

TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Riigi- ja haldusõiguse õppetool

Sandra Sillaots

**ISIKUANDMETE KAITSE REGULATSIOONI ÜHTLUSTAMINE ISIKUANDMETE
KAITSE ÜLDMÄÄRUSE EELNÕUS JA SELLE MÕJU EESTILE**

Magistritöö

Juhendaja

Professor Kalle Merusk

Tartu

2014

SISUKORD

SISSEJUHATUS	4
1. ISIKUANDMETE KAITSE KEHTIV REGULATSIOON	9
1.1 Informatsioon ja infoühiskond.....	9
1.2 Isikuandmete kaitse reguleerimisel kaitstavad põhiõigused	10
1.3 Isikuandmete kaitse institutsionaalsed lähtekohad	12
1.3.1 Rahvusvaheline õigus	13
1.3.1.1 Euroopa inimõiguste ja põhivabaduste kaitse konventsioon	13
1.3.1.2 Majandusliku Koostöö ja Arengu Organisatsiooni 23.09.1980 juhend eraelu kaitsest ja piirülesest isikuandmete kaitsest.....	15
1.3.1.3 Euroopa Nõukogu 1981 aasta isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon	16
1.3.2 Euroopa Liidu õigus	17
1.3.2.1 Euroopa Ühenduse direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta	17
1.3.2.2 Euroopa Liidu põhiõiguste harta.....	20
1.3.3 Eesti õigus	21
1.3.3.1 Eesti Vabariigi põhiseadus.....	22
1.3.3.2 Isikuandmete kaitse seadus	23
1.4 Vahekokkuvõte.....	25
2. ISIKUANDMETE KAITSE ÜLDMÄÄRUSE PEAMISED EESMÄRGID.....	26
2.1 Isikuandmete kaitse regulatsiooni reform.....	26
2.2 Vajadus tugevdada andmesubjektide õiguste kaitset.....	28
2.2.1 Läbipaistvuse puudumine isikuandmete töötlemisel.....	29
2.2.1.1 Läbipaistvusprintsip	30
2.2.1.1 Vastutava ja volitatud töötleva vaheliste kohustuste täpsustamine.....	33
2.2.2 Andmesubjekti kontrolli tõhustamine enda isikuandmete üle.....	35
2.2.2.1 Õigus olla unustatud ja õigus andmete kustutamisele	36

2.2.2.2 Isikuandmete ülekantavus.....	41
2.3 Vajadus tagada paremad tingimused Euroopa Liidu siseturu toimimiseks	44
2.3.1 Õiguskindluse suurendamine.....	45
2.3.1.1 Otsekohalduva mõjuga õigusinstrument	45
2.3.2 Vajadus vähendada ettevõtete halduskoormust.....	48
2.3.2.1 Kulude vähendamine	49
2.3.2.2 Mikro-, väikese ja keskmise suurusega ettevõtetele erandite kohaldamine ..	50
2.4 Vahekokkuvõte.....	52
3. JÄRELEVALVE REGULATSIOON ISIKUANDMETE KAITSE ÜLDMÄÄRUSES	54
3.2 Järelevalveasutuste sõltumatus.....	55
3.2.1 Järelevalveasutuste ressursipuudus ja majanduslik sõltumatus.....	56
3.2.2 Järelevalveasutuste institutsionaalne sõltumatus.....	58
3.3 Järelevalveasutuste volitused.....	60
3.3.1 Uurimisvolitused	61
3.3.2 Sekkumisvolitused.....	61
3.3.3 Halduskaristused.....	63
3.3.4 Esindamisvolitused.....	66
3.4 Liikmesriikide järelevalveasutuste rahvusvaheline koostöö	68
3.4.1 Euroopa Andmekaitsekoogu.....	69
3.4.2 <i>One-stop shop</i> printsiip.....	70
3.4.3 Järjepidevusprintsiip.....	73
3.5 Vahekokkuvõte.....	75
KOKKUVÕTE	78
Harmonizing personal data protection regulation in the General Data Protection Regulation draft and its impacts on Estonia. Summary	83
KASUTATUD MATERJALID.....	90

SISSEJUHATUS

Euroopa Liidu liikmesriigid on jõudnud infoühiskonda – informatsioon on saanud oluliseks käibeobjektiks, aga ka kultuuriväärtuseks ja hüveks.¹ Informatsiooni saamiseks, säilitamiseks ja vahetamiseks arendatakse pidevalt uusi tehnoloogiaid ning enamus infotööstusest ei toimu enam mitte füüsiliselt määratletavates kohtades, vaid internetis kui suures „pilves“.²

Konkreetne info ehk andmed tähendab, et teave käib kellegi või millegi kohta.³ Kellegi kohta käivad andmed on isikuandmed.⁴ Õigusaktidega on kaitstav selline informatsioon, mille abil on võimalik tuvastada konkreetne isik.⁵ Arusaam sellest, mille abil on konkreetset isikut võimalik tuvastada, on ajapikku muutunud ja hägustunud.⁶ Isik on tuvastatav tema nime, isikukoodi ja telefoninumbri abil, aga ka tema arvuti IP aadressi⁷ ja hobisid ning töötingimusi puudutava informatsiooni abil.⁸

Interneti üha laialdasema leviku tõttu on andmekaitse muutunud siseriiklikust probleemist üheks Euroopa Liidu peamiseks eesmärgiks. Tehnoloogia ja andmetööstlusvahendite areng on toonud kaasa mitmeid probleeme, mis on tinginud vajaduse isikute kaitsmiseks just üle-euroopalisel tasemel.⁹ Õigus isikuandmete kaitsele on Euroopa Liidu tasandil sätestatud Euroopa Liidu põhiõiguste harta¹⁰ artiklis 8, kuid juba enne Euroopa Liidu põhiõiguste harta koostamist oli õigus isikuandmete kaitsele tuletatav Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklist 8.¹¹ Euroopa Liidu õiguses reguleerib isikuandmete töötlemist eelkõige Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (edaspidi direktiiv).¹²

¹ E. Tikk, A. Nõmper. Informatsioon ja õigus. Tallinn: Juura 2007, lk 14.

² P. De Filippi, S. McCarthy. Cloud Computing: Centralization and Data Sovereignty. - European Journal for Law and Technology. 2012/3, No. 2, p 2.

³ T. Erelt jt (koost). Eesti õigekeelsussõnaraamat ÕS 2006. Tallinn: Eesti Keele Sihtasutus 2006, lk 64.

⁴ M. Männiko. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011, lk 42.

⁵ *Ibid.*

⁶ W. B. Baker, A. Matyjaszewski. The changing meaning of personal data. Available: https://www.privacyassociation.org/resource_center/the_changing_meaning_of_personal_data, 23.04.2014.

⁷ Euroopa Kohus on võtnud seisukoha, et IP aadressid võimaldavad nende kasutajad täpselt tuvastada ja on seetõttu käsitatavad isikuandmetena, samas on selline lähenemine fikseeritud ainult väga väheste liikmesriikide siseriiklikus õiguses. Vt: EK 24.11.2011, C-70/10, *Scarlet Extended SA vs SABAM*, § 51.

⁸ EKO 06.11.2003, C-101/01, *Lindqvist*, § 24.

⁹ L. Danagher. An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data? - European Journal of Law and Technology 2012/3, No. 3, p 2.

¹⁰ Euroopa Liidu põhiõiguste harta. - ELT C 83, 30.03.2010, p 392 - 403.

¹¹ Inimõiguste ja põhivabaduste kaitse konventsioon (jõustunud 4. novembril 1950). - RT II 2010, 14, 54.

¹² Euroopa Parlamendi ja nõukogu 24.10.1995.a direktiiv üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. - ELT L 281, 23.11.1995, lk 31 - 50.

Eesti Vabariigi põhiseadus (edaspidi PS) eraldi õigust isikuandmete kaitsele ei sätesta, kuid see on tuletatav PS §-dest 19 ja 26.¹³ Esimene isikuandmete kaitse seadus (edaspidi IKS) kehtestati Eestis 1996.a,¹⁴ kuid Euroopa Liiduga liitumisel 01.05.2004 pidi Eesti seni Eestis kehtinud IKS-i viima kooskõlla direktiiviga ning aastast 2008 kehtib uus IKS.¹⁵

Aastast 2010 on üha enam räägitud vajadusest reformida isikuandmete kaitse regulatsiooni Euroopa Liidu tasandil. 1995.a koostatud direktiiv on suutnud isikutele pakkuda laiaulatuslikku ning tehnoloogianeutraalset kaitset 20 aastat, kuid nüüdseks on globaliseerumine, internetikasutajate vähene usaldus nendega seonduvate andmete töötlemisel ja isikuandmete töötlemise järelevalve ebapiisavad mehhanismid on tekitanud vajaduse uue kvaliteediga õigusinstrumendi järele.¹⁶ Euroopa Kohus mitmel puhul leidnud, et käesoleva ajani ei ole liikmesriigid suutnud viia siseriiklikku õigust täielikult direktiiviga kooskõlla.¹⁷

Euroopa Komisjoni initsiatiivil on koostatud Euroopa Parlamendi ja nõukogu määruse „üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta“ eelnõu (edaspidi üldmäärus) ning Euroopa Parlamendi ja nõukogu direktiivi „üksikisikute kaitse kohta seoses pädevates asutustes isikuandmete töötlemisega kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumise kohta“ eelnõu.¹⁸ Üldmäärusega soovitakse asendada praegu kehtiv direktiiv eesmärgiga tagada suurem usaldus isikuandmete kui käibeobjekti suhtes, harmoniseerida liikmesriikide seadusandlusi ning tõhustada järelevalvet isikuandmete töötlemise üle.¹⁹

Töö kirjutamise hetkeks on üldmäärus Euroopa Parlamendi poolt esimesel lugemisel heaks kiidetud. Üldmäärus loodetakse vastu võtta 2014 aasta lõpuks. Isikuandmete töötlemise üldpõhimõtteid sätestav üldmäärus on reformi käigus tekitanud palju kõneainet nii

¹³ Eesti Vabariigi põhiseadus. - RT 1992, 26, 349 ...RT I, 27.04.2011, 2.

¹⁴ Isikuandmete kaitse seadus. - RT I 1996, 48, 944.

¹⁵ Isikuandmete kaitse seadus. - RT I 2007, 24, 127... RT I, 30.12.2010, 11.

¹⁶ C. Cuijpers, N. Purtova, E. Kosta. Data Protection Reform and the Internet: the draft Data Protection Regulation. - Tilburg Law School Research Paper 2014, No. 3, p 1. Available: <http://ssrn.com/abstract=2373683>, 05.04.2014.

¹⁷ Näiteks vt: EKo 16.10.2012, C-614/10, *Commission vs Austria*.

¹⁸ Euroopa Komisjoni eelnõu „Euroopa Parlamendi ja nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta“. KOM(2012) 11. Brüssel: 25.01.2012; Euroopa Komisjoni eelnõu „Euroopa Parlamendi ja nõukogu direktiiv üksikisikute kaitse kohta seoses pädevates asutustes isikuandmete töötlemisega kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumise kohta“. KOM(2012) 10. Brüssel: 25.01.2012.

¹⁹ European Commission. Reform of the data protection regulation legal framework. Available: http://ec.europa.eu/justice/data-protection/review/index_en.htm, 02.02.2014.

liikmesriikide esindajate kui erinevate huvigruppide seas. Euroopa Parlamendi poolt valitud õiguslik instrument – otsekohalduv määrus – tõstatab küsimusi sellest, kas reformiga kavandatavad meetmed on tegelikkuses teostatavad ning efektiivsed, samuti siseriikliku ja Euroopa Liidu õiguse vahekorra.

Käesoleva töö eesmärgiks on teha kindlaks, kas üldmääruses saavutatakse praeguses sõnastuses pakutud lahendustega isikuandmete kaitse reformi peamised eesmärgid, st üksikisikute õiguste parem kaitse isikuandmete töötlemisel, andmete vaba liikumine siseturul ning efektiivne järelevalve isikuandmete töötlemise üle. Eesmärkide saavutamist hinnatakse vastavalt sellele, milliseid eesmäärke on Euroopa Komisjon reformi eestvedamisel ise püstitanud. Meetmete efektiivsuse ja eesmärkide saavutamise kriteeriumiks seatakse, kas soovitud tulemus üldmääruses kavandatud meetme abil saabub.

Käesoleva töö eesmärgiks ei ole, lähtudes püstitatud uurimisküsimustest ja töö mahust, selgitada välja ja analüüsida kogu üldmäärusega kaasnevat mõju Euroopa Liidu ja Eesti õigusele. Töö autor ei sea eesmärgiks anda hinnangut kõigile üldmäärusega kaasnevatele mõjudele ega võrrelda kogu Eesti isikuandmete kaitse regulatsiooni kavandatava üldmääruse omaga.

Sarnasel teemal uurimistöid ei ole autorile teadaolevalt varem tehtud, eelkõige seetõttu, et üldmääruse kavandamine on alles eelnõu faasis ning üldmäärus töös käsitletavas versioonis koostati alles 23.10.2013. Töös lähtutakse üldmääruse sõnastusest seisuga 23.10.2013, kuna Euroopa Parlament kiitis eelnõu 12.03.2014 toimunud hääletusel heaks just kodanikuvabaduste, justiits- ja siseasjade komisjoni poolt 23.10.2014 koostatud sõnastuses.²⁰ Üldmääruse sõnastus võib veel Euroopa Liidu Nõukogu ja Euroopa Parlamendi vahelise koostöö tulemusena muutuda, kuid põhimõttelisi muutusi ei ole oodata – ka võrreldes 25.01.2012 esitatud eelnõuga ei ole tehtud üldmäärusesse põhimõttelisi muudatusi. Isegi olukorras, kus üldmääruse sõnastust ja selles sätestatud meetmeid võidakse muuta või ka juhul kui üldmäärus jäetakse täielikult vastu võtmata, seisneb töö aktuaalsus selles, et töö pakub ajaks, mil isikuandmete kaitse reformi puudutav debatt Euroopa Parlamendis, Nõukogus aga ka ühiskonna jätkub, tugipunkte seisukohtade kujundamiseks.

²⁰ European Parliament legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Ordinary legislative procedure - first reading. P7_TA(2014) 0212. Strasbourg: 12.03.2014.

Töö teema on aktuaalne nii ettevõtete kui üksikisikute vaatepunktist, kuna üldmääruse koostamisel lähtuti kahest peamisest eesmärgist – tugevdada üksikisikute kaitset isikuandmete töötlemisel ning harmoniseerida isikuandmete kaitse regulatsiooni Euroopa Liidu siseselt. Sellest tulenevalt pakuvad töös toodud järeldused nii ettevõtetele kui üksikisikutele sisendit edasises dialoogis üldmääruse lõplikul väljakujundamisel. Riigi seisukohast on käesolevas töös esitatud järeldused aktuaalsed tulenevalt kavandatava üldmääruse otsekohalduvast iseloomust. Vabariigi Valitsus on kujundanud kavandatava üldmääruse suhtes küll esialgsed seisukohad,²¹ kuid käesolevas töös esitatud järelduste alusel on võimalik kujundada põhjalikumad seisukohad üldmääruse arutamisel Euroopa Nõukogus.

Töö on jaotatud kolme peatükki.

Üldmääruse mõju tuvastamiseks on vajalik asetada kavandatav isikuandmete kaitse regulatsiooni üldmäärus olemasolevasse õiguslikku raamistikku. Esimese peatükis tutvustatakse õigusakte, milles on otseselt kirjas või tuletatav õigus isikuandmete kaitsele ning õigusakte, mis on loodud selle õiguse tagamiseks ja kindlustamiseks. Viimaste puhul tuuakse välja nende õigusaktide probleemid ja kitsaskohad, mis võivad olla tinginud vajaduse uue õigusakti järele. Esimeses peatükis on püstitatud järgmine uurimisküsimus: Kas ja millised probleemid praegu kehtivate isikuandmete kaitset tagavate õigusaktide juures on viinud vajaduseni kehtestada Euroopa Liidu tasandil uus õigusakt?

Töö teine peatükk sõnastab isikuandmete kaitse reformi peamised lähtekohad ning tutvustab meetmeid, mida soovitakse eesmärkide saavutamiseks kasutada. Üheks reformi eesmärgiks on tagada üksikisikute parem kaitse, mida loodetakse saavutada, tagades parem läbipaistvus ja kontroll isikuandmete töötlemise üle. Teiseks soovitakse harmoniseerida liikmesriikide killustunud seadusandlust, kehtestades isikuandmete kaitse põhimõtted otsekohalduva määrusega. Määrusega soovitakse täpsustada isikuandmete kaitse regulatsiooni territoriaalset kohaldumisala, ühtlustada materiaaõigust ning vähendada ettevõtete halduskoormust. Peatüki raames püstitatud uurimisküsimuses otsitakse vastust küsimusele, kas meetmed, mida nende probleemide lahendamiseks soovitakse kasutada on efektiivsed ning milline mõju meetmetega kaasneb.

²¹ Vabariigi Valitsuse 29.03.2012 otsuse seletuskiri. Eesti seisukohad isikuandmete kaitset puudutavate Euroopa Komisjoni algatuste suhtes. Arvutivõrgus: <https://dhs.riigikantselei.ee/avalikteave.nsf/documents/NT0018C882?open>, 28.04.2014.

Kui teises peatükis käsitletavat meetmed on nii Euroopa Liidu kui Eesti õiguse mõttes uued, siis üldmäärusega ette nähtud järelevalveregulatsioon pigem muudab ja täpsustab olemasolevat regulatsiooni, mistõttu on võimalik võrdlus siseriikliku õigusega. Kolmandas peatükis tehakse kindlaks üldmääruse regulatsiooni ja siseriiklikus õiguses sätestatud järelevalveregulatsiooni erinevused. Kavandatavate eesmärkide elluviimiseks on üldmäärusega ette nähtud sätted, millega kohustatakse liikmesriike tagama järelevalveasutustele piisav ressurss, sätestatakse ühtne järelevalveasutuste pädevus ning lisatakse terve eraldi peatükk järelevalveasutuste rahvusvahelise koostöö reguleerimiseks. Kolmanda peatüki raames on püstitatud uurimisküsimus: kas meetmed mida isikuandmete töötlemise järelevalve tugevdamiseks soovitakse rakendada on efektiivsed ja siseriiklikus õiguses kohaldatavad.

Töö esimeses peatükis on kasutatud dogmaatilist meetodit ning tehtud kindlaks isikuandmete töötlemist puudutava kehtiva regulatsiooni peamised puudujäägid. Töö teises ja kolmandas peatükis on kasutatud võrdlev- analüütilist meetodit, kus töö autor on võrrelnud praegu kehtivaid peamisi Euroopa Liidu ja Eesti õigusakte kavandatava üldmäärusega ning analüüsinud kavandatavate muudatuste efektiivsust ja võimalikke tagajärgi.

Lisaks asjakohastele õigusaktidele ja üldmääruse eelnõule, on töös kasutatud ka Euroopa Komisjoni poolt koostatud dokumente, sealjuures üldmääruse eelnõuga kaasnevat mõjuanalüüsi. Euroopa Komisjoni allikaid on kasutatud pigem olemasolevate probleemide kaardistamisel, mitte üldmäärusega kaasnevate mõjude hindamisel, kuna komisjoni objektiivsus üldmäärusega kaasnevate mõjude hindamisel on erialases kirjanduses seatud kahtluse alla. Meetmetega kaasnevate mõju analüüsimisel on kasutatud Euroopa Andmekaitseinspektori kommentaare üldmääruse esialgsele versioonile ning direktiivi artikli 29 alusel loodud töörühma arvamusi, samuti erialaseid publikatsioone ning uuringuid. Euroopa Kohtu (edaspidi EK) ja Euroopa Inimõiguste Kohtu (edaspidi EIK) praktikat on kasutatud olemasolevate probleemide kaardistamiseks.

Töö kokkuvõttes esitatakse vastus töös püstitatud uurimisküsimustele ning võetakse kokku töös tehtud järeldused.

Magistritöös on aluseks võetud õigusaktide tekst seisuga 23.10.2013.

1. ISIKUANDMETE KAITSE KEHTIV REGULATSIOON

1.1 Informatsioon ja infoühiskond

Tehnoloogia arengust tulenev informatsiooni laiem levik ja osatähtsuse suurenemine tõi 20 sajandi keskel kaasa teatud riikide liikumise tööstusühiskonnast infoühiskonda.

V. Prausti käsitluse kohaselt mõistetakse infoühiskonna all elukorraldust, kus enamik inimkonna loodud väärtusi on kätketud teabesse. Enamikku infoühiskonnas talletatud teavet hoitakse, teisendatakse ja edastatakse universaalsel digitaalsel kujul. Üldist andmeedastusvõrku kasutades on juurdepääs teabele kõigil ühiskonnaliikmetel. Samuti on infoühiskonnas rutiinne vaimne töö usaldatud masinate hoolde.²² Informatsioonist on kujunenud majandusfaktor, kultuuriväärtus ja põhiseaduslikult kaitstav hüve, aga ka võimalik oht.²³

20. sajandi lõpus toimunud hüppeline areng infotehnoloogia valdkonnas on muutnud riigid ja ühiskonnad järjest rohkem sõltuvaks informatsiooni kättesaadavusest, kvaliteedist ja kommunikatsiooni efektiivsusest.²⁴

Tekkinud on vajadus reguleerida informatsiooni käibe eeldusi, tagajärgi, sisu ja vormi – informatsioon on muutunud õiguse objektiks.²⁵ Informatsiooni käivet reguleeritakse enam siseriiklikul tasandil, rahvusvaheliselt on reguleeritud vaid teatud informatsioonikategooriad – isikuandmed ja loomealane informatsioon.²⁶

Käesoleva töö eesmärgist lähtuvalt omab informatsiooni puudutava regulatsiooniga seonduvalt eelkõige tähtsust isikuandmete kaitsega seonduv. Isikuandmed on mistahes andmed, mille alusel on võimalik füüsilist isikut identifitseerida, kuid andmekaitse seisukohalt kitsendatakse mõistet kriteeriumiga, mille kohaselt omavad tähendust ainult sellised andmed, mille puhul kulub isiku identifitseerimiseks andmete alusel mõistlik aeg.²⁷

²² V. Praust. Infotehnoloogia haldusjuhtimises. Infoühiskond ja selle teetähised. - Majandus- ja kommunikatsiooniministeeriumi aastaraamat, 1998. Arvutivõrgus: <http://www.riso.ee/aastaraamatud/et/pub/1998it/12.htm>, 01.03.2014.

²³ S. Lodde. Informationsrechte des Bürgers gegen den Staat. Carl Heymanns Verlag KG 1996.

²⁴ *Ibid*, lk 25.

²⁵ E. Tikk ja A. Nõmper, lk 19.

²⁶ *Ibid*, lk 19-20.

²⁷ M. Männko, lk 42.

Isikuandmete kaitse töötlemise reguleerimise eesmärgiks on kaitsta isikut, kelle andmeid töödeldakse, mitte töödeldavaid andmeid.²⁸ Alljärgnevalt on käsitletud võimalikke põhiõigusi, mille kaitsmisest isikuandmete kaitse lähtub.

1.2 Isikuandmete kaitse reguleerimisel kaitstavad põhiõigused

Aastal 1890 kirjutatud artiklis “The Right to Privacy” defineerisid Warren ja Brandeis privaatsust kui õigust olla rahule/üks jätetud.²⁹ Eraelu kaitsmine tähendas varem eelkõige isiku tegevuste saladuses hoidmist võõraste eest, enda kohta käivat teavet varjati füüsiliste vahenditega – näiteks kõrge aiaga. Moraalinormid mõistsid hukka ka teise inimese kirjade lugemise.³⁰

Massiteabevahendite levikuga suurenes oht võimalikeks eraelu riiveteks. Aastatel 1960 - 1970 arenes kontseptsioon informatsioonilisest enesemääramisõigusest, mis eristus teistest privaatsuse aspektidest, nagu füüsiline sekkumine kellegi erasfääri või jälitustegevus.³¹ Informatsioonilist enesemääramist hakati defineerima kui isiku õigust otsustada millal, kuidas ja millises ulatuses edastatakse teda puudutavat infot teistele³² ning kui isiku võimet kontrollida enda kohta käivate andmete ringlemist.³³

Saksamaa konstitutsioonikohus tunnustas aastal 1983 informatsioonilist enesemääramisõigust eraldiseisva õigusena. Kohtuotsuse kohaselt on igatühe põhiseaduslik õigus määrata, kellele oma isikuandmeid üle anda ning lubada neid töödelda.³⁴

Koos informatsioonilise enesemääramisõiguse tunnustamisega arenes ka andmekaitse regulatsioon. Infotehnoloogia ja andmete automatiseeritud kujul töötlemise ülikiire areng tekitas vajaduse isikuandmete kaitse järele, kuna andmete töötlemine muutus nii lihtsaks ja ulatuslikuks, et oht informatsioonilise enesemääramisõiguse kahjustamisele suurenes hüppeliselt.³⁵ 1970ndatel algas andmekaitse kui õigusharu kiire areng.³⁶

²⁸ M. Männiko, lk 42.

²⁹ S. D. Warren, L. D. Brandeis. The Right to Privacy. - Harvard Law Review 1890/4, No. 5.

³⁰ M. Männiko, lk 13.

³¹ A. Warren, J. Dearlney, C. Oppenheim. Sources of Literature on Data Protection and Human Rights. - Journal of Information Law and Technology 2001/2, p 4.

³² A. F. Westin., Privacy and Freedom. New York: Atheneum, 1967.

³³ A. Miller. The assault on privacy. Ann Arbor: University of Michigan Press, 1971.

³⁴ C. DeSimone. Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive. - German Law Journal 2010/11, No. 3, p 293.

³⁵ A. C. Evans. European Data Protection Law. - The American Journal of Comparative Law 1981/29, No. 4, p 571.

³⁶ A. Warren *et al*, p 5.

Isikuandmete kaitse lähtepunktideks on seega nii õigus privaatsusele kui ka õigus informatsioonilisele enesemääramisele. Need põhiõigused on mitmes osas kattuvad ning leidub tõlgendusi, mille kohaselt on privaatsusõigus enesemääramisõiguse üks osa, mistõttu on kaitstavaks õigushüveks õigus informatsioonilisele enesemääramisele.³⁷ E. Tikk ja A. Nõmperi õpikus “Informatsioon ja õigus” määratletakse õigus informatsioonilisele enesemääramisele ühena kolmest info põhiõigusest.³⁸ Samas käsitletakse õpikus isikuandmete kaitse ja informatsioonilise enesemääramisõiguse sisulise lähtekohana õigust privaatsusele, mis justkui viitaks, et informatsiooniline enesemääramisõigus (mis hõlmab õigust isikuandmete kaitsele) on üks osa privaatsusõigusest.³⁹

Õigust isikuandmete töötlemise kaitsele ei ole võimalik selgelt paigutada mõne põhiõiguse kaitsealasse. Töö autori arvates annab aga kõige selgema lahenduse see, kui nõustuda, et nii privaatsusõigus kui informatsiooniline enesemääramisõigus on eraldiseivad osad neid ühendavast enesemääramisõigusest⁴⁰ ning isikuandmete kaitset puudutavas osas nende kaitsealad kattuvad. Tuleb nõustuda, et õigus informatsioonilisele enesemääramisõigusele on esialgu kasvanud välja õigusest privaatsusele, kuid käesolevaks hetkeks ei ole see õigus hõlmatud enam sama ulatusega, mis õigus privaatsusele. See tähendab, et nii privaatsusõigusel kui informatsioonilisel enesemääramisõigusel on tänapäeval valdkondi, mis ei puutu kokku isikuandmete kaitsega – vastavat nt füüsiline sekkumine kellegi eraellu (nt isiku jälgimine tema teadmata) ja isiku vajadus olla teadlik enda kohta kogutavate andmete hulgast liigist ja määrast, et olla ühiskonnas aktiivne kodanik. Eeltoodud järeldust toetab ka Saksa konstitutsioonikohtu otsus, millest nähtuvalt mõjutab see, palju on isikul teavet enda kohta käiva informatsiooni töötlemise kohta, tema käitumist aktiivse kodanikuna, mis jääb väljapoole eraelu sfääri.⁴¹

Euroopa Liidu põhiõiguste harta loomisega loobuti sisustamast õigust isikuandmete kaitsele läbi privaatsuse või õiguse informatsioonilisele enesemääramisele. Uue lähenemise kohaselt on õigus isikuandmete kaitsele iseseisev põhiõigus, mis hõlmab endas mõlema eelmainitud

³⁷ M. Männiko, lk 41.

³⁸ E. Tikk, A. Nõmper, lk 37.

³⁹ *Ibid*, lk 72.

⁴⁰ A. Jóri. Data protection law - an introduction. The notion of data protection. Available: <http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.Dataprotection>, 27.04.2014.

⁴¹ C. DeSimone, p 294 - 295.

õiguse kaitsealasid, kuna isikuandmete kaitse ulatub väljapoole traditsioonilisi arusaamu privaatsusest.⁴²

1.3 Isikuandmete kaitse institutsionaalsed lähtekohad

Isikuandmete töötlemise regulatsiooni eesmärgiks ei ole keelata isikuga seotud andmete töötlemine, vaid tagada isikuandmete töötlemine õiguslikul alusel. Esimesed isikuandmete töötlemise õiguslikud regulatsioonid loodi 1970ndatel, kui tehnoloogia areng võimaldas isikuandmeid töödelda automatiseeritult. Sellega kaasnes hüppeliselt andmetöötamise maht aga ka suurem oht üksikisikute õigushüvedele. Pidades silmas käesoleva töö eesmärki ja mahtu, on ebamõistlik siinkohal käsitleda kõiki isikuandmete kaitsega seonduvaid akte.

Töös on käsitletud õigusakte, mis sätestavad Euroopa kontekstis otseselt või kaudselt õiguse isikuandmete kaitsele (Euroopa inimõiguste ja põhivabaduste kaitse konventsioon ja Euroopa Liidu põhiõiguste harta) ning instrumentid, mis nende õiguste tagamiseks on loodud ning mis reguleerivad käsitletavaid küsimusi Euroopa Liidus ja Eestis. Töö autor on valinud käsitletavateks instrumentideks:

- a) Majandusliku Koostöö ja Arengu Organisatsiooni juhendi eraelu kaitsest ja piiriülesest isikuandmete kaitsest 23.09.1980;⁴³
- b) Euroopa Nõukogu 1981. aasta isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni;⁴⁴
- c) Euroopa Ühenduse direktiivi 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta.⁴⁵

Instrumentide valikut õigustab asjaolu, et need sisaldavad andmekaitse põhiprintsiipe, mis on tänase päevani siseriikliku andmekaitseõiguse aluseks.⁴⁶ Samuti on just need õigusaktid rahvusvahelisel tasandil mõjutanud hiljem koostatud andmekaitse reguleerivaid instrumente, k.a üldmäärust.

Eesti kontekstis käsitleb käesolev peatükk Eesti Vabariigi Põhiseadust ja sealt tuletatavat õigust isikuandmete kaitsele ning õigusi tagavat instrumenti isikuandmete kaitse seaduse näol.

⁴² L. A. Bygrave. The place of privacy and data protection law. - University of New South Wales Law Journal 2001/6. Available: <http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html>, 12.04.2014.

⁴³ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD 1980.

⁴⁴ Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (jõustunud 28.01.1981). - RT II 2001, 1, 3.

⁴⁵ L. A. Bygrave. Data protection law: approaching its rationale, logic and limits. Hague: Kluwer Law International 2002, p 29.

⁴⁶ L. A. Bygrave 2002, p 30.

Peatükis antakse vastus küsimusele, miks ei piisa olemasolevatest õigusinstrumentidest, et tagada üksikisikute kaitse isikuandmete töötlemisel ning andmete vaba liikumine Euroopa Liidus.

1.3.1 Rahvusvaheline õigus

1.3.1.1 Euroopa inimõiguste ja põhivabaduste kaitse konventsioon

Euroopa inimõiguste ja põhivabaduste kaitse konventsioon (edaspidi EIÕK) võeti vastu aastal 1950 ning see jõustus aastal 1953.⁴⁷

Konventsioon ei sätesta selgesõnaliselt õigust isikuandmete kaitsele. Selline õigus on tuletatav EIÕK artiklis 8 sätestatud õigusest era- ja perekonnaelu kaitsele.

Artiklis 8 ei sisaldu termineid „andmed“ või „informatsioon“, kuid EIK ulatuslik praktika annab tunnistust sellest, et ka informatsiooniline enesemääramisõigus (ja sellega hõlmatud õigus isikuandmete kaitsele) on artikkel 8 kaitsealas.⁴⁸ Esimest korda mainitakse õigust isikuandmete kaitsele (informatsioonilise enesemääramise kaudu) EIÕK artikli 8 kontekstis aastal 1984 EIK otsuses *Malone vs The United Kingdom* kohtunik Pettiti eriarvamuses, kes tõi välja, et avaliku võimu poolt õigusliku aluseta telekommunikatsioonivahendite mõõtmine, rikub isiku õigust informatsioonilisele enesemääramisele ning rõhutas, et EIÕK eesmärgiks on kaitsta inimest ning tänapäeva inimesel on vajadus säilitada oma identiteet, keelduda ühiskonna täielikust läbipaistvusest ning säilitada oma isiksuse privaatsus.⁴⁹ Mõned aastad hiljem on EIK leidnud, et EIÕK artikli 8 kaitsealas on ka informatsiooni kogumine ja avaldamine võimaldamata isikul ebaõiget informatsiooni ümber lükata⁵⁰ ning isiku õigus nõuda ligipääsu enda kohta kogutud andmetele.⁵¹

Eelnevalt viidatud EIK otsustest nähtuvalt saab rääkida EIÕK artikli 8 riivist ka isikuandmete töötlemise kontekstis. Andmete töötlemisel ei oma tähtsust see, kas töödeldavad andmed kuuluvad era- või avalikku sfääri, tähtsust omab see, kas andmed on seostatavad konkreetse isikuga.⁵² EIK on asunud seisukohale, et läbiotsimise teostamine ka isiku töökohas kujutab

⁴⁷ The Council of Europe. A Convention to protect your rights and liberties. Available: <http://human-rights-convention.org/>, 27.04.2014.

⁴⁸ E. Tikk, A. Nõmper, lk 39.

⁴⁹ EIKo 02.08.1984, 8691/79, *Malone vs The United Kingdom*, concurring opinion of judge Pettiti.

⁵⁰ EIKo 26.03.1987, 9248/81, *Leander vs Sweden*, § 59.

⁵¹ EIKo 07.07.1989, 10454/83, *Gaskin vs The United Kingdom*, §§ 41, 49.

