

TALLINNA TEHNIKAÜLIKOOL
Majandusteaduskond
Ragnar Nurkse innovatsiooni ja valitsemise instituut

Grete Õigemeel

**ISIKUANDMETE KAITSE ÜLDMÄÄRUSEGA KAASNEVAD VÄLJAKUTSED JA
MÕJUD VÄIKEETTEVÕTETE RAKENDUSKOORMUSELE: EESTI TURUNDUS- JA
REKLAAMIVALDKONNA ETTEVÕTETE KAASUS**

Magistritöö

Juhendaja: Tarmo Kalvet, PhD
Kaasjuhendaja: Kärt Salumaa, MA

Tallinn 2018

Deklareerin, et olen koostanud töö iseseisvalt ja olen viidanud kõikidele töö koostamisel kasutatud teiste autorite töödele, olulistele seisukohtadele ja andmetele, ning ei ole esitanud sama tööd varasemalt ainepunktide saamiseks. Töö pikkuseks on 10 930 sõna sissejuhatusest kuni kokkuvõtte lõpuni.

Grete Õigemeel

(allkiri, kuupäev)

Üliõpilase kood: 123240 HAAMM

Üliõpilase e-posti aadress: grete.oigemeel@gmail.com

Juhendaja: Tarmo Kalvet, PhD

Töö vastab kehtivatele nõuetele

.....

(allkiri, kuupäev)

Kaasjuhendaja Kärt Salumaa, MA

Töö vastab kehtivatele nõuetele

.....

(allkiri, kuupäev)

SISUKORD

SISSEJUHATUS	5
1. ETTEVÕTETE RAKENDUSKOORMUS MUUTUVAS ANDMEKAITSEKESKKONNAS – TEOREETILINE RAAMISTIK	8
1.1 Regulatsioonide mõju rakenduskoormusele	8
1.2 Teoreetilised lähtekohad mõjude hindamisel	9
1.2.1 Tehingukulude teooria	10
1.2.2 Biheivioristlik teooria	13
1.3 Privaatsus ja andmekaitse	16
1.3.1 Privaatsuse kontseptsiooni roll andmekaitsekeskkonna väljakujunemisele	16
1.3.2 GDPR mõjud Euroopa Liidu ettevõtetele	17
1.4 VKE muutuv as andmekaitseraamistik - turundus- ja reklaamisektor	20
1.5 Analüüsiraamistik	22
2. EMPIIRILINE ANALÜÜS	26
2.1 Andmekaitse areng Eestis	26
2.2 Uurimismeetodid	27
2.3 Analüüs GDPR nõuete mõju ja ulatuse hindamiseks	29
2.3.1 Eesmärgipärane isikuandmete töötlemine ning võimalikult väheste andmete kogumine	30
2.3.2 Andmekvaliteedi tagamine ja isikuandmete piiratud säilitamine	32
2.3.3 Isikuandmete turvalisuse tagamine	34
2.3.4 GDPR rakendamise kitsaskohad ja mõjud	36
3. DISKUSSIOON	39
SUMMARY	46
KASUTATUD ALLIKAD	49
LISAD	59
Lisa 1. Intervjuude loetelu	59
Lisa 2. Poolstruktureeritud intervjuu küsimused	59
Lisa 2. Isikuandmete tööstustoimingute kaardistamine ja võrdlus GDPR ja IKS põhjal	62

LÜHIKOKKUVÕTE

Tehnoloogia areng ja digitaliseerimine on toonud kaasa olukorra, kus olemasolevad andmekaitsereeglid ei ole piisavad tagamaks laiapõhjalist isikuandmete kaitset. Seetõttu nähti vajadust uuendatud, laiema spektriga ja tugevama andmekaitseraamistiku järgi, mis pani aluse isikuandmete kaitse üldmääruse (ingl. *General Data Protection Regulation*, edaspidi: GDPR) väljatöötamisele. GDPR, mida hakatakse kohaldama alates 25. mai 2018, annab andmesubjektidele suuremad õigused enda isikuandmete kontrollimise ja kaitsmise üle.

Erinevate uuringute põhjal on selgunud, et GDPR suurendab ettevõtete halduskoormust. Lisaks on esile tõusnud, et teadlikkuse tase GDPR kaasnevatest kohustustest ja ettevõtete üldine valmisolek GDPR nõuete täitmiseks on madal. Sellest lähtudes soovitakse teada, millised on GDPRiga kaasnevad väljakutsed ja mõjud väikeettevõtete rakenduskoormusele. Magistritöö eesmärgi saavutamiseks püstitatakse kaks uurimisküsimust. Esimese uurimisküsimusega soovitakse teada, millised on peamised väljakutsed GDPR nõuete rakendamisel ning teise uurimisküsimusega hinnatakse GDPR nõuete mõju väikeettevõtete rakenduskoormusele. Magistritöö on jagatud kolme peatükki.

Magistritöö eesmärgi saavutamiseks ja küsimustele vastamiseks toetutakse akadeemilistes allikates üldlevinud teoreetilistele seisukohtadele. Mõjude hindamise, regulatsioonide poolt püstitatud väljakutsete ning regulatsiooninõuete täitmise raamistamiseks tuginetakse tehingukulude ja biheivioristlikule teooriale.

Analüüsi tulemustest selgub, et peamiste väljakutsetena kerkisid esile regulatsiooni tõlgendamine, läbipaistvuse tagamine, organisatoorse valmisoleku saavutamine ning tööstustoimingute registri väljatöötamine. Selgema arusaamise puudumine GDPRist võib näidata seda, et riigi roll GDPR kaasnevate kohustuste teadvustamisel ja ettevõtete teavitamisel võib olla madal.

Võtmemõisted: GDPR, IKS, VKE, rakenduskoormus, halduskoormus, tehingukulud

SISSEJUHATUS

Ükski toimiv majandus ei saaks korralikult funktsioneerida ilma regulatsioonideta, kuna õigesti loodud regulatsioonid loovad aluse ühiskonna ja majanduse stabiilsele arengule (Munnich 2004, 5). Regulatsioonid aitavad edendada majanduslikku ja sotsiaalset kasvu, kuid võivad luua samas ebavajalikke takistusi, vähendada innovatiivsust, investeringute osakaalu, tuues kaasa majandusliku ja sotsiaalse kulu suurenemise (Bageri 2011, Munnich 2004; Voermans 2015; Bradford 2004, 5-6). Arnold *et al.* (2008) leiab, et ranged regulatsioonid mõjutavad otseselt kasvu ja arengut, põhjustades sellega omakorda probleeme tänapäeva kapitalistlikus ühiskonnas tegutsevatele ettevõtetele, kus aeg on raha ning nõudlus ja tarbimus pideva innovatsiooni, kaupade, teenuste, ideede järgi on suur (Pollitt 2008). Selle asemel, et ettevõtted saaksid panustada arengusse, peavad nad tegelema regulatsioonide poolt seatud nõuete täitmise ja järgimisega (Bageri *et al.* 2011, 6). Nõuete ja reeglite täitmise poolt põhjustatud koormus segab neid paratamatult keskendumast ettevõtte põhitegevusele, sunnib neid ebaefektiivselt kasutama oma ressursse (Hopkins 1998, 315), kuna valitsuse poolt kehtestatud reeglite ja kohustuste täitmine nõuab aega ja raha, mida nad oleksid saanud kasutada efektiivsemal viisil (Bianco, Bripi 2010; Bageri *et al.* 2011, 13; Hopkins 1998; Government of Canada 2010).

Tehnoloogia areng on toonud kaasa inforevolutsiooni, mis on loonud ettevõtetele palju võimalusi ja väljakutseid (Bergerson 2016, 29), suurendanud huvi isikuandmete kasutamise vastu (Acquisti 2013, 2), mille korral on andmesubjektid jäänud tihtipeale informatsioonisulgu ning teadmatusse, kuidas nende andmeid kasutatakse (Magnusson 2017, 4). GDPR, mida hakatakse kohaldama alates 25. mai 2018, annab andmesubjektidele suuremad õigused enda isikuandmete kontrollimise ja kaitsmise üle, vähendades sellega isikuandmete oportunistlikku kasutamist ettevõtete poolt (*Ibid.*) GDPR, mis on välja kasvanud 13. detsembril 1995. aastal jõustunud andmekaitse direktiivist 95/46/EU (ingl. *Data Protection Directive*, edaspidi DPD), ei käi välja uut ideoloogiat isikuandmete kaitsmiseks, vaid tugevdab olemasolevat õiguslikku raamistikku (Böröcz 2016, 470). Ettevõtete usaldusväärsust hakkab üha enam demonstreerima see, kas isikuandmete kaitsmine on struktureeritud ja tõhus (Flett, Wilson 2017, 4), pannes proovile ettevõtete

jätksuutlikkuse (Manne 2016). GDPR toob ettevõtteid andmesubjektidele lähemale ning muudab tegevuse läbipaistvamaks. Kuid läbipaistvuse suurendamisega kaasnevad ettevõtetele ka märkimisväärsed muudatused (Böröcz 2016), mis võivad piirata ettevõtlustegevust, suurendada ettevõtetele langevat koormust ja nõrgestada seeläbi kasvu ning innovatiivsust (London Economics 2017, 2).

Magistritöö eesmärk on välja selgitada, tuginedes teoreetilisele raamistikule ja uurimuse käigus läbiviidud intervjuudele, kas ja kuidas mõjutab GDPR turundus- ja reklaamivaldkonnas tegutsevate väikeettevõtete rakenduskoormust. Töö kitsendamiseks keskendutakse kindlale sektorile. Mikroettevõtete, väikese ja keskmise suurusega ettevõtete (edaspidi VKE) seast keskendutakse eelkõige väikeettevõtetele, sest erinevate uuringute põhjal tuleb esile, et teadlikkus ja valmisolek GDPRiks on väikeettevõtete (1-49 töötajat) seas kõige madalam, samas mõjud väikeettevõtetele on suured (Fearn 2018). Kuna akadeemilised allikad ei keskendu väikeettevõtetele eraldi, vaid käsitlevad VKE ühtse kontseptsioonina, siis väikeettevõtete käsitus põhineb teoreetilises osas VKE raamistikul. Digitaliseerumine on muutnud andmete kasutamise üha kessemaks töövahendiks reklaami- ja turundussektoris, samas muudab GDPR andmete kasutamise piiratumaks, tuues neile kaasa uued väljakutsed. Samas nähakse tegevust pärssivat mõju turundussektorile (Berkeley 2018). Eelolevale tuginedes otsustati antud magistritöös keskenduda põhiorhuga väikeettevõtetele, reklaami- ja turundussektori kaasusele.

Magistritöö eesmärgi saavutamiseks püstitatakse järgmised uurimisküsimused:

1. Millised on väikeettevõtete peamised väljakutsed GDPR nõuete rakendamisel?
2. Millised GDPR nõuded mõjutavad väikeettevõtete rakenduskoormust enim?

Magistritöö eesmärgi saavutamiseks toetatakse akadeemilistes allikates üldlevinud teoreetilistele seisukohtadele, mis on privaatsuse, regulatsioonide ja nende mõjude omavaheliste seoste tõlgendamiseks, keskenduses aspektile, kas soovitud tulemused isikuandmete kaitsmisel saavutatakse nii, et ettevõtetele ei lasu ebamõistlikku koormust (OECD 2014, 61). Sellest lähtuvalt analüüsitakse käesolevas magistritöös GDPR mõju biheivioristliku teooria, tehingukulude teooria seisukohtadele ja rahvusvahelistele uuringutulemustele toetudes, mis aitavad testida töös esitatud väiteid ning seletada põhjuslikke seoseid regulatsioonide ja ettevõtetele langeva koormuse vahel (Kirkpatrick, Parker 2012).

Magistritöö on jagatud kolme peatükki. Esimene peatükk moodustab teoreetilise raamistiku, kus vaadatakse lähemalt rakenduskoormuse ja privaatsuse kontseptsiooni olemust ning selle käsitlemist VKE kontekstis. Seejärel kaardistatakse Euroopa Liidu ettevõtete põhjal läbiviidud uuringutele toetudes GDPR peamised kulukohad, mis aitavad empiirilises osas analüüsida GDPR koormuse ulatust väikeettevõtetele. Teine peatükk moodustab empiirilise osa. Empiirilise osa esimene alapeatükk annab ülevaate isikuandmete kaitse arengust Eestis. Teine alapeatükk keskendub kasutatavatele uurimis- ja andmekogumismeetoditele. Empiirilise peatüki kolmandas osas analüüsitakse intervjuude käigus saadud vastustele tuginedes kaardistatud nõudeid rakenduskoormuse hindamiseks. Käesoleva magistritöö kolmanda osa moodustab analüüsi tulemusi süvitsi käsitlev diskussiooni peatükk. Antud töö empiiriline osa peaks vastama teoreetilises osas püstitatud eesmärgile ning kinnitama või ümber lükkama seal väljatoodud seisukohti.

Autor tänab juhendajaid ja intervjueeritavaid olulise panuse eest magistritöö valmimisse.

1. ETTEVÕTETE RAKENDUSKOORMUS MUUTUVAS ANDMEKAITSEKESKKONNAS – TEOREETILINE RAAMISTIK

1.1 Regulatsioonide mõju rakenduskoormusele

Regulatsioone käsitletakse kui sotsiaalse struktuuri kogumit, millel on võimekus mõjutada seatud kohustusi (Kitching, 2006, 7). Seetõttu on ettevõtted sunnitud muutma oma toiminguid, tootma, talletama ja edastama suures koguses andmeid (Arendsen, van Engers 2004, 2), tuues kaasa kasvavad rakenduskulud¹, mida nad endale vabatahtlikult ei valiks (Nijsen 2000, 20, 43). Rakenduskoormuse (*ingl. compliance burden*) tähenduse, olemuse ja mõõtmise lahtimõtestamine on komplekssemaid ja keerulisemaid tegevusi, kuna selle olemus sõltub suuresti uurimuse valdkonnast ning autori antud definitsioonist (Rantaša 204, 28; Boylaud *et al.* 2000, 17; Acquisti, Romanosky 2009, 1062).

Kuigi autorite (Munnich 2004; Wegrich 2009; Harvey *et al.* 2014; Bageri *et al.* 2011; Heinrich 2015, 405) lähenemine rakenduskoormuse defineerimisel võib erineda, nähakse siduva joonena seda kui bürokraatia osa, mis on ettevõtetele koormaks nii ajas kui rahas. Sinna alla võib lugeda akadeemilises kirjanduses läbivate terminitena rakenduskulusid² ja administratiivkulusid³ (Chittenden *et al.* 2002, 10; OECD 2014, 13).

Vaadates seaduste, regulatsioonide kujunemist ajas, tuuakse välja, et regulatsioonide kulude kasv suureneb majandusharu kasvuga (Stigler 1971, 12). Erinevate autorite seisukohtadest nähtub, et

¹ Õigusnormide täitmisega seotud rakenduskulud (*eng. compliance costs*) on kõik kulud, mida tehakse ettevõtete või teiste osapoolte poolt, kellele antud regulatsioon on suunatud selleks, et järgida regulatsiooni nõudeid (OECD 2014, 12).

² Kulutused tööjõule, seadmetele, tarkvarale, õppimisele, süsteemi haldamisele (OECD 2014).

³ Kulu ajas ja rahas, mis tekib infokohustuste täitmisega (OECD 2014; Kox 2005, 2; Wegrich 2009).

ülereguleerimine võib mõjutada negatiivselt majanduskasvu (Voermans 2015, 96; Butter *et al.* 2009, 2; Bianco 2010). Kuid see ei pruugi tingimata tähendada, et uued regulatsioonid toovad kaasa ettevõtetele rakenduskoormuse kasvu. Bennett *et al.* (2010) toob välja, et olemasolev õigusraamistik, mille peale rajatakse uus regulatsioon võib vähendada tehingukulusid ning kui ühendada olemasolev regulatiivne raamistik uuega, siis ei pruugi see tähendada ainult tehingukulude vähenemist, vaid ka väiksemat halduskoormust ettevõtetele. Seetõttu on oluline uue regulatsiooni disainimisel arvestada, et see ei pärsiks ettevõtete arengut ja kasvu (Lundstrom, Stevenson 2005, 10; Harvey *et al.* 2014; Kirkpatrick, Parker 2012, 9). Sest kui seadustega kaasnevad tehingukulud on nii kõrged, et need ületavad sellest saadavat kasu⁴, võib see pidurdada regulatsiooni plaanitud mõju (Ciriani 2015, 51; Oprysk 2016, 31). Võib tekkida olukord, mis viib eemale investeeringutest, takistab uutele turgudele sisenemist, vähendab töökohtade loomist ning halvab ettevõtlust (Munnich 2004, 9; Kljucnikov 2016, 17; Wegrich 2009, 7; Hampton 2005, 33; Barazzoni *et al.* 2006, 27).

