18.04.2017

ISIKUANDMETE KAITSE UUE ÕIGUSLIKU RAAMISTIKU KONTSEPTSIOON

Sisukord

1. Sissejuhatus ja eesmärk

Tehnoloogia on viimase paarikümne aastaga läbi teinud murrangulise arengu – nii näiteks on 21. sajandil laialdaselt levinud nii nutitelefonid, kiire internetiühendus kui ka erinevad e-lahendused, mille abil on võimalik kiirelt ja hõlpsalt edastada ning töödelda isikuandmeid. Kiire tehnoloogia areng on tinginud vajaduse infoühiskonnale vastava õigusraamistiku järele isikuandmete kaitse valdkonnas, kuivõrd uute tehnoloogiate kasutuselevõtuga on isikuandmete töötlemine võimalik senisest kiiremalt ning ulatuslikumas mahus. Võttes arvesse ulatuslikku tehnoloogilist arengut ning majanduse globaliseerumist, on Euroopa Liit (edaspidi *EL*) tõdenud, et andmekaitsereegleid tuleb kohandada digiajastu vajadustega ning luua õigusraamistik, mis arvestaks vajalikul määral majanduse vajadustega, tagades seejuures kõrge isikuandmete kaitse taseme.[1]

Õigus isikuandmete kaitsele on lahutamatu osa õigusest eraelu puutumatusele ning kohustus tagada isikuandmete kaitse tuleneb nii Euroopa inimõiguste ja põhivabaduste kaitse konventsioonist kui ka Eesti Vabariigi põhiseadusest (edaspidi *PS*). Füüsiliste isikute kaitse isikuandmete töötlemisel on Euroopa Liidu põhiõiguste harta artikli 8 lõikes 1 ja Euroopa Liidu toimimise lepingu artikli 16 lõikes 1 sätestatud põhiõigus. Eestis reguleerib isikuandmete kaitse valdkonda isikuandmete kaitse seadus[2] (edaspidi *IKS*), mis võtab üle Euroopa Parlamendi ja nõukogu direktiivi 95/46/EÜ[3].

Euroopa Liit on viimastel aastatel isikuandmete kaitset puudutava teemavaldkonna uuendamisega põhjalikult tegelenud ning selle tulemusena on vastu võetud järgnevad õigusaktid:

- Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (edaspidi *üldmäärus*) (ingl. k. *General Data Protection Regulation, GDPR*)[4].
- Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 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[5] (*edaspidi õiguskaitsevaldkonna direktiiv)*.

Üldmäärust hakatakse kohaldama alates 2018. aasta 25. maist (üldmääruse art 99 lg 2) ning see on tervikuna siduv ja vahetult kohaldatav kõikides Euroopa Liidu liikmesriikides. Määruse eesmärgiks on ajakohastada kehtivad andmekaitsereeglid, võttes arvesse majanduse digitaliseerumist, uute tehnoloogiate kasutuselevõttu ning piiriüleste tehingute arvu kasvu.

---

[1] Vt lähemalt Euroopa Komisjoni pressiteade, http://europa.eu/rapid/press-release_IP-12-46_et.htm.

[2] Isikuandmete kaitse seadus RT I 2007, 24, 127; RT I, 06.01.2016, 1 https://www.riigiteataja.ee/akt/106012016010.

[3] Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT L 281, 23.11.1995, lk 31).

[4] ELT L 119, 04.05.2016, lk 1–88.

[5] ELT L 119, 04.05.2016, lk 89 –131.

Hetkel reguleerib riigisisesel tasandil isikuandmete kaitse õigust üldseadusena IKS, mis põhineb direktiivil 95/46/EÜ. Alates 2018. a 25. maist asendab üldmäärus direktiivi 95/46/EÜ, sest üldmääruse art-ga 94 tunnistatakse direktiiv 95/46/EÜ kehtetuks. Kuna IKS põhineb direktiivil, mis tunnistatakse kehtetuks, tuleb riigisiseselt kehtiv ja direktiivi üle võtnud IKS omakorda tunnistada kehtetuks, kuivõrd tulevikus tuleb esmajärjekorras lähtuda otsekohalduvast EL üldmäärusest. Üldmääruse sätete üldmääruses lubatud ulatuses täpsustamiseks ning konkretiseerimiseks koostab Justiitsministeerium uue IKS tervikteksti, mis hõlmab üldmääruse rakendamist. On hetkel kaalumiskoht, kas lisada samasse seadusesse ka direktiivi ülevõtvad sätted.

Üldmäärusest ja õiguskaitsevaldkonna direktiivist koosnev andmekaitsepakett on digitaalse ühtse turu[6] ja ELi julgeoleku tegevuskava[7] toimimiseks võtmetähtsusega. Nende strateegiate elluviimisel on olulise tähtsusega ka EL liikmesriikide poolne panus EL õigusnormide rakendamisel ja ülevõtmisel – laiemalt on reformi eesmärgiks tagada isikuandmete kaitse valdkonnas õiguslikult ühtne lähenemine kõigis 28-s EL liikmesriigis, et tagada andmete vaba liikumine ning isikuandmete kaitse kõrge tase.

EL andmekaitsereformi üheks peamiseks eesmärgiks on tugevdada üksisiku ehk andmesubjekti kaitset uutes digiajastu tingimustes, andes isikule senisest suurema kontrolli oma andmete üle. Reformiga suurenevad näiteks oluliselt isiku võimalused nõuda teda puudutavate andmete töötlemise lõpetamist ning andmete kustutamist, samuti on isikul tulevikus lihtsam kaitsta oma õigusi ning saada rikkumiste korral tõhusamalt hüvitist.

Üldmääruse põhjenduspunkt (edaspidi *pp*) 8 kohaselt võivad liikmesriigid sidususe seisukohast vajalikul määral ja liikmesriigi õiguse sätete arusaadavaks muutmiseks isikutele, kelle suhtes neid kohaldatakse, integreerida määruse elemente oma õigusesse, kui üldmääruses on ette nähtud eeskirjade täpsustamine või piiramine liikmesriigi õigusega. Seega on Justiitsministeeriumil pärast kontseptsiooni saatmist kooskõlastusringile plaanis esitada kooskõlastamiseks ka üldmääruse rakendamise seaduse ning direktiivi ülevõtmise eelnõu.

Kontseptsioonis ja eelnõus nähakse üldmääruse puhul ette ainult nende teemavaldkondade reguleerimine, milleks üldmäärus *expressis verbis* võimaluse ette näeb. Üldmääruse norme riigisisesesse õigusesse ümber ei kirjutata, kuivõrd andmekaitse üldmääruse puhul on tegemist EL liikmesriikide jaoks otsekohalduva õigusaktiga. Riigisisesel seadusandjal on üldmääruse puhul võimalus sätestada oma õiguses üksnes need aspektid, mida üldmäärus ei reguleeri ja kus üldmäärus on jätnud liikmesriigile otsustusõiguse. Euroopa Kohus on märkinud, et EL määrused tulevad liikmesriigi õiguskorda automaatselt ning nende ülevõtmine pole mitte ainult üleliigne, vaid ka vastuolus EL õigusega.[8] Seega üldmäärust Eesti seadusandlusesse ümber ei kirjutata ega dubleerita. Kõik riigisisesed isikuandmete kaitset puudutavad õigusnormid peavad üldmääruse kohaldamise ajaks (25. mai 2018) olema täielikus kooskõlas üldmäärusega, sest vastuolu korral kehtib üldmäärus, mistõttu reguleeritakse üldmääruse rakendamise seaduses ainult neid küsimusi, milleks üldmäärus liikmesriigile volituse annab.

---

[6] Vt lähemalt digitaalse ühtse turu kohta: http://ec.europa.eu/priorities/digital-single-market/.

[7] Vt lähemalt ELi julgeoleku tegevuskava kohta: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

[8] Euroopa Kohtu 07.02.1973 otsus, Euroopa Komisjon *vs.* Itaalia, C-39/72, ECLI:EU:C:1973:13 ja Euroopa Kohtu 02.02.1997 otsus, Amsterdam Bulb BV *vs.* Produktschap voor Siergewassen, C-50/76, ECLI:EU:C:1977:13.

Andmekaitsereformi sihtrühmaks üldmääruse puhul on nii avalik kui ka erasektor, kuivõrd üldmäärus on mõningate üldmääruses toodud erisustega kohaldatav mõlemale. Reformist on puudutatud kõik füüsilised isikud, kelle isikuandmeid töödeldakse, ning need füüsilised ja juriidilised isikud (nii avalik kui ka erasektor), kes isikuandmeid töötlevad. Menetlejana on üldmääruse puhul õiguslikest muudatustest mõjutatud Andmekaitse Inspektsioon kui sõltumatu riiklik järelevalveasutus.

Andmekaitsereformi riigisiseses õiguses rakendamise ja ülevõtmise eesmärgiks on viia Eesti seadusandlus vastavusse Euroopa Liidu õigusega. Samuti aidata EL liikmesriigina kaasa vabadusel, turvalisusel ja õigusel rajaneva ala ning majandusliidu saavutamisele, majanduslikule ja sotsiaalsele arengule, riikide majanduse tugevdamisele ja lähendamisele siseturul ning füüsiliste isikute heaolule (üldmääruse pp 2). Üldmäärus lähtub ideest, et füüsiliste isikutel peaks olema kontroll oma isikuandmete üle ning tugevdada tuleks õigus- ja tegelikku kindlust füüsiliste isikute, ettevõtjate ja avaliku sektori asutuste seisukohast (üldmääruse pp 7).

Õiguskaitsevaldkonna direktiivi ülevõtmise tähtajaks on 6. mai 2018.a (art 63 lg 1). Tulenevalt EL toimimise lepingu artiklist 288 on direktiivid liikmesriikidele siduvad saavutatava tulemuse osas. Seejuures jääb liikmesriigi otsustada direktiivis sätestatud tulemuse saavutamiseks vajalike muudatuste riigisiseses õiguses rakendamise meetod ja vorm. Seega peab Eesti tagama, et riigisisesed õigusnormid oleksid kooskõlas direktiivis sätestatud põhimõtetega, täidaks direktiivist tulenevaid eesmärke ja saavutaks nõutava tulemuse.

Õiguskaitsevaldkonnas kehtib ELis hetkel raamotsus 2008/977/JSK, mis reguleerib andmekaitset piiriülese kriminaalõigus- ja politseialase koostöö raames. Seega käesoleval hetkel ei kehtesta EL õigus andmekaitsereegleid, mis kohalduks politsei ja teiste pädevate asutuste tegevusele väljaspool piiriülest koostööd. Vastava valdkonna reguleerimine on seni olnud liikmesriikide pädevuses. Lissaboni lepinguga laiendati mõnevõrra Liidu pädevust andmekaitse osas, nähes ette eraldiseisva kohustuse tagada igaühe õiguse isikuandmete kaitsele (ELTL art 16 lg 1). See andis ELile võimaluse luua reeglid ka õiguskaitsevaldkonnas, kuivõrd erinevalt kehtivast korrast ei vaadelda andmekaitset enam üksnes majanduskeskkonna arengut soodustava õigusvaldkonnana, vaid eelkõige põhiõiguste kontekstis.

Kehtiva andmekaitsedirektiivi 95/46/EÜ ülevõtmisel otsustas Eesti laiendada isikuandmete kaitse seaduse reguleerimisala ka nn õiguskaitsevaldkonnale ning hetkel hõlmab IKSi kohaldamisala kogu Eesti territooriumil toimuvat andmetöötlust igas valdkonnas (erandiks on siinkohal isikuandmete töötlemine isiklikul otstarbel ning riigisaladuse regulatsioon). IKS § 2 lg 2 sätestab, et IKSi kohaldatakse ka kriminaalmenetlusele ja kohtumenetlustele menetlusseadustikes sätestatud eranditega. Sellest tulenevalt kehtib hetkel IKS ka väärteo- ja kriminaalmenetluses nii kohtuvälise, kohtueelse kui kohtumenetluse faasis. Õiguskaitsevaldkonna direktiivi eesmärk on kehtestada EL-s ühtsed andmekaitsereeglid ka nn õiguskaitsevaldkonnas. Erinevalt raamotsusest on direktiivi kohaldamisala laiem, hõlmates kogu andmetöötlust pädevate asutuste poolt juhul, kui selline andmetöötlus leiab aset asutuste põhiülesannete täitmise raames. Praegusel ajal on raamotsuse sätted üle võetud Eesti õigusesse eelkõige IKSi kui üldseadusega ning täiendavalt KrMS §-dega 489^3 - 489^5.

2. Uuringud ja analüüsid

Eurobaromeeter on 2015. aastal koostanud isikuandmete kaitse kohta Euroopas laiaulatusliku raporti[9]. Raporti tulemustest selgub näiteks, et ainult 15% uuringus osalenutest tundsid, et nad omavad kontrolli nende andmete üle, mille nad internetis esitavad, ning ligi kolmandik ehk 31% leidsid, et neil puudub sellekohane kontroll sootuks. 67% vastanutest pidasid probleemseks, et neil polnud täit kontrolli nende andmete üle, mida nad internetis esitasid. Üle poolte vastanutest (57%) ei nõustunud väitega „isikuandmete esitamine ei ole minu jaoks oluline küsimus“[10]. Eeltoodud näidete pinnalt nähtub, et EL-is on isikuandmete kaitse aktuaalne ning tähelepanu vajav teema. Seetõttu on õigustatud muudatused isikuandmete kaitse õiguse valdkonnas, mis vastaksid õigussubjekti tänapäevastele ootustele.

Inimõiguste Instituut on 2014. aastal viinud läbi uuringu[11], mille fookuses oli privaatsusõiguse kaitse igapäevatehnoloogiate kasutamisel. Üle-eestilises avalikus küsitluses osales 959 inimest vanuserühmas 15–74 eluaastat ja tulemused on laiendatavad kogu Eesti vastavas eas elanikkonnale. Uuringu tulemustest selgus näiteks, et suurem osa vastanutest (53%) oli seisukohal, et mure isikuandmete pärast on asjakohane. Küsitluse ajal uuriti ka, milliste osapoolte poolt andmete kogumist peetakse privaatsuse ohuks. Huvitav oli see, et kõikide küsitluses toodud osapoolte (riik, teised riigid, tööandja, eraettevõtted, nutiseadmed, tuttavad ja võõrad inimesed) poolt andmete töötlust peeti potentsiaalseks ohuks privaatsusele. Kõige enam tajutakse ohtlikuna nutiseadmete ja rakenduste kaudu informatsiooni kogumist. Niisiis võib privaatsuseõiguse ja andmekaitse teemasid pidada inimeste jaoks aktuaalseks ning oluliseks nii EL-is kui ka Eestis.

3. Üldmääruse ja direktiivi erinev kohaldamisala

Reformipaketti kuuluvad üldmäärus ja direktiiv reguleerivad mõlemad isikuandmete töötlemist. Seetõttu on asjakohane käesolevas dokumendis selgitada üldmääruse ja direktiivi kohaldamisala temaatikat ehk küsimust, millal tuleb kohaldada üldmäärust ja millal direktiivi.

Üldmääruse sisulise ja territoriaalse kohaldamisala ulatus on toodud üldmääruse artiklites 2 ja 3 ning nende sätete puhul pole jäetud EL liikmesriikidele otsustusõigust riigisiseses õiguses üldmääruse täiendamiseks. Üldmääruse pp 19 kohaselt käsitletakse füüsiliste isikute kaitset isikuandmete töötlemisel pädevate asutuste poolt süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja ennetamise eesmärgil, ning selliste andmete vaba liikumist eraldiseisvas liidu tasandi õigusaktis ehk Euroopa Parlamendi ja nõukogu direktiivis (EL) 2016/680. Seetõttu ei tuleks üldmäärust kohaldada nimetatud eesmärkidel teostatavate isikuandmete töötlemise toimingute suhtes. Üldmääruse pp 20 kohaselt kohaldatakse üldmäärust muu hulgas kohtute ja muude õigusasutuste tegevuse suhtes. Kohtusüsteemi sõltumatuse kaitsmiseks kohtumenetlusega seotud ülesannete täitmisel,

[9] Eurobaromeetri 2015. a andmekaitse raport: http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf.
[10] Samas, lk 9.
[11] Inimõiguste Instituudi uuring 2014 „Privaatsusõigus inimõigusena ja igapäevatehnoloogiad“ kokkuvõte: http://www.humanrightsestonia.ee/wp/wp-content/uploads/2014/11/EST-Uuringu-II-osa-Uuringu-kokkuvote1.pdf.

sealhulgas otsuse tegemisel, ei hõlma järelevalveasutuste pädevus isikuandmete töötlemist juhul, kui kohtud täidavad oma õigust mõistvat funktsiooni. Seega laienevad üldmääruse nõuded küll näiteks kohtukantseleide poolt isikuandmete töötlemisele, aga ei laiene kohtunike tegevusele kohtuotsuse tegemisel.

Õiguskaitsevaldkonna direktiivi kohaldamisala on piiritletud pädevate asutuste (*competent authorities)* tegevusega süütegude (*criminal offence)* ennetamisel, avastamisel, uurimisel ning süüdistuse esitamisel (*prevention, detection, investigation and prosecution)*, sh avalikku julgeolekut ähvardavate ohtude eest kaitsmisel ja nende ennetamisel. Seega on direktiivi kohaldamisala määratlemisel oluline tähelepanu pöörata järgmistele kriteeriumidele:

- isikuline kohaldamisala – direktiiv kohaldub ainult kindlaksmääratud pädevate asutuste tegevusele;
- materiaalne kohaldamisala – direktiiv kohaldub üksnes osale pädevate asutuste tegevustest.

Seega jääb direktiivi kohaldamisalast välja selline pädeva asutuse tegevus, mis ei ole suunatud süütegude ennetamisele, avastamisele, uurimisele või süüdistuse esitamisele ega avaliku julgeoleku tagamisele, näiteks pädeva asutuse haldustegevus (sh dokumendihaldus, personalitöö jt). Pädevate asutuste haldustegevuse osas kohaldub üldmäärus.

Direktiivi kohaldamisala piiritlemiseks on oluline riigisisese õiguse alusel sisustada, milliseid tegevusi hõlmab materiaalne kohaldamisala ning millised on pädevad asutused direktiivi isikulise kohaldamisala mõttes.

Materiaalse kohaldamisala piiritlemisel tuleb määratleda esiteks termini „süütegu“ (*criminal offence)* tähendus ning teiseks hõlmatud tegevuste ulatus Eesti õiguses.

