Andmekaitse Inspektsiooni peadirektori
ÜLEVAADE
EL andmekaitsereformi rakendamise seisust Eestis 14.10.2016

Sisukord

I. Muutused Euroopa Liidu õiguses

25.05.2018 jõustub EL isikuandmete kaitse üldmäärus 2016/679.[1] Üldmäärus on otsekohalduv. Ta asendab senist andmekaitsedirektiivi 95/46 ning sellel põhinevaid liikmesriikide seadusi. Eestis seega isikuandmete kaitse seadust (IKS).

Samaaegselt jõustub ka andmekaitse reformipaketi teine akt – süüteomenetlusalane andmekaitse direktiiv 2016/680 (edaspidi tekstis: direktiiv).[2] See asendab politsei- ja kriminaalvaldkonna piiriüleste infosüsteemide ja infovahetuse raamotsust 2008/977. Direktiiv on sellest oluliselt laiem, normides ka riigisisest menetlust.

Üldmäärus ning direktiiv volitavad Euroopa Komisjoni andma erinevaid rakendusakte. Inspektsioonil puudub praegu teave nende valmimise kohta.

Eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi 2002/58 asemele koostatakse samuti uut määrust. See normiks isikuandmete kaitse erinõuded elektroonilise side valdkonnas – kordamata seda, mis juba on üldmääruses sätestatud.

Taustainfoks lisan, et liikmesriigid peavad 2018. a. maikuuks üle võtma ka uue võrgu- ja infoturbe direktiivi 2016/1148.[3] See normib infoturvet nii avalikus sektoris kui erasektori elutähtsates teenustes.

[1] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)

[2] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK

[3] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148, 6. juuli 2016, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus

II. Euroopa andmekaitseasutuste töörühma tegevused

Andmekaitse Inspektsioon osaleb andmekaitsedirektiivi artikli 29 alusel moodustatud Euroopa andmekaitseasutuste töörühmas (tulevases andmekaitsenõukogus). Seal praegu koostatavatest juhenditest tõstan esile järgmisi:

1) rahvusvahelise ettevõtte peamise tegevuskoha määratlemise juhend. Järelevalvet sellise ettevõtte üle hakkab juhtima peamise tegevuskoha järgse riigi andmekaitseasutus. Mõnikord võib määratlemine olla päris keeruline: juhatus on ühes, kuid kliendihaldust juhitakse teisest ja personalihaldust kolmandast riigist. Mõnikord võivad järelevalvet teostada ka teised andmekaitseasutused kas üksi või koostöös (vt. üldmääruse art. 56, 60-62);
2) andmete ülekantavuse juhend. See on uus põhimõte, mis annab kliendile õiguse viia teenusepakkuja vahetamisel oma isikuandmed masinloetaval kujul ühest ettevõttest teise (vt. üldmääruse art. 20);
3) andmekaitsespetsialistide (määrus nimetab neid ametnikeks) juhend. Andmekaitsespetsialist tuleb määrata kõigis avaliku sektori asutustes. Ettevõttes on määramine nõutav, kui põhitegevuseks on inimeste ulatuslik süsteemne jälgimine või ulatuslik delikaatsete andmete kogumine või avaliku ülesande täitmine. Juhend aitab andmekaitseasutustel seda kohustust ühtlustatult piiritleda (vt. üldmääruse art. 37-39, direktiivi art. 32-34);
4) juhend andmekaitselise mõjuhinnangu kohta, mida peab tegema kõrge riskiga andmetöötluse korral. See on uus nõue, mis asendab senist delikaatsete isikuandmete registreerimise kohustust. Juhend aitab seda veelgi lahtisemat nõuet ühtlustatult piiritleda (vt üldmääruse art. 35, direktiivi art. 27). Kõrge riski määratlus on oluline ka andmetöötlustoimingute registreerimise kohustuse ulatuse paikapanekuks (vt. üldmääruse art. 30, direktiivi art. 24, 25);
5) sertifitseerimise juhend. Andmekaitselise usaldusväärsuse kohta võib välja töötada vabatahtlikke märgiseid. Märgise, pitserite jms saamiseks võtab ettevõte endale vabatahtlikke kohustusi (vt. üldmääruse art. 42-43).