⁵² EIKo 04.05.2000, 28341/95, *Rotaru vs Romania*, § 46.

endast artikkel 8 riivet, kuigi tegemist ei ole eraelu ega perekonnaelu riivega artikli 8 grammatilise tõlgenduse mõttes.⁵³

EIÕK artiklist 8 ei tulene mitte ainult kohustus austada eraelu, vaid seadusandja kohustus kehtestada eraelu kaitset tagavad õigusaktid.⁵⁴

Tänaseks päevaks on kõik Euroopa Nõukogu 47 liikmesriiki konventsiooni ratifitseerinud ja tunnistanud sellega konventsiooni õiguslikku siduvust.⁵⁵ Kõik Euroopa Liidu liikmesriigid on liitunud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga ning käimas on läbirääkimised Euroopa Liidu ühinemiseks konventsiooniga.⁵⁶

EIÕK on aktuaalne isikuandmete kaitse alus ka tänapäeval, kuid isikuandmete kaitse õigusliku alusena on see üldsõnaline. EIÕK ei sisalda sõnaselget viidet isikuandmete kaitsele ning vaatamata ulatuslikule kohtupraktikale, puudub õiguskindlus selles, millal jäävad isikuandmete töötlemisega seonduvad küsimused EIÕK kaitsealasse ja millal mitte. EIÕK artiklis 8 sätestatud “eraelu” definitsioon oli ebaselge, peamine rõhk artikli rakendamisel seonduvalt andmekaitsega puudutas avaliku võimu sekkumist.⁵⁷

EIK on rõhutanud, et piisava regulatsiooni kehtestamine isikuandmete kaitse tagamiseks on liikmesriikide ülesanne⁵⁸ mistõttu ei paku EIÕK lahendust vajadusele positiivse regulatsiooni järele.⁵⁹ EIÕK artikli 8 kaitsealas on üksnes need isikuandmete töötlemisega seotud juhtumid, millega kaasneb võimalik oht isiku eraelu riivele, kuid artiklist 8 ei saa tuletada üldist kohustus isikuandmete nõuetekohaseks töötlemiseks.⁶⁰ EIÕK kaitsealast jääb välja ka isikuandmete töötlemine erasektori poolt, mis moodustab märkimisväärse osa isikuandmete töötlemisest.⁶¹ Samuti on tähelepanuväärne, et EIÕK koostati aastal 1950, mil ei suudetud veel ette nähta tehnoloogia ja eelkõige interneti arenguga kaasnevaid ohtusid.⁶²

⁵³ EIKo 16.12.1992, 13710/88, *Niemietz vs Germany*, §§ 29-33.

⁵⁴ EIKo 17.07.2008, 20511/03, *I vs Finland*, § 38.

⁵⁵ The Council of Europe. European Convention on Human Rights. Impact in 47 countries. Available: <http://human-rights-convention.org/impact-of-the-european-convention-on-human-rights/>, 28.04.2014.

⁵⁶ The Council of Europe. European Convention on Human Rights. Accession of the European Union. Available: <http://hub.coe.int/what-we-do/human-rights/eu-accession-to-the-convention>, 27.04.2014.

⁵⁷ P. De Hert, S. Gutwirth. *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action. Reinventing Data Protection*. Dordrecht: Springer Science 2009, p 5.

⁵⁸ EIKo 17.07.2008, 20511/03, *I vs Finland*, § 38.

⁵⁹ P. De Hert, S. Gutwirth, p 5.

⁶⁰ EIKo 14.03.2013, 24117/08, *Bernh Larsen Holding AS and others vs Norway*, §§ 172-173.

⁶¹ A. C. Evans, p 572.

⁶² *Ibid.*

1.3.1.2 Majandusliku Koostöö ja Arengu Organisatsiooni 23.09.1980 juhend eraelu kaitsest ja piirülesest isikuandmete kaitsest

Majandusliku Koostöö ja Arengu Organisatsioon (edaspidi OECD) koostas 23.09.1980 juhendi privaatsuse ja üle piiri edastatavate isikuandmete kaitseks. Juhend käsitles mitmeid andmekaitse aluspõhimõtteid.

OECD juhendi (nagu ka paljude teiste rahvusvaheliste andmekaitse instrumentide) väljatöötamist ajendas 1970ndatel märkimisväärselt intensiivistunud isikuandmete töötlemine, mis väljendus nii laiaulatuslikus isikuandmete kogumises ja töötlemises ning tingis mitmete riikide seadusandliku tegevuse.⁶³

OECD juhendi koostamise eesmärgiks oli koostada mittesiduvad juhised riikidele siseriikliku andmekaitseõiguse harmoniseerimiseks. Juhendis sisalduvad OECD liikmesriikide poolt kokku lepitud peamised põhimõtted loodi eesmärgiga toetada ja harmoniseerida riikide siseriiklikku õigust ning juhtudel, kus siseriiklik õigus andmekaitse valdkonnas puudus, panna alus siseriikliku regulatsiooni loomisele.⁶⁴

OECD juhend väljastati ajal, mil paljud riigid nii Euroopas kui ka mujal tegelesid andmekaitse regulatsiooni väljatöötamisega, mistõttu mõjutas juhend mitme riigi andmekaitseõiguse arengut oluliselt, muuhulgas ka näiteks Jaapani, Austraalia, Uus-Meremaa ja Hong Kongi.⁶⁵

OECD juhend on märkimisväärne just seetõttu, et sellest lähtub ja selles kajastub isikuandmete töötlemise põhimõtted ka tänapäeval.⁶⁶ OECD juhend sätestas andmekaitse seisukohast olulised definitsioonid (andmete töötleja, isikuandmed ning isikuandmete piiriülene levik) ning kehtestas esmakordselt tänaseks üldist tunnustamist leidnud õiguspärase andmetöötamise üldpõhimõtteid.⁶⁷

Aastal 2013 uuendas OECD esmakordselt oma 1980 koostatud juhendi. Uuendatud juhendi eesmärgiks oli tugevdada privaatsuse kaitse rakendamist praktikas läbi riskide haldamise ning

⁶³ R. Clarke. The OECD Data Protection Guidelines: A Template for Evaluating Information Privacy Law and Proposals for Information Privacy Law. Canberra: Australian National University 1989, p 1. Available: <http://www.rogerclarke.com/DV/PaperOECD.html>, 28.04.2014.

⁶⁴ OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Preface. Available: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>, 28.04.2014.

⁶⁵ L. A. Bygrave 2002, p 32.

⁶⁶ *Ibid.*

⁶⁷ M. Männiko, lk 57.

suurendada riikidevahelist koostööd privaatsuse tagamisel, pidades silmas privaatsuse globaalset dimensiooni.⁶⁸

OECD juhend on eelkõige suunatud osalisriikidele. OECD-sse kuuluvad 34 liikmesriiki, sealjuures riigid Põhja- ja Lõuna-Ameerikast ning Kagu-Aasiast.⁶⁹

OECD juhendi tähtsust andmekaitsevaldkonna reguleerimisel vähendab selle soovituslik iseloom ning asjaolu, et juhendi tegemise hetkeks kuulus OECD-sse kõigest 24 riiki.⁷⁰ OECD juhendist tulenevate põhimõtete järgimise kindlustamiseks puudub igasugune jõustamismehhanism, mistõttu ei ole juhend sobiv instrument Euroopa Liidu tasemel isikuandmete kaitse reguleerimiseks. Kuna tegemist on üldpõhimõtteid tutvustava juhendiga, et ole juhend sobiv reguleerima isikuandmetega töötlemise spetsiifilisemaid küsimusi.⁷¹

1.3.1.3 Euroopa Nõukogu 1981 aasta isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon

28.01.1981 võeti vastu Euroopa Nõukogu isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon ETS 108 (edaspidi konventsioon 108). Tegemist oli esimese ülemaailmse siduva õigusliku instrumendiga andmekaitse valdkonnas.⁷² Konventsiooni vastuvõtmisele eelnesid mitmed Euroopa nõukogu ministrite komitee soovitusel, mille pinnalt tegeleti valdkonna kodifitseerimisega.⁷³

Konventsiooni 108 peamine eesmärk on kaitsta indiviidi isikandmete kogumise ja töötlemisega kaasnevate võimalike kuritarvituste eest ning teisalt reguleerida andmete piiriülest liikumist.⁷⁴ Konventsiooni artikli üks kohaselt on: “konventsiooni eesmärk tagada osalisriigi territooriumil igale isikule, olenemata tema kodakondsusest või alalisest elukohast, tema õiguste ja põhivabaduste austamine. Eriti oluline on isikuandmete automatiseeritud töötlemisel tagada isiku õigus säilitada privaatsus («andmekaitse»).

⁶⁸ OECD. OECD work on privacy. Available: <http://www.oecd.org/sti/ieconomy/privacy.html>, 28.04.2014.

⁶⁹ OECD. Members and partners. Available: <http://www.oecd.org/about/membersandpartners/>, 27.04.2014.

⁷⁰ L. A. Bygrave 2002, p 32.

⁷¹ R. Clarke, p 7 - 8.

⁷² G. Greenleaf. The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. - International Data Privacy Law 2012/2, No. 2, p 68.

⁷³ M. Männiko, lk 58.

⁷⁴ A. C. Evans, p 578.

Konventsioon 108 sõnastab isikuandmete töötlemise põhimõtted, mis on tänapäeval isikuandmete kaitse põhialusteks.⁷⁵

Lisaks isiku põhiõiguste tagamisele, reguleerib konventsioon 108 ka andmete piiriülest levikut. Konventsiooni 108 artikkel 12 p 2 näeb ette osalisriigi õiguse andmete vabaks edastamiseks teise riigi territooriumile.

Aastal 2001 koostatud konventsiooni 108 lisaprotokoll sätestab piirangud andmete ekspordile ja näeb ette sõltumatu järelevalveasutuse loomise, õiguse edasikaebamisele ning sätestab seega praktiliselt sarnased meetmed andmekaitse direktiiviga 95/46/EÜ.⁷⁶

Konventsiooniga on 2014 aasta aprilli seisuga liitunud 46 47st Euroopa Nõukogu liikmesriigist. Mitteliikmesriikidena on konventsiooniga ühinenud Uruguai ja Maroko.⁷⁷

Aastal 1981 oli konventsioon 108 olemasolevatest rahvusvahelistest õigusaktidest kõige spetsiifilisem, kuna oli koostatud pidades silmas tehnoloogia arengut ning on osalisriikidele siduv. Konventsioonil puudub konkreetne jõustamismehhanism ning tulenevalt eesmärgist ühtlustada isikuandmete kaitset üle maailma ei ole instrument sobiv Euroopa Liidu siseturu küsimuste reguleerimiseks.⁷⁸ Konventsioon 108 on ka mõningal määral iganenud ega arvesta üha kasvava internetikasutajate arvuga.

1.3.2 Euroopa Liidu õigus

Kuigi Euroopa Liidu tasandil sätestab õiguse isikuandmete kaitsele Euroopa Liidu põhiõiguste harta (edaspidi harta), ei olnud hartat direktiivi koostamise ajaks veel loodud. Sellest tulenevalt on Euroopa Liidu tasandil käsitletavat õigusaktid toodud kronoloogilises järjekorras.

1.3.2.1 Euroopa Ühenduse direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta

Euroopa Liidu tasandil on praegu peamiseks õigusinstrumendiks isikuandmete kaitse reguleerimisel direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta.

⁷⁵ G. Greenleaf, p 81.

⁷⁶ *Ibid*, lk 73-74.

⁷⁷ The Council of Europe. Treaty Office. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.:108. Available: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG>, 28.04.2014.

⁷⁸ G. Greenleaf, p 81.

Direktiiv võeti vastu 1995 eesmärgiga ühtlustada ja harmoniseerida liikmesriikide vahel isikuandmete töötlemisega seonduvaid õigusakte.⁷⁹ Direktiivi koostamisel lähtuti kahest eesmärgist – tagada kaupade, kapitali ja teenuste vaba liikumise raames ka andmete vaba liikumine ja efektiivne siseturu toimimine ning teisalt tagada isikute põhiõiguste ja -vabaduste kaitse.⁸⁰

Direktiiv loodi eesmärgiga täpsustada juba olemasolevaid õigusakte, mis nähtub ka direktiivi preambulast 10. Preambula 10 kohaselt on direktiivi eesmärk kaitsta EIÕK artiklis 8 ja üldistes põhimõtetes tunnustatud põhiõigusi ning preambula 11 kohaselt täpsustavad ja võimendavad direktiivis sisalduvad üksisikute õiguste ja vabaduste, eriti eraelu puutumatus õiguse kaitsmise põhimõtted konventsioon 108 omi.

Direktiivi peetakse õiguslikest instrumentidest Euroopa Liidus kõige mahukamaks ja olulisemaks.⁸¹ Võrreldes varasemalt eksisteerinud regulatsiooniga (konventsioon 108 ja EIÕK) on vastu võetud direktiiv ka oluliselt konkreetsem.

Euroopa Kohus on märkinud, et Euroopa Liidu õigusaktid on isikuandmete kaitse määratlemisel üldised ja sätestavad väga laia tähendusega terminid.⁸²

Direktiiviga anti liikmesriikidele aega kuni 24.10.1998, et siseriiklik seadusandlus direktiiviga vastavusse viia, tegelikkuses jõudis tähtaegselt valmis ainult Rootsi.⁸³

Direktiiv kohaldub kõigile Euroopa Liidu 28 liikmesriigile ning laieneb Euroopa Majandusühenduse riikidele Norrale, Liechtensteinile ja Islandile. Euroopa Kohus omab jurisdiktsiooni otsustamiseks, kas liikmesriik on direktiivist tulenevad kohustused täitnud. Samuti annab kohus eelotsuseid seonduvalt direktiivi tõlgendamisega.⁸⁴

Direktiivi artikli 3 (2) kohaselt on direktiivi kohaldumisalast välistatud andmetöötlus, mis toimub sellise tegevuse käigus, mis jääb väljapoole ühenduse õigust, näiteks Euroopa Liidu lepingu V ja VI jaotises nimetatud tegevused ning tegevused, mis on seotud avaliku korra, riigikaitse, riigi julgeoleku (sealjuures majanduslik heaolu, kui töötlemine on seotud riigi julgeoleku küsimustega) ja riigi toimingutega kriminaalõiguse valdkonnas. Kolmas erand

⁷⁹ P. Carey. Data protection: a practical guide to UK and EU law. Oxford: Oxford University Press 2004, p 3.

⁸⁰ P. De Hert, S. Gutwirth, p 5.

⁸¹ E. Tikk, A. Nömper, lk 67; L. A. Bygrave 2002, p 30.

⁸² EKo 20.05.2003, C-465/00, C-138/01, C-139/01, *Verfassungsgerichtshof*, § 43.

⁸³ P. Carey, p 4.

⁸⁴ *Ibid.*

näeb ette, et direktiiv ei kohaldu andmete töötlemisele füüsilise isiku poolt isiklikel või kodustel eesmärkidel.

Sisulises mõttes kohaldub direktiiv vastavalt EL primaarõigusele ainult siseturuga seonduvatele küsimustele. Direktiivi kohaldumisalast välja jäävatest asjadest on kõige märkimisväärsem isikuandmete töötlemine politsei- ja õigusalase koostöö raames. Seda valdkonda reguleerib Euroopa Nõukogu 27. novembri 2008 raamotsus 2008/977/JSK kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta.⁸⁵

Direktiiv kohaldub ainult liikmesriikidele, mistõttu tekkis vajadus kehtestada täiendav regulatsioon isikuandmete töötlemiseks Euroopa Liisu institutsioonides. Selleks kehtestati Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aastal määrus nr 2001/45/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta.⁸⁶ Direktiivi 95/46 täpsustab ja täiendab ka Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatus kaitset elektroonilise side sektoris.⁸⁷ Käesoleva töö eesmärgipüstitusest ja mahust lähtuvalt viidatud direktiividel pikemalt ei peatuta.

Direktiiv kehtestati aastal 1995 ning ei suuda arvestada kõigi tänapäeva tehnoloogiate, näiteks pilvandmetöötluse, erisustega.⁸⁸ Direktiivide olemusest tulenevalt on direktiivides sätestatu siduv üksnes eesmärkide osas ning direktiivid jätavad seetõttu liikmesriikidele meetodite ja vormi osas valikuvabaduse.⁸⁹ Ka direktiiv 95/46/EÜ on jätnud EL liikmesriikidele mitmes osas vabad käed. Selle tulemusena on tekkinud olukord, kus isikuandmete kaitse regulatsioon

⁸⁵ Euroopa Nõukogu 27. novembri 2008 raamotsus 2008/977/JSK kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta. - ELT L 350, 30.12.2008, lk 60-71.

⁸⁶ Euroopa Parlamendi ja nõukogu 18. detsembri 2000.a määrus nr 2001/45/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta. - ELT L 195, 19.07.2001, lk 46-49.

⁸⁷ Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatus kaitset elektroonilise side sektoris (eraelu puutumatus ja elektroonilist sidet käsitlev direktiiv). - ELT L 201, 31.07.2002, lk 37 - 47.

⁸⁸ N. Robinson, H. Graux, M. Botterman, L. Valeri. Review of the European Data Protection Directive. Cambridge: RAND, 2009, p 36. Available: http://www.hideproject.org/downloads/references/review_of_eu_dp_directive.pdf, 29.04.2014.

⁸⁹ P. Craig, G. de Burca. EU law. Text, Cases and Materials. Fifth edition. Oxford: Oxford University Press 2011, p 106.

on liikmesriigiti erinev. Erinevustest tulenevalt ei ole saavutatud ka direktiiviga soovitud eesmärke ning isikuandmete kaitse tase on liikmesriigiti erinev.⁹⁰

Ebaühtlane isikuandmete kaitse regulatsioon ja liikmesriikidele jäetud ulatuslik otsustusõigus teatud valdkondades raskendavad isikuandmete piirulest töötlemist ja edastamist. Liikmesriigid ei ole suutnud kehtestada efektiivset järelevalve regulatsiooni, et tagada direktiivist tulenevate põhimõtete elluviimine.⁹¹

1.3.2.2 Euroopa Liidu põhiõiguste harta

Euroopa Liidu aluslepingutes ei sisaldunud viidet inimõigustele ega nende kaitsele. Euroopa Kohus oli üha sagedamini sunnitud lahendama vaidlusi, mis puudutasid inimõiguste rikkumisi Euroopa Liidu õiguse raames, mistõttu tekkis vajadus sõnastada põhilised inimõigused ka Euroopa Liidu õiguses.⁹²

7. detsembril aastal 2000 kuulutati välja Euroopa Liidu põhiõiguste harta. Harta hõlmab Euroopa kodanike tsiviil-, poliitilisi-, majanduslikke ja sotsiaalseid õigusi.

Algselt oli harta ainult poliitiline dokument, aga Lissaboni lepingu jõustumisega 1. detsembril 2009 sai harta osaks Euroopa Liidu primaarõigusest. Kuigi harta teksti iseenesest lepingusse ei inkorporeeritud, sätestab Euroopa Liidu Lepingu artikkel 6 (1), et Liit tunnustab 7.12.2000 Euroopa Liidu põhiõiguste hartas, nagu seda on kohandatud 12.12.2007 Strasbourgis, sätestatud õigusi, vabadusi ja põhimõtteid, millel on aluselepingutega võrreldes samaväärne õigusjõud.⁹³

Harta sätestab artiklis 7 sarnaselt EIÕK-le isiku õiguse eraelu kaitsele ning seda isegi samas sõnastuses kui konventsioonis. Samas näeb harta selle kõrval ette eraldi õigusena artiklis 8 õiguse isikuandmete kaitsele.⁹⁴

Euroopa Liidu põhiõiguste hartaga on seotud kõik Euroopa Liidu liikmesriigid ning institutsioonid.⁹⁵

⁹⁰ European Commission report. First report on the implementation of the Data Protection Directive (95/46/EC). COM(2003) 265 final. Brussels: 15.05.2003. Available: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52003DC0265#text>, 29.04.2014.

⁹¹ N. Robinson *et al*, p 35.

⁹² Fundamental Rights Agency, European Commission. Handbook on European Data Protection law. Luxemburg: Publications office of the European Union, 2014, p 20. Available: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, 01.05.2014.

⁹³ Euroopa Liidu lepingu konsolideeritud versioon. - ELT C 326/1, 26.10.2012, lk 13 - 46.

⁹⁴ P. De Hert, S. Gutwirth, lk 4.

Pidades silmas, et varem ei olnud õigust isikuandmete kaitsele eraldiseisvalt mainitud EIÕK-s ega üheski teises põhiõigusi sätestatavas õigusallikas, tõi selle õiguse lisamine kaasa kvalitatiivse muutuse konstitutsioonilisel tasandil nii direktiiv kui ka konventsioon 108 tagasid varasemalt olemas olnud põhiõiguse – õiguse privaatsusele – kaitse, kuid harta loomisega on seadusandja läinud kaugemale ning loonud uue põhiõiguse.⁹⁶

Direktiivi kehtestamisel peeti pigem silmas Euroopa Liidu siseturu huvisid ning üksikisikute õiguste kaitse ei olnud direktiivi kehtestamisel võrdväärseks eesmärgiks, millele viitas direktiivi ettevõtja-sõbralik regulatsioon. Hartas isikuandmete kaitse õiguse kui põhiõiguse sätestamine võimaldas huvisid rohkem tasakaalustada.⁹⁷ Sellele vaatamata ei lahendanud harta direktiivi probleeme, kuna põhiõigusi sisaldava dokumendina ei näe see ette spetsiifilisi reegleid isikuandmete töötlemiseks.

1.3.3 Eesti õigus

Eesti Põhiseadus ei sätesta eraldi õigust isikuandmete kaitsele, kuid see õigus on Põhiseadusest tuletatav. Isikuandmete kaitset reguleerib IKS, mida muudeti liitumisel Euroopa Liiduga eesmärgiga viia see kooskõlla direktiiviga ning saavutada IKS-iga direktiivis ette nähtud eesmärgid.⁹⁸ Isikuandmete töötlemist puudutab ka avaliku teabe seadus,⁹⁹ aga ka eriseadused, näiteks infoühiskonna teenuse seadus.¹⁰⁰ Samuti käsitleb isikuandmetega seonduvat võlaõigusseaduse lepinguväliste võlasuhete regulatsioon osas, mis see võimaldab näiteks nõuda ebaõigete andmete ümberlükkamist.

Pidades silmas käesoleva töö mahtu ja eesmärki ei ole Eesti õigust analüüsid käsitlenud teisi õigusakte peale Põhiseaduse, kust on tuletatav isikuandmete kaitse alus ning IKS-i, mis sätestab spetsiifilise normistiku isikuandmete töötlemiseks ja töötlemise üle järelevalve teostamiseks.

Tuleb silmas pidada, et mitmed rahvusvahelised õigusaktid on Eestile siduva iseloomuga. Eesti on seotud Euroopa inimõiguste- ja põhivabaduste kaitse konventsiooniga, kuna ratifitseeris selle välislepingu aastal 1996 kui ka konventsiooniga 108, mille ratifitseeris aastal

⁹⁵ European Commission. EU Charter of Fundamental Rights. Available: http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm, 29.04.2014.

⁹⁶ P. De Hert, S. Gutwirth, lk 4.

⁹⁷ *Ibid*, lk 5.

⁹⁸ Isikuandmete kaitse seaduse eelnõu. 1026 SE, lk 1. - Arvutivõrgus: [https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/IKS%20SELETUSKIRI%20\(1\).rtf](https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/IKS%20SELETUSKIRI%20(1).rtf), 29.04.2014.

⁹⁹ Avaliku teabe seadus. - RT I, 19.12.2012, 5.

¹⁰⁰ Infoühiskonna teenuse seadus. - RT I, 06.01.2011, 12.

2002. Eestile on siduvad ka kõik eelpool nimetatud Euroopa Liidu õigusinstrumentid, kuna alates liitumislepingu allkirjastamisest aastal 2004 muutusid Euroopa Liidu õigusaktid Eestile siduvaks. Eesti on OECD liige alates 2010 aastast, mistõttu on OECD juhend soovituslik ka Eestile.

1.3.3.1 Eesti Vabariigi põhiseadus

Põhiseaduslik garantii isikuandmete kaitsele väljendub riikide põhiseadustes reeglina õigusena eraelu kaitsele ning kodu- ja sõnumisaladuse puutumatusse. Väga väheste Euroopa riikide põhiseadused sätestavad selgesõnaliselt õiguse isikuandmete kaitsele. Ilmselt on põhjus selles, et riikide põhiseadused koostati ajal, mil õigust isikuandmete kaitsele ei peetud eraldiseisvaks õiguseks. Hilisemad konstitutsioonid sätestavad isikuandmete kaitse eraldiseisva õigusena: näiteks aastal 2011 koostatud Ungari konstitutsiooni artikkel VI näeb ette, et igal on õigus isikuandmete kaitsele ning õigus saada avalikuks kasutamiseks mõeldud infot.¹⁰¹

Aastal 2003 Andmekaitse Inspektsiooni poolt koostatud ülevaates Riigikogu põhiseaduskomisjonile ja õiguskantslerile seostatakse isikuandmete kaitse regulatsioon küll informatsioonilise enesemääramisõigusega, kuid see õigus arvatakse olevat PS § 26 sätestatud eraelu kaitse üks osa.¹⁰² IKS-i eelnõu seletuskirjas viidatakse samuti informatsioonilisele enesemääramisõigusele kui kaitstavale õigushüvele.¹⁰³

Õigus informatsioonilisele enesemääramisele paigutub PS § 19 kaitsealasse, mille kohaselt on isikul õigus vabale eneseteostusele.¹⁰⁴ Õigus vabale eneseteostusele on üldine isiksuspõhiõigus, mis hõlmab endas ka enesemääramisõigust. Enesemääramisõigus koosneb aga muuhulgas ka informatsioonilisest enesemääramisõigusest, mis tähendab igal õigust otsustada, kas ja kui palju tema kohta andmeid kogutakse ja salvestatakse.¹⁰⁵

PS § 26 sätestab igal õiguse perekonna- ja eraelu puutumatusse. Riigikohus on asunud seisukohale, et eraelu puutumatus riivena tuleb käsitleda ka isikuandmete kogumist,

¹⁰¹ Courtesy translation of the consolidated version of the Fundamental Law of Hungary, effective as of 1 April 2013. Available: <http://tinyurl.com/q2x66k6>, 29.04.2014.

¹⁰² Andmekaitse Inspektsiooni ettekanne Riigikogu põhiseaduslikkuse komisjonile ja õiguskantslerile. 2003, lk 1. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/2003.rtf, 29.04.2014.

¹⁰³ Isikuandmete kaitse seaduse eelnõu. 1026 SE, lk 11.

¹⁰⁴ M. Ernits. §19/3.1.2.1. - E.J Truuväli jt (toim). Eesti Vabariigi Põhiseadus. Komm. vlj. 2. vlj. Tallinn: Juura 2008.

¹⁰⁵ *Ibid.*

säilitamist, kasutamist ja avalikustamist.¹⁰⁶ Tulenevalt sellest, et PS § 26 tõlgendamisel tuleb arvestada ka EIÕK artikliga 8 ja selle tõlgendustega, saab õigust informatsioonilisele enesemääramisele paigutada ka PS § 26 kaitsealasse,¹⁰⁷ kuna sarnaselt on teinud EIK mitmes oma lahendis artikli 8 tõlgendamisel.¹⁰⁸

R. Alexy on seisukohal, et PS § 26 ja 42 hõlmavad ainult osa informatsioonilise enesemääramise tahkudest, eriti oluliseks osutub informatsioonilise enesemääramisõiguse sisustamine läbi PS § 19 olukorras, kus riik üritab hankida teavet isiku hingelise seisundi ja iseloomu kohta.¹⁰⁹

Nagu eelpool mainitud, ei ole täpselt selge PS § 19 ja § 26 vahekord, mis puudutab isikuandmete töötlemisel kaitstavaid põhiõigusi. Siiski on tähelepanuväärne, et üha enam viidatakse isikuandmete kaitse seonduvates küsimustes eraldiseisva alusena PS §-st 19 tulenevale õigusele informatsioonilisele enesemääramisele. Õiguskantsler on asunud seisukohale, et liigse andmetöötluse eest kaitseb isikut nii PS § 19 kui PS § 26 ning kuigi reeglina on isikuandmete kaitse hõlmatud eraelu kaitsega, tulenevad piirangud juhul, kui tegevus ei lange PS § 26 kaitsealasse, PS §-st 19.¹¹⁰

Kuigi õigus isikuandmete kaitsele ei ole Eesti Põhiseaduses selgesõnaliselt sätestatud, pole kahtlust, et PS §-st 19 ja §-st 26 on see õigus tuletatav.

1.3.3.2 Isikuandmete kaitse seadus

Esimesed siseriiklikud isikuandmete kaitset reguleerivad õigusaktid kehtestati Euroopas 1970ndatel ja 1980ndatel.¹¹¹ Eestis kehtestati esimene redaktsioon isikuandmete kaitse seadusest aastal 1996. Võrdluseks samasisuline seadus võeti esmakordselt Sloveenias vastu 1999 aastal ning Lätis ja Leedus aastal 2000.¹¹²

¹⁰⁶ RKHKo 3-3-1-3-12 p 19, 12.06.2012.

¹⁰⁷ E. J. Truuväli jt (koost), lk 293 jj.

¹⁰⁸ EIKo 04.05.2000, 28341/95, *Rotaru vs Romania*; EIKo 16.12.1992, 13710/88, *Niemietz vs Germany*

¹⁰⁹ R. Alexy. Põhiõigused Eesti Põhiseaduses. - *Juridica* 2001/eriväljaanne, p 6.1.2.2.

¹¹⁰ Õiguskantsleri vastus Andmekaitse Inspeksiooni märgukirjale. Tallinn: 26.02.2014. Arvutivõrgus: http://oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_oigus_votta_nousolek_isikuandmete_tootlemiseks_tuupingimustes.pdf, 29.04.2014; Õiguskantsleri märgukiri justiitsministrile. Tallinn: 21.07.2011. Arvutivõrgus: http://lasteombudsman.ee/sites/default/files/field_document2/6iguskantsleri_margukiri_elatisvolglaste_nimekirja_de_avalikustamine.pdf, 29.04.2014.

¹¹¹ Esimene Saksamaa Liitvabariigi Hesseni liidumal 1970, seejärel Rootsi Kuningriik ning Norra, Taani ja prantsusmaa. Vt: E. Tikk, A. Nõmper, lk 66.

¹¹² Privacy International. Report: Latvia. Chapter I - legal framework. Available: <https://www.privacyinternational.org/reports/latvia/i-legal-framework>, 29.04.2014; Privacy International.

Esialgse IKS-i väljatöötamisel lähtuti konventsioonis 108 ning direktiivis sätestatud põhimõtetest.¹¹³ Aastal 2003 uuendati seadust seoses direktiivi ülevõtmisega ning viidi see direktiiviga kooskõlla.¹¹⁴ Aastal 2004 kehtima hakanud IKS rakendamisel ilmnis mitmeid sisulisi probleeme, millest tulenevalt tekkis vajadus seadust aastal 2007 uuesti reformida.¹¹⁵ Uue IKS-i kehtestamise eesmärgiks ei olnud muuta isikuandmete kaitse põhimõtteid, vaid kõrvaldada 2003. aasta seaduse kitsaskohad ning arendada juba olemasolevat õiguslikku raamistikku.¹¹⁶

Isikuandmete kaitse seaduse eesmärk on vastavalt § 1 lg-le 1 sarnaselt direktiivile kaitsta isikuandmete töötlemisel füüsilise isiku põhiõigusi- ja vabadusi, eelkõige õigust eraelu puutumatusel.

IKS lähtub oma eesmärkides nii EIÕK artiklis 8 kui harta artiklis 8 sätestatud põhiõiguste kaitsmisest. Seonduvalt konventsiooniga 108 on IKS seletuskirjas märgitud, et IKS, sarnaselt direktiivile, näeb ette konventsiooniga 108 võrreldes kõrgemad nõuded isikuandmete kaitsele, kuid tugineb üldpõhimõtete sõnastamisel muuhulgas ka konventsioonis 108 sätestatud põhimõtetele.¹¹⁷

IKS kohaldumisalast jääb välja isikuandmete töötlemine füüsilise isikute poolt isiklikul otstarbel ning isikuandmete edastamine läbi Eesti territooriumi neid töötlemata. Kriminaal- ja kohtumenetlusega seonduvalt kohaldatakse IKS-i vastavatest menetlusseadustest tulenevate eristustega. Samuti on IKS kohaldumisalast välistatud isikuandmeid sisaldava teabe avalikustamine avalike ülesannete täitjate poolt, kuna seda küsimust reguleerib avaliku teabe seadus.

Algselt kehtestatud IKS oli mõeldud isikuandmete kaitse regulatsiooni üldosana, kuid eriseadusi spetsiifiliste valdkondade kehtestamiseks loodud ei ole. Sellest tulenevalt on IKS üldsõnaline ja kohati lünklik ning sama üldsõnaline, kui on direktiiv ise.¹¹⁸

Report: Lithuania. Chapter I - legal framework. Available: <https://www.privacyinternational.org/reports/lithuania/i-legal-framework>, 29.04.2014.

¹¹³ E. Rohtmets. Isikuandmete kaitse küsimused Euroopa Kohtu eelotsustes. Kohtupraktika analüüs. Tartu: Riigikohus, õigusteabe osakond 2013, lk 5. - Arvutivõrgus: http://www.riigikohus.ee/vfs/1455/Andmesubjekti%20oigused_EK_analuus.pdf, 29.04.2014.

¹¹⁴ *Ibid*, lk 6.

¹¹⁵ E. Tikk, A. Nõmper, lk 69.

¹¹⁶ Isikuandmete kaitse seaduse eelnõu. 1026 SE, lk 1.

¹¹⁷ *Ibid*, lk 2.

¹¹⁸ E. Rohtmets, L. Kanger. Eesti andmekaitse Euroopa Kohtu praktika peeglis. - Riigikogu toimetised 2013/28. Arvutivõrgus: <http://www.riigikogu.ee/rito/index.php?id=14437>, 29.04.2014.

Aastal 2011 justiitsministeeriumi analüüsis jõuti järeldusele, et IKS sisaldab siiani mitmeid probleemseid kohti, muuhulgas nii kohaldamisala, andmesubjekti õiguste kui ka andmesubjekti nõusolekuta andmete töötlemisega seondult. Eelkõige rõhutati, et isikuandmete töötlejate jaoks ei ole töötlemise õiguslikud alused piisavalt selged, samuti ei ole tagatud piisavalt tõhus järelevalve isikuandmete töötlemise üle. Eraldi regulatsiooni vajaks isikuandmete töötlemine töösuhete kontekstis.¹¹⁹

1.4 Vahekokkuvõte

Üksikisikute õiguste parimaks võimalikuks kaitseks on vaja tunnustada õigust isikuandmete kaitsele õigusaktides ning kehtestada vastav regulatsioon selle õiguse tagamiseks. Rahvusvahelised instrumendid on oma iseloomu tõttu pigem üldised ja abstraktsed ega suuda pakkuda lahendusi spetsiifilistes olukordades, samuti puudub nende aktide efektiivne jõustamismehhanism. Euroopa Liidu tasandil andmete töötlemise reguleerimiseks ei ole rahvusvahelised õigusaktid sobivad ka seetõttu, et ei arvesta Euroopa Liidu siseturu vajadustega tagada isikuandmete võimalikult kiire ja efektiivne edastamine siseturul.

Aastal 2000 vastu võetud harta sätestab võrreldes varasemaga õiguse isikuandmete kaitsele kui põhiõiguse, kuid selle põhiõiguse tagamist reguleeriv direktiiv ei täida oma eesmärke. Direktiiv ei vasta viimasel aastakümnel toimunud hüppelist tehnoloogia arengule, samuti on jätkuvalt probleeme direktiivi inkorporeerimisega siseriiklikesse õigustesse ning tõlgendamisega.

Eesti IKS on küll direktiiviga kooskõlas, kuid suuresti üle võetud sama abstraktsuse astmega. Sellest tulenevalt ei suuda IKS tagada üksikisikute õiguste parimat võimalikku kaitset, IKS-i regulatsioon on üldsõnaline ja ebamäärane.