Kuigi direktiivi tekst kasutab mõistet *criminal offence*, on Justiitsministeeriumi hinnangul kohane eestikeelne vaste *süütegu,* mitte aga *kuritegu*. Eesti õiguses kasutatakse õigusrikkumiste (karistatavate tegude) määratlemisel kahetasandilist lähenemist. Üldterminina kasutatakse mõistet *süütegu*, mis on defineeritud kui karistusseadustikus (edaspidi *KarS)* või muus seaduses sätestatud karistatav tegu (KarS § 3 lg 1). Süüteod jagunevad omakorda väärtegudeks ja kuritegudeks (KarS § 3 lg 2). Seejuures on mõlema süüteoliigi puhul tegemist riigi poolt õigusvastaseks tunnistatud tegudega, mille eest on ette nähtud karistus. Väärtegude ja kuritegude erinevus seisneb määratava sanktsiooni ranguses ning ette nähtud karistuse liigis. Seejuures mõlema süüteoliigi puhul on võimalik määrata nii rahaline sanktsioon (trahv või rahaline karistus) kui ka vabadusekaotus (arest või vangistus). Väärtegude puhul viib menetluse läbi kohtuväline menetleja, kuritegude puhul juhib kohtueelset menetlust prokuratuur, kuid mõlemale süüteoliigile kohalduvad karistusseadustikus sätestatud üldnormid ning kohtulikku menetlust toimetatakse kriminaalkohtutes (kuigi Eesti kohtusüsteemis ei eristata esimeses kohtuastmes eraldi kriminaalkohtuid, lahendatakse väärteoasju ning kuriteoasju Ringkonnakohtute kriminaalkolleegiumites ning Riigikohtu kriminaalkolleegiumis). EL õiguses lähtutakse termini *criminal offence* sisustamisel Euroopa Inimõiguste Kohtu poolt loodud nn Engeli kriteeriumidest[12], mille kohaselt tuleb süüteo määratlemisel võtta arvesse alljärgnevaid tingimusi:

[12] Euroopa Kohtu 5.06.2012.a otsus C-489/10 Bonda, ECLI:EU:C:2012:319. Euroopa Kohtu 26.02.2013.a otsus C-617/10 Åklagaren vs Hans Åkerberg Fransson, ECLI:EU:C:2013:105

- õigusnormi kvalifitseerimine karistusõiguse normiks riigisisese õiguse järgi;
- süüteo olemus (sh õigusnormi adressaatide ring, sanktsiooni ennetav, repressiivne ja karistuslik iseloom, sanktsiooni rakendaja olemus);
- kohaldatava karistuse raskus (sh vabaduskaotuslike karistuste puhul eeldatakse üldjuhul normi karistusõiguslikku iseloomu, samuti näiteks karistuse kandmine karistusregistrisse).

Hinnates Eesti väärtegusid Engeli kriteeriumide valguses, võib jõuda järeldusele, et vähemalt osa väärtegusid on liigitatavad EIÕK mõistes kuritegude (vt nt Riigikohtu 25.03.2004.a otsus nt 3-4-1-1-04, p 19) alla ning seega oleksid EL õiguse kohaselt hõlmatud terminiga *criminal offence*.

Eeltoodule tuginedes on Justiitsministeeriumi hinnangul põhjendatud õiguskaitsevaldkonna direktiivi kohaldamisala laiendamine nii väärteo- kui kriminaalmenetlusele kogu menetluse vältel. Seejuures peab Justiitsministeerium oluliseks, et direktiiviga oleks hõlmatud väärteomenetlus sõltumata sellest, millise sanktsiooniga on menetletav tegu karistatav, st kas rikkumise eest on võimalik määrata üksnes trahvi või ka aresti. Kuigi Riigikohus leidis, et Engeli kriteeriumide kohaselt võib EIÕK mõistes „kuriteoks" klassifitseerida üksnes osa väärtegusid, tuleb täiendavalt tähelepanu pöörata KarS § 72 lg-le 1, mille kohaselt on võimalik rahatrahvi asendamine arestiga.

Seega peavad direktiivi sätete kohaldamiseks olema täidetud kumulatiivselt nii materiaalse kui isikulise kohaldamisala kriteeriumid. Seega ei piisa direktiivi normide rakendamiseks sellest, et tegemist on pädeva asutusega, kui asutus tegutseb väljaspool materiaalses kohaldamisalas sätestatud ülesannete piire (näiteks politseiasutus värbab personali jt).

Lisaks süütegude ennetamise, uurimise avastamise ja nende eest süüdistuse esitamise funktsioonidele kohalduvad direktiivi sätted ka karistuse täitmisele pööramisele (*execution of criminal penalties).* Karistuse täitmisele pööramine hõlmab nii rahatrahvi ja aresti kui ka rahalise karistuse ja vangistuse täitmisele pööramist. Väärteomenetluses pöörab määratud karistuse täitmisele kas kohtuväline menetleja või maakohus (VtMS § 202), kriminaalmenetluses on karistuse täitmisele pööramine kohtu või valdkonna eest vastutava ministri käskkirjaga määratud asutus (KrMS § 414 ja § 417). Üldkasuliku töö, elektroonilise valve ja ravi täitmisele pööramise eest vastutab süüdimõistetu elukohajärgne kriminaalhooldusosakond (KrMS § 419, 419^1, 419^2). Kahtlemata tuleb direktiivi sätteid kohaldada vangistuse ja aresti täitmisele pööramise osas vanglate ja arestimajade tegevusele.

Direktiivi kohaldamisala laieneb ka sellistele tegevustele, mida võiks hõlmata määratlusega „avaliku korra / avaliku julgeoleku tagamine". Seejuures on siiski oluline arvestada, et avaliku korra mõiste sisustamisel ei ole võimalik lähtuda korrakaitseseaduse (*edaspidi KorS)* § 4 lg-s 1 antud avaliku korra definitsioonist, kuivõrd EL õiguse kontekstis on avaliku korra mõiste tähendus Eesti riigisisesest õigusest erinev. KorS § 4 lg 1 kohaselt loetakse avalikuks korraks ühiskonna seisundit, milles on tagatud õigusnormide järgimine ning õigushüvede ja isikute subjektiivsete õiguste kaitse. Direktiiviga hõlmatud tegevuste piiritlemisel tuleb arvestada põhjenduspunktides 11 ning 12 toodud selgitusi. Põhjenduspunkti 11 kohaselt tuleb esiteks arvestada, et pädevad asutused direktiivi tähenduses võivad olla mitte üksnes avaliku sektori asutused nagu õigusasutused, politsei ja teised õiguskaitseasutused, vaid ka kõik muud asutused või üksused, kes teostavad liikmesriigi õiguse kohaselt avalikku võimu direktiivi kohaldamisel. Põhjenduspunkt 12 selgitab, et politsei või muude õiguskaitseasutuste tegevus, sealhulgas politsei toimingud juhul, kui eelnevalt pole teada, kas tegemist on süüteoga,

keskenduvad peamiselt süütegude tõkestamisele, uurimisele, avastamisele või nende eest vastutusele võtmisele. Selline tegevus võib hõlmata ka avaliku võimu teostamist sunnimeetmete võtmisega, näiteks politsei tegevus demonstratsioonidel, suurtel spordiüritustel ja massirahutustel. See tegevus hõlmab ka avaliku korra säilitamist, mis on politseile või muule õiguskaitseasutusele antud ülesanne, et vajaduse korral kaitsta avalikku julgeolekut ja seadusega kaitstavaid ühiskonna põhihuve selliste ohtude eest ja hoida ära selliste ohtude teke avalikule julgeolekule ja seadusega kaitstavatele ühiskonna põhihuvidele, mis võivad viia süüteo toimepanemiseni. Liikmesriigid võivad anda pädevatele asutustele muid ülesandeid, mida ei täideta tingimata süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil, ning nii kuulub neil muudel eesmärkidel toimuv isikuandmete töötlemine niivõrd, kuivõrd see on liidu õiguse kohaldamisalas, määruse (EL) 2016/679 kohaldamisalasse.

Isikulise kohaldamisala määratlemisel on oluline arvestada, et direktiivi sätteid kohaldatakse ainult *pädevate asutuste* tegevusele. Pädevaks asutuseks on direktiivi art 3 p 7 kohaselt kas:

- riigiasutus (avaliku sektori asutus), kes on pädev süütegusid tõkestama, uurima, avastama või nende eest vastutusele võtma või kriminaalkaristusi täitmisele pöörama, sealhulgas kaitsma avalikku julgeolekut ähvardavate ohtude eest ja neid ohte ennetama, või
- muu asutus või üksus, kes teostab liikmesriigi õiguse kohaselt avalikku võimu süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil.

Ka riikliku järelevalve pädevusega asutuste osas, nagu seda on näiteks Terviseamet ja Tööinspektsioon, on vaja pöörata tähelepanu eelkõige määruse ja direktiivi erinevale kohaldamisalale. Kahe akti kohaldamine eeldab nende kohaldamisala eristamist (sh ka menetluslike üldaktide (nt KorS, HMS, VTMS) rakendamisel). Kuna üldmäärus kehtib nii era- kui avalikule sektorile ning direktiiv reguleerib muuhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmisel ja nende eesmärkide ennetamisel isikuandmete töötlemist, on erinevate aktide kohaldamisala piiritlemine kaaluka tähtsusega. Nii näiteks tuleb selgitada konkreetsed piirid, millal lähtub Terviseameti järelevalve osakond üldmäärusest (isikuandmete töötlemine avalduste/kaebuste lahendamisel) või millal direktiivist (ennetava järelevalve teostamisel nakkushaiguste epidemioloogia valdkonna tegevuses).[13] Eelpool kirjeldatud olukorras tuleks lähtuda loogikast, et riikliku järelevalve teostamisel kohaldatakse andmekaitse üldmäärust (KorS, HMS) ning direktiivi kohaldamine tuleb kõne alla siis, kui alustatakse väärteomenetlust (VTMS).

4. Võimalikud õiguslikud lahendused

Regulatiivse lahenduse kasuks võib otsustada siis, kui muul viisil probleemi lahendada saa ning kontseptsioonis ei pea kaaluma ilmselgelt ebamõistlikke mitteregulatiivseid alternatiive. Käesoleval juhul tuleneb õigusmuudatuse vajadus Euroopa Liidu õigusest – üldmääruse rakendamise ning direktiivi ülevõtmise vajadusest. Vajalikke eesmärke pole käesoleval juhul võimalik saavutada muul viisil kui õigusmuudatusega, mistõttu võimalike mitteregulatiivsete lahenduste juures pikemalt ei peatuta. Mitteregulatiivsed lahendused on isikuandmete kaitse

[13] Sotsiaalministeeriumi vastuskiri andmekaitse reformipaket ringkirjale, kiri nr 1.2-5/4007-5, lk 6.

reformipaketi riigisisesel rakendamisel ja ülevõtmisel sobimatud lahendused, kuna sellisel juhul ei täidaks Eesti endale võetud kohustusi EL ees. ELTL art 288 kohaselt kohaldatakse EL määrust üldiselt ning see on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides. Direktiiv on saavutatava tulemuse seisukohalt siduv iga liikmesriigi suhtes, kellele see on adresseeritud, kuid jätab vormi ja meetodite valiku selle riigi ametiasutustele.

Üldmääruse rakendamiseks on Justiitsministeeriumi poolt kavandatud koostada uus IKS terviktekst, mis hõlmaks endas ka Euroopa Parlamendi ja nõukogu määruse (EL) nr 2016/679 „Füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)“ rakendamist.

Õiguskaitsevaldkonna direktiivi normide ülevõtmise korraldamiseks on kaalutud kolme kahte võimalikku lahendust:

- direktiivi sätete paigutamine olemasolevatesse valdkonda reguleerivatesse õigusaktidesse (nt kriminaalmenetluse seadustik, väärteomenetluse seadustik, korrakaitseseadus, politsei ja piirivalve seadus, vangistusseadus jt);
- uue eraldi seaduse väljatöötamine eesmärgiga koondada andmekaitsealaseid õigusnorme üheks õigusaktiks;
- ühtne seadus nii määruse rakendamiseks kui ka direktiivi sätete ülevõtmiseks, mis muuhulgas käsitleks ka nende kahe õigusakti reguleerimisalast välja jäävad küsimused.

5. Andmekaitse üldmääruse rakendamiseks vajalikud muudatused ja nende kirjeldus

5.1. Seaduste muutmine, milles esinevad viited IKSile ning mille sisu ei ole kooskõlas üldmääruse regulatsiooniga

Seoses praegu kehtiva IKSi kehtetuks tunnistamisega ja uue IKS tervikteksti kehtestamisega tuleb asendada kehtivates õigusaktides viited direktiivil 95/46/EÜ põhinevale IKSile viidetega uuele kavandatavale terviktekstile või üldmäärusele endale. Viiteid teistes seadustes kehtivale IKSile, mis vajavad ülevaatamist, esineb kehtivas seadusandluses väga palju. Riigi Teataja veebipõhiste otsingutulemuste kohaselt on IKSile viidatud 80-s kehtivas terviktekstis, mis tähendab, et 80-s seaduses tuleks need viited üle vaadata ning vajadusel asendada viide IKSile viitega üldmäärusele või uuele terviktekstile.

Kuivõrd mitmetes seadustes esineb ka tarbetuid sätteid stiilis „käesolevas seaduses ette nähtud isikuandmete töötlemisele kohaldatakse isikuandmete kaitse seaduse sätteid“[14], on Justiitsministeerium kavandanud üldmääruse rakendusseaduse rakendussätetes ka selliste tarbetute sätete kehtetukstunnistamise, kuivõrd taolised deklaratiivsed sätted ei loo lisandväärtust ning ühtlasi muutuvad sellised sätted tarbetuks seoses asjaoluga, et isikuandmete kaitse valdkonnale kohaldatakse tulevikus otsekohalduvat andmekaitse üldmäärust koos riigisisese rakendusseadusega praegu kehtiva IKSi asemel.

Samuti vajavad ülevaatamist ning vajadusel üldmäärusega ja direktiivi sätetega kooskõlla viimist Eesti kehtivas seadusandluses eksisteerivad isikuandmete töötlemise alused ning teised isikuandmete töötlemist reguleerivad sätted, mis ei ole kooskõlas tulevikus jõustuva andmekaitse üldmäärusega ega direktiiviga. Üldmääruse art 6 lg 2 näeb ette, et liikmesriigid võivad säilitada või kehtestada konkreetsemad sätted, et kohandada üldmääruse sätete kohaldamist seoses isikuandmete töötlemisega art 6 lg 1 p-de c ja e täitmiseks, määrates üksikasjalikumalt kindlaks töötlemise konkreetsed nõuded ja teised meetmed, et tagada seaduslik ja õiglane töötlemine. Üldmääruse art 6 lg 1 p c kohaselt loetakse seaduslikuks isikuandmete töötlemiseks olukorrad, kus isikuandmete töötlemine on vajalik vastutava töötleja juriidilise kohustuse täitmiseks ning art 6 lg 1 p e kohaselt sellised olukorrad, kus isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks. Seega tuleb ka üldmääruse jõustudes tagada, et riigisisesed õigusaktid on kooskõlas eelpool nimetatud üldmääruse sätetega. See tähendab, et on vajalik tagada kooskõla üldmäärusega nii andmekogude põhimäärustes (ministeeriumide endi vastutusala) kui ka seadustes. Eelnõu rakendussätetega on kavandatud muudatused nende õigusaktide sätetes, mis praegu andmekaitse ja –töötluspõhimõtetega kooskõlas pole. Selliste seadussätete muutmisvajaduse väljaselgitamiseks soovib Justiitsministeerium teha koostööd teiste ministeeriumidega. Selleks kontakteerutakse ministeeriumide kontaktisikutega, kelle Justiitsministeerium palus nimetada 2016. a sügisel välja saadetud ringkirjas. Näitena vajab tulevikus muutmist mh vangistusseaduse (edaspidi *VangS*) § 5^1 lg 1 p 1, mis sätestab, et

[14] Sarnaseid kehtetuks tunnistatavaid sätteid leiab nt töötuskindlustuse seaduse (TKindlS) § 35 lg 4 ls-st 2: „Andmekogu pidamisele kohaldatakse isikuandmete kaitse seadust ja avaliku teabe seadust.“; finantskriisi ennetamise ja lahendamise seaduse (FELS) § 90 lg-st 2: „Kui teabevahetus puudutab isikuandmeid, kohaldatakse isikuandmete töötlemisel ja edastamisel kolmanda riigi ametiasutusele isikuandmete kaitse seadust.“; maaparandusseaduse (MaaParS) § 43 lg-st 2: „Isikuandmete avaldamise suhtes kohaldatakse isikuandmete kaitse seaduse sätteid.“

vangiregistri üheks eesmärgiks on isikuandmete töötlemine, mis ringdefinitsioonina ei saa olla isikuandmete töötlemise eesmärgiks. Kehtiv seadusandlus vaadatakse reformi valguses üle.

Mõju riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele

Sihtrühm: ministeeriumid, kaudselt ka asutused ja organisatsioonid, kes töötlevad isikuandmeid seadusest või teistest õigusaktidest tulenevatel alustel.

Kehtivate õigusaktide kooskõlla viimine üldmääruse ja selle rakendusseadusega ei mõjuta sihtrühmasid *per se*. Ministeeriumide töökoormus võib ajutiselt tõusta seoses valdkondlike määruste (sh andmekogude põhimääruste) viimisega üldmäärusega kooskõlla, kuid seaduste tasandil vastutab IKS-i viidete parandamise ja sätete kooskõlla viimise eest Justiitsministeerium. Kontseptsiooni koostamise ajal kehtis 78 seadust, mis sisaldavad viidet isikuandmete kaitse seadusele. Muutmist vajavate valdkondlike määruste (sh andmekogude põhimääruste) arv ei ole esialgu veel teada.

Sihtrühma täpset suurust ei ole võimalik hinnata. Võttes arvesse, et andmekogu kasutusele võtmisel tuleb see registreerida Riigi infosüsteemi haldussüsteemis (RIHA), siis saab lähendina välja tuua, et RIHA andmetel on Riigi infosüsteemis registreeritud ja X-teega liitunud 1161 asutust ja organisatsiooni[15]. Seadustest tulenevatel alustel isikuandmeid töötlevate asutuste ring on siiski laiem.

Mõjude seisukohalt tuleb eristada mõju teistele isikuandmeid töötlevatele asutustele, mis tuleneb eeskätt IKS-i kehtetuks tunnistamisest ja üldmääruse rakendamisest. Tegemist on tervet andmekaitsevaldkonda reformiva EL-i määrusega, mis sisaldab küll hulgaliselt muudatusi, kuid on liikmesriikidele otsekohalduv ja tervikuna siduv. Käesoleva kontseptsiooni raames kajastatakse ainult nende muudatuste mõju, mille osas on liikmesriikidel kaalutlusruumi.

5.2. Andmekaitseametniku regulatsioon

Andmekaitseametniku (ingl. k. *data protection officer, DPO*) määramine, ametiseisund ja ülesanded on reguleeritud üldmääruse artiklites 37–39. Tegemist on uue kohustuse ja mõistega eesti andmekaitseõiguses ning kuigi mõistes sisaldub nimetus „ametnik“, ei ole otseselt tegemist ametnikuga avaliku teenistuse seaduse (edaspidi *ATS*) § 7 lg-st 1 tähenduses. Seda põhjusel, et andmekaitseametniku määramise kohustus laieneb nii avalikule kui ka erasektorile. Üldmääruse pp 97 selgitab kokkuvõtvalt, et andmekaitseametnik on andmekaitsealaseid õigusakte ja tavasid eksperdi tasandil tundev isik, kes abistab ja kontrollib andmetöötlejat määruse täitmisel. Sisuliselt on tegu andmekaitsespetsialistiga.