Lisaks valmistatakse asutuste vahelise koostöö hõlbustamiseks IT-platvormi ning mehitatakse tulevase Euroopa Andmekaitsenõukogu sekretariaati. Nõukogu koosneb liikmesriikide andmekaitseasutuste esindajaist ja Euroopa andmekaitseinspektorist. Sekretariaat on osa Euroopa andmekaitseinspektori ametkonnast, alludes samas nõukogu eesistujale.

Inspektsioon on avaldanud Andmekaitsenõukogu kodukorra koostamise käigus muret, kuna:

a) selle kohaselt on nõukogu asjaajamine kavandatud läbipaistmatuks (otsuseid ettevalmistav tegevus on vaikimisi salajane kuni otsuse vastuvõtmiseni),
b) kaotatud on tänases töörühmas kehtiv liikmete õigus lisada otsuste juurde eriarvamusi. Juhendiloome ja asutuste vaheliste erimeelsuste lahendamine on nõukogu ülesanded, mis on sarnased parlamendi ja kohtu tööga. Parlamendis ja kohtus on otsuse suhtes

vähemusse jäänuil on võimalik oma seisukohti selgitada. Lisaks on andmekaitsevaldkond suure „halli ala“ osakaaluga, kus arvamuste kujundamine ei tähenda valiku tegemist õige ja vale lahenduse vahel;

c) määrus peab silmas, et otsuseid teeb andmekaitseasutuste esindajaist nõukogu ning sekretariaat osutab nõukogule eeskätt administratiivset tuge. Tegelikult mehitatakse sekretariaati andmekaitsejuristidega, mitte administratiivse tugipersonaliga. Tänane töörühm võtab otsuseid vastu oluliselt vähem kui nõukogu ning tänaste otsuste tegemisel ei ole (lühikest) menetlustähtaega. Me ei tahaks olukorda, kus nõukogu asemel hakkab tegelikult otsuste sisu dikteerima ja õiguspraktikat kujundama anonüümne sekretariaat. Otsuste ettevalmistamise skeem (nõukogu, selle ekspertrühmade ja sekretariaadi rollid) tulnuks kokku leppida enne sekretariaadiametnike värbamist.

III. Inspektsiooni soovitused Eesti rakendusseaduse asjus

Direktiiv vajab üle võtmiseks liikmesriigi rakendusnorme. Üldmäärus on otsekohalduv, kuid paljud ta sätted vajavad samuti rakendusnorme. Mitmes valdkonnas on liikmesriigil kohustus või võimalus kehtestada lisa- ja erandsätteid.

Justiitsministeerium saatis 19.09.2016 kirja kõigile ministeeriumidele küsimaks seadusandluse ülevaadet, mida tuleks andmekaitse alal üle vaadata. Erilist tähelepanu paluti pöörata üldmääruse artiklile 23, mis lubab liikmesriikidel teha erisusi avaliku sektori jaoks. Justiitsministeerium loodab rakenduseelnõu valmis saada enne eesistumist, 2017. a. I pooles.

Inspektsioonil on rakendusseaduse asjus järgmised soovitused:

1) seniste erinormide säilitamine

Säilitada isikuandmete kaitse seaduse (IKS) erinormid uue rakendusseaduse erinormidena:

a) isikuandmete ajakirjandusliku avaldamise alal (IKS § 11 lg 2-3 vs art. 85),
b) füüsiliste isikute maksehäireandmete avaldamise alal (IKS § 11 lg 6-7),
c) kaamerate kasutamise alal (IKS § 11 lg 8 avalikus kohas ja avalikul sündmusel salvestamise kohta, § 14 lg 3 turvakaamerate kohta);
d) samuti on otstarbekas töösuhetes isikuandmete töötlemise reeglite osas säilitada tänane paindlikkus (IKS üldpõhimõtted + TLS § 11, § 28 lg 2 p 11), mida täiendavad inspektsiooni juhised. Puudub tungiv vajadus üldmääruse art. 88 kohaselt täiendavaid norme luua;