Eeltoodust tulenevalt saab teha järelduse, et olemasolevad õigusaktid ei ole piisavad, rahuldamiseks kahte Euroopa Liidu peamist vajadust isikuandmete töötlemisega seondult: andmesubjektide õiguste kõrgeim võimalik kaitse ning andmete vaba liikumine Euroopa Liidu siseturul ja liikmesriikide ning kolmandate riikide vahel. Töö autor nõustub Euroopa Komisjoni seisukohaga, et aastaks 2010, kui algatati isikuandmete kaitse regulatsiooni reform, oli Euroopa Liidus tekkinud vajadus uueks õigusinstrumendiks.

¹¹⁹ M. Hirvoja. Õiguspoliitika arengutest ja justiitsministeeriumi rollist selles. 28.01.2011, lk 21. Arvutivõrgus: <http://www.just.ee/53263>, 29.04.2014.

2. ISIKUANDMETE KAITSE ÜLDMÄÄRUSE PEAMISED EESMÄRGID

2.1 Isikuandmete kaitse regulatsiooni reform

Isikuandmete kaitse regulatsiooni reformimine otsustati sidusrühmadega konsulteerimise tulemusena ning reformi initsiaatoriks ning eestvedajaks on Euroopa Komisjon eesotsas Euroopa Liidu õigusvoliniku Viviane Reding'iga. Probleemide kaardistamiseks korraldas komisjon mitmeid arutelusid, sihipäraseid konsulteerimisi huvigruppidega, konverentse ja ümarlaua.¹²⁰ Probleemid direktiiviga ilmnesid juba aastal 2003 tehtud esimesest ülevaatest direktiivi kohaldamise efektiivsuse kohta, kuid siis otsustati, et liikmesriikidele on vaja anda täiendavalt aega oma siseriiklike õiguste vastavusse viimiseks.¹²¹ Aastal 2010 väljastas komisjon teatise „Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus“ (edaspidi komisjoni 2010 teatis),¹²² millest nähtus, et direktiiviga seonduvaid probleeme pole jätkuvalt suudetud kõrvaldada. Kehtiva õigusliku regulatsiooni probleemide kaardistamisel kasutas komisjon ka aastal 2011 läbi viidud Eurobaromeetri uuringut.¹²³

Pärast peamiste probleemide välja selgitamist tegi Euroopa Komisjon 25.01.2012 ettepaneku isikuandmete kaitse regulatsiooni kõikehõlmavaks ja laiaulatuslikuks reformiks. Komisjoni reformipaketti kuulusid üldmäärus ja direktiiv, neid saatev seletuskiri,¹²⁴ aastal 2012 koostatud koostati üldmääruse ja kavandatava direktiivi mõjuanalüüs¹²⁵ ning komisjoni täiendav teatis (edaspidi komisjoni 2012 teatis).¹²⁶

¹²⁰ Euroopa Komisjoni eelnõu seletuskiri „Euroopa Parlamendi ja nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta.“ KOM(2012) 11. Brüssel: 25.01.2012, lk 3. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_et.pdf, 29.04.2014.

¹²¹ European Commission report, 2003.

¹²² Euroopa Komisjoni teatis Euroopa Parlamendile, nõukogule, majandus- ja sotsiaalkomiteele ning regioonide komiteele. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus. KOM(2010) 609 lõplik. Brüssel: 04.11.2010. Arvutivõrgus: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_et.pdf, 29.04.2014.

¹²³ Special Eurobarometer 359. Attitudes on data protection and electronic identity in European Union. Brussels: 2011. Available: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, 29.04.2014.

¹²⁴ Euroopa Komisjoni isikuandmete kaitse üldmääruse eelnõu seletuskiri.

¹²⁵ European Commission staff working paper. Impact assessment. SEC(2012) 72 final. Brussels: 25.01.2012. Available: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf, 29.04.2014.

¹²⁶ European Commission communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century. COM(2012) 09 final. Brussels: 25.01.2012. Available: <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012DC0009>, 29.04.2014.

Komisjon tegi ulatuslikku eeltööd. Pea kõik liikmesriigid ja huvigrupid on nõustunud komisjoni poolt välja toodud reformi lähtekohtade ja poliitiliste eesmärkidega.¹²⁷ Eesti on avaldanud seisukoha, milles toetatakse andmekaitse reformi üldiseid eesmärke ning rõhutatakse vajadust leida infoühiskonnale sobiv tasakaal andmete vaba liikumise ning eraelu puutumatuse vahel, mis tähendab direktiivis kehtestatud miinimumstandardite laiendamist. Samuti nõustutakse vajadusega vähendada ettevõtete halduskoormust ning lahendada direktiiviga tekkivaid kohalduva õiguse küsimusi.¹²⁸

Vastavalt Euroopa Liidu „Parema õigusloome“ poliitikale, kaaluti isikuandmete kaitse reformimisel kolme võimalikku varianti regulatsiooni täpsustamiseks ja täiendamiseks: võimalust täiendada regulatsiooni mittesiduvate teatiste ja suunistega ning kasutades suunavaid meetmeid nagu rahastusprogramme; adresseerida isikuandmete kaitse regulatsioonis tekkinud küsimused seadusandlikul tasandil läbi kehtiva regulatsiooni täpsustamise või koondada andmekaitse Euroopa Liidu tasandil läbi täpsete ja detailsete reeglite EL pädevusse ning luua EL institutsioon nende reeglite täitmise jälgimiseks. Lõpuks otsustati teise variandi kasuks ning regulatsiooni otsustati reformida üldmääruse abil, kuna teised meetmed ei olnud sobilikud ületamaks siseriiklike õiguste killustatuse probleemi ning kolmas variant ei olnud kooskõlas subsidiaarsuspõhimõttega.¹²⁹

Üldmääruse kehtestamise volitus sisaldub Euroopa Liidu toimimise lepingu¹³⁰ (edaspidi ELTL) artiklis 16 lg 2, mille kohaselt võivad Euroopa Parlament ja nõukogu kehtestada seadusandliku tavamenetluse kohaselt eeskirjad füüsiliste isikute kaitse kohta. Vastavalt ELTL artiklile 288 võtavad Liidu pädevuse teostamisel institutsioonid muuhulgas vastu määruseid ja direktiive.

12.03.2014 kiitis Euroopa Parlament üldmääruse esimesel lugemisel heaks – üldmääruse poolt andsid hääle 621 saadikut, vastu oli 10 ning erapooletuid 22; direktiivi poolt andsid hääle 371 saadikut, vastu olid 276 ning erapooletuid 30. Euroopa Parlamendi

¹²⁷ The Council of European Union press release. 3279th Council meeting. Justice and home affairs. PR CO(2013) 17342. Brussels: 05. - 06.12.2013, p 2. Available: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/139938.pdf, 29.04.2014; The United Kingdom Ministry of Justice. Impact assessment: Proposal for an EU data protection regulation. 22.11.2012, p 5. Available: Proposal for an EU Data Protection Regulation - government impact assessment, 29.04.2014.

¹²⁸ Vabariigi Valitsuse 29.03.2012 otsuse seletuskiri, lk 6.

¹²⁹ Euroopa Komisjoni isikuandmete kaitse üldmääruse eelnõu seletuskiri, lk 4 ja 5.

¹³⁰ Euroopa Liidu toimimise lepingu konsolideeritud versioon. - ELT C 326/1, 26.10.2012, lk 47-200.

koosseisumuutus seoses 2014 aasta mais toimuvate valimistega ei saa enam mõjutada parlamendi positsiooni andmekaitse reformi paketi osas.¹³¹

Vaatamata põhimõttelisele üksmeelele isikuandmete kaitse regulatsiooni reformi lähtepunktide osas, on komisjoni poolt välja pakutud ning kodanikuvabaduste, justiits- ja siseasjade komisjoni poolt täiendatud lahendused eesmärkide saavutamiseks tekitanud palju pahameelt erinevate huvigruppide seas, muuhulgas ei ole erimeelsustest tulenevalt oma seisukohti veel lõplikult kujundanud Euroopa Nõukogu.¹³² Kodanikuvabaduste, justiits- ja siseasjade komisjonile laekus esialgse üldmääruse eelnõule 4000 parandusettepanekut nii ettevõtjatelt, üksikisikutelt, kolmanda sektori esindajatelt kui ka teistelt komisjonidelt.¹³³

Komisjoni poolt pakutud lahendustele lisaks on kritiseeritud ka asjaolu, et komisjon on eiranud komisjonisisest sõltumatu mõjuanalüüsi nõuet.¹³⁴ Euroopa Mõjuanalüüsi Nõukogu, mis hindab Euroopa Komisjoni poolt tehtud mõjuanalüüsi, andis üldmäärust puudutavale mõjuanalüüsile pigem negatiivse hinnangu ning rõhutas vajadust mõjude detailsemaks analüüsiks.¹³⁵ Täiendavat mõjuanalüüsi komisjoni poolt tehtud ei ole. Lisaks on olemasolevale mõjuanalüüsile ette heidetud seda, et selles puudub mõjuhindang liikmesriikidele, ettevõtlust puudutavaid hinnanguid on nimetatud lausa fantaasiaks.¹³⁶

2.2 Vajadus tugevdada andmesubjektide õiguste kaitset

Tulenevalt harta artiklist 8 on õigus isikuandmete kaitsele Euroopa Liidu õiguses fundamentaalne õigus. Vajadus tagada harta artiklist 8 tuleneva õiguse kaitse on üks reformi

¹³¹ European Commission MEMO. Progress on EU data protection reform now irreversible following European Parliament vote. MEMO/14/186. Brussels: 12.03.2014. Available: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm, 29.04.2014.

¹³² C. Cuijpers *et al*, p 1-2.

¹³³ C. Kuner, C. Burton, A. Pateraki. The Proposed EU Data Protection Regulation Two Years Later. - Privacy and security law report. 2014, p 2. Available: <http://www.wsgr.com/eudataregulation/pdf/kuner-010614.pdf>, 01.05.2014.

¹³⁴ A. Barberis, the president of Eurochamber. Letter to mr José Manuel Barroso. Impact assessment on data protection Directive / Regulation (COM 2012 10 & 11). Brussels: 13.02.2012. Available: <http://www.eurochambres.eu/Content/Default.asp?PageID=1&DocID=4212>, 29.04.2014; V.Peep. Andmekaitse Inspektisoon Euroopa Komisjoni algatatud andmekaitsereformist. 07.06.2012, lk 1. Kättesaadav: www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Andmekaitse%20Inspektisoon%20Euroopa%20Komisjoni%20algatatud%20reformist%2008.6.2012.rtf, 29.04.2014.

¹³⁵ European Commission Impact Assessment Board. Opinion. DG JUST - Impact assessment on reform of personal Data protection in EU. D(2011). Brussels: 09.09.2011. Available: http://ec.europa.eu/smart-regulation/impact/ia_carried_out/docs/ia_2012/sec_2012_0074_en.pdf, 30.04.2014.

¹³⁶ V. Peep. Andmekaitse Inspektisoon Euroopa Komisjoni algatatud andmekaitsereformist. 07.06.2012. Arvutivõrgus: <http://tinyurl.com/p22wdl3>, 29.04.2014.

peamiseid eesmärke.¹³⁷ Üldmääruse preambula 5 kohaselt on üldmäärus ajendatud vajadusest võimaldada andmete vaba liikumist tagades samal aja isikuandmete kõrgetasemeline kaitse.

Aastal 2011 avalikustatud Eurobaromeetri uuringu kohaselt kardab 70% küsitletud eurooplastest, et nende isikuandmeid kasutatakse muudeks eesmärkideks, kui see, milleks need on kogutud; 75% küsitletutest sooviksid võimalust kustutada veebilehelt igal hetkel oma andmeid; 32% küsitletutest usaldab telefonioperaatoreid ja interneti teenusepakkujaid ning 22% usaldab internetiteenuseid nagu otsingumootoreid, sotsiaalvõrgustikke ja e-kirja teenuseid. Samas peavad 74% küsitletutest isikuandmete avalikustamist paratamatuks osaks tänapäeva elust.¹³⁸

Eeltoodust nähtub, et inimeste usaldus seonduvalt nende isikuandmete töötlemisega on väga madal, teisalt on vajadus isikuandmete avaldamiseks paratamatu. Eurobaromeetri uuringust nähtuvalt on madal usaldus otseselt seotud sellega, et andmesubjektid tunnevad, et neil puudub ülevaade sellest, mida nende andmetega tehakse ning sellega, et neil pole oma andmete üle kontrolli.¹³⁹ Komisjoni 2010 teatises tuuakse isikute õiguste tugevdamise eesmärgi peamiste lähtepunktina välja vajadus suurendada läbipaistvust ja kontrolli isikuandmete töötlemisel.¹⁴⁰

2.2.1. Läbipaistvuse puudumine isikuandmete töötlemisel

Läbipaistvus isikuandmete töötlemisel on eelduseks kontrollile enda isikuandmete üle. Kui andmesubjekt ei tea, kes ja kui palju tema kohta andmeid kogub, on tal enda õiguste kaitsmine raskendatud. Selline olukord võib tulla ette näiteks veebireklaami puhul, kus osapoolte arvukuse ja tehnilise keerukuse tõttu pole võimalik mõista, kas tema kohta kogutakse isikuandmeid, kes neid kogub ning millisel eesmärgil neid kogutakse. Teiseks on märkimisväärne probleem, et isikutele esitatav teave nende andmete töötlemise kohta ei ole neile arusaadav.¹⁴¹

¹³⁷ Euroopa Komisjoni teatis. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus, lk 4.

¹³⁸ Special Eurobarometer 359, 2011, p 2.

¹³⁹ Special Eurobarometer 359, 2011, p 137.

¹⁴⁰ Euroopa Komisjoni teatis. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus, lk 5 jj; European Commission communication. Privacy in a Connected World A European Data Protection Framework for the 21st Century, ch 2.

¹⁴¹ Komisjoni teatis. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus, lk 6.

Direktiivis sätestatud üldpõhimõtete kohaselt tuleb isikuandmeid töödelda õiglaselt ja seaduslikult. Direktiivis sätestatud meetmed läbipaistvuse tagamiseks on ebapiisavad.¹⁴²

Üldmääruse artikkel 5 (a) tutvustab uue üldpõhimõttena kohustust töödelda isikuandmeid andmesubjekti jaoks läbipaistval viisil.

Eesti IKS-i regulatsioon ei erine andmesubjekti teavitamise osas direktiivist, mistõttu tooks üldmääruse kehtestamine kaasa samad põhimõttelised muudatused, mis kaasnevad võrreldes direktiiviga.

Kõige otsesemalt realiseerub läbipaistvuse põhimõtte üldmääruse artiklites 11 ja 14 sätestatud läbipaistvusprintsibiina,¹⁴³ aga kaudselt saavutatakse üldmäärusega suurem läbipaistvus ka vastutava ja volitatud töötleja vahelise vastutuse täpsustamisega.¹⁴⁴ Alljärgnevalt on käsitletud kahte läbipaistvuse suurendamiseks tutvustatud meetet – läbipaistvusprintsipi ning vastutava ja volitatud töötleja vahelist regulatsiooni.

2.2.1.1 Läbipaistvusprintsip

Ettevõtete poolt andmesubjektidele esitatud informatsioon ettevõtte privaatsusepoliitikast on tihti keeruliselt sõnastatud ning sisaldab tehnilist ja juriidilist terminoloogiat, mis ei pruugi olla andmesubjektile mõistetav.¹⁴⁵ Praegused andmetöötlejate teatised, mis sisaldavad informatsiooni andmesubjekti andmete töötlemise kohta, on keerulised, kuna need on kirjutatud juristide poolt ja juristidele ning nõuded teatistele erinevad liikmesriigiti oluliselt. Lõpptulemuseks on pikad ja segased teavitused, mis on andmesubjektile arusaamatud ning mida andmesubjekt ei loe.¹⁴⁶

Vajadust läbipaistvuse suurendamiseks isikuandmete kaitse reformimisel rõhutas juba aastal 2009 direktiivi artikli 29 alusel loodud töörühm (edaspidi töörühm).¹⁴⁷

¹⁴² N. Robinson *et al*, p 29 - 30.

¹⁴³ Euroopa Komisjoni isikuandmete kaitse üldmääruse eelnõu seletuskiri, lk 8.

¹⁴⁴ Euroopa Komisjoni isikuandmete kaitse üldmääruse eelnõu seletuskiri, lk 10.

¹⁴⁵ Commission staff working paper. Impact assessment, p 22.

¹⁴⁶ N. Robinson *et al*, p 29 - 30.

¹⁴⁷ Article 29 Data protection working party. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. The future of privacy. WP 168. Brussels: 01.12.2009, p 6, *passim*. Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf, 30.04.2014.

Üldmääruse preambulas 46 on märgitud, et läbipaistvusprintsipi eesmärgiks on tagada, et avalikkusele või andmesubjektile suunatud informatsioon oleks lihtsasti ligipääsetav ja arusaadav. Informatsiooni andmisel tuleks kasutada selget ja lihtsalt keelt.

Üldmääruse artikkel 11 (1) näeb ette, et vastutav töötleja kehtestab läbipaistvad isikuandmete töötlemise ja andmesubjektide õiguste kaitsmise põhimõtted ning teeb need lihtsalt kättesaadavaks. Artikkel 11 (2) sätestab kohustuse anda teavet isikuandmete töötlemisest arusaadavas vormis ning andmesubjektile kohandatud selges ja lihtsas keeles, eelkõige kui teavet esitatakse lapsele.

Töö autori arvates aitab artikkel 11 tutvustamine üldmääruses kaasa paremale läbipaistvusele isikuandmete töötlemisel. Andmesubjektid ei süvene nende andmete töötlemist puudutavatesse informatsiooni tihti seetõttu, et andmetöötleja poolt esitatud privaatsustingimused on väga pikad ning keeruliselt sõnastatud. Üldmääruse artikkel 11 kohustab ettevõtjaid tulema andmesubjektidele nõu poolele teele vastu, nähes ette nõude esitada informatsiooni andmesubjektile arusaadavalt. Teisalt on artikli 11 kohaldamine praktikas mõnevõrra problemaatiline. Üldmääruse artikkel 11 (2) sisaldab väga avatud mõisteid nagu “arusaadav vorm” ning “andmesubjektile kohandatud selge ja lihtne keel”. Andmesubjektide teadlikkus (ja seega võime aru saada teda puudutavatest privaatsusepoliitika sätetest) erineb oluliselt, ning “andmesubjektile arusaadav vorm” on väga individuaalne ja subjektiivne kontseptsioon. Määratlemata õigusemõisted panevad ettevõtteid keerulisse olukorda, kuna neil on raske hinnata, kas nende privaatsuspoliitika vastab üldmääruses sätestatud „arusaadavuse“ kriteeriumile või mitte. Üheks lahenduseks selle probleemi ületamiseks on pakutud võimalust lubada ettevõtetel kinnitada enda teatise vastavust tunnustatud sertifikaadiga, mida annaks välja liikmesriigi järelevalveasutus.¹⁴⁸

Üldmääruse artikkel 11 kehtestab üldised standardid, et muuta ettevõtete poolt esitatav informatsioon andmesubjektidele senisest arusaadavamaks. Eeldades, et sätte rakendamisel ei tohiks ilmnedagi väga suuri takistusi (ja/või need on ületatavad), on töö autor seisukohal, et sellise põhimõtte tutvustamine on efektiivne ning aitab kaasa isikuandmete töötlemise läbipaistvuse suurendamisele. Positiivne muutus on artiklis 11 rõhutatud vajadus tagada teabe arusaadavus eelkõige kui teavet esitatakse lapsele. Praegu kasutavad 38% lastest vanuses 9 - 12 ja 77% lastest vanuses 13-16 sotsiaalvõrgustikke, olgugi et enamike sotsiaalvõrgustike

¹⁴⁸ Passing Clouds: The EC's data protection reform plans and their relevance for cloud computing. 2013. Available: https://www.taylorwessing.com/globaldatahub/article_passing_clouds.html, 30.04.2014.

privaatsuspoliitika seda ei luba,¹⁴⁹ mistõttu on laste kaitse vajadusele tähelepanu pööramine igati õigustatud.

Üldmääruse artiklid 13a ja 14 näevad ette mitteammendava loetelu teabest, mida vastutav töötaja peab andmesubjektile isikuandmete töötlemisel esitama. Üldmääruse artikkel 13a näeb ette kohustuse veel enne andmesubjektile artiklis 14 loetletud teabe edastamist kohustuse teavitada andmesubjekti sellest, kas isikuandmeid kogutakse ja salvestatakse töötlemise eesmärgiga võrreldes suuremas ulatuses kui minimaalselt vajalik, kas andmeid kasutatakse muuks otstarbeks kui see, milleks neid koguti, kas andmeid edastatakse kolmandatele osapooltele kommertseesmärkidel ning kas andmeid salvestatakse krüpteeritult. Võrreldes direktiivi artiklitega 10 ja 11, sisaldab üldmääruse artikkel 14 täiendavalt kohustust anda infot isikuandmete säilitamise tähtaja kohta ja õiguse kohta esitada kaebus järelevalveasutusele.

Artiklites 13a ja 14 ette nähtud ulatuslike teavitamiskohustustega kaasnevad varasemast suuremad kulud.¹⁵⁰ Olukorra tasakaalustamiseks on ette nähtud üldmääruse artiklis 14 (4)(bb) erand, mille kohaselt esitatakse nimetatud informatsioon ainult andmesubjekti palvel juhul, kui andmetöötlejaks on mikro- või väikeettevõtja, kes töötleb andmeid kõrvaltegevusena. Mikro- ja väikeettevõtjaks kvalifitseerumisel lähtutakse vastavalt üldmääruse preambulale 10 komisjoni soovitusel 2003/361/EÜ sätestatud kriteeriumitest.¹⁵¹

Üldmääruse artikkel 15 näeb sarnaselt direktiiviga ette ka õiguse tutvuda enda kohta kogutavate andmetega. Üldmäärus ei sätesta aega, kaua peab andmeid säilitama, kuid artikli 15 (2b) kohaselt ei välista isiku õigus tutvuda enda kohta kogutavate andmetega andmetöötleja kohustust kustutada andmed, mis pole enam vajalikud. Selline lähenemine on kooskõlas ka Euroopa Kohtu otsusega, milles kohus leidis, et direktiiv 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ, tuleb kuulutada tühiseks.¹⁵² Euroopa Kohtu otsuse kohaselt on direktiiv 2006/24/EÜ, millega nähakse ette andmetöötlejate kohustus töödelduid

¹⁴⁹ Commission staff working paper. Impact assessment, p 23.

¹⁵⁰ N. Robinson *et al*, p 29 - 30.

¹⁵¹ Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. - ELT L 124, 20.05.2003, p 36 - 41.

¹⁵² Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, 15. märts 2006, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ.- ELT L 105, 13.04.2006 p 54-63.

andmeid 6-24 kuud säilitada, vastuolus Euroopa Liidu põhiõiguste harta artiklitega 7, 8 ja 52 (1).¹⁵³

Läbipaistvusprintsipi on kritiseeritud, kuna juba praegu on mitmed andmete töötlemist puudutavat infot sisaldavad teatise detailsed ja pikad, mistõttu ei vaevu tarbijad nendega tutvuma.¹⁵⁴

Töö autor sellise kriitikaga ei nõustu – teavituste pikkus ei ole põhjus, miks andmesubjekte nende õigustest mitte teavitada. Olukorras, kus nähakse ette üldine standard teatiste arusaadavamaks muutmiseks, suurendatakse tõenäosust privaatsuspoliitikatega tutvumiseks. Teiseks on teavituste pikkuse lühendamiseks välja pakutud nõ „kihiliste“ privaatsusteavituste loomist, kus esialgses teatises sisaldub ainult kõige olulisem info, kuid andmesubjektil on võimalik teavituses asuva viite abil avada täpsemat informatsiooni sisaldav teavitus jne.¹⁵⁵ Oluline on seega teavituste sisu arusaadavus ja mitte teavituste pikkus.

Üldmääruse artiklites 13a ja 14 ette nähtud meetmed võimaldavad andmesubjektil paremat ülevaadet tema kohta kogutud andmete eesmärgist ja hulgast. Tegemist on positiivse ja efektiivse meetmega.¹⁵⁶

2.2.1.1 Vastutava ja volitatud töötleva vaheliste kohustuste täpsustamine

Kavandatava üldmäärusega soovitakse lahendada isikuandmete töötlevate vastutuse ebaselgus. Suur osa isikuandmete töötlemisest toimub pilvandmetöötlemise raames. See tähendab, et andmeid ei salvestata füüsilistele andmekandjatele, vaid andmete kogumine, salvestamine ja töötlemine toimub nõ suures pilves. Pilvandmetöötlemise puhul on tavaline, et teenusepakkujad ehk pilve haldajad pakuvad teenuseid erinevatele internetiteenuse pakkujatele, kes omakorda pakuvad üksikisikutele nende andmete töötlemisega seonduvat teenust. Pilvandmetöötlemises osaleb seega mitmeid töötlevaid, mistõttu võib andmesubjektil osutada raskeks tuvastada, kes täpselt ning millises ulatuses andmeid töötleb. Pilvandmetöötlemise teenuse ostja kui vastutav töötleva (näiteks mõni sotsiaalvõrgustik) ostab pilvandmetöötlemise teenust ning teenusepakkuja

¹⁵³ EKO 08.04.2014, C-293/12, C-594/12, *Digital Rights Ireland Ltd jt*, § 69.

¹⁵⁴ European Payment Institutions Federation. EPiF's position paper on the European Commission's proposal for a general data protection regulation. 26.04.2013, p 3. Available: <http://www.paymentinstitutions.eu/documents/download/17/attachement/epif-position-paper-on-the-proposed-general-data-protection-regulation.pdf>, 28.04.2014.

¹⁵⁵ N. Robinson *et al*, p 43.

¹⁵⁶ Samal seisukohal on ka Euroopa Andmekaitseinspektor. Vt: European Data Protection Supervisor. On the data protection reform package. Brussels: 12.03.2012, p 22. Available: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf, 30.04.2014.

kui volitatud töötaja volitab erinevad osad andmetöötlusprotsessist ja erinevad andmed edasi teistele andmetöötajatele. Sellises pikas andmetöötlusahelas ei ole tihti selge, kuidas jaguneb andmetöötlusprotsessis osalejate vastutus.¹⁵⁷ Direktiivi regulatsioon on selles osas iganenud ega paku piisavat kaitset.¹⁵⁸

Üldmäärusega nähakse ette vastutuse printsiip, mis nõuab vastutavalt töötajalt esiteks meetmete rakendamist, mis tagaks andmete töötlemise kooskõlas üldmääruses sätestatuga ning teiseks, et vastutav töötaja oleks võimeline järelevalveasutuse palvel neid meetmeid ka demonstreerima.¹⁵⁹ Üldmääruse artikli 5 (f) kohaselt töödeldakse isikuandmeid vastutava töötaja kohustuste raames ja vastutusel ning vastutav töötaja tagab ja tõendab, et töötlemistoimingud vastavad üldmäärusele, artikkel 22 täpsustab artiklis 5 (f) üldist printsiipi ning sätestab nimekirja vastutava töötaja kohustustest, muuhulgas nähakse ette ka vastutava töötaja kohustus teostada volitatud töötaja poolt kasutatud meetmete üle kontrolli.

Artikkel 23 sätestab, et üldmäärusega kehtestatakse täiendavalt kaasvastutavate töötajate vastutus (art 24) ning määratakse kindlaks ka volitatud töötaja ülesanded (art 26). Eraldi väärrib väljatoomist artikkel 26 (2)(d), mille kohaselt võib teisi töötajaid kaasata üksnes vastutava töötaja eelneval loal. Sealjuures on tähelepanuväärne, et IKS § 7 lg 5 sätestab selle nõude juba praegu, kuid direktiivis vastavasisuline säte puudub. Vastutaval töötajal on kohustus 24 tunni jooksul teavitada järelevalveasutust isikandmete töötlemisega seotud rikkumistest (art 31 (1)).

Vastutava töötaja vastutuse printsiibi kindlustamiseks on üldmääruse artiklites 32a ja 33 ette nähtud vastutava töötaja kohustus teatud tingimustel hinnata isikuandmete kaitsese avaldatavat mõju. Artikkel 35 näeb ette andmekaitseametniku ametisse määramise, kui tegemist on avaliku sektori asutusega, erasektori asutusega, kus on rohkem kui 250 töötajat või kui vastutava töötaja peamiseks tegevuseks andmete töötlemisel on andmesubjektide tegevuse regulaarne ja süstemaatiline jälgimine.

¹⁵⁷ Article 29 Data Protection Working Party. Opinion 05/2012 on cloud computing. WP 196. Brussels: 01.07.2012, p 9. Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf, 30.04.2014.

¹⁵⁸ N. Robinson *et al*, p 35.

¹⁵⁹ Vastutuse printsiibi tutvustamise vajadust on jaatanud nii töörühm kui ka Euroopa Andmekaitseinspektor: Article 29 Data Protection Working Party. Opinion 3/2010 on the principle of accountability. WP 173. Brussels: 13.07.2010, p 8. Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf, 30.04.2014; European Data Protection Supervisor, p 27.

Vastutava ja volitatud töötaja vastutuse sätestamine ja piiritlemine on üldmäärukses laias laastus õnnestunud, kuigi mõned sätted on jäetud liiga üldsõnaliseks ning mõned defineeritud liiga spetsiifiliselt.¹⁶⁰

Töö autor on seisukohal, et terve uue peatüki lisamine üldmääruksesse on võrreldes direktiivis sätestatud kahe vastutava ja volitatud töötaja vastutust puudutava sättega vaatamata mõningatele puudustele arvestatav edasimineku suurema läbipaistvuse tagamisel. Üldmäärus sätestab varasemast selgemini vastutava töötaja vastutuse ja ülesanded, samuti näeb ette riskide maandamise ja sisekontrollinõuded. Reguleerimine parandab isikute õiguste kaitset, kuna võimaldab paremat ülevaadet andmetöötajate ringist ning nende omavahelistest kohustustest nii andmetöötajatele endale kui andmesubjektidele ning on seetõttu efektiivne meede isikuandmete töötlemise läbipaistvuse suurendamisel.

2.2.2 Andmesubjekti kontrolli tõhustamine enda isikuandmete üle

Euroopa Komisjon on isikuandmete kõrgetasemelise kaitse eeldusena nimetanud andmesubjekti õigust omada efektiivset kontrolli enda andmete üle.¹⁶¹ Vastavalt Eurobaromeetri uuringule tundis ainult 26% sotsiaalmeedia kasutajatest ning 18% internetikaubanduse võimaluste kasutajatest, et omavad oma andmete üle täielikku kontrolli, 72% küsitletutest kardab, et nende kohta kogutud andmeid kuritarvitatakse.¹⁶²

Probleemi ilmestab Austria tudengi Max Schrems'i kohtuasi, mis on töö kirjutamise hetkel veel arutamisel Iirimaa Ülemkohtus. Esitatud kaebuse kohaselt sai noormees sotsiaalmeediavõrgustikult *Facebook* üle 1200 lehekülje andmeid, mida oli tema kohta rohkem kui kolme aasta jooksul kogutud. Andmetest nähtuvalt talletas *Facebook* muuhulgas ka informatsiooni, mida Max Schrems sotsiaalmeediavõrgustiku kasutajana enda arvates oli kustutanud – näiteks eraelulisi detaile sisaldavaid sõnumeid, samuti kogus *Facebook* infot andmesubjekti kohta ilma andmesubjekti teavitamata.¹⁶³

¹⁶⁰ C. Cuijpers *et al*, p 17; Samal arvamusel: W. K. Hon, E. Kosta, C. Millard, D. Stefanatou. Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation. London: Queen Mary University of London, School of law, 2014, p 14 - 15. Available: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2405971, 30.04.2014; P. M. Schwartz. The EU - U.S. privacy collision: a turn to institutions and procedures. Harvard Law Review 2013/1966, p 2002-2003.

¹⁶¹ Euroopa Komisjoni teatis. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus, lk 7.

¹⁶² Commission staff working paper. Impact assessment, p 23.

¹⁶³ Kohtusse esitatud 22 kaebuse tekstid ning muu kaebusi puudutav materjal. Vt: Europe vs Facebook. Legal procedure against Facebook Ireland Limited. Available: <http://europe-vs-facebook.org/EN/Complaints/complaints.html>, 30.04.2014.

Üldmäärusega kaasnevast mõjuanalüüsist nähtuvalt on eriti oluline tagada üksikisikute kontroll enda isikuandmete üle profileerimise, andmekaeve ja tehnoloogiliste uuenduste tõttu, mis lihtsustavad isikuandmete vahetamist ja töötlemist.¹⁶⁴

Eesmärgiga suurendada üksikisikute kontrolli enda andmete töötlemisel on nii komisjoni 2010 teatises¹⁶⁵ kui ka komisjoni 2012 teatises¹⁶⁶ toonud lahendusena välja kaks peamist viisi kontrolli suurendamiseks ja tugevdamiseks: esiteks õigust olla unustatud ja õigust oma andmete kustutamisele, mis tähendab andmesubjekti õigust nõuda vastutavalt töötlejalt ennast puudutavate andmete täielikku kustutamist ning teiseks õigust andmete ülekantavusele, mis hõlmab andmesubjekti õigust nõuda töödeldavate andmete kohta koopiat ning edastada teavet teisele teenusepakkujale.¹⁶⁷

2.2.2.1 Õigus olla unustatud ja õigus andmete kustutamisele

Komisjon on õigust olla unustatud ja õigust andmete kustutamisele (millest on kodanikuvabaduste, justiits- ja siseasjade komisjoni muudatuste tagajärjel saanud ainult õigus andmete kustutamisele)¹⁶⁸ nimetanud lausa üheks neljast reformi alussambast.¹⁶⁹ Õigus enda andmete kustutamisele suurendab andmesubjekti kontrolli oma andmete üle läbi selle, et annab andmesubjektile õiguse otsustada, mis saab tema andmetest ka pärast andmete avalikustamist, st õiguse need andmed internetiavarustest nõ “tagasi küsida.” Üldmäärusega ette nähtud õigus tugineb põhimõttele, et andmesubjekt omab enda kohta käivaid andmeid.¹⁷⁰

Direktiivi artikkel 12 (b) näeb ette andmesubjekti võimaluse vastavalt vajadusele parandada, kustutada või sulgeda need andmed, mille töötlemine ei vasta direktiivi sätetele, eelkõige seetõttu, et andmed on ebatäielikud või ebaõiged. Kavandatud reformiga soovitakse seda õigust täpsustada ning täiendada,¹⁷¹ kuna praktikas on andmesubjektil direktiivi alusel selle

¹⁶⁴ Commission staff working paper. Impact assessment, p 23.

¹⁶⁵ Euroopa Komisjoni teatis. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus, lk 8; Commission staff working paper. Impact assessment, p 28.

¹⁶⁶ European Commission communication. Safeguarding Privacy in a Connected World, p 2.

¹⁶⁷ Euroopa Komisjoni teatis. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus, lk 8.

¹⁶⁸ Data Guidance. EU right to be forgotten now right to erasure. 2013, p 10. Available: http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2119, 30.04.2014.

¹⁶⁹ European Commission MEMO 12.03.2014.

¹⁷⁰ V. Reding. The EU Data Protection Reform 2012: Safeguarding Privacy in a Connected World. Speech. 25.01.2012, p 4. Available: http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/data-protection-reform2012_en.pdf, 30.04.2014.