Arnold *et al.* (2008) leiab, et ettevõtte riskid suurenevad koos regulatsiooninõuete täitmisest tulenevast koormusest. Regulatsiooninõuete täitmisega kaasnevat koormust ja bürokraatiat peetakse oluliseks takistuseks ettevõtte arendamisel ja ka uue ettevõtte loomisel (Kljucnikov, Sobeková 2016, 17; Bageri *et al.* 2011, 13). Peamine probleem seisneb selles, et paljud kulud, sealhulgas administratiivkulud, on fikseeritud ning sellest tingituna ei jagu paljudel ettevõtetel piisavalt ressursse (rahalised, ajalised, ekspertteadmised). Sellest tulenevalt võivad olla ettevõtted erinevatele muutustele haavatavamad (Kitching 2006, 18; Kljucnikov, Sobeková 2016).

1.2 Teoreetilised lähtekohad mõjude hindamisel

Hästi disainitud regulatsioonid peaksid arvesse võtma regulatsiooni jõustamise ja rakendamisega seotud normatiivseid soovitusi, piiranguid ning eeldatavaid takistusi, mis kujundavad regulatsiooninõuete täitmisega kaasnevat koormust reguleeritavatele (Stiglitz 2009, 13). Kitching *et al.* (2015) toob välja, et ettevõtted reageerivad regulatsioonide ja seaduste poolt pandud kohustustele mitmel viisil – nad lihtsalt ei järgi seatud nõudeid või järgivad neid viisil, mis on erinev regulatsiooni või seaduse poolt sätestatust. Seetõttu on oluline, et regulatsioonid võtaksid

⁴ Väga mitmed majandusanalüüsid on toonud välja, et Euroopa ettevõtetele peale pandav rakenduskoormus kaalub üle saadava tulu (Ciriani 2015).

arvesse erinevaid dünaamilisi mõjutusi ettevõtete tegevusele ja sooritusele. Sellele tuginedes valiti käesoleva magistritöö teemast lähtuvalt mõjude väljaselgitamise raamistamiseks teoreetilised seisukohad, mis ei tugine eeldusele, et inimesed teevad ainult ratsionaalseid otsuseid, vaid teooriad, mis võtavad arvesse otsuseid, mis on tehtud olukorras, kus informatsioon on asümmeetriline ja reaalsed tulemused võivad olla teadmata (Lunn 2012, 433). Kahneman 2002. aastal Nobeli auhinnaga pärjatud tööle toetudes võib välja tuua, et üha rohkem on liigutud kaugemale traditsioonilisest majandusteooriast, kuna on selgunud, et inividid käituvad süstemaatiliselt viisil, mis on erinev sellest, mida on võetud aluseks ratsionaalse teooria mudelite puhul (Stiglitz 2009, 16). Sellele tuginedes võivad aidata tehingukulude teooria ja biheivioristlik teooria paremini mõista neid aspekte, mis mõjutavad regulatsiooninõuete täitmisega kaasnevat väljakutseid ja rakenduskoormust ettevõtetele.

1.2.1 Tehingukulude teooria

Regulatsiooni võib kirjeldada läbi tehingukulude prisma kui ebatäiuslikku pikaajalist lepingulist suhet (Williamson 1976, 91), mis tähendab ettevõtetele aega ja raha, mida kulutatakse seaduse poolt pandud kohustuste täitmiseks (Martin 2013; Borgesius 2013, 31). Kui tavaline majandusteooria rõhub tulemustele, siis tehingukulude teooria keskendub protsessile ja pakub värskemad perspektiivi seletamiseks ettevõtte otsuseid ning seda, kuidas osapooled kaitsevad ennast lepingulises suhtes esilekerkivate ohtude eest (Carroll, Teece 1999, 54, 90). Tehingukulude teooriaga on liigutud kaugemale “majandusliku mehe” ideest, mida kasutatakse traditsioonilises majandusteaduses otsuste seletamiseks läbi ratsionaalse majandusteooria. Tehingukulude teoreetikud ei ole antud kontseptsiooni küll hüljanud, kuid on üha enam hakanud vaatama suunas, kus “majanduslik mees” optimeerib oma otsuseid ebatäiuslikumas maailmas (Tisdell 2004; Simon 1997, 1985). Seetõttu on ka lepingud juba loomu poolest ebatäiuslikud, sest puudulik informatsioon ja teadmised jätavad lepingud lünklikuks ning ei täpsusta asjaolusid täielikult. See aga ilmestab aspekti, kus informatsioon ei ole mitte ainult asümmeetriline, vaid ka kulukas. (Simon 1997)

Williamson (1979) toob välja, et tehingukulude suurust ja loomust iseloomustavad peamiselt oportunity, ebakindlus ja varade spetsiifilisus. Kui traditsiooniline majandusteooria eeldab, et inimene teeb alati ratsionaalse otsuse, mis annab parima tulemuse isegi puuduliku informatsiooni

korral (Department of Public Expenditure and Reform 2014, 4), siis tehingukulude teooria toob välja, et inimesed on piiratud ratsionaalsusega ja oportunistlikud (Williamson 1979; 2005; 1999; Simon 1985), nad ei ole võimelised ennast kogu informatsiooniga kurssi viima ning igasse tehingusse põhjalikult süvenema (Jenöffy-Lochau 1996, 744). Sellest tulenevalt puuduvad ettevõtjatel piisavad teadmised kõikide vajalike regulatsioonidest tulenevate kohustuste kohta⁵ (Lundstrom, Stevenson, 2005, 236) ning tihtipeale on vajalikule informatsioonile ligipääsetavus raskendatud (Hampton, Philips 2004, 23). Mistõttu on oluline informatsiooni kättesaadavus ja valitsusepoolne infotugi (Lundstrom, Stevenson, 2005, 240), kuna informatsiooni puudulikkus raskendab privaatsusega seonduvate otsuste tegemist ning võib tuua kaasa tehingukulude ebaproportsionaalse suurenemise (Acquisti 2007) - *ex ante* kulud (loe: tehingu eelsed) võivad olla küll algselt madalad, kuid viivad hilisemalt kõrgemate *ex post* (loe: tehingu järgsed) kuludeni (Crosson 2000).

Ebakindlus on Williamsoni (1979) käsitluse järgi üks tehingukulusid mõjutavatest teguritest ning regulatsiooni jõustumise eelselt käib kaasas alati teatud ebakindlus (Stewart 2010, 4), mis võib suurendada tehingukulusid (Jenöffy-Lochau 1996, 749). Ebakindlus võib olla tingitud asjaolust, kui seadusest ei saada hästi aru, ei nähta selles saadavat kasu, puudub piisav kogemus, võimekus ja vajalikud ressursid regulatsiooninõuete täitmiseks (Dale *et al.* 2005, 10-11; Pyykkö 2012). Seega ebakindlus võib suurendada ebaproportsionaalselt kulutusi tööjõule, seadmetele, tarkvarale ning kulutusi inimeste koolitamisele (OECD 2014, 13; Acquisti, Romanosky 2009, 1072). Ebakindluse tekkebaasiks on regulatsiooni seatud liiga keerulised kohustused, infokohustuste käsitlemiseks puuduv läbipaistvus ja sellega kaasnev ebaõiglane jaotus⁶ (Nijsen 2000, 70). Käitumuslik ebakindlus tõstab tehingukulusid, kui olulised aspektid üleminekus (ühelt seaduselt teisele) on liiga etteennustamatud või kui seaduse eelsed ja järgsed mõjud ei ole väga kergesti tuvastatavad (Williamson 1985; Christensen 2011, 8).

Kolmanda määratlusena, mis tehingukulude suurust mõjutab on varaspetsiifilisus, mis jaguneb omakorda kolmeks: asukohaspetsiifilisus, reaalvara spetsiifilisus ja inimkapitali spetsiifilisus (Williamson, 1985, 1996). Varaspetsiifilisus eksisteerib kui ettevõtte omab spetsiaalseid

⁵ Väiksemad ettevõtted on siinkohal ebavõrdsemas seisus (Bradford 2004), kuna neil puudub tihtipeale majasisene kompetents, mis võib olla olemas suurematel ettevõtetel (Bageri *et al.* 2011, 13).

tehnoloogilisi või juhtimislikke teadmiseid (Brouthers 2013) ning tehingukulu teooria eeldab, et varaspetsiifilisus võib aidata vähendada kulusid (Williamson 1979, 240).

Carter, Hodgson (2006, 464) toovad välja, et varaspetsiifilisuse ja välise ebakindluse vahel leiab positiivse seose ehk mida suurem on majanduslik ebakindlus, seda suurem on varaspetsiifilisus, mis võib omakorda mõjutada positiivselt *ex post* tehingukulusid.

Reaalvarade spetsiifilisus tähendab, et ettevõtte on teinud investeeringud spetsiaalsesse seadmetesse, tarkvarasse, mis teeb selle kasulikuks teatud grupile (Ducos 2007; Williamson, 1985, 1996). Kuna seadustega määratud kohustuste täitmiseks peavad ettevõtted paratamatult tegema ühel või teisel määral investeeringuid, millest tulenevalt võivad suurenedada ettevõtte kulutused (Bradford 2004, 7-11)⁷, siis võib eeldada, et ettevõtted, kes on spetsiaalselt investeerinud süsteemide loomisesse ning loonud etteulatuvalt struktuuri, mis tagab tugevama isikuandmete turvalisuse, kannavad väiksemaid tehingukulusid ühelt regulatsioonilt teisele üle minnes. Seda väidet aitab toetada Hornung (2012, 68) ja Irish SME Association (2018) läbiviidud uuring, mis tõi välja, et tugeva reguleeritusega riikides ja sektoris on uuele regulatsioonile üleminek kergem. Organisatsiooni varajases staadiumis tehtud investeeringud turvalisuse suurendamiseks (investeeringud spetsiifilisse tarkvarasse, lõimitud andmekaitse olemasolu) aitavad vältida andmete lekkimise võimalust, mis omakorda vähendab finantskulutusi (siinkohal trahvid, nõuded), mida ettevõtted peaksid tegema kahju tekitamise tõttu (Acquisti, Romanosky 2009, 1069).

Vajalike oskuste ja teadmistega on ettevõtetel võimalik ennast kindlustada riskide eest. Seetõttu mängib inimkapitali spetsiifilisus tehingukulude mõjutajana olulist rolli. Inimkapitali spetsiifilisus hõlmab kindlaid investeeringuid töötajatesse, et suurendada ettevõttespetsiifilisi teadmiseid ja tõsta produktiivsust (Christensen 2011, 7). Meyer (2001) väidab, et teadmiste puudumine turutoimingutes ja funktsioonides suurendab tehingukulusid ehk siit võib järeldada, et ettevõtetel, kellel on tugev majasisene andmekaitsealane kompetents, võivad kanda väiksemaid tehingukulusid. Tehingu kulud, mis on seotud inimkapitali spetsiifilisusega, on pannud ettevõtteid toetuma organisatsioonisisestele spetsialistidele, mis võib vähendada, võrreldes teenuse sisseostmisega, tehingukulusid. (Shekhovtsev 2018)

Tehingukulude teooria kasutamise üheks nõrkuseks on selle keskendumine liialt kulude minimeerimisele (Bartle, Ma 2001, 168) ning kaldub ignoreerima õppimise ja kogemusega seotud

⁷ Isikuandmete kaitse seaduse eelnõu seletuskiri (2018, 74).

mõjusid (Nooteboom 1993). Carroll, Teece (1999, 69) toovad välja, et tehingukulude teooria kasutamine analüüsi läbiviimisel kannab endas võimetust tegeleda probleemidega, mis käsitlevad ettevõtete üldist toimetulekut, alatähtsustab korralduslikke kulusid ning sotsiaalset suhet majanduslikes tehingutes.

1.2.2 Biheivioristlik teooria

Vaatamata sellele, et regulatiivsete mõjude hindamise raamistik on suuresti mõjutatud veel traditsioonilisest majandusteooriast, on üha rohkem hakatud kasutama erinevate teoreetikute poolt mõjude hindamisel biheivioristlikku mudelit (Simon 1955; Acquisti, Grossklags 2007; Kooreman, Prast 2007). Biheivioristliku teooria kasutamine mõjude selgitamisel pakub realistlikumat lähenemist (Simon 1959), aitab regulatsiooniga tekkivatest probleemkohtadest paremini aru saada ning lahti mõtestada, kuidas regulatsioon mõjutab majanduslikke otsuseid (Lunn 2012, 433, 427). Toetudes biheivioristlikule teooriale analüüsi läbiviimisel, võib see aidata täita tühimikku jälgitud majandusliku käitumise ja traditsioonilise majandusteooria eelduste vahel (Civita *et al.* 2011, 2). Kuna regulatsiooni peamine eesmärk on muuta teatud käitumismalli, mis aitab parandada sotsiaalset ja majanduslikku heaolu (Kirkpatrick, Parker 2012, 41; Solove 2002, 13), siis biheivioristliku majandusteooria kasutamine mõjude hindamisel aitab poliitika kujundajatel paremini disainida väiksemate kuludega poliitikaid, ilma, et sisseviidud nõuded moonutaks turgu ja piiraks indiviidi otsuseid (Kooreman, Prast 2007).

Coglianesi (2012, 18, 22) rõhutab, et käitumise hindamine võib aidata paremini selgitada vahetuid mõjusid – kui palju aitab regulatsioon muuta organisatsioonide käitumist, lahendada probleeme ning selgitada, miks muutused toimusid ja miks ei toimunud. Andmekaitse temaatika puhul on tegemist ühiskondlikult tundliku teemaga, mille laiaulatuslikuma reguleerimiseni on viinud teatud käitumismallid – otsused, hoiakud, valikud - privaatsuse kontseptsiooni adresseerimisel (Acquisti 2007, Coglianesi 2012, 8). Seega eesmärgiks on suunata ettevõtete käitumist, kuidas nad peaksid andmeid töötlema ja kaitsma (Manne 2016, 15). Kuna tugevad biheivioristlikud mõjud on nendes valdkondades, mis on seotud teatud tüüpi riskiga (andmete kaitsmine lekkimise eest, mõju ettevõtte reputatsioonile) (Department of Public Expenditure and Reform 2014, 13), siis aitab biheivioristlik teooria avada neid aspekte, mis on teiste teooriatega raskendatud ning näidata, kuidas on otsused mõjutatud keskkonnast, kus inividid opereerivad (Lunn 2012, 430). Seega

nägemus ohtudest, potentsiaalsetest kahjudest, vajadustest ja võimalustest mõjutavad üha rohkem andmetöötlust (Acquisti 2007).

Kuna regulatsioonidest tulenev koormus mõjutab ettevõtete käitumist juba enne seaduse jõustumist, mille tulemusena hakkavad ettevõtted suunama oma ressursse regulatsiooni täitmise suunas (Stewart 2010, 2), siis peab olema regulatsiooni funktsioon konkreetne, arusaadav ning regulatsioon kui reegel peaks töötama majandusharu kasuks (Acquisti, Romanosky 2009, 1076; Hertog 2010, 22). See on oluline seetõttu, et ettevõtted ei kulutaks ebaefektiivselt ressursse regulatsiooni nõudmistega vastavusse viimisel (PWC 2017). Acquisti (2010), Posner (1978, 1981) ja Stigler (1980) toovad välja, et privaatsuse kaitsmine valitsuse sekkumise läbi loob turul ebaefektiivsust ja on hukule määratud, kuna majanduslikku tootlikkust tõstvad ressursse kasutatakse sellisel juhul ebaefektiivsemalt, kuna informatsioon nende kvaliteedi kohta on turult eemaldatud. Näiteks turult eemaldatud andmete puhul, ei ole ettevõtetel uue töötaja palkamisel võimalik läbi viia taustakontrolli ja seeläbi võib ettevõtte palgata vale inimese (Acquisti 2013, 4). Samas on toonud Aubert, Rivard (2015) välja, et andmekaitse seadused võivad tõsta toomiskulusid ning välja ei saa jätta eeldatavat topeltmõju VKEdele. EBA ja RSM (2017) artiklis märgiti, et seadusest suurenevate kulude tõttu võivad hakata suurettevõtted kokkuhoidu tegema just VKEde ja allhankijate arvelt, kes on olnud partneriks mõne toote või teenuse väljatöötamisel. Seega võib järeldada, et GDPR võib teatud juhtudel tekitada väikeettevõtetele topeltkoormuse – ühelt poolt võivad väheneda tulud koostöö arvelt ja teiselt poolt võivad kulutada VKEd ebaproportsionaalselt rohkem seaduse täitmiseks. Siinkohal tõstatub probleemkoht - kas regulatsioonide täitmise kaasnep eeldatav suurem koormus VKEdele võib panna küsimuse alla nende jätkusuutlikkuse (Manne 2016, 11). Samas toovad Hermalin, Katz (2006) Murphy (1996) vastukaaluks Acquisti (2010), Posner (1978, 1981) ja Stigler (1980) seisukohtadele, et privaatsuse kaitsmisesse ei peaks nii kriitiliselt suhtuma, sest sellel võib hoopis olla positiivne mõju majanduslikule heaolule (Acquisti 2010, 5).

