Inspektsiooni plaanid järgnevaks perioodiks

Ka järgneval perioodil jätkab Andmekaitse Inspektsioon sarnaste märksõnade egiidi all - teadlikkuse tõstmine ja koostöö arendamine riigi- ning kohalike omavalitsuste asutustega. Eesmärgiks jääb endiselt isikutele võimaluse andmine oma õiguste rakendamiseks ning töötlejatele ja teabevaldajatele teadmuse andmine andmekaitse nõuete paremaks rakendamiseks oma kohustuste täitmisel. Teadlikkuse tõstmine on järgnevaks tegevusperioodiks kavandatud läbi erinevate teabe- ja juhendmaterjalide avaldamise meedia vahendusel.

Aruandlusperioodi lõpul asusime kavandama 28. jaanuaril 2008. aastal tähistatava Rahvusvahelise Andmekaitse päeva konverentsi, mis oma järjekorras oli teine. Esimene konverents toimus 2007.aastal ja kandis nime “Isikuandmete kaitse ja E- Riik”, seekordsel tähtpäeva konverentsil seoti isikuandmete kaitse teema meedia küsimustega.

Aruandeperioodil tõusetunud valdkonnad kajastuvad Andmekaitse Inspektsioon järgmise aruandeperioodi valdkonna prioriteetidena, milleks on isikuandmete töötlemine hotellides, turismifirmades lennupiletite müümisel, krediidiasutustes, maksehäireregistris ja videojärelevalve teostamisel. Samuti tõusetub päevakajalisi teemasid, mille kohta inspektsioon on otsustanud võtta avaliku seisukoha järgmise perioodi jooksul, üheks selliseks teemaks, mis tänaseks on jõudnud laiemat kõlapinda pälvida, on sünnipäevaõnnitluste edastamine meedia vahendusel. Nimetatud ja jooksvalt tõusetuvatel teemadel avaldatakse soovituslikud juhised.

Oleme planeerinud jätkuvalt rääkida noorte inimestega nende kodanikuks olemisest ning üheks eesmärgiks selles oleme seadnud panna noori inimesi mõtlema selle üle, kui palju ning milliseid andmeid ja pilte nad enese kohta Interneti keskkondadesse laadima peaksid.

Sarnaselt vaadeldavale perioodile, mil inspektsioon võttis erilise tähelepanu alla apteegiteenuse osutajad, kellel on seadusest tulenev kohustus delikaatsete isikuandmete töötlemine registreerida, planeerime võtta vaatluse alla haridusasutused.

Jätkub rahvusvaheline koostöö andmekaitse valdkonna asutuste ja teiste riikide andmekaitse järelevalve asutustega.

Kokkuvõte

Oma eelmise aruandeperioodi ettekandes isikuandmete kaitse seaduse ja avaliku teabe seaduse täitmisest, seadis Andmekaitse Inspektsioon järgneva tegevusperioodi märksõnadeks avalikkuse teadlikkuse tõstmise ja hea haldustava arendamise, sh haldussuutlikkuse tõstmise.

Tulenevalt neist märksõnadest koostati 2007.aasta tegevusperioodid, milledest ettekandes ülevaade anti. Valitud meede oli igati tõhus ning sellest tulenevalt jätkab Andmekaitse Inspektsioon nimetatud tegevust.

Tervikuna võib tõdeda, et möödunud aruandeperiood oli töömahukas ja osutus tulemuslikuks, täites ootused, mis seati tööplaani koostamisel ja meetmete valimisel selle täitmiseks.

Seega on Andmekaitse Inspektsioon muutunud peamiselt registreerimist teostavast institutsioonist vahetut järelevalvet teostavaks institutsiooniks.

Täna, mil Andmekaitse Inspektsioon asub teises valitsemisalas võrreldes eelmiste aruandlusperioodidega, soovime me avaldada suurt tänu Siseministeeriumile möödunud pikkade aastate jooksul tehtud meeldiva koostöö eest.

Samuti tuleb lausuda tänusõnad õiguskantsler Allar Jõksile ning tema büroole, kes oma ametiajal on Andmekaitse Inspektsioonile möödunud aastate jooksul saatnud mitmeid asjakohaseid märgukirju ning osutanud valdkonnale suurt tähelepanu.

Lisad

Lisa 1.

Isikuandmete edastamine välisriiki

Isikuandmete edastamine piisava andmekaitse tasemega välisriiki

Isikuandmete edastamine Eestis asuvast andmekogust on lubatud riiki, kus on tagatud piisav andmekaitse tase. Andmekaitse piisava taseme saavutamise eelduseks on andmekaitsedirektiivi ehk direktiivi 95/46/EÜ nõuete transponeerimine ning läbi siseriikliku õiguse vastava organisatsioonilise ja õigusliku olukorra loomine, mis võimaldaks isikuandmete töötlemisel austada ja kaitsta isiku eraelu puutumatust ning muid põhiõigusi- ja vabadusi.

Isikuandmete edastamine on lubatud kõikidesse 27-sse Euroopa Liidu liikmesriiki ning Euroopa Majanduspiirkonna lepinguga ühinenud riiki (Norra; Island; Liechtenstein). Ülejäänud välisriikidele viidatakse sageli kui kolmandatele riikidele. Kolmandasse riiki on isikuandmete edastamine lubatud, kui selle riigi isikuandmete kaitse taset on Euroopa Komisjon hinnanud piisavaks. Andmekaitse taset hinnatakse pidades silmas kõiki andmete edastamise toimingute või andmete edastamise toimingute kogumi asjaolusid; tähelepanu pööratakse eelkõige andmete laadile, kavandatud töötlemistoimingu või töötlemistoimingute eesmärgile ja kestusele, päritoluriigile ja lõppsihtriigile, kõnealuses kolmandas riigis kehtivatele nii üldistele kui ka konkreetse sektori õigusnormidele ja kõnealuses riigis järgitavatele ametieeskirjadele ja turvameetmetele.

Euroopa Komisjoni otsused kolmandate riikide andmekaitse taseme tunnustamise kohta leiad siit:

http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

Samas ei tähenda asjaolu, et välisriigis on tagatud piisav andmekaitse tase, seda et sinna võib isikuandmeid piiramatult edastada vaid üksnes seda, et sinna isikuandmete edastamisel ei ole vaja rakendada täiendavaid garantiisid andmesubjekti õigustele ja eraelule. Igal juhul peab ka piisava andmekaitse tasemega riiki isikuandmete edastamiseks eksisteerima õiguslik alus, millisteks isikuandmete kaitse seaduse kohaselt on kas:

andmesubjekti informeeritud nõusolek (IKS § 12). Juhul, kui andmesubjekti isikuandmeid kavatsetakse välisriiki edastada peab isikuandmete vastutav või volitatud töötleja andmesubjektile enne tema isikuandmete töötlemiseks nõusoleku küsimist muuhulgas teatavaks tegema kas asjaolu, et nõusoleku andmisel edastatakse tema isikuandmeid välisriiki.

kui isik, kellele andmed edastatakse, töötleb isikuandmeid seadusega ettenähtud kohustuse täitmiseks (IKS § 14 lg 2 p 1) ;

edastamine on vajalik andmesubjekti või muu isiku elu, tervise või vabaduse kaitseks (IKS § 14 lg 2 p 2).

kui kolmas isik taotleb teavet, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites ja sellele teabele ei ole kehtestatud juurdepääsupiirangut (IKS § 14 lg 2 p 2).

Seega võib piisava andmekaitse tasemega välisriiki isikuandmeid edastada samadel tingimustel kui nende edastamisel Eesti siseselt. Isikuandmete edastamisel tuleb kindlasti tähelepanu pöörata isikuandmete töötleja kohustusele tagada andmete olemasolu isikuandmete edastamise kohta: millal, kellele ja millised isikuandmed edastati, samuti selliste andmete muutusteta säilimine (IKS § 19 lg 2 p 5) ning kohustusele tagada, et isikuandmete edastamisel andmesidevahenditega ja andmekandjate transportimisel ei toimuks isikuandmete omavolilist lugemist, kopeerimist, muutmist või kustutamist (IKS § 19 lg 2 p 5). Samuti tuleb arvestada sihtriigi andmekaitsealast seadusandlust, näiteks võib sihtriigi andmekaitsealase seadusandluse kohaselt olla vajalik sealse andmekaitse järelevalveasutuse teavitamine.

Isikuandmete edastamine piisava andmekaitse tasemeta välisriiki

Andmekaitsedirektiivi ehk direktiivi 95/46/EÜ artikli 26 kohaselt võivad liikmesriigid lubada isikuandmete edastamist või edastamistoimingute kogumit kolmandasse riiki, mis ei taga kaitse piisavat taset artikli 25 lõike 2 tähenduses, kui vastutav töötleja esitab piisavad tagatised üksikisikute eraelu puutumatuse ning põhiõiguste ja -vabaduste kaitse ja vastavate õiguste kasutamise kohta; sellised tagatised võivad tuleneda eelkõige asjakohastest lepingutingimustest.

Isikuandmete kaitse seaduse § 28 lg 4 kohaselt võib isikuandmeid välisriiki, kus ei ole tagatud piisav andmekaitse tase, edastada üksnes Andmekaitse Inspektsiooni loal, kui:

1) vastutav töötleja garanteerib konkreetsel juhul andmesubjekti õiguste ja eraelu kaitse selles riigis;

2) konkreetsel isikuandmete edastamise juhul on riigis tagatud piisav andmekaitse tase. Andmekaitse taseme hindamisel tuleb arvesse võtta isikuandmete edastamisega seotud asjaolusid, sealhulgas andmete koosseisu, töötlemise eesmärke ja kestust, andmete edastamise siht- ja lõppriiki ning riigis kehtivat õigust.

Loa saamiseks tuleb isikuandmete vastutaval töötlejal, kes kavatseb isikuandmeid mittepiisava andmekaitse tasemaga välisriiki edastada (andmeeksportija), esitada Andmekaitse Inspektsioonile alljärgnevad dokumendid ja teave:

Taotlus loa saamiseks isikuandmete edastamiseks kolmandas riigis asuvale isikuandmete töötlejale, millest nähtub taotleja (andmeeksportija) ja kolmandas riigis asuva isikuandmete töötleja (andmeimportija) isik, kolmanda riigi nimetus, andmete edastamise eesmärk ning periood, milliseks luba taotletakse;

Kinnitus selle kohta, et kolmandas riigis asuva isikuandmete töötleja poolt toimub isikuandmete töötlemine eesmärgil ja ulatuses, milleks on olemas õiguslik alus;

Kinnitus selle kohta, et vastutav töötleja garanteerib konkreetsel juhul andmesubjekti õiguste kaitse kolmandas riigis ning et konkreetsel isikuandmete edastamise juhul on riigis tagatud piisav andmekaitse tase (kolmandas riigis asuva töötlejaga sõlmitud lepingu koopia ning muud tõendid ja dokumendid, mida isikuandmete töötleja peab vajalikuks esitada).

Andmekaitse Inspektsioon vaatab vastava taotluse läbi ning annab loa või keeldub põhjendatult selle andmisest 30 päeva jooksul alates taotluse esitamisest. Taotluse läbi vaatamiseks vajalike asjaolude täiendavaks selgitamiseks võib Andmekaitse Inspektsioon taotluse läbivaatamise tähtaega pikendada kuni 60 päeva võrra. Tähtaja pikendamisest teatatakse taotluse esitajale kirjalikult.

Erandid

Andmekaitsedirektiivi 95/46/EÜ kohaselt on keelatud isikuandmete edastamine kolmandatesse riikidesse, kus nende kaitse tase ei ole piisav. Erandid on lubatud juhuks, kui.

a) andmesubjekt on andmete kavandatud edastamiseks andnud oma ühemõttelise nõusoleku või

b) edastamine on vajalik andmesubjekti ja vastutava töötleja vahelise lepingu täitmiseks või andmesubjekti taotlusel võetud lepingueelsete meetmete rakendamiseks või

c) edastamine on vajalik andmesubjekti huvides vastutava töötleja ja kolmanda isiku vahel sõlmitud lepingu sõlmimiseks või täitmiseks või

d) edastamine on vajalik või seaduste kohaselt nõutav üldiste huvidega seotud olulistel põhjustel või õigusnõuete koostamiseks, esitamiseks või kaitsmiseks või

e) edastamine on vajalik andmesubjekti eluliste huvide kaitsmiseks või

f) edastatavad andmed on pärit registrist, mis õigusnormide kohaselt on mõeldud avalikkuse teavitamiseks ja on tutvumiseks avatud laiemale avalikkusele või kõigile õigustatud huvidega isikutele, kuivõrd konkreetsel juhul täidetakse tingimusi, mis õigusaktidega on tutvumiseks ette nähtud.