¹⁷¹ Euroopa Komisjoni teatis. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus, lk 7.

õiguse maksmata panemine vastutava töötaja suhtes oluliselt raskendatud ning võimalused erinevad liikmesriigiti oluliselt.¹⁷²

Õigus andmete kustutamisele üldmääruse eelnõus tähendab, et andmesubjektil on õigus teatud tingimustel paluda internetiteenuse pakkujalt oma isikuandmete kustutamist. Õigus andmete kustutamisele on isikul juhul vastavalt üldmääruse artiklile 17 kui: 1) andmeid ei ole enam vastavalt nende kogumise eesmärgile vaja; 2) andmesubjekt võtab tagasi oma nõusoleku andmete töötlemiseks; 3) andmete säilitamise tähtaeg on möödunud; 4) andmesubjekt vaidlustab andmete töötlemise vastavalt artiklis 19; 5) andmete töötlemise kohustus on ette nähtud jõustunud kohtuotsuses; 6) andmete töötlemine toimub õigusliku aluseta. Kui isikuandmed on avalikustatud ilma õigusliku aluseta, on teenusepakkujal kohustus teavitada ka teisi, kes kasutavad viiteid samadele andmetele või omavad andmetest koopiaid, et viimased kustutaks samuti need andmed.

Üldmääruse artikkel 17 (2) näeb ette vastutava töötaja kohustuse võtta tarvitusele kõik mõistlikud abinõud, et andmed kustutatakse, kaasarnatud kolmandate osapoolte poolt, kui andmed on avalikustatud ilma seadusliku aluseta. Võimaluse korral teavitab vastutav töötaja andmesubjekti tähtsustavate kolmandate osapoolte tegevusest.

Kavandatavate muudatusega soovitakse ümber pöörata tõestuskoormis – kui varem oli andmesubjekti kohustus tõendada, miks andmeid ei tohiks enam töödelda, siis nüüd on see ettevõtte kohustus tõendada, miks on vajalik andmete jätkuv töötlemine.¹⁷³

Õigus andmete kustutamisele on saanud ulatuslikku kriitikat. Kaks peamist põhjust, miks kavandatavad õigust kritiseeritakse on kaheldavus selle põhimõtte rakendamises reaalsuses ning probleemid, mis seonduvad sõnavabadusega.

Euroopa Andmekaitseinspektor on seisukohal, et põhimõtte, mida artikkel 17 endas kannab, on teretulnud ja vajalik, kuid peab olema rakendatav ka reaalsuses. Teatud juhtudel võib kõikide kolmandate osapoolte teavitamine olla vastutavale töötajale tohutu pingutus, kuna puudub ülevaade sellest, kelle kätte andmed on jõudnud.¹⁷⁴ Töörühm on märkinud, et kuigi sellise õiguse tutvustamine on tervitatav, ei vasta üldmääruses sätestatud regulatsioon

¹⁷² G. Zanfir. The right to Data portability in the context of the EU data protection reform. - International Data Privacy Law 2012/2, No. 3, p 156.

¹⁷³ European Commission MEMO. Data Protection Day 2014: Full Speed on EU Data Protection Reform. MEMO/14/60. Brussels: 27.01.2014. Available: http://europa.eu/rapid/press-release_MEMO-14-60_en.htm, 30.04.2014.

¹⁷⁴ European Data Protection Supervisor, p 24.

tegelikkusele sellest, kuidas internet töötab.¹⁷⁵ Suurbritannia justiitsminister on asunud seisukohale, et sätte pealkiri tekitab ebarealistlikke ootusi, kuna lubab palju, tekitades ebarealistlikke ootusi, kuid praktikas võimaldab vähe.¹⁷⁶ Praktikas toimub internetis andmete töötlemine ja taaskasutamine nii kiiresti ja nii suures ulatuses, et vastutaval töötlejal on sisuliselt võimatu omada ülevaadet kõikidest kolmandatest osapooltest, kes võivad avaldatud andmeid taasavaldada.

Üheks peamiseks probleemiks on see, et ka vastutav töötleja ei pruugi olla teadlik kõigist kolmandatest osapooltest, kes on asunud andmeid töötleva. Samuti ei ole üldmääruses sätestatud kolmandate isikute kohustust andmesubjekti palvel andmete kustutamiseks, kui tegemist ei ole vastutava töötlejaga. Reguleerimata on jäänud ka olukord, kus vastutavat töötlejat enam ei eksisteeri või temaga ei ole võimalik kontakteeruda.¹⁷⁷

Asjaolu, et vastutavatel töötlejal lasub kohustus ise ühendust võtta kolmandate osapooltega, kes on vastutavate töötlejate poolt avaldatud andmeid samuti kasutanud, suurendab oluliselt nende töökoormust ning sellele on vastu suured ettevõtted nagu *Facebook* ja *Google*,¹⁷⁸ aga ka mitmed liikmesriigid, eesotsas Suurbritanniaga.¹⁷⁹ Kohustus paneb olulise koormuse just otsingumootori teenuseid pakkuvatele ettevõtjatele, kes peaksid õiguse teostamisel tagama, et kustutatavad andmed enam otsingumootoris päringu tegemisel ei ilmu. See aga väga keeruline ja kulukas.

Euroopa Kohtus on arutlusel kohtuasi, kus isik palus *Google*'il eemaldada kaks tema isikuandmeid sisaldavad ajaleheartiklit, mis ilmuvad vastena andmesubjekti nime sisestamisele *Google*'i otsingumootoris. Kohtujuristi arvamuse kohaselt ei tulene praegu kehtivast direktiivist absoluutset õigust andmete kustutamisele, mis hõlmaks andmete kustutamise alusena andmesubjekti subjektiivseid eelistusi, vaid kohaldada tuleb selliseid kriteeriume nagu töötlemise eesmärk ja sellega teenitavad huvid võrrelduna andmesubjekti omadega. Kohtujurist on asunud seisukohale, et otsingumootori teenuse pakkujale sellise

¹⁷⁵ Article 29 Data Protection Working Party. Opinion 01/2012 on the data protection reform proposals. WP 191. Brussels: 23.03.2012, p 13. Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf, 30.04.2014. Samal arvamusel: C. Cuijpers *et al*, p 13.

¹⁷⁶ The United Kingdom Ministry of Justice. Government response to Justice Select Committee's opinion on the European Union Data Protection framework proposals. January 2013, p 7. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/217296/response-eu-data-protection-framework-proposals.pdf, 29.04.2014.

¹⁷⁷ Article 29 Data protection Working Party, Opinion 01/2012, p 14.

¹⁷⁸ EK 25.06.2013, C-131/12, *Google Spain SL*, kohtujurist N. Jääskinen ettepanek, § 22.

¹⁷⁹ The United Kingdom Ministry of Justice, 2013, p 7.

kohustuse ette nägemine, mille kohaselt tuleks vastavalt andmesubjekti soovile andmed otsingumootorist kustutada, on eaproportsionaalselt koormav ning vastuolus ka veebilehe avaldaja sõnavabadusega, kelle veebilehelt andmed maha võetakse.¹⁸⁰ Kodanikuvabaduste, justiits- ja siseasjade komisjoni poolt tehtud muudatused on kooskõlas kohtujuristi arvamusega viidatud kohtuasjas, kuna piiravad õigust nõuda andmete kustutamist artiklis 17 (1) toodud alustel.

Eesti on Euroopa Liidu justiits- ja siseministrite 17. ja 18. jaanuari 2013. a mitteametlikul kohtumisel väljendanud seisukohta, et õigus andmete kustutamisele ei tohiks kehtida avaliku sektori valduses olevate andmete kohta. Samuti väljendas Eesti seisukohta, et nõue teavitada andmete kustutamise soovist kolmandaid isikuid on ebamõistlik.¹⁸¹

Euroopa Komisjoni arvates tasakaalustab ettevõtetele asetavat koormust üldmääruse artikli 17 (2) sõnastus, mille kohaselt on vastutava töötaja kohustuseks võtta tarvitusele kõik võimalikud abinõud, et ka kolmandad osapooled oleksid andmesubjekti soovidest teadlikud ning keegi ei eelda, et vastutav töötaja suudaks kustutada kõik olemasolevad isikuandmed internetis. Sõnastus „*võtta tarvitusele kõik võimalikud abinõud*“ ei tähenda komisjoni arvates enamikel juhtudel muud, kui ühe e-kirja saatmist.¹⁸²

Komisjoni selline seisukoht kinnitab eelnevalt väljendatud muret, et üldmääruse rakendamine praktikas võib osutuda keeruliseks ning mitte väga tulemuslikuks. Umbmäärane kohustus teha vastutava töötaja poolt kõik endast olenev, olukorras, kus tal ei olegi võimalik teada kõiki kolmandaid osapooli, seab üldmäärusega taotletava parema kontrolli saavutamise reaalsuses kahtluse alla.

Töö autor nõustub töörühma poolt väljendatud seisukohaga, mille kohaselt peaks lisaks artiklis 17 sätestatud õigusele praeguses vormis kaaluma ka andmesubjektide pöördumist otse kolmandate osapoolte poole.¹⁸³ Selline lähenemine tasakaalustaks paremini ka andmesubjekti õigusi ja kohustusi, kuna olukorras, kus isik on näiteks sotsiaalvõrgustikku lisanud endast piinliku pildi, ei peaks kogu vastutus selle pildi eemaldamiseks internetist lasuma pildi üleslaadimist võimaldanud sotsiaalvõrgustikul kui vastutaval töötlejal.

¹⁸⁰ EK 25.06.2013, C-131/12, *Google Spain SL*, kohtujurist N. Jääskinen ettepanek, §§ 108, 134.

¹⁸¹ Eesti seisukohad justiitsküsimustes Euroopa Liidu justiits- ja siseministrite 17. ja 18. jaanuari 2013. a mitteametlikul kohtumisel. Arvutivõrgus: <http://tinyurl.com/oq6pqsr>, 30.04.2014.

¹⁸² European Commission MEMO. 27.01.2014.

¹⁸³ Article 29 Data Protection Working Party. Opinion 01/2012, p 14. Samal arvamusel: W. K. Hon *et al*, p 43.

Komisjon on rõhutanud, et õigus olla unustatud ei ole absoluutne õigus ning selliste õiguste tasakaalustamiseks nagu õigus vabale eneseväljendusele ja teaduslikul eesmärkidel andmete töötlemisele on artikli 17 (3)(a) ning artikli 80 koosmõjus liikmesriikidel volitus võtta vastu õigusakte, mis tagaksid ka nende põhiõiguste olemasolu.¹⁸⁴ Erandite lubamise eesmärgiks on tagada, et andmete kustutamise õiguse teostamisel ei rikutaks teise inimese õigusi, näiteks õigust vabale eneseväljendusele. Selline konflikt võib tekkida näiteks olukorras, kus isik soovib teostada oma õigust andmete kustutamisele teda negatiivselt kujutava ajalehe artikli osas, nagu Euroopa Kohtu asjas C-131/12.¹⁸⁵ Sellisel juhul tuleb riivatavaid põhiõigusi kaaluda ning kaalumise mehhanism on jäetud liikmesriikide kehtestada.

Üldmääruse artikli 17 suhestumine õigusega vabale eneseväljendusele on saanud ulatuslikku kriitikat. Üldmääruse artiklis 17 (3) sätestatud volitused andmete kustutamise õigusele vajavad täpsustamist. Euroopa Andmekaitseinspektor on avaldanud arvamust, et tulenevalt üldisest erandite süsteemist, mis on sätestatud artiklis 21, on artikkel 17 (3) kasutu ning tuleks kustutada.¹⁸⁶

Töö autor nõustub kriitikaga, mille kohaselt ei ole nende kahe õiguse – õiguse olla unustatud ja õiguse vabale eneseväljendusele – lepitamise jätmine liikmesriikide diskretsioonotsuseks artikli 17 (3) ja artikli 80 alusel efektiivne lahendus, mis võib viia lausa tsensuurini.¹⁸⁷ Pidades silmas üldmääruse eesmärki tagada kõigi üksikisikute võrdne kaitse kogu Euroopa Liidus, on sõnavabaduse küsimuse liikmesriikidele otsustusruumi jätmine üllatav, kuna vaba eneseväljenduse erandite sätestamine liikmesriikide poolt kahjustab isikute ühetaolise kaitse põhimõtte kohaldamist.

Eestile tähendaks üldmääruse artiklis 17 sätestatud põhimõtte kohustust kehtestada õigusaktidega erandid artiklist 17 seonduvalt sõnavabaduse, terviseandmete töötlemise, ajalo- , statistikauurimuste ning teadustöö eesmärgil andmete töötlemisega. Pidades silmas asjaolu, et Eestis puudub peale avaliku teabe seaduse igasugune valdkonnaspetsiifiline regulatsioon seonduvalt isikuandmete töötlemisega, kaasneb kavandatavate meetmete kehtima hakkamisega ulatuslik seadusloome.

Kokkuvõttes võib järeldada, et kuigi andmete kustutamise õiguse eesmärgiks on tugevdada üksikisikute kontrolli enda andmete üle, siis tegelikkuses saavutatakse selline tulemus pigem

¹⁸⁴ European Commission MEMO. 27.01.2014.

¹⁸⁵ EK 25.06.2013, C-131/12, *Google Spain SL*, kohtujurist N. Jääskinen ettepanek, §§ 108, 134.

¹⁸⁶ European Data Protection Supervisor, p 24 - 25.

¹⁸⁷ L. Danagher, p 2.5.

näiliselt. Kuigi andmesubjektidele võib jääda mulje, et nende õigust andmete kustutamisele on võrreldes direktiivis sätestatuga oluliselt tugevdatud, ei ole nende õigused praktikas efektiivselt tagatud. Ettevõtetal ei ole võimalik teavitada kõiki kolmandaid osapooli, kes andmeid kasutavad, kuna arvestades andmete töötlemise hulka ja kiirust internetis, ei pruugi vastutavatel töötajatel olla kolmandate osapoolte andmeid, eriti problemaatiline on see pilvandmetöötluse, hiigelsuurte andmemahtude (Big Data) töötlemise ning otsingumootorite kontekstis. Üldmääruses puuduvad meetmed kolmandate osapoolte survestamiseks ning kogu vastutus on asetatud ainuüksi vastutavale töötlejale, samas ei ole vastutava töötleja kohustus “võtta tarvitusele kõik tarvilikud meetmed” piisav tagamaks isikute õiguste kaitse. Lisaks on üldmääruses jäetud lahtiseks küsimus sellest, millised saavad olema liikmesriikide poolt kehtestatavad erandid sõnavabaduse kaitseks, millistest kriteeriumitest need lähtuvad ning millise liikmesriigi õigust tuleb erandite suhtes kohaldada juhul, kui andmed, mida kustutada soovitakse on juba jõudnud mitmesse EL liikmesriiki.

Eeltoodust tulenevalt ei ole õigus isikuandmete kustutamisele praeguses vormis efektiivne meede tagamaks andmesubjektide suuremat kontrolli enda isikuandmete üle. Meede ei ole praktikas rakendatav ning loob sellest tulenevalt üksnes näilise turvatunde, koormab vastutavat töötajat ebaproportsionaalselt ning jätab ebaselgeks, millised on selle õiguse realiseerimise erandid.

2.2.2.2 Isikuandmete ülekantavus

Vajadus kehtestada õigus isikuandmete ülekantavusele on tingitud asjaolust, et käesoleval hetkel ei ole isikutel võimalik enda isikuandmeid (näiteks fotosid, sõprade nimekirju jms) eemaldada ühest keskkonnast viisil, mis võimaldaks nende andmete taaskasutamist teises sarnases keskkonnas ehk võimaldaks samade andmetega pöörduda mõne teise teenusepakkuja poole, et kasutada teenuseid, mis võivad olla odavamad ja tagada parema privaatsuse kaitse.¹⁸⁸

Teenusepakkuja vahetamine võib endaga kaasa tuua isiklikult ja sotsiaalselt olulise info kadumise. Juhtudel, kus info on võimalik uuesti käsitsi sisestada, toob see endaga kaasa ebamõistliku aja- ja rahakulu.¹⁸⁹ Lisaks vajadusele liigutada isikule olulisi andmeid (sõprade nimistu, kontaktiraamat jne) ühest keskkonnast teise, puudutab andmete liigutatavus ka enda identiteedi ja reputatsiooni üle kandmist ühest keskkonnast teise – näiteks võib tuua

¹⁸⁸ Commission staff working paper. Impact assessment, p 28.

¹⁸⁹ *Ibid.*

internetikaubanduse, kus eduka kauplemise eelduseks on teiste sama keskkonna kasutajate poolt antud positiivsed hinnangud. Olukorras, kus isik otsustab vahetada keskkonda, kaotab ta ka selles keskkonnas tema identiteediga kaasnenud reputatsiooni ning peab uues keskkonnas alustama otsast peale.¹⁹⁰

Kindlustamaks suuremat kontrolli isikute andmete üle, loodi andmete kustutamise õiguse kõrvale isikuandmete ülekantavuse põhimõte, mis võimaldab andmete liigutamist ühe vastutava töötleja juurest teise juurde. Üldmääruse artikli 15 kohaselt on andmesubjektil õigus struktureeritud ja üldkasutatavas vormingus olevate isikuandmete elektroonilise töötlemise korral saada vastutavalt töötlejalt töödeldavate andmete elektrooniline struktureeritud ja üldkasutatavas vormingus koopia, mida andmesubjekt saab omakorda kasutada. Andmesubjekti palvel võib vastavalt üldmääruse artiklile 15 (2a) andmed edastada otse ühelt vastutavalt töötlejalt teisele, kui see on tehniliselt võimalik ja mõistlik. Selline üldmääruses sätestatud õigus on võrreldes direktiiviga täiesti uus.¹⁹¹ Töörühma arvamuse kohaselt tugevdab selle õiguse tutvustamine andmesubjektide õigusi ja võimaldab suuremat kontrolli oma isikuandmete üle.¹⁹² Lisaks võimaldab andmete ülekantavus andmesubjektidel paremini liikuda ühe teenusepakkuja juurest teise juurde, mis omakorda soodustab teenusepakkujate konkurentsi ning loob eelduslikult tingimused paremate teenuste pakkumiseks (kuna kliendid ei ole enam sunnitud kasutama ühe teenusepakkuja teenust).¹⁹³

Esiolgses üldmääruse sõnastuses jäi ebaselgeks, kuidas suhestuvad omavahel õigus enda andmete kustutamisele ning õigus andmete ülekantavusele, kuid uues sõnastuses on ebaselgus kõrvaldatud artikli 15 (2b) lisamisega, mille kohaselt ei välista andmete ülekantavuse sätte kohaldamine üldmääruse artikli 5 (1)(e) kohaldamist, mille kohaselt säilitatakse isikuandmeid ainult seni, kuni nende säilitamine on vajalik säilitamise eesmärgi täitmiseks. Sellest tulenevalt saab järeldada, et peale andmete ülekandmist ühe teenusepakkuja juurest teise juurde, tuleb esimesel andmed kustutada.

Huvigrupid, peamiselt pilvandmetöötluse teenusepakkujad ei poolda andmete ülekantavuse õiguse tutvustamist, samuti rõhutatakse, et on ebaselge milliste andmete ülekantavust uus loodud õigus puudutab.¹⁹⁴ Samal seisukohal on ka Euroopa Andmekaitseinspektor, kelle

¹⁹⁰ G. Zanfir, p 151.

¹⁹¹ Commission staff working paper. Impact assessment, p 23.

¹⁹² Article 29 Data protection Working Party, Opinion 01/2012, p 6.

¹⁹³ G. Zanfir, p 152.

¹⁹⁴ Commission staff working paper. Impact assessment, Annex 4 p 75.

arvates peaks õigus andmete ülekantavusele hõlmama ka muid andmeid, kui andmesubjekti enda poolt vastutavale töötlejale töötlemiseks antud andmeid.¹⁹⁵

Tegelikkuses on kasutajate kohta käivate andmete liigutamine erinevate kasutajaliidest vahel juba praegu võimalik ning pidades silmas asjaolu, et teenusepakkujad teostavad isikuandmete vahetust endaga seotud ettevõtetega juba praegu, peaks selle õiguse rakendamise kulud olema minimaalsed.¹⁹⁶ Näiteks juba praegu võimaldab *Facebook* andmesubjektil enda arvutisse salvestada kõik andmesubjekti kohta käiva informatsiooni, mis tähendab, et informatsiooni saab edastada ka uuele teenusepakkujale.

Kuigi selline õigus võib esialgu teenusepakkujatele kulukaks osutuda, survestab selline regulatsioon pilvandmetöötluste teenuse pakkujaid kasutama tehnoloogiaid, mis võimaldavad andmeid erinevate „pilvede“ vahel odavamalt ja lihtsamini liigutada, kuna nende peamised teenuse tarbijaid, st vastutavad töötlejad, on huvitatud just sellise teenuse ostmisest, mis võimaldab hiljem vastutaval töötlejal kergesti täita oma artiklist 15 tulenevat kohustust.¹⁹⁷

Töö autor on seisukohal, et andmete liigutatavuse õiguse tutvustamine aitab parandada üksikisikute kontrolli enda isikuandmete üle. Võrreldes isikuandmete kustutamise õigusega, on andmete liigutatavus praktikas oluliselt lihtsamini rakendatav. On arusaadav, et sellise õiguse tutvustamine on teenusepakkujate hulgas ebapopulaarne, kuid eeldusel, et selle õiguse rakendamisega ei kaasne ettevõtjatele liiga suuri kulusi, tagab selline võimalus isikute õiguste parema kaitse, kuna suurendab realselt kontrolli enda isikuandmete üle. Kuigi tutvustatav õigus vajab täpsustamist reguleerimisala osas, võimaldab see oma andmed kaasa võtta ning pöörduda teenusepakkuja poole, kes pakub andmesubjekti jaoks paremat teenust ning seda vaba konkurentsi tingimustes. Selliselt ei pea isikud, kes kasutavad teenusepakkuja teenust peamiselt põhjusel, et selles keskkonnas on kõik olulised andmed, enam olema sunnitud seda teenust kasutama, vaid saavad valida teenusepakkujaid, kelle teenus on kvaliteetsem, turvalisem ja vastab paremini tarbija vajadustele.

¹⁹⁵ European Data Protection Supervisor, p 25.

¹⁹⁶ Commission staff working paper. Impact assessment, Annex 5 p 106.

¹⁹⁷ W. K. Hon *et al*, p 45. Samal arvamusel: C. Cuijpers *et al*, p 12.

2.3 Vajadus tagada paremad tingimused Euroopa Liidu siseturu toimimiseks

Isikuandmete kaitse regulatsioon Euroopa Liidu tasandil peab tegelema küsimusega, kuidas leida sobiv tasakaal üksikisikute õiguste kaitsmise ja siseturu efektiivse toimimise vahel.¹⁹⁸

Isikuandmete kaitse reformi üheks lähtekohaks oli vajadus eemaldada turubarjäär ettevõtetele ja avaliku sektori asutustele, mis tulenes kohaldatava õiguse killustatusest, õiguskindluse puudumisest ning ebajärjepidevast õiguse jõustamisest.¹⁹⁹ Eelkõige on reform vajalik rahvusvahelistele ettevõtetele, kes tegutsevad mitmes EL liikmesriigis ning kes peavad praeguse regulatsiooni kohaselt arvestama liikmesriikide erinevate seadusandlustega.²⁰⁰

Euroopa Kohus rõhutas oma eelotsuses ühendatud kohtuasjades C-468/10 ja C-469/10, et direktiivi eesmärgiks ei ole mitte saavutada minimaalne ühte standard, vaid siseriiklike seadusandluste täielik harmoniseerimine, mistõttu tuleb rakendamisel lubatud diskretsiooni kasutada lähtudes üksnes direktiivi eesmärkidest, mis on isikuandmete vaba liikumine ja eraelu kaitse.²⁰¹

Praegused erinevused direktiivist tuleneva õiguse kohaldamisel, tõlgendamisel ja jõustamisel takistavad andmete vaba liikumist Euroopa Liidu siseturul. Erinevused toovad endaga kaasa lisaks õiguskindluse puudumisele ka ühtlustamisega seonduvaid kulusid, mis puudutab andmete töötlemist ja edastamist liikmesriikide vahel, tagamata samas isikuandmete kaitset piisaval tasemel. Komisjoni hinnangul võib regulatsiooni killustumusest tulenev halduskoormus minna ettevõtetele maksma ligi 3 miljardit eurot aastas.²⁰²

Ettevõtete osas on tekkinud ebavõrdne olukord suurte ning keskmiste ja väikeste ettevõtete vahel, kuna suurtel ettevõtetel on rohkem ressursi, et tagada oma tegevuse vastavus õigusaktidele, sealjuures erinevate liikmesriikide õigustele, samas kui väikse ja keskmise suurusega ettevõtetel sellist võimalust pole, mistõttu loobuvad väiksema- ja keskmise suurusega ettevõtted oma teenuste pakkumisest internetis või teenindavad kliente ainult oma liikmesriigi jurisdiktsioonis.²⁰³

¹⁹⁸ W. K. Hon *et al*, p 15.

¹⁹⁹ Commission staff working paper. Impact assessment, p 11.

²⁰⁰ Euroopa Komisjoni teatis. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus, lk 3.

²⁰¹ EKo 24.11.2011, C-468/10 & C-469/10, *ASNEF & FECEMD*, § 34.

²⁰² W. K. Hon *et al*, p 40.

²⁰³ Commission staff working paper. Impact assessment, p 11.

2.3.1 Õiguskindluse suurendamine

Liikmesriigid on direktiivi inkorporeerinud siseriiklikku õigusesse erinevalt ning seetõttu on erinevusi nii isikuandmete mõistete sisustamisel (näiteks mõned riigid peavad IP aadresse isikuandmeteks ning mõned mitte) kui ka suuremates kontseptsioonides, näiteks isiklike ja koduste eesmärkide erandi sisustamisel, millest oleneb direktiivi materiaalne kohaldumisala.²⁰⁴ Aastal 2003 tehtud direktiivi kohaldamise analüüsist nähtub, et direktiivi artikli 4 kohaldamisel, mis määrab kohaldatava siseriikliku õiguse (territoriaalse kohaldumisala) esineb probleeme, mille vältimine oli artikli 4 peamine eesmärk.²⁰⁵

Isikuandmete kaitse regulatsioon erineb liikmesriigiti ning sätestab ettevõtetele erinevad kohustused ning toob kaasa ebaühtlase standardi isikuandmete kaitsmisel. Sealjuures tekivad kohalduva õiguse probleemid olukordades, kus vastutav töötaja peab oma tegevuses vastama mitme liikmesriigi siseriikliku õigusega kehtestatud nõuetele, rahvusvaheline ettevõtte asub rohkem kui ühes liikmesriigis või kui andmete töötaja ei asu üheski liikmesriigis, kuid pakub teenuseid EL-i residentidele.²⁰⁶ Ettevõtetele ei ole piisavalt õiguskindlust, sest nad ei saa rahvusvaheliselt tegutsedes olla kindlad, milliseid nõudeid neile ühes või teises liikmesriigis tegutsemisel esitatakse, tihti peab ettevõtte olema suuteline vastama mitme liikmesriigi erinevatele nõuetele.

Õiguskindluse suurendamine eeldab materiaalõiguse ühtlustamist ning territoriaalse kohaldumisala probleemide lahendamist, et rahvusvaheliselt tegutsevatel ettevõtetel oleks võimalik prognoosida, milline õiguslik tagajärg on ühel või teisel nende teol. Eeltoodust tulenevalt on põhjendatud käsitleda komisjoni tutvustatava lahendusena õiguskindluse suurendamiseks otsust kehtestada uus regulatsioon otsekohalduva määrusega.

2.3.1.1 Otsekohalduva mõjuga õigusinstrument

Euroopa Komisjon on andmekaitse regulatsiooni reformi ühe alussambana rõhutanud põhimõtet „üks kontinent, üks seadus.“²⁰⁷ Tulenevalt ELTL artiklist 288, on määrus tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

²⁰⁴ *Ibid*, Annex 2, p 14.

²⁰⁵ European Commission report, 2003, § 3.2.

²⁰⁶ Euroopa Komisjoni teatis. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus, lk 11.

²⁰⁷ European Commission MEMO 12.03.2014.

Euroopa Komisjon on põhjendanud valikut kehtestada isikuandmete kaitse regulatsioon just määrusega tulenevalt sellest, et selline õiguslik instrument viib ebakõlad siseriiklikus õiguses minimaalsele tasemele ning tagab ettevõtjatele parima võimaliku õiguskindluse.²⁰⁸

Kehtima hakkav üldmäärus muudab vastavalt üldmääruse artiklile 88 (1) direktiivi kehtetuks. Üldmääruse artikkel 88 (2) sätestab, et viiteid kehtetuks tunnistatud direktiivile käsitletakse viidetena üldmäärusele ning viiteid direktiivi alusel loodud töörihm viitena üldmäärusega loodavale Euroopa Andmekaitseõukogule. Sätte eesmärgiks on tagada, et Euroopa Kohtu ulatuslik praktika direktiivi tõlgendamisel ja sisustamisel ei muutuks asjakohatuks. Preambula nr 7 kohaselt on ka üldmääruses direktiivi eesmärgid ja põhimõtted asjakohased.

Otsekohalduv määrus muudab IKS-i praeguses sõnastuses kehtetuks, kuigi teatud juhtudel võivad liikmesriigid otsustada, et kehtestatud määrus tuuakse üle siseriiklikku õigusesse ning kehtestatakse siseriiklik õigusakt.²⁰⁹ Eestis sisaldavad isikuandmete regulatsiooni 115 kehtivat seadust ning 263 Vabariigi Valitsuse või ministri määrust, millele lisanduvad omakorda kohalike omavalitsuste õigusaktid.²¹⁰ Eeltoodust nähtuvalt omab üldmääruse kehtestamine Eesti siseriiklikule õigusele ulatuslikku mõju, kuigi detailsemat mõjuanalüüsi veel tehtud ei ole.

Vastavalt Vabariigi Valitsuse seisukohtadele sätestab üldmäärus direktiiviga võrreldes erineva eesmärgi – kui direktiivi mõte oli tasakaalustada isikuandmete töötlemist eraelu puutumatusena, siis üldmäärusega on eesmärgiks seatud füüsiliste isikute põhiõiguste tagamine. Vabariigi Valitsuse arvates ei võimalda üldmäärus kaaluda ettevõtjate huvisid üksikisikute omadega, vaid seab üksikisikute õiguste kaitse esikohale, takistades seega teaduse arengut, innovatsiooni ja ettevõtlust.²¹¹

Mõjuanalüüsis on märgitud, et väga detailse regulatsiooni kehtestamise korral võib ilmned probleeme üldmääruse rakendamise ja liikmesriikides, mille eripärasid regulatsioon ei arvesta.²¹² Peamine põhjus, miks liikmesriigid on isikuandmete kaitse määrusega reguleerimise vastu, seisnebki selles, et praeguses sõnastuses on üldmäärus kohati väga detailne ega arvesta siseriiklike õigussüsteemide eripäradega.²¹³ See omab aga olulist mõju ettevõtlusele, sest tulenevalt liikmesriikide eripäradest ja huvidest erineb ka nendes

²⁰⁸ Commission staff working paper. Impact assessment, p 87.

²⁰⁹ P. Craig, G. de Burca, p 105.

²¹⁰ Vabariigi Valitsuse 29.03.2012 otsuse seletuskiri, lk 15-16.

²¹¹ *Ibid*, lk 8.

²¹² Commission staff working paper. Impact assessment, p 71.

²¹³ P. M. Schwartz, p 2004.

liikmesriikides seadusandlusega kehtestatav ettevõtluskeskkond. Näiteks ei ole Balti riikide käivet ning siin tegutsevate ettevõtete suurus silmas pidades mõeldav, et järelevalveasutuse ametnik teeks mõnele ettevõttele 100 000 000 euro suuruse trahvi, nagu seda võimaldab üldmääruse artikkel 79 (2a)(c), kuna see viiks ettevõtte maksejõuetuseni.

Üldmääruse artiklites 30-39 sätestatud nõuded (näiteks riskianalüüsi tegemise ja andmekaitse ametniku määramise kohustus) vastutavale töötlejale toovad endaga kaasa oluliselt suuremad administratiivsed kulud võrreldes sellega, kui vähe kasu on nendest sätetest oodata.²¹⁴ Üldmäärusega kaasnevatest dokumentidest (eelkõige mõjuanalüüsist) ei nähtu, et enne eelnõu koostamist oleks põhjalikult võrreldud liikmesriikide siseriiklike regulatsioone ning üldmääruse võimalikku mõju. Kehtestades üldmäärusega regulatsioon, mida liikmesriigid ei ole suutelised rakendama, ei saavutata ka soovitud õiguskindlust.

Tasakaalustamaks detailseid ettekirjutusi andmetöötlejatele, näeb üldmäärus ette liikmesriikide volitused kehtestada teatud valdkondades täiendav siseriiklik regulatsioon. Sealjuures on liikmesriikidel kohustus sätestada siseriikliku seadusandlusega erandid mitmetest üldmääruse peatükkidest näiteks isikuandmete töötlemiseks ajakirjanduse ja kirjandusliku või kunstilise eneseväljenduse huvides (art 80), samuti avaliku võimu poolt kogutava info avalikustamiseks (art 80a), terviseandmete töötlemiseks (art 81) ning andmete töötlemiseks töösuhete kontekstis (art 82). Samuti näeb üldmääruse artikkel 21 ette liikmesriigi õiguse teatud juhtudel piirata üldmääruse kohaldumisala ning teatud juhtudel konkreetsete sätete kohaldumisala (art 6 (4) ja art 17 (3)(d)).

Euroopa Andmekaitseinspektor on juhtinud tähelepanu sellele, et üldmääruses ette nähtud volitusnormid, mis võimaldavad liikmesriikidele ulatusliku pädevuse (mh spetsiifilisema regulatsiooni kehtestamiseks ning erandite tegemiseks), viivad taaskord siseriiklike õiguste killustatusest tuleneva õiguskindluse puudumiseni, mis on vastupidine soovitud eesmärgile.²¹⁵

Sealjuures tõusetub seoses volitusnormidega ka territoriaalse kohaldumisala küsimus. Üldmäärus ei reguleeri siseriikliku õiguse kohaldamist.²¹⁶ Olukorras, kus liikmesriik X kehtestab üldmäärusega võrreldes spetsiifilisemad tingimused näiteks töösuhetega seonduvalt, jääb ebaselgeks, kas rahvusvahelisele ettevõttele, kellel on asutused ka teistes liikmesriikides,

²¹⁴ *Ibid*; Council of European Municipalities and Regions. General Data Protection Regulation. Revise the existing directive for the public sector. Brussels: November 2012, p 5. Available: http://www.ccre.org/docs/cemr_position_paper_data_protection_en.pdf, 01.05.2014.

²¹⁵ European Data Protection Supervisor, p 17.