Kui ratsionaalse valiku teooria eeldab, et otsusetegijatel on piisav informatsioon otsuste tegemiseks, siis biheivioristlik teooria ütleb, et inimesed ei tee alati otsuseid, mis maksimeerivad kasumlikkust. Inimestel on otsuste tegemiseks piiratud hulk informatsiooni, läbi on võimalik kaaluda ainult teatud hulga otsuseid ning kui saadaval on liiga palju informatsiooni, viib see omakorda segaduseni või teatud tegevuse edasilükkamiseni. (Simon 1959; Department of Public Expenditure and Reform 2014, 4) Biheivioristlik majandusteooria tõstab esile, et toimijad ei tee ilmingimata otsuseid rangelt kaalutletud ratsionaalse analüüsi alusel, kuna neil on piiratud

kognitiivne võimekus. Mõnikord teevad nad otsuseid, mis ei ole seotud otseselt nende pikaajaliste plaanidega või tehtud otsused on mõjutatud kellegi teise huvidest (Civita *et al.* 2011).

Biheivioristlik teooria rõhutab, et inimesed peavad tegema otsuseid olukordades, mille puhul reaalsed tulemused on teadmata (Lunn 2012, 433). See võib viia olukorrani, kus regulatsiooninõude täitmiseks tehtud lisakulusid alahinnatakse või ülehinnatakse, mis viib ressursside ebaefektiivse jaotamiseni ja tehingukulude suurenemiseni (PWC 2017). Samas selgus Fenn ja Veljanovski (1988, 1055) poolt läbiviidud uuringust, et seaduse kuluteadlikkus viib vastupidise käitumiseni ehk regulatsiooninõuete täitmise vältimiseni.

Kuna regulatsioon peaks muutma nende inimeste, organisatsioonide käitumist, kellele regulatsioon on suunatud (Coglianese 2012, 12), siis ettevõtetel, kes on varasemalt viinud enda organisatsiooni vastavusse andmekaitseseadusega ning ellu viinud andmete lekkimisele reageerimise kava, on võimalik efektiivsemalt ootamatustele reageerida (Flett, Wilson 2017, 6). Suurenenud risk andmete lekkimiseks ei pane ettevõtteid mitte ainult kasutama efektiivsemaid meetmeid ja lahendusi, vaid paneb ettevõtted adopteerima rohkem andmetõhusaid ärimudeleid (Manne 2016, 7).

Pham *et al.* (2017, 70) tõstab esile, et efektiivseks käitumise suunamiseks turvanõuete täitmisel ja tugevdamisel on karistused reeglite rikkumise eest. Trahvid, sanktsioonid motiveerivad täitma regulatsioonist tulenevaid nõudeid (Fenn, Veljanovski 1988, 1055; Pham *et al.* 2017, 70), kuid samas trahvidega hirmutamine ei ole jätkusuutlik, kuna sellel on tugev mõju käitumisele (Flett, Wilson 2017), mis võib omakorda suurendada oportunismi (Carroll, Teece 1999). Mõju käitumisele, mis mõjutab kulude vahetamist, ei pruugi olla ainult ettevõtete suunalt, vaid ka andmesubjektide suunalt – tulemuseks võib tekkida olukord, kus andmesubjektid hakkavad liiga kergekäeliselt ära kasutama oma positsiooni ja leidma võimalusi ettevõtete karistamiseks⁸ määruses loodud õigustega (Hofheinz, Mandel 2014). Herath, Rao (2009) läbiviidud uuringus selgus, et töötajad, kes tundsid suuremat tõenäosust vahele jääda turvanõuete rikkumisega, järgisid reegleid rangemalt. Kuid samas tuuakse välja, et trahvidega hirmutamine võib viia valetamiseni, petmiseni ning kohustustest kõrvalehiilimiseni (Pham *et al.* 2017, 71). Sholtz (2001) rõhutab, et isikuandmete kaitsmine ei pruugi alati tulla valitsuse kehtestatud trahvimäärast, vaid pigem võimalikust negatiivsest meedia tähelepanust ettevõtetele.

⁸ Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, artikkel 82.

1.3 Privaatsus ja andmekaitse

1.3.1 Privaatsuse kontseptsiooni roll andmekaitsekeskkonna väljakujunemisele

Privaatsuse defineerimine on erinevate autorite seisukohtadele toetudes komplitseeritud, kuna varieerub vastavalt üksikisiku käsitlest (Acquisti *et al.* 2016, 9; Solove 2006; Elder *et al.* 2015, 6). Vaatamata sellele, et privaatsuse ja andmekaitse mõisted on omavahel seotud, tuleks antud kontseptsioone laiemalt käsitleda (ENISA 2014, 3). Kui privaatsuse kontseptsioon keskendub peamiselt normatiivsetele ja praktilistele käsitlestele andmetöötluses (Elder *et al.* 2015, 6), siis andmekaitse hõlmab indiviidide autonoomia edendamist (Bergkamp 2002, 36), reeglite kogumikku, mille eesmärgiks on saavutada suurem läbipaistvus (Andrade 2010,5) füüsiliste isikute õiguste ja vabaduste kaitsmisel (Tzanou 2013, 89; Henry 2015).

Vaadates andmekaitse ajaloolist kujunemist, siis oluline samm privaatsuse tugevdamisele ja kaitsmisele oli laiaulatuslikuma andmekaitseraamistiku loomiseks 13. detsembril 1995. aastal jõustunud DPD, mis määratles esmakordselt ära isikuandmete töötlemise ja andmete vaba liikumise korra Euroopa Liidus (Bergkamp 2002, 32; Tzanou 2013, 88; Cooper 2010). Kuid kiire tehnoloogiline areng tingis vajaduse uuendatud, laiema spektriga ja tugevama andmekaitseraamistiku järgi, mis pani aluse GDPRi väljatöötamisele. Kui DPD eesmärk oli kaitsta indiviidide privaatsust ja vähendada riske, mis kaasnevad andmete töötlemisega, reguleerides üldisemalt isikuandmete töötlemist (Bergkamp 2002, 35), siis GDPR on palju laiema spektriga, kindlustades pideva füüsiliste isikute kaitse, eemaldades takistused piiriüleises liikumises⁹ ning ühtlustades üleeuroopalist andmekaitsemaastikku. GDPR rakendamine peaks suurendama läbipaistvust, andmesubjektide ligipääsu andmetele, elimineerima ebavajalikud kulud, muutma regulatiivset keskkonda lihtsamaks, vähendama rahvusvaheliste ettevõtete halduskoormust, tooma andmesubjektid ja ettevõtted üksteisele lähemale (Rubinstein 2013; Koops 2014). Kuid Bergkamp (2002, 35) rõhutab, et nii kaua kui Euroopa Liit (edaspidi EL) portreerib andmekaitsega seonduvat probleemi, kui probleemi andmesubjekti ja ettevõtte vahel (luues väärpildi ettevõtte ja

⁹ Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, artikkel 1.

informatsiooni rollist majanduses), keskendudes andmekaitse karmimale reguleerimisele ja ettevõtete käitumise suunamisele, võib tekkida olukord, kus põhirõhk on aruandekohustustel ja dokumentatsioonil, mitte andmete reaalsel kaitsmisel (Koops 2014, 7). Pidev vormide ja reeglite täitmine võib viia olukorrani, kus reegleid jälgitakse ainult paberil.

1.3.2 GDPR mõjud Euroopa Liidu ettevõtetele

Läbiviidud uuringud on näidanud, et GDPR mõju Euroopa majandusele on märkimisväärne ning uurijad tugeva andmekaitse traditsioonidega riikidest on esile tõstnud, et GDPRiga astutakse hoopis samm tagasi. Samas on rõhutatud, et tugeva reguleeritusega riikides ja sektoris on valmisolek GDPR rakendamiseks suurem (Hornung 2012, 68; Irish SME Association 2018).

Mitmed uuringud, mis on GDPR mõjude analüüsimiseks läbiviidud, osutavad, et sellest saadav kahju EL majandusele võib olla suurem kui kasu, mille tulemusena kulutavad ettevõtted ebaefektiivselt aega ja ressursse, et adresseerida GDPRiga kaasnevaid kohustusi (Ciriani, 51; Flett, Wilson 2017, 7; PWC 2017). Pyykko (2012) toonitab, et märkimisväärne koormus ei lange pelgalt VKEdele, vaid siinkohal tuleb spetsiifiliselt vaadata ka sektori põhiselt. Brown (2017) tõi välja, et ettevõtted jagunevad kaheks - need kes näevad selles takistust ja need, kes näevad võimalust¹⁰. Uuringu käigus selgus, et GDPR paneb ebavõrdsesse olukorda finantssektori ning pidurdab finantsteenuste efektiivset pakkumist. Tarbijate usaldus krediitiasutuste vastu küll tõuseb, kuid samal ajal langeb teenuste pakkumise kvaliteet. Christensen *et al.* (2013) uuringust selgus, et GDPR võib tõsta ka ettevõtete tootmiskulusid, mistõttu väheneb nõudlus tööjõu juurdepalkamise järgi ning kõrgemad tootmiskulud raskendavad uute konkurentide turule tulemist. Tootmiskulude tõusu märkasid ka Bauer *et al.* (2013) ja Aubert, Rivard (2015). Samas rõhutavad uuringu läbiviijad, et suurenenud halduskoormus pärsib digitaalteenuste pakkujate konkurentsivõimet ning avaldab negatiivset mõju VKEdele, eelkõige andmetöötlusprotseduuride väljakujundamises ja süsteemide loomises. Suure probleemina tõstati ettevõttesisene andmekaitseline mõjuhinnang, selle sünkroniseerimine IT projektidega¹¹, andmekaitseametniku määramine ning vastutava töötaja - volitatud töötaja vahelise vahekord, mis võib tekitada tarbetuid dubleerivaid kulusid.

¹⁰ Võimalusena näevad seda pangandus, kütuse- ja õliettevõtted, telekomunikatsioon. Takistusena näevad seda tootmine, hulgimüük, transport, meedia, haridus.

¹¹ Tulemusena kiirem riskide avastamine ja ennetamine.

Christensen *et al.* (2013) toob välja, et GDPR on piiravam just nende ettevõtete suhtes, kes töötlevad suures mahus andmeid¹² (Hofheinz, Mandel 2014). GDPR võib tekitada olukorra, mille puhul andmesubjektide kätte langenud võim võib suunata neid ettevõtteid liiga kergekäeliselt karistama (*Ibid.*). Bauer *et al.* (2013) mõjuanalüüs ekspordisektori põhjal näitas, et Euroopa Liidu SKP väheneb, kui äritõkked kasvavad - katkestused tarneahelates ja andmete liikumises halvavad Euroopa Liidu ettevõtteid rohkem kui välispartnereid. Lisaks äritõketele valmistab paljudele ettevõtetele probleeme arusaamatus teatud nõuetes, mis suurendab omakorda ebakindlust. Ebakindluse ja regulatsiooni tõlgendamise problemaatilisuse nüanss tuli ka välja Irish SME Association (2018) uuringust, mis viidi läbi 502 VKE põhjal. Tulemustest selgus, et 82% ettevõtetest on teadlikud uuest määrusest, kuid 62% ettevõtetest ei oska öelda, mis muutuseid GDPR kaasa toob. 70% ettevõtetest ei ole läbi mõelnud samme, kuidas viia oma ettevõtte uute reeglitega vastavusse.

PWC poolt 2017. aastal läbiviidud uuringus 120 ettevõtte põhjal uuriti ettevõtete suhtumist privaatsusesse ning kuidas kujuneb ettevõtetel üleminek vanalt seaduselt uuele. Selgus, et kuna inimesi kirjeldatakse kui nõrgimat lüli privaatsuse juures, siis ettevõtted teadvustasid, et teadlikkuse tõstmine ja koolitused mängivad olulist rolli uue määruse rakendamisel¹³. Uuringust selgus ka, et organisatsioonid, kes puutusid pideva reguleeritusega kokku, olid ka GDPRiks ennast paremini ette valmistanud (sama tulemus Brown 2017. aasta uuringus). Peamise probleemina tõusis üles, et GDPR ei paku ülevaadet, kuidas tuleks sealseid kohustusi prioriseerida – kuna organisatsioonid järgivad tavaliselt kindlat lineaarset teed, siis võib tekkida olukord, kus ettevõtted kulutavad tulutult palju aega ja raha ennast GDPR nõudmistega vastavusse viimisel¹⁴. Antud uuringust selgus, et mida suurem on ettevõtte (töötajate arvu arvestades), seda suurema tõenäosusega teeb ta investeeringuid andmekaitseprotsesside tõhustamiseks ja täiendamiseks¹⁵. London Economics 2013 uuringust, 506 Suurbritannia ettevõtte põhjal, selgus samuti, et ettevõtetel on probleeme regulatsioonist arusaamisega ning seetõttu valitseb ebakindlus. Infopuudus ja arusaamatus näitasid, et riigi poolt ei ole olnud piisavalt tuge ettevõtjate harimisel ja teadlikkuse tõstmisel muudatuste osas. Uuring leidis veel, et seadusest mitteamusaamine viib ressursside ebaefektiivse jaotamiseni ja suurendab tehingukulusid (sarnane tulemus selgus ka

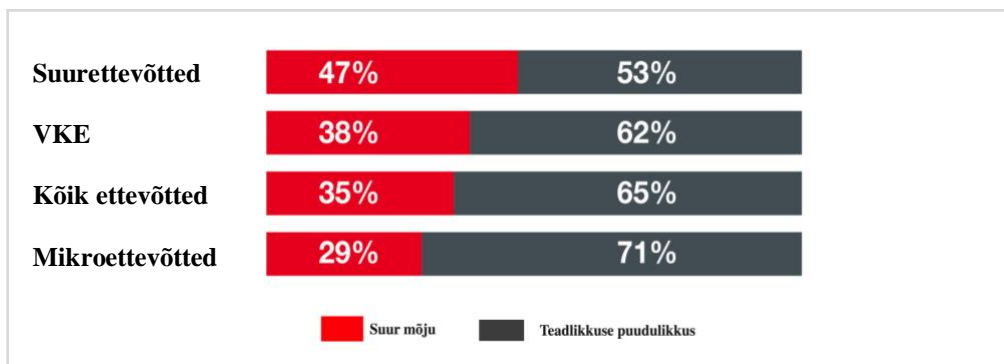
¹² Kuna VKEd on peamised, kes on saanud ennast infokeskse majanduse abil kõige rohkem arendada, siis võib andmekaitsemäärus just neid kõige raskemalt tabada (Hofheinz, Mandel 2014).

¹³ Samas selgus, et 45% ei ole viinud uue andmekaitse regulatsiooni valguses koolitusi läbi ning 35% vastanutest ütlesid, et kõik töötajad ei saa regulaarset koolitust.

¹⁴ Võib tekkida informatsiooni asümmeetria - organisatsioonid ei pruugi informatsioonipuudusest/teadmatuses pöörata tähelepanu kohustustele, mis on olulised erinevatele osapooltele.

¹⁵ Suuremad ettevõtted lähenevad regulatsiooni täitmisele struktureeritult, kuna risk mainekahjaks andmete lekkimise korral on suurem.

PWC 2017. aasta uuringust). One Poll läbi viidud uuring 500 Suurbritannia suurettevõtte seas tõstis esile, et ettevõtted seisavad silmitsi kolme suure takistusega: ülevaate puudumine andmete asukohtadest¹⁶, suur isikuandmete sissevool ning ebakindlus andmete omandiõiguses (Mayers 2017). Sama muster ilmnis ka Jonas 2018. aastal läbi viidud uuringust¹⁷. Jonas (2018) tõi välja, et paljud ettevõtted ei tea, kus ja kuidas on andmed hoiustatud ning olid pigem trahvinõuetes ignorantsemad. Uuringust ilmnis, et VKEd suhtuvad väiksema tõsidusega GDPR reeglitesse ja kalduvad alahindama karistuste mõju mittetäitmisel võrreldes suurettevõtetega. Allolev graafik näitab, et ettevõtted, kes olid GDPRga kaasnevate muudatustega rohkem kursis, hindasid ka mittetäitmise korral ilmnevaid finantskohustusi tõsisemaks.



Joonis 1. Teadlikkuse ja GDPR nõuete mittetäitmisega kaasnevate finantskohustuste suhte eeldatav mõju ettevõtete hinnangul

Allikas: Jonas (2018)

Võrdlusena EL riikides läbiviidud uuringutele on ka Eesti ettevõtete teadlikkus GDPRs madal - vastavalt IKS eelnõu seletuskirjas (2018) väljatoodud justiitsministeeriumi poolt tellitud ja Turu-uuringute AS läbiviidud küsitlusest 2017. aasta detsembris¹⁸ nähtub, et isikuandmete töötlemise ulatus Eestis tegutsevate ettevõtete seas on kõrge (mida ilmestab 95% määr rohkem kui 10 töötajaga ettevõtete seas), kuid ettevõtete teadlikkus samal ajal GDPRst madal¹⁹.

¹⁶ Umbes pooled vastanutest jagavad isikuandmeid oma koostööpartneritega.