Üldmääruse art 37 lg 1 sätestab, millised isikuandmete töötlejad peavad määrama andmekaitseametniku. Üldmääruse art 37 lg 1 p a näeb ette, et andmekaitsespetsialisti peavad määrama kõik avaliku sektori asutused (v.a. kohtud oma õigust mõistva funktsiooni täitmisel) ehk Eesti õiguse kohaselt avaliku ülesande täitjad (riigi- ja omavalitsusasutused ja avalik-

[15] Enne andmekogu kasutusele võtmist tuleb see RIHA-s registreerida (AvTS § 43^7 lg 1) ning liituda infosüsteemide andmevahetuskihiga X-tee (AvTS § 43^9). Samas ei kasuta X-teed mitte üksnes andmekogud (nende asutamine ja kasutamine on sätestatud seaduses või mõnes muus õigusaktis), vaid ka näiteks erasektori ettevõtted, mistap on sihtrühma suuruse määratlus ligikaudne.

õiguslikud või eraõiguslikud isikud, kes täidavad avalikke ülesandeid), nt ministeeriumid, kohalikud omavalitsused, ülikoolid.[16]
Erasektorile üldine andmekaitseametniku määramise kohustus täies ulatuses ei laiene. Küll aga tekib see kohustus siis, kui andmetöötleja töötleb isikuandmeid, mille laad, ulatus ja/või eesmärk tingivad ulatusliku andmesubjektide korrapärase ja süstemaatilise jälgimise (nt telekommunikatsiooniettevõtted) – üldmääruse art 37 lg 1 p b. Lisaks, kui üldmääruse art 37 lg 1 p c kohaselt moodustab andmetöötleja põhitegevuse andmete eriliikide (üldmääruse art 9) ulatuslik töötlemine, nt haiglad, perearstikeskused ja ka terviseuuringute teostajad, kui kasutatakse isikustatuid andmeid.
Määruse artikkel 37 lg 6 järgi võib andmekaitseametniku rolli täita nii andmetöötleja koosseisuline töötaja (nt eraldi ametikoht), andmetöötleja allüksus (nt osakond) kui ka andmetöötleja väline juriidiline isik (nt teenuslepingu alusel). Seega ei eelda reform tingimata seda, et asutuse isikkooseis peaks tingimata suurenema. Samuti on üldmääruse art 38 lg 6 kohaselt lubatud andmekaitseametnikul täita muid ülesandeid ja kohustusi, kuid sellisel juhul peab andmetöötleja tagama, et sellised ülesanded ja kohustused ei põhjustaks huvide konflikti.
Üldmääruse art 39 kohaselt on andmekaitseametnikul vähemalt järgmised ülesanded:

a) teavitada ja nõustada vastutavat töötlejat või volitatud töötlejat ning isikuandmeid töötlevaid töötajaid seoses nende kohustustega, mis tulenevad käesolevast määrusest ja muudest liidu või liikmesriikide andmekaitsenormidest;
b) jälgida andmekaitse määruse, muude liidu või liikmesriikide andmekaitsenormide ja vastutava töötleja või volitatud töötleja isikuandmete kaitse põhimõtete järgimist, sealhulgas vastutusvaldkondade jaotamist, isikuandmete töötlemises osaleva personali teadlikkuse suurendamist ja koolitamist, ning seonduvat auditeerimist;
c) anda taotluse korral nõu seoses andmekaitsealase mõjuhinnanguga ning jälgida selle toimimist;
d) teha koostööd järelevalveasutusega;
e) tegutseda isikuandmete töötlemise küsimustes järelevalveasutuse jaoks kontaktisikuna, sealhulgas artiklis 36 osutatud eelneva konsulteerimise osas, ning konsulteerida vajaduse korral ka muudes küsimustes.

Andmekaitse Inspektsioon on koostamas soovituslikke kompetentse[17], mis on eelduseks andmekaitseametniku rolli tulemuslikul täitmisel. Kuna andmekaitse põhimõtete rakendamise osaks on oskus rakendada pädevaid turvameetmeid, peab andmekaitseametnikul olema teadmus ka infoturbe põhimõtetest ning sellega seotud tehnoloogiatest.
Kompetentside alusel on koolitusasutustel tulevikus võimalik luua kas põhiõppe osana või täienduskoolitusena andmekaitsespetsialisti õppekava(d) ja kursused. See tähendab, et Andmekaitse Inspektsiooni poolt koostatud kompetentsimudeli abil on ülikoolidel ja teistel koolitajatel võimalik hakata pakkuma andmekaitsekursuste ja/või –koolituste läbimist. Kursuse läbinul saab tulevikus olema vabatahtlik võimalus end Andmekaitse Inspektsioonis atesteerida (vabatahtlikku teadmistekontrolli läbides).
Kontseptsiooni koostamise käigus on kohtutud SA-ga Kutsekoda, mis korraldab kutsestandardite koostamist ja koordineerib kutseeksamite korraldamist. Tulevikku on planeeritud andmekaitseametniku kutsestandardi väljatöötamine (kutse kutseseaduse tähenduses), kuid kuivõrd tegemist on ajamahuka protsessiga (vajalik on koostada kutsestandard haridus- ja teadusministri 28.11.2008 määrusest nr 69 „Kutsestandardite koostamise, muutmise ja vormistamise kord“, mis on kehtestatud kutseseaduse § 5 lg 3 alusel,

[16] Vt selle kohta lähemalt AKI veebileheküljelt: http://www.aki.ee/et/andmekaitse-reform/kes-peavad-maarama-andmekaitsespetsialisti ja art29WP arvamust: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.
[17] Vt lähemalt http://www.aki.ee/et/andmekaitse-reform/andmekaitsespetsialisti-ulesanded-teadmised-ja-oskused.

lähtuvalt) ning tõenäoliselt ei saaks see valmis 2018.a 25. maiks, kui tuleb hakata rakendama üldmäärust, on koostöös Kutsekoja ja Andmekaitse Inspektsiooniga jõutud arusaamisele, et kõige efektiivsem lahendus on see, kui kuni kutsestandardi väljatöötamiseni korraldab andmekaitseametnike atesteerimist Andmekaitse Inspektsioon. Tegemist on vabatahtliku atesteerimisega, mille läbimine näitaks konkreetse isiku puhul vajalike teadmiste olemasolu. Samuti oleks see garantiiks tööandjale, et tema alluvuses töötab vajalike andmekaitsealaste teadmiste ja kompetentsidega isik. Andmekaitse Inspektsioon on väljendanud valmisolekut ajutiselt kuni kutsestandardi väljatöötamiseni ise atesteerimist läbi viia. Seega oleks tegemist ajutise lahendusega kuni kutsestandardi väljatöötamiseni.
Seoses üldmääruse kohaldamisega kaob tulevikus ära kohustus registreerida delikaatsete isikuandmete töötlemine Andmekaitse Inspektsioonis, mille regulatsiooni näeb ette praegu kehtiva IKSi peatükk 5. Praegu kehtiva regulatsiooni kohaselt tuleb delikaatsete isikuandmete töötlemisel määrata isikuandmete töötleja poolt isikuandmete kaitse eest vastutav isik või registreerida delikaatsete isikuandmete töötlemine Andmekaitse Inspektsioonis (IKS § 27). Kuivõrd uue üldmääruse valguses asendab vastutava isiku määramise ja registreerimiskohustuse andmekaitseametniku määramise kohustus, kaotab üldmääruse kohaldamisel senine regulatsioon oma tähtsuse ning kehtetuks tunnistamist vajab nii IKSi praegu kehtiv regulatsioon kui ka Vabariigi valitsuse määrus „Isikuandmete töötlejate ja isikuandmete kaitse eest vastutavate isikute registri pidamise põhimäärus“.

Mõju riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele, kuludele ja tuludele

Sihtrühm 1: avaliku sektori asutused, v.a kohtud oma õigust mõistva funktsiooni täitmisel.

Sihtrühma suuruse hindamisel võib aluseks võtta majandusüksuste institutsionaalsete sektorite klassifikaatori, mille kohaselt oli 2016. aasta detsembri seisuga Eestis kokku 3116 valitsemissektorisse kuuluvat asutust ja avaliku sektori osalusega ettevõtet (v.a kohtud)[18]. Jättes kõrvale äriühingud, milles on osanikuks või aktsionäriks keskvalitsus, või kohaliku omavalitsuse osalusega äriühingud, mille puhul ei pruugi andmekaitseametniku määramine olla tingimata vajalik, jääb 2829 valitsemissektori asutust, kellele on andmekaitseametniku kaasamine edaspidi kohustuslik.

Tabel 1. Valitsemissektori asutused põhitegevusalade lõikes 2016. aastal (N=3116)

EMTAK	Tegevusala	Asutuste arv	%
P85	Haridus	1223	39%
R91	Raamatukogude, arhiivide, muuseumide ja muude kultuuriasutuste tegevus	511	16%
O84	Avalik haldus ja riigikaitse, kohustuslik sotsiaalkindlustus	447	14%
R93	Sporditegevus ning lõbustus- ja vaba aja tegevused	325	10%
Q87	Hoolekandeasutuste tegevus	113	4%
Q88	Sotsiaalhoolekanne majutuseta	67	2%
D35	Elektrienergia, gaasi, auru ja konditsioneeritud õhuga varustamine	63	2%
E36	Veekogumine, -töötlus ja -varustus	51	2%
Q86	Tervishoid	49	2%
L68	Kinnisvaraalane tegevus	47	2%
M71	Arhitekti- ja inseneritegevused	25	1%

[18] Arvestatud on valitsemissektori asutusi (klassifikaatorid S1311-S1314) ja avaliku sektori mittefinantsettevõtteid (S11001), arvestatud ei ole kohtuid ja registrist kustutatud üksuseid. Andmed statistikaameti kodulehelt: http://www.stat.ee/majandusuksuste-klassifitseerimise-abiinfo (seisuga 25.01.2017).

M72	Teadus- ja arendustegevus	22	1%
R90	Loome-, kunsti- ja meelelahutustegevus	22	1%
M70	Peakontorite tegevus, juhtimisalane nõustamine	15	0%
H52	Laondus ja veondust abistavad tegevusalad	13	0%
E38	Jäätmekogumine, -töötlus ja -kõrvaldus, materjalide taaskasutusele võtmine	12	0%
	Muud tegevusalad	111	4%

Üldmääruse artikkel 37 lg 3 sätestab, et kui isikuandmete töötleja on avaliku sektori asutus, võib mitme sellise asutuse jaoks määrata ühe andmekaitseametniku olenevalt asutuste organisatsioonilisest struktuurist ja suurusest. Seega on tõenäoline, et sarnaste funktsioonide või struktuurilise ülesehitusega asutused määravad ühise andmekaitseametniku või ostavad ühiselt teenust sisse (nt kohaliku omavalitsuse heaks töötav andmekaitseametnik saab täita andmekaitseametniku ülesandeid ka kohaliku raamatukogu jaoks). Samuti võib andmekaitseametniku ülesandeid hakata täitma asutuse koosseisuline töötaja või allüksus. Kuna andmetöötlejatele on siinkohal jäetud suhteliselt suur otsustusruum, siis ei ole võimalik ette prognoosida ametikohtade (sh lisanduvate ametikohtade) tegelikku arvu.

Samal põhjusel ei ole võimalik välja tuua ka koondandmeid andmekaitseametniku määramisega kaasnevate kulude kohta asutustele ega riigile tervikuna. Lähtudes andmekaitseametniku ülesannetest ja kompetentsidest, võib huvirühmade hinnangul olla sellega võrreldavaks tegevusalaks auditeerimine: ühe enamkasutatava töövahendusportaali andmetel oli 2015. aastal auditeerimise valdkonna keskmine netokuupalk 1345 eurot[19] (palgakulu tööandjale 2271 eurot). Kulud kaasnevad ka andmekaitseametnike koolitamise või teenuse ostmisega, kuid kuna tegemist on täiesti uue tegevusvaldkonnaga nii nõudluse kui pakkumise seisukohast, siis ei ole võimalik neid kulusid prognoosida.

Avalikule sektorile tervikuna on andmekaitseametniku regulatsiooni näol tegemist ulatusliku ja otsest rahalist mõju avaldava muudatusega, samas ühe asutuse tasandil võib mõju olla pigem väike sõltuvalt valitud lahendusest. Muudatuse mõju avaldub sageli ning suurele sihtrühmale.

Sihtrühm 2: Andmekaitse Inspektsioon

AKI täidab Eestis andmekaitse järelevalveasutuse funktsiooni üldmääruse mõistes. Järelevalveasutuse ülesanded on sätestatud üldmääruse artiklis 57 ning hõlmavad muu hulgas üldmääruse kohaldamise tagamist, üldsuse ja andmetöötlejate teadlikkuse edendamist, koostööd teiste liikmesriikidega ja Euroopa Liiduga, uurimiste läbiviimist jm. Lisaks korraldab AKI ajutiselt andmekaitseametnike atesteerimist kuni kutsestandardi väljatöötamiseni. Andmekaitseametnik on andmetöötleja esmaseks kontaktisikuks AKI-ga.

AKI prognoosib enda kuludeks seoses üldmääruse rakendamisega 18 kuu jooksul kokku üle 112 000 euro, mis sisaldab kahe täistöökoormusega ametikoha personalikulusid, majandamiskulusid ja välislähetusi. AKI töökoormus on eelduslikult suurem just üldmääruse rakendamisele eelnevalt ja selle algusperioodil, vähenedes aja jooksul.

[19] Palgaandmed ametikohtade järgi: http://www.palgad.ee/salaryinfo. Tegemist on valimi põhjal saadud tulemusega, mis ei pruugi olla üldistatav üldkogumile.

Tabel 2. Isikuandmete kaitse üldmääruse rakendamise prognoositavad kulud Andmekaitse Inspektsioonile aastatel 2018–2019 (eurod)

	2018 (12 kuud)	2019 (6 kuud)	Kokku (18 kuud)
Personalikulud	61 013	30 506	91 519
Majandamiskulud	10 840	10 320	21 160
Kokku	**71 853**	**40 826**	**112 679**

Üldmäärusest tulenevate muudatustega kaasneb sihtrühmale ulatuslik ja tervikuna oluline[20] mõju. Seejuures on andmekaitseametniku regulatsioon üks suurema mõjuga muudatusi – AKI roll on olla informatsiooni jagajaks nii andmetöötlejatele, üldsusele, sh andmesubjektidele, kui ka muudele huvirühmadele (ülikoolid, koolitajad, erialaliidud, teenuseosutajad).

Mõju majandusele: ettevõtluskeskkond ja ettevõtete tegevus

Sihtrühm 1: erasektori andmetöötlejad

Vastavalt üldmääruse artiklile 37 peavad ka erasektori füüsilised ja juriidilised isikud (ka kolmanda sektori organisatsioonid) edaspidi määrama andmekaitseametniku, kui:

a) nende **põhitegevuse** moodustavad isikuandmete töötlemise toimingud, mille laad ulatus ja/või eesmärk tingivad **ulatusliku andmesubjektide korrapärase ja süstemaatilise jälgimise**, või
b) nende põhitegevuse moodustab andmete **eriliikide**[21] ja süüteoasjades **süüdimõistavate kohtuotsuste ja süütegudega seotud isikuandmete ulatuslik** töötlemine.

Andmekaitse Inspektsioon on enda kodulehel neid kriteeriume selgitanud ning toonud näiteid valdkondadest, milles tegutsevatele ettevõtetele tekib andmekaitseametniku määramise kohustus[22]. Paraku ei ole võimalik hinnata selliste ettevõtete koondarvu, sest kriteeriumidele vastavust tuleb vaadata juhtumipõhiselt.

Registriandmetele tuginedes saab üldistatult välja tuua äriühingud (tegevusalade kaupa), kellele võib rakenduda andmekaitseametniku määramise kohustus, st nende põhitegevus võib hõlmata andmesubjektide ulatuslikku, korrapärast ja süstemaatilist jälgimist või andmete eriliikide ja süütegudega seotud isikuandmete töötlemist. Tegemist on informeeriva, kuid kindlasti mitte täpse ega ammendava loeteluga (tabel 1).

Tabel 1. Äriühingute arv, kelle põhitegevus võib hõlmata isikuandmete ulatuslikku, korrapärast ja süstemaatilist jälgimist[23]

Põhitegevusala	N	Hõlmatud EMTAK koodid
Kinnisvaraalane tegevus (sh kinnisvarabürood,	5043	6831, 68311, 6832, 68321, 68322, 68329

[20] Mõju olulisust hinnatakse lähtudes mõju ulatusest, sagedusest, mõjutatud sihtrühma suurusest ja ebasooritavatest riskidest.

[21] Isikuandmete eriliigid on isikuandmed, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilised andmed, füüsilise isiku kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed, terviseandmed ja andmed füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta.

[22] Andmekaitse Inspektsioon: http://www.aki.ee/et/andmekaitse-reform/kes-peavad-maarama-andmekaitsespetsialisti (26.01.2017)

[23] Äriregistri andmed majanduslikult aktiivsete äriühingute kohta (st andmed ei sisalda MTÜ-sid, SA-id ja riigi- ja kohaliku omavalitsuse asutuste riiklikusse registrisse kuuluvaid asutusi) seisuga 02.02.2017.

kinnisvara haldus)		
Finants- ja kindlustustegevus (sh investeerimine, laenuandmine, pangad, finantsnõustamine, kindlustus, fondide valitsemine jm)	3822	64191, 64301, 6492, 64921, 64929, 65111, 65121, 65301, 66111, 6612, 66121, 66129, 6619, 66191, 66199, 66211, 66221, 66291, 66301
Jaemüük posti või interneti teel	3182	47911
Haldus- ja abitegevused (sh tööhõiveagentuurid, reisibürood, turvatöö, inkassoteenused jm)	2655	78101, 78201, 78301, 79111, 79121, 80101, 80201, 80301, 82911
Tervishoid ja sotsiaalhoolekanne (sh üldarstiabi, hambaravi, õendusabi jm)	2412	86101, 8621, 86211, 86231, 8690, 86901, 86902, 86903, 86904, 86905, 86906, 86909, 87101, 8720, 87201, 87301, 879, 8790, 87901, 87909
Info ja side (sh andmetöötlus, veebihosting, veebiportaalid, telekommunikatsioon, ajakirjade kirjastamine jm)	2407	58121, 58131, 58141, 6110, 61101, 61109, 6120, 61201, 61209, 61301, 61901, 63111, 63121
Kutse-, teadus- ja tehnikaalane tegevus (sh teadus ja arendus biotehnoloogia vallas, reklaami vahendamine, turu-uuringud ja küsitlused)	1126	72111, 7312, 73121, 73201
Majutus (sh hotellid, motellid, külalistemajad)	584	5510, 55101, 55102, 55103

Allikas: äriregister

Vastavalt üldmääruse artikli 37 lõikele 6 võib andmekaitseametnik olla andmetöötleja koosseisuline töötaja või täita ülesandeid teenuslepingu alusel. Üks andmekaitseametnik võib töötada mitme andmetöötleja (või nt kontserni) heaks, samas huvirühmadega konsulteerimisel avaldati arvamust, et andmekaitseametnik peab ettevõtet ja selle tööprotsesse väga hästi tundma, mistõttu võiks tegemist olla pigem ettevõttesisese töötajaga. AKI hinnangul vastab andmekaitseametniku ametikohale tänases Eesti seaduses ettenähtud isikuandmete töötlemise eest vastutav isik. Vastutavaid isikuid on seni määratud üle 1100[24].