²¹⁶ W. K. Hon *et al*, p 23.

kohaldub liikmesriigi X regulatsioon kõigi asutuste või ainult liikmesriigis X asuva asutusega seondult. Probleem oleks lahendatav, kui üldmäärusesse lisataks sätte, mis selgitab siseriikliku regulatsiooni ja üldmääruses sätestatu kohaldumisasialasid.²¹⁷

Suurbritannias läbi viidud uuringu kohaselt ei tagata kavandatava üldmäärusega õiguskindlust tulenevalt üldmääruse mitme sätte ebamäärasusest, ebaselgest kohaldumisasialast ning ulatuslikest volitusnormidest. Tulemuseks võib olla hoopis ühtlustumise vähenemine.²¹⁸

Töö autor on seisukohal, et vaatamata üldmääruse puudustele praeguses sõnastuses, ei ole isikuandmete kaitse regulatsiooni kehtestamine määrusega iseenesest halb otsus. Isikuandmete töötlemise reguleerimine direktiiviga on osutunud ebaefektiivseks ning määrus võimaldab kõige suurema tõenäosusega tagada ühtse alusplatvormi isikuandmete kaitsmiseks ning andmete vabaks liikumiseks.²¹⁹

Üldmäärusega ei saavutata praeguses sõnastuses soovitud õiguskindlust, kuna liigse detailsuse tõttu ei ole üldmäärus kõigis liikmesriikides kohaldatav ega pea silmas liikmesriikide erinevusi. Olukorras, kus osad liikmesriigid ei suuda üldmääruses sätestatut ellu viia, ei ole tagatud ka materiaalõiguse ühtlane kohaldamine. Lisaks on töö autor seisukohal, et üldmäärus ei ole piisavalt kõikehõlmav ja sidus. Üldmääruses ei ole leitud head tasakaalu liikmesriikidele piisava vaba otsustusruumi ja soovitud õiguskindluse tagamise vahel.²²⁰ Sealjuures on jäetud liikmesriikide otsustada väga põhimõttelised küsimused (näiteks sõnavabaduse erand), jättes samal ajal lahtiseks küsimuse liikmesriikide siseriiklike regulatsioonide territoriaalsest kohaldumisasialast.

2.3.2 Vajadus vähendada ettevõtete halduskoormust

Suurema õiguskindluse tagamise tulemuseks peaks komisjoni hinnangul olema halduskoormuse vähenemine ettevõtetele. Kulutused vastutavatele töötlejatele, eelkõige direktiivi artiklis 18 sätestatud kohustusest teavitada andmete töötlemisest järelevalveasutust, on viinud komisjoni hinnangul ebamõistlike administratiivsete kulutusteni, mis ulatuvad rahvusvaheliste ettevõtete puhul 2,3 miljardi euron aastast.²²¹ Ulatuslikud administratiivsed kulutused puudutavad eelkõige väikseid ning mikroettevõtteid, kelle jaoks võib praegune suur

²¹⁷ European Data Protection Supervisor, p 10.

²¹⁸ London Economics. Implications of the European Commission's proposal for a general data protection regulation for business. Final report to the Information Commissioner's Office. London: May 2013, p 13 - 14.

²¹⁹ L. Danagher, § 2.2.

²²⁰ European Data Protection Supervisor, p 4.

²²¹ V. Reding, p 3.

administratiivne koormus osutada takistuseks rahvusvahelisele turule sisenemiseks ja seal tegutsemiseks.²²²

Kulude hindamisel arvestas Euroopa Komisjon andmesubjektide teavitamisest tulenevaid kulusid, kulusid seonduvalt andmesubjektide palvetega enda kohta käiva info muutmiseks, parandamiseks või kustutamiseks, järelevalveasutuste teavitamisega seonduvaid kulusid (direktiivi art 18) ning direktiivi artiklis 20 sätestatud eelkontrollist tulenevad kulutusi.²²³

2.3.2.1 Kulude vähendamine

Suurimad kulutused kaasnevad Euroopa Komisjoni hinnangul praegu direktiivis ette nähtud teavitamiskohustusega. Arvestuslikult peab vastutav töötaja iga teavituse eest kandma kulutusi keskmiselt 200 euro ulatuses.²²⁴ Teavitamiskohustusega kaasnevate kulutuste vältimiseks on direktiivi artiklites 18 ja 19 sätestatud järelevalveasutuse teavitamise kohustus asendatud üldmääruse artikliga 28, mille kohaselt on vastutaval töötlejal kohustus säilitada andmete töötlemisega seonduv dokumentatsioon.

Mõjuanalüüsis esitatud arvutused administratiivsete kulude kohta ei peegeldada siiski tegelikku olukorda. Praeguse halduskoormuse arvutamiseks on aluseks võetud ebapiisavad andmed, samuti on jäetud arvestamata mitmed üldmääruse rakendamisega kaasnevad kulud.²²⁵

Üldmäärus sätestab lisaks andmete säilitamise kohustusele ka kohustuse viia läbi teatud juhtudel riskianalüüs (art 33), konsulteerida andmekaitseasutustega (art 34) ning määrata andmekaitseametnik (art 35) kõikides era- ja avaliku sektori asutustes, kus on rohkem kui 250 töötajat. Nende kohustustega kaasnevad ulatuslikud kulutused, kuna eeldavad muuhulgas täiendava tööjõu palkamist. Märkimisväärsed püsi- ja muutuvkulud kaasnevad ka kohustusega teavitada järelevalveasutust rikkumisest 24 tunni jooksul (art 31).²²⁶ Sealjuures puudutavad üldmäärusega kehtestatavad täiendavad nõuded suuremat hulka ettevõtteid, kui direktiivi artiklist 18 tulenev kohustus teavitada andmete töötlemisest järelevalveasutusi, kuna

²²² Commission staff working paper. Impact assessment, p 12.

²²³ *Ibid*, Annex 9, p 141.

²²⁴ *Ibid*, p 15, 19.

²²⁵ The United Kingdom Ministry of Justice. Impact assessment, p 9.

²²⁶ London Economics, p 60.

teavitamiskohustusest võivad liikmesriigid direktiivi artikli 18 (2) kohaselt ette näha ulatuslikumaid erandeid.²²⁷

Üldmääruses kavandatavate meetmetega ei saavutata halduskoormuse vähenemist, halduskoormus ettevõtetele pigem suureneb. Suurbritannias läbi viidud uuringu kohaselt on ettevõtted seisukohal, et ulatuslikumad vastutava töötaja kohustused seoses õigusega olla unustatud (art 17), kohustused teavitada järelevalveasutust isikuandmete kaitsega seonduvatest rikkumistest 24 tunni jooksul pärast rikkumise toimumist (art 31) ning kohustus teavitada andmesubjekti (art 32) toovad pigem endaga kaasa töömahu ja seega ka kulutuste suurenemise.²²⁸ Kahtlusi administratiivse koormuse vähenemise osas rahvusvahelistele ettevõtetele on väljendanud ka Euroopa Andmekaitseinspektor, muuhulgas kaasnevad ulatuslikud kulutused juba ainuüksi artiklis 28 (2) sätestatud dokumentide säilitamise kohustusega.²²⁹

Vastavalt Suurbritannias läbi viidud uuringule, ei osanud 82% küsitletud andmetöötajatest ise hinnata praegu kehtiva direktiivi nõuetest tulenevaid kulusid,²³⁰ mis seab töö autori arvates kahtluse alla komisjoni pädevuse mõjuanalüüsis toodud arvutuste tegemiseks. Töö autor on seisukohal, et isegi juhul, kui üldmäärusega kaasneksid senisest suuremad (ühekordsed) kulutused, ei tähenda see, et üldmäärus tuleks jätta kehtestamata. Küll aga on kahetsusväärne, et praegused analüüsid on äärmiselt ebatäpsed. Vastupidiselt komisjoni hinnangule on mitmed uuringud leidnud, et halduskulud hoopis suurenevad. Eelduslikud kaasnevad täiendavad kulutused ei ole praeguses sõnastuses proportsionaalsed saavutatavate kasudega.²³¹

2.3.2.2 Mikro-, väikese ja keskmise suurusega ettevõtetele erandite kohaldamine

Mikro-, väikse ja keskmise suurusega ettevõtete puhul soovitakse administratiivset koormust vähendada (ja ühtlasi konkurentsivõimet suurendada) läbi erandite ja lävendite süsteemi, mis näeksid sellistele ettevõtetele ette teistsugused reeglid, kui suurematele ettevõtetele.²³² Erandid on ette nähtud seoses kolmandate riikide vastutavate töötajate kohustusega määrata endale esindaja liidus (art 25), kohustusega dokumenteerida isikuandmete töötlemise protsessi (art 28 (4)), järelevalveametniku määramise kohustusega (art 35) ning seoses määratavate halduskaristustega. Reeglina kehtivad erandid ettevõtetele, kus on alla 250 töötaja.

²²⁷ V. Peep, lk 2.

²²⁸ London Economics, p 60.

²²⁹ European Data Protection Supervisor, p 31.

²³⁰ London Economics, p 59.

²³¹ L. Danagher, § 3.1

²³² Commission staff working paper. Impact assessment, Annex 4, p 80.

Esiteks on leitud, et üldmäärusega kaasnev halduskoormuse suurenemine tähendab väikese- ja keskmise suurusega ettevõtetele vaatamata erandite süsteemile senisega võrreldes 300 - 7200 eurot lisakulutusi aastas, mis moodustavad 16 - 40% selliste ettevõtete infotehnoloogia alastele kulutustele mõeldud eelarvest.²³³

Teiseks tekib küsimus erandi õigustatusest – kuigi kohustus vastata teatud nõuetele toob endaga kaasa ka administratiivse koormuse, on sellised ettekirjutused ühtlasi ette nähtud selleks, et tagada üksikisikute õiguste parem kaitse. Üldmäärus näeb ette erandi, et ettevõttes, kus on alla 250 töötaja, ei ole vajalik andmekaitseametniku määramine, kes kontrolliks töötajate andmete töötlemise seaduslikkust. Sellest erandi kohaselt jääks ilma täiendava kaitseta umbes 60% ettevõtete töötajaid.²³⁴ Olukorras, kus isiku õigused on vähem kaitstud tulenevalt mikro-, väikse ja keskmise suurusega ettevõtetele kohaldatavatest eranditest, ei ole tagatud isikuandmete kaitse reformi esimene eesmärk, st isikute õiguste tugevdamine. Samale seisukohale on asunud nii Euroopa Andmekaitseinspektor²³⁵ kui ka töörühm.²³⁶ Parema tasakaalu ettevõtjate huvide ning üksikisikute õiguste kaitse vahel saavutaks ilmselt lahendus, kus erandid koormavatest nõuetest on seotud andmete töötlemise olemuse ja ulatuse, mitte ettevõtte suurusega,²³⁷ sama mehhanismi on soovitanud ka Majandus- ja Sotsiaalkomitee.²³⁸

Töö autor on seisukohal, et halduskoormuse vähendamine ei ole üldmääruses sätestatud vahenditega saavutatav, vähemalt mitte suurtele rahvusvahelistele ettevõtetele. Üldmääruses ei ole leitud head tasakaalu üksikisikute õiguste kaitse ning ettevõtjate õiguste vahel, sest ühe eesmärgi saavutamine tuleb paratamatult teise arvelt. Euroopa Komisjon viitab üldmääruses ette nähtud täiendavatele vastutavale töötlejale sätestatud nõuetele vastavalt vajadusele kui meetmetele, mis tagavad isikuandmete kaitse garantii²³⁹ samas, kui mikro-, väikse ja keskmise suurusega ettevõtjate puhul käsitletakse samu kohustusi kui „administratiivset koormat.“²⁴⁰

²³³ L. Christensen, A. Colciago, F. Etro and G. Rafert. The Impact of the Data Protection Regulation in the E.U. 2013, p 2. Available: <http://www.intertic.org/Policy%20Papers/CCER.pdf>, 01.05.2014. Siiski vähendab viidatud allika usaldusväarsust asjaolu, et uuringut rahastas *Google*.

²³⁴ European Economic and Social Committee. Opinion on the „Proposal for General Data Protection“. - ELT C 229, 31.07.2012 p 90 - 97, p 95.

²³⁵ European Data Protection Supervisor, p 13.

²³⁶ Article 29 Data Protection Working Party. Opinion 01/2012, p 8.

²³⁷ Article 29 Data Protection Working Party. Opinion 01/2012, p 8.

²³⁸ European Economic and Social Committee, p 95.

²³⁹ European Commission MEMO. 12.03.2014.

²⁴⁰ V.Reding, p 3.

2.4 Vahekokkuvõte

Peatükis analüüsiti Euroopa Komisjoni poolt üldmäärusega kavandatavate meetmete efektiivsust seonduvalt üksikisikute kaitse ning siseturu efektiivse toimimisega ning üksikisikute ja ettevõtjate huvide tasakaalustamisega.

Üksikisikute õiguste paremaks tagamiseks seati eesmärgiks tagada suurem läbipaistvus isikuandmete töötlemisel ning võimaldada andmesubjektidele paremat kontrolli enda isikuandmete üle.

Suurema läbipaistvuse saavutamiseks on üldmääruses sätestatud läbipaistvusprintsip ning kehtestatud selgem regulatsioon vastutava ja volitatud töötleja vahelistest kohustustest. Mõlemad kavandatud vahendid tagavad parema läbipaistvuse isikuandmete töötlemisel, kuna kohustavad vastutavaid töötlejaid informeerima andmesubjekti temale arusaadaval viisil ning määravad selged vastutuse piirid olukorras, kus samu andmeid töötlevad mitmed ettevõtted.

Suurendamiseks andmesubjekti kontrolli enda isikuandmete üle, on üldmääruses ette nähtud õigus andmete kustutamisele ning õigus andmete ülekantavusele. Analüüsi käigus selgus, et õigus andmete kustutamisele ei ole praktikas tõenäoliselt rakendatav ning loob andmesubjektile pigem võltsturvatunde. Palju realistlikum on üldmäärusega tutvustatav õigus andmete ülekantavusele, mis võimaldab senisest paremini vahetada internetis erinevaid teenusepakkujaid, võimaldades isikutel valida teenusepakkujaid vastavalt nende teenuse turvalisusele ja kvaliteedile, mitte hoides neid kinni ühe teenusepakkuja juures põhjusel, et teenusepakkuja vahetamisega kaoks oluline osa teenusepakkuja juures hoitavatest andmetest (nt kontaktid, e-kirjad jms). Lisaks on üldmäärus praeguses sõnastuses ebaselge andmete kustutamise õiguse erandite ulatus, eelkõige, mis puudutab sõnavabadusele tehtavat erandit. Liikmesriikidele laia otsusediskretsiooni jätmine ei aita kaasa isikute andmete kaitsmise taseme ühtlustamisele, vaid loob võimalused lugematuteks kohtuvaidlusteks sõnavabaduse erandi sisustamise üle.

Andmetöötlejate õiguste paremaks tagamiseks ning isikuandmete vaba liikumise tagamiseks sooviti suurendada õiguskindlust ning vähendada ettevõtete halduskoormust, mis oli tingitud isikuandmete kaitse regulatsiooni killustatusest liikmesriigiti.

Õiguskindluse tagamiseks ei tutvustatud võrreldes üksikisikute õigustega mingisugust konkreetset õigust. Euroopa Komisjoni poolt valitud meetmena nii materiaalõiguse kui territoriaalse kohaldumisala täpsustamiseks tuleb käsitleda otsust reguleerida isikuandmete

kaitse Euroopa Liidu tasandil otsekohalduva määrusega. Praeguses sõnastuses on üldmäärus kohati liiga detailne ning seetõttu pole praktikas rakendatav, kuna ei arvesta liikmesriikide ega seal tegutsevate ettevõtete eripärade ja suurusega. Teisalt on mitmed olulised küsimused (näiteks spetsiifiline regulatsioon andmete töötlemiseks töösuhete kontekstis) jäetud siseriikliku õiguse lahendamata, mis võimaldab uuteks erinevusteks, pidades sealjuures silmas asjaolu, et üldmäärusega ei ole reguleeritud siseriiklike eriregulatsioonide territoriaalset kohaldumisaala.

Ettevõtete halduskoormuse vähendamiseks on üldmääruses soovitud vähendada kulutusi, muuhulgas kaotades ära direktiivi artiklist 18 tulenev teavitamiskohustus. Mikro-, väikeste ja keskmise suurusega ettevõtete võrdsemaks kohtlemiseks on tutvustatud erandite süsteem, mille kohaselt ei pea ettevõtteid, kus on alla 250 töötaja mitmeid kohustusi täitma. Erinevate uuringute kohaselt ei ole mõjuanalüüsis tehtud arvutused täpsed, arvestamata on jäetud mitmed üldmäärusega kaasnevad lisakulud, näiteks dokumentide säilitamise ja andmekaitseametniku määramise kohustus. Kuigi üldmäärusega soovitakse suurendada mikro-, väikese ja keskmise suurusega ettevõtete konkurentsivõimet, kehtestades neile erandid mitmetest kohustustest, ei pruugita ka siis nende ettevõtete kulutusi vähendada. Isegi kui kulutusi vähendatakse, tuleb see üksikisikute õiguste arvelt, kuna praeguses sõnastuses ei ole erandite tegemise seostatud mitte andmete töötlemise hulgaga, vaid ettevõtte töötajate arvuga.

Üldmääruses ei ole leitud tasakaalu üksikisikute kui andmesubjektide ja ettevõtjate huvide vahel. Kuigi regulatsioon kehtestab mitmed õnnestunud õigused üksikisikule, on sellega kaasnev negatiivne mõju ettevõtetele ebalproportsionaalselt suur. Praeguses sõnastuses üldmääruse kehtestamine ei tagaks senisest efektiivsemat siseturu toimimist.

3. JÄRELEVALVE REGULATSIOON ISIKUANDMETE KAITSE ÜLDMÄÄRUSES

3.1 Vajadus ühtlustada järelevalve regulatsiooni

Efektiivne järelevalve on eelduseks eelnevas peatükis käsitletud eesmärkide saavutamisele. Isikuandmete regulatsiooni reformiga sooviti tugevdada andmekaitsega tegelevate järelevalveasutuste rolli ning suurendada nende iseseisvust, sest just seeläbi on võimalik saavutada isikuandmete kaitse peamised eesmärgid – st üksikisikute õiguste piisav kaitse ning andmete vaba liikumine ja nende efektiivne tasakaal.²⁴¹

Teisalt on Euroopa Komisjoni poolt sõnastatud vajadus ühtlustada järelevalve regulatsiooni reformi eraldiseisev eesmärk, sest aastal 2003 tehtud uuringust selgus, et direktiivi peamine probleem on direktiivist tulenevate õiguste ja kohustuste tagamine praktikas. Probleemi põhjuseks peeti andmekaitseametnike piiratud ressursse ning soovimatust tegeleda direktiivi ja selle alusel kehtestatud õigusaktide jõustamist puudutavate ülesannetega.²⁴²

Aastal 2010 koostatud Euroopa Liidu Põhiõiguste Agentuuri (edaspidi ELPA) analüüsist nähtuvalt ei ole probleem siiani lahendust leidnud – probleemid esinevad nii institutsionaalsel, funktsionaalsel kui operatiivsel tasandil. Mitme liikmesriigi ametiasutused ei ole piisavalt sõltumatud ja autonoomsed, paljudel järelevalveasutustel puuduvad tegutsemiseks vajalikud ressursid ning seadustega ette nähtud pädevused.²⁴³

Mõjuanalüüsist nähtuvalt on probleeme ka liikmesriikide järelevalveasutuste rahastamisega, mistõttu ei ole osade liikmesriikide järelevalveasutused võimelised menetlema kõiki neile esitatavaid kaebuseid. Samuti erineb järelevalveasutuste pädevus liikmesriigiti – näiteks puudub Belgias järelevalveasutusel õigus nõuda andmete töötlemise peatamist, Saksamaal ning Rootsis puudub õigus nõuda andmete kustutamist. Mitmetes riikides puudub järelevalveasutusel pädevus määrata rikkujatele trahve (Belgia, Leedu, Ungari), liikmesriikides, kus trahvide määramine on lubatud, erinevad määratavad summad märkimisväärselt.²⁴⁴

Rahvusvahelisel tasandil ei ole järelevalveasutuste koostöö efektiivne – järelevalveasutused on vastuseks tööühma järelepärimistele toonud välja, et põhjuseks on selge ja arusaadava

²⁴¹ Euroopa Komisjoni teatis. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus, lk 17.

²⁴² European Commission report, 2003.

²⁴³ Fundamental Rights Agency. Data Protection in the European Union: the role of National Data Protection Authorities. Luxembourg: Publications office of the European Union 2014, p 6.

²⁴⁴ Commission staff working paper. Impact assessment, p 17 - 18.

mehhanismi puudumine puhkudeks, kui rahvusvahelise koostöö osutub vajalikuks.²⁴⁵ Direktiivi artikli 29 alusel loodud töörühm ei ole koostöö reguleerimisel efektiivne, sest tal puudub pädevus anda siduvaid otsused²⁴⁶ ning mittesiduvaid suuniseid on liikmesriigid praktikas siseriikliku õiguse muutmisel arvestanud ainult paaril korral.²⁴⁷

Praegu Eestis kehtivale isikuandmete töötlemise järelevalve regulatsiooni sisaldavale IKS-ile on ette heidetud kõrget abstraktsuse taset, millest tulenevalt ei suudeta tagada piisavalt tõhus järelevalve isikuandmete töötlemise üle.²⁴⁸ Tulenevalt direktiivi poolt loodud kõrgeast kaalutusõiguse osakaalust, vajab IKS efektiivsemaks toimimiseks täpsustusi.²⁴⁹

Pidades silmas, et direktiivis on järelevalve küsimust käsitletud sisuliselt kolmes artiklis (direktiivi art 28-30), on üldmääruses direktiiviga võrreldes antud palju konkreetsemad suunised järelevalve regulatsiooni osas. Sellest tulenevalt on ka üldmäärusega kaasnevad mõjud isikuandmete järelevalvele Eestis ulatuslikud.

Üldmääruse järelevalveregulatsioonis on eeltoodust tulenevalt lähtutud vajadusest tugevdada järelevalveasutuste sõltumatust, tagada järelevalveasutuste pädevuste ühtlustamine ning selgemini reguleerida järelevalveasutuste rahvusvahelist koostööd.

3.2 Järelevalveasutuste sõltumatus

ELPA 2010 uuringust selgub, et mitmes liikmesriigis on järelevalveasutuste efektiivsus ja võimekus oma ülesandeid täita problemaatiline. Probleem tuleb eelkõige sellest, et järelevalveasutustel puudub vajalik autonoomia ning majanduslik sõltumatus, probleeme on ka institutsionaalse sõltumatusega.²⁵⁰

Eestis teostab isikuandmete töötlemise üle järelevalvet Andmekaitse Inspektsioon (edaspidi AKI), kes kontrollib IKS ja selle alusel kehtestatud õigusaktide järgimist (IKS § 32). Vastavalt IKS § 32 lg-le 2 on AKI oma ülesannete täitmisel sõltumatu ja tegutseb lähtudes IKS-ist, muudest seadustest ja nende alusel kehtestatud õigusaktidest.

²⁴⁵ Article 29 Data Protection Working Party. Advice paper on the practical implementation of the Article 28(6) of the Directive 95/46/EC. Brussels: 04.04.2011, p 3. Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex3_en.pdf, 01.05.2014.

²⁴⁶ Commission staff working paper. Impact assessment, p 18.

²⁴⁷ *Ibid*, Annex 2, p 46.

²⁴⁸ M. Hirvoja, lk 21.

²⁴⁹ E. Rohtmets, L. Kanger, ptk "Hinnang Eesti isikuandmete kaitse seadusele."

²⁵⁰ Fundamental Rights Agency. The role of National Data Protection Authorities, p 6.

Euroopa Kohus sõnastas lahendis C-518/07 vajaduse tagada siseriiklike järelevalveasutuste täielik sõltumatus. Kohtu põhjenduste kohaselt tähendab sõltumatus mitte ainult järelevalveasutuste üle riikliku järelevalve teostamisest tulenevaid mõjutusi, vaid igasuguseid mõjutusi, mis seavad kahtluse alla järelevalveasutuste tegevuse üksikisikute õiguste tagamise ja andmete vaba liikumise vahel tasakaalu loomisel.²⁵¹ Vaatamata kehtivas direktiivis ette nähtud nõudele säilitada järelevalveasutuste sõltumatus, on praktikas mitmes liikmesriigis vajaliku autonoomsuse saavutamiseks peamiseks takistusteks praktilised ja normatiivsed probleemid.²⁵²

3.2.1 Järelevalveasutuste ressursipuudus ja majanduslik sõltumatus

Paljude EL liikmesriikide järelevalveinstitutsioone rahastatakse riigieelarvest (nt Itaalia, Prantsusmaa ja Holland), neist enamike puhul moodustab järelevalveasutuse eelarve justiitsministri poolt määratud eelarve. Teistes liikmesriikides moodustab kogu järelevalveasutuse sissetuleku isikuandmete töötajate teavitustelt makstav tasu ning töötajatele kohaldatavad rahalised sanktsioonid (nt Luksemburg ja Malta).²⁵³

Ressursipuuduses vaevlevad mitmed Euroopa järelevalveasutused, sh Austria, Itaalia, Prantsusmaa ja Portugali omad,²⁵⁴ sealjuures ei ole sel põhjusel osade liikmesriikide järelevalveasutuste esindajatel võimalik regulaarselt osaleda töörühma kokkusaamistel.²⁵⁵

Kehtestamiseks liikmesriikidele ühtsemaid standardeid rahastamise osas ning tagamiseks seeläbi järelevalveasutuste parem sõltumatus, on üldmääruses ette nähtud artikkel 47 (5), mis sätestab liikmesriigi kohustuse tagada järelevalveasutusele piisavalt inim-, tehnilist ja rahalist ressursi ja muid töötamiseks vajalikke vahendeid ning artikkel 47 (6), mis sätestab liikmesriigi kohustuse tagada järelevalveasutusele personal, mis on järelevalveasutuse juhi alluvuses.

Andmekaitse Inspektsiooni puhul otseselt ressursipuudusest rääkida ei saa. AKI-s töötas 2014 1. aprilli seisuga 17 inimest,²⁵⁶ aastal 2013 oli AKI eelarve 631 329 eurot, mis võrreldes teiste riiklike inspektsioonidega ei ole väike (nt keeleinspektsioonile eraldati 296 246 eurot, soolise

²⁵¹ EKo 09.03.2010, C -518/07, *Commission vs Germany*, § 25. Vt ka: EKo 16.10.2012, C-614/10, *Commission vs Austria*.

²⁵² Fundamental Rights Agency. The role of National Data Protection Authorities, p 20.

²⁵³ Commission staff working paper. Impact assessment, Annex 2, p 41.

²⁵⁴ Fundamental Rights Agency. The role of National Data Protection Authorities, p 20.

²⁵⁵ Commission staff working paper. Impact assessment, Annex 2, p 42.

²⁵⁶ Andmekaitse Inspektsioon. Palgaandmed 2014 1. aprilli seisuga. Arvutivõrgus: <https://www.aki.ee/et/palgaandmed-2014-1-aprilli-seisuga>, 01.05.2014.

võrdõiguslikkuse ja võrdse kohtlemise voliniku kantseleile kõigest 62 351 eurot,²⁵⁷ samas kui töötajaid oli aastal 2013 neis inspektsioonides vastavalt 12 ja 4).²⁵⁸

Töörühm on kritiseerinud sätete üldsõnalisust, kuna ainuüksi üldmääruses sätestatud kohustus tagada „piisav ressurss“ ei too ilmselt kaasa muutusi liikmesriikide eelarvepoliitikates seonduvalt järelevalveasutuste rahastamisega. Selleks, et kindlustada järelevalveasutustele piisava ressursi eraldamine ka tegelikkuses, tuleks välja arvestada konkreetne summa, mis tagaks kõigi liikmesriikide järelevalveasutuste minimaalsed vajadused nende ülesannete täitmiseks, mis on kõigi liikmesriikide kohustus. Täiendavalt tuleks lisada summa, mis arvutatakse välja arvestades liikmesriikide elanikkonna suurust ja SKP-d, samuti liikmesriigis paiknevate rahvusvaheliste ettevõtete peakorterite arvu.²⁵⁹

Töö autor on seisukohal, et praeguses sõnastuses ei lahenda üldmäärus järelevalveasutuste ressursipuuduse probleemi. Pidades silmas liikmesriikide väga erinevat suurust ja majanduslikku arengut, ei ole põhjendatud fikseerida konkreetne järelevalveasutustele eraldatav summa, ka riigieelarvest eraldatava summa arvutamine valemi abil ei pruugi osutada tulemuslikuks. Siiski, eeldusel, et järelevalveasutuse rahastamine on vähemalt mingis osas liikmesriigi prioriteetide küsimus, pooldab töö autor selgemate kriteeriumite tutvustamist osas, mida tähendab piisav ressurss, näiteks võiks kaaluda järelevalveasutuste töötajate ametikohtade loomist vastavalt aastast läbi vaadatud keskmisele kaebuste arvule.

Lisaks sellele, kui palju eraldatakse järelevalveasutustele majanduslikke vahendeid, oleneb majanduslik sõltumatus ka sellest, kas järelevalveasutus on oma eelarve osas valitsusasutustest ja teistest sarnastest asutustest sõltumatu. Üldmääruse artikkel 47 (7) näeb ette liikmesriigi kohustuse tagada, et järelevalveasutusel oleks eraldi aastaelarve, mis avalikustatakse. Artikli 47 (7a) kohaselt allub järelevalveasutus eelarve kontrolli mõttes riigi parlamendile.

²⁵⁷ 2013. aasta riigieelarve seadus. - RT I, 28.12.2012, 9.

²⁵⁸ Keeleinspeksioon. Keeleinspeksiooni ametnike palgaandmed 2013. Arvutivõrgus: <http://www.keeleinsp.ee/?menu=32&news=1045>, 01.05.2014; Soolise võrdõiguslikkuse ja võrdse kohtlemise volinik. Ametnike palgaandmed. Arvutivõrgus: <http://www.svv.ee/index.php?id=551>, 01.05.2014.

²⁵⁹ Article 29 Data protection Working Party, Opinion 01/2012, p 17.

AKI majanduslik sõltuvus täidesaatva võimu otsusediskretsioonist ei vasta täieliku sõltumatuse nõudele.²⁶⁰ AKI majanduslikku sõltuvust justiitsministeeriumist on analüüsitud direktiiviga vastavuse kontekstis,²⁶¹ kuid üldmääruse spetsiifilisemat reeglistikku silmas pidades, tuleb ilmselt AKI eelarvega seonduvat regulatsiooni muuta.

Eestis on toodud eeskujuks suuremast majanduslikust sõltumatusest soolise võrdõiguslikkuse ja võrdse kohtlemise voliniku kantselei.²⁶² Soolise võrdõiguslikkuse ja võrdse kohtlemise voliniku kantselei põhimääruse²⁶³ § 4 lg 1 näeb ette, et voliniku ja kantselei tegevuseks vajalikud kulud kaetakse riigieelarvest ning nähakse ette sotsiaalministeeriumi eelarves eraldi real. Soolise võrdõiguslikkuse ja võrdse kohtlemise voliniku rahastamisel on tagatud suurem iseseisvus, kuna puudub ministri kontroll eelarve kinnitamise, muutmise ja täitmise üle.

Direktiiviga võrreldes kõrgemate tingimuste sätestamine järelevalveasutuste majandusliku sõltumatuse tagamiseks on pigem õigustatud. Kuigi kõigis liikmesriikides ei pruugi üldmääruse artiklites 47 (5) ja 47 (6) sätestatud nõuded tagada järelevalveasutusele piisav ressurss olla praktiliselt teostatav, seab üldmäärus sellega siiski üldkehtiva standardi. Eelarvega seonduv regulatsioon sätestab varasemast selgemad nõuded järelevalveasutuse iseseisvaks eelarveks, mis tagab praktikas rakendamisel parema sõltumatuse valitsusasutustest. Üldmääruse artiklites 47 (7) ja 47 (7a) sätestatud nõuded aitavad kõrvalda direktiivi laiast tõlgendamisruumist tulenevad riived järelevalveasutuste sõltumatusele, muuhulgas ka Eesti õiguses.

3.2.2 Järelevalveasutuste institutsionaalne sõltumatus

Lahendis C-518/07 rõhutas EK vajadust tagada järelevalveasutuse organisatsiooniline sõltumatus ning sõltumatus täidesaatva võimu järelevalvest.²⁶⁴ Liikmesriigiti erineb järelevalveasutuste koht riikide õigussüsteemis oluliselt. Kreekas ja Portugalis on sõltumatu järelevalveasutus ette nähtud konstitutsioonis, Maltal ning Hispaanias on järelevalveasutustele antud eriline õiguslik staatus. Prantsusmaal, Hispaanias ja Portugalis määratakse järelevalveasutuste liikmed ametisse protseduuri abil, mis hõlmab nii seadusandliku,

²⁶⁰ Samal arvamusel: K. Käsper. Inimõiguste kaitse riiklik organisatsiooniline raamistik. Arvutivõrgus: <http://humanrights.ee/inimõiguste-aruanne-2/inimõigused-eestis-2012/inimõiguste-kaitse-riiklik-organisatsiooniline-raamistik/>, 01.05.2014.

²⁶¹ E. Rohtmets, L. Kanger.

²⁶² *Ibid*, pkt „Andmekaitse inspeksiooni sõltumatuse riived.“

²⁶³ Soolise võrdõiguslikkuse ja võrdse kohtlemise voliniku ning kantselei põhimäärus. - RT I 2010, 33, 170.

²⁶⁴ EKo 09.03.2010, C -518/07, *Commission vs Germany*, §§ 31-56.

täidesaatva kui ka kohtuvõimu, samas määrab paljudes liikmesriikides järelevalveasutuse personali ainult valitsus või justiitsminister (näiteks Iirimaa, Taani, Holland).²⁶⁵ Ministeeriume ei peeta sõltumatuteks asutusteks ning seetõttu ei peeta olukorda, kus järelevalveasutus on ministeeriumi valitsemisalas (nagu Eestis või Saksamaal) vastavaks sõltumatuse nõudele.²⁶⁶

Vastavalt Andmekaitse Inspeksiooni põhimääruse (edaspidi Põhimäärus) § 1 lg-le 1 on AKI justiitsministeeriumi valitsusalas asuv valitsusasutus. Vastavalt Vabariigi Valitsuse seaduse (edaspidi VVS)²⁶⁷ § 41 lg-le 1 on AKI aruandekohustuslik justiitsministeeriumi ees. VVS § 95 lg 1 kohaselt teostab justiitsminister AKI ja tema ametiisikute tegevuse seaduslikkuse kontrolli. VVS § 101 lg 1 kohaselt lahendatakse valitsus- ja riigiasutuste omavahelised vaidlused alluvuskorras, st AKI ja justiitsministeeriumi vaheline vaidlus tuleks lahendada alluvuskorras, kus justiitsministeeriumil on vaidlustes lõplik sõnaõigus.²⁶⁸

Üldmääruse artikkel 47 (1) sätestab, et järelevalveasutus tegutseb oma kohustuste täitmisel ja volituste teostamisel täiesti sõltumatult ning artikkel 47 (2) sätestab, et järelevalveasutused ei küsi ega võta oma kohustuste täitmisel juhiseid mitte kelleltki.