¹⁷ Uuring viidi läbi Prantsusmaa, Suurbritannia, Saksamaa, Itaalia ja Hispaania ettevõtete seas.

¹⁸ Uuringu valim koosnes 166 Eestis tegutsevast ettevõttest, kus töötas rohkem kui üks töötaja (IKS eelnõud seletuskiri 2018).

¹⁹ Küsitlusele vastanutest ettevõtetest 36% ei olnud GDPRst midagi kuulnud, 47% ettevõtetest oli veidi kuulnud, 15% ettevõtetest oli kursis ja 2% ettevõtetest ei omanud selles osas seisukohta. Suurem teadlikkus GDPRst esines rohkem üle 50 töötajaga ettevõtete seas (IKS eelnõu seletuskiri 2018).

1.4 VKE muutuv as andmekaitseraamistikus - turundus- ja reklaamisektor

Vastavalt Euroopa Komisjoni andmetele on Euroopa Liidus 99% ettevõtetest VKEd, mille määratlemisel tuginetakse tabelis väljatoodud näitajatele.

	Töötajate arv	Aastakäive	Aastabilansi kogumaht	Aktiivsete ettevõtete osakaal Eestis 2017. a.
Mikroettevõte	< 10	≤ € 2 m	≤ € 2 m	119 887
Väikeettevõte	< 50	≤ € 10 m	≤ € 10 m	6 391
Keskmise suurusega ettevõte	< 250	≤ € 50 m	≤ € 43 m	1 150

Tabel 1. VKE määratlus väljatoodud parameetrite alusel

Allikas: Euroopa Komisjon (2003), Eesti Statistikaamet (2018)

Bageri *et al.* (2011, 13) väidab, et VKEd seisavad võrreldes suurettevõtetega silmitsi suuremate probleemidega, mida regulatsioonide rakendamisega kaasnev koormus neile põhjustab ning seeläbi võivad kanda ebavõrdselt suuremaid rakenduskulusid²⁰ (Lundstrom, Stevenson 2005, 196; Kitching 2006, 17; Baldwin 2004; Wegrich 2009; Bradford 2004; Dale *et al.* 2005; Kirkpatrick, Parker 2012, 51). Lundstrom ja Stevenson (2005, 59) rõhutavad, et ebaproportsionaalne ei ole ainult rahaline kulu, vaid ka ajakulu, mis regulatsiooninõuete täitmise peale kulutatakse²¹.

²⁰ Munnich (2004, 4) toob välja, et VKE jaoks on regulatsiooniga seatud kohustuste kulu peaaegu kuus korda suurem, kui keskmise ja suurema ettevõtte jaoks ning teenuse sektoris umbes kaks kolmandikku kõrgemad kulud kui toomissektoris tegutsevatele ettevõtetele.

²¹ Mikroettevõtted 1-2 töötajaga kulutavad peaaegu 5 tundi rohkem regulatsioonide poolt pandud kohustuste täitmiseks, kui ettevõtted 50 ja rohkema töötajaga (Baldwin 2004, 8).

Nooteboom (1993, 289, 291) on välja toonud, et VKEd kannavad suuremaid tehingukulusid, kuna nad on rohkem mõjutatud ebakindlusest, oportunistlikust käitumisest ning piiratud ratsionaalsusest, mille piiratus esineb peamiselt kolmes mõõtnes:

1. Laius – vähem võimalusi töötajate toetamisel.
2. Sügavus – üldiselt madalam haridustase. Siinkohal on oluline teha vahet tehniliselt rohkem arenenud ettevõtetel, kus töötajate haridustase on kõrgem, kui traditsionaalsemates valdkondades.
3. Mitmekesisuse puudumine – ettevõtja isikliku nägemuse domineerimine.

Munnich (2004) rõhutab, et VKEdel on väiksem võimekus kõikide seaduse poolt kehtestatud nõuetega hakkama saada piiratud ressursside tõttu (Munnich 2004) ning eriti sellistel juhtudel, kus ettevõtte juht on vastutav kõikide ettevõtte tegevuste ja sellega kaasnevate riskide eest (Dale *et al.* 2005, 10; Dixon *et al.* 2006, 14). Seetõttu on VKEd tavaliselt riskikartlikumad, kuna piiratud ressursside tõttu on nad vähem võimelised reageerima ootamatustele ning on probleemide tekkimisel haavatavamad (Dixon *et al.* 2006, 4; Lloyd 2006). Kui suurettevõtetel on võimalik adresseerida seaduse täitmisega seotud probleeme efektiivsemalt, võimalus jaotada oma ressursse kulutõhusamalt, siis VKEd otsivad suurema tõenäosusega soodsamaid võimalusi infrastruktuuri säilitamiseks ja haldamiseks (Oprysk 2016, 23).

Ülaltoodud põhjal nähtub, et regulatsiooninõuete täitmisega kaasnev koormus mõjutab VKEsid rohkem kui suurettevõtteid. Kuna GDPR toob kaasa mitmeid nõudeid, mille täitmine on sama vaatamata ettevõtte suurusest, on oluline analüüsida, arvestades VKE osakaalu majanduses, mis on GDPR täitmisega kaasnevad väljakutsed ja mõjud VKE rakenduskoormusele.

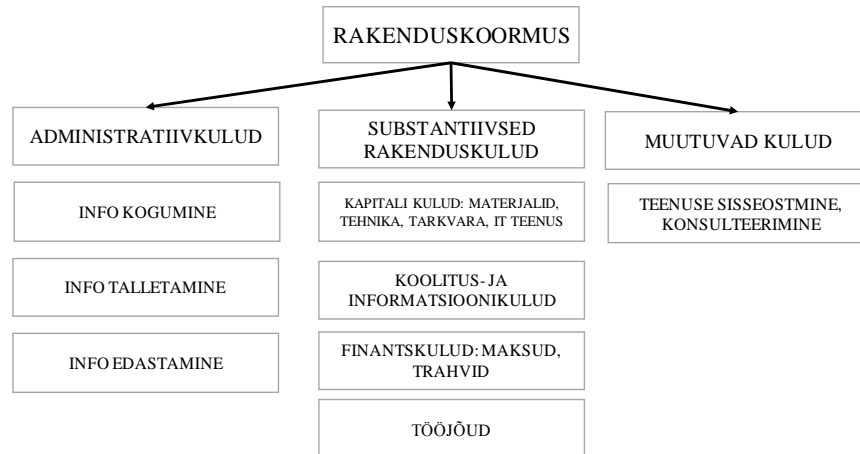
Weissbrot (2018) ja London Economics (2013, 60) toovad välja, et GDPR toob kaasa mitmeid piiranguid ettevõtetele, kes tegelevad turunduse, digitaalturunduse ning e-kaubandusega, kus reaalsed mõjud, eriti digitaalturundusele, on veel teadmata (Lindberg 2017). Tehnoloogia areng on toonud kaasa turunduses andmemahtude suurenemise, muutes andmete kasutamise üha olulisemaks, sest nendele toetudes on võimalik mõista, mis on brändi jaoks oluline (Tänase 2016) ning seeläbi jõuda vajaliku sihtgrupini (Lindberg 2017). Kuna turundusvaldkonnas tegutsevad ettevõtted ei töötle ainult personaliandmeid, vaid sageli ka koostööpartneritelt saadud andmeid, siis võivad nad samal ajal kanda nii vastutava töötleja kui volitatud töötleja rolli (Hon 2017, Lindberg 2017, 35). Vastutava töötleja – volitatud töötleja vahet on olulisematest GDPR sätestatud muudatustest. Alsenoy (2016) toob välja, et praegune ühiskondlik ja tehnoloogiline

areng võib muuta nende kontseptsioonide rakendamise praktikas keeruliseks, kuna alati ei ole võimalik täielikult eristada, kes on vastutav töötleja ja kes on volitatud töötleja, eriti olukorras, kus andmetöötlus nõuab mitmeid osapooli. Seetõttu ei pruugi andmetöötlusega seotud kohustusi reguleerida ainult GDPR, vaid sageli ka vastutava töötleja – volitatud töötleja vahelised lepingud, mille kasvav roll andmetöötlustoimingute reguleerimiseks suureneb (Hon 2017). Siinkohal võib eeldada, et turundusvaldkonnas tegutsev väikeettevõtte, olles nii vastutava töötleja kui volitatud töötleja rollis, võib kanda suuremat rakenduskoormust, kuna peab vastutavatele töötlejatele presenteerima organisatoorseid ja tehnilisi meetmeid, mis tõendavad nende vastavust GDPRle. Samas peavad olema võimalised koostöö alustamiseks ja/või jätkamiseks leppima vastutava töötleja poolt nõutud tingimustega (k. a. finantsvastutuse jagamine andmete lekkimise korral). Lisaks võivad nad silmitsi seista võimalike suurenevate õiguskuludega lepinguliste suhete reguleerimiseks. (Myers 2016, Weissbrot 2018) Sellest lähtuvalt võib GDPR mõjutada oluliselt vastutava töötleja – volitatud töötleja rollis olevaid väikeettevõtteid, kuna neil ei pruugi olla piisavat võimekust, ressursse ja teadmiseid GDPR adresseerimiseks, millel võib olla omakorda negatiivne mõju ettevõtte reputatsioonile (Kennedy 2018). Seetõttu võivad väikeettevõtted kogeda regulatsiooninõuete täitmisega kaasnevaid mõjusid sagedamini, kuna toimuvad muudatused kuludes, saadaolevates ressurssides, muutuvast toote või teenuse müügis (Hart *et al.* 2015, 136). Samas tuginedes tehingukulude teooriale, mis eeldab, et organisatsioonid kohanevad keskkonnaga kiiresti (Carroll, Teece 1999, 69), võib avaldada seadus ainult piiratud mõju, kuna kulud, mida tehakse, kantakse lõpptootesse / teenusesse, mille maksab kinni lõppklient (*Ibid.*, 132).

1.5 Analüüsiraamistik

Vastavust (ingl. *compliance*) defineeritakse kui protsessi, mille käigus viiakse ettevõtte vastavusse nõudmistega, mis tulenevad seadustest, regulatsioonidest, standarditest, lepingutest jt. (Elgammal *et al.* 2016). Eelkäsitletu on välja toonud, et GDPR võib kaasa tuua märkimisväärse koormuse kasvu nii ettevõtte vastavusse viimisel kui vastavuses püsimisel. Posner (1978, 22) rõhutab, et igasugune privaatsuse kaitsmine suurendab tehingukulud - kulud, mida tehakse privaatsust tagava tehnoloogia peale; ajakulu, mida kulutatakse regulatsiooniga tegelemiseks, õppimiseks ja informatsiooniga kursis olemiseks (Acquidity 2010, 19; Acquisti *et al.* 2016, 23); kulud tööjõu palkamiseks või teenuse sisseostmiseks, selleks et täita seadusega nõutud kohustusi (Steven Bradford 2004, 7-11).

Ettevõtted peavad regulatsioonide kohaldumisel vastama uutele reeglitele ning nende täitmine toob kaasa erinevaid kulusid (OECD 2014). Alloleva graafiku põhjal on kaardistatud teadusallikatele ja läbiviidud uuringutele toetudes peamised rakenduskoormusega kaasnevad kuluallikad.



Joonis 2. Regulatsiooni kohaldumisega kaasnevad kulud ettevõttele

Allikas: OECD (2014); Dale *et al.* (2005); Munnich (2004); Butter *at al.* (2009); Harvey (2014)

Eelnevalt väljatoodud uuringutulemuste põhjal nähtub, et GDPR võib avaldada negatiivset mõju ettevõtlusele, kuigi GDPR eesmärk on muuta andmekaitsekeskkond Euroopas ühtlasemaks ning tuua sisse läbipaistvust isikuandmete töötlemisel. Peamine probleem, mis GDPR puhul esineb on segadus mõistete ja kohustuste tõlgendamises. Ehk turul valitseb ettevõtete seas olukord, mille puhul ei saada GDPR nõuetest täpselt aru. Kui ettevõtete seas valitseb ebakindlus ning regulatsiooni funktsioon ei ole selgesti arusaadav, võib tekkida olukord, kus ettevõtted ülehindavad või alahindavad plaanitud kulutusi ning finantskohustuste riski andmete lekkimise korral. Haavatavamad on siinkohal VKEd, kes on lisaks piiratud ressurssidele ja ratsionaalsusele tundlikumad oportunistlikumale käitumisele²².

GDPRga muutub tegutsemiskeskond kõikidele ettevõtetele olenemata suurusest, pannes proovile nende tehnilise ekspertiisi kui ka valmisoleku ootamatustele vastu seista (Fitzgerald, Medno 2005, 123). Ettevõtted peavad demonstreerima enda organisatoorset ja tehnilist võimekust

²² Turul leiduvate teenusepakujate hulga tõttu võib olla raskendatud erapooletu ja usaldusväärse nõu saamine, mis aitaks ettevõtetel kulutõhusamalt GDPR nõudeid rakendada.

andmetöötusel²³ - tagama reageerimisvõimekuse isikuandmetega seotud rikkumise korral²⁴; muutama andmetöötlusprotsessid läbipaistvamaks²⁵; võimaldama andmesubjektidele ligipääsu nende andmetele; olema valmis andmete parandamiseks ja kustutamiseks ning jälgima, et andmetöötlus oleks eesmärgipärane ja andmete kogumine oleks viidud miinimumini²⁶.

Hindamaks GDPR mõju ulatust, võib öelda, et mitmedki nõuded võrreldes hetkel kehtivas Isikuandmete kaitse seaduses (edaspidi: IKS) sätestatuna jäävad samaks²⁷ ning sellest tulenevalt võib eeldada, et mõju rakenduskoormusele ei pruugi olla nii ulatusliku haardega. Kuid GDPR kitsendab isikuandmete töötlemise ulatust vastavalt GDPR artiklis 5 äratoodud põhimõtetele, mis sätestavad, kuidas antud protsess oleks vastavuses seadusega, läbipaistev ja eesmärgipärane. Andmesubjektide ja andmetöötlejate nägemust sellest, kuidas isikuandmeid töödeldakse, mõjutavad eesmärgipärane andmetöötlus, võimalikult väheste andmete kogumine, säilitustähtaegade määramine, andmekvaliteedi ja turvalisuse põhimõtte juurutamine.²⁸

GDPR kohaldumisega ei pruugi muutuda ainult administratiivsed toimingud, vaid ka tehnoloogilised ja operatiivsed meetmed kindlustamaks isikuandmete kaitse riskide vähendamiseks. Kuna GDPR määratleb spetsiifiliselt ära andmetöötamise läbiviimise alused, ei pruugi see mõjutada ainult ettevõtete administratiivseid toiminguid, vaid võib avaldada mõju selles, kas tehtavad otsused ja toimingud on korraldatud korrektselt ja seadusele vastavalt. Siinkohal tõstatubki regulatsiooni korrektse tõlgendamise olulisus, sest seadusest arusaamine on oluline samm regulatsiooni täitmise suunas, mis kujundab protsessi, kuidas ettevõtte sätestatud kohustusi täidavad (Lohmann 2012). Piirangute kehtestamine ning samal ajal vältida ettevõtte väärtuse kaotamist nõuab uusi investeeringuid andmeturve infrastruktuuri tugevdamiseks, vajadusel uute töökohtade loomist ning võib kaasa tuua organisatoorse muutuse (Engan 2017, 4).

Sellest johtuvalt tõuseb küsimus, kas väikeettevõtteid, kes GDPR põhjenduspunkti 3 alusel peaksid

²³ PWC (2017) uuringust selgus, et paljud ettevõtteid ei tea, kus kõik andmed asuvad, kuna informatsiooni juhtimine ja haldamine on algstaadiumis.

²⁴ Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, artikkel 33, lõige üks sätestab, et “*isikuandmetega seotud rikkumise korral teatab vastutav töötleja isikuandmetega seotud rikkumisest artikli 55 kohasele pädevale järelevalveasutusele põhjendamatult viivituse ja võimaluse korral 72 tunni jooksul pärast sellest teada saamist, välja arvatud juhul, kui rikkumine ei kujuta endast tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele. Kui järelevalveasutust teavitatakse hiljem kui 72 tunni jooksul, esitatakse teates selle kohta põhjendus*”.

²⁵ Digiajastu võidukäigule eelnevalt olid andmed rohkem struktureeritud ja füüsiline hoiustamine levinum (CD plaadid, disketid), kuid digitaalse ajastu arenemisega on hakanud tekkima üha enam struktureerimata andmeid (Bridge 2014), mistõttu võib andmetöötlusprotsesside läbipaistvuse suurendamine muutuda ettevõtetele oluliseks väljakutseks.

²⁶ Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, artikkel 5.

²⁷ Vt. lisa 2. Isikuandmete töötlustoimingute kaardistamine ja võrdlus GDPR ja IKS põhjal.