Muudatus suurendab sihtrühma halduskoormust. Mõju olulisust on keeruline hinnata, kuivõrd see sõltub ettevõtte tegevusvaldkonnast, töödeldavate andmete iseloomust ja valitud lahendusest andmekaitseametniku määramiseks, kuid on tõenäoline, et sihtrühma ettevõtetele toob regulatsioon kaasa täiendava rahalise kulu.

Muud sihtrühmad: tulevased andmekaitseametnikud, teenust osutama hakkavad ettevõtted, ülikoolid ja teised koolitajad, andmesubjektid

Andmekaitseametniku regulatsiooniga tekib tööturul vajadus uue, praegu puuduva ametikoha järele. See eeldab vastava kvalifikatsiooniga töötajate olemasolu. On tõenäoline, et turul tekib nõudlus nii koolitusteenuse kui ka andmekaitsega seotud teenuste pakkumise järele. Paraku ei ole võimalik kontseptsiooni etapis täpsemalt hinnata, kui paljusid ettevõtteid regulatsioon otseselt või kaudselt puudutama hakkab või milline on mõju turuosalistele ja tööjõuturule.

Muudatusel on tervikuna positiivne mõju ka andmesubjektidele, kelle isikuandmeid töödeldakse - paremini on tagatud nende õigus isikuandmete kaitsele ning isikuandmetega seotud rikkumistele reageerimine.

[24] Andmekaitse Inspektsiooni peadirektori ülevaade, lk 10: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ylevaade_reformist_14102016.pdf .

5.3. Isikuandmete töötlemine pärast andmesubjekti surma

Üldmääruse pp 27 kohaselt ei kohaldata andmekaitse üldmäärust surnuid puudutavate isikuandmete suhtes ning liikmesriikidele on üldmääruse poolt jäetud võimalus näha ette riigisiseselt kehtivad surnuid puudutavate isikuandmete töötlemise eeskirjad. Põhjenduspunkti 27 täiendavad veel üldmääruse pp 158 (arhiveerimine) ja pp 160 (ajaloouuringud). Seega surnud isikute andmete regulatsiooni osas üldmäärus liikmesriikide õigust ei harmoneeri, vaid jätab liikmesriikidele võimaluse ise vastav regulatsioon kehtestada.
IKS § 12 lg-st 6 kohaselt kehtib praegu eesti õiguses andmesubjekti nõusolek tema eluajal ning 30 aastat pärast andmesubjekti surma, kui andmesubjekt ei ole otsustanud teisiti. IKS § 13 lg 1 alusel on pärast andmesubjekti surma andmesubjekti isikuandmete töötlemine lubatud andmesubjekti pärija, abikaasa, alaneja või üleneja sugulase, õe või venna kirjalikul nõusolekul, välja arvatud juhul, kui isikuandmete töötlemiseks nõusolekut ei ole vaja või juhul, kui andmesubjekti surmast on möödunud 30 aastat.
Siinkohal on Andmekaitse Inspektsioon väljendanud seisukohta, et hädavajalik oleks uues riigisiseses regulatsioonis kehtestada kaitserežiim pärilike haiguste andmete osas (kusjuures 30 aastat surmast on liiga lühike aeg).[25] Ka Sotsiaalministeeriumi hinnangul[26] ei peaks terviseandmed olema kasutatavad pärast isiku surma laialdaselt ja piiranguteta ning arvestama peaks isiku võimaliku tahteavaldusega, mis on antud enne surma. Kui inimene on oma elu jooksul avaldanud soovi, et tema terviseandmed on peale surma suletud (nt tervise infosüsteemis või avaldus vastutavale töötlejale), ei ole põhjendatud sellekohase soovi ignoreerimine. Sellekohase tahteavalduse peaksid saama esitada ka pärijad. Vaatamata suletud andmetele saab (ja tulebki) andmeid jätkuvalt kasutada avaliku huvi eesmärgil statistika tegemisel ja teadusuuringutes, mis aga kitsendab andmete laialdast kasutamist kui igaühe õigust.
Oluline on siinkohal märkida, et absoluutset keeldu isikuandmete töötlemisele pärast andmesubjekti surma panna ei saa (isikuandmete eriliike võib olla vaja töödelda avalikes huvides rahvatervisega seotud valdkondades ilma andmesubjekti nõusolekuta, nt surma põhjused jms).
Üldmääruse pp 54 täpsustab, et isikuandmete eriliike võib olla vaja töödelda avalikes huvides rahvatervisega seotud valdkondades ilma andmesubjekti nõusolekuta. Sellisel töötlemisel tuleks kohaldada sobivaid ja konkreetseid meetmeid, et kaitsta füüsiliste isikute õigusi ja vabadusi. Selles kontekstis tuleks mõistet „rahvatervis“ tõlgendada vastavalt Euroopa Parlamendi ja nõukogu määrusele (EÜ) nr 1338/2008 (11), mille kohaselt rahvatervis on kõik tervisega seotud asjaolud, nimelt tervislik seisund, sealhulgas haigestumus ja puuded, tervislikku seisundit mõjutavad tegurid, tervishoiualased vajadused, tervishoiule eraldatud vahendid, tervishoiuteenuse osutamine ja selle üldine kättesaadavus, samuti kulutused tervishoiule ja selle rahastamine ning suremuse põhjused. Sellise terviseandmete avalikes huvides töötlemise tulemusel ei tohiks isikuandmeid muudel eesmärkidel töödelda kolmandad isikud, näiteks tööandjad või kindlustus- ja pangandusettevõtjad.
Üldmääruse rakendamisega soovitakse suuremas osas säilitada surnud isikute andmete osas praegu kehtiv õiguslik regulatsioon, kuid kaitset andmetele on plaanis laiendada pärilike haiguste osas (80 aastat ehk ligikaudu keskmine oodatav eluiga). Samuti on kavandatud rakendusseaduses kitsendada IKS § 13 lg-s 1 toodud isikute ringi, kelle nõusolekul on pärast andmesubjekti surma isikuandmete töötlemine lubatud, nii et sellise loa andmise õigus oleks

[25] AKI vastus ringkirjale, lk 7.
http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ylevaade_reformist_14102016.pdf.
[26] Sotsiaalministeeriumi vastuskiri andmekaitse reformipaket ringkirjale, kiri nr 1.2-5/4007-5, lk 2.

ainult andmesubjekti pärijatel. Kavandatavate muudatuste eesmärgiks on muuta õiguskord tegelikele vajadustele paremini vastavaks ning arusaadavamaks.

Sotsiaalne mõju

Sihtrühmad: andmesubjektid, nende pärijad, andmetöötlejad

Isikuandmete töötlemist pärast andmesubjekti surma puudutavad muudatused (kokku võetud tabelis 2) mõjutavad sihtrühmi väikses ulatuses ja harva. Muudatustega muutub isikuandmete töötlemine pärast andmesubjekti surma mõnevõrra rangemaks, samas ei ole ette näha võimalikke ebasoovitavaid tagajärgi. Mõju on tervikuna väheoluline.

Tabel 2. Isikuandmete töötlemine pärast andmesubjekti surma kehtiva ja kavandatava regulatsiooni korral

	Kehtiv regulatsioon	**Kavandatav regulatsioon**
Isikuandmete töötlemise keeld pärast andmesubjekti surma (IKS § 13)	30 aastat	30 aastat
sh pärilike haiguste osas	30 aastat	80 aastat
Isikud, kelle nõusolekul on töötlemine lubatud	pärija, abikaasa, alaneja või üleneja sugulane, õde või vend	pärija
Andmete eriliikide/delikaatsete isikuandmete töötlemine	Nõusoleku korral või IKS § 14 lg 1 tulenevatel alustel (sh seaduse alusel)	Nõusoleku korral või avalikes huvides rahvatervisega seotud valdkondades

5.4. Sertifitseerimine

Üldmääruse järgimise tõendamise elemendina on võimalik kasutada heakskiidetud sertifitseerimismehhanismi. Üldmääruse pp 100 kohaselt tuleks selleks, et parandada läbipaistvust ja üldmääruse järgimist, soodustada sertifitseerimismehhanismide, andmekaitsepitserite ja -märgiste kehtestamist, mis annavad andmesubjektidele võimaluse kiiresti hinnata asjakohaste toodete ja teenuste andmekaitse taset. Andmekaitsalane sertifitseerimine on vabatahtlik ning ligipääsetav protsessi kaudu, mis on läbipaistev (üldmääruse art 42 lg 3). Tegemist ei ole kohustusega, vaid võimalusega tõendada ning näidata väljapoole, et andmetöötlus tõepoolest tugineb isikuandmete kaitse põhimõtetele ning selleks on vastav tõendus sertifitseerimismehhanismi kaudu saadud. Paralleele saab tõmmata näiteks e-kaubanduses kasutusel oleva usaldusmärgisega „Turvaline ostukoht“, mida annab alates 2010. aastast välja E-kaubanduse Liit ning mille eesmärgiks on anda tarbijale ostukoha osas kindlustunne.

Sertifitseerimine ei ole riigi ja kohaliku omavalitsuse andmekogude puhul võrreldav ISKE (infosüsteemide kolmeastmelise etalonturbe süsteem) auditiga[27], kuivõrd ISKE auditi eesmärgiks on hinnata, kas rakendatud on ISKE turvameetmed. Sertifitseerimise eesmärgiks on tõendada üldmääruse nõuete järgimist laiemalt ning see ei piirdu ainult turvalisuse põhimõtte tõendamisega, kuivõrd üldmääruse art 5 lg 1 p-st f on usaldusväärsus ja konfidentsiaalsus (turvalisuse põhimõte) üks põhimõte mitmest, mida tuleb isikuandmete töötlemisel rakendada.

Kontseptsiooni väljatöötamise käigus on küsitud sertifitseerimisega seoses arvamust SA Eesti Akrediteerimiskeskuse sertifitseerimise, inspekteerimise ja tõendamise üksuselt. Üldmääruse art 43 kohaselt väljastab sertifikaadi ja pikendab seda sertifitseerimisasutus, millel on andmekaitse vallas asjakohased ekspertteadmised. Liikmesriikidele on jäetud kohustus kehtestada, kas sertifitseerimisasutusi akrediteerib kas üks või mõlemad järgmistest: pädev järelevalveasutus (AKI), riiklik akrediteerimisasutus (nt SA Eesti Akrediteerimiskeskus). SA Eesti Akrediteerimiskeskus on akrediteerinud asutusi akrediteerimisstandardi EVS-EN ISO/IEC 17065:2012 (nõuded asutustele, kes sertifitseerivad tooteid, protsesse ja teenuseid) järgi. See standard on ka üldmääruse järgi aluseks sertifitseerimisasutuste akrediteerimisel andmekaitse valdkonnas. Erinevate asutuste akrediteerimisel on aga lisaks akrediteerimis-standardi nõuete tundmisele oluline teada ka spetsiifilist valdkonda. SA Eesti Akrediteerimis-keskuselt saadud tagasisidest ilmneb, et selles spetsiifilises valdkonnas pole SA seni ühtegi asutust akrediteerinud ning selline kompetents andmekaitse valdkonnas neil puudub. Kompetentsi tekitamine uues spetsiifilises valdkonnas on aja- ja ressursimahukas ning akrediteerimise alustamisel analüüsib SA alati ka turuvajadust. Kuivõrd SA-l endal hetkel andmekaitsealane kompetents puudub, oleks üldmääruse rakendamisel Justiitsministeeriumi hinnangul sobilikuks lahenduseks see, kui sertifitseerimisasutuste akrediteerimine jääks riigisiseses kontekstis pädeva järelevalve asutuse (AKI) ülesandeks. Samas ei tuleks rakendusseaduses täielikult välistada olukorda, kus sertifitseerimisasutusi poleks tulevikus võimalik akrediteerida mõnel riiklikul akrediteerimisasutusel, kuivõrd andmekaitsealase kompetentsi tekkimine riikliku akrediteerimisasutuse juurde pole tulevikus täielikult välistatud. Seega soovib Justiitsministeerium olla antud küsimuse reguleerimisel paindlik ning arvestada rakendusseaduse koostamisel võimaliku muutuva turuvajadusega.

Järgnevalt on toodud üldmääruse sätted, mis seonduvad sertifitseerimismehhanismi regulatsiooniga, ning elemendid, mida sertifitseerimisega on võimalik tõendada:

- Üldmääruse art 24 lg 3 kohaselt võib vastutava töötleja kohustuste järgimise tõendamise elemendina kasutada art-s 40 osutatud heakskiidetud toimimisjuhendite või art-s 42 osutatud heakskiidetud sertifitseerimismehhanismi järgimist.
- Üldmääruse art 25 kohaselt võib art 25 lg-te 1 ja 2 (lõimitud ja vaikimisi andmekaitse) sätestatud nõuete järgimise tõendamise elemendina kasutada artikli 42 kohast heakskiidetud sertifitseerimismehhanismi.
- Üldmääruse art 28 lg 5 kohaselt võib volitatud töötleja poolt artiklis 40 osutatud heakskiidetud toimimisjuhendite või artiklis 42 osutatud heakskiidetud sertifitseerimismehhanismi järgimist kasutada elemendina selleks, et tõendada art 28 lõigetes 1 („Kui töödeldakse vastutava töötleja nimel, kasutab vastutav töötleja ainult selliseid volitatud töötlejaid, kes annavad piisava tagatise, et nad rakendavad asjakohaseid tehnilisi ja korralduslikke meetmeid sellisel viisil, et töötlemine vastab käesoleva määruse nõuetele ja sealjuures tagatakse andmesubjekti õiguste kaitse.“) ja 4 („Kui volitatud töötleja kaasab vastutava töötleja nimel konkreetsete isikuandmete töötlemise toimingute tegemiseks teise volitatud töötleja, nähakse lepingus või muus liidu või liikmesriigi õiguse

[27] ISKE rakendamise auditite läbiviimise kohustus on reguleeritud Vabariigi Valitsuse 20. detsembri 2007. a määruses nr 252 „Infosüsteemide turvameetmete süsteem“ (nn ISKE määrus).

kohases õigusaktis asjaomase teise volitatud töötleja suhtes ette samad andmekaitsekohustused, mis on sätestatud lõikes 3 osutatud vastutava töötleja ja volitatud töötleja vahelises lepingus või muus õigusaktis; eelkõige annab see piisava tagatise, et rakendatakse asjakohaseid tehnilisi ja korralduslikke meetmeid sellisel viisil, et töötlemine vastaks käesoleva määruse nõuetele. Kui see teine volitatud töötleja ei täida oma andmekaitsekohustusi, jääb algne volitatud töötleja vastutava töötleja ees täielikult vastutavaks kõnealuse teise volitatud töötleja kohustuste täitmise eest.“) osutatud piisava tagatise olemasolu.

- Üldmääruse art 28 lg 6 kohaselt, ilma et see mõjutaks vastutava töötleja ja volitatud töötleja vahelist individuaalset lepingut, võib art 28 lg-tes 3 ja 4 osutatud leping või muu õigusliku toimega dokument põhineda täielikult või osaliselt käesoleva artikli lõigetes 7 ja 8 osutatud lepingu tüüptingimustel, sealhulgas kui need on osa vastutavale töötlejale või volitatud töötlejale artiklite 42 ja 43 kohaselt antud sertifikaadist.
- Üldmääruse art 32 lg-s 1 osutatud nõuete (töötlemise turvalisus) järgimise tõendamise elemendina võib kasutada artiklis 40 osutatud heakskiidetud toimimisjuhendite või artiklis 42 osutatud heakskiidetud sertifitseerimismehhanismi järgimist. Üldmääruse art 32 lg 1 kohaselt, võttes arvesse teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning arvestades isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke, samuti erineva tõenäosuse ja suurusega ohte füüsiliste isikute õigustele ja vabadustele, rakendavad vastutav töötleja ja volitatud töötleja ohule vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid, hõlmates muu hulgas vastavalt vajadusele järgmist:
  a) isikuandmete pseudonümiseerimine ja krüpteerimine;
  b) võime tagada isikuandmeid töötlevate süsteemide ja teenuste kestev konfidentsiaalsus, terviklus, kättesaadavus ja vastupidavus;
  c) võime taastada õigeaegselt isikuandmete kättesaadavus ja juurdepääs andmetele füüsilise või tehnilise vahejuhtumi korral;
  d) tehniliste ja korralduslike meetmete tõhususe korrapärase testimise ja hindamise kord isikuandmete töötlemise turvalisuse tagamiseks.

Mõju riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele

Sihtrühm: AKI ja võimalikud sertifitseerimisasutused (nt erialaliidud)

Tõendamaks, et andmetöötleja isikuandmete töötlemise toimingud vastavad üldmäärusele, võib järelevalveasutus (AKI), akrediteeritud sertifitseerimisasutus või andmekaitsenõukogu väljastada andmetöötlejale sellekohase sertifikaadi. Sertifitseerimine on andmetöötlejatele vabatahtlik, küll aga on liikmesriik kohustatud välja töötama sertifitseerimisasutuste akrediteerimisprotsessi ning julgustama sertifitseerimismehhanismide ja andmekaitsepitserite ja –märgiste kasutuselevõttu.

Võimalikeks sertifitseerimisasutusteks võivad tulevikus olla erialaliidud, kes oskaksid arvestada valdkonna ettevõtete andmetöötluse vajaduste ja eripäradega. Riigiportaali www.eesti.ee andmetel tegutseb Eestis 55 erialaliitu[28]. Sertifitseerimisasutustele antakse akrediteering maksimaalselt viieks aastaks.

Esialgse plaani kohaselt jääb sertifitseerimisasutuste akrediteerimine AKI ülesandeks (vähemalt esialgu), millega kaasneb täiendav töökoormus. Lisaks akrediteerimisele peab

[28] Erialaliitude loetelu: https://www.eesti.ee/est/kontaktid/erialaliidud_1 (31.01.2017)

AKI koostama ja heaks kiitma ka sertifitseerimise kriteeriumid (art 42 lg 5) ja tulevikus jooksvalt läbi vaatama toimimisjuhendeid ja vajaduse korral neid heaks kiitma (art 40 lg 5).

Mõju majandusele: ettevõtluskeskkond ja ettevõtete tegevus

Sihtrühm 1: andmetöötlejad
Sihtrühm 2: andmesubjektid

Andmetöötlejate ja andmesubjektide seisukohast on sertifitseerimisel signaliseeriv efekt – selle kaudu saab tõendada andmesubjektidele (nt klientidele) toodete või teenuste andmekaitse taset ja seega suurendada isikuandmete töötlemisega seotud usaldusväärsust. Teisest küljest saab sertifitseerimisega tõendada üldmääruse erinevate sätete järgimist ja nõuetele vastavust (vt käesolev alapunkt lk 18). Andmetöötleja tegevusele saab anda andmekaitse sertifikaadi maksimaalselt kolmeks aastaks (art 42 lg 7).