Sarnaseid erandeid isikuandmete mittepiisava tasemega kolmandatesse riikidesse edastamise keelust sisaldab ka isikuandmete kaitse seadus. Isikuandmete kaitse seaduse § 28 lõike 6 kohaselt võib Andmekaitse Inspektsiooni loata isikuandmeid edastada välisriiki, kus ei ole tagatud andmekaitse piisav tase:

1) kui andmesubjekt on selleks andnud nõusoleku;
2) isikuandmete kaitse seaduse § 14 lõikes 2 sätestatud juhtudel;
3) kui andmed edastatakse välisriiki šifreeritud kujul ning dešifreerimiseks vajalikke andmeid ei viida välisriiki.

Lisa 2.

Ohud ehk võimalused veebiotsingu maailmas

Veebi võib võrrelda hiigelsuure, kuid korrastamata teabekogumiga, mille killukesed on maailma eri paikades laiali, kuigi vajadusel võrgutsi – täpsemalt öeldes vaataja ehk veebisirvija arvutisse – kokku viidavad. Et sellest pealtnäha segadusest midagi üles leida, on tarvis sellele hiigelsuurele tohuvabohule peale ehitada otsisüsteemid, mis seda pealtnäha korratut asja süstematiseerivad ning võimaldavad kasutajal saada kätte just selle teabe, mida ta soovib.

Eelistele lisaks ka ohud

Veebiotsingu võimalustest ja eelistest teame me kõik, kes oleme vähemalt kord-paargi seda kasutanud. Lihtsalt vajalikke märksõnu teades ning veidigi otsimist osates suudame me üsna kiiresti ja mugavalt leida üle kogu maailma üles täpselt need avalikud veebilehed, mis neid teemasid kajastavad. Tihti annab otsing vastuseks liiga palju lehti, kuid kes tunneb täiustatud otsingu eripärasid, see saab kasutada üsna keerulisi otsiskeeme, mis võimaldab siiski üsna täpselt välja õngitseda vaid soovitud lehed. Millised on aga veebiotsingu ohud ning kuivõrd tõsised nad on?

Kolm erinevat ohtu

Suurim otsingu varjukülg on võimalik isiku privaatsuse kadu. Esiteks võib see puudutada veebilehel kajastatud isikut, teiseks aga ka veebis lehitsejat (surfajat). Lisaks mainitutele olemas ka kolmas oht – oht veebiväljundiga infosüsteemi nendele andmetele võimalikule turvakaole.

Oht 1: oht andmesubjekti privaatsusele. Kui te olete aktiivne kodanik ning teie andmeid on paljudel erinevatel veebilehtedel kajastatud, saab potentsiaalne otsija teie nime järgi kogu teie elust üsna korraliku ettekujutuse. Vahel lipsab nii saadud andmete sisse ka selliseid fakte, mis peaksid jääma inimese eraelu saladuseks. Kui ka selliseid fakte seal otseselt ei ole, on siiski inimese eraelu tihti paljus häiritud tänu sünergeetilisele ehk kumulatiivsele efektile – suure hulga faktide omamine, nende kõrvutamine ning sealt järelduste tegemine võimaldab sageli saada teada palju rohkemat, kui seal faktides enestes kirjas on.

Oht 2: oht veebis seilaja privaatsusele. Aktiivne ja teadmistehimuline võrgukodanik, kes vägagi sageli seilab võrgus ning kas kasutab otsisüsteeme mitmete asjade teadasaamiseks, avaldab otsisõnades ja -fraasides tihti väga palju teavet enda, oma eelistuste, eluhoiakute jms kohta. Asjaolu, et serveripoolelt on tihti võimalik teada saada, et päringud tulevad samast arvutist või isegi sama inimese poolt, võimaldab otsisüsteemi haldajatel neid andmed kokku pannes inimese kohta paljutki järeldada.

Oht 3: oht veebiväljundiga infosüsteemi andmetele. Kaasaja veebileht ei ole tavaliselt mitte eraldiseisev kogumik avalikke artikleid/teavet, vaid on tihti mingi suurema

andmebaasi/infosüsteemi väljund, millest vaid osad andmed on mõeldud veebis avalikustamiseks. Kui need tehnilised lahendused, mis nimetatud andmebaasi veebi näitavad, ei ole piisavalt korralikult koostatud, siis on vahel võimalik sealtkaudu andmebaasi sisse tungida. Täpsemalt – nii avalikustamiseks mittemõeldud andmeid vaadata kui ka andmeid omavoliliselt muuta ja kustutada.

Kõikide nende ohtude vastu on olemas üsna toimivad vastumeetmed, kui asjaosalised neid ohte vaid teadvustavad ning suudavad vastavalt tegutseda. Olulist rolli mängivad siin kaks valdkonda:

- veebikeskkonna (veebilehed + otsisüsteemid) erinevus trükimeediumist;
- otsisüsteemide toimimise aluspõhimõtted.

Enamik meetmeid – nii andmesubjekti, andmete töötleja kui ka otsisüsteemi pidaja jaoks – toetuvadki nimetatud valdkondade teadmistele.

Veebikeskkonna erinevus trükimeediumist

Kui mingid andmed on veebis avalikustatud, siis võib neid paljus võrrelda andmetega, mis on avaldatud trükitud meediumis. Samas on nende meediumiliikide vahel ka mitmed erinevused.

Digimeediumi sarnasus trükimeediumiga seisneb selles, et ühe isiku või asutuse poolt avaldatu võib jõuda väga paljude lugejateni ning seda võidakse algallikast edasi tsiteerida. Sealhulgas võivad digimeediumit (st veebilehte) tsiteerida ka paberväljaanded.

Digimeediumi ja trükimeediumi erinevuseks on kõigepealt asjaolu, et igaüks võib veebilehe püsti panna, samal ajal kui ajalehe korral otsustavad toimetajad, kelle artikleid ja millistel tingimustel seal võib avaldada. Põhimõtteliselt on küll võimalik, et serveriteenuse (hostingu) pakkuja kontrollib seal avaldatavaid artikleid ka sisu osas, kuid sellisel tegevusel on kindlad ja konkreetsed piirid.

Kõigepealt võib serveripidajal olla selline teenusepakkumise poliitika, et veebilehtede ülespanijad vastutavad ise oma teabe eest. Samuti ei suuda serveripidaja operatiivselt lisandunud teabe lisamisel tavaliselt sellele hetkeliselt reageerida, mistõttu ebasoovitav teave jõuab seal veebilehel mõnda aega juba üleval olla. Eestikeelses veebikeskkonnas ei ole vähetähtis ka asjaolu, et väljaspool Eestit keegi eesti keelt tavaliselt ei loe – nii võib soovija majutada omaenda veebilehe või veebikeskkonna väljapoole Eestit olevasse serverisse, tagades juba ainuüksi selle faktiga selle, et serveripidaja lehe sisust aru ei saa.

Teiseks erinevuseks trükimeediumi ja veebilehe vahel on lugejate arvu suurem diferentseerumine – üht veebilehte võivad lugeda nii mõned inimesed kui ka mõned miljonid. Kolmandaks on võimalik digimeediumi (veebilehte) erinevalt trükitud ja levitatud ajalehest ka muuta või kustutada, st see ei pruugi olla püsiv

Neljandaks korrastavad (indekseerivad) kõiki – või vähemalt valdavat enamikku veebilehti – mitmesugused otsisüsteemid. Tavaliselt leiab lugeja vastava artikli või veebilehe üles just otsisüsteemide kaudu.

Otsisüsteemide aluspõhimõtted

Otsisüsteemide osas on kaasajal "jäme ots" rahvusvaheliste süsteemide käes, mingi riigi, keelepiirkonna, kultuuri vm põhised lokaalsed süsteemid jäävad neist maha. Hetkel juhib suure edumaaga *Google* (*www.google.com*), millel järgnevad teatud vahega kobaras koos nii *Yahoo* (*www.yahoo.*com), *LiveSearch* (*www.live.com*), *Clusty* (*www.clusty.com*) kui ka mitmed teised. Valdav enamik neist asub füüsiliselt USAs, riigis kust nii Internet kui ka veeb alguse sai ja kus ta kõige rohkem arenenud on.

Üks üleilmne otsisüsteem kujutab endast tavaliselt üht suurt viidete hulka erinevatele veebilehtedele, millele lisandub avalike lehtede kopeeritud sisu, mis on korrastatud erinevate märksõnade järgi.

Inimene nimetatud protsessi tavaliselt ei sekku, sellega tegeleb spetsiaalne tarkvara, mida nimetatakse **otsirobotiks**. Otsiroboti ülesandeks on otsida veebist avalikke lehti, need endale alla laadida, korrastada/indekseerida vastavalt märksõnadele ning salvestada andmebaasi. Inimese abistav roll piirdub tavaliselt sellega, et vajadusel saab otsirobotile käsitsi ette anda veebilehe (mingi süsteemi pealehe) aadressi, kust robot "teab" hakata otsinguid alustada. Kui uue lehega koos tekivad vastavad viited juba olemasolevatele (ja roboti jaoks juba tuttavatele) lehtedele, siis sellist käsitsi lisamist vaja ei ole – robot leiab lisandunud lehe sedakaudu iseseisvalt üles.

Seega otsisüsteemid ei muuda veebis avalikustatud teavet ega tee midagi muud, kui korraldavad ja organiseerivad veebi avalikult väljapandud teavet seda omapoolselt muutmata. Kuna arvutisüsteemid – sh ka otsirobot – inimkeelsest tekstist aru ei saa, ei "tea" ei otsirobot ega ka otsisüsteem tavaliselt ka midagi veebilehe sisust: ta vahendab ja korrastab vaid teatud märkide "jorusid".
Kui veebileht on kustutatud või muutunud, siis otsisüsteem reageerib sellele tavaliselt väikese hilinemisega, milleks on tavaliselt ajavahemik nädalast kuni mõne kuuni. Umbes selle ajaga suudab robot läbi käia ja üle kontrollida kõik varemleitud ja korrastatud leheküljed. See periood on tavaliselt paika pandud otsisüsteemi taga olevate arvutite võimsusega, mistõttu seda ei õnnestu tavaliselt ei andmesubjektil ega ühelgi välisel subjektil omapoolselt kiirendada.

Enamik globaalseid süsteeme on muide huvitatud selle perioodi lühendamisest – st efektiivsemast ja dünaamilisemast toimimisest –, kuid oma piiri seavad siin arvutiressursid. Tuleb arvestada, et paljude veebilehtede teabe korrastamine ja struktureerimine on meeletut arvutusressurssi nõudev tegevus, mis paneb toimimiskiirusele peale omad ajalised piirid. Lõppkokkuvõttes taandub see rahale. Näiteks maailma üheks parimaks üleilmseks otsisüsteemiks peetav *Google* viitab praegu

umbes 16 miljardile leheküljele; tema kannul olevad otsisüsteemid *Yahoo*, *LiveSearch*, *Clusty* jt aga ka juba miljarditele lehtedele.

Andmesubjekti privaatsuskao riski vähendamine

Peamine skeem, kuidas veebikeskkond koos otsisüsteemidega teie kui andmesubjekti privaatsust kahjustab on järgmine. Keegi paneb oma veebilehele üles andmeid, mis teie privaatsust kahjustab, misjärel globaalsed otsisüsteemid vahendavad seda teavet kõigile soovijatele.

Kui see on toimunud, oleks teil mõistlik keskendada enamik oma energiast algallika muutmisele või kõrvaldamisele, mitte aga otsisüsteemidele. Kui veebileht asub Eesti keskkonnas, on selle kõrvaldamine või muutmine tavaliselt juriidiliselt üsnagi lihtne tegevus, sest Eesti Vabariigi territooriumil kehtivad Eesti Vabariigi seadused.

Kui leht asub aga mingis väljaspool Eestit olevas serveris, võib selle muutmine või kõrvaldamine olla küllaltki tülikas, sest vajab tihti rahvusvahelist protsessi. Mingis välisriigis teenust pakkuv firma ei pruugi reageerida Eesti eraisikute ja ametiasutuste vastavasisulistele järelepärimistele mitte kuidagi.

Tasub tähele panna, et igasugused seadused, järelepärimised jms on senini maailmas vägagi riigipiiri-tundlikud protsessid, samal ajal kui võrgus (Internetis) liikuv teave riigipiire ei tunne ning lisaks ei võimalda võrgu tehniline ülesehitus selliseid piire ka seada.

Arvestada tuleb, et kui te olete oma privaatsust riivava teabe suutnud algallikast kustutada, võivad seda olla juba tsiteerinud nii teised veebilehed kui ka trükiväljaanded. Kui see on juhtunud, peate oma energia suunama ka seal oleva teabe kõrvaldamisele, kui see enam võimalik on.