²⁸ Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, artikkel 5.

kandma väiksemaid kohustusi²⁹, seisavad silmitsi hoopis suurema regulatsiooninõuete täitmisest tuleneva koormusega just tehnilise ekspertiisi ja kapitali puudumise tõttu? Läbiviidud rahvusvahelistest uuringutest on selgunud, et enamik VKEd ei ole GDPR kohaldamise kuupäevaks ennast ette valmistanud, kuna arvavad, et see ei puuduta neid. Seetõttu on oluline analüüsida, kas regulatiivne ebakindlus ja informatsiooni asümmeetria tekitavad olukorra, kus regulatiivset riski alahinnatakse (Klinke, Renn 2002, 1079) uute väljakutsete adresseerimisel.

²⁹ Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, põhjenduspunkt 3 sätestab, et määruse kohaldamisel võetakse arvesse mikro-, väikeste ja keskmise suurusega ettevõtjate erivajadusi, kus on näiteks ette nähtud erand andmete kogumisele kuni 250 töötajaga ettevõtete poolt.

2. EMPIIRILINE ANALÜÜS

2.1 Andmekaitse areng Eestis

Isikuandmete kaitset Eestis hakkas eraldi seadusega reguleerima 1996. aastal vastu võetud IKS, mille väljatöötamisel „lähtuti nii 1981. aasta andmekaitse konventsioonist kui 1995. aastal jõustunud DPDst“. IKS uuendati 2003. aastal DPD ülevõtmisega Eesti õigusesse. (Rohtmets 2013) Uuesti reformiti IKS 2007. aastal IKS rakendamisel ilmnenud probleemide tõttu ning arendati edasi olemasolevat õiguslikku raamistikku (Nõmper, Tikk 2007 viidatud Sillaots 2014, 24). Kanger, Rohtmets (2013) toovad välja, et IKSil on mitmed kitsaskohad, puuduvate eriosa normide tõttu võivad tekkida rakendajal kohaldamisraskused ning õiguslikud alused võivad olla andmetöötajate jaoks abstraktse loomusega. Vaatamata IKS ilmnevatele kitsaskohtadele, on loodud IKStega Eestis tugev andmekaitsekeskkond võrdluses Forrester andmekaitsekaardil väljatoodud riikidega³⁰.

GDPR, mis kohaldub 25. mai 2018, jätab põhimõtted IKStega sarnaseks, kuid muudab isikuandmete töötlemise struktureeritumaks, loob andmetöötajatele kitsamad piirid ja toob kaasa rangemad reeglid. Andmetöötajad on kohustatud üle vaatama kasutatavad andmetöötlustehnikad, dokumenteerima GDPR artikkel 30 lõike 5 tingimustel isikuandmete töötlemise toimingud³¹, tugevdama andmeturvet ja jälgima, kas kogutud andmed järgivad GDPR artikkel 5 põhimõtteid. Samas kui võrrelda hetkel kehtivat IKS sätteid GDPR omadega, siis muudatused ei ole väga suured (Lisa 2 kaardistab ära hetkel kehtivad kohustused ja GDPRst lähtuvad kohustused ettevõtetele, mis aitab luua selgema pildi GDPRiga kaasnevate muudatuste ulatusest). Kuna GDPR puhul on tegemist otsekohalduva EL määrusega, siis selle rakendamiseks ei ole seda vajalik ratifitseerida

³⁰ Forrester 2016. aasta andmekaitsekaart, baseerudes 54 riigi andmekaitseprintsipiidele, näitab, et Eesti on üks tugevamatest andmekaitseraamistikuga riigidest.

³¹ Andmekaitse Inspeksioon toob välja, et „GDPR eesmärk justkui vähendada VKE ettevõtete (vähem kui 250 töötajat) halduskoormust, vabastades nad andmetöötlustoimingute registreerimisest, on loosunglik“.

koos liikmesriigi poolsete õigusaktidega, kuid liikmesriikidele on siiski jäetud GDPR rakendamisel võimalus konkreetsmaid sätteid kehtestada³². Sellest lähtuvalt on GDPR rakendamiseks Eestis antud välja kolm õigusakti: uus IKS, IKS rakendusseadus (eriseaduste muutmise) ja karistusseadustiku muutmise seadus (KarS muutmise seadus) (trahvid).

2.2 Uurimismeetodid

Käesoleva magistritöö puhul kasutatakse kvalitatiivset analüüsimeetodit, kuna kvalitatiivuuringud pakuvad sügavamat ja kontekstikesksemat lähenemist võrreldes kvantitatiivuuringuga (Recker 2013). Seeläbi on võimalik saada põhjalikum ülevaade sellest, mis väljakutseid ja koormisi toob GDPR rakendamine väikeettevõtetele. Kuna kvalitatiivuuringud keskenduvad kogemustele ja hoiakutele (Patton 2002), siis analüüsi läbiviimiseks kasutatakse intervjuusid. Intervjuude kasutamise eeliseks on saadud informatsiooni detailirikkus ja kontekstikesksemad andmed, mis küsimustike puhul ei pruugi ilmned (Recker 2013).

Intervjuude läbiviimiseks kasutati poolstruktureeritud küsimustikke, mis annavad suurema võimaluse diskussiooniks ning intervjuueeritavate seisukohtade väljatoomiseks (Recker 2013). Intervjuude eesmärk on saada põhjalikum ülevaade teoreetilises osas väljatoodud põhiprobleemidele, vastates uurimisküsimustele, millised on peamised väljakutsed GDPR nõuete täitmisel ning missugune mõju on GDPR nõuetel väikeettevõtete rakenduskoormusele. Probleemistik, mis kvalitatiivsete meetodite kasutamisega tõstatub, on andmete üldistamatus väikese valimi tõttu (Patton 2002), ressursimahukus ning tulemused võivad olla mõjutatud uurija subjektiivsetest vaatenurkadest. Samas võimaldab kvalitatiivne lähenemine analüüsida, miks ja kuidas mingi nähtus ilmneb. (Sadovnik 2007, 424).

Intervjuude läbiviimiseks ei kasutata juhuvalimit, vaid kvalitatiivsele uurimusele iseloomulikku ettekavatsetud valimit (eng: *purposive sampling*). See tähendab, et intervjuueeritavad on valitud

³² Üldmääruse art 6 lg 2 näeb ette, et liikmesriigid võivad säilitada või kehtestada konkreetsamad sätted, et kohandada üldmääruse sätete kohaldamist seoses isikuandmete töötlemisega art 6 lg 1 p-de c ja e täitmiseks, määrates üksikasjalikumalt kindlaks töötlemise konkreetsed nõuded ja teised meetmed, et tagada seaduslik ja õiglane töötlemine (Justiitsministeerium 2018).

kindla tunnuse järgi, mis võib uuringu jaoks genereerida kasulikke andmeid (Patton 2002). Antud magistritöö eesmärgiks ei ole tulemuste üldistatavus laiemale valimile, vaid pigem analüüsida turundus- ja reklaamisektori põhiselt GDPR mõju valitud ettevõtete rakenduskoormusele. Intervjueeritavate valik baseerus Inforegistri andmetel ning turundus- ja reklaamiagentuuride TOP listidel, mis on erinevate väljaannete (Äripäev, Ärileht) poolt avaldatud. Intervjuude läbiviimiseks võeti ühendust 20 reklaami- ja turundussektori ettevõttega, kus nõusolek intervjuuks saadi 6 ettevõtte esindajalt. Anonüümsed intervjuud viidi läbi intervjueeritavale sobival ajal ja kohas perioodil 11.04.2018-07.05.2018. Intervjuud baseerusid ettevalmistatud küsimustikul, mida muudeti vastavalt intervjueeritava ajapiirangust ja IKS ning GDPR baseeruvatest teadmistest lähtuvalt.

Lisaks formuleeritud küsimustele kasutati eeldatava mõju hindamiseks Likert tüüpi 5-palli skaalat (Likert 1932), mille puhul pidid intervjueeritavad lähtuvalt enda arvamuselt hindama GDPR nõuete mõju halduskoormusele ning ettevõtte kuludele etteantud äärmuste vahel. Mõju ulatust hinnati järgneva 5- palli süsteemi alusel: 1- mõju puudub, 2- väike mõju, 3- keskmine mõju, 4- suur mõju, 5- täielik mõju. Kuna halduskoormuse kvantitatiivne hindamine on ressursirohke, siis vastavalt OECD (2004, 7) soovitusel järgi piirdui halduskoormuse kvalitatiivse hindamisega. Sellest lähtuvalt otsustati, et Likert tüüpi skaala sobib antud töö ja ettevõtete valmiduse ulatuse tõttu.

Halduskoormuse hindamiseks kõige sagedamini kasutatavat standardiseeritud kulumudelit (ingl. *Standard Cost Model*, edaspidi SCM) (Charite et al. 2004) ei kasutatud, kuna GDPR infokohustuste loomuse ja valitud ettevõtete valmidus olla GDPR nõuetega vastavuses raskendab SCM kasutamist. SCM mudelit kasutatakse peamiselt *ex post* halduskoormuse mõõtmiseks, mis aitab mõõta reaalselt halduskoormust, mis toimub seaduse kohaldumise järgselt (Charite et al. 2004)³³.

Käesoleva magistritöö väike valim on antud töö üheks suuremaks piiranguks. Väikese valimi tõttu ei ole võimalik teha üldistusi kogu sektori põhjal, kus on väikeettevõtted nii volitatud töötleja kui vastutava töötleja rollis. Kuid piirangutele vaatamata on antud magistritöö olulise tähendusega, kuna GDPR mõjude uurimine Eesti kontekstis on algusjärgus ning vajalike uuringute valik piiratud. Seetõttu võib antud töö olla kasulikuks põhjaks edaspidistele uuringutele, et välja

³³ SCM mõõdab seaduse kohaldumise järgseid administratiivseid tagajärgi ehk aega ja raha, mida kulutatakse infokohustuste täitmiseks (Barazzoni et al. 2006).

selgitada, kuidas ettevõtted reageerivad regulatsioonile ning miks on valmisolek GDPR täitmiseks madal.

Ettevõte	Intervjueeritav	Töötajate arv	Tegevusvaldkond
Intervjueeritav A	Juhatuseliige	21	Reklaamiagentuurid
Intervjueeritav B	Tegevjuht	22	Reklaamiagentuurid
Intervjueeritav C	Juhatuseliige	9	Programmeerimine / Reklaamiagentuurid
Intervjueeritav D	Tegevjuht	20	Reklaamiagentuurid
Intervjueeritav E	Digisuuna juht	21	Reklaami vahendamine
Intervjueeritav F	Tegevjuht	21	Reklaami vahendamine

Tabel 2. Intervjueeritud ettevõtted

Allikas: Autor (2018); intervjueeritavatelt saadud info põhjal.

2.3 Analüüs GDPR nõuete mõju ja ulatuse hindamiseks

Töö analüüsi osa käsitleb läbiviidud intervjuudele tuginedes teoreetilises raamistikus väljatoodud põhiprintsiipide mõju ulatust ettevõtete halduskoormusele ja kuludele. Teoreetilises osas ilmneva uurimisprobleemistiku väljaselgitamiseks formuleeritud küsimused aitavad hinnata, mis on GDPR rakendamisele kaasnevad väljakutsed, kuidas need mõjutavad ettevõtete halduskoormust ning kas uurimisraamistikus püstitatud väited VKE ebaproportsionaalse halduskoormuse kohta GDPR rakendamisel peavad paika. Kuna iga kohustuse (Lisa 2) eraldi analüüsimine on väga ressursimahukas, siis keskendutakse GDPR analüüsimisel ja intervjuuküsimuste kategoriseerimiseks GDPR artiklis 5 väljatoodud põhiprintsiipidele, millega kaardistati VKE temaatikast lähtuvad küsimused, mis aitavad efektiivsemalt analüüsida rakenduskoormuse mõju väikeettevõtetele.

2.3.1 Eesmärgipärane isikuandmete töötlemine ning võimalikult väheste andmete kogumine

GDPR artikli 5 lõike 1 punktides a, b ja c määratletakse ära, et *“isikuandmete töötlemine peab olema seaduslik, õiglane ja andmesubjektile läbipaistev ning isikuandmeid tohib koguda ainult täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel. Isikuandmeid ei tohi töödelda viisil, mis on nende eesmärkidega vastuolus”*³⁴ ning koguda tohib neid andmeid, mida ainult eesmärgi täitmise seisukohalt vaja läheb. Sellele tuginedes uuriti intervjueeritavatel, kas ja kuidas on nende ettevõtetes isikuandmete töötlemine ära kaardistatud, kas nad järgivad eesmärgipärase töötlemise põhimõtet ning kuidas selle põhimõtte järgimine piirab isikuandmete töötlemist. Lisaks uuriti, kas ettevõtted järgivad võimalikult väheste andmete kogumise nõuet ja millised oleks ettevõttesisesed muutused võimalikult väheste andmete kogumiseks.

Intervjuude käigus selgus, et eesmärgipärasuse printsiipi küll järgitakse isikuandmete töötlusprotsessi läbiviimisel, kuid spetsiaalselt tööstustoimingute läbiviimise eelset kaardistamist ei ole toimunud, vaid tuginetakse olemasolevale majasisesele kompetentsile ja teadmistele. Lisaks toodi välja, et antud nõue on keeruliselt hoomatav ja tekitab mitmeid tõlgendamise küsimusi, eriti valdkonnas, mis puudutab personali palkamist (Intervjuu A, B, D 2018). Siinkohal üritatakse vältida näiteks intervjuude käigus tundlike küsimuste küsimist (Intervjuu D 2018). Lisaks võib antud nõue muuta suhtlemise mehaanilisemaks, võib takistada õige inimese palkamist, lepingute läbiviimist ning orgaanilist suhtlemist andmetöötlejate ja andmesubjektide vahel (Intervjuu A, B, D 2018).

Lisaks toodi välja, et antud nõue toob kaasa bürokraatia ja halduskoormuse suurenemise dokumenteerimiskohustuse tõttu (Intervjuu A, D, F 2018). Halduskoormuse suurenemist ei saa üksnes hinnata administratiivsete toimingute läbiviimisel, vaid tuleb arvestada ka antud printsiibi kohaldamisel kaasnevat ebakindlust otsuste tegemisel – ehk kas otsused, mida isikuandmete töötlemisel tehakse, on vastavuses seadusega ja andmed küsitud eesmärgipäraselt (Intervjuu A, D, E, F, 2018). Nähakse projektijuhtidel koormuse suurenemist. Intervjueeritavad B ja C tõid välja, et kui andmete kogumisel lähtutakse miinimumi printsiibist, siis see oluliselt ei piira

³⁴ Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, artikkel 5.

isikuandmetega seotud toiminguid, kuna võimalikult väheste andmete küsimine aitab ennetada eesmärkidest väljumist.

Kuna võimalikult väheste andmete kogumise põhimõte on sätestatud nii IKS § 6 (3) kui GDPR artikkel 5, siis uuriti intervjueeritavatelt, kas antud printsiipi on varasemalt järgitud ning kui ei, siis missuguseid muudatusi see nende hinnangul kaasa toob. Kui ettevõtte ei ole varasemalt antud põhimõtet järginud, siis see nõuab GDPR valguses ettevõtetelt andmetöötlustoimingute ülevaatamist, kindlustamaks, et toimuks võimalikult väheste andmete kogumine.

Intervjuude käigus selgus, et kõikides ettevõtetes on juba juurutatud võimalikult väheste andmete kogumine, kuna infokoormus on niigi suur. Intervjueeritavad C ja E tõid esile, et turunduses on juba praktikas välja kujunenud olukord, kus kampaaniate läbiviimiseks küsitakse võimalikult vähe andmeid. Samuti tõi intervjueeritav F välja, et andmebaase andmetega, mida kasutatakse kampaaniate läbiviimiseks, välditakse enda süsteemis hoidmisel juba pikemat aega.

Turunduskampaaniate korral, mis viiakse läbi klientide tellimuse alusel, küsitakse andmesubjektidelt minimaalselt andmeid kampaanias osalemise jaoks. Pärast kampaania lõppu on rutiiniks kujunenud kampaania läbiviimiseks saadud listide, mis sisaldavad näiteks andmesubjektide emaile, turunduskampaania tellijale tagastamine ning oma andmebaasist antud andmete kustutamine. See kindlustab, et andmebaasidesse ei jää andmeid, mis ei täida minimaalsuse nõuet (Intervjuu A, B, C, D, E 2018).

Võimalikult väheste andmete kogumisel peeti halduskoormust suureks, kui hinnati, et antud nõue tingib tööprotsesside ja andmebaasides olevate andmete ülevaatamist, et need järgiksid minimaalsuse nõuet. See aga mõjutab omakorda töökoormuse suurenemist (Intervjuu A, F 2018). Samas hinnati, et minimaalsuse nõue vajab täpsustamist (Intervjuu A ja B 2018), et sellega ei kaasneks hilisemalt eeldatust suurem halduskoormus ja kulutused. Intervjueeritavate B, C, D ja E hinnangul varieerus mõju nii halduskoormusele kui kuludele keskmisest (Intervjuu B ja D 2018) kuni minimaalse mõjuni (Intervjuu C ja E 2018). Väiksema halduskoormuse ja kulubaasi hindamise puhul peeti oluliseks, et kui varasemalt on juurutatud võimalikult väheste andmete kogumine, siis määruse kohaldumisel see märkimisväärset mõju ei avalda. Intervjueeritad C ja E tõid välja, et mõju halduskoormusele ja kuludele on väiksem, kui kitsaskohtade analüüsimisel on olemas majasisene kompetents.