2) avaliku sektori avatus ja selle korrektiivid

Säilitada Eestile omane avaliku sektori teabe kättesaadavus (sh andmekogude avatus) ning andmekogude ristkasutus (sh andmete ainult üks korda esitamise põhimõte). Eeldan, et see vajab mitmel puhul eri- või lisasätteid vastavalt üldmääruse art. 23, art. 6 lg 2 ja 3. Karistusregistri avatuse säilitamine vastavalt art. 10 tuleb välja mõelda head põhjendused. Sama isikukoodi kasutamise kohta vastavalt art. 87.

Mõne registri puhul vajab aga senine avatus tõsist järelemõtlemist ja pigem kitsendamist. Pean silmas näiteks abieluvararegistrit, mille juurdepääsu ulatus pärineb paberkataloogi ajast. Veebipõhise juurdepääsu ja masinloetava allalaetavuse ajastul peaks seda piirama. Problemaatiline on näiteks ka füüsilisest isikust ettevõtjate (iseäranis registrist kustutatute) kontaktandmete avalikkus äriregistris – suure tõenäosusega kattuvad füüsilisest isikust ettevõtja ettevõtte kontaktandmed tema kui füüsilise isiku era-kontaktidega.

Üldmääruse kohaselt jääb liikmesriigi õigusega (Eestis avaliku teabe seadusega, AvTS) ettenähtud juurdepääs avalikule teabele (üldmääruses: ametlikele dokumentidele) püsima (art. 86). Siiski vajab kaalumist, kas AvTS-s üldmäärust dubleeriv iseenda andmetele juurdepääsu aspekt (vt nt § 14 lg 2, ristviitena ka § 39 kaudu) peaks alles jääma. Ilmselt võiks, sest ta sätestab kiirema vastamistähtaja (5 tööpäeva, pikendus 15 tööpäevani, § 18, 19) kui üldmäärus

(1 kuu, pikendus kahe kuu võrra, art. 12 ja 15). Üle tuleb vaadata tasu küsimus (AvTS § 25-27 vs. art. 12 lg 5)

3) rahvatervise ja sotsiaalkaitse alal hoiduda halduskoormuse suurendamisest

Tervishoid ja sotsiaalkaitse on see valdkond, kus tundlike isikuandmete kontsentratsioon on kõige suurem.

Andmekaitselise mõjuhinnangu tegemist nõuab üldmäärus üksnes siis, kui isikuandmete töötlemine on esiteks kõrge riskiga ja teiseks ulatuslik (art. 35). Mõjuhinnangu tegemise nõude alt jäävad seega välja väiksemad tervishoiu- ja sotsiaalkaitse asutused (nt. perearstipraksised, üksikapteegid, hooldekodud), sest nende andmetöötlus ei ole ulatuslik (vt üldmääruse 91. põhjenduspunkti lõppu).

Paraku on inspektsiooni hinnangul just nende riskitase kõrgem ja teadlikkus madalam kui suurtel töötlejatel. Mõistlik oleks riigisiseselt kehtestada tervishoiu ja sotsiaalkaitse valdkonnas üldine andmekaitselise mõjuhinnangu tegemise kohustus – andmetöötlejad ise hindavad ja maandavad oma riskid. Paraku näib, et üldmäärus seda ei võimalda.

See-eest lubab üldmäärus liikmesriikidel kehtestada rahvatervise ja sotsiaalkaitse valdkonnas üldise eelkonsulteerimis- ja loanõude – töötlemise ulatust ja riskitaset arvestamata (art. 36 lg 5, art. 58 lg 3 p. c).

Kuid lisaks peavad kõik tervishoiuteenuste osutajad niigi saama tegevusloa Terviseametist, sotsiaal(hoolekande)teenuse osutajad Sotsiaalkindlustusametist või maavalitsustelt.