Ning lõpuks tuleb teadvustada, et kui teave on algallikast (veebilehelt) kustutatud, siis jäävad otsisüsteemid seda mõnda aega (tavaliselt nädalast mõne kuuni) veel tsiteerima. Harilikult tuleb andmesubjektil see periood lihtsalt ära kannatada, kuna otsisüsteemi taga oleva piiratud arvuti- ja inimvõimsuse tõttu ei suudeta seal olevat teavet lihtsalt kiiremini uuendada – ärgem unustagem, et just nimetatud ressurss on kaasajal kõikide otsisüsteemide kitsaskohaks.

Paljudel üleilmsetel otsisüsteemidel on olemas ka koht, kus saab teatada valest või muutunud lehtedest, eemaldamist vajavatest lehtedest vms. Nende linkide kasutamine ei pruugi seda protsessi aga kiirendada – põhjuseks ikka seesama ressursside nappus otsisüsteemi pool, sest kolossaalse hulga teabekogumite korrastamine nõuab ka kolossaalseid ressursse. Võrdluseks – kui näiteks teie isiklikku postkasti laekuks ühel päeval ootamatult näiteks mõni tuhat kiiret vastamist vajavat kirja, jääksite te tõenäoliselt samuti vastamisega hätta.

Kokkuvõttes – digimeediumis kord juba avalikult avaldatud teabe hilisem "tagasivõtmine" on tihtipeale loterii. See õnnestub vaid juhul, kui vastaval veebilehel ei olnud väga palju lugejaid ning seda lehte ei tsiteeritud teiste meedialiikide poolt. Ning ka sel juhul tuleb arvestada väikese puhverajaga nädalast mõne kuuni, mille jooksul suudab otsisüsteemide robot oma teabebaasi uuendada. Kui aga veebis avalikustatud teave on osutunud bestselleriks ning seda on palju viidatud/tsiteeritud, siis sellise teabe eemaldamine võrgust on praktiliselt võimatu.

Selsamal põhjusel peaks iga andmetöötleja võtma isikuandmeid sisaldava teabe veebis avalikustamist vägagi tõsiselt – tegu on protsessiga, mida tihtipeale enam tagasi võtta ei saa.
Ega asjata ei öelda, et parim viis andmetest hävimatut varukoopiat teha on andmed võimalikult laialdaselt veebis avalikustada. **Seega – enne, kui panete kellegi isikuandmeid veebilehele välja, mõelge, kas see teguviis on kooskõlas kehtivate isikuandmete kaitse põhimõtetega.**

Veebis seilaja privaatsuskao riski vähendamine

Igast Internetis tehtud päringust jääb maha hulk nn metateavet (nt arvuti võrguaadress jm), mis võib otsisüsteemi sisemises keskkonnas alles jääda ning avada paljutki seilaja isikuomaduste, eelistuste jm kohta nende jaoks, kes sellele teabele otsisüsteemi pool ligi pääseb.

Kaasajal on rahvusvahelisel tasemel otsisüsteemidele juba üsna palju ette kirjutatud, milliseid otsinguandmeid, kui pikalt ja millise detailsusega ning seostatusega võivad nad ülepea säilitada ning kes seda teavet võib vaadata.

Lähitulevikus on seoses otsisüsteemide ja temaatiliste kataloogide arenguga võimalikud mitmed arengud, mida prognoosida on raske. Esiteks – kui "maailma suured" suudavad temaatilise kataloogi tegemise ülimahuka käsitsitöö kuidagi vähegi efektiivselt automatiseerida, siis võib ka see võrgukorrastamise turuosa minna väiksemate tegijate käest ära.

Teisest küljest – kui arvutile ja veebikorrastussüsteemidele suudetakse selgeks õpetada näiteks eesti keele grammatika (nt otsisõna kõikvõimalikud grammatilised vormid), võib see väiksemate otsisüsteemide osatähtsust ja võimekust hoopis tõsta.

Kokkuvõttes võiks otsisüsteemide agaratele kasutajatele soovitada siiski aeg-ajalt mõelda, kas ning milliseid asju saab tema kohta otsifraaside põhjal järeldada. Seda kasvõi põhjusel, et tavaliselt on kogu side kasutaja poolt kuni otsisüsteemini turvamata ning lisaks otsisüsteemile endale näeb kogu seda teavet ka juhuslik pahatahtlik häkker (kes kuulab nt turvamata traadivaba sidet pealt). Loomulikult – kui kasutada otsinguks erinevaid arvuteid; mingi asutuse/firma vahendusservereid, mille taga on terve "tulemüüristatud" alamvõrk; fikseerimata IP-aadressiga ADSL-ühendust jt, siis on seda teavet killukeste põhjal väga raske kokku panna ja risk on üsna olematu.

Ohud veebiväljundiga infosüsteemi andmetele

Veebiväljundiga infosüsteemide korral koostatakse veebileht mitte ühe kindla inimese (veebiadministraatori) poolt, vaid automaatselt asutuse infosüsteemi teatud osadest, mis vajavad avalikustamist. Seepärast ei saa sellistel juhtudel lugeda andmete publitseerijaks mitte üht inimest, vaid paljusid Teie infosüsteemiga seotud isikuid või mõningatel juhtudel isegi automaatset infotöötlussüsteemi ennast (kui veebiväljundiga andmed võetakse automaatselt mingist välisest andmekogust ilma inimese otsese sekkumiseta). Selliste süsteemide korral võib anda kaks peamist riski maandavat soovitust.

Esimene soovitus on hoida oma andmebaas ja sellele ehitatud välise veebi rakendused (info)tehnilise poole pealt kaasaegsel turbetasemel. Viimastel aastatel on olnud väga palju juhuseid, kus tehnilist oskusteavet valdav ründaja suudab asutuse veebiliidese kaudu infosüsteemist "välja meelitada" ka selliseid andmeid, mida algselt ei olnud mõeldud veebis avalikustada.

Kui keegi häkkeritest on sellise "augu" üles leidnud ning selle kaudu mingeid avalikustamisele mitte mõeldud andmeid veebitsi "välja meelitanud", siis ka neid andmeid võivad veebi otsisüsteemid võimendada.

Otsisüsteemid "ei tea", kas need andmed, mida mingi veebiväljundiga süsteem avalikkusele välja annab, olid algselt mõeldud avalikustamiseks või ei – ta indekseerib reeglina kõik need andmed, mille ta leiab olevat avalikult välja pandud, levitades automaatselt viiteid nendele andmetele kõigile soovijatele. Sellisel juhul ei saa süüdistada mitte otsisüsteemi, vaid siiski veebiväljundiga infosüsteemi kui andmete algset allikat otsisüsteemi suhtes.

Teine soovitus on hoida korras veebiväljundiga infosüsteemide andmehõive. Sellise süsteemi omaniku/haldaja poolt **oleks mõistlik analüüsida oma andmete liikumise äriloogikat ning fikseerida selles kõik võimalikud teed ja viisid, kuidas võivad selles võimalikud isikuandmed sattuda lõppkokkuvõttes teie veebilehele.** Sellise analüüsi tulemusena saab fikseerida nende isikute ja/või protsesside ringi, kelle või mille tegevuse tulemusena isikuandmeid veebis avalikustada võidakse (ja mille avalikustamist otsisüsteemid võimendavad).

Nimetatud analüüsi tulemus tooks selgelt välja nende isikute/ametnike ringi, keda peaks asutuse sees kehtivate õigusaktide ja isikuandmete kaitse heade tavade osas kindlasti koolitama ja teavitama.

Lisa 3.

TELEFONIKÕNEDE LINDISTAMISE LUBATAVUS

Taust

Õigus eraelu kaitsele, mille üheks osaks on õigus sõnumisaladusele, kuulub Euroopa Liidu põhiõiguste hartas tunnustatud põhiõiguste hulka. Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivis 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, kohustatakse liikmesriike tagama füüsiliste isikute õigused ja vabadused, eelkõige õigus eraelu puutumatusele isikuandmete töötlemisel, et seega tagada isikuandmete vaba liikumine ühenduses.

Euroopa Parlamendi ja nõukogu 12. juuli 2002 aasta direktiivis 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side valdkonnas, austatakse põhiõigusi ja selles järgitakse eelkõige Euroopa Liidu põhiõiguste hartas tunnustatud põhimõtteid. Side konfidentsiaalsus tagatakse inimõigusi käsitlevate rahvusvaheliste dokumentide (eelkõige inimõiguste ja põhivabaduste kaitse Euroopa konventsiooni) ja liikmesriikide põhiseaduste kohaselt.

Direktiivi 2002/58/EÜ art 5 sätestab, et liikmesriigid tagavad üldkasutatava sidevõrgu ja üldkasutatavate elektrooniliste sideteenuste kaudu toimuva side ja sellega seotud liiklusandmete konfidentsiaalsuse siseriiklike õigusaktidega. Eelkõige keelatakse nende siseriiklike õigusaktidega isikutel, kes ei ole sideteenuse kasutajad, kuulata, salaja pealt kuulata, salvestada või muul viisil pealt kuulata või jälgida sidet ja sellega seotud liiklusandmeid ilma asjaomaste kasutajate loata. See nõue ei mõjuta seadusega lubatud side ja liiklusandmete jäädvustamist õiguspärase äritegevuse käigus selleks, et esitada tõendeid äritehingu või muu äritegevusega seotud side kohta. Samuti peavad olema ette nähtud erisused juhul, kui side ja liiklusandmete jäädvustamine on vajalik kuriteo tõkestamiseks või uurimiseks. Liikmesriigid tagavad, et elektrooniliste sidevõrkude kasutamine teabe salvestamiseks või juurdepääsuks abonendi või kasutaja lõppseadmesse salvestatud teabele on lubatud ainult tingimusel, et asjaomasele abonendile või kasutajale esitatakse direktiivi 95/46/EÜ kohaselt selge ja arusaadav teave muu hulgas andmete töötlemise eesmärgi kohta ning talle antakse võimalus keelduda vastutava andmetöötleja teostatavast töötlemisest.

Direktiivi 2002/58/EÜ seletuskiri täpsustab, et igasuguse andmeedastuse puhul peab kehtima tingimus, et andmeid võib kasutada ainult sel otstarbel, milleks need on kogutud. Kui osaline, kes on kogunud andmeid abonendilt, või kolmas isik, kellele on andmed edastatud, soovib kasutada andmeid mõnel muul otstarbel, peab kas andmete esmakoguja või kolmas isik, kellele andmed on edastatud, saama abonendilt uue nõusoleku.

Abonentide kohta käivad andmed, mida töödeldakse elektroonilistes sidevõrkudes ühenduse loomiseks ja teabe edastamiseks, sisaldavad teavet füüsiliste isikute eraelu kohta. Selliseid andmeid võib säilitada ainult sel määral, kui on vaja teenuse osutamise puhul arveldamiseks ja sidumistasude maksmiseks, ning piiratud aja jooksul. Selliste andmete igasugust täiendavat töötlemist, mida üldkasutatavate elektrooniliste sideteenuste osutaja võib soovida teha elektrooniliste sideteenuste turustamiseks või lisaväärtusteenuste osutamiseks, võib lubada ainult siis, kui abonent on sellega nõustunud

täpse ja täieliku teabe põhjal, mille üldkasutatavate elektrooniliste sideteenuste osutaja on talle edastanud, kavandatud täiendavate töötlemisviiside kohta ja abonendi õiguste kohta jätta oma nõusolek selliseks töötlemiseks andmata või tühistada selline nõusolek.

Ka artikkel 29 töögrupp[23] on arvamusel, et esiletõstmist väärib õigus konfidentsiaalsusele üldkasutatavate elektrooniliste sideteenuste kasutamisel. Samuti kasvab eravõrkude tähtsus igapäevaelus üha enam ja sellest tulenevalt suurenevad ka ohud privaatsusele, seda eriti seetõttu, et sellised võrgud on muutunud üha spetsiifilisemaks (nt töötajate käitumise jälgimine liiklusandmete põhjal). Samuti muutuvad teenused üha enam avalike ja erateenuste kombinatsiooniks.

EV põhiseadus sätestab §-s 26, et igaühel on õigus privaatsuse kaitsele. Koos õigusega era- ja perekonnaelu kaitsele vaadeldakse ka EV põhiseaduse §-s 43 sätestatud igaühe õigust tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele. Sõnumisaladust võib piirata vaid kriminaalmenetluse seadustikus, jälitustegevuse seaduses ja julgeolekuasutuste seaduses sätestatud alustel.

Isikuandmete kaitse seadus sätestab §-s 4 lõikes 1, et isikuandmed on kõik andmed, mille alusel on võimalik isikut tuvasta ja §-s 5, et isikuandmete töötlemine on iga isikuandmetega tehtav toiming.