2.3.2 Andmekvaliteedi tagamine ja isikuandmete piiratud säilitamine

GDPR artikli 5 lõike 1 punktis e sätestatakse ära, et *“isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse.”* Lisaks peavad olema GDPR artikli 5 lõike 1 punkti d kohaselt olema isikuandmed *ja vajaduse korral ajakohastatud ning, et ettevõtte võtaksid kõik mõistlikud meetmed, et töötlemise eesmärgi seisukohast ebaõiged isikuandmed kustutataks või parandataks viivitamata („õigsus“).*

Ettevõtetele tähendab see olukorda, kus isikuandmete kaardistamisel tuleb neile juurde määrata seadusega ettenähtud säilitamistähtaeg, mille möödudes tuleb vastutaval töötlejal isikuandmed kustutada, et neid ei oleks võimalik hilisemalt taastada. Seadusega ettenähtud säilitamisperioodi puudumise korral tuleb ettevõttel vastavatele isikuandmetele ise määrata, mis perioodi tagant need kustutatakse. Lisaks on andmesubjektidel õigus saada andmetöötlejalt informatsiooni enda andmete kohta ning andmetöötleja peab andmesubjektile edastama tema kohta kogutud informatsiooni lihtsas ja arusaadavas keeles. Sellest lähtuvalt sooviti teada, kuidas antud nõue mõjutab isikuandmetega seotud toiminguid – kas on viidud läbi kaardistus, mis annaks selgema ülevaate isikuandmete asukohtadest ning andmesubjekti kohta kogutud informatsioonist. Kuidas on läbi viidud isikuandmete säilitamisega seonduvad protseduurid ning seeläbi lasti hinnata kohustuste mõju ulatust ettevõtte halduskoormusele ja kuludele.

Intervjuude käigus selgus, et säilitamistähtajad on määratud ainult seadusega ettenähtud dokumentidele ning põhjalikumat isikuandmete säilitamise protseduuri ei ole paika pandud. Kuna isikuandmete seadusliku ja õiglase töötlemise tagamiseks tuleb piirduda andmete säilitamisel rangelt minimaalsega, siis intervjueeritavad hindasid, et nõude täitmiseks tuleb ära määrata kõikide isikuandmete tüüpide hoiustamistähtajad. Nii intervjueeritavad A, B, D ja F hindasid selle nõude mõju halduskoormusele keskmisest suuremaks, kuna antud sätte puhul peeti kõige koormavamaks süsteemi, töötlustoimingute registri loomist ning selle regulaarset haldamist. D ja F tõid välja, et selleks on vaja luua täpsemad protseduurid ning kaardistada andmed, mis nõuab omakorda mitme töötaja panust, tuues kaasa kulude suurenemise. Kui suurettevõtetel on osakonnad, kes töötlustoimingute registri väljatöötamisega tegelevad, siis väikeettevõtete puhul nõuab see lisafunktsiooni loomist või tööülesannete mahu suurendamist olemasolevatele töötajatele (Intervjuu F 2018).

Kui intervjueritav B hindas antud nõudega tekkivaid kulusid keskmiseks, siis intervjueritavad C ja E ei näinud, et andmete kaardistamise ja säilitamisega seonduvate protseduuride paikapanemine tooks kaasa kulutusi ning suurendaks halduskoormust. Peamiselt mõjutas intervjueritavate hinnangut see, et ettevõttes on isikuandmetest olemas hea ülevaade ning intervjueritava E puhul andmed varasemalt kaardistatud. Samas märkisid intervjueritav A, D ja F, et halduskoormus tõuseb antud kohustuse rakendamisel, kuna protseduuri läbiviimine võib minna ajamahukaks – vajalik luua süsteem, kuidas määrata säilitustähtajad (mis ei tulene seadusest) ning määrata kindlaks, kuidas viia läbi andmete kustutamine. Intervjueritavad tõid välja, et antud nõude puhul võib suurendada halduskoormust, kuna register, kus on ära määratletud andmete säilitamise tähtajad, vajab aeg-ajalt kontrollimist ja uuendamist (A, D ja F 2018). Intervjuu käigus toodi välja, et kustutamistähtaegade määramine, mis ei ole seaduse poolt paika pandud, vajab spetsialistipoolset täpsustamist, kuna hetkel on selgusetu, mille alusel määrata seaduse poolt mittedefiniitud isikuandmetele kustutamise tähtaeg (Intervjuu A, B, D 2018).

Intervjuudest selgus, et ühtne süsteem hetkel puudub, mis võimaldaks halduskoormust suurendamata vastata andmesubjekti päringutele ning tagada, et ettevõttes hoiustatud isikuandmetes ei esineks vigu (Intervjuu A, B, D 2018), kuid samas nähakse, et valmisolek andmesubjekti päringutele vastamiseks on kõikides ettevõtetes hea, sest üldpildis on ülevaade isikuandmete asukohtadest olemas. Protseuuride väljatöötamist lihtsustaks, kui oleks olemas valdkonnaspetsiifiline juhend ning praktiliste näidete olemasolu, mis aitab vähendada ettevõtete halduskoormust ning tagada andmekvaliteedi põhimõtte tõhusama juurutamise (Intervjuu A ja B 2018). Intervjueritavad A ja B tõid välja, et kui üldiselt on andmekvaliteedi nõue arusaadav, võib selle rakendamine kujuneda reaalsuses oodatust keerulisemaks (Intervjuu A ja B, 2018) ning sellega kaasnev halduskoormus võib kujuneda suureks (Intervjuu A, D ja F 2018). Teised intervjueritavad hindasid mõju halduskoormusele keskmiseks (Intervjuu B 2018) ja väikseks (Intervjuu C, E 2018). Intervjueritav C tõi välja, et nende ettevõttes juurutatakse uut süsteemi, mis annab võimaluse integreerida isikuandmetega seonduv haldus loodava süsteemi juurde, vähendades sellega nii kulusid kui hilisemat halduskoormust.

2.3.3 Isikuandmete turvalisuse tagamine

GDPR artikli 5 lõike 1 punktis f sätestatakse isikuandmete töötlemise viis, mis *“tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid („usaldusväärsus ja konfidentsiaalsus“).* “

Kuna antud nõude alusel peavad ettevõtetel olema tagatud organisatoorsed, füüsilised ja infotehnoloogilised turvameetmed riskide minimeerimiseks, siis sooviti teada, kas ettevõttes on määratud vastutav töötaja ning kuidas mõjutab vastutava töötaja määramine kulutusi tööjõule? Lisaks sooviti teada, kuidas on isikuandmete töötlemine dokumenteeritud ning kuidas antud protsess ettevõttes toimub. Kas tõhustatakse meetmeid, mis aitavad tagada andmete asjakohase turvalisuse? Lisaks uuriti, kas plaanitakse kulutusi turvameetmete tugevdamiseks.

Intervjuude käigus selgus, et füüsilised turvameetmed isikuandmete kaitsmiseks on ettevõtetes hästi tagatud. Koostöö oma IT-partneritega tagab pidevate uuenduste olemasolu riskide minimeerimiseks (Intervjuu A, B, C, D 2018), kogu e-mailidega seonduv tegevus on arhiveeritud (Intervjuu A 2018) ning sisse viidud kaheastmeline tuvastussüsteem lisakaitse tagamiseks (Intervjuu C 2018). Kõik intervjuueeritavad tõid välja, et isikuandmetele on ligipääs ainult volitatud isikutel nagu juhatuse liikmetel ja raamatupidajal. GDPR eest vastutav isik on määratud hetkel kahes ettevõttes ning GDPR eest vastutava isiku roll ühel juhul juba ametijuhendisse sisse kirjutatud (Intervjuu B 2018). Teistel ettevõtetel ei ole veel isikuandmete kaitse eest vastutavat isikut määratud, kuid plaan on seda teha (Intervjuu A, C, E 2018). Intervjuueeritav E tõi välja, et ettevõttes spetsiaalselt vastutavat töötajat või andmekaitse spetsialisti määratud ei ole, kuid antud rolli võtab peamiselt ettevõttes olev jurist. Intervjuueeritav A ütles, et hetkel vastutab iga osakond oma valdkonna eest, et oleks tagatud võimalikult kuluefektiivne töökorraldus, kuid tulevikus on plaan määrata kindel vastutav isik ettevõtte seest. Intervjuudest selgus, et vastutava isiku rolli võtab kas tegevjuht, raamatupidaja või finantsjuht.

Kaks ettevõtet hindasid, et vastutava isiku määramine mõjutab kulutusi tööjõule, sest vastavalt kohustuse ulatusest selgub, kas GDPR täitmisel tuleb täita uus ametikoht või määrata kohustused olemasolevale töötajale (Intervjuu A ja B 2018). Intervjuueeritavad C, D ja E ei näinud tööjõukulutuste kasvu, sest läbiviidavate muudatuste ulatus ei ole väga suur. Intervjuueeritav D tõi välja, et kuna peamised kohustused võtavad üle tegevjuht ja raamatupidaja, siis kulutused tööjõule

ei suurene. Lisaks nägid kõik intervjueeritud andmetööstustoimingute dokumenteerimise vajalikkust läbipaistvuse tagamiseks ja riskide minimeerimiseks. Vaatamata sellele, et kõikides ettevõtetes on isikuandmed hästi turvatud, on isikuandmete turvameetmete tagamisel veel siiski arenguruumi. Nimelt peab intervjueeritav A oluliseks ühtlustada andmete asukoha struktuuri isikuandmetest parema ülevaate saamiseks.

Teoreetilisele osale tuginedes tuuakse välja, et inimfaktorit nähakse privaatsustoimingute läbiviimisel nõrga lülina ning seetõttu on teadlikkuse tõstmisel oluline roll isikuandmete kaitse tagamisel (Hooson 2015). Sellest lähtuvalt uuriti intervjueeritavatel, kas ja kui palju pööratakse nende ettevõttes tähelepanu teadlikkuse tõstmisele ja koolitusvajadusele. Kuna töötajate kompetentsi peetakse piisavalt heaks, siis turul pakutavate koolituste lisandväärtusesse väga ei usuta, sest koolitustelt saadav info on pigem teoreetiline ning praktiline pool puudub (Intervjuu A, B, C, D, E 2018). Intervjueeritavad B, C, D ja E tõid välja, et nende kollektiivist on paar inimest koolitusel käinud ning intervjueeritav D hinnangul kogu kollektiivi koolitustele saata ei ole. Kõige põhjalikuma koolitusprogrammi on läbinud iseõppimise kaudu Intervjueeritav F, kes oli turundusvaldkonnale keskendunud GDPR koolitusel esinejaks. Toodi välja, et antud protsessi läbitegemine andis põhjaliku ettevalmistuse ning ülevaate, kui suur halduskoormus väikeettevõtetele tegelikult langeb. Kuna turul pakutavate koolituste osas on intervjueeritavad üldiselt kriitiliselt meelestatud, siis nähakse pigem kompetentsi suurendamiseks vajadust palgata tööle isik, keda on võimalik kasutada nii GDPR nõuete rakendamisel kui ka üldiste tööülesannete täitmisel (Intervjuu B 2018). Ettevõtted hindasid, et teadlikkuse tõstmine ettevõtete sees toimub ning teadvustatakse igal tasandil, mida tohib teha ja mida mitte (Intervjuu A, B, C, D, E ja F 2018). Välja on kujunenud suhtumine, et kui isikuandmete töötlemisel tekib takistus, siis edasiste juhtiste saamiseks pöörduakse riskide minimeerimiseks vastutava isiku või juhi poole (Intervjuu B 2018). Hinnatakse, et organisatoorne teadlikkus isikuandmetest on piisavalt hea, mida tugevdab omakorda privaatsust eelistav kollektiiv (Intervjuu C 2018). Kõige suurema riskina toodi välja töötajatepoolsete andmete kogumist reeglite väliselt (Intervjuu E 2018).

Kolmel juhul hinnati nõudega kaasneva koormuse ulatust suureks (Intervjuu A, B, F 2018) ning kolme vastanu arvates madalaks (C, D, E 2018). Intervjueeritav C leiab, et kuna olemasolev süsteem suudab tagada isikuandmete piisava turvalisuse, on ka sellega kaasnev halduskoormus madal ning kulude suurenemist nähakse pigem ilmnevate kohustuste väljaselgitamiseks (Intervjuu C 2018).

2.3.4 GDPR rakendamise kitsaskohad ja mõjud

Käesolevas peatükis tuginetakse intervjuude käigus esile kerkinud GDPR nõuete täitmise kitsaskohtade ning ettevõtete rakenduskoormust mõjutavate aspektide kaardistamisele.

GDPR sätete **tõlgendamine** ja **regulatiivne ebakindlus** oli üks suuremaid kitsaskohti, mis intervjuude käigus ilmnis. Intervjueeritavad tõid välja, et GDPR pika juriidilise teksti tõlgendamine praktilisteks juhisteks vajab lisakonsulteerimist valdkonna spetsialistiga. Näidisrakenduste puudumine ja GDPR keerukuse tõttu võib kujuneda problemaatiliseks vajalike tegevuste kaardistamine ehk mis on kõige olulisemad sammud, mida ettevõtetel on vaja ära teha. Sellest lähtuvalt toodi välja, et keeruline on adekvaatselt hinnata, kui töömahukaks GDPR nõuete rakendamine kokkuvõttes kujuneb. Kuna GDPR poolt sätestatud nõudeid saab tõlgendada mitmeti, siis on suureks raskuseks teema selgeks tegemine ja aru saamine, kuidas oleks kõige mõistlikum GDPR nõuete täitmisele läheneda. Kitsaskohana toodi välja, et kui majasisene kompetents GDPRiga tegelemiseks puudub, siis võib välise abi või koolitustelt saadud info põhjal minna GDPR nõuete täitmine väikeettevõttele kulukaks. Selle põhjenduseks viidati, et koolitustelt saadud soovitused nõuetele vastamiseks on viidud maksimumini ning puudub praktiline juhend ettevõtetele, mis oleks vajalik minimaalselt ära teha. Siinkohal toovad ettevõtted välja, et oleks vaja praktilisemaid koolitusi, mitte regulatsiooni kirjeldamist. Selgema arusaamise puudumine GDPRist võib näidata seda, et Andmekaitseinspeksiooni roll GDPR kaasnevate kohustuste teadvustamisel ja ettevõtete teavitamisel võib olla puudulik ning meedia poolt üles külvatud paanika võib tekitada rohkem segadust.

Organisatoorne valmisolek 25. maiks 2018. aastaks oli samuti üheks suuremaks kitsaskohaks, mis intervjuude käigus ilmnis. Valmisolek, kuid mitte täielik, oli kahel ettevõttel neljast. Intervjueeritavad tõid välja, et GDPR juures mängib olulist rolli protsesside hindamine ning andmemahutudega kursis olemine, mis võib kaasa tuua halduskoormuse kasvu, kui IKS valguses ei ole nende kohustustele varasemalt nii kriitiliselt tähelepanu pööratud. Üks kõige koormavamatest ja keerulisematest tegevustest on süsteemi juurutamine ning mõistmine, mida tähendab GDPR mõistes vastav olemine. Näidisrakenduste puudumine ja GDPR tõlgendamisega tekkivad raskused (ehk peab oskama seadust lugeda) võivad tekitada olukorra, kus algselt tunduv madal kulu võib muutuda suureks kuluks. Ettevõtted tõid välja, et kui võtta suund täitmaks 100%

ulatuses nõutud kohustusi, võib see kaasa tuua märkimisväärse koormuse kasvu. Seetõttu hinnati, et antud teemale on vajalik läheneda mõistlikult ning vältida meedia poolt õhutatud paanikat. Meedia poolt tekitatud paanika võib viia olukorrani, kus ettevõtted kulutavad antud nõuete täitmiseks rohkem, kui reaalselt vastavuse saavutamiseks vajalik. Samas toodi välja positiivse aspektina, et GDPR annab võimaluse väikeettevõtetele vahetada oma vanad andmesüsteemid uute vastu välja ning kõik, mis võib tunduda alguses kuluna, võib muutuda hiljem tuluks (Intervjuu C 2018). Organisatoorne valmisolek regulatsiooninõuete täitmiseks esitab ettevõtetele siiski väljakutse. Seetõttu nähakse neljas ettevõttes kuuest, et vastutava isiku määramine, kes aitab kaasa vastavuse saavutamise protsessile, on oluline määrata. Kuna ühe ettevõtte puhul, kes kuulub rahvusvahelisse kontserni on vastavusse läbiviimist tegemas sisseostetud ettevõtte, siis nende puhul on vastavuse saavutamine teistest intervjuueeritavatest sujuvam. Kõik tegevused, mis on vajalikud läbiviimiseks, tehakse järjekindlalt ja kava kohaselt. Samas võimaldas see antud intervjuueeritaval välja tuua selle, et kui mahukas töö reaalselt väikeettevõtteid ees ootab, kellel ei ole valdkonnaspetsialisti ettevõtte seest võtta. Seetõttu hinnati ka antud ettevõtte poolt GDPR kaasnevat halduskoormust suureks.