Vabariigi Valitsus avaldas oma esialgse seisukoha, millest nähtuvalt ei toeta Eesti üldmääruse artiklites 47 ja 48 sätestatud nõuete kehtestamist määruse tasandil, kuna liikmesriigile peab jääma võimalus sobitada andmekaitseasutus üldisesse riikliku järelevalve süsteemi.²⁶⁹

Praegu ei ole AKI institutsionaalne sõltumatus tagatud. Selliselt ei ole praegune olukord kooskõlas ei direktiivi artikliga 28 (1) ega ka üldmääruse artikliga 47 (eelkõige art 47 (2)). AKI on järelevalveasutusena osa täitevvõimu struktuurist, mis ei ole vastavuses võimude lahususe põhimõttega. Veelgi enam – AKI tegevuse üle teostab omakorda järelevalvet justiitsminister, kellel on õigus tunnistada kehtetuks AKI peadirektori akte ja toiminguid, seda mh ebaotstarbekuse tõttu. Justiitsministeeriumi ja justiitsministri ulatusliku mõju tõttu ei ole AKI ei näiliselt ega ka tegelikkuses sõltumatu. Võrdlusena võib tuua soolise võrdõiguslikkuse ja võrdse kohtlemise volinikuga, kes on eraldi institutsioon ning mitte valitsusasutus.

²⁶⁵ Commission staff working paper. Impact assessment, Annex 2, p 41.

²⁶⁶ D. Korff. EC study on implementation of Data Protection Directive. Comparative summary of national laws. Cambridge: September 2002, p 203. - Available: <http://www.garanteprivacy.it/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE,01.05.2014>.

²⁶⁷ Vabariigi Valitsuse seadus. - RT I, 27.12.2013, 33.

²⁶⁸ Rohtmets, L. Kanger, ptk „Andmekaitse inspeksiooni sõltumatuse riived“.

²⁶⁹ Vabariigi Valitsuse 29.03.2012 otsuse seletuskiri, lk 11.

AKI peaks asuma täieliku sõltumatuse tagamiseks riigiasutuste süsteemis väljaspool ühegi ministeeriumi kontrolli nii majanduslikus kui ka organisatsioonilises mõttes. Juhul, kui üldmäärus hakkab kehtima samas või sarnases sõnastuses, annab see loodetavasti tõuke reformida ka AKI rolli ning täpsustada AKI puudutavaid sätteid suures ulatuses, tagamaks selliselt paremini AKI sõltumatus.

Liikmesriikide järelevalveasutuste erinev positsioon ja õiguslik staatus tingib olukorra, kus järelevalveasutuste sõltumatus on tagatud väga erineval tasandil. Üldmääruse artikkel 47 (2) sätestab selgema standardi järelevalveasutuste sõltumatuseks. Arvestades liikmesriikide õigussüsteemide eripära, ei saakski seada spetsiifilisemaid nõudeid, st sätestada täpselt järelevalveasutuste personali määramise korda jms. Direktiivist selgema standardi kehtestamine sunnib aga loodetavasti liikmesriike oma järelevalveasutuste institutsionaalset sõltumatust kriitilisemalt üle vaatama. Järelevalveasutuste täielik sõltumatus, mis mitte ainult ei ole, vaid ka näib olevat, aitab tugevdada andmesubjektide ja andmetöötajate usaldust järelevalveinstitutsiooni, mis omakorda tugevdab järelevalveasutuse rolli ühiskonnas.

3.3 Järelevalveasutuste volitused

Direktiivi artikkel 28 sätestab järelevalveasutustele väga üldised volitused. Direktiivi ülevõtmisel siseriiklikku õigusesse tekkis direktiivi üldsõnalisuse tõttu kaks peamist käsitlust järelevalveinstitutsiooni ülesannetest ja rollist. Soomes, Rootsis ja Iirimaaal nähakse järelevalveasutuste rolle pigem preventiivse ja proaktiivse (nn *ex-ante* roll), samas kui teistes liikmesriikides nagu Läti, Tšehhi ja Kreeka täidab järelevalveasutus pigem jõustamis- ja kontrollifunktsioone (nn *ex-post* roll).²⁷⁰

Tulenevalt erinevatest ülesannetest erinevad ka liikmesriikide järelevalveasutuste volitused oma ülesannete täitmisel varieerudes suunavast ja nõuandlikust rollist nn *ex-ante* rolliga järelevalveasutuste puhul sanktsioonide ja trahvide kehtestamise volitusteni nn *ex-post* järelevalveasutuste puhul.

Direktiivi artikkel 28 (3) sätestab järelevalveasutuse pädevustena eelkõige uurimisvolitused, sekkumisvolitused (anda arvamusi, korraldusi, keelata töötlemine, teha hoiatus või märkus) ning volitused osaleda kohtumenetluses, kui direktiivi kohaselt vastuvõetud siseriiklikke sätteid on rikutud või juhtida kõnealustele rikkumistele õigusasutuste tähelepanu.

²⁷⁰ Fundamental Rights Agency. The role of National Data Protection Authorities, p 20.

Üldmääruse artikkel 53 näeb ette nimekirja järelevalveasutuste volitustest, mis hõlmavad endast nii uurimis-, sekkumis- kui ka esindusvolitusi. Varasemaga võrreldes on volitused üldmääruses selgesõnaliselt sätestatud. Uuendusena on tutvustatud ka järelevalveasutuste volitust kohaldada halduskaristusi. Euroopa Andmekaitseinspektori arvamuse kohaselt on spetsiifilise nimekirja tutvustamine üldmääruses teretulnud.²⁷¹

3.3.1 Uurimisvolitused

Direktiivi artikli 28 (3)(1) kohaselt on iga liikmesriigi järelevalveasutusel uurimisvolitused, näiteks volitused tutvuda töödeldavate andmetega ja koguda oma järelevalvekohustuse täitmiseks vajalikku teavet. Tulenevalt direktiivi üldsõnalisusest on järelevalveasutuste uurimisvolituste ulatus liimesriigiti erinev. Kui enamikes riikides on järelevalveasutustel õigus siseneda andmetöötleja ruumidesse ja territooriumile, siis Prantsusmaal ja Maltal on see lubatud ainult kohtu loal ning Rumeenias puudub selline õigus sootuks.²⁷²

IKS § 33 lg 4 kohaselt on AKI pädeval ametiisikul õigus kontrollimiseks siseneda isikuandmete töötleva territooriumile või ruumi, samuti saada juurdepääs töötleva dokumentidele ja seadmetele, salvestatud andmetele ja kasutatavale tarkvarale.

Üldmääruse artikli 53 (2) sätestab järelevalveasutuse õiguse saada juurdepääs kõikidele isikuandmetele ja kogu teabele, mis on vajalik järelevalveasutusele tema ülesannete täitmiseks (art 53 (2)(a)) ning vastutava või volitatud töötleva tööruumidele (53 (2)(b)).

Töö autor on seisukohal, et uurimisvolituste varasemast selgem väljatoomine aitab ühtlustada liikmesriikide järelevalveasutuste pädevust. Kuigi AKI-le üldmääruses ette nähtud uurimisvolitused olulist muutust kaasa ei too, võivad erinevad uurimisvolitused (õigemini nende puudumine) takistada osades liikmesriikides rikkumiste avastamist ja seega viia ebaühtlase õiguste kaitse tasemeni Euroopa Liidus. Järelevalveasutuste uurimisvolituste täpsem sätestamine üldmääruses on õnnestunud ja positiivne muutus.

3.3.2 Sekkumisvolitused

Direktiivi artikli 28 (3) kohaselt on järelevalveasutuse tõhusad sekkumisvolitused eelkõige õigus avaldada artikli 20 kohaselt arvamust enne töötlemise alustamist ja tagada sellise

²⁷¹ European Data Protection Supervisor, p 39. Samal arvamusel: G. Hornung. A general Data Protection Regulation for Europe? Light and shade in the commissions draft of 25 January 2012. - Scripted 2012/9, No. 1, p 78.

²⁷² Fundamental Rights Agency. The role of National Data Protection Authorities, p 21.

arvamuse asjakohane avalikustamine, anda korraldusi, keelata töötlemine või teha andmetöötlejale märkus, samuti näeb direktiiv ette õiguse suunata küsimus liikmesriigi parlamenti või teistesse poliitilistesse institutsioonidesse.

Liikmesriikide järelevalveasutused kasutavad sekkumisvolitusi viimase võimalusena – järelevalveasutused näevad endal pigem nõuandvat ja lepitavat rolli.²⁷³ Järelevalveasutuste sekkumisvolitused erinevad liikmesriigiti oluliselt – osades riikides on teatud juhtudel järelevalveasutusel õigus autoriseerida andmetöötlejaid andmeid töötleva, samas kui teistes mitte; kui enamikes liikmesriikides on järelevalveasutusel volitus nõuda andmete kustutamist või hävitamist, siis Belgias, Saksamaal ja Suurbritannias see õigus puudub; osades liikmesriikides nagu Austria, Taani ja Bulgaaria on kohustuslik, et enne siduvate meetmete tarvitusele võtmist oleks kasutatud soovitusi, arvamusi või hoiatuste tegemist.²⁷⁴

Eestis on AKI poolt läbi viidav menetlus haldusmenetlus, mida alustatakse reeglina HMS § 35 ning IKS § 33 alusel.²⁷⁵ AKI-l on haldusmenetluse raames õigus teha ettepanekuid puuduste kõrvaldamiseks ning vajadusel ettekirjutusi ja vaideotsuseid (IKS § 40). Olukorras, kus rikkumist ei kõrvaldata ka pärast ettekirjutust, on AKI-l õigus IKS § 42 ja § 43 sätestatud juhtudel viia läbi väärteomenetlus.

Üldmääruse artikkel 53 (1) sätestab ammendava loetelu järelevalveasutuste õigustest, muuhulgas volitus nõuda andmetöötlejalt rikkumise kõrvaldamist „kindlal viisil“, anda välja käsk, teha hoiatusi ja märkusi, nõuda andmete kustutamist, keelata andmete töötlemine, anda välja isikuandmete töötlemisega seonduvaid arvamusi ja teavitada parlamenti, valitsust või muud poliitilist institutsiooni või avalikkust isikuandmete kaitsega seonduvatest teemadest.

Üldmäärusega kehtestatav nimekiri volitustest aitab kõrvaldada andmekaitseasutuste sekkumisvolituste erinevused, muuhulgas näeb ette pädevuse kõigil järelevalveasutustel nõuda andmete töötlemise lõpetamist ja andmete kustutamist.

Üldmääruse kehtivast sõnastusest ei ole võimalik aru saada, kas järelevalveasutuse poolt tehtavad käsud, märkused ja ettekirjutused oleksid käsitletavad haldusmenetluse toimingutena, kas nad alluksid kontrollile haldusmenetluse raames või millised on võimalused nende käskude, märkuste ja hoiatuste vaidlustamiseks. Samuti jääb ebaselgeks, millised on õiguslikud tagajärjed ette nähtud kohustuste täitmata jätmisel. Üldmääruse artiklis 53 (1)

²⁷³ D. Korff, p 206.

²⁷⁴ Fundamental Rights Agency. The role of National Data Protection Authorities, p 23.

²⁷⁵ Välja arvatud avaliku teabe seaduse alusel läbi viidav menetlus.

sätetatud järelevalveasutuse volituste ning artiklis 53 (4) ja artiklis 79 sätestatud õiguse kohaldada haldusrikkumise puhul sanktsioone omavaheline suhe pole piisavalt selge.²⁷⁶

Sisuliselt on sätestab IKS juba praegu kõik üldmäärusega ettenähtavad sekkumisvolitused. AKI teeb hoiatusi ja märkusi, milles palub rikkumine lõpetada nii ettekirjutuste kui muude haldusmenetluse vahendite kaudu, teabenõuete kaudu kohustab andmetöötletajat esitama informatsiooni ning hoiatab töötlejaid sunniraha kohaldamise eest.

Töö autor on seisukohal, et sekkumisvolituste täpsustamine aitab kaasa järelevalveasutuste rolli tugevdamisele ja ühtlustamisele liidus. Üldmäärus aitab ühtlustada liikmesriikide sekkumisvolitusi, kuigi täpsustamist vajab sekkumisvolituste ja järelevalveasutuste sanktsioonide kohaldamise õiguse omavaheline suhe. Omaette küsimus on see, kas ja millises ulatuses olemasolevaid volitusi kasutatakse – näiteks Luksemburgis kasutati aastal 2009 - 2011 volitust teha hoiatus üks kord, Küprosel 8 ning Rumeenias 66.²⁷⁷ Volituste kasutamine liikmesriigi siseselt on aga probleem, millega üldmääruse tasemel ei saagi tegeleda.

3.3.3 Halduskaristused

Asjaolu, et järelevalveasutused teevad pigem rikkujale meeldetuletusi ja hoiatusi, ei ole iseenesest halb, kuid need meetmed oleksid efektiivsemad, kui neid toetaks efektiivsed jõustamismeetmed, puhuks, kui rikkujate teistele meetmetele ei allu.²⁷⁸

Direktiiv eraldi halduskaristuste regulatsiooni ette ei näe, siiski on trahvide ja teiste karistava iseloomuga meetmete kasutamine liikmesriikides laialt levinud. Kõige enam kasutatakse karistatavatest meetmetest trahvide tegemise võimalust, aga ka õigust tühistada andmetöötletaja luba andmete töötlemiseks. Trahvide tegemise tihedus ja suurus erineb liikmesriigiti oluliselt. Kuigi siinkohal ei saa jätta arvestamata liikmesriikide suurust ning järelevalveasutuste prioriteete (osad liikmesriigid keskenduvad ennetusele), on erinevused siiski märkimisväärsed. Ajavahemikus 2009 - 2011 määrasid järelevalveasutused trahve Rootsis kaks ning Suurbritannias üheksa korda, samas kui Hispaanias määras järelevalveasutus trahve 1715 korda (vrld Eesti 101 ning Läti 68). Trahvide suurused erinevad Sloveenias üksikisikule

²⁷⁶ European Data Protection Supervisor, p 39.

²⁷⁷ Fundamental Rights Agency. Access to data protection remedies in EU Member States. Data protection remedies at national level. Luxemburg: Publications office of the European Union, 2013, p 21.

²⁷⁸ D. Korff, p 207.

määratavast maksimumkaristusest 830 eurot kuni Suurbritannias ja Hispaanias määratava 500 000 euron. ²⁷⁹

IKS § 40 lg 1 kohaselt on AKI-l õigus teha isikuandmete töötlejale ettekirjutusi. IKS § 40 lg 2 kohaselt võib AKI rakendada ettekirjutuse mittetäitmisel sunniraha ülemmääraga 9600 eurot, v.a riigiasutuste suhtes. Kui riigiasutusest isikuandmete töötleja ei ole ettekirjutust määratud tähtjaks täitnud, pöördub AKI halduskohtusse. Väärteomenetluses on määratava trahvi suuruseks kuni 300 trahviühikut või juriidiliste isikute puhul 32 000 eurot.

Üldmääruse artikli 53 (4) ja üldmääruse artikli 79 eesmärgiks on anda järelevalveasutustele halduskaristuste määramise õigus. Artikli 79 (2a) kohaselt on järelevalveasutus kohustatud igapäevale, kelle tegevus ei ole üldmäärusega kooskõlas, kohaldama ühe järgnevatest karistustest: hoiatuse (esmakordsete ja mittetahtlike rikkumiste puhul), regulaarse isikuandmete kaitse auditi või trahvi kuni 100 000 000 eurot või kuni 5% ettevõtte aastasest ülemaailmsest sissetulekust, olenevalt sellest kumb summa on suurem.

Üldmääruses tutvustatud halduskaristustega seonduvalt on kerkinud üles mitmeid probleeme. Esiteks ei ole üldmääruses üheselt arusaadav, kas artiklis 79 (2a) märgitud „rahatrahvide“ näol on tegemist sunniraha või väärteokaristusega. Eesti õiguse mõttes on sellel oluline vahe. ²⁸⁰

Eesti siseriiklikus õiguses on väärteokaristuse ja sunniraha iseloom täiesti erinev, sealjuures on sunniraha mõjutusvahend ja mitte karistus. ²⁸¹ Halduskaristuse ja väärteokaristuse eristamisest oleneb see, kas karistust saab rakendada korduvalt ning kas karistus tuleks kanda karistusregistrisse. ²⁸² Juhul, kui artiklis 79 sätestatud halduskaristusi käsitleda väärtegude eest mõistetavate trahvidena, laiendab see oluliselt ka väärteokoosseise, kuna sellisel juhul muutub iga üldmääruse rikkumisega seonduv tegu väärteoks. See omakorda suurendaks oluliselt AKI koormust väärtegude menetlejana ning poleks ilmselt praktikas teostatav.

Üldmäärusega kehtestatavad sekkumisvolitused (art 53), karistused (art 78) ja halduskaristused (art 79) ei ole piisavalt täpselt piiritletud ega arvesta liikmesriikide siseriiklike õigussüsteemide erinevusega. Kavandatavate halduskaristuste mõistest ei nähtu,

²⁷⁹ Fundamental Rights Agency. Access to data protection remedies, p 21.

²⁸⁰ Vabariigi Valitsuse 29.03.2012 otsuse seletuskiri, lk 10.

²⁸¹ Riigikohtu üldkogu leidis lahendis 3-2-1-4-13, et sunnirahal puudub nii materiaalselt kui formaalselt karistuslik iseloom. Vt: RKÜK 3-2-1-4-13 p 40, 17.12.2013.

²⁸² Eestis on väärteo- ja halduskaristuste erinevust käsitletud J. Sootak. Vt: J. Sootak. Karistusõiguse revisjon kuriteo-, väärteo- ja haldusõiguse piirimail. - Juridica 2013/IV.

millisel eesmärgil peaks neid kohaldama (kas karistamiseks või mõjutamiseks), kas need võib kohaldada korduvalt ning kas halduskaristuse kohaldamise andmed kantakse riiklikku registrisse või mitte. Efektiivseks toimimiseks tuleks halduskaristustega seonduvat üldmääruses täpsustada.

Teiseks on kritiseeritud üldmääruses sätestatud jäikasad ja segaseid aluseid halduskaristuste kohaldamiseks. Üldmääruses on oluliselt piiratud järelevalveasutuse diskretsiooni osas, millal kohaldada kirjalikku hoiatust ning millal auditit ja/või trahvi. Kirjalikku hoiatust võib kohaldada ainult juhul, kui tegemist on esmakordse ja tahtmatu rikkumisega. Samas ei ole üldmääruses sätestatud, kas halduskaristusi võib kohaldada kumulatiivselt (nt kas võib korraga kohaldada trahvi ja auditit), kuidas suhestuvad artiklis 53 toodud sekkumisvolitused halduskaristustesse (nt kuidas suhestub art 53 (1)(e) ette nähtud hoiatus art 79 (2a)(a) ette nähtud hoiatusesse) ega erista halduskaristuse määramise alusena andmetöötaja poolt mõne üldise nõude täitmata jätmist spetsiifilise juhise eiramisest.²⁸³

Euroopa Andmekaitseinspektor on viidanud vajadusele tagada suurem paindlikkus halduskaristuste määramisel.²⁸⁴ Töörühm on rõhutanud vajadust halduskaristuse määramisel arvestada järelevalveasutuste erinevaid prioriteete.²⁸⁵ AKI arvates kehtestab üldmäärus liialt jäiga sunni- ja karistusmehhanismi, kuna ette nähtud regulatsioon selle kohta, millal võib hoiatada ja millal trahvida, on liiga spetsiifiline.²⁸⁶

Töö autor on seisukohal, et halduskaristuse kohaldamise alused on üldmääruses sätestatud ebaselgelt ega ole praeguses sõnastuses praktikas rakendatavad. Üksikisikute õiguste kaitset ei ole võimalik tagada ebaselgete volitustega väga koormavate meetmete kasutamiseks. Ette nähtud meetmed on liiga karmid, eelkõige osas, mis lubab kirjalikku hoiatust kohaldada ainult esmakordsel ja tahtmatul rikkumisel.

Kolmandaks on paljude riikide seas tekitanud pahameelt määratavate halduskaristuste suurus. Üldmääruse artikli 79 (2a)(c) kohaselt võib teha trahvi kuni 100 000 000 eurot või kuni 5% ettevõtte aastasest ülemaailmsest sissetulekust, olenevalt sellest kumb summa on suurem.

Üldmääruses kehtestatavate haldustrahvide suurust põhjendati vajadusega tugevdada järelevalveasutuste mõju sekkumisvolituste rakendamisel. Väikesed rahalised karistused ei

²⁸³ European Data Protection Supervisor, p 45.

²⁸⁴ *Ibid.*

²⁸⁵ Article 29 Data protection Working Party, Opinion 01/2012, p 18.

²⁸⁶ V. Peep, lk 2.

olnud piisavaks hoiatuseks suurtele ettevõtetele andmete töötlemisega seonduvatest rikkumistest hoidumiseks. Seoses üldmääruses sätestatud halduskaristuste suurusega Eestis on Vabariigi Valitsus avaldanud arvamust, et ette nähtud halduskaristuse suurus on ebamõistlikult suur.²⁸⁷

Töö autor nõustub Vabariigi Valitsuse seisukohaga osas, et Eesti kontekstis on rahatrahvina nimetatud halduskaristuse määr, st kuni 100 000 000 euro suurune rahatrahv, ebaproportsionaalselt suur. Kuigi üldmääruse artikkel 79 (2a)(c) näeb ette trahvi suuruse ülemmäära, on 100 000 000 euro suurune trahvi ülemmäär Eesti kontekstis ebaproportsionaalne. Vaatamata sellele, et maksimaalset karistust tegelikkuses tõenäoliselt ei kohaldata, kahjustab see oluliselt õiguskindlust, kuna karistuse määr võib olla täiesti ettearvamatu. Lisaks näeb üldmääruse artikkel 79 (7) ette komisjoni volitused võtta vastu delegeeritud õigusakte eesmärgiga ajakohastada haldustrahvide kogusummat. Selline tõlgendus ei võimalda isikuandmete töötlejatele õiguselgust, kuna tegelikkuses ei ole isegi üldmäärusega tagatud õiguskindlust kohaldatavate halduskaristuste osas.

Töö autori arvates ei arvesta kavandatav süsteem liikmesriikide siseriikliku õiguse eripäradega. Ette nähtud halduskaristuste piirmäärad võivad olla efektiivsed suurtes Kesk-Euroopa liikmesriikides, kuid Eestis põhjustaks 100 000 000 euro suurune halduskaristus iga kohaliku ettevõtte maksejõuetuse. Juhul kui nii suuri karistusi tegelikkuses ei kohaldataks, ei took see kaasa ka soovitud järelevalveasutuste rolli tugevdamist, sest järelevalveasutused rakendaksid jätkuvalt trahve ulatuses, mis on neile tavapärane.

Tulenevalt mitmetest ebaselgustest seonduvalt halduskaristuste eesmärgi ja sekkumisvolituste ja halduskaristuse kohaldumisalast, ei too üldmääruses ette nähtud halduskaristused kaasa järelevalveasutuste rolli tugevdamist. Ebaselge regulatsioon ning liiga jäigad (või umbmäärased) reeglid viivad selleni, et praktikas ei hakka järelevalveasutused üldmääruses ette nähtud meetmeid kasutama. Lisaks riivatakse ebaproportsionaalselt karmide halduskaristuse kohaldamise tingimuste (teistkordsel rikkumisel määratakse juba trahv või audit) ning karistuste ebaproportsionaalse suuruse tõttu oluliselt ettevõtjate õigusi.

3.3.4 Esindamisvolitused

Osades liikmesriikides, näiteks Sloveenias, on järelevalveasutustel pädevus algatada ise menetlus konstitutsioonikohtus, osade liikmesriikide seadus näeb ette järelevalveasutuse

²⁸⁷ Vabariigi Valitsuse 29.03.2012 otsuse seletuskiri, lk 10.

õiguse juhtida õiguskaitseasutuste tähelepanu isikuandmete töötlemise nõuete rikkumisele.²⁸⁸ Eesti, Läti ja Austria on ainsad riigid, kelle seadusandlus ei sätesta selgesõnaliselt järelevalveasutuse õigust juhtida õigusasutuste tähelepanu isikuandmete töötlemise nõuete rikkumisele.²⁸⁹ Osades liikmesriikides on kohtusse pöördumise õigus üksnes erasektori andmetöötlejatega seoses (vrđl IKS § 40 lg 4 – AKI pöördub protestiga halduskohtusse, kui riigiasutusest andmetöötleja ei täida AKI ettekirjutust).

Direktiivi artikkel 28 (3) näeb ette järelevalveasutuse volitused osaleda kohtumenetluses, kui direktiivi kohaselt vastu võetud siseriiklikke sätteid on rikutud või juhtida vastavatele õigusasutustele tähelepanu.

IKS-i kohaselt osaleb AKI kohtumenetluses juhul, kui riigiasutusest andmete töötleja ei täida AKI ettekirjutust selleks ette nähtud tähtaja jooksul (IKS § 40 lg 4). IKS § 44 lg 2 kohaselt on AKI olukorras, kus rikutakse delikaatsete isikuandmete töötlemise registreerimise kohustust või ei täideta AKI ettekirjutust, AKI kohtuväliseks menetlejaks väärteomenetluses. IKS-i kohaselt on seega AKI pädevuses lahendada isikute kaebusi ning viia läbi väärteomenetlust. Kuna AKI on väärteomenetluse korral ise kohtuväliseks menetlejaks ning haldusmenetluse korral on AKI-l õigus kohtusse pöörduda, puudub IKS-is vajadus eraldi sätestada AKI pädevus juhtida õigusasutuste tähelepanu isikuandmete töötlemise nõuete rikkumisele.

Üldmääruse artikli 53 (3) kohaselt on järelevalveasutusel õigus juhtida õigusasutuste tähelepanu üldmääruses sätestatud nõuete rikkumisele ja osaleda kohtumenetluses, eelkõige vastavalt artiklitele 74 (4) ja 75 (2). Vastavalt üldmääruse artiklile 74 (4) on andmesubjektil õigus nõuda, et tema elukohariigi järelevalveasutus esitaks tema nimel taotluse alustada menetlust teise riigi järelevalveasutuse suhtes, kes on teinud andmesubjekti kohta otsuse. Üldmääruse artikli 75 (2) kohaselt algatatakse menetlus vastutava töötleja vastu selles riigis, kus vastutav töötleja asub või alternatiivselt kus asub andmesubjekti alaline elukoht, v.a juhul kui andmetöötleja on avaliku sektori ametiasutus.

Olulisi muutusi seoses esindamisvolitustega üldmääruse kehtima hakkamine võrreldes praeguse Eestis kehtiva regulatsiooniga kaasa ei too. Vaatamata sellele, et IKS-is ei ole AKI esindamisvolitusi sõnaselgelt ette nähtud, on AKI-l võrreldes teiste liidu riikidega ulatuslikud esindamispädevused. Üldmääruses sätestatud esindamisvolitused võimaldavad Euroopa Liidu

²⁸⁸ Fundamental Rights Agency. The Role of National Data Protection Authorities, p 26.

²⁸⁹ *Ibid*, p 25.

tasandil järelevalveasutuste pädevust ühtlustada, see võib positiivselt mõjutada ka rahvusvahelise koostöö tegemise võimalusi.

3.4 Liikmesriikide järelevalveasutuste rahvusvaheline koostöö

Isikuandmete kaitse reformi üheks keskseks lähtepunktiks on järelevalveasutuste riikidevahelise koostöö suurendamine. Direktiivi artiklis 28 (6) ette nähtud kohustust rahvusvaheliseks koostööks on siseriiklikesse õigustesse inkorporeeritud erinevalt. Taani, Prantsusmaa ja Portugali siseriiklike regulatsioonide kohaselt on järelevalveasutused kohustatud teise järelevalveasutuse palvel tegutsema, samas mitmetes liikmesriikides (Tšehhi, Eesti) on ette nähtud üldine säte, mille kohaselt liikmesriigi järelevalveasutus teeb koostööd välisriikide järelevalveasutustega.²⁹⁰

Järelevalveasutuste esindajad on seisukohal, et puudub efektiivne mehhanism, mis reguleeriks järelevalveasutuste koostööd, mistõttu kasutatakse vastastikuse abi puhul pigem konventsiooni 108 vastastikuse abi sätteid.²⁹¹ Erakordselt problemaatiline on olukord siis, kui järelevalveasutuste poolt kindlaks määratud jurisdiktsioon ja kohalduv õigus ei ühildu ning pole selge, millise liikmesriigi järelevalveasutusel on pädevused, millist õigust tuleb kohaldada ning mida tuleks teha olukorras, kui liikmesriikide materiaalõiguse normid seonduvalt isikuandmete kaitsega erinevad oluliselt. Koostööd viiakse läbi pigem mitteametlikul tasandil, vastavalt sellele, kas ja millist kolleegi teise riigi järelevalveasutusest tuntakse, puudub kindlaksmääratud kontaktisik.²⁹²

Vajadust tegutseda rahvusvahelisel tasandil tuleb globaliseerivas maailmas üha tihedamini ette. Iseloomulik näide on *Google*'iga juhtunu. *Google* alustas aastal 2007 oma programmi *Street View*, mille eesmärgiks oli pildistada *Google*'i spetsiaalsete autodega üles kõik läbitavad teed Euroopas, et pakkuda *Google*'i kasutajatele võimalust saada 360° panoraamvaade kohtadest, kust *Google*'i autod on läbi sõitnud. *Google*'i tegevus ärritas mitmete liikmesriikides järelevalveasutusi. Paljudes riikides seati *Google*'ile täiendavaid tingimusi (nt kohustus teavitada elanikke ette autode saabumisest teatud piirkonda). 11.05.2009 peatati *Google*'i autode tegevus Kreekas seoses algatatud uurimisega, 22.05.2010 teatas Šveits, et koostöös Euroopa Andmekaitseinspektoriga on alustatud uurimist seoses *Google*'i autode poolt kogutud informatsiooniga, mida autod kogusid inimeste traadita võrgu

²⁹⁰ Commission staff working paper. Impact assessment, Annex 2, p 45.

²⁹¹ *Ibid.*

²⁹² Article 29 Data Protection Working Party. Advice paper on the practical implementation of the Article 28(6), p 1.

levialadest, 28.05.2010 keelas Austria *Google*’il autode kasutamise. Erinevates liikmesriikides algatatud uurimise tulemusena määrati *Google*’le liikmesriigiti ulatuslikke trahve – Prantsusmaa järelevalveasutus määras ettevõttele trahvi 100 000 eurot, Itaalia 1 miljonit eurot, Saksamaa 145 000 eurot, samas mitmes liikmesriigis ei olnud *Google*’il oma tegevusega mingeid probleeme.²⁹³ Eeltoodu ilmestab järelevalveasutuste puudulikku koostööd, mis viib liikmesriigiti ebaühtlase õiguse kohaldamiseni.

Üldmäärusega soovitakse lahendada rahvusvahelise koostööga seonduvad probleemid, tutvustades uue supranatsionaalse institutsioonina Euroopa Andmekaitsekoogu, *one-stop shop* printsiipi ning järjepidevusmehhanismi.

3.4.1 Euroopa Andmekaitsekoogu

Direktiivi artikkel 29 alusel loodud töörühm on nõuandev organ, kes peaks aitama kaasa isikuandmete kaitse ühtlustamisele Euroopa Liidu tasandil. Töörühm on vastu võtnud ligi 200 arvamust, mis selgitavad direktiivis sätestatud mõisteid ning käsitlevad spetsiifilisi teemasid, näiteks andmete edastamist kolmandatesse riikidesse.²⁹⁴

Tegelikkuses on töörühma roll andmekaitsereeglite ühtlustamisel olnud pigem tagasihoidlik – liikmesriigid on oma siseriiklikku õigust täiustanud vastavalt töörühma arvamustele paaril korral. Töörühm on rõhutanud vajadust tugevdada töörühma kesket rolli, muuhulgas muutes selle otsused järelevalveasutustele siduvaks, samuti on rõhutatud vajadust suurendada töörühma rolli rahvusvaheliste juurdluste läbiviimisel ja koordineerimisel.²⁹⁵

Üldmääruste artikli 64 alusel luuakse Euroopa Andmekaitsekoogu (edaspidi EAN), kes hakkab asendama direktiivi alusel loodud töörühm. Sarnaselt direktiivi artiklis 29 (2) sätestatule, kuuluvad üldmääruse artikli 64 alusel Andmekaitsekookku iga liikmesriigi järelevalveasutuse juht ning Euroopa Andmekaitseinspektor. Komisjoni esindajal on õigus osaleda EAN-i tegevustes ja koosolekutel ning EAN teavitab komisjoni kõigist oma tegevustest. EAN annab sarnaselt töörühmale, mittesiduvaid otsuseid üldmääruse kohaldamise ja selle alusel antavate õigusaktide kohta, propageerib ja koordineerib järelevalveasutustevahelist koostööd ning edendab ühiste koolitusprogrammide korraldamist ja hõlbustab personalivahetust järelevalveasutuste vahel.

²⁹³ Electronic Privacy Information Centre. Investigations of Google Street View. Available: <http://epic.org/privacy/streetview/>, 01.05.2014.

²⁹⁴ Commission staff working paper. Impact assessment, Annex 2, p 46.

²⁹⁵ Article 29 Data Protection Working Party. Advice paper on the practical implementation of the Article 28(6), p 6.

EAN jätkab suuresti tööühma ülesandeid, kuid need on varasemast oluliselt selgemini üldmäärusesse kirja pandud.²⁹⁶

Töö autori arvates on Euroopa Andmekaitsekoostöö loomine positiivne muudatus, mis võimaldab paremini ja selgemini koordineerida rahvusvahelist koostööd. EAN-i keskne roll realiseerub aga järelevalvemehhanismi rakendamisel, mida käsitletakse punktis 3.4.3.

3.4.2 *One-stop shop* printsiip

Tutvustatavat *one-stop shop* (edaspidi OSS) printsiipi on peetud andmekaitse reformi üheks olulisemaks uuenduseks ning üheks neljast reformi alussambast.²⁹⁷ Teisalt on vastuoluline printsiip üheks põhjuseks, miks isikuandmete kaitse regulatsiooni reform ei ole edenenud esialgu loodetud tempos.²⁹⁸ OSS printsiibi eesmärgiks on selgitada järelevalveasutuste kohustuste ja vastutuse jagunemist olukorras, kus rahvusvaheline ettevõtte on pannud toime isikuandmete töötlemisega seonduvaid rikkumisi mitmes liikmesriigis.

Ettevõtteid puudutava OSS põhimõtte kohaselt on vastavalt üldmääruse artiklile 54a (1) mitmes liikmesriigis toimiva piiriülese isikuandmete töötlemise puhul rikkumise korral juhtivaks järelevalveasutuseks selle riigi järelevalveasutus, kus asub töötleja peamine tegevuskoht. Üldmääruse artikli 4 (13) kohaselt on peamine tegevuskoht vastutava või volitatud töötleja ettevõtte või ettevõtete grupi tegevuskoht, kus tehakse peamised otsused isikuandmete töötlemise eesmärkide, tingimuste ja vahendite kohta. Muuhulgas võib peamise tegevuskoha üle otsustamisel lähtuda sellistest objektiivsetest kriteeriumitest nagu vastutava või volitatud töötleja peakontori asukoht, ettevõtte üksuse asukoht, mis on asukoha mõttes parim juhtivfunktsioonide ja administratiivsete kohustuste täitmiseks ja määruses sätestatud reeglite jõustamiseks või asukoht, kus efektiivne ja tegelik juhtimistegevus aset leiab.²⁹⁹

OSS printsiibi tulemusena peaks Euroopa Liidus tegutsevad rahvusvahelised ettevõtted nüüd tegemist tegema ainult ühe järelevalveasutusega. Eelduslikult alandab selline muutus ettevõtete kulusid ning lihtsustab äri tegemist Euroopas, tagades samal ajal üksikisikute parema kaitse.³⁰⁰

²⁹⁶ P. Schwartz, p 1099.