Isikuandmete kaitse seaduse § 14 sätestab, et isikuandmete töötlemine on lubatav ilma isiku nõusolekuta, kui isikuandmeid töödeldakse:

1) andmesubjektiga sõlmitud lepingu täitmiseks või lepingu täitmise tagamiseks;

Näiteks vastavalt elektroonilise side seaduse §-le 104 võib sideettevõtja kliendi nõusolekuta töödelda ja säilitada andmeid sideteenuse kasutamise üksikasjade kohta, sidevõrgu kaudu edastatava sõnumi sisu ja vormi kohta, andmeid sõnumi edastamise aja ja viisi kohta, kui see on vajalik kliendile arve esitamiseks, sealhulgas sidumistasude kindlaksmääramiseks ja arvestamiseks. Siinjuures peab järgima isikuandmete kaitse seaduse §-s 6 sätestatud isikuandmete töötlemise põhimõtteid, sh minimaalsuse printsiipi, eesmärgikohasuse printsiipi jt. Elektroonilise side seadus sätestab täiendavalt, et sideettevõtja peab tagama sidevõrgu turvalisuse ning mitte võimaldama kolmandatel isikutel pääseda ilma seadusliku aluseta ligi andmetele sideteenuse kasutamise üksikasjade kohta, sidevõrgu kaudu edastatava sõnumi sisu ja vormi kohta, andmetele sõnumi edastamise aja ja viisi kohta. Samuti on sideettevõtja kohustatud hoidma saladuses kõiki talle sideteenuse osutamise käigus teatavaks saanud andmeid kliendi ja teiste isikute kohta, kes ei ole sõlminud lepingut sideteenuse osutamiseks, ent kes kasutavad sideteenust kliendi nõusolekul, eelkõige: andmeid sideteenuse kasutamise üksikasjade kohta; sidevõrgu kaudu edastatava sõnumi sisu ja vormi kohta; andmeid sõnumi edastamise aja ja viisi kohta.

2) andmesubjekti või muu isiku elu, tervise või vabaduse kaitseks;
Näiteks on tegemist olukorraga, kus kõne vastuvõtmise aeg on aegkriitiline, sest sellest võib sõltuda isikute elu ja/või tervis. Siin võib tulla kõne alla nt hädaabinumber, kiirabi jms.

[23] Artikkel 29 on andmekaitse töögrupp, mis on loodud Direktiiv 95/46/EÜ alusel.

3) seaduse või välislepinguga ettenähtud ülesande täitmiseks.
Näiteks sõnumisaladust võib piirata juba viidatud kriminaalmenetluse seadustikus, jälitustegevuse seaduses ja julgeolekuasutuste seaduses sätestatud alustel.

Muudel juhtudel võib isikuandmeid töödelda üksnes isiku enda nõusolekul.

Samuti tuleb isiku nõusolek võtta juhul, kui andmetöötluse eesmärk võrreldes esialgsega muutub nt toimub telefonikõnede lindistamine klienditeeninduse taseme kontrolliks ja pretensioonide lahendamiseks, mille eesmärk on asutuse klienditeeninduse taseme hoidmine ja parandamine.

Andmekaitse Inspektsiooni poolt teostatud järelevalve

Ülaltoodust selgub, et telefonikõnede lindistamine on sõnumisaladuse kontekstis puutumuses eraelu kaitsega. Eesmärgiga kaardistada Eesti Vabariigis suhteliselt uudne valdkond ja selle tulemusel anda soovitusi isikuandmete paremaks kaitseks telefonikõnede lindistamisel, viis Andmekaitse Inspektsioon läbi omaalgatuslikud kontrollid asutustes ja ettevõtteis.

Kontrolliti järgmiseid ettevõtteid ja asutusi:
AS Eesti Energia, Sotsiaalkindlustusamet, Eesti Haigekassa ja Häirekeskus.

Selgunud telefonikõnede salvestamise eesmärgid:
Kõik kontrollitud asutused salvestavad ainult kõnekeskusse saabuvaid kõnesid. Kõik kontrollitud asutused tõid telefonikõnede salvestamise eesmärgina välja vajaduse kontrollida kõnekeskuse töö kvaliteeti. Täiendava eesmärgina toodi välja kõnesalvestiste kasutamine klientide pretensioonide korral. Vastavalt eriala spetsiifikale kasutatakse lisaks eelpool mainitud eesmärkidele kõnesalvestisi Häirekeskuses helistaja tervisliku seisundi tuvastamiseks.

Salvestatavate isikuandmete koosseis:
Kõik kontrollitud asutused töötlevad isikuandmeid, eesmärgiga helistajat identifitseerida. Näiteks AS Eesti Energia identifitseerib kliendi isikukoodi alusel. Sotsiaalkindlustusamet ja Häirekeskus töötlevad lisaks isikuandmetele ka delikaatseid isikuandmeid. Sotsiaalkindlustusamet töötleb andmeid puude raskusastme kohta ning Häirekeskus helistaja tervisliku seisundi tuvastamiseks.

Andmesubjekti ja töötajate teavitamine:
Ükski kontrollitud asutustest ei teavita kõne alguses andmesubjekti, et käesolev kõne salvestatakse. AS Eesti Energia teavitab andmesubjekti kliendilepingu tüüptingimuste kaudu.

Kõigi kontrollitute sõnul on töötajad, kelle kõnesid lindistatakse lindistamisest teadlikud. Samas on töötajaid teavitatud suuliselt. AS Eesti Energia töötajad on allkirjaga kinnitanud, et on teadlikud kõnede lindistamisest.

Telefonikõnede salvestiste säilitamine:
Säilitamise tähtajad on erinevad ja jäävad vahemikku 1-3 kuud (Eesti Haigekassa, Sotsiaalkindlustusamet ja AS Eesti Energia) kuni 1 aasta (Häirekeskus). Häirekeskus säilitab salvestisi 3 kuud, misjärel need arhiveeritakse 1 aastaks. Selline pikem säilitamise

periood on vajalik, kuna julgeolekuasutustel on seaduslik õigus vajadusel 1 aasta jooksul salvestisi kasutada.

Ligipääs salvestistele:
Kõikides kontrollitud asutustes on salvestistele ligipääs võimaldatud ainult töötajatele, kelle tööülesannete täitmiseks see on vajalik.

Tähelepanekud:
Eesti Haigekassa, Sotsiaalkindlustusameti ja Häirekeskuse puhul ei ole tegemist süsteemse isikuandmete töötlemisega. Isikuandmed satuvad kõnesalvestistele juhul, kui helistaja annab need omal algatusel või on helistaja identifitseerimine hädavajalik. Näiteks küsitakse Häirekeskuses isiku nime ainult siis, kui isik asub maapiirkonnas ning kiirabil võib tekkida vajadus tuvastada isiku elukoht kolmanda isiku kaudu.

Enamus kontrollitud asutustest kasutas lepingu alusel kolmanda juriidilise isiku kõnesalvestamise teenust. Lepingutes oli sätestatud konfidentsiaalsuskohustus. Üks asutus haldas kõnesalvestamise infosüsteemi ise. Mitu kontrollitud asutust märkisid ka ära, et nad ei anna telefoni teel isiku kohta välja majanduslikku informatsiooni. Näiteks on Sotsiaalkindlustusametis keelatud edastada telefoni teel hüvitise suurust.

Kokkuvõte

Andmekaitse Inspektsioon juhib kõigepealt tähelepanu eraelu kaitse (PS § 26 ja 43) parandamise vajadusele telefonikõnede lindistamisel. Siinjuures rõhutame, et eraelu kaitse parandamise juures tuleb arvesse võtta nii ettevõttes telefoniga töötava töötaja kui ka ettevõtte klientide õiguste kaitset, samuti aga elektroonilise side abil saadavate teenuste vastu usalduse tekitamist.

Isikuandmete kaitse seadusest tulenevalt on Andmekaitse Inspektsioonil ülesanne anda soovituslikke juhiseid seaduse paremaks rakendamiseks. Tulenevalt leiab Andmekaitse Inspektsioon, et isikute eraelu kaitse paremaks rakendamiseks on tingimata vajalik isiku nõusoleku võtmine telefonikõne lindistamiseks. Siinjuures on nõusoleku võtmine vajalik nii klientidelt, kui ka kõigilt töötajatelt, kes telefoniga töötavad. Nõusolek peab olema võetud enne lindistamise algust ja töötajate puhul enne tööle asumist. Soovitav on võtta nõusolek töötajatelt kirjalikult, sest vaidluse korral eeldatakse, et nõusolekut ei ole antud ja sel juhul on asutusel kohustus tõendada, et nõusolek oli olemas.

Nõusolek peab vastama isikuandmete kaitse seaduse § 12 sätestatule ning sisaldama isikuandmete töötlemise eesmärki, isikuid või nende kategooriaid, kellele isikuandmete edastamine on lubatud, vastutava töötleja või tema esindaja nime ja vastutava töötleja tegevuskoha aadressi, juhtusid, millal andmesubjektil on õigus nõuda isikuandmete töötlemise lõpetamist ning isikuandmete parandamist, sulgemist, kustutamist, juhtusid, millal andmesubjektil on õigus saada juurdepääs tema kohta töödeldavatele isikuandmetele.

Siinjuures ei kehti klientidelt nõusoleku võtmise kohustus juhul, kui kõne alustamine on andmesubjekti elu, tervise ja vabaduse kaitse tähenduses aegkriitiline. Sel juhul toimub isikuandmete töötlemine vastavalt isikuandmete kaitse seaduse § 14 lg 1 p 2 isiku elu ja tervise kaitseks.

Juhul, kui telefonikõnede lindistamine toimub seaduses ettenähtud kohustuste täitmiseks, piisab töötajate teavitamisest, mis peaks sisaldama vähemalt teavet lindistamise eesmärkide ja andmete säilitamise aja kohta.

Andmekaitse Inspektsioon tänab asutusi ja ettevõtteid konstruktiivse ja meeldiva koostöö eest valdkonna praktilise kaardistamise perioodil. Oleme väga tänulikud AS Eesti Energia, Sotsiaalkindlustusamet, Eesti Haigekassa ja Häirekeskusele kannatlikkuse ja vastutuleliku suhtumise eest.

Koostanud:

Merit Vaim, Kontrolliosakonna juhataja

Tõnu Tomik, Kontrolliosakonna järelevalvetalituse juhataja kt

Stiina Liivrand, Arengu-ja Analüüsiosakonna nõunik

Isikuandmete töötlemine ID-pileti projekti raames

Vastavalt isikut tõendavate dokumentide seadusele on Eestis esmane ja ainus kohustuslik isikutunnistus ID-kaart, mida väljastab Kodakondsus- ja Migartsiooniamet. Tänaseks on ID-kaarte väljastatud üle miljoni eksemplari.
ID-kaardil on lai kasutusala: isikuttõendav dokument, reisidokument, isikutuvastus internetis (autentimine), digiallkirjastamine, krüpteerimine, e-hääletamine, ID-pilet jne.

Käesolev dokument vaatleb ID-kaardi kasutamist teenuse ostmist tõendava dokumendina Tallinnas kehtiva ID-pileti süsteemi näitel, juhtides eelkõige tähelepanu isikuandmete töötlemisega seonduvale taolistes süsteemides. Juhend on mõeldud eelkõige avalik- ja eraõiguslikele organisatsioonidele, kes soovivad luua infosüsteeme, mis kasutavad teenuse või toote saamise õigust tõendava dokumendina ID-kaarti.

Ülevaade ID-pileti süsteemist

2003. aastal Tallinna korraldatud elektroonilise tasukogumissüsteemi teostamise riigihanke võitsid ühispakkumisega AS Sertifitseerimiskeskus, Eesti Ühispank ja EMT, kes töötasid välja ID-pileti süsteemi.
Elektroonilise tasukogumissüsteemi üks osa on internetikeskkond www.pilet.ee, mis võimaldab osta pilet ning kontrollida ka pileti kehtivuse hetkeseisu. Samuti on nimetatud Internetikeskkonnast võimalik saada informatsiooni süsteemi töötamise põhimõtete ning andmekaitse tingimuste kohta.

Reisija, kes soovib endale soetada ühistranspordi perioodipiletit (ID-piletit), saab seda teha otsekorraldusega, internetipanga-, mobiiltelefoni- või lauatelefoni vahendusel, samuti on võimalik osta pilet sularahas. Kui teenusepakkuja (nt transpordiettevõte) poolt osutatava teenuse hind sõltub kliendi elukohast, sooritatakse pileti müümisel automaatne päring Rahvastikuregistrisse ning tulemuse põhjal tuvastatakse ID-pileti hind. ID-pileti müüjale ei kuvata ID-pileti kasutaja elukohta ega muud infot päringutulemustest.