Andmete kaardistamine ja protsesside **dokumenteerimine** oli samuti probleemkohtadest, mis intervjuude käigus esile tõusis. Kuigi ettevõtted tõid üldise seisukohana välja, et ülevaade andmete asukohtadest on enamjaolt olemas, siis paikapandud kaardistust ja süsteemi ei ole veel välja töötatud. Lisaks toodi esile, et täpselt ei saada aru, kuidas peaks toimuma töötlusprotsesside dokumenteerimine ning millises ulatuses on see väikeettevõtetele kohaldatav. Kuna GDPR mõistes on töötlustoimingute registri loomiseks andmete kaardistamine ja töötlusprotsessist selge ülevaade saamine olulise tähtsusega, siis nähakse siin vajadust väikeettevõtteid toetava selge raamistiku järgi. Selge ülevaade saamine mitte ainult ei võimalda ettevõtetele kergemini saavutada vastavust, vaid lisaks võib see anda tugevama võimekuse reageerida ootamatustele, mis võivad kaasneda andmesubjektide päringutega ning andmete lekkimisele reageerimisel. Ülevaade saamine võimaldab ettevõtetele paremini kontrollida olemasolevate andmete vastavust regulatsioonile ehk kas kogutavad andmed järgivad eesmärgipärasuse printsiipi.

GDPR mõjusid ettevõtete **kuludele** hindasid **madalaks** neli ettevõtet kuuest (üks ettevõtte hindas 5- palli skaalal keskmiseks ja 1 suureks). Nähakse, et GDPR toob kaasa pigem **halduskoormuse suurenemise**. Halduskoormuse hindasid pigem 5- palli skaalal madalaks kaks ettevõtet ning keskmiseks ja sellest suuremaks 4 ettevõtet. Kuna antud valdkonna ettevõtted on seotud ka suurettevõtetega, kellele nad on volitatud töötajad, siis toodi välja, et kindlasti muutuvad lepingud

detailsemaks, mis võivad tuua kaasa lisakohustusi ning panna väikeettevõtte suurema surve ja halduskoormuse alla. Omakorda võivad suurened ka õiguskulud. Koostöö käigus tekkiv infokohustustega kaasnev **topeltkoormus** võib mõjutada negatiivselt väikeettevõtte haldussuutlikkust, mistõttu võivad jääda teatud tööd vastu võtmata. Sellel võib olla aga omakorda negatiivne mõju ettevõtte arengule. Lisaks nähakse kahe ettevõtte põhjal kulude suurenemist ka tarkvarale, mis võimaldaks muuta andmetöötlusprotsessid läbipaistvamaks ning tugevdada vajadusel andmeturvet. Hinnati, et mida suurem on andmebaaside maht, seda keerukamaks ja aeganõudvamaks muutuvad andmetöötlusprotsesside läbiviimine. Ettevõttes, kus on GDPR vastavuse tagamine paika pandud suurkorporatsiooni poolt, kelle alla nad kuuluvad, toodi välja, et vaatamata sellele, et nad üritavad hoida minimalistlikku joont GDPR nõuete täitmisel, on siiski ettevõtetele pandud kohustused probleeme tekitavad. Antud intervjueeritava poolt hinnati ajalist kulu kõige suuremaks, mis nõuete täitmiseks kulub.

Intervjuude käigus uuriti ettevõtetelt, kui suur on nende hinnangul GDPR poolt määratud trahvide mõju GDPR nõuete täitmisel ning kas trahvidega hirmutamise kiirendab ettevõtte GDPR nõuetega vastavusse viimist. Neli ettevõtet kuuest tõid välja, et GDPR poolt kehtestatud trahvid avaldavad vähe mõju GDPR nõuete täitmisel ning üks ettevõtte hindas mõju suureks. Intervjueeritavad tõid välja, et praktikas on trahvide mõju suur, kuid arvatavasti ei hakata ettevõtteid kohe trahvima. Ametvõimudel on väga raske kontrollida, kas ettevõtteid täidavad 100% GDPR nõudeid või mitte. Antud protsess oleks väga ajamahukas mõlemale poolele. Pigem on olulisemaks aspektiks GDPR nõuete täitmisel mainekahju tekkimise ohu viimine miinimumini. Seetõttu on vajalik protsessid läbi viia rahuliku järjekindlusega, mitte kiirusega.

Ühe teemana, mis paari intervjuu puhul esile kerkis oli **vastutuse määratlemine**, eriti mis reguleerib vastutava töötaja-volitatud töötaja vahekorda. Vaatamata sellele, et GDPR määratleb ära vastutava töötaja ja volitatud töötaja täpsed kohustused, toodi siinkohal siiski välja, et antud vahekorra määratlemine võib osutada praktikas keerulisemaks. Sama kitsaskohta kinnitab ka teoreetilises osas väljatoodud uuring (Alsenoy 2016).

3. DISKUSSIOON

Teoreetilisele osale tuginedes võib välja tuua, et regulatsioon mõjutab väikeettevõtteid suurettevõtetest erinevalt (Lundstrom, Stevenson 2005, 196; Kitching 2006, 17; Baldwin 2004; Wegrich 2009; Bradford 2004; Dale *et al.* 2005; Kirkpatrick, Parker 2012, 51). Kuigi antud analüüsi läbiviimisel keskenduti üksnes väikeettevõtetele, võib eeldada, et GDPR kohaldamise järgne mõju ei erine teoorias väljatoodud seisukohtadest. Eriti seetõttu, et nõuded ja protsessid, mida peavad ettevõtted GDPR nõuete täitmiseks rakendama on nii väikeettevõtetele kui suurettevõtetele ilma suurte eranditeta samad. GDPR puhul mängib väikeettevõtetele langeva rakenduskoormuse osas pigem rolli IKS nõuete eelnev täitmine, ettevõtete valmisolek ja hoiak GDPR järgimiseks ning ka üldine sektori reguleerituse tase. Kuna antud sektori ettevõtted peavad pidevalt arvestama töös ettetulevate seaduste poolt sätestatud piirangutega (autoriõiguse seadus, reklaamiseadus jt), siis tuginedes teoreetilises osas väljatoodud seisukohtadele, võib eeldada, et tugeva reguleeritusega sektoris on GDPR üleminek kergem (Hornung 2012, 68, Irish SME Association 2018). Kuid teisest küljest põhineb see väide ainult teoreetilises osas väljatoodud seisukohtadele ning antud väite tõestamiseks oleks oluline sarnase uuringu läbiviimine olukorras, kus ettevõtted on täielikult vastavuses. Rahvusvahelistele uuringutele toetudes on välja toodud, et ettevõtetel on raskuseid GDPR nõuete täitmisega ning teadlikkuse tase GDPRiga kaasnevatest kohustustest vaatamata üldisest reguleerituse tasemest on EL ja Eesti ettevõtete seas madal (Ciriani, 51; Flett, Wilson 2017, 7; PWC 2017; Pyykko 2012; London Economics 2013; Mayers 2017; Jonas 2018; Justiitsministeerium 2018). Vaatamata sellele, et Eestis on loodud IKS põhjal tugev andmekaitseraamistik ning muutused IKS GDPR üle minnes ei ole esmapilgul suured (Vt. lisa 2. Isikuandmete töötlustoimingute kaardistamine ja võrdlus GDPR ja IKS põhjal), mis peaksid ettevõtetele tagama juba etteulatavalt andmetöötlusprotsessides vajaliku organisatoorse ja tehnilise kindluse, selgus siiski intervjuude käigus, et teadlikkus GDPR nõuetest ja sellega kaasnevatest kohustustest on madal.

Intervjuusid läbi viies selgus, et ülevaade olemasolevatest andmetötlusega seonduvatest protseduuridest on heal tasemel, kuigi põhjalikult on GDPR nõuete täitmise lõppfaasi jõudnud ainult 2 ettevõtet. Intervjueeritavad tunnistavad, et isikuandmete töötlemise protsessi on suuresti mõjutanud koostöö suuretevõtetega, sest lähtutakse andmetötlusprotsesside läbiviimisel paljugi suurkliendi poolt kehtestatud nõuetest. Antud aspekt võib toetada teoreetilises raamistikus Williamson (1979, 240) väljatoodud väidet, et ettevõtte varaspetsiifilisuse tõttu ei toimu ulatuslikku tehingukulude suurenemist, kuna eelnevalt loodud süsteem võimaldab ettevõtetel kuluefektiivsemalt nõudeid täita. Kuid samas GDPR poolt tekitatud ebakindlus, eelkõige nõuetest arusaamisel ja kohustuste rakendamisel, panid intervjueeritavaid pigem hindama, et kehtestatud nõuded võivad kasvatada andmetötlusprotsesside läbiviimisel nende halduskoormust. Süsteemi juurutamine ja igapäevane haldamine tõstavad ettevõtete halduskoormust ning GDPRst saadavat kasu, praktiliste näidete puudumise tõttu, on raske hinnata. Tuginedes biheavioristliku teooria seisukohtadele, kus inimesed peavad tegema otsuseid olukordades, mille puhul on reaalsed tulemused teadmata (Lunn 2012, 433), võib välja tuua, et praegune olukord on prevaleeriv ka nende intervjueeritavate hinnangul – regulatsiooninõuetega esinev selgusetus ning nende rakendamisega ning vastavuse taseme määramisega kaasnev ebakindlus (sealhulgas valdkonnaspetsiifilise juhendi puudumine andmetötlusprotsessi väljakujundamiseks) paneb ettevõtted olukorda, mille puhul on reaalne halduskoormuse ja kulude hindamine raskendatud.

Teoreetilises raamistikus väljatoodud seisukohtadele tuginedes võib väita, et regulatsiooni korrektse tõlgendamise olulisus kujundab GDPR nõuete täitmise protsessi (Lohmann 2012). Williamson (1979) käsitluse järgi on ebakindlus üks tehingukulusid mõjutavatest teguritest ning kui ettevõtetel ei ole võimalik aru saada GDPR rakendamise praktilistest aspektidest ning saadaoleva informatsiooni rohkuse tõttu on raskendatud olulise info väljasünteesimine, võib see viia tegevuse edasilükkamiseni (Simon 1959). Antud väidet võib aidata ilmetada üldine ettevõtete madal GDPR vastavuse tase, vaatamata sellele, et aega nõuetega vastavusse viimisel on olnud alates 2016. aastast. Sama selgus ka läbiviidud intervjuude põhjal, et kui ettevõtetel ei ole võimalik aru saada GDPR rakendamise praktilistest aspektidest, võivad ettevõtete kulud kujuneda regulatsiooninõuete täitmisel oodatust suuremaks või nõuete täitmine võib lükkuda hilisemale perioodile, kui on välja kujunenud hoomatavamad näited GDPR nõuete täitmisest. GDPR mitmeti mõistmine on praegusel ajahetkel mõistetav, kuna praktilised näited selle rakendamisprobleemide osas puuduvad. Seetõttu peavad ettevõtted tuginema kas olemasolevale ettevõttesisesele

kompetentsile või pöörduma abi saamiseks väljaspool organisatsiooni oleva eksperdi poole (üheks võimaluseks koolituse käigus saadud teadmiste rakendamine). Seetõttu oleks oluline, et regulatsiooninõuete täitmine toetuks parimatele praktikatele ja võrdlevatele uuringutele, mis võimaldab ettevõtetel vähendada nõuete rakendamisega kaasnevat kulusid ning tegeleda efektiivsemalt kitsaskohtadega, mida regulatsiooni täitmine võib kaasa tuua.

Niikaua, kui ei osata hinnata GDPRga kaasnevat kasu, nähakse seda kui ebameeldiva kohustusena ning ettevõtlust takistava tegurina. Antud aspekti juures tuuakse teoreetilises raamistikus välja, et madal teadlikkus võib olla seotud regulatsiooniga kaasneva koormuse ala- või ülehindamisega. Sellest lähtuvalt paluti intervjueeritavatel hinnata GDPR nõuete arusaadavust ja GDPR mõju halduskoormusele ja kuludele, et näha kas ilmneb seos suurenenud halduskoormuse ja madala teadlikkuse vahel. Kuigi analüüsi tulemusi ei saa üldistada, ilmnes läbiviidud intervjuude põhjal, et mida parem oli teadlikkus GDPR osas, seda väiksemaks hinnati mõju kuludele. Kuid samas ei puugi see tähendada, et nii *ex ante* kui *ex post* kulusid ei ilmne, kuna hetkel on kõik intervjueeritavad, peale kahe, GDPR nõuete rakendamise algfaasis.

Kuid GDPR kaasnevad väljakutsed ja kulud ei piirdu ainult regulatsiooninõuete tõlkimisega praktilistest juhenditeks. Sellega võrdväärseks nähakse andmetöötlusprotseduuride paikapanemist ettevõtte siseselt (tegevused, mis hõlmavad töötlustoimingute registri loomist). Antud tegevused on ühed olulisemad, mida GDPR sätestab, kuna määratleb ära andmete kogumise eesmärgipärasuse, nende kustutamise ja võimalikult väheste andmete kogumise. Sellest lähtuvalt on ettevõtetel võimalik aru saada, kus andmed asuvad ja mis andmed on ettevõttes saadaval. See aga võimaldab efektiivsemalt demonstreerida GDPR vastavust ja suurendada läbipaistvust. Intervjuude käigus ilmnes, et ettevõtetes on viidud juba varasemalt sisse võimalikult väheste andmete kogumine halduskoormuse vähendamiseks. See võimaldab ettevõtetel vähendada neile langeva vastutuse ulatust, mis aga omakorda aitab vähendada trahvide saamise võimalust ja negatiivset mõju ettevõtte mainele. Intervjuude käigus tuli esile, et ettevõtte maine, positiivse kuvandi tagamine ning hea kliendisuhete hoidmine mõjutasid olulisemalt GDPRga sätestatud kohustuste täitmise ulatust, kui GDPR poolt sätestatud trahvimäärad. Seega ei saa teoreetilises raamistikus väljatoodud väite põhjal kinnitada, et trahvid motiveerivad täitma regulatsioonist tulenevaid nõudeid (vt. Fenn, Veljanovski 1988, 1055; Pham *et al.* 2017, 70). Siinkohal võib välja tuua, et ettevõtete käitumist võib mõjutada trahvide reaalne rakendamine, kuid trahvidega hirmu külvamine, vähemalt antud ettevõtete põhjal, kiiremat GDPR nõuete vastavuse saavutamist ei taga.

Vaatamata sellele, et akadeemilistes uuringutes on nähtud privaatsusregulatsioonide mõju ettevõtetele pigem takistuse ja koormana, on GDPR rakendamist toetavad allikad välja toonud selle positiivse mõju konkurentsivõimele. Intervjuude käigus ilmnis, et üldjuhul ei nähta GDPR puhul konkurentsieelist, sest antud valdkonnas peab niikuinii lähtuma andmetöötlustel suurklientide ja seadusega kehtestatud nõuetest. Pigem hinnatakse, et liiga piiravad ja abstraktsed reeglid isikuandmete töötlemisel mõjutavad negatiivselt tegevusi, mis puudutavad värbamisprotsessi. Kaudselt võivad seeläbi kulud suurened, sest põhiprintsiipidele tuginedes võivad abstraktselt sõnastatud nõuded tekitada segadust ja seeläbi võivad jääda küsimata küsimused, seadusega vastuollu minemist vältides, mis aitaksid hinnata paremini inimese sobivust kollektiivi. Sama probleemistik tuleb esile ka Acquisity (2010), Posner (1978, 1981) ja Stigler (1980) seisukohtadest, kus tuuakse välja, et turult eemaldatud andmed loovad turul ebaefektiivust ning võivad raskendada õige inimese palkamist.

Teoreetilises raamistikus väljatoodud seisukohtadele tuginedes inimeste piiratud ratsionaalsuse osas (Williamson 1979; 2005; 1999; Simon 1985) võib välja tuua, et vajaliku informatsiooni kättesaadavus ja valitsusepoolne infotugi on regulatsiooninõuete täitmisel oluline, eriti seaduste, regulatsioonide osas, mis on niivõrd olulise kaalu ja mõjuga. Peamine probleemistik, mis intervjuude käigus ilmnis, oli see, kas GDPR nõudeid täidetakse korrektselt. Madala GDPR teadvustamise taseme juures võib mängida rolli selle liiga keerulised kohustused ning valitsusepoole vähene teavitustöö ja tugi GDPR kohustuste prioriseerimisel. Seetõttu on vaja selgemat väljatoodud raamistikku GDPR nõuete täitmisel, mis aitaks väikeettevõtetel GDPR täitmisel halduskoormusega kaasnevad kulud viia miinimumini, sest halduskulude loomuse tõttu (need kulud on sageli fikseeritud) on väikeettevõtted erinevatele muutustele haavatavamad (Kitching 2006, 18; Kljucnikov, Sobeková 2016).