Muudatusel on sihtrühmadele positiivne, kuid väheulatuslik mõju. Kuna sertifitseerimine on vabatahtlik ja peab toimuma läbipaistvalt, siis puudub ka ebasoovitavate mõjude risk.

5.5. Trahvid

Üldmääruse pp-s 151 on ära toodud Eestile oluline erisus üldmäärusest, mis puudutab haldustrahve (ingl. k. *administrative fines*) ja nende kohaldamist. Eesti õigussüsteem ei võimalda määrata trahve üldmääruses sätestatu kohaselt (haldustrahve Eesti õiguses ei eksisteeri). Trahve käsitlevaid eeskirju lubab üldmäärus kohaldada selliselt, et Eestis määrab trahvi järelevalveasutus (Andmekaitse Inspektsioon) väärteomenetluse raames, tingimusel et eeskirjade sellisel kohaldamisel nimetatud liikmesriikides on samaväärne toime nagu järelevalveasutuste määratud trahvidel. Sellepärast peaksid pädevad riiklikud kohtud võtma arvesse trahvi algatava järelevalveasutuse soovitust. Igal juhul peaksid määratavad trahvid olema tõhusad, proportsionaalsed ja heidutavad.

Seni on Andmekaitse Inspektsioon rikkumistele reageerimiseks kasutanud sunniraha (sunniraha määramisele eelneb sunniraha hoiatust sisaldav ettekirjutus), kuid küsimusi on tekitanud sellise süsteemi jätkumine üldmääruse rakendamisel, kuivõrd Eesti õiguse kohaselt ei ole sunniraha karistus (asendustäitmise ja sunniraha seaduse (edaspidi *ATSS*) § 3 lg 2 kohaselt ei käsitata sunnivahendi rakendamist karistusena). Alljärgnevalt on esitatud selgitused järelevalveasutuse volituste ja trahvide määramise kohta.
Andmekaitse järelevalveasutuse ehk Andmekaitse Inspektsiooni uurimis- ja parandusvolitused ning lubavad ja nõuandvad volitused on toodud üldmääruse art-s 58. Üldmääruse art 58 lg 2 loetleb, millised parandusvolitused (ingl. k. *corrective powers*) on järelevalveasutusele antud. Art 58 lg 2 on otsekohalduv säte ning seega puudub liikmesriikidel võimalus sätet üldmääruses toodust riigisiseselt teisiti kohaldada. Art 58 lg-s 2 toodud korraldust võib riigisiseses kontekstis tõlgendada kui ettekirjutust haldusmenetluse seaduse (edaspidi *HMS*) tähenduses. Seega jääb AKI-le ka tulevikus alles õigus anda rikkumise lõpetamiseks korraldusi/ettekirjutusi. Art 58 lg 4 sätestab täiendavalt, et järelevalveasutuse poolt erinevate volituste elluviimisel tuleb tagada ka kaitsemeetmete rakendamine, sh õigus kohtulikule kaitsele vastavalt riigisisesele õigusele. Antud sätet tuleks tõlgendada selliselt, et AKI poolt art 58 lg 2 kohase ettekirjutuse tegemisele või mistahes muu meetme rakendamisele kohaldatakse HMS tulenevaid reegleid, sh vastavat kaebemenetlust.

Üldmääruse art 83 lg 2 annab AKI-le õiguse kas lisaks üldmääruse art 58 lg 2 p-des a–h ja j osutatud parandusvolitustele või nende asemel määrata trahve (sh AKI korralduse/ettekirjutuse täitmata jätmise eest (art. 83 lg 6)).
Üldmääruse art 83 alusel määratud trahve saab üldmääruse kohaldamisel määrata eesti õiguses väärteotrahvidena, kui nad on määratud ilma üldmääruse art 58 lg-s 2 toodud korralduse/ettekirjutuseta või nendega paralleelselt (on kohe asutud karistama, sest rikkumine on juba toimunud ja selle lõpetamisele sundimist pole võimalik enam ette võtta). Samuti tuleb kõne alla väärteotrahvide kohaldamine siis, kui sama rikkumise asjas viiakse läbi nii haldus- kui ka väärteomenetlust (rikkumise lõpetamisele sundimine ja selle eest ühtlasi heidutavalt karistamine). Trahvi määramisel peab järelevalveasutus arvestama art 83 lg-s 2 loetletud asjaoludega (punktid a–k).

Seega saab Andmekaitse Inspektsioon tulevikus kohaldada:
1) nii järelevalvet koos sunnirahaga (üldmääruse art 55 lg 2 korraldus + art 83 lg 6 trahv);
2) väärteo korras karistamist (üldmääruse art 83 ühekordsed trahvid ja lisaks art 84 alusel muude koosseisude korral määratavad väärteotrahvid);
3) nii sunniraha kui ka väärteo korras karistamist (samas asjas nii rikkumise lõpetamise korraldus ja selle eiramisel korduv sundiv trahv + samas asjas ka karistav trahv).

Tähelepanu väärib asjaolu, et seal, kus üldmäärus näeb ette trahvi kohaldamise, pole võimalik riiklikul sõltumatul järelevalveasutusel (AKI-l) jätta üldmääruses ette nähtud trahve kohaldamata. Seega olukordades, kus üldmäärus näeb ette trahvide kohaldamise, tuleb kohaldada trahve ning sunniraha on võimalik määrata sellele lisaks (*in addition to*), aga mitte üldmääruses ette nähtud trahvi asemel (*instead of*).

Üldmääruse art 83 lg 4 loetleb rikkumised, mille korral peab määratava trahvi suurus olema kuni 10 000 000 € või kuni 2% ettevõtte eelneva majandusaasta ülemaailmsest aastasest kogukäibest. Üldmääruse art 83 lg-d 5 ja 6 loetlevad rikkumised, mille korral peab määratava trahvi suurus olema kuni 20 000 000 € või kuni 4 % ettevõtte eelneva majandusaasta ülemaailmsest aastasest kogukäibest. Art 83 lg 5 p e sätestab, et art 58 lg 2 kohase järelevalveasutuse korralduse eiramise eest või art 58 lg 1 sätestatud järelevalveasutuse juurdepääsuõiguse rikkumise eest peab määratava trahvi suurus olema kuni 20 000 000 € või kuni 4% ettevõtte ülemaailmsest aastakäibest. Sanktsioonide rakendamisele tuleb kohaldada asjakohaseid kaitsemeetmeid ja tagatisi, sh kohtuliku kaitse võimalusi.
Üldmääruse art 83 lg 7 kohaselt võivad liikmesriigid näha ette eeskirju selle kohta, kas ja millisel määral võib trahve määrata selles liikmesriigis asutatud avaliku sektori asutustele ja organitele. Tegemist on liikmesriikide jaoks kaalutluskohaga, kuid Justiitsministeeriumi hinnangul ei pruugi olla kõige mõistlikum Eesti kontekstis selliseid norme rakendusseaduses kehtestada, kuivõrd piltlikult öeldes oleks tegemist riigi rahakotist raha ühest taskust teise tõstmisega. Selle asemel võiks avaliku sektori puhul näha lahendusena võimalust, kus järelevalveasutusel on muud tõhusad meetmed selleks, et tagada andmekaitsenõuetest kinnipidamine (nt Andmekaitse Inspektsiooni õigus peatada rikkumise korral andmete töötlemine).

Käesolev kontseptsioon haakub karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (EL õiguses sätestatud haldustrahvide kohaldamine Eesti õiguses) väljatöötamiskavatsusega[29] (edaspidi *VTK*), mille Justiitsministeerium on esitanud

[29] Karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (EL õiguses sätestatud haldustrahvide kohaldamine Eesti õiguses) väljatöötamiskavatsus: http://eelnoud.valitsus.ee/main/mount/docList/af8feea7-5e75-435b-8152-18ece419983f#CeiKGUqR.

kooskõlastamiseks 2016. a lõpus. VTK väljatöötamise põhjus seisneb asjaolus, et Euroopa Parlament ja nõukogu on võtnud vastu finantsõigust ja andmekaitset puudutavates valdkondades (andmekaitse üldmäärus) mitmeid erinevaid direktiive ja määrusi, milles kohustatakse liikmesriike võimaldama teatud nõuete rikkumise eest kohaldada halduskaristusi ja muid haldusmeetmeid. Rahatrahvide ülemmäärad ning nende arvutamise alused ei sobitu hetkel kehtiva riigisisese õigusega, mistõttu on probleemile otsustatud läheneda süsteemselt. VTK eesmärgiks on muudatuste ja täienduste abil viia seadusandlik olukord vastavusse EL õigusest tulenevate nõuetega ning võimaldada Eestis kohaldada EL õigusaktides sätestatud ülemmääradega rahalisi sanktsioone. Kõnealusele VTK-le viitamine käesolevas kontseptsioonis on oluline, kuivõrd VTK-ga saavutatavatest tulemustest oleneb ka andmekaitse üldmääruses ette nähtud halduskaristuste ja haldusmeetmete kohaldamine. Seetõttu siinkohal EL õiguses ette nähtud haldustrahvide Eesti õiguses kohaldamise temaatikal pikemalt ei peatuta, kuivõrd probleemile otsitakse lahendust teise õigusdokumendi raames.

Määruse rakendamiseks on kavandatud koostada rakendusseaduse peatüki „Vastutus“ alla väärteokoosseisud üldmääruse art 83 lg 4 p-de a–c, lg 5 p-de a–e ja lg 6 alusel. Nt üldmääruse art 83 lg 4 p-le a vastav väärteokoosseis on kavandatud Eesti õiguses kohalduma järgmiselt:

„§ X. Vastutava töötleja või volitatud töötleja kohustuse rikkumine
(1) Üldmääruse artiklite 8, 11, 25–39, 42 ja 43 nimetatud vastutava ja volitatud töötleja kohustuste rikkumise eest –
karistatakse rahatrahviga kuni 10 000 000 eurot.
(2) Käesoleva paragrahvi lõikes 1 sätestatud teo eest, kui selle on toime pannud juriidiline isik, –
karistatakse rahatrahviga 10 000 000 eurot või kuni 2% tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem.“.

Mõju julgeolekule

Sihtrühmad: andmetöötlejad, AKI

Andmekaitsega seotud rikkumiste arvu ei ole võimalik ette prognoosida, kuid võrdluseks saab välja tuua senise IKS-i alusel registreeritud väärtegude arvu ning Andmekaitse Inspektsiooni sunnivahendi (sunniraha) rakendamise praktika. 2015. aastal saabus Andmekaitse Inspektsioonile kokku 446 kaebust, vaiet või väärteoteadet. IKS § 42 alusel registreeriti 16 väärtegu, mis seisnesid isikuandmete töötlemise nõuete rikkumises. 15 rikkumise puhul määrati karistusena trahv või rakendati sunnivahendina sunniraha.

Tabel 3. Andmekaitse Inspektsiooni järelevalvestatistika, 2012–2015

	2012	**2013**	**2014**	**2015**
Ettekirjutused	187	120	86	77
Väärteoasjad	43	29	11	16
Määratud trahv või sunniraha	39	22	8	15

Allikas: Andmekaitse Inspektsioon

Analoogselt praegusele regulatsioonile annab ka üldmäärus AKI-le volituse teha korraldusi (praegu ettekirjutusi), kuid üldmäärtuse art 58 lg 2 sätestab detailsemalt ka uued parandusvolitused. Kuigi järelevalvet puudutavad muudatused avaldavad mõningat töökorralduslikku mõju AKI igapäevatööle, siis sisuline mõju nii AKI-le kui

andmetöötlejatele on väike. Erandiks võivad olla väärteomenetlused, milles määratavad trahvid võivad oluliselt suureneda (praegu on võimalik IKS § 42 alusel karistada juriidilist isikut rahatrahviga kuni 32 000 eurot).

5.6. Isikuandmete töötlemise erinormide säilitamine ja kehtestamine

Andmekaitse Inspektsioon on teinud ettepaneku säilitada IKS erinormid uue rakendusseaduse erinormidena:
a) isikuandmete ajakirjandusliku avaldamise alal (IKS § 11 lg 2-3 vs üldmääruse art. 85);
b) füüsiliste isikute maksehäireandmete avaldamise alal (IKS § 11 lg 6–7), tehingukäibe usaldusväärsuse huvides lubab IKS praegu maksehäire- ehk võlaandmete avaldamist teistele isikutele ilma inimese enda nõusolekuta, kuivõrd teiste isikute kaitset halbade tehingute tegemise eest loetakse kaalukamaks kui võlgniku eraelu kaitset; samas püüab IKS ära hoida ka võlgnike üleliigset kahjustamist (õigus oma võlgniku maksehäireandmeid edastada ei tähenda andmete avalikustamist piiramatule arvule tuvastamata isikutele);
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.[30]

Üldmääruse art 85 näeb ette isikuandmete töötlemise sõna- ja teabevabaduse kontekstis. Üldmääruse art 85 lg-st 1 tuleneb liikmesriikidele kohustus ühitada õigusaktiga õigus isikuandmete kaitsele ning sõna- ja teabevabaduse õigus (muu hulgas seoses isikuandmete töötlemisega ajakirjanduslikel eesmärkidel ning akadeemilise, kunstilise või kirjandusliku eneseväljenduse tarbeks).
Hetkel kehtiva IKS § 11 lg 2 kohaselt võib isikuandmeid võib ilma andmesubjekti nõusolekuta ajakirjanduslikul eesmärgil töödelda ja avalikustada meedias, kui selleks on ülekaalukas avalik huvi ning see on kooskõlas ajakirjanduseetika põhimõtetega. Andmete avalikustamine ei tohi ülemääraselt kahjustada andmesubjekti õigusi.
Seega on hetkel kehtiva IKS poolt kaetud küll isikuandmete töötlemine ajakirjanduslikel eesmärkidel, kuid reguleeritud pole võimalikke erandeid ja vabastusi isikuandmete kaitse regulatsioonist akadeemilise, kunstilise ja kirjandusliku eneseväljenduse tarbeks. Seetõttu kavandatakse üldmääruse art 85 sisustamiseks regulatsiooni, kus ka näiteks uudisväärtuseta kirjandus- ja kunstiteoste puhul oleks teatud tingimustel lubatud isikuandmete avalikustamine ilma inimese enda nõusolekuta (erand üldmääruse II peatükist). Sellise erandi loomine on vajalik, kuivõrd andmesubjektil on õigus nõusolek oma isikuandmete töötlemiseks tagasi võtta (üldmääruse art 7 lg 3). Nõusoleku isikuandmete töötlemiseks tagasivõtmine võib osutuda problemaatiliseks näiteks olukordades, kus koostatud on filmistsenaarium või elulooraamat[31], nõusoleku isikuandmete töötlemiseks tagasivõtmine tingiks vajaduse filmi[32] või raamatu levitamise lõpetamise (müügilt korjamise) järele ning kokkuvõttes tekitaks ebamõistlikult suure riski majandusliku kahju tekkeks. Seega soovitakse kavandatava regulatsiooniga piirata võimalust isikuandmete töötlemiseks antud nõusolekut tagasi võtta selleks, et tagada sõna- ja teabevabaduse kaitse.

[30] Andmekaitse Inspektsiooni peadirektori ülevaade, lk 5.
[31] Vt ka RKo 3-2-1-153-16 p 25, kus kolleegium nõustus maakohtu seisukohaga, milles leiti, et eluloolises väljaandes (elulooraamat), millel pole uudisväärtust, isikuandmete avalikustamine ei kvalifitseeru ajakirjanduslikul eesmärgil isikuandmete avalikustamise alla.
[32] Vt ka RKo 3-2-1-104-09, Magnuse filmi levitamise keelamise kaasus.

Üldmääruse 86 reguleerib isikuandmete töötlemist ja üldsuse juurdepääsu ametlikele dokumentidele. Antud valdkonda reguleerib eesti õiguses avaliku teabe seadus (AvTS) ning artikkel loetakse kaetuks AvTS regulatsiooniga.

Üldmääruse art 87 sätestab, et liikmesriigid võivad täiendavalt kindlaks määrata konkreetsed tingimused, mille kohaselt võib töödelda riiklikku isikukoodi või muud üldkasutatavat tunnust. Isikukoodi regulatsioon on kehtivas seadusandluses leitav rahvastikuregistri seaduse (RRS) 9. peatükist. Seetõttu pole üldmääruse art 87 katmiseks kavandatud täiendavat regulatsiooni luua.

Üldmääruse art 89 sätestab kaitsemeetmed ja erandid seoses isikuandmete töötlemisega avalikes huvides toimuva arhiveerimise, teadus- ja ajaloouuringute või statistilisel eesmärgil. Justiitsministeerium nõustub AKI nägemusega, et säilitada saab teadusuuringute loamenetluse (IKS § 16) kui kolmanda alternatiivi seadusekohase ja nõusolekupõhise teadusuuringu kõrval. Topeltprotseduuride vältimiseks saab võrdsustada loamenetluse läbimise üldmääruse kohase eelkonsulteerimisega (üldmääruse art 36). AKi on teinud ka ettepaneku jätta loamenetlusest välja ajaloouuringud. Teadusuuringu loamenetlus on mõeldud nende uuringute tarvis, kus sisendiks on isikuandmed ja väljundiks üldistused; ajalooteaduses on isikuandmed aga reeglina ka väljundiks. Ajaloouuringutega seonduv reguleeritakse arhiiviseaduses.

Üldmääruse art 90 kohaselt võivad liikmesriigid vastu võtta ka erieeskirju, et kehtestada üldmääruse art 58 lg 1 p-des e ja f sätestatud järelevalveasutuste volitused seoses andmetöötlejatega, kellel on liidu või liikmesriigi õiguse või riiklike pädevate eeskirjade asutuste kehtestatud eeskirjade alusel ametisaladuse hoidmise kohustus (nt advokaadi kutsesaladus) või muu samaväärne saladuse hoidmise kohustus, kui see on vajalik ja proportsionaalne, et ühitada isikuandmete kaitse õigus ja saladuse hoidmise kohustus. Neid eeskirju lubab üldmäärus kohaldada üksnes nende isikuandmete suhtes, mida vastutav töötleja või volitatud töötleja on saanud saladuse hoidmise kohustusega hõlmatud tegevuse käigus. Antud küsimuses puudub Justiitsministeeriumil arvates vajadus praegu kehtivast regulatsioonist erinevat regulatsiooni kehtestada.

5.7. Üldmääruse artikkel 80 ja nn populaarkaebused

Üldmääruse art-st 80 tuleneb uudsena populaarkaebuse esitamise õiguse võimalus andmekaitse valdkonnas. Tegemist ei ole liikmesriigi jaoks siiski imperatiivse sättega, vaid liikmesriikidele on jäetud üldmäärusega võimalus sellise esindusõiguse sätestamiseks riigisiseses õiguses.

Üldmääruse art 80 lg 2 kohaselt võivad liikmesriigid ette näha, et mittetulunduslikke eesmärke teenivatel asutustel, organisatsioonidel ja ühendustel on andmesubjekti volitustest sõltumatult õigus esitada pädevale järelevalveasutusele (AKI) kaebus ning kasutada tõhusat õiguskaitsevahendit, kui see asutus, organisatsioon või ühendus leiab, et andmesubjekti õigusi on isikuandmete töötlemise tulemusena rikutud.