²⁹⁷ European Commission MEMO 12.03.2014.

²⁹⁸ W. K. Hon *et al*, p 7.

²⁹⁹ Käesoleva töö kirjutamise hetkeks ei ole üldmääruse uuemat sõnastust eesti keelde tõlgitud, mistõttu üldmääruse art 4 (13) eesti keelse versiooni näol tegemist autori tõlkega.

³⁰⁰ Commission staff working paper. Impact assessment, Annex 5, p 98.

Oktoobris 2013 jõuti EL justiits- ja siseküsimuste nõukogus põhimõttelisele kokkuleppele selles, et mingisugune mehhanism riigiüleseks koostööks on vajalik, et lahendada rahvusvaheliste ettevõtetega seotud probleeme.³⁰¹

Euroopa Parlamendi poolt kinnitatud sõnastuses on OSS printsiip kompromiss, kuna sooviti leida tasakaal juhtiva järelevalveasutuse kui üksnes teabevahendaja ja koordineerija ning teisalt järelevalveasutuse kui rahvusvahelise menetluse juhi vahel. Kompromissi kohaselt on juhtival järelevalveasutusel ainuõigus võtta vastu ettevõtte suhtes regulatiivseid meetmeid, kuid samal ajal on juhtiv järelevalveasutus kohustatud tegema ulatuslikku koostööd teiste järelevalveasutustega ning oma tööd nendega koordineerima.³⁰²

Ministrite Nõukogu koosolekul 07. ja 08.10.2013 olid enamike liikmesriikide esindajad selle poolt, et jätkata just sellise mehhanismi täiendamist, mille puhul langetab otsuse küll peamise tegevuskoha järgne juhtiv järelevalveasutus, kuid selle asutuse pädevusi piiratakse teatud ulatuses, kuid toetati ka koosotsustamise mehhanismi ning osad liikmesriigid ei ole veel küsimuses seisukohta võtnud.³⁰³

Viimase toimunud arutelu kohaselt on otsustatud jätkata suunal, kus juhtival järelevalveasutusel on vastavalt ettevõtte peamisele tegevuskohale peamine pädevus, kuid pädevus ei pruugi olla eksklusiivne ning seda võib teatud juhtudel piirata. Samuti on arutatud võimalust, kus juhtiva järelevalveasutuse korraldusi viib liikmesriigi poolt ellu ikkagi ainult kohalik järelevalveasutus koostöös juhtiva järelevalveasutusega – näiteks võib tuua olukorra, kus juhtiv järelevalveasutus palub kohalikul järelevalveasutusel viia läbi audit, et saada informatsiooni võimalike rikkumiste kohta ja seejärel otsustada regulatiivsete meetmete kohaldamine.³⁰⁴

Siiski on jätkuvalt liikmesriikide vahel vaidlused osas, kuidas jõuda OSS printsiibi kasutamiseni praktikas. Printsiibi rakendamine on tõstatanud väga palju küsimusi „peamise tegevuskoha” mõiste selgusest,³⁰⁵ aga ka peamise tegevuskoha järelevalveasutuse ja teiste ettevõtetega seotud järelevalveasutuste pädevuse piiritlemisest.³⁰⁶ Vastavalt artiklile 54a (2) omab juhtiv järelevalveasutus ainupädevust otsustamiseks vastutavale töötajale kohaldatavate

³⁰¹ The Council of European Union press release. 3260th Council meeting. Justice and home affairs. PR CO(2013) 14149. Luxembourg: 07. - 08.10.2013, p 7.

³⁰² C. Kuneret *al*, p 4.

³⁰³ The Council of European Union press release, p 7.

³⁰⁴ The Council of Europe. Note from Presidency. 5882, 31.01.2014, p 4. Available: <http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&f=ST%205882%202014%20INIT>, 01.05.2014.

³⁰⁵ Article 29 Data protection Working Party, Opinion 01/2012, p 18.

³⁰⁶ *Ibid*; European Data Protection Supervisor, p 39.

meetmete üle. Nii Euroopa Andmekaitseinspektor kui töörühm on oma seisukohtades rõhutanud, et juhtiva andmekaitseorgani pädevus ei peaks olema eksklusiivne, vaid peaks pigem kohustama juhtivat järelevalveasutust juhtima koostööprotsessi teiste järelevalveasutustega teistes liikmesriikides ning tagama vastastikuse abi ja koostöö.³⁰⁷

Töö autori arvates on valitud õige mudel, mille edasi arendamist jätkata. Juhtiva järelevalveasutuse olemasolu võimaldab koondada järelevalveasutuste vastutust ja sellest tulenevalt tagada parem koostöö, samas kui nende järelevalveasutuste kasutamine, mis asuvad kohas, kus andmed töödeldakse, võimaldab leida lahendusi siseriiklikul tasandil. Juhtiva järelevalveasutuse pädevus on piiritletud õnnestunult – vaatamata artiklis 54a (2) sätestatud ainuvolitustele kohaldada õiguslike tagajärgi omavaid meetmeid, näeb sama säte ette ka põhjaliku konsulteerimise ja teiste järelevalveasutuste ärakuulamise kohustuse. Selliselt on otsustamisprotsessi kaasatud kõik asjaomased järelevalveasutused, kuid lõplik vastutus meetmete kohaldamiseks lasub ühel järelevalveasutusel. Lahendus võimaldab suurendada õiguskindlust samal ajal tugevdades järelevalveasutuste koostööd.

Eelviidatud lahendus tõstatab aga uue probleemi. Juhul, kui juhtiv järelevalveasutus teeb otsuse rakendada meetmeid, tekib vajadus seda otsust tunnustada ja täita teistes liikmesriikides. Üldmäärus ei reguleeri teises riigis vastu võetud otsuse tunnustamise küsimust. Eesti on rõhutanud vajadust tegeleda haldusotsuse rakendamise temaatikaga teises liikmesriigis ning kaaluda muuhulgas haldusmenetluse läbiviimist reguleerivate sätete sisseviimist üldmäärusesse.³⁰⁸

OSS printsiibi kohaldamine üldmääruses kavandatud versioonis põhineb eeldusel, et üldmääruse kehtima hakkamisel on kõikides liikmesriikides tagatud ühtne isikute õiguste kaitse ning ühtsed järelevalve- ja jõustamismehhanismid, samuti piisav ressurs järelevalveasutuste efektiivseks toimimiseks. Töö autor ei usu, et menetlussätete tutvustamisega oleks võimalik ületada siseriiklikud haldussüsteemide erisused (muuhulgas erinevate haldusotsuste ja väärtootsuste olemuslikud küsimused). Pidades silmas seda, et üldmäärusele heidetakse ette liigset detailsust, suurendaks haldusmenetluse reeglite tutvustamine vastumeelsust üldmääruse osas liikmesriikide seas veelgi. Samas, pidades silmas üldmääruse artiklis 54a (2) sätestatud ulatuslikku koostöökohustust, peaks olema võimalik kõrvaldada ka suuremad probleemid juhtiva järelevalveasutuse otsuse jõustamisel, kuna juhtiv

³⁰⁷ Article 29 Data protection Working Party, Opinion 01/2012, p 18.

³⁰⁸ Vabariigi Valitsuse 29.03.2012 otsuse seletuskiri, lk 2.

järelevalveasutus saaks meetmete valimisel arvestada teiste puudutatud liikmesriikide siseriiklike õiguste eripärasid ning võimalusi meetme jõustamiseks.³⁰⁹

OSS printsiip näeb ühelt poolt ette kohustust ulatuslikuks konsulteerimiseks ning teisalt sätestab konkreetse vastutuse. See aitab vältida olukorda, kus ükski järelevalveasutus ei võta initsiatiivi rikkumise menetlemisel. Tutvustatav printsiip tagab õiguse ühetaolisema kohaldumise ning seega parema õiguskindluse ja üksikisikute kaitse. Praktikas ei pruugi printsiip efektiivselt rakenduda, kuna järelevalveasutustel on väga erinev ressurss ning pädevus, samuti on kõrvaldamata järelevalveasutuste otsuste tunnustamise ja täitmise probleem teises liikmesriigis. Töö autor on seisukohal, et Euroopa Liidu tasandil regulatsiooniga ei olegi võimalik kõiki rakendamise probleeme kõrvaldada. Kaasnevad probleemid on ületatavad ning pakutav lahendus seega positiivne uuendus.

3.4.3 Järjepidevusprintsiip

Direktiivis puudub efektiivne mehhanism, kuidas rahvusvahelist koostööd reguleerida ja organiseerida. OSS printsiip lahendab üksnes küsimuse sellest, kes vastutab koostöö organiseerimise eest, kuid ei paku lahendusi rahvusvahelise menetluse läbiviimiseks. Üldmääruse artiklites 57 - 63 tutvustatava järjepidevusmehhanismi idee on koos OSS printsiibiga tagada üldmääruse ühetaoline ja järjepidev rakendamine liikmesriikides.³¹⁰

Esialgses versioonis nägi üldmäärus ette komisjoni ulatusliku pädevuse järjepidevusmehhanismi rakendamisel. Varasemas sõnastuses nägid artiklid 58 (2), (3) ja (4), et rahvusvahelise mõõtmega küsimuse korral või olukorras, kus mõne liikmesriigi järelevalveasutus seda nõuab, peab Euroopa Andmekaitseinspektsiooni ühe kuu jooksul andma arvamuse. Juhul kui komisjon leiab, et järjepidevus on ohus, annab komisjon omakorda arvamuse. Kui järelevalveasutus seda eirab, on komisjoni pädevuses peatada meetme rakendamine kuni 12 kuuks ning tegutseda erinevate järelevalve asutuste lepitamisel. Viimaks on komisjonile ette nähtud õigus mitte ainult teatud juhtudel tühistada liikmesriikide järelevalveasutuste otsuseid, vaid võtta vastu ka rakendussätteid, mis omavad kohest mõju.

Komisjoni ulatuslikud õigused ning komisjonile jäetud viimane sõna tekitas pahameelt.³¹¹ Euroopa Andmekaitseinspektor leidis, et selline lahendus kahjustab oluliselt

³⁰⁹ Council of Europe. Note from Presidency, p 5-6.

³¹⁰ Commission staff working paper. Impact assessment, p 98.

³¹¹ Prantsusmaa, Saksamaa, Itaalia, Luxembourg, Norra, Poola, Rootsi ja Suurbritannia väljendasid esialgses üldmääruse eelnõus kõik oma vastumeelsust just selle aspekti osas. Vt: P. Schwartz, p 2000.

järelevalveasutuste sõltumatuse põhimõtet, kuna muudab järelevalveasutused otseselt komisjonist sõltuvaks,³¹² tööühma arvates on komisjonile antud põhjendamatult ulatuslik pädevus ilma konkreetse piiritluseta ning oluline on suurendada loodava Euroopa Andmekaitsekoostöö rolli, mitte tugevdada komisjoni pädevust.³¹³ Kuigi komisjon püüdis veel 2013 aasta alguses õigustada enda rolli järjepidevusprintsipi supranatsionaalse institutsioonina, mis lahendaks vaidlusi üksnes äärmistel juhtudel,³¹⁴ on Euroopa Parlamendi heakskiidu pälvinud versioonist komisjoni rolli ulatuslikult kärbitud. Euroopa Komisjoni pädevust on võrreldes esialgse versiooniga kärbitud ligi 40% ulatuses.

Vastavalt üldmääruse artiklile 57 teevad järelevalveasutused üksteise ja komisjoniga koostööd järelevalvemehhanismi abil nii üldiste küsimuste kui ka üksikjuhtumite korral. Üldmääruse viimases versioonis eristatakse “üldisi küsimusi” ja “üksikjuhtumeid”, mille lahendamisele on ette nähtud erinev mehhanism.

“Üldised küsimused” hõlmavad endas laiaulatusliku üldmõjuga otsuste vastu võtmist nagu näiteks kolmandatesse riikidesse edastamisel standardklauslite kehtestamist, volitatud või vastutava töötaja ja järelevalveasutuse poolt volitatud andmesaaja vaheliste lepingutingimuste kehtestamist ning siduvate ettevõtluseeskirjade kehtestamist. Enne selliste meetmete vastuvõtmist näeb järjepidevusmehhanism ette liikmesriigi järelevalveasutuse kohustuse edastada kavandatava meetme projekt EAN-ile ning komisjonile. Juhul kui liikmesriik seda ise teinud ei ole, on nii EAN-il kui teiste riikide järelevalveasutustel kui ka komisjonil õigus nõuda, et “üldistes küsimustes” vastu võetud meede võetaks vastu kooskõlas järelevalvemehhanismiga. Üldistes küsimustes võtab EAN vastu lihthääle enamusega otsuse. Teatud juhtudel on EAN-il õigus otsustada, kas üleüldse otsus vastu võetakse.

Üksikküsimustes näeb OSS mehhanismi rakendamise esimene samm ette, et enne õiguslike tagajärgedega meetme rakendamist jagab juhtiv järelevalveasutus teiste puudutatud järelevalveasutustega informatsiooni ning edastab neile kavandatava meetme projekti. Kolme nädala jooksul on puudutatud järelevalveasutustel õigus esitada kavandatavale meetmele vastuväiteid. Juhul kui juhtiv järelevalveasutus ei esita kavandatava meetme projekti teistele puudutatud järelevalveasutustele, puudutatud järelevalveasutustel on kavandatava meetme osas vastuväiteid või juhtiv järelevalveasutus ei vasta üldmääruse artiklites 55 ja 56 sätestatud

³¹² European Data Protection Supervisor, p 41.

³¹³ Article 29 Data protection Working Party, Opinion 01/2012, p 20.

³¹⁴ European Commission. Data protection regulation: consistency mechanism explained. 06.02.2013. Available: http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm, 01.05.2014.

koostöö ja vastastikkuse abistamise reeglitele, arutab küsimust EAN. EAN kaalub küsimust, arvestades kavandatava meetme mõju ulatust andsubjektide fundamentaalsete õigustele ja vabadustele ning otsustab lihthäälteenamusega, kas annab küsimuse kohta arvamuse või mitte. Otsus selle kohta, kas EAN väljastab otsuse, tuleb teha kahe nädala jooksul. Juhul, kui EAN otsustab küsimuse kohta otsuse väljastada, teeb ta seda kuue nädala jooksul. Sellisel juhul on juhtiv järelevalveasutus kohustatud igati arvestama EAN-i arvamusega ning on kohustatud kahe nädala jooksul teavitama EAN-i juhti sellest, kas kavatseb kavandatud meetmeid muuta ja kohandada. Juhul, kui juhtiv järelevalveasutus otsustab mitte EAN-i otsust järgida, peab ta oma seisukohta põhjendama. Kui EAN ei ole jätkuvalt nõus juhtiva järelevalveasutuse kavandatava meetmega, võib EAN ühe kuu jooksul võtta 2/3 häälteenamusega vastu meetme, mis on järelevalveasutusele siduv.

Järelevalvemehhanism uues sõnastuses on tasakaalustatum ning pakub reaalseid lahendusi olukordades, kus ühe andmetöötleja rikkumistega peavad tegelema mitme liikmesriigi järelevalveasutused.³¹⁵ Töörühm on teinud ettepaneku tutvustada omakorda veel EAN-i poolt järelevalvemehhanismi raames vastu võetud otsuste jõustamise mehhanismi, et tagada EAN-i otsuste täitmine olukorras, kus EAN-i poolt väljastatud otsust ei järgi mitme liikmesriigi järelevalveasutused.³¹⁶ Töö autor on seisukohal, et üldmääruse tasemel puudub sellise regulatsiooni vajadus. EAN-i roll on üldmääruses sätestatud meetmete abil piisavalt tugev, täiendavate õiguste andmine viiks järjekordsete viivitusteni kokkuleppele jõudmisel.

Töö autor on seisukohal, et üldmääruses on rahvusvahelise koostöö regulatsioon laias laastus õnnestunud. Kuigi tuleb nõustuda, et rahvusvahelise koostöö efektiivne toimimine reaalsuses oleneb ka järelevalveasutuste ressurssidest,³¹⁷ luuakse üldmääruse regulatsiooniga eeldused koostöö toimimiseks.

3.5 Vahekokkuvõte

Järelevalve regulatsiooni reformimisel lähtuti kolmest peamisest eesmärgist: esiteks sooviti suurendada järelevalveasutuste majanduslikku ja institutsionaalset sõltumatust, teiseks ühtlustada järelevalveasutuste pädevusi ning kolmandaks luua efektiivne mehhanism rahvusvaheliseks koostööks.

³¹⁵ Samal arvamusel: W. K. Hon, E. Kosta, C. Millard, D. Stefanatou, p 23.

³¹⁶ Article 29 Data protection Working Party, Opinion 01/2012, p 20.

³¹⁷ C. Cuijpers, N. Purtova, E. Kosta, p 16.

Järelevalveasutuste suurem sõltuvus loodetakse saavutada kehtestades üldmääruises selgesõnaliselt liikmesriigi kohustus tagada järelevalveasutusele toimimiseks piisav ressurss. Töö autor on seisukohal, et ainuüksi sellise kohustuse sätestamine ei taga järelevalveasutuste paremat rahastamist. Üldmääruises sätestatud nõuet tuleks täpsustada, sätestades selgemad kriteeriumid selle kohta, mida peetakse „piisavaks ressursiks“. Kuigi AKI-l ei ole teiste siseriiklike järelevalveasutustega olulist ressursipuudust, on AKI majanduslik sõltumatus siiski kaheldav. Järelevalveasutused on ka oma eelarve mõttes valitsusasutustest sõltuvad, kuna tihti määrab ja kinnitab need justiitsminister. Üldmäärus sätestab järelevalveasutusele eraldi aastaeelarve koostamise kohustuse. Üldmäärusega kehtestatakse senisest kõrgem standard järelevalveasutuste majanduslikuks sõltumatusseks. Kuigi see ei lahenda osade liikmesriikide ressursiprobleeme, on tegemist pigem positiivse muutusega, mis tagab ka AKI suurema majandusliku sõltumatuse justiitsministrist.

Euroopa Kohtu otsus C-518/07 rõhutas vajadus tagada järelevalveasutuste sõltumatus täidesaatva võimu järelevalvest. Liikmesriikide järelevalveasutuste erinev paik siseriiklikus struktuuris tingib olukorra, kus sõltumatus on liikmesriigiti tagatud väga erineval tasandil. Üldmäärus ei too kaasa olulist kvalitatiivset muutust, vaid sätestab, et järelevalve asutused tegutsevad täiesti sõltumatult ning ei küsi ega võta oma kohustuste täitmiselt juhiseid mitte kelleltki.

Liikmesriigiti on järelevalveasutustel väga erinev pädevus, erinevused ilmnevad nii uurimis-, sekkumis-, kui ka esindusvolitustes. IKS-is sätestatuga võrreldes üldmäärus andmekaitse inspeksiooni volituste osas suuri muutusi kaasa ei too, küll aga aitab volituste selgesõnaline kehtestamine ühtlustada järelevalveasutuste rolle liikmesriigiti ning tagada seega kõigile EL elanikele võrdsem kaitse isikuandmete töötlemisel.

Üldmäärusega ette nähtud halduskaristuste regulatsioon ei ole praeguses sõnastuses õnnestunud. Jääb ebaselgeks, kas halduskaristuste eesmärgiks on üksikisikute karistamine või on tegemist pigem sunnimeetmega või kuidas suhestuvad halduskaristused teiste sekkumisvolitustega. Üldmääruises sätestatud halduskaristuste regulatsioon ka ebaproportsionaalselt karm – järelevalveasutus võib määrata hoiatuse üksnes esmakordsele rikkujale, korduvatele rikkujatele on ette nähtud audit või trahv kuni 100 000 000 eurot. Sätestatud meetmed ei arvesta liikmesriikide majanduse eripäradega ning pole praktikas rakendatavad. Kuna trahvisummade ülemmäär on väga kõrge, tähendaks see sisuliselt ikkagi seda, et liikmesriikide järelevalveasutused rakendaksid neile tavapäraseid trahvimäärasid. Halduskaristuse rakendatavuse probleemide tõttu ei saavutata tegelikkuses järelevalveasutuste

senisest efektiivsemaid jõustamismeetmeid ning isegi kui need praktikas oleksid rakendatavad, ei tagaks need niivõrd kõrge ülemmäära tõttu sellele vaatamata ühetaolist kohaldamist.

Rahvusvahelise koostöö regulatsiooni osas on üldmääruses veel mitmeid ebaselgusi, suuresti tulenevalt sellest, et puuduvad selged juhised Euroopa Liidu tasandil, kuidas toimida, kui isikuandmete töötlemise nõudeid on rikkunud andmetöötaja, kes tegutseb mitmes liikmesriigis. Vastutuse täpsustamiseks tutvustatakse üldmääruses juhtiva järelevalveasutuse kontseptsiooni. Kuigi printsiibi rakendamisel praktikas esinevad ilmselt mõned probleemid (näiteks tulenevalt järelevalveasutuste piiratud ressursist), on vastutuse ja koostöö printsiipide sätestamine üldmääruses positiivne muutus. Järelevalvemehhanismi uues sõnastuses on oluliselt vähendatud komisjoni pädevust ning tugevdatud varasema sõnastusega võrreldes uue loodava institutsiooni Euroopa Andmekaitsekojale pädevust.

KOKKUVÕTE

Töö põhieesmärk oli teha kindlaks, kas kavandatava isikuandmete kaitse üldmääruses sätestatud meetmetega saavutatakse Euroopa Komisjoni poolt seatud isikuandmete kaitse regulatsiooni reformi peamised eesmärgid. Komisjoni poolt seatud eesmärgid seonduvad eelkõige sooviga tagada üksikisikute õiguste parem kaitse, siseturu efektiivsem toimimine ning isikuandmete regulatsiooni efektiivne rakendamine praktikas.

Töös leitakse, et olemasolevad õigusaktid, mis reguleerivad isikuandmete kaitset, ei vasta tänapäevase õiguskorra vajadustele Euroopa Liidus. Rahvusvahelised instrumendid nagu Euroopa Nõukogu 1981 aasta isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon on üldsõnalised ning iganenud. OECD juhend eraelu kaitsest ja piiriülesest isikuandmete kaitsest on üksnes soovitusliku iseloomuga, mistõttu puudub igasugune jõustamismehhanism juhendist tulenevate põhimõtete järgimise kindlustamiseks. Euroopas isikuandmete kaitset reguleeriv direktiiv 95/46/EÜ on iganenud ega ole vastavuses tänapäeva tehnoloogiliste uuendustega, samuti on direktiiv 95/46/EÜ liikmesriikidele siduv üksnes saavutatava eesmärgi osas. Eestis kehtiv isikuandmete kaitse seadus on üle võetud samas üldisuse astmes, kui on direktiiv 95/46/EÜ, mistõttu on isikuandmete kaitse regulatsioon Eestis kohati lünklik ja üldsõnaline.

Liikmesriikide suur otsusediskretsioon isikuandmete kaitse reguleerimisel on viinud märkimisväärsete erinevusteni liikmesriikide siseriiklikes õigustes. Selliselt on tekkinud olukord, kus isikuandmete kaitse tase on liikmesriigiti erinev ning isikuandmete töötlemisega tegelevad ettevõtjad on sunnitud rahvusvahelisel turul tegutsedes vastama väga mitmetele erinevate liikmesriikide siseriiklikust õigusest tulenevatele nõuetele. Õiguse killustumusest tulenevad barjäärid ja kulud tingivad ettevõtjate, eelkõige väikese ja keskmise suurusega ettevõtjate, rahvusvahelisel turul konkureerimisest loobumise. Töös leitakse vastusena esimesele uurimisküsimusele, et olemasolev seadusandlus Euroopa Liidu ja Eesti tasandil ei taga piisavalt kõrget üksikisikute õiguste kaitse taset ega vasta siseturu vajadustele tagada võimalikult efektiivne andmete vaba liikumine siseturul.

Euroopa Komisjon algatas 2010.a isikuandmete kaitse regulatsiooni reformi. Reformipaketi keskmes on isikuandmete kaitse üldmäärus, mis on mõeldud asendama direktiivi 95/46/EÜ. Kavandatava isikuandmete kaitse üldmäärusega soovib Euroopa Komisjon tugevdada ühest küljest andmesubjekti õigusi ning teisalt luua andmetöötlejatele sobiv keskkond andmete töötlemiseks Euroopa Liidu siseturul.

Euroopa Komisjon soovib üksikisikute õiguste kaitset tugevdada, suurendades läbipaistvust isikuandmete töötlemisel, kuna isikute usaldus andmetöötajate vastu on madal ning isikud tunnevad, et neil puudub piisav info selle kohta, milleks täpselt nende andmeid töödeldakse. Töös leitakse, et selle probleemi lahendamiseks ette nähtud läbipaistvusprintsiipt on õnnestunud lahendus. Üldmäärus sätestab direktiiviga 95/46/EÜ võrreldes kohustuse selgitada andmesubjektile tema andmete töötlemisega seonduvat olulist informatsiooni andmesubjektile arusaadavalt. Üldmääruse otsekohalduva iseloomu tõttu kohalduks printsiipt ka Eestis. Läbipaistvusprintsiipt paneb ettevõtetele kohustuse muuta oma andmetöötlus- ja privaatsuspoliitikat puudutav informatsioon andmesubjektile arusaadavamaks. Töös jõutakse järeldusele, et läbipaistvusprintsiipt võimaldab anda andmesubjektile parema ülevaate tema kohta kogutud andmete kogumise eesmärgist ja hulgast, mis on oluline eeldus, võimaldamaks andmesubjektile oma õigusi kaitsta.

Teiseks komisjoni poolt kavandatavaks meetmeks läbipaistvuse suurendamisel on vastutava ja volitatud töötaja vaheliste kohustuste täpsustamine. Töös leitakse, et terve uue peatüki lisamine üldmäärusesse on direktiiviga võrreldes oluline kvalitatiivne edasimineku. Tänapäevaste tehnoloogiate, eelkõige pilvandmetöötluse, tõttu ei ole andmesubjektidele (ega ka andmetöötajatele) sageli mõistetav, kes on andmetöötlusprotsessis vastutav töötaja ning millised on andmetöötlusprotsessis osalejate vastutus ja ülesanded. Üldmäärusega täpsustatakse vastutava töötaja vastutust ning määratakse kindlaks kaasvastutavate töötajate ülesanded ja võimalik kaasvastutus. Vastutava ja volitatud töötaja kohustuste täpsustamisega saavutatakse üksikisikute õiguste parem kaitse, kuna selliselt luuakse andmesubjektile varasemast parem ülevaade andmetöötajate ringist ning nende omavahelise vastutuse jagunemisest. Eesti IKS sätestab juba praegu direktiiviga võrreldes selgemalt vastutava ja volitatud töötaja vaheliste ülesannete ja vastutuse jagunemise. Kuigi Eestile vastutava ja volitatud töötaja vastutuse ja kohustuste sätestamine olulisi muutusi kaasa ei too, aitab regulatsioon siiski saavutada paremat läbipaistvust isikuandmete töötlemisel nii andmetöötlusprotsessis osalejate kui andmesubjekti jaoks, mis omakorda võimaldab tagada andmesubjekti õiguste parema kaitse.

Euroopa Komisjoni ettepanekul on üldmääruses tutvustatud õigust andmete kustutamisele. Töös jõutakse järeldusele, et tutvustatav meede on ebaõnnestunud kahel põhjusel. Esiteks ei vasta kavandatav õigus arusaamale sellest, kui kiiresti ja millises ulatuses toimub tänapäeval andmetöötlus internetis. Kõigi kolmandate isikute väljaselgitamine, kes on töödeldanud samu andmeid, on praktikas võimatu ning vastutavale töötajale ebaproportsionaalselt suur

kohustus. Töös tehakse ettepanek sätestada üldmäärusega andmesubjekti enda õigus pöörduda kolmandate osapoolte poole. Teiseks on meede ebaõnnestunud, kuna jätab erandite tegemiseks liikmesriikidele liialt suure kaalutusruumi, seda eelkõige sõnavabadusega seonduvalt. Töö autori arvates on andmete kustutamise õiguse efektiivseks toimimiseks vajalik täpsustada erandite tegemise aluseid. Praeguses sõnastuses saavutatakse andmete kustutamise õiguse tutvustamisega pigem andmesubjektide võltsturvatus kui üksikisikute parem kaitse. Ebaselged volitusnormid sõnavabaduse erandi kehtestamiseks võivad viia liikmesriigiti erineva ja kohati ebaproportsionaalse ajakirjandus- ja sõnavabaduse piiramiseni.

Lisaks andmete kustutamise õigusele nähakse üldmääruses ette ka isikute õigus andmete ülekantavusele. Töös leitakse, et andmete ülekantavuse õigus on praktikas rakendatav ega too endaga kaasa ebaproportsionaalseid kulusi ettevõtjatele. Andmete ülekantavuse õiguse tutvustamine aitab parandada andmesubjekti kontrolli enda andmete üle, kuna võimaldab tal kergemini vahetada teenusepakkujaid ning valida nende teenuste vahel tulenevalt teenuse kvaliteedist, mitte sellest, milline teenusepakkuja omab rohkem andmesubjekti andmeid.

Töös järeldatakse, et neljast üksikisikute õiguste parandamiseks pakutavast meetmest kolm on efektiivsed ning praktikas rakendatavad, kuid õigus andmete kustutamisele vajab üldmääruses täpsustamist.

Euroopa Liidu siseturu paremaks toimimiseks rõhutas Euroopa Komisjon vajadust tagada ettevõtjatele suurem õiguskindlus ning vähendada õiguse killustumisest tulenevat halduskoormust.

Õiguskindluse tagamiseks on Euroopa Komisjon otsustanud kehtestada isikuandmete kaitse regulatsiooni otsekohalduva määrusega. Tulenevalt ETL artiklist 288 on määrus tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides, mistõttu muudaks üldmäärus kehtetuks ka Eestis kehtiva IKS-i. Töös järeldatakse, et isikuandmete kaitse reguleerimine määrusega on põhjendatud ega riku subsidiaarsusprintsipi, kuid praeguses sõnastuses ei saavutata üldmäärusega soovitud õiguskindlust, kuna üldmäärus ei ole piisavalt sidus ega kõikehõlmav. Töös tehakse ettepanek jätta liikmesriikidele vastutava töötleja vastutuse osas suurem otsustusruum, täpsustades samas üldmääruse alusel kehtestatud siseriiklike eriregulatsioonide kriteeriume ning territoriaalset kohaldumisaala rahvusvahelise vaidluse korral.

Euroopa Komisjon ei saavuta üldmääruse kehtima hakkamisel tõenäoliselt soovitud halduskulude vähendamist. Töös leitakse, et komisjoni arvutused üldmäärusega kaasnevate halduskulude osas jätaavad mitmed olulised kulutused arvestamata, näiteks seonduvalt

andmekaitseametnike määramise ja riskianalüüside läbiviimise kohustusega. Väikestele ja keskmise suurusega ettevõtetele ette nähtavad erandid ei suurenda ettevõtete konkurentsivõimet rahvusvahelisel tasandil. Isegi kui üldmäärusega ette nähtud erandid, mille kohaselt alla 250 töötajaga ettevõtted ei pea mitmeid üldmääruses sätestatud nõudeid täitma (näiteks määrama andmekaitseametnikku), aitaks kaasa ettevõtete konkurentsivõimele, kahjustaks see üksikisikute õigusi ning kohalduks ligi 60%-le ettevõtetele. Töös leitakse, et teatav kulude kasv on paratamatu, kuid väikeste ja keskmise suurusega ettevõtete olukorra parandamiseks peaks erandite kriteeriumid sõltuma sellest, millises hulgas ning millistel eesmärkidel ettevõtted andmeid töötlevad, mitte töötajate arvust.

Vastuseks teisele uurimisküsimusele leitakse, et üldmääruses ei ole leitud sobivat tasakaalu andmesubjektide ja andmetöötajate huvide vahel, mistõttu ei saa kavandatavaid meetmeid pidada efektiivseks. Euroopa Komisjoni eesmärkidest tagada üksikisikute parem kaitse ja siseturu efektiivsem toimimine, saavutatakse vaid üks. Kuigi üldmäärus näeb ette mitmeid efektiivseid meetmeid üksikisikute õiguste suurendamiseks, on kavandatava üldmääruse negatiivne mõju ettevõtetele ebaoproportsionaalselt suur. Euroopa Liidu aluslepingutest tulenevalt on Euroopa Liidu üheks aluspõhimõtteks kindlustada lisaks võrdsetele õigustele Liidu raames ka siseturu efektiivne toimimine, mida praeguses sõnastuses üldmäärusega saavutata.

Üksikisikute õiguste parema kaitse ja siseturu toimimise eelduseks on andmekaitsereeglite kohaldamine ja jõustamine praktikas. Praegusel juhul on järelevalve isikuandmete kaitse üle liikmesriigiti erineva tasemega. Üldmääruses soovitakse järelevalveasutuste rolli tugevdada ja ühtlustada, tagades neile sõltumatus ja ühesugused volitused kõigis liikmesriikides ning tutvustades ühtset mehhanismi rahvusvahelise koostöö tegemisel.

Töös järeldatakse, et mitmetel liikmesriikidel, sealhulgas Eestil, on probleeme järelevalveasutuste sõltumatuse tagamisega. Andmekaitseinspeksioon on justiitsministeeriumi valitsemisalas ning tema eelarve kinnitab justiitsminister. Selline olukord on vastuolus Euroopa Kohtu lahendiga C-518/07, mille kohaselt peab olema tagatud järelevalveasutuste täielik sõltumatus. Töös leitakse, et kuigi üldmäärus ei sätesta spetsiifilisi nõudeid järelevalveasutuste sõltumatuse tagamiseks, on üldmäärusega seatav standard direktiiviga võrreldes kõrgem ning järelevalveasutuste sõltumatuse paremaks saavutamiseks piisav.

Eesti IKS näeb AKI-le ette ulatuslikud uurimis-, sekkumis- ja esindamisvolitused. Töös leitakse, et üldmääruse regulatsioon ei too Eestile kaasa olulisi muutusi, kuid aitab ühtlustada järelevalveasutuste pädevust liikmesriigiti.

Töö käigus jõutakse järeldusele, et üldmäärusega ette nähtud halduskaristuste regulatsioon ei ole praeguses sõnastuses õnnestunud. Praeguses sõnastuses ilmneb halduskaristuste regulatsioonis mitmeid puudusi: jääb ebaselgeks, kas tegemist on sunni- või karistusmeetmega; ei ole selge, kuidas suhestuvad üldmäärusega ette nähtud sekkumisvolitused halduskaristustega; halduskaristuste määramise alused ning trahvide ulatus on liiga karmid. Töös jõutakse järeldusele, et praeguses sõnastuses ei tugevdata halduskaristuste määramise õigusega järelevalveasutuste rolli, kuna halduskaristused pole praktikas rakendatavad. Halduskaristuste regulatsiooni olemust tuleks üldmääruses täpsustada ning jätta liikmesriikide järelevalveasutustele karistuste liikide ja määrade osas suurem diskretsioon.

Üldmäärusega tutvustatakse järelevalveasutuste rahvusvahelise koostöö parandamiseks *one-stop shop* printsiipi, luuakse uus supranatsionaalne organisatsioon Euroopa Andmekaitsekoostöö ja viiakse sisse järjepidevusmehhanism. Vastusena kolmandale uurimisküsimusele leitakse, et vaatamata mõningatele ebaselgustele, on vastutuse ja koostöö täpsustamine rahvusvahelisel tasandil positiivne muutus ning pakub varasemaga võrreldes parema ja selgema mehhanismi rahvusvaheliste küsimuste lahendamiseks. Arvestades liikmesriikide esindajate erimeelsusi printsiibi detailide osas, võib arvata, et üldmäärust rahvusvahelist koostööd puudutavas osas veel täiendatakse, kuid töö autori arvates on praegu sätestatud üldpõhimõtted efektiivsed ja praktikas rakendatavad.