ID-pileti kasutaja peab ühistranspordis piletikontrolörile esitama oma ID-kaardi (sisestama selle vastavasse kontrollseadmesse), mille abil tehakse kindlaks ID-pileti kehtivus ja tüüp. Alla 15-aastased ID-pileti kasutajad võivad ID-kaardi asemel kontrolörile esitada ka õpilaspileti, mis on varustatud foto ja isikukoodiga.
Elektroonilise tasukogumissüsteemi- ning ID pileti kontrollseadmete süsteemi haldaja, AS Sertifitseerimiskeskus (ainus töötleja, kes pääseb ligi teenusetarbija isikustatud andmetele), säilitab oma andmebaasides seitsme aasta jooksul ID-piletite kohta järgmised andmed:

- ID-pileti tüüp
- Kasutaja isikukood
- ID-pileti kehtivuse algus- ja lõppaeg
- ID-pileti hind ja müügikanal
- Info ID-pileti müüja kohta (statistilistel eesmärkidel).

Seega piletikontrolli käigus ei salvestu ID-pileti kasutaja liikumistrajektoor ega ka valitud sõiduvahendi marsruut.

ID-pileti Internetipõhisest keskkonnast näeb andmesubjekt infot enda poolt viimase aasta jooksul ostetud piletite kohta. Koondstatistikat teenusele müüdud ID-piletite kohta avaldatakse teenusepakkujale isikustamata kujul.

Isikuandmete töötlemise üldised tingimused

Isikuandmete kaitse seisukohalt on oluline arvestada isikuandmete töötlemise üldiseid põhimõtteid, mis on sätestatud isikuandmete kaitse seaduse §-s 6 ning mida nii isikuandmete vastutav kui ka volitatud töötleja on kohustatud isikuandmete töötlemisel jälgima. Antud põhimõteteks on:

- seaduslikkuse põhimõte – isikuandmeid võib koguda ausal ja seaduslikul teel;
- eesmärgikohasuse põhimõte – isikuandmeid võib koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning isikuandmeid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkide saavutamisega kooskõlas;
- minimaalsuse põhimõte – isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks;
- kasutuse piiramise põhimõte – isikuandmeid võib muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal;
- andmete kvaliteedi põhimõte – isikuandmed peavad olema ajakohased, täielikud ning vajalikud antud andmetöötluse eesmärgi saavutamiseks;
- turvalisuse põhimõte – isikuandmete kaitseks tuleb rakendada turvameetmeid nende tahtmatu või volitamata muutmise, avalikuks tuleku või hävimise eest;
- individuaalse osaluse põhimõte – andmesubjekti tuleb teavitada tema kohta kogutavatest andmetest, talle tuleb võimaldada juurdepääs tema kohta käivatele andmetele ja tal on õigus nõuda ebatäpsete või eksitavate andmete parandamist.

Isikuandmete kaitse seaduses on eelpool toodud põhimõtete täitmisega seonduvat ka täpsustatud, nt turvalisuse põhimõtet on täpsemalt lahti kirjutatud isikuandmete kaitse seaduse §-s 19.

Isikuandmete kaitse alased soovitused süsteemi loomisel

Rakendades süsteemi, mis võimaldab ID-kaarti kasutades osta teenust või toodet, on oluline silmas pidada järgnevaid soovitusi isikuandmete kaitseks:

- Kliendil peab säilima ka alternatiivne võimalus teenuse või toote anonüümseks tarbimiseks, kasutades nt sularaha eest tavapileti ostmise võimalust;
- Loodav süsteem peaks olema ülesehitatud arvestades klientide õigust isikuandmete kaitsele, koguda tuleb isikuandmeid vaid sellises ulatuses ja tähtajaga, mis on vajalik määratletud eesmärkide täitmiseks;
- Süsteemi iga osapool võib omada ligipääsu vaid temale pandud ülesannete täitmiseks vajalikele isikuandmetele ning isikuandmetega teostatud toimingud sh isikuandmete vaatamine peab olema tagantjärgi tuvastatav;
- Luua auditisüsteem isikuandmete väärkasutusest hoidumise kontrolliks;
- Teenuste müügi efektiivsuse ja statistilisteks analüüsideks tuleb kasutada anonümiseeritud andmeid;

- Klienti tuleb selgelt ja igakülgselt informeerida tema isikuandmete töötlemisest (kogutavate andmete hulk, andmete säilitamise tähtajad ning kellele andmeid edastatakse);
- Kliendil peab olema võimalus ka omapoolselt kontrollida temaga seonduvat informatsiooni (nt ID-pileti kehtivust ja isikuandmete õigsust).

Andmekaitse Inspektsioon tervitab algatusi, mis võimaldavad ID-kaardi kasutusala laiendada ning mis samas arvestavad igakülgselt kodaniku õigust temasse puutuvate isikuandmete kaitsele.

Koostanud:

Maarja Kirss
nõunik
arengu- ja analüüsiosakond

Tõnu Tomik
Kontrolliosakonna järelevalvetalituse juhataja kt

Lisa 5.

Juhendmaterjal KOV-ide isikuandmeid sisaldavate õigusaktide avalikustamiseks

Käesolev juhendmaterjal on mõeldud eelkõige valla- või linnasekretäridele, kes kohaliku omavalitsuse korralduse seaduse (edaspidi KOKS) § 55 lg 4 p-i 3 kohaselt korraldavad valitsuse õigusaktide avaldamist ja töö avalikustamist; punkti 4 kohaselt korraldavad volikogu õigusaktide avaldamist ja töö avalikustamist; punkti 8 kohaselt osalevad valitsuse istungite ettevalmistamisel ja korraldavad istungite protokollimist ning punkti 9 kohaselt annavad valla- või linnakantselei sisemise töö korraldamiseks käskkirju.

Käesoleva juhendmaterjali eesmärgiks on aidata kohalikel omavalitsustel leida tasakaal kahe olulise põhimõtte vahel, millele kohalik omavalitsus KOKS-i §-i 3 kohaselt rajaneb - igaühe seaduslike õiguste ja vabaduste, sealhulgas informatsioonilise ensemääramisõiguse, kohustusliku tagamise ning oma tegevuse avalikkuse tagamise vahel. Eelmainitud kahe põhimõtte kõrval ei saa vähem tähtsaks lugeda põhimõtet järgida oma ülesannete ja kohustuste täitmisel seadusi, antud juhendmaterjali kontekstis eelkõige avaliku teabe seadust, isikuandmete kaitse seadust ning muidugi ka KOKS-i.

Kohaliku omavalitsusüksuse ülesandeks on korraldada antud vallas või linnas sotsiaalabi ja -teenuseid, vanurite hoolekannet, noorsootööd, elamu- ja kommunaalmajandust, veevarustust ja kanalisatsiooni, heakorda, jäätmehooldust, territoriaalplaneerimist, valla- või linnasisest ühistransporti ning valla teede ja linnatänavate korrashoidu, juhul kui need ülesanded ei ole seadusega antud kellegi teise täita.

Samuti on omavalitsusüksuse ülesandeks korraldada antud vallas või linnas koolieelsete lasteasutuste, põhikoolide, gümnaasiumide ja huvialakoolide, raamatukogude, rahvamajade, muuseumide, spordibaaside, turva- ja hooldekodude, tervishoiuasutuste ning teiste kohalike asutuste ülalpidamist, juhul kui need on omavalitsusüksuse omanduses. Nimetatud asutuste osas võidakse seadusega ette näha teatud kulude katmist kas riigieelarvest või muudest allikatest.

Samas ei ole eeltoodud ülesannete loetelu ammendav. Lisaks eelmainitud ülesannetele otsustab ja korraldab omavalitsusüksus neid kohaliku elu küsimusi:
1) mis on talle pandud teiste seadustega;
2) mis ei ole seadusega antud kellegi teise otsustada ja korraldada.

Eelmainitud ülesannete täitmist korraldavad ning ka täidavad omavalitsusorganid, millisteks on volikogu - kohaliku omavalitsusüksuse esinduskogu, mis valitakse valla või linna hääleõiguslike elanike poolt kohaliku omavalitsuse volikogu valimise seaduse alusel ning valitsus - volikogu poolt moodustatav täitevorgan. Kõigi kohaliku elu küsimuste lahendamise õigus eeldab KOV-ide organite õigust kehtestada üld-ja üksikakte. Volikogul ja valitsusel on õigus üldaktidena kehtestada määrusi ning volikogul üksikaktidena vastu võtta otsuseid, valitsusel aga anda korraldusi. Volikogu ja valitsuse õigusaktid kehtivad antud omavalitsusüksuse haldusterritooriumil. Kõigile kohaliku omavalitsuse organite õigusaktidele laienevad üldise haldusmenetluse põhimõtted, mis on sätestatud haldusmenetluse seaduses.

Kõigi kohaliku elu küsimuste lahendamisel töötlevad kohaliku omavalitsusorganid isikuandmeid ehk siis andmeid füüsiliste isikute kohta ning sageli sisaldavad isikuandmeid ka volikogu ja valitsuse õigusaktid, eelkõige üksikaktid – otsused ja korraldused, samuti volikogu ja valitsuse istungite ja komisjonide protokollid.

Tulenevalt kohaliku omavalitsuse korralduse seaduse (KOKS) § 31 lõikest 1 avalikustatakse valla- ja linnavalitsuse õigusaktid ning need peavad olema kättesaadavad kõigile isikutele seaduses ja valla või linna põhimääruses sätestatud korras. Kui valla või linna põhimääruses ei ole sätestatud teisiti, avalikustatakse valitsuse õigusaktid väljapanekuga valla- või linnakantseleis. Sama paragrahvi lõike 2 kohaselt ei avalikustata andmeid, mille väljastamine on seadusega keelatud või mõeldud üksnes valla või linna ametiasutuse siseseks kasutamiseks.

Avaliku teabe seaduse (AvTS) § 4 lõike 1 kohaselt on teabevaldajad kohustatud demokraatliku riigikorralduse tagamiseks ning avaliku huvi ja igaühe õiguste, vabaduste ja kohustuste täitmise võimaldamiseks tagama juurdepääsu nende valduses olevale teabele seaduses sätestatud tingimustel ja korras. Samas peab teabele juurdepääsu võimaldamisel olema tagatud isiku eraelu puutumatus (§ 4 lg 3).

AvTS-i § 8 kohaselt võimaldatakse juurdepääs teabele teabevaldaja poolt teabe avalikustamisega või teabenõude täitmisega. Seega eristatakse n.ö aktiivset ja passiivset teabe avalikustamist. Aktiivse avalikustamise puhul tuleb initsiatiiv mingi teabe avalikustamiseks teabevaldaja poolt ning teabevaldaja teeb seda omal algatusel, näiteks põhjusel, et seadus kohustab seda tegema. Passiivse avalikustamise puhul tuleb initsiatiiv teabele juurdepääsu saamiseks teabenõudjalt, kes esitab teabele juurdepääsu saamiseks teabenõude AvTS-is sätestatud korras. Passiivne avalikustamine võimaldab teabevaldajal enne teabe väljastamist hoolega kaaluda teabe väljastamisega kaasneda võivaid aspekte muuhulgas ka tagajärgi, mida teabe väljastamine võib andmesubjekti jaoks kaasa tuua.

Aktiivne avalikustamine (internetis) kujutab endast tänapäevaste infotehnoloogiliste vahendite juures isiku privaatsusele suuremat ohtu, kui passiivne avalikustamine. Seisukohta toetab IKS-i § 14 lg 2 p 3, mille kohaselt isikuandmete edastamine või nendele juurdepääsu võimaldamine kolmandale isikule on lubatud andmesubjekti nõusolekuta kui kolmas isik taotleb teavet, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites ja sellele ei ole kehtestatud juurdepääsupiirangut. Seega peab kolmas isik teavet teabenõudega taotlema, mitte teabevaldaja seda ise omal initsiatiivil aktiivselt avalikustama. Ehkki formaalselt võttes on raske eristada aktiivselt ja passiivselt avalikku teavet (üks oleks justkui rohkem avalik), on tegelikult andmete leviku (ning seeläbi üksikisiku huvide kaitse) seisukohalt suur vahe, kas teave on hõlpsasti Internetist otsitav ja leitav, või tuleb informatsiooni saamiseks esitada teabenõue ning teabele juurdepääsu taotleda.