Üldine kohtusse pöördumise õigus tuleneb Eesti Vabariigi põhiseaduse § 15 lõike 1 esimesest lausest, mis sätestab, et igaühel on õigus pöörduda oma õiguste ja vabaduste rikkumise korral kohtusse. Selle lause põhiseaduslik sõnum on, et iga subjektiivset õigust peab olema võimalik

realiseerida kohtus tõhusas ja ausas menetluses mõistliku aja jooksul.[33] Samas, kohtutee garantii ei laiene nn populaarkaebusele (erand Århusi konventsiooni art 9 lg 3).[34]

Kuivõrd Andmekaitse Inspektsiooni hinnangul tuleks jätta nn populaarkaebused seadustamata, kuna Eesti õiguses on see valdkond juba kaetud märgukirja regulatsiooniga,[35] ning ka õiguskirjanduses on mainitud, et populaarkaebus on pigem erandlik kaebeõiguse vorm[36], ei kavandata käesoleva kontseptsiooniga eesti õiguses andmekaitsevaldkonnas muudatusi, mis näeksid mittetulunduslikele asutustele, organisatsioonidele ja ühendustele ette andmesubjekti volitustest sõltumatult järelevalveasutusele kaebuse esitamise võimaluse (nn populaarkaebuse esitamise võimaluse). Justiitsministeeriumi hinnangul on ka tulevikus õigustatud senise praktika jätkumine, kus isikutel on võimalus adressaadile (nt AKI) teha ettepanekuid asutuse või organi töö korraldamiseks või valdkonna arengu kujundamiseks ning anda adressaadile teavet märgukirjale ja selgitustaotlusele vastamise seaduses sätestatud korras. Andmesubjekti õigust oma õiguste kaitseks ise kohtusse pöörduda ei piirata.

5.8. Lapse nõusolek seoses infoühiskonna teenustega

Üldmääruse kohaselt on lapse isikuandmete töötlemine seaduslik ainult juhul, kui laps on vähemalt 16-aastane, kui kohaldatakse üldmääruse art 6 lg 1 p a (isikuandmete töötlemine loetakse seaduslikuks, kui andmesubjekt on andnud nõusoleku töödelda oma isikuandmeid ühel või mitmel konkreetsel eesmärgil) seoses infoühiskonna teenuste pakkumisega otse lapsele (lapse nõusolek). Kui laps on noorem kui 16-aastane, on selline isikuandmete töötlemine seaduslik üksnes sellisel juhul ja sellises ulatuses, kui selleks on sellise nõusoleku või loa andnud isik, kellel on lapse suhtes vanemlik vastutus. Liikmesriigid võivad seadusega sätestada madalama asjaomase vanuse tingimusel, et selline madalam vanus ei ole vähem kui 13 aastat (art 8 lg 1). Selline võimalus vahemikus 13–16 eluaastat lapse kehtiva nõusoleku piir kehtestada eksisteerib ka eesti seadusandluse jaoks.

Vastutav töötleja on kohustatud kättesaadavat tehnoloogiat arvesse võttes tegema mõistlikud jõupingutused selleks, et kontrollida sellistel juhtudel, et nõusoleku või loa on andnud isik, kellel on lapse suhtes vanemlik vastutus (seaduslik esindaja)(art 8 lg 2). Üldmäärus ei mõjuta liikmesriigi üldist lepinguõigust, näiteks õigusnorme, mis käsitlevad lapsega seotud lepingu kehtivust, koostamist ja mõju (art 8 lg 3).

Infoühiskonna teenuse all on üldmääruse art 4 p 25 kohaselt peetud silmas teenust, mis vastab Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/1535[37] artikli 1 lõike 1 punktile b ehk infoühiskonna iga teenus ehk kõik vahemaa tagant elektroonilisel teel ja teenusesaaja isikliku taotluse alusel ning tavaliselt tasu eest osutatavad teenused. Üldmääruse loogika järgib põhimõtet, et laste isikuandmed väärivad erilist kaitset, kuna lapsed ei pruugi olla piisavalt teadlikud asjaomastest ohtudest, tagajärgedest ja kaitsemeetmetest ning oma õigustest seoses isikuandmete töötlemisega. Niisugune eriline kaitse peaks eelkõige rakenduma laste isikuandmete kasutamisel turunduse eesmärgil või isiku või kasutajaprofiili loomiseks ja laste

[33] Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. E.-J. Truuväli jt (toim.). Teine, täiendatud väljaanne. Tallinn: Juura 2008, § 15 komm. 1.2.
[34] Samas, komm. 2.1.1.
[35] AKI vastus ringkirjale, lk 9.
[36] Ploom, T., Kärner, M., Juridica VII/2015. Kannatanu huvide realiseerimine kriminaalmenetluses, lk 509.
[37] Euroopa Parlamendi ja nõukogu 9. septembri 2015. aasta direktiiv (EL) 2015/1535, millega nähakse ette tehnilistest eeskirjadest ning infoühiskonna teenuste eeskirjadest teatamise kord (ELT L 241, 17.9.2015, lk 1).

isikuandmete kogumisel otse lastele pakutavate teenuste kasutamise puhul. Vanemliku vastutuse kandja nõusolekut ei peaks olema vaja seoses lapsele otse pakutavate ennetavate või nõustamisteenustega.[38]

Andmekaitse Inspektsiooni hinnangul tuleks Eesti õiguses selles küsimuses otsustada kõige madalama vanusemäära ehk 13 eluaasta kasuks.[39]

Eesti õiguses on tsiviilseadustiku üldosa seaduse (edaspidi *TsÜS*) § 8 lg 2 kohaselt täielik teovõime 18-aastaseks saanud isikul (täisealisel). Paragrahvis 8 sätestatud reeglid teovõime kohta määravad isikute võime teha kehtivaid tehinguid ning omavad tähendust kõigis eraõiguse valdkondades.[40] Alla 18-aastasel isikul (alaealisel) on piiratud teovõime. Seega teeb üldmääruse art 8 erisuse TsÜS üldregulatsioonist. Selline erisus TsÜS-ist poleks siiski esmakordne. Lisaks TsÜS-ile on eri seadustes mitmesuguseid täpsustusi. Näiteks töölepingu sõlmimise osas sätestab töölepingu seadus (edaspidi *TLS*) mitmed erisused, võrreldes TsÜS üldreeglitega alaealistega töölepingu sõlmimise kohta, vt TLS §-d 7 ja 8.[41] Samuti teeb üldregulatsioonist erisuse VÕS § 766 lg 4 nähes ette, et piiratud teovõimega patsiendi puhul kuuluvad VÕS § 766 lõigetes 1 ja 3 nimetatud õigused patsiendi seaduslikule esindajale niivõrd, kuivõrd patsient ei ole võimeline poolt- ja vastuväiteid vastutustundeliselt kaaluma.

Mitmed olulised õigused-kohustused antakse noortele enne 18. eluaastat. Nii saab näiteks 14-aastast isikut võtta vastutusele tehtud väär- või kuriteo eest, perekonnaseaduse § 1 lõike 3 kohaselt võib kohus alaealise teovõime laiendamise sätete kohaselt laiendada vähemalt 15-aastaseks saanud isiku teovõimet nende toimingute tegemiseks, mis on vajalikud abielu sõlmimiseks ning abieluga seotud õiguste teostamiseks ja kohustuste täitmiseks. 16-aastane isik võib osaleda kohaliku omavalitsuse volikogu valimisel ja taotleda B-kategooria (auto) piiratud juhilube.

Arvestada tuleb aga sellega, et kuigi üldmääruse kohaselt on andmete töötlemiseks nõusoleku andmiseks vaja seadusliku esindaja nõusolekut juhul, kui laps on alla 16-aastane ning liikmesriigid võivad sätestada madalama vanusepiiri, siis alaealise isiku poolt kehtiva lepingu sõlmimiseks mõne infoühiskonnateenuse kasutamiseks on ikkagi TsÜS-i kohaselt vajalik seadusliku esindaja nõusolek või heakskiit. Erandiks on TsÜS-i § 11 lõikele 3 vastavad tehingud ehk tehingud, millest ei teki alaealisele isikule otseseid tsiviilkohustusi või mille alaealine täidab vahenditega, mille andis talle selleks otstarbeks või vabaks kasutamiseks tema seaduslik esindaja või viimase nõusolekul kolmas isik.

Planeeritava õigusmuudatuse tulemusena soovitakse lisada infoühiskonna teenuse seadusesse säte, millega reguleeritakse vanusepiir, millest alates on Eesti õiguses lapse poolt antud nõusolek infoühiskonna teenuse kasutamiseks kehtiv ning seaduslik. Valikuvariandid on 13, 14, 15 ja 16 eluaastat alaealise nõusoleku vanusemäära kehtestamiseks. Justiitsministeeriumi esialgsel hinnangul väärib kaalumist idee kehtestada vanusepiir 13 eluaasta ehk madalaima võimaliku määra peale. Vanusepiiri kehtestamise osas ootab Justiitsministeerium tagasiside kooskõlastusringilt.

Sotsiaalne mõju

[38] Üldmääruse pp 38.
[39] AKI vastus ringkirjale, lk 7.
[40] Varul, P. jt. Tsiviilseadustiku üldosa seadus. Kommenteeritud väljaanne. Kirjastus Juura 2010. Lk 33.
[41] Samas, lk 34.

Sihtrühm: noored ja nende vanemad. Statistikaameti andmetel oli 2016. aasta 1. jaanuari seisuga Eestis kokku 223 793 alla 16-aastast last ja noort, nende hulgas oli 13-aastaseid 12 426, 14-aastaseid 12 061 ja 15-aastaseid 12 348.

Kaalumisel on neli alternatiivi alaealise isikuandmete töötlemisega seotud vanusepiiri kehtestamiseks. Vanusepiirist nooremate laste isikuandmete töötlemine infoühiskonna teenuse pakkumisel ei ole seaduslik, kui töötlemise tingimuseks on andmesubjekti nõusolek (nt sotsiaalmeedia teenused). Alaealise nõusolek loetakse seaduslikuks alates 16. eluaastast. Vanuse poolest sinna vahele jäävate noorte isikuandmete töötlemine eeldab edaspidi lapsevanema nõusoleku küsimist.

Üldmäärus jätab konkreetse vanusepiiri iga liikmesriigi otsustada, kaldudes sellega mõnevõrra eemale regulatsiooni EL-i sisesest harmoniseerimise eesmärgist. Nii andmekaitse valdkonna kui ka noortega tegelevate spetsialistide hulgas puudub üksmeel, milline peaks vanusepiir olema[42]. Peamiseks vastuargumendiks kõrge vanusepiiri (16 eluaastat) kehtestamiseks on infoühiskonna teenuste kättesaadavuse halvenemine noorte jaoks ja sellega kaasnevad negatiivsed tagajärjed[43], pooltargumendiks on alaealiste isikuandmete kaitse tõhustamine.

Kontseptsiooni koostajad paluvad Eesti spetsialistide ja huvirühmade arvamust sobivaima lahenduse osas – kas vanusepiir, millest alates on alaealise (või tema vanema) poolt antud nõusolek infoühiskonna teenuste kasutamiseks seaduslik, võiks olla 13, 14, 15 või 16 eluaastat?

Majanduslik mõju

Sihtrühm: infoühiskonna teenuseid pakkuvad ettevõtted (andmetöötlejad)

Infoühiskonna teenuste puhul võib isikuandmete töötlemine seisneda nende kogumises ja kasutamises näiteks turunduse eesmärgil, isiku või kasutajaprofiili loomiseks või otseselt teenuse pakkumiseks. Arvestades teenuste mitmekesisust, ei ole võimalik hinnata sihtrühma suurust arvuliselt, kuid juba ainuüksi telekommunikatsiooni, programmeerimise, andmetöötluse, veebiportaalide ja veebihostinguga tegelevaid ettevõtteid on Eestis ligi 3000 kogukäibega ligi 1,5 miljardit eurot aastas[44]. Eesti elanike enamkülastatavate veebilehtede hulgas on ülekaalus siiski rahvusvahelised portaalid, Eesti ettevõtete osatähtsus jääb alla poole[45].

Riigisisesele turule orienteeritud teenusepakkujate jaoks on kõrgem isikuandmete töötlemise vanusemäär turgu kitsendava mõjuga, eriti arvestades, et noorte vanuserühmades on infotehnoloogiliste vahendite kasutamise osakaal keskmisest kõrgem (näiteks 16-24-aastaste hulgas on internetikasutajate osakaal ligi 100%[46]). Samas ei pruugi ka madalama vanusepiiri kehtestamisel teenusepakkujad seda rakendama hakata, kui

[42] Rohkem infot IAPP (*The International Association of Privacy Professionals*) kodulehel: https://iapp.org/news/a/will-gdpr-move-age-of-consent-to-16/ (02.02.2017)
[43] Noorteorganisatsioonide arvamus vanusepiiri kohta: http://www.antibullyingpro.com/blog/2015/12/11/letter-expressing-concern-to-the-draft-general-data-protection-regulation-13to16 (02.02.2017)
[44] Statistikaameti andmed IKT ettevõtete majandusnäitajate kohta 2014. aastal.
[45] Veebilehtede külastatavust riikide lõikes jälgib analüütikaportaal Alexa: http://www.alexa.com/topsites/countries/EE (06.02.2017)
[46] Eesti Statistika Kvartalikiri 3/15, lk 87, http://www.stat.ee/valjaanne-2015_eesti-statistika-kvartalikiri-3-15 (06.02.2017)

seadusliku esindaja nõusoleku saamine toob ettevõttele kaasa ebaproportsionaalsed kulud. Vanusepiiri regulatsioonist on rohkem mõjutatud teenusepakkujad, kes tegutsevad rahvusvaheliselt ning peavad edaspidi hakkama arvestama mitme riigi regulatsiooniga.

Kokkuvõtvalt võib järeldada, et kuigi isikuandmete töötlemise vanusepiiri kehtestamine võib teenusepakkujatele kaasa tuua rahalise kulu turu kitsenemise või isikutuvastamise meetmete kasutuselevõtu näol, siis valik konkreetsete alternatiivide vahel (13, 14, 15 või 16) on pigem väheolulise mõjuga. Muudatuste tagajärjel ettevõtjate halduskoormus tervikuna suureneb.

5.9. Erandid üldmääruse kohaldamisest

Justiitsministeerium on saatnud 19.09.2016 ministeeriumitele ja AKI-le andmekaitse reformipaketi ringkirja (kiri nr nr 10-4/6761-1), milles on palunud erilist tähelepanu pöörata just üldmääruse artikli 23 eranditele, mis jätab liikmesriigile võimaluse riigisiseses õiguses kehtestada piiranguid määruse mõningate artiklite rakendamiseks.

Õigus isikuandmete kaitsele ei ole absoluutne õigus, vaid seda tuleb kaaluda vastavalt selle ülesandele ühiskonnas ning tasakaalustada muude põhiõigustega vastavalt proportsionaalsuse põhimõttele (üldmääruse pp 4 ls 2). Sellest loogikast lähtuvalt võib üldmääruse art 23 kohaselt vastutava või volitatud töötleja suhtes kohaldatavas liidu või liikmesriigi õiguses seadusandliku meetmega piirata üldmääruse artiklites 12–22 (III peatükk andmesubjekti õigused), artiklis 34 (andmesubjekti teavitamine isikuandmetega seotud rikkumisest) ja artiklis 5 (isikuandmete töötlemise põhimõtted) sätestatud kohustuste ja õiguste ulatust, kuivõrd selle sätted vastavad üldmääruse artiklites 12–22 sätestatud õigustele ja kohustustele, kui selline piirang austab põhiõiguste ja –vabaduste olemust ning on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede, et tagada:

a) riigi julgeolek;
b) riigikaitse;
c) avalik julgeolek;
d) süütegude tõkestamine, uurimine, avastamine või nende eest vastutusele võtmine või kriminaalkaristuste täitmisele pööramine, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja nende ennetamine;
e) liidu või liikmesriigi muud üldist avalikku huvi pakkuvad olulised eesmärgid, eelkõige liidu või liikmesriigi oluline majanduslik või finantshuvi, sealhulgas rahandus-, eelarve- ja maksuküsimused, rahvatervis ja sotsiaalkindlustus;
f) kohtusüsteemi sõltumatuse ja kohtumenetluse kaitse;
g) reguleeritud kutsealade ametieetika rikkumiste ennetamine, uurimine, avastamine ja nende eest vastutusele võtmine;
h) jälgimine, kontrollimine või regulatiivsete ülesannete täitmine, mis on kas või juhtumipõhiselt seotud avaliku võimu teostamisega punktides a–e ja g osutatud juhtudel;
i) andmesubjekti kaitse või teiste isikute õiguste ja vabaduste kaitse;
j) tsiviilõiguslike nõuete täitmise tagamine.

Seadusandlik meede, millega ülaltoodud eesmärke tagatakse, peab sisaldama konkreetseid sätteid vähemalt järgmise kohta (üldmääruse art 23 lg 2):

a) töötlemise või selle kategooriate eesmärgid;
b) isikuandmete liigid:
c) kehtestatud piirangute ulatus;
d) kuritarvitamist või ebaseaduslikku andmetega tutvumist või nende edastamist tõkestavad kaitsemeetmed;
e) vastutava töötleja või vastutavate töötlejate kategooriate määratlus;
f) säilitamise ajavahemikud ja kohaldatavad kaitsemeetmed, võttes arvesse töötlemise või selle kategooriate laadi, ulatust ja eesmärki;
g) andmesubjektide õigusi ja vabadusi ähvardavad ohud ning
h) andmesubjektide õigus olla piirangust teavitatud, välja arvatud juhul, kui see võib mõjutada piirangu eesmärki.

Üldmääruse kohaldamist (üldmääruse art-st 23 tulenevalt) on Eesti kontekstis plaanitud piirata riigisaladuse ja salastatud välisteabe seadusega, taustakontrolli seadusega, maksukorralduse seadusega (maksuhalduri uurimispõhimõte), korrakaitseseadusega (osaga, mida õiguskaitsevaldkonna direktiiv ei kata), hädaolukorra seadusega (HOS § 6 lg 3 kohaselt on pädeval asutusel õigus saada muudelt asutustelt ja isikutelt hädaolukorra riskianalüüsi koostamiseks vajalikku teavet), kaitseväeteenistuse seadusega (§ 14), kohtutäituri seadusega (§ 11, ametisaladuse hoidmise kohustus), äriseadustikuga (ärisaladus), krediidiasutuste seadusega (pangasaladus), advokatuuriseadusega (kutsesaladus), kohtute seadus (§ 2, õigusemõistmine ja kohtu sõltumatus; üldmäärus ei kohaldu kohtutele nende õigusmõistmise funktsiooni täitmise raames).