Kahekordne loakohustus oleks ülemäärane halduskoormus teenuseosutajaile ning ebamõistlik ressursikasutus järelevalveasutustele. Seetõttu võiks tervishoiu- ja hoolekande alal olemasolev valdkondlik loamenetlus hõlmata ka infoturvet. Täiendavaid kohustusi art. 36 lg 5 alusel ei peaks kehtestama;

4) vältida halduskoormuse kasvu ka teistes reguleeritud valdkondades

Isikuandmete töötlemise ja turvalise hoidmise reeglistikul on kokkupuude rahandusettevõtete (pangandus, muu krediiditurg, kindlustus, väärtpaberiturg) teenuste ning saladuse hoidmise valdkondlike reeglitega.

Samuti on isikuandmete reeglistikul kokkupuude turvaettevõtjate ja sideettevõtjate teenuste ja infoturbereeglitega. Kõigis neis valdkondades kehtib tegevusloa nõue.

Mõistlik oleks nende valdkondade infoturbereeglid üle vaadata ning siduda nende täitmine vastava tegevusloa saamise ja säilitamisega. Nii on võimalik paremini arvestada valdkondlike eripäradega ning vältida vertikaalse valdkonnajärelevalve ja horisontaalse andmekaitse dubleerimisest tulenevat halduskoormust. Järelevalvelise dubleerimise vältimine hoiab kokku ka riigi ressurssi.

Kaaluda võib samasugust lähenemist veel kahes valdkonnas, kus on kõrgem ootus andmetöötluse usaldusväärsusele ning kehtib tegevusloa nõue: postiteenus ja hasartmängu korraldamine;

5) säilitada teadusuuringute loamenetlus, jätta sellest välja ajaloo-uuringud

Säilitada teadusuuringute loamenetlus (tänane IKS § 16) kui kolmas alternatiiv seadusekohase ja nõusolekupõhise teadusuuringu kõrval. Topeltprotseduuride vältimiseks võrdsustada loamenetluse läbimine üldmääruse-kohase eelkonsulteerimisega (art. 36).

Jätta loamenetlusest välja ajaloo-uuringud. Teadusuuringu loamenetlus on mõeldud nende teadushariduse tarvis, kus sisendiks on isikuandmed ja väljundiks üldistused; ajalooteaduses on isikuandmed aga reeglina ka väljundiks. Ajaloo-uuringuid saab katta arhiiviseadusega;

6) lubada interneti-teenuse kontod avada vähemalt 13-aastastel

Määrata interneti-teenuste konto avamise vanus 13 aasta peale (liikmesriigi valik vahemikus 13-16 aastat) vastavalt art. 8;

7) surnute andmete kaitserežiim

Tänane isikuandmete kaitse seadus tagab teatud kaitserežiimi surnu andmetele 30 aastaks. Üldmäärus ei hõlma surnute andmeid, kuid annab liikmesriigile õiguse vastavaid erinorme kehtestada. Inspektsiooni hinnangul on hädavajalik kaitserežiim pärilike haiguste andmete osas (kusjuures 30 aastat surmast on liiga lühike).

Muus osas võiks surnute andmete suhtes pieteedi tagamise lisada arhiiviseadusse;

8) andmekaitse järelevalveasutuse staatus

Andmekaitse Inspektsiooni tänane staatus (sisutegevuse sõltumatuse tagatistega valitsusasutus, peadirektori voliniku-laadne seisund) üldiselt vastab üldmääruse sõltumatuse ja tõhusate volituste nõuetele. Täiendavalt vajab normimist:

a) kõrgemalseisva asutuse (ministeeriumi) teenistusliku järelevalve ulatus (VVS 7. ptk). Teenistusliku järelevalve korras sekkumist on täna kitsendatud vaid riiklikus järelevalves. Kuid sekkuda saab esiteks haldusjärelevalvesse ning teiseks kõigisse järelevalve-välistesse ülesannetesse (loamenetlused, eelkonsulteerimine, andmekaitsenõukogus osalemine, juhendiloome). Probleem on laiem kui kitsalt andmekaitsereformi rakendamine;
b) inspektsiooni peadirektori asenduskorra, inspektsiooni põhimääruse ja tööplaani kehtestamine võiks liikmesriikide Schengeni infosüsteemi alase hindamise käigus kujunenud seisukohtadega arvestades olla inspektsiooni enda pädevuses;
c) inspektsiooni ühiskondlikule nõukojale kõrgema ehk seadusjärgse staatuse andmine. Nõukoja põhifunktsioon on avaldada arvamust inspektsiooni juhendite kohta. Andmekaitseline juhendiloome puudutab ühiskondlikke väärtusi ning selle legitiimsus ei ole piisav, kui see sünnib vaid ametnike loominguna;
d) inspektsiooni peadirektori julgeolekukontrolli tegemise võiks sarnaselt prokuröridega anda Kaitsepolitseiametilt üle Teabeametile (viimasega inspektsioonil puuduvad järelevalvelised kokkupuuted);

9) andmekaitse järelevalveasutuse volitused ja menetlusreeglid

Andmekaitse Inspektsiooni tänased volitused ja menetlusreeglid üldiselt tagavad tõhusad hoovad andmekaitsereeglite täitmise tagamiseks. Täiendavad ettepanekud sel alal:

a) Riigikohtu 11.05.2015 otsuse nr 3-3-1-90-14 valguses võib olla vajalik inspektsiooni menetluspädevuse täpsustamine haldusjärelevalve alal. Riigikohus leidis, et haldusjärelevalve hõlmab üldjuhul vaid haldusorganeid Vabariigi Valitsuse seaduse mõttes; põhiseaduslikele institutsioonidele laieneb haldusjärelevalve üksnes erinormi olemasolul. Üldmäärust saab ilmselt pidada erinormiks. Siiski on mõistlik täpsustada art. 55 lõiget 3, mille kohaselt andmekaitsejärelevalve ei hõlma kohtuid õigusemõistmise osas. Vajalik on selgus, mis ulatuses hõlmab andmekaitsejärelevalve kohtu muid tegevusi. Seda eeskätt kohtukantselei tegevuse osas ning kohtulahendite ja karistusandmete kohtumenetluse-järgse avalikustamise osas. Kohtute sõltumatus on niivõrd oluline küsimus, et võimalikud vaidlused tuleks rakendusseadusega ennetada. Samuti on Riigikohtu eelviidatud otsuse valguses mõistlik vaadata üle inspektsiooni haldusjärelevalve ulatus inspektsiooni muude ülesannete osas (avaliku teabe juurdepääs, juurdepääsupiiranguga teabe kaitse, andmekogude pidamise järelevalve);
b) seadusandlik tugi *online*- ehk võrgupõhisele menetlusele: andmekaitseametniku määramisteate (art. 37 lg 7), rikkumisteate (art. 33), samuti kaebuse (art. 57 lg 2), selgitustaotluse, märgukirja esitamiseks. See peaks võimalikult palju vähendama käsitsi-sisestust ja vigade-puudustega tegelemist (seotus dokumendiregistriga, etteantud valikvastuseid, vigade automaatkontroll, automaatõpetused, masinotsused). Vajalik on volitusnorm üleminekuks kohustuslikule võrgupõhisele menetlusele (siis, kui infosüsteem seda võimaldab). Üldmääruse art. 57 lg 1 punktis „u“ nimetatud registri (rikkumised/järelevalved, hoiatused, karistused) saab ühitada asutuse dokumendiregistriga;
c) delikaatsete isikuandmete töötlemise register (IKS 5. ptk) likvideeritakse, samuti kustutatakse viited selle kohta teistes seadustes. Mida teha aga registreerimise alternatiivina registrisse kantud vastutavate isikutega? Avaliku sektori asutuste osas oleks mõistlik muuta nad automaatselt andmekaitsespetsialistideks (-ametnikeks). Erasektori osas oleks see aga problemaatiline, sest tänane registreerimiskohustus ja tulevane andmekaitseametniku määramise kohustus on erineva ulatusega;
d) Eesti andmekaitseasutusel ei ole eriseaduste kohaselt, mis sisaldavad ammendavat juurdepääsuõiguste loetelu, juurdepääsuõigust maksusaladusele (kuigi maksuhalduri tegevust kontrollib inspektsioon nii IKS kui AvTS alusel) ega pangasaladusele (kuigi inspektsioon kontrollib panga tegevust IKS alusel). See on vastuolus üldmäärusega;
e) võimalus teha kokkuleppelist ühisjärelevalvete teiste riigisiseste järelevalveasutustega (mitte viia läbi korraga kahte menetlust, vaid ühist menetlust, nii vähendame halduskoormust). Koostöövajadus on näiteks Tarbijakaitseametiga, Riigi Infosüsteemi Ametiga, Terviseametiga, Sotsiaalkindlustusametiga, Tööinspektsiooniga, Finantsinspektsiooniga jne. Loomulikult ei ole see andmekaitse-spetsiifiline küsimus, vaid üldine halduskorralduse küsimus, mille lahendus peaks hõlmama ka inspektsiooni.