Teabe aktiivse avalikustamise (eelkõige veebilehe vahendusel) põhireeglid tulenevad AvTS §-dest 28-30. Põhimõtteliselt võib teabevaldaja aktiivselt avalikustada mistahes

teavet (AvTS § 28 lg 1 p 32), kuid isikuandmete puhul tuleb silmas pidada isikuandmete töötlemise lubatavuse kriteeriume. Isikuandmete aktiivseks avalikustamiseks peab eksisteerima seadusest tulenev selgesõnaline volitus. Kuigi kohaliku omavalitsusorganite õigusaktide aktiivse avalikustamise kohustust AvTS-i § 28 ei sätesta, on paljud kohalikud omavalitsused oma põhimäärustes õigusaktide kõigile isikutele kättesaadavaks tegemise viisiks valinud nende aktiivse avalikustamise kohaliku omavalitsuse veebilehel. Samas sätestab KOKS-i § 31 lg 2 et ei avalikustata andmeid, mille väljastamine on seadusega keelatud või mõeldud üksnes valla või linna ametiasutuse siseseks kasutamiseks.

Võttes arvesse asjaolu, et üksikaktide puhul langevad haldusakti taotleja ja haldusakti adressaat ehk siis normiadressaat – isik, kellele haldusakt on suunatud – üldjuhul kokku, on selliste õigusaktide igaühele kättesaadavaks tegemise ainsaks eesmärgiks luua võimalused avalikkuse kontrolliks avalike ülesannete täitmise üle. See eesmärk saavutatakse ka juhul, kui aktiivselt avalikustatakse KOV-i üksikaktid ilma isikuandmeteta ehk siis seal sisalduvad isikuandmed asendatakse XXXXXX-idega. Samas avalikustatakse üksikakti ülejäänud tekst ja rekvisiidid – sealhulgas akti vastuvõtja, vastuvõtmise kuupäev ja number. See võimaldab avalike ülesannete täitmise üle kontrolli teostada teabele, mille rekvisiidid on aktiivse avalikustamise tulemusena teabenõudjale teada, juurdepääsu taotledes esitades selleks teabenõude AvTS-is sätestatud korras. Seega täidetakse AvTS-i eesmärk teabe passiivse avalikustamisega. Samas tuleb ka teabe passiivsel avalikustamisel tagada isikute eraelu puutumatus.

AvTS-i § 35 lg 1 p-i 10 kohaselt on teabevaldaja kohustatud tunnistama asutusesiseseks kasutamiseks (sünonüüm KOKS-is sisalduvale mõistele „ametiasutuse siseseks kasutamiseks”) mõeldud teabeks teabe, mis sisaldab eraelulisi või delikaatseid isikuandmeid.
Eraeluliste ja delikaatsete isikuandmete määratlus on sätestatud isikuandmete kaitse seaduse §-is 4.

Eraelulised isikuandmed on:
1) perekonnaelu üksikasju kirjeldavad andmed;
2) sotsiaalabi või sotsiaalteenuste osutamise taotlemist kirjeldavad andmed;
3) isiku vaimseid või füüsilisi kannatusi kirjeldavad andmed;
4) isiku kohta maksustamisega kogutud teave, välja arvatud teave maksuvõlgnevuste kohta.

Delikaatsed isikuandmed on:
1) poliitilisi vaateid, usulisi ja maailmavaatelisi veendumusi kirjeldavad andmed, välja arvatud andmed seadusega ettenähtud korras registreeritud eraõiguslike juriidiliste isikute liikmeks olemise kohta;
2) etnilist päritolu ja rassilist kuuluvust kirjeldavad andmed;
3) andmed terviseseisundi või puude kohta;
4) andmed pärilikkuse informatsiooni kohta;
5) andmed seksuaalelu kohta;
6) andmed ametiühingu liikmelisuse kohta;
7) kriminaalmenetluses või muus õigusrikkumise väljaselgitamise menetluses kogutav

teave enne avalikku kohtuistungit või otsuse langetamist õigusrikkumise asjas või juhul, kui see on vajalik kõlbluse või inimeste perekonna- ja eraelu kaitseks või kui seda nõuavad alaealise, kannatanu, tunnistaja või õigusemõistmise huvid.

Eelnevalt loetletud kriteeriumitele vastavaid andmeid sisaldava avaliku teabe tunnistab teabevaldaja asutusesiseseks kasutamiseks ning juhul, kui teabenõudja taotleb teabenõudega sellisele teabele juurdepääsu, keeldub teabevaldaja teabenõude täitmisest vastavalt AvTS-i § 23 lg-le 1, kuna taotletava teabe suhtes kehtivad juurdepääsupiirangud ja teabenõudjal ei ole taotletavale teabele juurdepääsuõigust.

Nö tavalisi isikuandmeid ehk siis andmeid, mis ei ole ei delikaatsed ega eraelulised, sisaldava avaliku teabe passiivsel avalikustamisel on seadusandja jätnud õiguse teabevaldajal hinnata ehk kaaluda huvisid, kas teabele juurdepääsu võimaldamisega kahjustatakse oluliselt andmesubjekti eraelu puutumatus või mitte (AvTS § 35 lg 1 p 11). Kaalumisel tuleks hinnata milliseid tagajärgi võib andmetele juurdepääsu võimaldamine endaga kaasa tuua. Lähtuda tuleks taotletavate isikuandmete iseloomust (mida väljastatav teave võimaldab isiku kohta teada saada, näiteks seda kus ta elab, millises lasteaias või koolis käivad tema lapsed, kus töötab tema abikaasa vms), hulgast (kui suure hulga andmesubjektide kohta käivat teavet soovitakse saada, igasuguste nimekirjade väljastamist tuleks hoolega kaaluda), teabenõudjast ning teabe saamise eesmärkidest (kes ja mille jaoks soovib taotletavat teavet kasutada) ning kas olulisemad on andmesubjekti või andmete saaja huvid.

Võimaluse korral tuleks kaalutlusotsuse tegemiseks küsida ka andmesubjekti arvamust, kuna viimane teab kõige paremini, kas teabele juurdepääsu võimaldamine kahjustab oluliselt tema eraelu puutumatust või mitte. Seda võib andmesubjektilt küsida ka proaktiivselt, näiteks juhul kui isik esitab KOV-ile mingi taotluse.

Samas piirab teabevaldaja eelmainitud kaalutlusõiguse teostamise ulatust muuhulgas AvTS § 36 lõige 1 punkt 9, mille kohaselt ei tohi riigi- ja kohalikust omavalitsuse asutusest ja avalik-õiguslikust juriidilisest isikust teabevaldaja tunnistada asutusesiseseks kasutamiseks dokumente riigi, kohaliku omavalitsuse üksuse või avalik-õigusliku juriidilise isiku eelarvevahendite kasutamise ning eelarvest makstud tasude ja hüvitiste kohta.

Samas võimaldab AvTS-i § 38 lg 2 juhul kui teabele juurdepääsu võimaldamine võib põhjustada juurdepääsupiiranguga teabe avalikuks tulemise, tagada juurdepääs üksnes sellele osale teabest või dokumendist, mille kohta juurdepääsupiirangud ei kehti.

Andmekaitse Inspektsiooni hinnangul täidab teabevaldaja AvTS § 36 lõige 1 punktis 9 sätestatud kohustuse kooskõlas AvTS-i § 38 lg-ga 2 ka juhul, kui isikuandmeid sisaldavate üksikaktide puhul võimaldatakse teabevaldajale juurdepääs üksnes üksikakti resolutiivosas sisalduvatele isikuandmetele ning ülejäänud aktis sisalduvad isikuandmed asendatakse XXXXXX-idega või muudetakse muul viisil loetamatuks. Dokumendi resolutiivosaks on haldusorgani mingis küsimuses tehtud otsusus ilma õigusliku ja faktilise põhjenduseta, HMS-i § 60 lg-st 2 tulenevalt on resolutiivosa haldusaktiga

kindlaksmääratavaid õigusi ja kohustusi sisaldav osa. Resolutiivosa on asja suhtes otsustatu, resolutiivosasse ei kuulu viited otsuse tegemise õiguslikule alusele, samuti ei ole resolutiivosa käsitatav otsustuse faktoloogia – asjaolude kirjeldus ning selgitused, miks konkreetse sisuga otsus tehti.

Samas tuleb tähelepanu pöörata ka asjaolule, et isikuandmeid sisaldava üksikakti resolutiivosale juurdepääsu võimaldamisel järgitakse eelmainitud isikuandmete töötlemise minimaalsuse printsiipi ning üksikaktide resolutiivosa passiivsel avalikustamisel ei avalikustata isiku elukohta ega isikukoodi. IKS §-i 16 kohaselt on isikukoodi töötlemine lubatud ilma andmesubjekti nõusolekuta, kui isikukoodi töötlemine on ette nähtud välislepingus, seaduses või määruses. Seega võib isikukoodi töödelda (sealhulgas avalikustada) kui selleks on isiku nõusolek või see tuleneb seadusest.

Selliselt redigeeritud üksikaktidele juurdepääsupiirangu kehtestamise aluseks või siis seal sisalduvate isikuandmete asutusesiseks kasutamiseks tunnistamise aluseks on AvTS-i § 35 lg 1 p 11, kuna teave sisaldab isikuandmeid ning teabele juurdepääsu võimaldamine kahjustab oluliselt andmesubjekti eraelu puutumatust. Juhul, kui teabenõudja soovib teabenõudega üksikakti täisversioonile juurdepääsu, keeldub teabevaldaja teabenõude täitmisest vastavalt AvTS-i § 23 lg-le 1, kuna taotletava teabe suhtes kehtivad juurdepääsupiirangud ja teabenõudjal ei ole taotletavale teabele juurdepääsuõigust ning kooskõlas AvTS-i § 38 lg-ga 2 tagab juurdepääsu üksnes sellele osale teabest või dokumendist, mille kohta juurdepääsupiirangud ei kehti.

Eeltoodust tulenevalt tuleks KOV-i organite üksikaktides enne nende veebilehel avalikustamist asendada seal sisalduvad isikuandmed (kõik andmekoosseisud, mis võimaldavad füüsilisest isikust andmesubjekti otseselt tuvastada - nimi, isikukood, elukoha aadress, töökoht, ametinimetus vms) XXXXXXXXXXXX-dega või olenevalt teabekandjast muuta selline teave muul viisil loetamatuks ning avalikustada üksikakt redigeeritud kujul. Samas peab üksikakt sisaldama vähemalt akti vastuvõtja nime, kuupäeva ja numbrit võimaldamaks avalike ülesannete täitmise üle kontrolli teostamiseks esitada teabevaldajale teabenõue aktile juurdepääsuks.

Teabenõude korras teabe väljastamisel ehk siis teabe passiivsel avalikustamisel tuleks akt väljastada selliselt, et isikuandmed sisalduvad üksnes akti resolutiivosas ning ülejäänud aktis sisalduvad isikuandmed asendatakse XXXXXX-idega või muudetakse muul viisil loetamatuks. Dokumendi resolutiivosaks on haldusorgani mingis küsimuses tehtud otsusus ilma õigusliku ja faktilise põhjenduseta. Resolutiivosa on asja suhtes otsustatu, resolutiivosasse ei kuulu viited otsuse tegemise õiguslikule alusele, samuti ei ole resolutiivosa käsitatav otsustuse faktoloogia – asjaolude kirjeldus ning selgitused, miks konkreetse sisuga otsus tehti.

Lisa 6.

Laps ja tema õigused isikuandmete töötlemisel

Andmekaitse Inspektsioon analüüsis laste isikuandmete töötlemist erinevates igapäevaelu valdkondades. Avaldatu aluseks võeti peamised rahvusvahelisel tasandil laste õigusi käsitlevad õigusaktid, siseriiklikud vastavate valdkondade normid, läbiviidud järelevalvetulemid ja praktikas kasutatavad käitumisharjumused erinevates keskkondades.

Regulatsioon

Peamiseks laste õigusi käsitlevaks rahvusvaheliseks lepinguks on ÜRO lapse õiguste konventsioon, millega Eesti ühines 1991. aastal. Konventsiooniga ühinemisel võeti kohustus tagada rahvusvaheliselt tunnustatud õigused igale Eesti territooriumil elavale lapsele.

ÜRO lapse õiguste konventsioon on lepinguks laste ja täiskasvanute ning laste ja valitsuse vahel. Sellest tulenevalt on strateegiliseks eesmärgiks kohaldada siseriiklike seaduste ja tavade vastavus nimetatud konventsioonile ja teistele rahvusvahelistele inimõiguste standarditele ning edendada nende printsiipide rakendamist, samuti jälgida ÜRO lapse õiguste konventsioonist kinnipidamist nii siseriiklikes kui rahvusvahelistes õigussuhetes.

Eesti Vabariigi lastekaitse seadus (edaspidi LaKS) sätestab lapse rahvusvaheliselt tunnustatud õigused, vabadused ja kohustused ning nende kaitse Eesti Vabariigis. LaKS võeti vastu 8.06.1992. aastal.

Eestis on põhjalikult reguleeritud laste õiguste kaitse nii perekonnaseaduses, lastekaitse seaduses, kui lastekaitse konventsioonis.

Kes on laps?