Üldmääruse pp 73 (selgitab üldmääruse artiklit 23) kohaselt võib liikmesriigi õiguses kehtestada piirangud, mis puudutavad

- konkreetseid põhimõtteid ja õigust saada teavet,
- õigust andmetega tutvuda,
- nõuda nende parandamist ja kustutamist või
- õigust andmeid ühest süsteemist teise üle kanda,
- õigust esitada vastuväiteid,
- profiilianalüüsil põhinevaid otsuseid,
- samuti andmesubjekti isikuandmetega seotud rikkumisest teavitamist,
- ning vastutavate töötlejate teatavaid seonduvaid kohustusi,

kui selline piirang on demokraatlikus ühiskonnas vajalik ja proportsionaalne selleks, et tagada

- avalik julgeolek, sealhulgas inimelude kaitsmine eelkõige loodus- ja inimtegevusest tingitud õnnetustele reageerimisel,
- süütegude tõkestamine, uurimine ja nende eest vastutusele võtmine või kriminaalkaristuste täitmisele pööramine, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmine või nende ennetamine või
- reguleeritud kutsealade ametieetika rikkumise ennetamine,
- liidu või liikmesriigi muu üldise avaliku huvi, eelkõige liidu või liikmesriigi olulise majandus- või finantshuvi oluline eesmärk;
- üldisest avalikust huvist lähtuvate avalike registrite pidamine,
- arhiveeritud isikuandmete täiendav töötlemine endise totalitaarse riigikorra tingimustes toimunud poliitilise tegevusega seotud konkreetse teabe andmiseks,
- andmesubjekti kaitse või teiste isikute õiguste ja vabaduste kaitse, sealhulgas sotsiaalkaitse, rahvatervis ja humanitaareesmärgid.

Nimetatud piirangud peaksid vastama hartas ning Euroopa inimõiguste ja põhivabaduste kaitsekonventsioonis sätestatud nõuetele.

5.10. Süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete töötlemine ja võimalikud muudatused riiklikes registrites

Süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete töötlemine

Hetkel kehtiva Eesti õiguse kohaselt loetakse delikaatseteks isikuandmeteks selliseid andmeid, mis käsitlevad süüteo toimepanemist või selle ohvriks langemist enne avalikku kohtuistungit või õigusrikkumise asjas enne otsuse langetamist või asja menetluse lõpetamist (IKS § 4 lg 2 p 8). Üldmääruse art-ga 10 kehtestatakse alates 2018. a 25. maist nõue, et süüteoasjades süüdimõistvate kohtuotsuste ja süütegude või nendega seotud turvameetmetega seotud isikuandmeid töödeldakse üldmääruse art 6 lg 1 kohaselt ainult ametiasutuse järelevalve all või siis, kui töötlemine on lubatud liidu või liikmesriigi õigusega, milles on sätestatud asjakohased kaitsemeetmed andmesubjektide õiguste ja vabaduste kaitseks.

Süüteoasjades süüdimõistvate kohtuotsuste terviklikku registrit peetakse ainult ametiasutuse järelevalve all.
Seega ei näe üldmääruse art 10 IKS § 4 lg 2 p-ga 8 sarnast kitsendavat kriteeriumi ning eritingimused kohalduvad ka sellisele teabele, mis käsitleb süütegude toimepanemist või kohaldatud karistusi sõltumata sellest, kas asjas toimub avalik kohtuistung või on tehtud otsus. Art-s 10 loetletud andmete töötlemine on lubatud ning selliseid andmeid ei käsitleta isikuandmete eriliigina üldmääruse art 9 tähenduses, kuid siiski tuleb süütegude toimepanemist ja karistusi käsitlevate andmete töötlemisel lähtuda alljärgnevatest tingimustest:
- töötlemine toimub ametiasutuse kontrolli all või
- töötlemine toimub seaduse alusel, mis näeb ette kohaseid andmesubjekti õiguste ja vabaduste tagatisi.
Lisaks sätestatakse, et karistuste registrit tohib pidada ainult ametiasutuse järelevalve all.

Eestis on karistusregister loodud karistusregistri seadusega (*edaspidi KarRS)*. KarRS sätted vastavad selles osas määruses sätestatud tingimustele, et karistusandmete töötlemine toimub ametiasutuse kontrolli all. Karistusregister on riigi infosüsteemi kuuluv andmekogu, mille vastutav töötleja on Justiitsministeerium. Küll aga ei pruugi olla üldmäärusega kooskõlas KarRS § 7, mille kohaselt on registrisse kantud andmed avalikud. Kõige suuremaks probleemiks on siinkohal avalikkuse poolt ilma põhjuseta päringute tegemine, kuivõrd sellisel juhul ei ole võimalik tagada asjakohaste kaitsemeetmete ja tagatiste rakendamist. Karistusandmete avaldamise üldmäärusega kooskõlla viimiseks tuleb kaaluda lahendusi, mis võimaldaks tagada esiteks päringute õiguspärasuse ning teiseks sisaldaks piisavaid kaitsemeetmeid ning tagatisi andmesubjekti õiguste kaitseks.
Üheks võimalikuks lahenduseks saaks tarvitusele võtta avalikkuse juurdepääsu karistusregistrisse kantud andmetele täielikku lõpetamist. Siiski oleks Justiitsministeeriumi hinnangul selline lähenemine ebaproportsionaalne, kuivõrd teatud juhtudel võib isiku karistusandmete saamine olla põhjendatud. Küll aga tuleks sätestada tingimus, mille kohaselt peab päringu tegemisel olema legitiimne eesmärk, mis oleks kooskõlas karistusregistri pidamise eesmärkidega (KarRS § 3). Samuti aitaks isiku õigusi ja vabadusi tõhusamalt kaitsta olukord, kus väljastatavad andmed on võimalikult üldised ega hõlma näiteks konkreetset kuriteokvalifikatsiooni, samuti kui avalikkusele väljastatakse andmeid ainult raskemate kuritegude kohta, kuivõrd see oleks senisest rohkem kooskõlas proportsionaalsuse põhimõttega ning ühtlasi ka registri pidamise eesmärkidega. Samuti võib teha päringu kaheetapiliseks: esimesel etapil saab isik teavet selle kohta, kas huvipakkuval isikul on kriminaalkaristus või mitte (nn faktipäring) ja seejärel on isikul võimalik pöörduda põhjendatud taotlusega lisateabe saamiseks, mille raames otsustatakse andmete väljastamise põhjendatud ja kooskõla.

Andmekaitse üldmäärusega kooskõlla viimist eeldab ka KarRS § 3, eelkõige olemasoleval kujul on registri eesmärgid sätestatud liialt laialt ega ole üheselt piiritletavad. Muutmist võivad vajada ka teised karistusregistri sätted.

Karistusregistriga seonduvaid küsimusi lahendatakse eraldi KarRS ülevaatamise raames. Vastav analüüs on hetkel koostamisel ning lähiajal koostatakse analüüsi pinnalt väljatöötamiskavatsus.

Võimalikud muudatused riiklikes registrites

Mistahes e-lahenduse väljatöötamisel, e-teenuse pakkumisel või õigusliku regulatsiooni kehtestamisel tuleb tagada praegu ja ka tulevikus kooskõla andmekaitse reeglitega. Andmekaitsereformi valguses on sealjuures vajalik hinnata, kas ning mil määral on vajalik muuta isikuandmete töötlemist ja selle ulatust riiklikes registrites nagu näiteks karistusregister, äriregister, kinnistusraamat, abieluvararegister ja pärimisregister. Üldmääruse rakendamisel võib osutuda vajalikuks registritest andmete kättesaadavust piirata ning kehtestada täiendavalt kaitsemeetmeid, et riivet õigustada ja tagada riive proportsionaalsus. Selleks on olemas erinevaid võimalusi, näiteks võrreldes praegusega suuremate tasumäärade kehtestamine ja masspäringute piiramine. Vajalik on hinnata ja sisustada ka kõikide täna kogutavate ja avalikustatavate andmete vajalikkus ning välja selgitada, kas kõikide tänaste andmete avalikustamine ja selle viis on ka edaspidi eesmärgipärane ja kooskõlas EL andmekaitsenõuetega.

Näiteks väärib kaalumist päringute tegemise korra muutmine kinnistusraamatus, kus praegu on võimalik otsida isiku nime järgi andmesubjektile kuuluvat kinnisvara ning seeläbi on väga lihtsalt ja kiirelt võimalik saada terviklik ülevaade isikule kuuluvatest kinnistutest (kinnistusraamatuseaduse § 74). Selline isiku nime järgi kinnistute otsimine kinnistusraamatust on aga tõenäoliselt ebaproportsionaalsem kui alternatiiv, kus kinnistusraamatu andmeid oleks võimalik pärida kinnistu aadressi alusel. Kaaluda võiks päringute tegemise korra muutmist kinnistusraamatus nii, et üldsusele kaoks ära võimalus teostada päringuid nime järgi ning jääks alles võimalus teostada päringuid aadressi järgi. Antud muudatuse jõustamiseks oleks vajalik kinnistusraamatuseaduse § 74 muutmine ning lisaks ka infotehnoogilised muudatused e-kinnistusraamatus.

Abieluvararegistri puhul vajab senine avatus ülekaalumist ja pigem kitsendamist, kuivõrd abieluvararegistrile juurdepääsu ulatus pärineb paberkataloogi ajast. Veebipõhise juurdepääsu ja masinloetava allalaetavuse ajastul peaks seda piirama.[47]

Üldises plaanis püütakse isikuandmete reformi raames säilitada Eestile omane avaliku sektori kättesaadavus ja andmekogude ristkasutus läbi X-tee, sh *once-only* põhimõte ehk andmete ühekordse küsimise põhimõte.

Mõju riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele, kuludele ja tuludele

Sihtrühm 1: andmekogude (registrite) vastutavad ja volitatud töötlejad
Sihtrühm 2: andmesubjektid
Sihtrühm 3: avalikke andmeid kasutavad era- ja juriidilised isikud

Praegu veel puudub täpne ülevaade, kui paljudes andmekogudes[48] tuleb uue andmekaitse üldmääruse valguses isikuandmete töötlemist ja andmete avalikustamist piirata. RIHA andmetel on riigi ja kohalike omavalitsuste valitsemisalas kasutusel 245 infosüsteemi, kus

[47] Vt selle kohta ka Andmekaitse Inspektsiooni peadirektori ülevaade, lk 5: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ylevaade_reformist_14102016.pdf.

[48] Andmekogu on riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks (AvTS § 43^1).

töödeldakse isikuandmeid, sh 70 sellist, kus töödeldakse delikaatseid isikuandmeid[49]. Tõenäoliselt puudutavad muudatused neist siiski vaid väikest osa.

Andmekogude muutmisega võib kaasneda täiendav kulu andmekogude vastutavatele töötlejatele, kes peavad tagama vajalikud infotehnoloogilised muudatused. Mõju on siiski väikse ulatusega ja harv (ühekordne). Vähesel määral on mõjutatud ka era- ja juriidilised isikud, kes soovivad avalikke andmeid kasutada (nt kinnisvarabürood), kuid tuleb rõhutada, et iga muudatuse puhul kaalutakse selle proportsionaalsust nii andmesubjektide kui kasutajate seisukohast.
Kaasnevaid mõjusid on võimalik täpsemalt kirjeldada siis, kui on teada, milliseid andmekogusid ning millises ulatuses on tarvis muuta. Arvestades mõjude eelduslikult väikest ulatust ja harva esinemissagedust, on mõju sihtrühmadele tervikuna väheoluline.

5.11. Loakohustus sotsiaalkaitse ja rahvatervise valdkonnas ning teistes reguleeritud valdkondades[50]

Üldmääruse art 36 lg 5 ja art 58 lg 3 p c näevad ette võimaluse liikmesriigi õigusega näha ette, et vastutavad töötlejad peavad konsulteerima järelevalveasutusega (AKI) ja saama neilt eelneva loa, kui vastutav töötleja kavatseb töödelda isikuandmeid vastutava töötleja poolt avalikes huvides täidetava ülesande raames, mis hõlmab sellist isikuandmete töötlemist seoses sotsiaalkaitse ja rahvatervisega.

Majandustegevuse seadustiku üldosa seaduse (edaspidi *MsÜS*) § 16 lg 1 kohaselt peab seaduses sätestatud juhul ettevõtjal enne tegevusalal majandustegevuse alustamist olema tegevusluba. Praegu eesti õiguses kehtiva regulatsiooni kohaselt peavad kõik tervishoiuteenuste osutajad saama tegevusloa Terviseametist, Sotsiaalkindlustusametist (sotsiaalteenuse osutajad) või maavalitsustelt (seoses haldusreformiga maavalitsuste kaotamisega tegevusloa väljastamise kord muutub, tulevikus on see tõenäoliselt kohaliku omavalitsuse pädevuses). Nii justiitsministeerium kui ka AKI on seisukohal, et kahekordne loakohustus oleks ülemäärane halduskoormus teenuseosutajatele ning ebamõistlik ressursikasutus järelevalveasutusele, mistõttu pole täiendava loakohustuse kehtestamine mõistlik ega vajalik. Kõige optimaalsemaks lahenduseks võiks olla see, kui tervishoiu- ja hoolekande alal olemasolev valdkondlik loamenetlus hõlmaks ka infoturvet ja andmekaitset, et vältida halduskoormuse suurenemist. Antud lahendusega tagataks see, et isikuandmete töötlemine oleks nõuetega vastavuses, samas täiendavaid kohustusi üldmääruse art 36 lg 5 alusel ei kehtestataks.

Tegevusloa saamise kohustuse sidumine andmekaitse nõuete järgimisega on mõeldav ka teistes valdkondades peale sotsiaalkaitse ja rahvatervise valdkonna. Isikuandmete töötlemise ja turvalise hoidmise reeglistikul on kokkupuude rahandusettevõtete (pangandus, muu krediiditurg, kindlustus, väärtpaberiturg) tegevusega.

5.12. Andmekaitse Inspektsioon kui andmekaitse järelevalveasutus

[49] Andmed sisaldavad ka osade infosüsteemide alamsüsteeme, mistõttu on tegemist ligikaudse arvuga. Info on leitav: https://riha.eesti.ee/riha/main#1486469103164e4ExlFEzN5GkhIq (07.02.2017).
[50] Vt selle kohta ka Andmekaitse Inspektsiooni peadirektori ülevaade, lk 6: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ylevaade_reformist_14102016.pdf.

Üldmääruse VI peatükk sätestab sõltumatute järelevalveasutuste regulatsiooni. Seega asendab üldmääruse VI peatükk tulevikus IKSi praeguse 6. peatüki. Üldmääruse valguses vajab muutmist ka justiitsministri 14.02.2007 määrus nr 10 „Andmekaitse Inspektsiooni põhimäärus ja koosseis".

Üldmääruse art 51 lg 1 kohaselt näeb liikmesriik ette ühe või mitu sõltumatut riigiasutust (järelevalveasutus), kes vastutavad üldmääruse kohaldamise järelevalve eest. Eestis on andmekaitse nõuete täitmise üle järelevalvet teostanud alates 1999. aastast Andmekaitse Inspektsioon ning seetõttu on kavandatud ka üldmääruse valguses nende ülesannete delegeerimine just Andmekaitse Inspektsioonile. Andmekaitse Inspektsiooni kõrvale täiendava(te) riigiasutuste loomist Eesti väiksust arvestades ei kavandata, mistõttu puudub vajadus ka üldmääruse art 51 lg-s 3 toodud juhtiva järelevalveasutuse määramiseks.

Üldmääruse art 53 lg-st 1 tulenevalt peavad liikmesriigid tagama, et nende järelevalveasutuse liikme (Eesti kontekstis AKI peadirektori) peab läbipaistva menetluse teel ametisse nimetama kas liikmesriigi parlament, valitsus, riigipea või sõltumatu asutus. Selles küsimuses ei ole Justiitsministeeriumi hinnangul muudatuste tegemine võrreldes *status quo*ga vajalik ning ka tulevikku on kavandatud regulatsioon, kus Andmekaitse Inspektsiooni peadirektori määrab justiitsministri ettepanekul viieks aastaks ametisse Vabariigi Valitsus, kuulates ära Riigikogu põhiseaduskomisjoni arvamuse.

Üldmääruse art 54 kohaselt tuleb kavandatavas üldmääruse rakendusseaduses sätestada:

a) järelevalveasutuse asutamine;
b) järelevalveasutuse peadirektori ametisse nimetamiseks nõutav kvalifikatsioon ja tingimused;
c) eeskirjad ja menetlused järelevalveasutuse peadirektori ametisse nimetamiseks;
d) järelevalveasutuse peadirektori vähemalt nelja aasta pikkune ametiaeg, välja arvatud pärast 24. maid 2016 esimest korda ametisse nimetamisel, mil osa liikmete ametiaeg võib olla lühem, kui see on vajalik, et kaitsta järkjärgulise ametisse nimetamise abil järelevalveasutuse sõltumatust;
e) see, kas ja kui mitmeks ametiajaks saab järelevalveasutuse peadirektori ametisse tagasi nimetada, ning
f) tingimused, mis reguleerivad järelevalveasutuse peadirektori ja töötajate kohustusi, nende kohustustega kokkusobimatuid tegevusi, tegevusalasid ja hüvesid ametiajal ja pärast selle lõppu ning töösuhte lõppu käsitlevad normid.

Eeltoodud nõuete täitmiseks on kavandatavas IKS terviktekstis planeeritud luua alus järelevalveasutuse asutamiseks (AKI), säilitada IKS §-des 34–36 toodud sätted ning kehtestada tingimused, mis reguleerivad järelevalveasutuse peadirektori ja töötajate kohustusi jms.

IKS §-s 33 toodud Andmekaitse Inspektsiooni ülesanded on üldmääruse kohaldamisel asendatud üldmääruse art-ga 57.

Üldmääruse rakendusseaduse eelnõusse kavandatakse ka säte, millega oleks täidetud üldmääruse art 58 lg-st 5 tulenev nõue: „*Liikmesriik näeb seadusega ette, et tema järelevalveasutusel on õigus juhtida õigusasutuste tähelepanu käesoleva määruse rikkumistele ning alustada vajaduse korral kohtumenetlus või osaleda selles muul viisil, et tagada käesoleva määruse sätete täitmine.*".

Üldmääruse art 58 lg-st 6 tulenevalt võib liikmesriik seadusega ette näha ka selle, et tema järelevalveasutusel on täiendavad volitused lisaks lõigetes 1, 2 ja 3[51] osutatud volitustele. Järelevalveasutuste volituste kohta on pikemalt kirjutatud käesoleva kontseptsiooni trahve puudutavas osas ning muus osas järelevalveasutusele täiendavaid volitusi kavandatud ei ole.

Andmekaitse Inspektsiooni puudutava regulatsiooni osas tehakse koostööd Andmekaitse Inspektsiooniga ning arvestatakse Andmekaitse Inspektsiooni peadirektori ülevaate ja soovitustega[52] EL andmekaitsereformi rakendamise kohta nii palju kui võimalik.