Inspektsiooni puhul on see vajadus kõige akuutsem (isikuandmete töötlemine on läbi põimunud valdkondlike eriregulatsioonidega ja nende järelevalvega);

f) nn. populaarkaebused (art. 80) tuleks jätta seadustamata, kuna Eesti õiguses on see juba kaetud märgukirjaga;
g) kontrollostu tegemine – erinevalt Tarbijakaitseametist ei ole inspektsioonil sellise meetme kasutamise õigust. Korrakaitseseaduse loogika kohaselt peavad aga kõik erimeetmed olema ammendavalt seaduses loetletud;
h) avaliku sektori andmekogud peavad üldjuhul enne riigi infosüsteemi haldussüsteemis registreerimist läbima kooskõlastusmenetluse Andmekaitse Inspektsioonis. Tundliku sisuga andmekogude puhul on tõenäoline ka üldmääruse- või direktiivi-kohane mõjuhinnangu nõue. Andmekoosseisust tuleneva sagedusega (iga 2, 3 või 4 aasta tagant) peavad andmekogud läbima ka infoturbeauditi. Mõistlik oleks andmekogude pidajaid mitte ülemääraselt koormata ning anda kooskõlastamisele ja auditile ka mõjuhinnanguline tähendus;

10) halduskaristuste sobitamine Eesti õigusse

Üldmäärus kehtestab konkurentsiõiguse eeskujul halduskaristustena trahvid kuni 20 mln eurot või kuni 4% eelneva majandusaasta üleilmsest käibest (art. 88). Üleilmsete hiidettevõtete jaoks kujundatud trahvimäärad ei sobi füüsiliste isikute, samuti väiksemate ettevõtete karistamiseks. Eestis tuleks haldustrahve kohaldada väärteokaristustena (vt. põhjenduspunkt 151). Väärteokaristus on suunatud füüsilistele isikutele, juriidilise isiku karistamine on väga kohmakalt rakendatav erand. Väärteomenetlusõigus vajab ses osas uuendamist, EL õigus loob sarnaseid ettevõtteile (mitte ettevõtte töötajaile) suunatud haldustrahve ka väljaspool andmekaitset.

Inspektsioon eelistab jätkuvalt rikkumistele reageerimiseks sunniraha (sunniraha määramisele eelneb sunniraha hoiatust sisaldav ettekirjutus);

11) rakendusseaduse rakenduskulud

Andmekaitse Inspektsiooni majanduskulud kindlasti kasvavad, kuna andmekaitseasutuste koostöös, eeskätt Euroopa andmekaitsenõukogus osalemine suurendab. Ebaselge on veel tõlkekulude vajadus kaebuste edastamisel andmekaitseasutuste vahel.

Andmekaitsereformi rakendamise eel ja järel kasvab inspektsiooni töökoormus vähemalt ajutiselt. Püsiva hinnangu saab teha 2019. aastal. Eeltoodud ettepanekud nr 3 ja 4 aitaksid vähendada inspektsiooni tööjõukulude kasvu vajadust;

12) andmekaitsespetsialisti kutseoskused ja teadmised

Seda teemat, mis samuti vajab rakendusseaduses käsitlemist, analüüsitakse järgmise peatüki 1. alajaotuses.