LaKS-i kohaselt peetakse lapseks kuni 18-aastasi inimesi. Antud regulatsiooni toetab ka tsiviilseadustiku üldosa seaduse (TsüS) § 8 lg 2 mille kohaselt on täielik teovõime 18-aastaseks saanud isikul (täisealisel).

Alla 18-aastasel isikul (alaealisel) ja isikul, kes vaimuhaiguse, nõrgamõistuslikkuse või muu psüühikahäire tõttu kestvalt ei suuda oma tegudest aru saada või neid juhtida, on piiratud teovõime.

TsüS § 9 lõiked 1 ja 2 sätestavad, et kohus võib vähemalt 15-aastase alaealise piiratud teovõimet laiendada, kui see on alaealise huvides ja alaealise arengutase seda võimaldab. Sel juhul otsustab kohus, milliseid tehinguid võib alaealine teha iseseisvalt. Alaealise piiratud teovõimet võib laiendada tema seadusliku esindaja nõusolekul.

Kui nõusoleku andmisest keeldumine on ilmselt vastuolus alaealise huvidega, võib kohus alaealise teovõimet laiendada seadusliku esindaja nõusolekuta.

Lapse isikuandmete töötlemine ja eraelu puutumatus

Isikuandmete kaitse seaduse (edaspidi IKS) eesmärk on isikuandmete töötlemisel füüsilise isiku põhiõiguste ja põhivabaduste kaitsmine kooskõlas avalike huvidega.

Isikuandmete kaitse seadus sätestab §-s 4 lõikes 1, et isikuandmed on kõik andmed, mille alusel on võimalik isikut tuvastada ja §-s 5, et isikuandmete töötlemine on iga isikuandmetega tehtav toiming. Seega tuleb lapse isikuandmete töötlemisel lähtuda samuti IKS-is sätestatud põhimõtetest.

Tulenevalt LaKS-i §-ist 13 on lapsel õigus privaatsusele. Lapsel on õigus isiklikule elule, suhtlus- ja sõprusringile. Lapse õigust eraelule ei tohi kahjustada meelevaldse või ebaseadusliku sekkumisega, riivates lapse au, väärikust, kiindumusi ja head mainet. Korduv jõhker sekkumine lapse eraellu võib olla aluseks administratiiv- või distsiplinaarvastutusele võtmiseks või vanemlike õiguste äravõtmiseks. Lapsele adresseeritud kirja ning lapse isiklikke märkmeid ei ole õigus ilma lapse loata lugeda.

Lapse eraelu puutumatust toetavad ka lapse õiguste konventsiooni artikli 16 punktid 1 ja 2, mille järgi ei tohi mitte ühegi lapse eraellu, perekonnaellu, kodusse ega kirjavahetusse meelevaldselt ega ebaseaduslikult sekkuda, samuti ei tohi ebaseaduslikult rünnata tema au ja head mainet. Lapsel on õigus seaduslikule kaitsele niisuguse vahelesegamise ja rünnakute vastu.

Laps ja veebikaamerad koolides

Tänapäeval kiiresti arenev tehnoloogia annab võimaluse lapsevanemal jälgida oma lapse tegemisi praktiliselt 24 tundi ööpäevas.

Nii Euroopas kui Eestis on hakatud kasutama lapse tegevuse jälgimiseks veebikaameraid - seda nii kodus kui väljaspool kodu. Praktikas on esinenud näiteid erinevates Euroopa riikides (nt. Rumeenia), kus lasteaedadesse on paigaldatud veebikaamera, mis võimaldab vanemal jälgida oma lapse tegemisi terve päeva vältel reaalajas.

Samuti on alustatud Eestis asuvatesse koolidesse (nt. Laagri Kool, Jüri Gümnaasium) videokaamerate paigaldamist, mis salvestavad informatsiooni 24 tundi ööpäevas.

Videojärelevalve vajadust on põhjendatud turvalisuse kaalutlustele tuginedes. Samas mõjutab igasugune andmete videolindile salvestamine isiku põhiõigusi.

Videojärelevalve süsteemi paigaldamisel peavad lapsed ja nende vanemad olema eelnevalt teavitatud sellest, et koolis/lasteaias on videojärelevalve süsteem.

Siiski jääb tihti videojärelevalve süsteemi paigaldamise vajadus ning eesmärk sellisel kujul isikuandmeid töödelda selgelt määratlemata või põhjendatamatuks ning ei ole kooskõlas isikuandmete kaitse seaduse põhimõtetega, millede kohaselt võib isikuandmeid koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks.

Lisaks ei või isikuandmeid töödelda viisil, mis ei ole andmetöötluse eesmärkide saavutamisega kooskõlas.

Seega peab lapse tegevuse üle teostatav kontroll olema proportsioonis ühelt poolt lapse õigusega privaatsusele ning teisest küljest üldhuvidest lähtuvalt nagu näiteks turvalisusega, kuritegude ennetamisega jne.

Laps ja hinded

Palju küsimusi ja küsitavusi on tõusetunud koolis õpilaste hinnete avaldamisel.

Euroopa riikides on selles osas praktika erinev. On koole kus õpilase teadmistele antud hinne ei kuulu avalikustamisele ning jääb rangelt vaid õpetaja ja õpilase või tema vanema/esindaja teada. Samas on riike, kus õpilase teadmisele antav hinne avaldatakse ka teistele isikutele.

Eestis on rakendunud E-kooli süsteem, kuhu märgitakse õpilaste hindeid ning tema osalemine tundides ning kus andmetele pääsevad ligi lapse seaduslikud esindajad, laps ise ja õpetaja, kes andmeid sisestab. E-Kooli loomise idee on iseenesest hea ja vajalik, kuid samas peavad nii lapsed, lapsevanemad kui õpetajad olema teadlikud, et andmete ka sellises keskkonnas töötlemine ei ole alati turvaline ning andmetele võivad ligi pääseda ka selleks mitte luba omavad isikud (nt. paroolide varastamine, kaotamine, nime põhjal tuletamine) ning neid oma huvides ära kasutada.

Laps ja meedia

Lapse meedias eksponeerimine on lubatud vaid lapse seadusliku esindaja informeeritud nõusolekul s.t. lapsevanema või kohtu poolt määratud eestkostja nõusolekul.

Viimastel aastatel on Eesti meedias sagenenud lastega seotud negatiivse kontekstiga juhtumite kajastamine, milles võib näha rikkumisi nii meedia-eetilisest seisukohast kui vastuollu minemist laste õiguste ja huvidega ning seadustega.

Eesti meediaväljaannetes pole sageli tagatud lapse igakülgne füüsiline ja vaimne, aga eelkõige emotsionaalne turvalisus – selle peamise näitena võib välja tuua laste identifitseerimise võimalikkuse ajakirjanduses.

Laps on sageli meedias objekt, keda kasutatakse ära vahendina ärilistel eesmärkidel, suurendamaks meediaväljaande populaarsust ning müügiedu.

Lapsega tegelevad inimesed – lapsevanem, õpetaja, klassijuhataja, politsei, lastepsühhiaater – ei ole sageli teadlikud andmete ja oma arvamuse avaldamise võimalikest tagajärgedest ning tihti moonutatakse arvamuses avaldatut. Seetõttu ei suuda lapse probleemidega kokku puutuvad lähedased isikud ja spetsialistid sageli tagada lapsele igakülgset kaitset ja turvalisust.

Laps ja Internet

Erilist tähelepanu vajab ka internetis toimuv, kuna sisuliselt ei vastuta keegi seal andmete avaldamise õiguspärasuse eest.

Sellest tulenevalt peab rohkem tõstma nii laste kui ka nende vanemate/seadluslike esindajate teadlikkust.

Koolides tuleb nii õpetajate kui õpilaste (nt arvutiõpetuse tunnis) hulgas teha rohkem selgitustööd ning tuua praktilisi näiteid, kuidas isikuandmete avaldamine näiteks Internetis võib tulevikus kahjustada eraelu puutumatust ja millised tagajärjed võivad ilmneda.

Internet on kujunenud meediakanaliks, mille puhul on vanemal/esindajal äärmiselt keeruline olla teadlik lapse poolt hangitava või juhuslikult saadavast informatsioonist. See tingib asjaolu, et lapsega tegelev isik on osalt võimetu tagama lapsele tasakaalustatud infokeskkonda.

Lastele suunatud turundustegevus lähtub eelkõige turustajate huvidest, mis mõnede turundusmeetmete osas põhjustab vastuolu lapse huvide parimate lahendustega. Lastele suunatud müügiedenduskampaaniates ja tarbijamängudes on põhirõhk toote tarbimiselt viidud tootevälisele lisaväärtusele, mis põhjustab valearusaamu vajadustest ning nii toodete kui ka raha väärtusest.

Võimalus manipuleerida lastega ja laste kaudu ka nende vanemate või eeskostjatega loob lastele väära maailmapildi, kus taolised võtted on ühiskonna poolt aktsepteeritavad.

Kehtivas reklaamiseaduses on küll sätestatud, et lastele suunatud reklaamis ei tohi ära kasutada laste loomulikku kergeusklikkust ja kogemuste puudust, kuid taoliste turundusvõtete puhul just neid lapse omadusi ära kasutataksegi.

Vanemate/esindajate, laste ja õpetajate teadlikkuse tõstmiseks on avatud uus internetilehekülg Veebivend, mis on suunatud kõigi alg- ja põhikooli õpilastele, aga samuti lastevanematele ning õpetajatele, et selgitada kuidas internetis õigesti käituda. Ühe alapunktina on käsitletud ka teemat - laste isikuandmed ja fotod internetis.

Põlvkondadevahelised erinevused meedia kasutamisel ning mõtestamisel on kahetsusväärselt suured. Sageli puudub lapsevanemal või eeskostjal ülevaade lapse meediatarbimisest (seda eriti Interneti puhul), samuti pole täiskasvanud alati pädevad kasutama või selgitama meedianähtusi. Vastutus lapse kasvatamisel ning hariduse omandamisel lasub küll täiskasvanutel, kuid viimase aja arengud meedia valdkonnas ei võimalda neil seda vastutust piisavalt tõhusalt kanda. Samad probleemid tõusetuvad ka laste isikuandmete töölemise teemal.

Järelevalvetulemid

Eestis käivitunud projekti, elektroonilise õpilaspileti kasutuselevõtmiseks, raames alustas Andmekaitse Inspektsioon (edaspidi AKI) 23.02.2007 järelevalvemenetlust, et tuvastada Gustav Adolfi Gümnaasiumis elektroonilise õpilaspileti (edaspidi õpilase ID) kasutamise õiguspärasus ning õpilase ID kasutamise käigus kogutud isikuandmete töötlemise seaduspärasus ning turvalisus.

Kohapealse kontrolli käigus tuvastati, et Tallinna Gustav Adolfi Gümnaasiumis (edaspidi kool) on alates 04.10.2006 kasutusel õpilase ID (raadiokiipi sisaldav plastikkaart, millele on trükitud õpilase andmed).

Alates 04.10.2006 ei väljastata alternatiivina enam paberkandjal olevat õpilaspiletit (haridusministri 23.03.1999 määrusega nr 17 kinnitatud „Õpilaspileti väljaandmise kord").

Õpilase ID võimaldab siseneda koolimaja hoonetesse ja väljuda koolimaja hoonetest (5 hoonet), laenutada raamatukogust raamatuid ning saada sööklas koolitoitu. Kõiki eelpool nimetatud õpilase ID abil teostatavaid tegevusi pole õpilasel võimalik teha õpilase ID-d omamata. Kooli direktori sõnade kohaselt on õpilase ID üheks eesmärgiks koolikohustuse täitmise kontroll. Õpilase ID-ga on tema sõnade järgi võimalik tuvastada kooli hoonetesse sisenemist ja väljumist ning reguleerida sööklas söömist. Samuti on õpilase ID-d võimalik kasutada Tallinnas ühistranspordis sõiduõigust kinnitava dokumendina alternatiiviks ID kaardile. Kõiki õpilase ID kasutamisi salvestatakse ning salvestustele on võimaldatud juurdepääs erinevatel isikutel (kooli juhtkond, klassijuhataja, toitlustaja firma, IT-süsteemi arendaja). Kooli direktori vastuskirja

kohaselt säilitatakse kõikide õpilase ID kasutamiste salvestusi terve õppeaasta. Kuna kõik õpilased on kohustatud õpilase ID-d igal sisenemisel ning väljumisel elektroonilises kaardilugejas registreerima ning kool ei väljasta haridusministri 23.03.1999 määrusega nr 17 kinnitatud paberkandjal olevat õpilaspiletit, siis on kõikide kooliõpilaste õppehoonetesse sisenemised väljumised elektrooniliselt salvestatud.

Vastuolu isikuandmete kaitse seadusega, õppehoonetesse sisenemisel ja väljumisel oma liikumine elektrooniliselt registreerida, ei tuvastatud.