Töös jõutakse järeldusele, et üldmäärusega ei saavutata praeguses sõnastuses kõiki Euroopa Komisjoni poolt sõnastatud eesmärke. Kuigi tutvustatavate meetmetega tagatakse üksikutele suuremad õigused, ei tagata siseturu paremat toimimist. Üldmäärus on kohati liiga detailne, jättes samal ajal mitmed valdkonnad siseriikliku õiguse reguleerimisalasse. Järelevalveasutusi puudutav regulatsioon ühtlustab küll asutuste pädevuse, kuid halduskaristuste ja rahvusvahelise koostöö osas vajab üldmäärus täpsustamist. Euroopa Parlamendi poolt esimesel lugemisel vastu võetud üldmäärus ei ole praktikas rakendamiseks valmis.

Harmonizing personal data protection regulation in the General Data Protection Regulation draft and its impacts on Estonia. Summary

With the technological developments and with the European Union (hereinafter EU) countries reaching the information society, information has become a relevant asset. It is not only a currency, but a cultural value and a benefit.

Specific information is called data. Personal data is all data by which a person is identified or identifiable. Due to the growing number of internet users and the development of technology and means for data processing, data protection has become the main goal of the European Union, instead of being a local problem of national legislations.

Since 2010 there have been consultations and discussions on the need to reform data protection regulation. The legal instruments regulating data protection on international level such as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data are general in terms and outdated. Many of the international legal instruments, such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data have a non-binding nature and thus lack of enforcement mechanisms to ensure the principles in the guidelines are followed. The directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter the directive), which is the main instrument regulating personal data protection in the EU, has stood up to technological challenges for almost 20 years, but by this day has become outdated as well. The directive is binding to the member states only as far as the goals of the directive are concerned and does not regulate data protection on a very specific level. The Estonian Data Protection Act (hereinafter EDPA) implemented the directive on the same principle level and is thus rather general in terms and lacks solutions to certain important problems.

With the initiative of the Commission of the European Union a draft of a regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) was composed along with a draft directive on the processing of data in criminal proceedings.

The General Data Protection Regulation (hereinafter GDPR) was drafted with a purpose to harmonize the existing rules of personal data protection across the EU. Wide range of

discretion offered by the directive has led to substantial differences within the national legislations of member states. It has created a situation where the level of protection for personal data varies across the union and international enterprises that process data are forced to comply with many different rules set by national legislations. The legal fragmentation creates substantial costs and market barriers for enterprises, especially micro-, small and medium sized enterprises, who, as a result, often decide to give up competing on the international market.

The research problem of this master thesis is the effectiveness of the means proposed in the GDPR. The purpose of this paper is to conclude whether the means introduced by the GDPR draft in this wording help to achieve the main goals of the reform set by the commission, i.e. higher level of protection of individuals while processing personal data, free movement of personal data in the internal market and effective enforcement of data protection legislation by the supervisory authorities. The author of the thesis does not aim to analyze all the problems and effects GDPR might bring related to EU law and Estonian law or to compare the whole national legislation of personal data protection to the GDPR.

The first chapter of the thesis is based on the dogmatic method to conclude what are the main weaknesses of the current legislation on international, EU and national level. The second and third chapters of the study are based on a comparative- systematic method where the author has compared the means set out in the GDPR to the directive and EDPA and concluded whether the means proposed by the GDPR solve the existing problems and help to reach the goals of the reform.

The thesis starts off with mapping all the most important legal instruments that state the right to data protection directly or indirectly and the most important legal instruments that are meant to ensure and enforce that right. It is concluded that the current legislation on EU or national level does not provide for a high level of protection of the rights of the individuals concerning personal data nor does it comply with the needs of the internal market to ensure free movement of personal data within the internal market. Current legislation is either too general, does not contain effective enforcement mechanisms or does not comply with the needs of EU internal market because of legal fragmentation.

The study continues to deal with the main goals of data protection reform of the European Commission. Data protection is always about balancing the interests of individuals with the

interests of enterprises processing data. GDPR hopes to achieve a higher level of protection of individuals while guaranteeing better conditions for the enterprises as well.

The study then concerns the first goal of the data protection reform - to strengthen the protection of individuals by increasing transparency when processing personal data. Surveys have shown that trust towards data processors is low and individuals feel that they do not have sufficient information on what exactly their data is processed for. It is found that the transparency principle introduced is an effective and positive change. Compared to the directive, the GDPR states an obligation to introduce privacy policies and notifications to the data subject in a clear and understandable manner. Due to the direct effect of the regulation, this principle will be directly applicable to the Estonian law as well. It is concluded that the transparency principle sets out reasonable standards for the data processor to ensure better overview of whether the data collected is adequate, relevant and limited to the minimum necessary. This overview is a necessary precondition for an individual to protect his or her rights.

The second measure used in the GDPR to achieve transparency is the explicit regulation of the duties and responsibilities of the controller and the processor. Due to many participants in the process of data processing it is often not clear, who is the controller and who is the processor, the responsibilities of the parties are often unclear as well. By introducing a whole new chapter concerning the controller and processor a new level of quality is added to the existing legislation of the directive, yet it does not bring substantial changes compared to the EDPA. A higher level of protection of individuals is achieved by this, as the data subject will now have a much better overview of the parties to the processing of personal data and of their responsibilities.

GDPR introduces the right to erasure hoping to improve the control of the data subject over ones data. Right to erasure means that the data subject has under some conditions the right to demand the controller to erase his or her data. In case the data is published without legal basis, the controller is obliged to do all in its powers to inform all the processors or third parties of the data subject request. It is concluded that this measure, right to erasure, is unsuccessful for two reasons. Firstly, the right to erasure in the current wording of the GDPR does not comply with the reality on how the internet works. The amount and speed of data processed and reused makes it virtually impossible for the processor to comprehend who are all the third parties that should be notified and is thus an unproportional obligation to the data controller. Secondly, the GDPR leaves a wide discretion to the member states to make

exceptions form the right to erasure, including in the case of colliding rights such as freedom of speech. The author is of the opinion that the grounds for exemptions need to be specified, as the current wording leaves too much room for discretion, which leads to fragmentation and possible disputes on restricting the freedom of speech unproportionally. The goal of the reform to achieve better control over ones data is not achieved.

The commission wishes to strengthen the control over ones data by introducing the right to data portability. Data portability gives the data subject the right to take ones data stored by one service provider and take it to another on- e.g. data subjects could move their e-mails, contacts and other information from *Google* to *Hotmail*. It is concluded that this right, unlike the right to erasure, helps to strengthen control over ones data more effectively as it is enforceable in reality and does not come with unproportional costs for the data processors. Data portability helps the data subject to choose between service providers based on the quality of theirs services, effectiveness of their privacy policies etc and not depending on which service provider owns more data about the data subject.

It is concluded that three out of four measures introduced by the GDPR to ensure a higher level of protection of the individuals are effective and enforceable. The transparency principle, regulation of processor and controller and data portability are all welcomed changes both in EU and Estonian law. The right to erasure will not be enforceable and needs further specifications.

Next, the thesis touches upon the European Commissions goal to improve legal certainty within the EU from the aspect of enterprises. Legal certainty is to be achieved by introducing the principle “one continent, one law” which means that the European Commission has chosen a regulation as a legal instrument to regulate data protection across the EU. The proposed GDPR would repeal EDPA in its current wording, as the regulation is directly applicable. It is concluded that the choice of the legal instrument is justified, but in its current wording legal certainty is not achieved, as the GDPR lacks comprehensiveness in many aspects. It is proposed to leave more room for discretion concerning the demands for the controller, as different member states have different economic environments and the GDPR is too rigid in its current wording. The territorial scope of exceptions provided by national laws in relation to the GDPR need to be specified.

The study then deals with the purpose of the reform to reduce administrative costs. The European Commission has proposed that the GDPR would save enterprises 2, 3 billion Euros

a year. Reducing costs by introducing the new legislation as a regulation would help to save money and ensure a level playing field for micro, small and medium sized enterprises. The study indicates that these calculations are insufficient and selective. While calculating the costs, the commission had counted all the current costs but left out the costs coming from the proposed GDPR such as the obligation to appoint a data protection officer and an obligation to conduct impact assessments. Alternative studies show that even the enterprises processing data are not able to assess their costs under the directive, which makes it hard to believe that the calculations of the commission are accurate. Even if the costs of micro, small and medium sized enterprises would decrease (which they will not according to some reports), the decrease of costs would come on the account of the protection of individuals. The exceptions provided in the GDPR for enterprises such as not having to appoint a data protection officer when the enterprise has less than 250 employees, would mean that around 60% of employees would be left without a higher level of protection the data officer is meant to provide. It is proposed to set the criterias of exceptions based on the amount of data processed by the enterprise and not based on the number of its employees.

It is concluded that GDPR does not offer a good balance between the rights of the individual and the rights of enterprises processing data. The proposed measures have failed to ensure a high level of protection of individuals while not hampering the rights of the enterprises. Current wording of the GDPR proposes some good measures that help to provide a higher level of protection of individuals but the negative effect on enterprises is too big. The GDPR is not comprehensive enough to ensure legal certainty and reduce costs for the enterprises.

Next the thesis touches upon the subject of supervisory authorities that ensure the enforcement of data protection regulations. Strengthening enforcement of data protection rules is on one hand a measure to ensure that the two goals mentioned above, higher level of protection of individuals and effective functioning of the free market, are reached. On the other hand it can be considered as a separate goal of the data protection reform, as the role, duties and powers of data protection authorities (hereinafter DPA-s) differ greatly across EU.

Concerning DPA-s the thesis firstly touches upon the issue of independence. The recent ruling of the European Court of Justice C-518/07 stated that member states need to ensure full independence for the DPA-s of data processing, including economical and institutional independence. The current situation in the member states is not good – many DPA-s, including the Estonian Data Protection Inspectorate, do not meet the requirements for independence under the directive. GDPR, unlike the directive, sets standards, such as a need

to ensure the DPA has a separate budget from the ministry of justice or other bodies of the government. It is impossible for the GDPR to set specific standards to ensure economical and institutional independence, but the criteria set is ought to improve the situation.

Next, the thesis discusses the different powers of national DPA-s. The directive states that DPA-s must have investigative powers, powers of intervention and powers of representation in legal proceedings. It is found in the thesis that national DPA-s currently have very different powers, as the directive is very general in stating what the powers should be. The EDPA is much more specific compared to other legislations concerning the powers of DPA-s and thus introducing a specific list of powers by the GDPR helps to harmonize the powers of national DPA-s across the union but does not bring substantial changes compared to the current situation in Estonia.

The thesis continues with the problems of administrative sanctions. GDPR means to strengthen the role of national DPA-s by giving them the power to impose administrative sanctions up to 100 000 000 Euros. The current wording of GDPR leaves many questions unanswered. It is not clear, whether the administrative sanctions should be considered as an administrative penalty or as a punishment. The relation of administrative sanctions to the powers of intervention of DPA-s is not clear and the grounds for imposing administrative sanctions are too strict. The administrative sanctions in the GDPR do not take into consideration the differences of member states, as it would not be feasible to enforce administrative sanctions to companies residing e.g. in the Baltics of up to 100 000 000 Euros, as that would in most cases lead to insolvency. Thus administrative sanctions are not enforceable in reality and the category, grounds and scale of the administrative sanctions should leave more discretion to the member states.

Lastly the thesis deals with the question of international cooperation. Right now DPA-s lack of mechanisms for international cooperation in cases where an international investigation needs to be conducted. The GDPR introduces the principle of the lead authority, which means that one DPA shall be the lead DPA to conduct investigations in cases of international data breaches. The *one-stop shop* providing the lead authority is backed by the consistency mechanism that ensures specific rules to ensure effective and consistent enforcement of the GDPR across the union. Compared to the first draft of the GDPR, the role of the commission to give implementing acts has been reduced significantly and more power is given to the European Data Protection Board, to be created as the successor of the Article 29 Working Party. The European Data Protection Board is given the right to issue binding decisions is

some cases, thus strengthening the role of an international DPA. It is concluded, that better international cooperation is achieved with the GDPR.

The study concludes that not all of the goals set by the European Commission are reached with the current draft of GDPR. The GDPR will provide higher standard of rights to the individuals, but the measures meant to achieve this standard might not work in practice. Even if the means are enforceable, they will come with unproportional costs for the enterprises which process data. The choice of a legal instrument is welcomed by the author, but a regulation in this wording does not solve the problems of legal fragmentation and high administrative costs. The GDPR lacks of comprehensiveness, leaving a large area of discretion in some areas (e.g. exceptions to the right of erasure) while being too specific in others (e.g. the administrative sanctions). GDPR helps to harmonize the powers of DPA-s, but does not manage to set out effective regulation on administrative sanctions. The GDPR needs amendments in many areas, including the right to erasure, exceptions for micro, small and medium sized enterprises and administrative sanctions.

Sandra Sillaots

Tartu, 05.05.2014.a

KASUTATUD MATERJALID

Kasutatud kirjandus

1. Alexy, R. Põhiõigused Eesti Põhiseaduses. - Juridica 2001/eriväljaanne.
2. Baker, W. B., Matyjaszewski, A. The changing meaning of personal data. Available: https://www.pri.vacyassociation.org/resource_center/the_changing_meaning_of_personal_data, 23.04.2014.
3. Barberis, A. Letter to mr José Manuel Barroso. Impact assessment on data protection Directive / Regulation (COM 2012 10 & 11). Brussels: 13.02.2012. Available: <http://www.eurochambres.eu/Content/Default.asp?PageID=1&DocID=4212>, 29.04.2014.
4. Bygrave, L. A. Data protection law: approaching its rationale, logic and limits. Hague: Kluwer Law International 2002.
5. Bygrave, L. A. The place of privacy and data protection law. - University of New South Wales Law Journal 2001/6. Available: <http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html>, 12.04.2014.
6. Carey, P. Data protection: a practical guide to UK and EU law. Oxford: Oxford University Press 2004.
7. Christensen, L., Colciago, A., Etro, F., Rafert, G. The Impact of the Data Protection Regulation in the E.U. 2013. Available: <http://www.intertic.org/Policy%20Papers/CCER.pdf>, 01.05.2014.
8. Clarke, R. The OECD Data Protection Guidelines: A Template for Evaluating Information Privacy Law and Proposals for Information Privacy Law. Canberra: Australian National University 1989. Available: <http://www.rogerclarke.com/DV/PaperOECD.html>, 28.04.2014.
9. Craig, P., de Burca, G. EU law. Text, Cases and Materials. Fifth edition. Oxford: Oxford University Press 2011.
10. Cuijpers, C., Purtova, N., Kosta, E. Data Protection Reform and the Internet: the draft Data Protection Regulation. - Tilburg Law School Research Paper 2014, No. 3. Available: <http://ssrn.com/abstract=2373683>, 05.04.2014.
11. Danagher, L. An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data? - European Journal of Law and Technology 2012/3, No. 3.
12. De Filippi, P., McCarthy, S. Cloud Computing: Centralization and Data Sovereignty - European Journal for Law and Technology 2012/3, No. 2.

13. De Hert, P., Gutwirth, S. Data protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action. Reinventing Data Protection. Dordrecht: Springer Science 2009.
14. DeSimone, C. Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive. - German Law Journal 2010/11, No. 3.
15. Erelt, T. (koost). Eesti õigekeelsussõnaraamat ÕS 2006. Tallinn: Eesti Keele Sihtasutus 2006.
16. Evans, A. C. European Data Protection Law. - The American Journal of Comparative Law 1981/29, No. 4.
17. Greenleaf, G. The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. - International data privacy law 2012/2, No. 2.
18. Hirvoja, M. Õiguspoliitika arengutest ja justiitsministeeriumi rollist selles. 28.01.2011. Arvutivõrgus: <http://www.just.ee/53263>, 29.04.2014.
19. Hon, W. K., Kosta, E., Millard, C., Stefanatou, D. Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation. London: Queen Mary University of London, School of law 2014. Available: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2405971, 30.04.2014.
20. Hornung, G. A general Data Protection Regulation for Europe? Light and shade in the commissions draft of 25 January 2012. - Scripted 2012/9, No. 1.
21. Jóri, A. Data protection law - an introduction. The notion of data protection. Available: <http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.Dataprotection>, 27.04.2014.
22. Kuner, C., Burton, C., Pateraki, A. The Proposed EU Data Protection Regulation Two Years Later. - Privacy and security law report. 2014. Available: <http://www.wsgr.com/eudataregulation/pdf/kuner-010614.pdf>, 01.05.2014.
23. Korff, D. EC study on implementation of Data Protection Directive. Comparative summary of national laws. Cambridge: September 2002. Available: <http://www.garanteprivacy.it/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE>, 01.05.2014.
24. Käsper, K. Inimõiguste kaitse riiklik organisatsiooniline raamistik. Arvutivõrgus: <http://humanrights.ee/inimoiguste-aruanne-2/inimoigused-eestis-2012/inimoiguste-kaitse-riiklik-organisatsiooniline-raamistik/>, 01.05.2014.

25. Lodde, S. Informationsrechte des Bürgers gegen den Staat. Carl Heymanns Verlag KG 1996 (Viidatud: Tikk, E., Nõmper, A. Informatsioon ja õigus. Tallinn: Juura 2007).
26. Miller, A. The assault on privacy. Ann Arbor: University of Michigan Press, 1971 (viidatud: Warren, A., Dearlney, J., Oppenheim C. Sources of Literature on Data Protection and Human Rights. - Journal of Information Law and Technology 2001/2).
27. Männiko, M. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011.
28. Peep, V. Andmekaitse Inspektisoon Euroopa Komisjoni algatatud andmekaitsereformist. 07.06.2012. Arvutivõrgus: <http://tinyurl.com/p22wdl3>, 29.04.2014.
29. Praust, V. Infotehnoloogia haldusjuhtimises. Infoühiskond ja selle teetähised. - Majandus- ja kommunikatsiooniministeriumi aastaraamat, 1998. Arvutivõrgus: <http://www.riso.ee/aastaraamatud/et/pub/1998it/12.htm>, 01.03.2014.
30. Reding, V. The EU Data Protection Reform 2012: Safeguarding Privacy in a Connected World. Speech. 25.01.2012. Available: http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/data-protection-reform2012_en.pdf, 30.04.2014.
31. Robinson, N., Graux, H., Botterman, M., Valeri, L. Review of the European Data Protection Directive. Cambridge: RAND, 2009. Available: http://www.hideproject.org/downloads/references/review_of_eu_dp_directive.pdf, 29.04.2014.
32. Rohtmets, E. Isikuandmete kaitse küsimused Euroopa Kohtu eelotsustes. Kohtupraktika analüüs. Tartu: Riigikohus, õigusteabe osakond 2013. Arvutivõrgus: http://www.riigikohus.ee/vfs/1455/Andmesubjekti%20oigused_EK_analuus.pdf, 29.04.2014.
33. Rohtmets, E., Kanger, L. Eesti andmekaitse Euroopa Kohtu praktika peeglis. - Riigikogu toimetised 2013/28. Arvutivõrgus: <http://www.riigikogu.ee/rito/index.php?id=14437>, 29.04.2014.
34. Schwartz, P. M. The EU - U.S. privacy collision: a turn to institutions and procedures. Harvard Law Review 2013/1966.
35. Sootak, J. Karistusõiguse revisjon kuriteo-, vääртеo- ja haldusõiguse piirimail. - Juridica 2013/IV.
36. Tikk, E., Nõmper, A. Informatsioon ja õigus. Tallinn: Juura 2007.
37. Truuväli, E.J jt (toim). Eesti Vabariigi Põhiseadus. Komm. vlj. 2. vlj. Tallinn: Juura 2008.
38. Zanfir, G. The right to Data portability in the context of the EU data protection reform. - International Data Privacy Law 2012/2, No. 3.

39. Warren, A., Dearlnley, J., Oppenheim, C. Sources of Literature on Data Protection and Human Rights. - Journal of Information Law and Technology 2001/2.
40. Warren, S. D., Brandeis, L. D. The Right to Privacy. - Harvard Law Review 1890/4, No. 5.
41. Westin, A. F. Privacy and Freedom. New York: Atheneum, 1967 (viidatud: Warren, A., Dearlnley, J., Oppenheim C. Sources of Literature on Data Protection and Human Rights. - Journal of Information Law and Technology 2001/2).

Kasutatud õigusaktid

1. Andmekaitse Inspeksiooni põhimäärus ja koosseis. - RT I, 05.03.2013, 5.
2. Avaliku teabe seadus. - RT I, 19.12.2012, 5.
3. Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. - ELT L 124, 20.05.2003, p 36-41.
4. Eesti Vabariigi põhiseadus. - RT 1992, 26, 349 ...RT I, 27.04.2011, 2.
5. Euroopa Liidu lepingu konsolideeritud verisoon. - ELT C 326/1, 26.10.2012, lk 13-46.
6. Euroopa Liidu toimimise lepingu konsolideeritud versioon. - ELT C 326/1, 26.10.2012, lk 47-200.
7. Euroopa Liidu põhiõiguste harta. - ELT C 83, 30.03.2010, p 392-403.
8. Euroopa Nõukogu 27. novembri 2008 raamotsus 2008/977/JSK, kriminaalasjades tehtava politsei- ja õiguslase koostöö raames töödeldavate isikuandmete kaitse kohta. - ELT L 350, 30.12.2008, lk 60 - 71.
9. Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrus nr 2001/45/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta. - ELT L 195, 19.07.2001, lk 46 - 49.
10. Euroopa Parlamendi ja nõukogu 24.10.1995.a direktiiv üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. - ELT L 281, 23.11.1995, lk 31 - 50.
11. Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). - ELT L 201, 31.07.2002, lk 37 - 47.
12. Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, 15. märts 2006, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ.- ELT L 105, 13.04.2006 p 54-63.
13. Infoühiskonna teenuse seadus. - RT I, 06.01.2011, 12.

14. Inimõiguste ja põhivabaduste kaitse konventsioon (jõustunud 4. novembril 1950). - RT II 2010.
15. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (jõustunud 28.01.1981). - RT II 2001, 1.
16. Isikuandmete kaitse seadus. - RT I 1996, 48, 944.
17. Isikuandmete kaitse seadus. - RT I 2007, 24, 127... RT I, 30.12.2010, 11.
18. Soolise võrdõiguslikkuse ja võrdse kohtlemise voliniku ning kantselei põhimäärus. - RT I 2010, 33, 170.
19. Vabariigi Valitsuse seadus. - RT I, 27.12.2013, 33.
20. 2013. aasta riigieelarve seadus. - RT I, 28.12.2012, 9.

Kasutatud kohtupraktika

1. EKo 20.05.2003, C-465/00, C-138/01, C-139/01, *Verfassungsgerichtshof jt.*
2. EKo 06.11.2003, C-101/01, *Lindqvist.*
3. EKo 09.03.2010, C -518/07, *Commission vs Germany.*
4. EKo 24.11.2011, C-468/10 & C-469/10, *ASNEF & FECEMD.*
5. EKo 24.11.2011, C-70/10, *Scarlet Extended SA vs SABAM.*
6. EKo 16.10.2012, C-614/10, *Commission vs Austria.*
7. EK 25.06.2013, C-131/12, *Google Spain SL*, kohtujurist N. Jääskineni ettepanek.
8. EKo 08.04.2014, C-293/12, C-594/12, *Digital Rights Ireland Ltd jt.*

9. EIK 02.08.1984, 8691/79, *Malone vs The United Kingdom*, kohtunik Pettiti eriarvamus.
10. EIKo 26.03.1987, 9248/81, *Leander vs Sweden.*
11. EIKo 07.07.1989, 10454/83, *Gaskin vs The United Kingdom.*
12. EIKo 16.12.1992, 13710/88, *Niemietz vs Germany.*
13. EIKo 04.05.2000, 28341/95, *Rotaru vs Romania.*
14. EIKo 17.07.2008, 20511/03, *I vs Finland.*
15. EIKo 14.03.2013, 24117/08, *Bernh Larsen Holding AS and others vs Norway.*

16. RKHKo 3-3-1-3-12.
17. RKÜK 3-2-1-4-13.

Muud allikad

1. Andmekaitse Inspektsiooni ettekanne Riigikogu põhiseaduslikkuse komisjonile ja õiguskantslerile. 2003. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/2003.rtf, 29.04.2014.
2. Andmekaitse Inspektsioon. Palgaandmed 2014 1. aprilli seisuga. Arvutivõrgus: <https://www.aki.ee/et/palgaandmed-2014-1-aprilli-seisuga>, 01.05.2014.
3. Article 29 Data Protection Working Party. Advice paper on the practical implementation of the Article 28 (6) of the Directive 95/46/EC. Brussels: 04.04.2011. Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex3_en.pdf, 01.05.2014.
4. Article 29 Data Protection Working Party. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. The future of privacy. WP 168. Brussels: 01.12.2009. Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf, 30.04.2014.
5. Article 29 Data Protection Working Party. Opinion 01/2012 on the data protection reform proposals. WP 191. Brussels: 23.03.2012. Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf, 30.04.2014.
6. Article 29 Data Protection Working Party. Opinion 03/2010 on the principle of accountability. WP 173. Brussels: 13.07.2010. Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf, 30.04.2014.
7. Article 29 Data Protection Working Party. Opinion 05/2012 on cloud computing. WP 196. Brussels: 01.07.2012. Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf, 30.04.2014.
8. Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. - ELT L 124, 20.05.2003, p 36 - 41.
9. Council of European Municipalities and Regions. General Data Protection Regulation. Revise the existing directive for the public sector. Brussels: November 2012. Available: http://www.ccre.org/docs/cemr_position_paper_data_protection_en.pdf, 01.05.2014.
10. Courtesy translation of the consolidated version of the Fundamental Law of Hungary, effective as of 1 April 2013. Available: <http://tinyurl.com/q2x66k6>, 29.04.2014.
11. Data Guidance. EU right to be forgotten now right to erasure. 2013. Available: http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2119, 30.04.2014.

12. Eesti seisukohad justiitsküsimustes Euroopa Liidu justiits- ja siseministrite 17. ja 18. jaanuari 2013. a mitteametlikul kohtumisel. Arvutivõrgus: <http://tinyurl.com/oq6pqsr>, 30.04.2014.
13. Electronic Privacy Information Centre. Investigations of Google Street View. Available: <http://epic.org/privacy/streetview/>, 01.05.2014.
14. Euroopa Komisjoni eelnõu „Euroopa Parlamendi ja nõukogu direktiiv üksikisikute kaitse kohta seoses pädevates asutustes isikuandmete töötlemisega kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumise kohta“. KOM(2012) 10. Brüssel: 25.01.2012. Arvutivõrgus: <http://eur-lex.europa.eu/legal-content/et/ALL/?uri=CELEX:52012PC0010>, 01.05.2014.
15. Euroopa Komisjoni eelnõu „Euroopa Parlamendi ja nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta“. KOM(2012) 11. Brüssel: 25.01.2012. Arvutivõrgus: <http://eurlex.europa.eu/legalcontent/ET/TXT/HTML/?uri=CELEX:52012PC0010&qid=1399011567208&from=EN>, 01.05.2014.
16. Euroopa Komisjoni eelnõu seletuskiri „Euroopa Parlamendi ja nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta.“ KOM(2012) 11. Brüssel: 25.01.2012. Arvutivõrgus: <http://eur-lex.europa.eu/legalcontent/ET/TXT/HTML/?uri=CELEX:52012PC0010&qid=1399011567208&from=EN>, 29.04.2014.
17. Euroopa Komisjoni teatis Euroopa Parlamendile, nõukogule, majandus- ja sotsiaalkomiteele ning regioonide komiteele. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus. KOM(2010) 609 lõplik. Brüssel: 04.11.2010. Arvutivõrgus: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_et.pdf, 29.04.2014.
18. European Commission communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century. COM(2012) 09 final. Brussels: 25.01.2012. Available: <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012DC0009>, 29.04.2014.
19. European Commission. Data protection regulation: consistency mechanism explained. 06.02.2013. Available: http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm, 01.05.2014.

20. European Commission. EU Charter of Fundamental Rights. Available: http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm, 29.04.2014.
21. European Commission Impact Assessment Board. Opinion. DG JUST - Impact assessment on reform of personal Data protection in EU. D(2011). Brussels: 09.09.2011. Available: http://ec.europa.eu/smartregulation/impact/ia_carried_out/docs/ia_2012/sec_2012_0074_en.pdf, 30.04.2014.
22. European Commission MEMO. Data Protection Day 2014: Full Speed on EU Data Protection Reform. MEMO/14/60. Brussels: 27.01.2014. Available: http://europa.eu/rapid/press-release_MEMO-14-60_en.htm, 30.04.2014.
23. European Commission MEMO. Progress on EU data protection reform now irreversible following European Parliament vote. MEMO/14/186. Brussels: 12.03.2014. Available: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm, 29.04.2014.
24. European Commission. Reform of the data protection regulation legal framework. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/review/index_en.htm, 02.02.2014.
25. European Commission report. First report on the implementation of the Data Protection Directive (95/46/EC). COM(2003) 265 final. Brussels: 15.05.2003. Available: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52003DC0265#text>, 29.04.2014.
26. European Commission staff working paper. Impact assessment. SEC(2012) 72 final. Brussels: 25.01.2012. Available: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf, 29.04.2014.
27. European Data Protection Supervisor. On the data protection reform package. Brussels: 12.03.2012. Available: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf, 30.04.2014.
28. European Economic and Social Committee. Opinion on the „Proposal for General Data Protection“. - ELT C 229, 31.07.2012.
29. European Parliament legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Ordinary legislative procedure - first reading. P7_TA(2014) 0212. Strasbourg: 12.03.2014. Available: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=%2f%2fEP%2f%2fTEXT%2bTA%2bP7TA20140212%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN>, 28.04.2014.

30. European Payment Institutions Federation. EPIF's position paper on the European Commission's proposal for a general data protection regulation. 26.04.2013. Available: <http://www.paymentinstitutions.eu/documents/download/17/attachement/epif-position-paper-on-the-proposed-general-data-protection-regulation.pdf>, 28.04.2014.
31. Europe vs Facebook. Legal procedure against Facebook Ireland Limited. Available: <http://europe-v-facebook.org/EN/Complaints/complaints.html>, 30.04.2014.
32. Fundamental Rights Agency. Access to data protection remedies in EU Member States. Data protection remedies at national level. Luxembourg: Publications office of the European Union 2013.
33. Fundamental Rights Agency. Data Protection in the European Union: the role of National Data Protection Authorities. Luxembourg: Publications office of the European Union 2014.
34. Fundamental Rights Agency, European Commission. Handbook on European Data Protection law. Luxembourg: Publications office of the European Union, 2014. Available: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, 01.05.2014.
35. Isikuandmete kaitse seaduse eelnõu. 1026 SE.
36. Keeleinspeksioon. Keeleinspeksiooni ametnike palgaandmed 2013. Arvutivõrgus: <http://www.keeleinsp.ee/?menu=32&news=1045>, 01.05.2014.
37. London Economics. Implications of the European Commission's proposal for a general data protection regulation for business. Final report to the Information Commissioner's Office. London: May 2013.
38. OECD. Members and partners. Available: <http://www.oecd.org/about/membersandpartners/>, 27.04.2014.
39. OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: 1980.
40. OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Preface. Available: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>, 28.04.2014.
41. OECD. OECD work on privacy. Available: <http://www.oecd.org/sti/ieconomy/privacy.html>, 28.04.2014.
42. Passing Clouds: The EC's data protection reform plans and their relevance for cloud computing. 2013. Available: https://www.taylorwessing.com/globaldatahub/article_passing_clouds.html, 30.04.2014.

43. Privacy International. Report: Latvia. Chapter I - legal framework. Available: <https://www.privacyinternational.org/reports/latvia/i-legal-framework>, 29.04.2014.
44. Privacy International. Report: Lithuania. Chapter I - legal framework. Available: <https://www.privacyinternational.org/reports/lithuania/i-legal-framework>, 29.04.2014.
45. Soolise vördõiguslikkuse ja vördse kohtlemise volinik. Ametnike palgaandmed. Arvutivõrgus: <http://www.svv.ee/index.php?id=551>, 01.05.2014.
46. Special Eurobarometer 359. Attitudes on data protection and electronic identity in European Union. Brussels: 2011. Available: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, 29.04.2014.
47. The Council of Europe. A Convention to protect your rights and liberties. Arvutivõrgus: <http://human-rights-convention.org/>, 27.04.2014.
48. The Council of Europe. Note from Presidency. 5882, 31.01.2014, p 4. Available: <http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&f=ST%205882%202014%20IN%20IT>, 01.05.2014
49. The Council of Europe. Treaty Office. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.:108. Available:<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG>, 28.04.2014.
50. The Council of European Union press release. 3260th Council meeting. Justice and home affairs. PR CO(2013) 14149. Luxembourg: 07. - 08.10.2013. Available: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/138925.pdf, 28.04.2014.
51. The Council of Europe. European Convention on Human Rights. Accession of the European Union. Available: <http://hub.coe.int/what-we-do/human-rights/eu-accession-to-the-convention>, 27.04.2014.
52. The Council of Europe. European Convention on Human Rights. Impact in 47 countries. Available: <http://human-rights-convention.org/impact-of-the-european-convention-on-human-rights/>, 28.04.2014.
53. The Council of European Union press release. 3279th Council meeting. Justice and home affairs. PR CO(2013) 17342. Brussels: 05. - 06.12.2013. Available: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/139938.pdf, 29.04.2014.

54. The United Kingdom Ministry of Justice. Impact assessment: Proposal for an EU data protection regulation. 22.11.2012. Available: Proposal for an EU Data Protection Regulation - government impact assessment, 29.04.2014.
55. The United Kingdom Ministry of Justice. Government response to Justice Select Committee's opinion on the European Union Data Protection framework proposals. January 2013. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/217296/response-eu-data-protection-framework-proposals.pdf, 29.04.2014.
56. Vabariigi Valitsuse 29.03.2012 otsuse seletuskiri. Eesti seisukohad isikuandmete kaitset puudutavate Euroopa Komisjoni algatuste suhtes. Arvutivõrgus: <https://dhs.riigikantselei.ee/avalikteave.nsf/documents/NT0018C882?open>, 28.04.2014.
57. Õiguskantsleri märgukiri justiitsministrile. Tallinn: 21.07.2011. Arvutivõrgus: http://lasteombudsman.ee/sites/default/files/field_document2/6iguskantsleri_margukiri_elatisvolglaste_nimekirjade_avalikustamine.pdf, 29.04.2014.
58. Õiguskantsleri vastus Andmekaitse Inspeksiooni märgukirjale. Tallinn: 26.02.2014. Arvutivõrgus: http://oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_oigus_votta_nousolek_isikuandmete_tootlemiseks_tuupingimustes.pdf, 29.04.2014.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Sandra Sillaots (sünnikuupäev: 06.04.1990),

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Isikuandmete kaitse regulatsiooni ühtlustamine isikuandmete kaitse üldmääruse eelnõus ja selle mõju Eestile,“ mille juhendaja on professor Kalle Merusk,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace'i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartu, 05.05.2014.a