IV. Inspektsiooni tegevused

1. Prioriteediks on andmekaitsespetsialistide kvalifikatsioon

Üldmäärus (art. 37-39) näeb ette, et kõik avaliku sektori asutused ning tundlike isikuandmete töötlejad äri- ja mittetulundussektoris peavad määrama andmekaitsespetsialisti (keda määrus nimetab ebaõnnestunult tõlgituna andmekaitseametnikuks).

Sisuliselt vastab andmekaitsespetsialistile tänases Eesti seaduses ettenähtud isikuandmete töötlemise eest vastutav isik. Andmetöötleja määrab vastutava isiku alternatiivina delikaatsete isikuandmete töötlemise registreerimisele. Vastutavaid isikuid on määratud üle 1100.

Kuid erinevalt mõnest teisest liikmesriigist on Eestis seni puudunud andmekaitsespetsialistide (vastutavate isikute) kvalifikatsiooninõuded. Mitmes riigis peavad andmekaitsespetsialistid läbima kvalifikatsiooni hindamise. Riikliku eksamineerimise kõrval on ka mitmeid vabatahtlikke eksamineerimis- ja sertifitseerimissüsteeme.

Tänane 11-leheküljeline IKS asendub 99-leheküljelise otsekohalduva üldmääruse, 49-leheküljelise direktiivi ning rohkete rakendusaktide ja -juhenditega. Teema valdamiseks on vajalik varasemast oluliselt põhjalikum juriidiline ettevalmistus.

Teiseks annavad üldmäärus ja direktiiv õigusnormi kaalu vaikimisi ja lõimitud andmekaitse printsiipidele, mis eeldavad rakendamiseks ka infotehnoloogilist asjatundlikkust. Infoturbe puudujäägid saavad üldmääruse jõustumisel olema ettevõttele/asutusele oluliselt raskemate tagajärgedega. Infotehnoloogia kiire areng nõuab samuti pidevat tööd kvalifikatsiooni omandamiseks ja säilitamiseks.

Inspektsiooni hinnangul ei taga Eesti kõrgkoolis omandatud õigusteaduse või infotehnoloogia alane kraad uutele vajadustele vastavat kutsekvalifikatsiooni. Isegi kui kiiresti täiendada õppekavasid, ei tagaks see andmekaitsereformi jõustumise järel piisavat hulka piisavalt kvalifitseeritud spetsialiste.[4]

Ettevõtteil ja asutustel, kes endale andmekaitsespetsialisti palkavad või teenuse sisse ostavad, on aga vaja kindlust, et nad saavad kvalifitseeritud teenust. Teenusepakkujal on aga vaja tõendada, et tal on eeldus saada tööga hakkama.

Kestlikuks lahenduseks oleks andmekaitsespetsialistide kutsestandardi kehtestamine ja kutse andmise protsessi käivitamine kutseseaduse alusel. Kutseseaduses ettenähtud riigihanget ja muid protseduure arvestades läheb sellega aga aega.

Seetõttu on mõistlik juba alustada inspektsiooni poolt andmekaitsespetsialisti soovitusliku kompetentsistandardi koostamisega koostöös ettevõtlus- ja erialaorganisatsioonidega. Seda

[4] Eestis vajaminevate andmekaitsespetsialistide arvu osas uuringud puuduvad. Üle Euroopa nõuab üldmääruse rakendamine erasektoris vähemalt 28 tuhandet andmekaitsespetsialisti (avalikku sektorit arvestamata). Vt Rita Heimes & Sam Pfeifle, Study: At least 28,000 DPOs needed to meet GDPR requirements, THE PRIVACY ADVISOR, Apr. 19, 2016, https://iapp.prog/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements.

standardit saavad kasutada kõrgkoolid ja teised koolitajad. Inspektsioonil endal ei ole võimalik koolitajaks hakata.

Üleminekulahendusena – kuni kutseseaduse-põhise kutse andmise protsessi käivitamiseni – võib inspektsioon ise korraldada soovijaile enda koostatud kompetentsistandardi alusel eksameid. Eksami korraldamise otsesed kulud kaetaks vastavast teenustasust.