6. Õiguskaitsevaldkonna direktiivi ülevõtmisega kaasnevad peamised muudatused

Õiguskaitsevaldkonna direktiivi ülevõtmiseks koostatavate sätete väljatöötamisel tuleb täies ulatuses lähtuda direktiivi sätetest ning arvestada teatud ulatuses ka üldmäärusest tuleneva regulatsiooniga. Direktiivi ülevõtmisel tuleb erilist tähelepanu pöörata järgmistele aspektidele:

a) Direktiivi kohaldamisala selge piiritlemine, sh pädevate asutuste ja direktiiviga hõlmatud ülesannete defineerimine (vt kontseptsiooni p 3).
b) Andmetöötluse üldpõhimõtete ülevõtmine. Kuigi andmetöötluse üldpõhimõtted direktiivi art-s 4 ning üldmääruse art-s 5 on üsna sarnased, sätestab direktiiv nõudeid mõnevõrra pehmemalt, võttes arvesse valdkonna eripära. Seega ei piisa regulatsiooni loomisel viitest üldmääruse tekstile, vaid direktiivi ülevõtvas seaduses tuleb kehtestada andmetöötluse põhimõtted, mis rakenduvad seadusega hõlmatud töötlemisele. Seejuures kuigi põhimõtted on sarnased hetkel IKS §-s 6 sätestatuga, tuleb näha ette ka selliseid kriteeriume, mis ei ole hetkel Eesti õiguses sõnaselgelt sätestatud. Eelkõige tuleb üheselt kehtestada kindla säilitamisperioodi sätestamise nõue ning keeld teatud hetkest alates säilitada isikuandmeid isikustatud kujul juhul, kui see ei ole eesmärgist tulenevalt enam vajalik (direktiivi art 4 lg 1 p e, art 5).
c) Erinevate andmesubjektide kategooriate eristamine (art 6). Direktiiv kehtestab nõude, mille kohaselt peab isikuandmete töötlemisel niipalju kui võimalik eristama erinevaid andmesubjektide kategooriaid. Kehtivas Eesti õiguses ei ole kehtestatud nõuet eristada andmesubjektide kategooriaid ning praktikas ei pruugi selline eristamine alati olla võimalik. Siiski tuleb näha ette töötleja kohustus võtta tarvitusele meetmed, mis võimaldavad eristamist niipalju kui võimalik. Näiteks tuleb erinevates andmetöötlustoimikutes ning registrites selgelt märkida, millise rolliga andmesubjekt menetluses on. Samuti tuleb kaaluda võimalust kehtestada erinevad andmetöötluse tingimused (nt säilitamistähtaeg, isikustatud kujul säilitamise kestus) erinevate andmesubjektide kategooriate lõikes.
d) Tingimused isikuandmete töötlemise lubatavuse tagamiseks muudel eesmärkidel kui need eesmärgid, mille jaoks andmeid koguti (art 9). Hetkel ei ole Eesti õiguses vastavat normi üheselt kehtestatud.
e) Andmesubjekti õiguste kataloog ning õiguste teostamise tingimused sätestatakse kehtiva korraga võrreldes täpsemalt, mis võimaldab andmesubjekti tõhusama õiguste kaitse ning loob selguse selles osas, millal ja kuidas on andmesubjektil võimalik oma õigusi teostada näiteks kriminaalmenetluses või politseiasutuse poolt isikuandmete töötlemisel. Vajadusele senisest täpsemalt reguleerida kriminaalmenetluses nii

[51] ELT-s avaldatud üldmääruse tekstis ekslikult „lõigetes 1, 1b ja 1c“, vastav info Euroopa Nõukogusse edastatud.
[52] http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ylevaade_reformist_14102016.pdf

andmekaitsereegleid laiemalt kui konkreetselt andmesubjekti õigustega seonduvat on rõhutanud ka Riigikohus oma otsuses 3-3-1-84-15.

f) Direktiivist tulenevalt tuleb senisest oluliselt detailsemalt sätestada isikuandmete töötlejate (sh nii vastutavate kui volitatud töötlejate) kohustused. Eraldi ära märkimist väärib direktiivi artiklis 27 ja põhjenduspunktis 58 sätestatud kohustus teostada andmekaitsealane mõjuanalüüs. Seejuures võib tõusetuda küsimus, kas mõjuanalüüs tuleb täiendavalt teostada ka sellisele töötlemisele, sh infosüsteemidele, mida rakendatakse kuni direktiivi ülevõtmistähtaja saabumiseni. Direktiivi põhjenduspunkt 96 täpsustab, et liikmesriigid peavad viima andmetöötluse kooskõlla direktiivi sätetega, kuid seejuures tuleb arvestada, et selliste kohustuste täitmine, mis puudutab eelnevat konsulteerimist järelevalveasutusega, ei ole nõutav, kui andmetöötlus on õiguspärane ning kooskõlas kuni direktiivi jõustumiseni kehtinud õigusnormidega. Ühtlasi näeb üldmääruse art 35 lg 10 ette, et juhul, kui mõjuanalüüsi sarnane analüüs on riigisisesest õigusest tulenevalt juba läbi viidud, ei pea uuesti mõjuanalüüsi teostama. Eeltoodust tulenevalt on Justiitsministeerium seisukohal, et juba kasutuses olevatele infosüsteemidele ei ole tarvis eraldi art 27 sätestatud uue mõjuanalüüsi läbiviimine. Samale tõlgendusele on viidanud ka Euroopa Komisjon.

g) Andmekaitseametniku määramise kohustus (direktiivi art 32-34). Direktiivi kohaldamisalasse jäävad asutused peavad määrama andmekaitseametnikku. Vastav kohustus on kooskõlas ka üldmääruse art 37 lg 1 p-ga a, kuivõrd kõik direktiivi mõistes pädevad asutused on alati ka Eesti õiguse mõistes avaliku sektori asutused. Andmekaitseametniku kontseptsiooni kohta vt p 2. Andmekaitseametniku positsiooni loomine pädevatesse asutustesse toob paratamatult kaasa täiendava ressursikulu, kuivõrd andmekaitseametniku määramine võib nõuda uue ametikoha loomist. Siiski tuleb märkida, et mitmes asutuses on juba määratud isikuandmete töötlemise eest vastutav isik IKS § 30 alusel. Ühtlasi võimaldab direktiivi art 32 lg 3 määrata ühe andmekaitseametniku mitmesse asutusse. Sellist lahendust oleks otstarbekas kasutada olukordades, kus tegemist on sama haldusala asutustega, aga ka muudel juhtudel, kus ühise andmekaitseametniku määramine ei avaldaks negatiivset mõju andmekaitseametniku ülesannete täitmise tõhususele.

h) Direktiivi art 35-40 sätestavad piiriülese andmevahetuse reeglid. Kuivõrd EL on kõrge andmekaitsetasemega piirkond, rakendatakse isikuandmete edastamisel väljapoole EL-i eritingimusi, mille eesmärgiks on tagada isikuandmete kaitse ning andmesubjekti õiguste tõhus rakendamine. Praegusel ajal on isikuandmete edastamine väljapoole EL-i reguleeritud näiteks IKS §-s 18, aga ka KrMS §-dega 489^3 - 489^5, politsei ja piirivalve seaduse §-s 7^{46}. Uue tervikseaduse kehtestamisel koondatakse kõik isikuandmete väljapoole EL-i edastamist reguleerivad sätted ühtseks regulatsiooniks. Kuigi isikuandmete edastamine väljapoole EL-i peab direktiivi kohaselt olema selgelt reguleeritud ning piiritletud, ei kitsenda see Justiitsministeeriumi hinnangul oluliselt andmevahetust väljaspool EL-i asuvate riikidega, kuivõrd direktiivis ette nähtud alused andmete vahetamiseks on piisavad ning võimaldavad pädevatel asutustel andmeid edastada, kui see on läbiviidava menetluse seisukohalt oluline;

i) Direktiivi artiklid 41-51 sätestavad liikmesriigi kohustuse luua sõltumatu andmekaitse järelevalveasutus ning anda järelvalveasutusele asjakohased volitused ning pädevused andmetöötluse üle kontrolli teostamiseks ning andmekaitsenormide jõustamiseks. Eestis on andmekaitse järelevalveasutuseks Andmekaitse Inspektsioon, mis on sõltumatu järelevalveasutus IKS § 32 kohaselt (vt kontseptsiooni p 5.13.) ning millel on hetkel kehtivas Eesti õiguses üldjuhul olemas vajalikud järelevalvevolitused ka direktiivi kohaldamisalasse jäävate asutuste osas. Direktiivi ülevõtmiseks koostatavas

seaduses ei ole otstarbekas sätteid üle korrata, Justiitsministeeriumi hinnangul piisab viitest üldmääruse rakendusseadusele.

j) Direktiivi art 57 kohaselt peab liikmesriik nägema ette karistused, jõustamaks andmekaitsereeglite täitmist. Karistused peavad olema tõhusad, proportsionaalsed ning hoiatavad. Erinevalt üldmäärusest ei näe direktiiv ette karistuste vormi ega summasid. Arvestades, et Eestis ei kohaldata avaliku sektori asutustele väärteotrahve ning ka haldussunni rakendamine riigiasutusele ei ole võimalik (ATSS § 5 lg 1), tõusetub paratamatult küsimus selle kohta, kuidas saavutada Eesti õiguses direktiivi art 57 nõuetekohane rakendamine. Sarnane regulatsioon on ka üldmääruse artikli 84, mille lg 1 sätestab karistuste kehtestamise kohustuse, sh nende subjektide osas, kelle suhtes ei kohaldata haldustrahve art 83 kohaselt. Hetkel kehtiv IKS regulatsioon näeb ette sunniraha määramist juhul, kui AKI ettekirjutust ei täideta (IKS § 40 lg 2), kuid seejuures on täpsustatud, et riigiasutustele sunniraha ei kohaldata. IKS § 40 lg 4 võimaldab AKI-l pöörduda protestiga halduskohtusse, kui riigiasutus ei ole täitnud AKi ettekirjutust. Konkreetse üksikisiku suhtes, kes rikkus teenistuskohustuste raames töötlemise reegleid, saab läbi viia distsiplinaarmenetluse. Siiski on Justiitsministeeriumi hinnangul kaheldav, kas hetkel olemasolevad mehhanismid on piisavad selleks, et tagada direktiivi sätete nõuetekohast jõustamist art 57 tähenduses. Kõnealune küsimus haakub laiema teemaga haldusjärelevalve meetmetest ning Justiitsministeerium analüüsib neid aspekte eraldi horisontaalselt.

Täitmaks direktiivi (ning ka üldmääruse) nõuded täpselt ettekirjutatud kujul, tuleks Eesti õiguses luua eraldi jõustamismehhanismid avaliku sektori asutuste jaoks. Kaaluda võib muuhulgas, kas:

- laiendada direktiivi mõistes pädevatele asutustele ning laiemalt avaliku sektori asutustele karistusõiguslike mõjutusvahendite (eelkõige väärteotrahv) kohaldamist või
- laiendada ATSS alusel haldussunni kohaldamise võimalust pädevate asutuste suhtes.

Kuigi lisaks sanktsioneerivale reaktsioonile peab järelevalveasutusel olema ka teisi parandusvolitusi (nt nõuda töötlemise kooskõlla viimist, peatada töötlemine jt), on vajalik ka täiendav jõustamismehhanism juhul, kui parandusvolitused ei anna tulemust. Normide jõustamine on andmekaitsereformi üks põhielemente, mistõttu tuleb luua Eesti õigusruumis sobiv lahendus reeglite jõustamiseks avaliku sektori asutuste suhtes.

k) Direktiivi art 61 sätestab, et liikmesriikide poolt kuni 6. maini 2016.a sõlmitud rahvusvahelised lepingud jäävad jõusse, kuni neid muudetakse, asendatakse või tühistatakse juhul, kui sellised lepingud on kooskõlas sõlmimisel hetkel kehtinud õigusega. Tegemist on ülimalt olulise sättega, mis võimaldab liikmesriikidel jätta jõusse kahe- või mitmepoolsed lepingud, mis on sõlmitud direktiivi vastuvõtmise kuupäevani.

Mõju riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele, kuludele ja tuludele

Sihtrühm: pädevad asutused (direktiivi art 3 p 7 mõistes), mis tegelevad süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise või kriminaalkaristuse täitmisele pööramisega, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamisega.

Eestis tegelevad süütegude (väärtegude või kuritegude) menetlemise ja karistuse täitmisele pööramisega järgnevad asutused:

- Andmekaitse Inspektsioon
- Finantsinspektsioon
- I ja II astme kohtud
- Justiitsministeerium
- Kaitsepolitseiamet
- Kaitseressursside Amet
- Kaitseväg
- Keeleinspektsioon
- Keskkonnainspektsioon
- kohalikud omavalitsused
- Konkurentsiamet
- Lennuamet
- Maanteeamet
- Maksu- ja Tolliamet
- Muinsuskaitseamet
- Politsei- ja Piirivalveamet
- Põllumajandusamet
- Päästeamet
- Rahandusministeerium
- Ravimiamet
- Riigikohus
- Tarbijakaitseamet
- Tehnilise Järelevalve Amet
- Terviseamet
- Tööinspektsioon
- vanglad ja kriminaalhooldusosakonnad
- Veeteede Amet
- Veterinaar- ja Toiduamet

Direktiivi kohaldamise tulemusel muutub süütegudega seotud isikuandmete töötlemine senisest mõnevõrra rangemaks. Muu hulgas kehtestatakse tähtajad isikuandmete kustutamiseks (või säilitamise vajaduse läbivaatamiseks), piiratakse tuvastamist võimaldavate andmete säilitamist, hakatakse eristama andmesubjektide kategooriaid (kahtlustatavad, süüdimõistetud, ohvrid, muud seotud isikud), senisest täpsemalt sõnastatakse andmesubjekti õigused (teavitamine, õigus tutvuda isikuandmetega jm) ja töötlejate kohustused (andmekaitseline mõjuhinnang, toimingute dokumenteerimine, andmekaitseametniku määramise kohustus jm). Kuivõrd süütegudega seotud isikuandmete töötlemine toimub suures osas elektrooniliselt, siis tuleb direktiivi ülevõtmise käigus erilist tähelepanu pöörata infotehnoloogilistele lahendustele, mistap võivad ajutiselt kasvada asutuste kulud infotehnoloogia tugiteenustele.

Mõnevõrra suurem kaalutlusruum on liikmesriikidel karistusnormide kehtestamisel, mida kohaldatakse direktiivi sätete rikkumise korral (direktiivi art 57). Nagu eespool selgitatud, siis Eestis on kaalumisel kaks varianti: karistusõiguslikud mõjutusvahendid (väärteotrahv) või haldussund (reguleerib ATSS). Tegemist on kahe õigusliku alternatiivi vahel valimisega, mille mõjud on sihtrühmale sisuliselt sarnased – karistused peavad lõpptulemusena olema tõhusad, proportsionaalsed ja heidutavad.

Direktiivi ülevõtmisega kaasneb sihtrühmale peamiselt töökorralduslikku laadi mõju, rahaline kulu võib kaasneda infotehnoloogiliste lahenduste väljatöötamisega, andmekaitseametniku regulatsiooniga (sh koolituskulud, atesteerimine), töötajate andmekaitsealase koolitamisega ning harvadel juhtudel ka karistuse rakendamisega.

Sotsiaalne mõju

Sihtrühm: andmesubjektid. 2016. aastal registreeriti Eestis 197 134 süütegu, sh 28 986 kuritegu ja 168 148 väärtegu[53]. Rõhutame, et üks isik võib olla toime pannud mitmeid süütegusid, samuti ei õnnestu alati süüteo toimepanijat tuvastada, lisaks töötlevad pädevad asutused ka ohvrite, tunnistajate ja teiste menetlusega seotud isikute isikuandmeid.

[53] Justiitsministeeriumi andmed 2016. aastal registreeritud kuritegude kohta (http://www.just.ee/et/uudised/2016-aasta-kriminaalstatistika-pohjal-uldine-kuritegevus-ja-tapmiste-arv-vahenenud, 13.02.2017) ja õiguskaitse valdkonna statistikakeskkonna andmed väärtegude kohta seisuga 20.01.2017.

Andmesubjektide jaoks suureneb kindlus, et nende isikuandmeid töödeldakse süüteomenetluses eesmärgipäraselt, ning senisest detailsemalt sätestatakse andmesubjektide andmekaitsealased õigused. Sihtrühma jaoks on tegemist positiivse, kuid üldjuhul väheulatusliku ja harva avalduva mõjuga.

7. Edasine tegevuskava ja kaasamine

Valitud lahendus

Üldmääruse rakendamiseks töötatakse välja uus tervikseadus.
Direktiivi sätete ülevõtmiseks sobiva lahenduse osas ei ole Justiitsministeeriumi hetkel veel otsust langetanud ning kaalumisel on kolm alternatiivi:

- direktiivi sätete paigutamine olemasolevatesse valdkonda reguleerivatesse õigusaktidesse (nt kriminaalmenetluse seadustik, väärteomenetluse seadustik, korrakaitseseadus, politsei ja piirivalve seadus, vangistusseadus jt);
- uue eraldi seaduse väljatöötamine, milles koondatakse direktiivi ülevõtmiseks vajalikud sätted üheks õigusaktiks;
- ühtne seadus nii määruse rakendamiseks kui ka direktiivi sätete ülevõtmiseks, mis muuhulgas käsitleks ka nende kahe õigusakti reguleerimisalast välja jäävad küsimusi.

Eeldatav seaduseelnõu mõjude analüüsi läbiviimise aeg

Täiendav mõjuanalüüs ei ole vajalik. Sätete mõju analüüsitakse vajadusel eelnõu seletuskirjas.

Eeldatav eelnõu kooskõlastamisele saatmise aeg

Suvi 2017

Eeldatav seaduseelnõu Vabariigi Valitsusele esitamise aeg

Sügis 2017

Õigusakti jõustumise aeg

Üldmääruse rakendusseaduse jõustumine – 25.05.2018, kui jõustub ka EL isikuandmete kaitse üldmäärus 2016/679.
Direktiivi üle võtva seaduse jõustumine on kavandatud hiljemalt 6.maiks 2018.a.

Kaasatavad valitsusasutused ja valitsusvälised organisatsioonid

Rahandusministeerium, Kaitseministeerium, Keskkonnaministeerium, Kultuuriministeerium, Maaeluministeerium, Majandus- ja Kommunikatsiooniministeerium, Siseministeerium, Haridus- ja Teadusministeerium, Välisministeerium, Õiguskantsleri Kantselei, Riigikohus, Andmekaitse Inspektsioon, Tarbijakaitseamet, Eesti Linnade Liit, Eesti Maaomavalitsuste Liit, MTÜ Lastekaitse Liit, SA Kutsekoda, Pangaliit, Tartu Ülikooli õigusteaduskond, Tallinna Tehnikaülikooli õiguse instituut, Tallinna Ülikooli õigusakadeemia, Eesti Infotehnoloogia ja Telekommunikatsiooni Liit, Eesti E-Kaubanduse Liit, Eesti Haiglate Liit, Eesti Kaupmeeste Liit, Eesti Kindlustusseltside Liit, Eesti Turvaettevõtete Liit.

Vastutavate ametnike nimed ja kontaktandmed

1) Julia Antonova, nõunik justiitsküsimustes EV alalises esinduses ELi juures, +32 2227 3916, julia.antonova@mfa.ee;
2) Kärt Salumaa, õiguspoliitika osakonna avaliku õiguste talituse nõunik, 620 8245, kart.salumaa@just.ee.