AKI poolt viidi 2007. aasta novembris läbi Laagri Koolis ja Jüri Gümnaasiumis järelevalve menetlus, mille eesmärgiks oli koolides paigaldatud videovalvesüsteemidega tutvumine.

Mõlemas koolis oli välja töötatud videovalvesüsteemi kasutamise kord, kus oli kirjeldatud videovalvesüsteemi paigaldamise eesmärk, selle kirjeldus, kaamerate poolt edastatava pildi jälgimine ning salvestatud informatsiooni kasutamine.

Videovalvesüsteemide paigaldamisest kooli ruumidesse oli informeeritud nii lapsi kui lapsevanemaid.

Koolijuhtide sõnul on tagasiside olnud positiivne ning kaebusi pole esitatud. Mõlemas koolis on olnud olukordi, millede lahendamisele videovalvesüsteem on kaasa aidanud.

Järelevalve käigus rikkumisi ei tuvastatud.

AKI ja Lastekaitseliit

AKI ja Lastekaitseliidu esindajate vahel toimus 30.11.2007 kohtumine, kus arutati AKI poolt järelevalvetoimingute käigus tuvastatud ja tõusetunud küsimusi seoses videovalvesüsteemidega koolides ning Gustav Adolfi Gümnaasiumis oleva ID õpilaspileti kasutamist.

Vestluse käigus selgus, et Lastekaitseliit ei olnud teadlik asjaolust, et ühes Harjumaa koolidest on klassiruumidesse paigaldatud videovalvesüsteem. Küsimus videovalvesüsteemi vajalikkusest koolides lubati läbi arutada vanematekogus.

Lastekaitseliit oli huvitatud koostööst AKI-ga laste isikuandmete kaitsega seonduvate teavituskampaaniate läbiviimisel (loengud ning selgitustöö haridusasutustes, osalemine vanematekogu koosolekutel) ja informatiivse materjali (postrid, voldikud, videoklipid, selgitavad juhendid ja õppematerjalid) väljatöötamisel ning rakendamisel.

Informatiivse materjali väljatöötamisel on otstarbekas aluseks võtta teistes Euroopa riikides (nt. Norras, Portugalis, Inglismaal, Tšehhis) kasutatud ja positiivset tagasisidet saanud formaadid ning vormid. Sihtgrupiks eelkõige 11-15 aastased lapsed samuti õpetajad ja lapsevanemad.

Kokkuvõte

Tulenevalt eelpoolkirjeldatust tuleb tõdeda, et laste privaatsuse kaitsel tuleb lähtuda kahest aspektist: vastutus ja teadlikkus.

Laste teadlikkuse tõstmine nende isikuandmete töötlemisest on nii perekonna, kooli kui andmekaitse järelevalveasutuse ülesanne.

Oluline on, et eelkõige lapsevanemad mõistaksid kui oluline on lastele selgitada isikuandmete avaldamisega kaasnevaid ohtusid ning tagajärgi, mis võivad kaasneda ning teeksid endast kõik sõltuva, et kaitsta lapse isikuandmeid ebaseadusliku töötlemise eest.

Nii kaupmeestel, massimeedial, Interneti keskkonna operaatoritel jne peab olema seatud suurem vastutus lastele suunatud kampaaniate, tarbimismängude, mängukeskkondade, tutvumisportaalide jne loomisel ning läbiviimisel kuna reaalne oht laste isikuandmete mitte eesmärgipärasel töötlemisel või ebaseaduslikul töötlemisel on tunduvalt suurem kui täiskasvanute puhul.

Valminud ülevaade on dünaamiline ja Andmekaitse Inspektsioon jätkab nimetatud teema analüüsi. Vajadusel täiendame ja avaldame uuendatud juhendmaterjali käsitletud valdkonnast.

Lisa 7.

Isikuandmete koosseis kliendikaardi väljastamisel

Käesolev soovitus on mõeldud isikutele, kes on mõne kaubandusettevõtte või teenuseosutaja (edaspidi ettevõte) püsiklient ehk kliendikaardi omanik (edaspidi klient) või soovib selleks saada. Soovituse eesmärgiks on anda ülevaade sellest, mida kujutavad endast kliendikaardid isikuandmete töötlemise seisukohalt ning kliendi õigustest antud vallas.

Mis on kliendikaart?
Kliendikaarte väljastavad ettevõtted, kes soovivad klientidega luua kestvaid ostusuhteid ehk selekteerida lojaalsed kliendid nn juhuslikest klientidest. Samal ajal pakutakse kliendile, kes omab kliendikaarti, mitmeid erinevaid püsi- ning ühekordseid soodustusi, samuti edastatakse kliendile informatsiooni tulvastest sooduspakkumistest, kampaaniatest ja muudest eelistest teiste klientide suhtes. Tihti kliendikaardi kasutusvõimalused ei piirdu vaid ühe konkreetse ettevõtte piires, kelle kliendikaarti klient omab, vaid laieneb ka antud ettevõtte partneritele.

Milliseid isikuandmeid esitada kliendikaardi taotlemisel?
Asjakohase kliendiandmebaasi loomiseks ning kliendikaartide väljastamiseks on ettevõttele vajalik teatud hulk isikuandmeid. Kõige tüüpilisemad isikuandmed (ehk nn kohustuslikud väljad taotlusel) on kliendi nimi (nii ees- kui ka perekonnanimi), sünniaeg, kontaktaadress ja telefoninumber. Pea alati pakuvad ettevõtted võimalust valida informatsiooni saamist sooduspakkumiste ja kampaaniate kohta, sellisel juhul tuleb ka enamasti esitada e-posti aadress. Lisaks eelpoolmainitud isikuandmete hulgale küsitakse kõikvõimalikku lisainformatsiooni lähtuvalt ettevõtte spetsiifikast, näiteks kaubandusettevõtted on huvitatud kliendi perekonna suurusest (laste arv), ametist, kuu sissetulekust, eluasemest jne.

Mida kliendi isikuandmetega tehakse?
Ostu sooritades ning selle käigus kliendikaarti kasutades jääb enamikel juhtudel maha jälg: kas ainult ostusumma suurus või ka konkreetne soetatud kaupade/teenuste nimekiri, mida on võimalik siduda kliendikaardi omanikuga.

Seega olemasoleva isikuandmete hulgaga, sh sooritatud ostud, avaneb ettevõttel võimalus profileerida oma kliente, saada teada nende käitumisharjumusi ja ostueelistusi ning seeläbi edastada klientidele suunatud reklaame, mis lähtuvad konkreetsest kliendist. Näiteks ostes viimase kvartali jooksul poest suurel hulgal majapidamistarbeid, võib ettevõtte teha sellest järelduse, et kliendil on kodusisustamine pooleli ning edastab talle personaalseid pakkumisi ka mööbli ostmiseks.

Nagu juba ka eelpool mainitud, on pea alati kliendikaardi taotlusel välja toodud võimalus valida kas klient soovib saada informatsiooni sooduspakkumiste kohta. Soovitame alati kliendil kaaluda antud võimaluse kasutamist, kuna enamasti kaasneb nõusoleku andmisega suurel hulgal nii elektroonilistesse kui ka tavapostkastidesse laekuvaid reklaampakkumisi. Samuti võib ettevõte edastada kliendi isikuandmeid vaid

kokkulepitud ulatuses kolmandatele osapooltele, kelle eesmärkideks on näiteks otseposituste edastamine.

Kliendi isikuandmed kuuluvad kliendile!
Kui klient on otsustanud soetada mõne ettevõtte kliendikaardi, siis tuleb arvestada, et sellega loobub ta väikesest osast oma eraelu puutumatusest.

Lähtudes isikuandmete kaitse seadusest[24], on ettevõttel (seaduse mõistes andmete vastutav või volitatud töötleja) kohustus klienti (seaduse mõistes andmesubjekt) teavitada:

- millised on tema kohta käivad isikuandmed,
- millisel eesmärgil tema isikuandmeid töödeldakse,
- kellele neid edastatakse,
- kes on vastutav töötleja ja tema tegevuskoha aadress,
- millistel juhtudel on kliendil õigus nõuda tema isikuandmete töötlemise lõpetamist, parandamist, sulgemist ja kustutamist,
- millistel juhtudel on kliendil õigus saada juurdepääs tema kohta töödeldavatele isikuandmetele.

Kui klient leiab, et tema õigusi on rikutud, siis on kliendil alati õigus pöörduda Andmekaitse Inspektsiooni või kohtu poole. Esmaselt aga soovitame pöörduda andmete töötleja ehk ettevõtte, kelle kliendikaarti klient omab, poole.

Seega soovitame:

- Kliendikaardi taotlusele märkida minimaalsel hulgal isikuandmeid, mis on eelduseks kaardi saamisel;
- Kliendikaarti taotledes kaaluda sooduspakkumiste ja kampaaniate informatsiooni kasutamise võimalust või sellest loobumist;
- Küsida ettevõttelt teavet isikuandmete töötlemise kohta.

Andmekaitse Inspektsioon jätkab nimetatud teema analüüsi ja vajadusel täiendame ning avaldame uusi juhendmaterjale käsitletud valdkonnast.

Koostanud:

Maarja Kirss
nõunik
arengu- ja analüüsiosakond

[24] RTI, 16.03.2007, 24, 127

Statistika

	2004.a 30.11.03-1.12.04	***2005.a 30.11.04-1.12.05***	***2006.a 01.10.2005-30.09.2006***	**2007.a 1.01.2007-31.12.2007**
Seaduseelnõudele arvamuste andmine	50	48	36	47
Koolitused	15	30	34	34
Registreerimine				
Registreerimistaotlused kokku:	464	187	456	629
sh esmakordsed			139	218
sh korduvad			317	305
Muudatustaotlused			88	106
Antud delikaatsete isikuandmete töötlemise load	314	203	351	644
Muudatused registreeritud			70	106
Tagastamine puuduste kõrvaldamiseks				46
Keeldumised	76	29	2	0
Jäeti läbi vaatamata			2	2
Vaie (menetleja otsus)				1
Ettekirjutused			4	56
Andmekogudele arvamuste andmine	40	16	3	11

Järelevalve

Kohapealne kontroll kokku:	35	28	63	114
1) Siseriiklik kontroll	35	28	62	110
sh menetlusvajadusest tingitud			23	23
sh omaalgatuslik	8	8	39	76
Vormistatud kontrollakte				100
2) Rahvusvaheline/EU	-	-	1	4
sh menetlusvajadusest tingitud	-	-	-	3
sh omaalgatuslik	-	-	1	1
Vormistatud kontrollakte			-	2
Puuduseid ei tuvastatud			13	62
Tuvastati puudused			36	48
sh ettekirjutused			7	2
sh väärteomenetlused			0	0
Sunnirahad-trahvid			9	0
Vaie (menetleja otsus)			-	0
Arvamused töötlemise valmisolekuks			-	741

Menetlus	***2004.a 30.11.03-1.12.04***	***2005.a 30.11.04-1.12.05***	***2006.a 01.10.2005-30.09.2006***	***2007.a 1.01.2007-31.12.2007***
Selgitused, märgukirjad,	61	83	131	251
Vaided, kaebused				110
Vaie (menetleja otsus)				57
Omaalgatuslikud järelevalved				41
Rikkumist ei tuvastatud				130
Tuvastati rikkumine				26
Ettekirjutusi	7	9	22	36
Väärteod	5	8	15	4
Sunnirahad+trahvid				2
Kohtuasjad				1

Andmekaitse Inspektsioon esitab iga aasta 1. aprilliks Riigikogu põhiseaduskomisjonile ja Õiguskantslerile isikuandmete kaitse seaduse § 41[25] lõike 1 ja avaliku teabe seaduse[26] § 54 lõike 1 alusel ettekande seaduste täitmise ja rakendamisega seotud asjaolude kohta.

Andmekaitse Inspektsiooni tegevusvaldkonnaks on riiklik järelevalve isikuandmete töötlemise ja avalikule teabele juurdepääsu üle ning muude seadusega või seaduse alusel antud õigusaktiga pandud ülesannete täitmine.

Ettekande koostamise töögruppi kuulusid: Gina Kilumets (arengu- ja analüüsiosakonna juhataja), Maarja Kirss (arengu- ja analüüsiosakonna nõunik), Bert Blös (arengu- ja analüüsiosakonna nõunik) Stiina Liivrand (arengu- ja analüüsiosakonna nõunik).

[25] RT I 2007, 24, 127 Arvutivõrgust kättesaadav: https://www.riigiteataja.ee/ert/act.jsp?id=12909389
[26] RT I 2000, 92, 597 Arvutivõrgust kättesaadav: https://www.riigiteataja.ee/ert/act.jsp?id=12900546