Nii oleks võimalik käivitada ajanõuetele vastav andmekaitsespetsialistide professionaliseerumine.

Samas ma ei poolda vähemalt erasektoris üldiste kvalifikatsiooninõuete seadusega kohustuslikuks muutmist.

2. Andmetöötlejate olulisemate kohustuste piiritlemine

Euroopa andmekaitseasutuste töörühma juhendite alusel koostab inspektsioon juhendid, millega piiritletakse andmetöötlejate kohustus:

a) teha mõjuhinnang (üldmääruse art. 35, direktiivi art. 27, art. 57 lg 1 p k),
b) registreerida töötlemistoimingud (üldmääruse art. 30, direktiivi art. 24, 25),
c) määrata andmekaitsespetsialist (üldmääruse art. 37-39, direktiivi art. 32-34),
d) esitada rikkumisteade (üldmääruse art. 25, direktiivi art. 31).

Mõjuhinnangu tegemise nõude piiritlemise osas peab juhendi esitama Euroopa andmekaitsenõukogule kooskõlastamiseks – vt üldmääruse art. 64 lg 1 p. a. Võimalik, et viivituse vältimiseks (mõjuhinnangu tegemise nõue jõustub 25. maist 2018, kuid ka nõukogu ise käivitub alles samast kuupäevast) lepitakse kokku, et kuni nõukogu käivitumiseni esitatakse juhendid kooskõlastamiseks tänasele andmekaitseasutuste töörühmale;

3. Näidised ja meelespead

Selleks, et ettevõtete ja asutuste rakenduskulud ülemääraselt ei kasva, koostab ja avaldab inspektsioon näidisdokumendid ja meelespead. Eeskätt pean silmas üldmääruse artikleid 7 (nõusoleku andmise tingimused) ning artikleid 12-22 (andmesubjekti õiguste kaitse ja talle teabe andmine).

4. Muud võimalikud juhendid

Inspektsioon:

a) koostab kaebuse näidisvormi, sh elektroonilise (üldmääruse art. 57 lg 2);
b) võib koostada vastutava ja volitatud töötleja vaheliste suhete kohta või volitatud töötleja ja tema kaasatud volitatud töötleja vaheliste suhete kohta tüüptingimused (üldmääruse art. 28 lg 8, art. 57 lg 1 p „j“, art. 58 lg 3 p. g“) – aga need esitatakse andmekaitsenõukogule arvamuse saamiseks (art. 64 lg 1 p „d“);

c) peab koostama vabatahtliku sertifitseerimise kriteeriumid (üldmääruse art. 42 lg 5, art. 57 lg 1 p „m“, art. 58 lg 3 p. „f“) – Eesti-siseselt siis, kui nende järgi tekib vajadus; EL-tasemel võib neid koostada andmekaitsenõukogu;
d) kui erasektor tuleb välja toimimisjuhendite ja sertifitseerimisettepanekutega, siis peab koostama toimimisjuhendite järelevalvaja ja sertifitseerimisasutuse akrediteerimise tingimused (üldmääruse art. 41, art. 43, art. 57 lg 1 p. „p“) – aga mõlemad esitatakse andmekaitsenõukogule arvamuse saamiseks (art. 64 lg 1 p „c“);
e) võib koostada 3. riiki isikuandmete edastamiseks standardsed andmekaitseklauslid, mille Komisjon peab heaks kiitma (üldmääruse art. 46 lg 2 p. „d“, art. 58 lg 3 p „g“ nimetab neid tüüpklausliteks) – need esitatakse andmekaitsenõukogule arvamuse avaldamiseks (art. 64 lg 1 p. „d“);

Üle tuleb vaadata ka inspektsiooni senised juhendid.

5. Toimimisjuhendid ja sertifitseerimine

Erasektori Eesti-tasemel vabatahtlike toimimisjuhendite ja sertifitseerimise ala on vajalik teha koostööd Tarbijakaitseametiga, tagamaks, et nad hõlmaksid nii andmekaitse kui tarbijakaitse aspekte.

Viljar Peep