Käesolevat magistritööd kirjutades ilmnis, et inimeste hoiakutel on seaduste järgimisel ja täitmisel üha olulisem roll. Seetõttu, uue seaduse loomisel, regulatsiooni kohaldamisel, tuleks üha enam arvesse võtta käitumise, õppimisega seonduvaid aspekte ning arvestama, et reguleeritavate käitumine ei pruugi järgida kindlat lineaarset rada.

KOKKUVÕTE

Eesti andmekaitsemaastikku hakkab kujundama alates 25. maist 2018. aastast kohalduv isikuandmete kaitse üldmäärus ehk GDPR, mis laiendab andmesubjektide õiguste ulatust andmesubjektide andmete töötlemisel. Oluliseks muudatuseks, mille GDPR kaasa toob on andmetöötlustoimingute läbipaistvuse suurendamine ehk andmeid tohib töödelda ainult täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel. Kuna GDPR toob ilma väga suurte eranditeta sarnased muudatused nii suurettevõtetele kui väikeettevõtetele, siis otsustati, väikeettevõtete osakaalu ja olulist rolli majanduses arvesse võttes analüüsida GDPR nõuete täitmisega kaasnevaid väljakutseid ja mõjusid väikeettevõtete rakenduskoormusele. Erinevate allikate põhjal on selgunud, et regulatsioonidega kaasnev koormus mõjutab väikeettevõtteid suurettevõtetest enam. Teema kitsendamiseks valiti reklaami- ja turundussektoris tegutsevad väikeettevõtted, kuna andmete kasutamise roll turunduses on muutunud üha kesksmaks digitaalajastu võidukäiguga ning reklaami- ja turundussektoris tegutsevad väikeettevõtted võivad olla samal ajal nii vastutava töötleja kui volitatud töötleja rollis, tuues kaasa neile vastutuste ja kohustuste osakaalu suurenemise.

Käesoleva töö eesmärgi saavutamiseks on teoreetilisele raamistikule toetudes analüüsida GDPR rakendamisega kaasnevaid väljakutseid ja regulatsiooninõuete mõju reklaami- ja turundussektoris tegutsevate väikeettevõtete halduskoormusele ja kuludele. Eesmärgi saavutamiseks püstitati järgnevad uurimisküsimused:

1. Millised on väikeettevõtete peamised väljakutsed GDPR nõuete rakendamisel?
2. Millised GDPR nõuded mõjutavad ettevõtete rakenduskoormust enim?

Töö eesmärgi saavutamiseks ja uurimisküsimustele vastamiseks andis autor töö teoreetilises osas esmalt ülevaate regulatsiooni olemusest, võimaldades lahti seletada regulatsiooni rolli ühiskonnas, selle mõju majanduskeskkonna kujundamisel ja spetsiifilisemalt väike ja keskmise suurusega ettevõtete toimimisele. Lisaks anti ülevaade andmekaitsemaastiku väljakujunemisest kuni GDPR

väljatöötamiseni ning analüüsiti, mis on olnud senised GDPR rakendamisega tekkinud väljakutsed ja eelmõjud Euroopa Liidu ettevõtetele.

Mõjude hindamise, regulatsioonide poolt püstitatud väljakutsete ning regulatsiooninõuete täitmise raamistamiseks tugineti käesolevas magistritöös tehingukulude (Williamson 1979) ja biheivioristlikule (Simon 1955, 1959) teooriale. Antud teoreetilised seisukohad valiti eelkõige seetõttu, et need aitaksid selgemini mõista piiranguid, mis võivad esile kerkida regulatsiooninõuete täitmisel. Mõjude hindamisel ja kitsaskohtade väljaselgitamisel peeti oluliseks aspekti, et ostuste tegemisel ei pruugi inimestel olla kogu saadaolevat informatsiooni, mis avaldab mõju regulatsiooninõuete täitmisele ja sellega kaasnevatele kuludele. Töö autori hinnangul leiti, et biheivioristliku teooria kasutamine aitab magistritöös paremini selgitada vahetuid mõjusid, eriti valdkondades, mis on seotud teatud tüüpi riskiga ning aidata analüüsida, miks muutused toimusid ja miks ei toimunud. Tehingukulude teooria aitab hinnata aspekte, mis võiksid suurendada või vähendada regulatsiooninõuete täitmisega kaasnevaid tehingukulusid.

Empiirilise osa struktureerimiseks loodi teoreetilises osas analüüsiraamistik, mis tugines teoreetilistele seisukohtadele, rahvusvaheliste uuringute tulemustele GDPR probleemkohtade ja kuluartiklite kaardistamisel. Andmekogumismeetoditena kasutati poolstruktureeritud intervjuusid. Analüüsi tegemiseks viidi läbi 6 reklaami- ja turundussektoris tegutseva väikeettevõttega poolstruktureeritud anonüümsed intervjuud.

Analüüsi tulemustest selgus, et andmetöötlusega seonduvad protseduurid on kõikides ettevõtetes heal tasemel, kuid GDPR nõuetele ei ole täielikku vastavust tagatud. Peamiste väljakutsetena kerkisid esile regulatsiooni tõlgendamine, läbipaistvuse tagamine, organisatoorse valmisoleku saavutamine, eesmärgipärane andmetöötlus ning tööstustoimingute registri väljatöötamine. Regulatsiooni tõlgendamise probleemistik on tõusnud esile nii akadeemilises kirjanduses kui intervjuude käigus. Euroopa tasandil läbiviidud uuringutes on selgunud, et GDPR avaldab negatiivset mõju ettevõtlusele ning põhiprobleemidena on tõstatunud regulatsiooni liiga keerulised kohustused ja ebaselgus GDPR nõuete täitmisel. Regulatsiooni keerulised kohustused, sellega kaasnev ebakindlus ning nõuete abstraktsusest tingitud tõlgendamisprobleemid tulid välja ka läbiviidud intervjuude käigus. Analüüs kinnitab, et ettevõtetel on täieliku vastavuse saavutamiseks läbida veel pikk protsess. Ettevõtted tõid välja, et puudub selge raamistik, rakendusjuhendite puudumine kohustuste prioriseerimiseks ning vastavuse saavutamiseks. Samas nähakse esimeste ülesannetena andmete kaardistamist ning andmetöötlusstrateegiate ülevaatamist ning täiendamist.

Analüüsi tulemustes selgus veel, et kuigi antud väikeettevõtted suurt mõju kulude suurenemisele ei näinud, siis hinnati, et GDPR nõuete täitmine toob kaasa halduskoormuse suurenemise. Kuna näidisrakendused puuduvad, siis ei osatud hinnata kui töömahukaks GDPR nõuete täitmine võib praktikas kujuneda. Infokohustuste täitmisega kaasnev halduskoormus, vastutava töötaja volitatud töötaja vahekorra määramine, volitatud töötaja vastutuse suurenemine võib panna väiksemad ettevõtted suurema surve alla ning vähendada nende konkurentsivõimet, sest võimekus info- ja lepinguliste kohustustega tegelemiseks on piiratud.

Käesoleva magistr töö järel dustena võib välja tuua, et madal teadlikkus GDPR nõuetest on suureks kitsaskohaks GDPR rakendamisel. See võib ilmestada olukorda, et riigipoolne tõhus ja intensiivne koostöö ning suhtlus ärikeskkonnaga on puudulik. Samuti saab kitsaskohana tõstatada põhjaliku mõjuanalüüsi puudumist, mis aitaks ettevõtetel selgemini mõista GDPR kaasnevaid väljakutseid. Kuna regulatsiooni eesmärk on muuta majandusagendi käitumist, siis tuleks ka regulatsiooni kujundamisel arvesse võtta piiranguid, mis võivad selle kohaldamisega tekkida. Piirangute mõistmise oluliseks alustalaks on mõjude eelanalüüs, probleemkohtade teadvustamine ja teadlikkuse suurendamine läbi tiheda koostöö, mis võimaldaks ka ettevõtetel arvesse võtta tulenevaid piiranguid ja selle mõju ettevõtte kulubaasile.

SUMMARY

THE CHALLENGES AND IMPACTS ARISING FROM THE GENERAL DATA PROTECTION REGULATION ON THE COMPLIANCE BURDEN OF SMALL ENTERPRISES: THE CASE STUDY OF ESTONIAN MARKETING AND ADVERTISING COMPANIES

Grete Õigemeel

From 25 May 2018, the Estonian Data Protection Landscape will be shaped by the implementation of the General Data Protection Regulation (GDPR), which extends the scope of the rights of data subjects in the processing of their data. An important change brought about by GDPR is an increase in the transparency of data processing operations. As GDPR brings about similar changes without major exceptions for both large and small enterprises, a decision was taken to analyse the challenges and impacts arising from GDPR on the compliance burden for small enterprises, taking into account the share and importance of small enterprises in the economy. Different sources have made clear that the burden arising from regulations affects small enterprises more than large enterprises. In order to specify the topic, small enterprises operating in the advertising and marketing sector were selected, as the role of data usage in marketing has become increasingly central due to the boom in the digital age.

In order to achieve the objective of this thesis, it is necessary, based on the theoretical framework, to analyse the challenges of the implementation of GDPR and the impact of regulative requirements on the administrative burden and costs of small enterprises operating in the advertising and marketing sector.

The following research questions were raised to achieve this objective:

1. What are the main challenges for small enterprises in implementing GDPR requirements?
2. Which GDPR requirements have the largest impact on the compliance burden of companies?

In order to answer the research questions, an overview of the nature of the regulation is given in the theoretical section, allowing the explanation of the role of this regulation in society, in particular its impact on the shaping of the economic environment. In addition, an overview of the development of the data protection landscape up to the development of GDPR is given, and the current challenges and impacts of the GDPR implementation for the EU companies are analysed.

In this master's thesis, the framing of impact assessment, regulatory challenges, and compliance with regulatory requirements are based on transaction cost (Williamson 1979) and behavioural (Simon 1955, 1959) theory. These theoretical views have been chosen primarily because they help to better understand the constraints that may arise in complying with regulatory requirements. In assessing impacts and identifying bottlenecks, it is important to consider that, in making decisions, individuals may not have all the available information that has an impact on compliance with regulatory requirements and the costs involved. The author has found that the use of behavioural theory in this master's thesis helps to better explain the immediate effects, especially in areas that are related to a certain type of risk, and this helps to analyse the reasons behind why the changes have or have not taken place. The theory of transaction costs helps to assess the aspects that could increase or decrease the transaction costs associated with compliance with the regulatory requirements.

Semi-structured interviews were used as data collection methods. In order to carry out the analysis, semi-structured anonymous interviews were conducted with six small enterprises operating in the advertising and marketing sector.

The analysis results indicate that data processing practices are at a good level in all companies, but full compliance with GDPR requirements is not ensured. The main challenges are interpretation of the regulation, ensuring transparency, achieving organisational preparedness, targeted data processing and developing a register of processing operations. The problem of the interpretation of regulation arose both in the academic literature and during the interviews. Studies carried out

on the European level have revealed that GDPR has a negative impact on business, and overly complex commitments as well as uncertainty in meeting GDPR requirements are raised as main issues. The complex commitments of the regulation, the related uncertainty and the problems of interpretation arising from the abstract nature of the requirements were also mentioned during the interviews conducted. The analysis confirms that companies have a long way to go in order to ensure full compliance. Companies have indicated that there is no clear framework, but there is a lack of implementation guidelines for prioritising commitments and ensuring compliance.

The results of the analysis reveal that although these small enterprises do not see any significant increase in costs, it is estimated that compliance with the GDPR requirements would lead to an increase in the administrative burden. The administrative burden of complying with information obligations, determination of the ratio between data controller and data processor, and the increase of the responsibility of data processor may put smaller enterprises under increased pressure and reduce their competitiveness, as their ability to deal with informative and contractual obligations is limited.

The conclusion of this master's thesis is that low awareness of GDPR requirements is a major bottleneck in the implementation of GDPR. This may characterise a situation where effective and intensive cooperation and communication with the business environment are inadequate. Another bottleneck may be the absence of impact analysis, which would help companies to better understand the challenges of GDPR. Since the purpose of the regulation is to change the behaviour economic agents, the regulation should also take into account the constraints that may arise from its implementation. An essential basis for understanding the constraints is the preliminary impact analysis, bringing out the problematic issues and awareness raising through close cooperation, which would allow companies to take into account the constraints and their impact on the company's cost base.

KASUTATUD ALLIKAD

Raamatud

- Allers, M. A. (1994). *Administrative and compliance costs of taxation and public transfers in the Netherlands*. Groningen: Wolters - Noordhoff.
- Arnold, J., Nicoletti, G., Scarpetta, S. (2008). *Product Market Policies, Allocative Efficiency and Productivity: A Cross-Country Analysis*. Paris: OECD.
- Barazzoni, F., Cerri, F., Hepburn, G. (2006) *Cutting red tape cutting red tape: National strategies for administrative simplification*. Paris: OECD Publishing.
- Charite, D., Lauritsen, S., Ahlin, J., Stene, O., Barnes, M. (2004). *International Standard Cost Model Manual. Measuring and reducing administrative burdens for businesses*. International SCM Network To reduce administrative burdens. Paris: OECD Publishing.
- Dale, T., Haraldsen, G., Hedlin, D., Jones, J. (2005) *Developing Methods for Assessing Perceived Response Burden*. Statistics Sweden, Statistics Norway, Office for National Statistics.
- Hodgson, G. M. (2010) *Limits of Transaction Costs Analysis*. Elgar Companion to Transaction Cost Economics. Cheltenham-Northampton: Edward Elgar Publishing.
- Lundstrom, A., Stevenson, L. A. (2005) *Entrepreneurship Policy: Theory and Practice*. International Studies in Entrepreneurship, Vol. 9. United States: Springer
- Mitchell, J. (2006) *The Use (and Misuse) of Surveys Research in Policy Analysis*. Handbook of Public Policy Analysis. Routledge.
- OECD (2014) *Regulatory Compliance Cost Assessment Guidance*. Paris: OECD Publishing.
- Patton, M. Q. (2002) *Qualitative Research & Evaluation Methods: Integrating Theory and Practice*. United States: Sage Publications.
- Recker, J. (2012) *Scientific research in information systems: a beginner's guide*. New York: Springer Science & Business Media.
- Simon, H. A. (1997) *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations*. Fourth ed. New York: The Free Press.
- Williamson, O. E. (1996) *The Mechanisms of Governance*. Oxford: Oxford University Press.

Artiklid

- Acquisti, A., Grossklags, J. (2007). "What Can Behavioral Economics Teach Us about Privacy?". *Digital Privacy: Theory, Technologies, and Practices*. Auerbach Publications, 363-379
- Acquisti, A., Romanosky, S. (2009). "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives." *Berkeley Technology Law Journal*, Vol. 24, No. 3, 1-44
- Acquisti, A., Taylor, C. R., Wagman, L. (2016). "The Economics of Privacy." *Journal of Economic Literature*, Vol. 52, No. 2, 1-64.
- Alsenoy, B. (2016). "Regulating Data Protection: The Allocation of Responsibility and Risk Among Actors Involved in Personal Data Processing." *Ku Leuven Faculty of Law*.
- Andrade, N. (2010) "Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights." *Privacy and Identity Management for Life*. Vol. 352. (Eds.) S., Fischer-Hübner, P. Duquenoy, M. Hansen. Berlin, 90-107.
- Anspal, S., Järve, J., Kallaste, E. (2009) "Isikuandmete kaitse regulatsiooni majanduslike mõjude analüüs." *Eesti Rakendusuringute Keskus*. Tallinn: Justiitsministeerium, 1-55.
- Arendsen, R., van Engers, T. M., Velde, R. (2006). "An Empirical Study on Business-to-Government Data Exchange Strategies to Reduce the Administrative Costs for Businesses." *IFIP International Federation for Information Processing*, Vol 226. Boston: Springer, 311-323.
- Arendsen, R., van Engers, T.M. (2004) "Reduction of the Administrative Burden: An e-Government Perspective." *Lecture Notes in Computer Science. Electronic Government*. Vol. 3183. Netherlands: Springer, 200.
- Aubert, B. A., Rivard, S. (2015). "Information Technology Outsourcing: Issues and Future Analyses." *Routledge*, 400-407.
- Bageri, V., Katsoulacos, Y., Makri, G. (2011) "Regulatory Burden, Competition and Growth." Report funded by Bank of Greece. Athens: Bank of Greece, 1-28.
- Baldwin, R. (2004) "Better Regulation: Is it Better for Business?" *Federation of Small Business*. London, 1-37.
- Bauer, M., Erixon, F., Krol, M., Lee-Makiyama, H., Verschelde, B. (2013) "The Economic Importance of Getting Data Protection Right: Protecting Privacy.", *Transmitting Data, Moving Commerce Brussels*. Brussels: ECIPE, 1-26.
- Bennett, J., Coggan, A., Whitten, S. M. (2010) "Influences of transaction costs in environmental policy." *Ecological Economics*, Vol. 69(9), 1777-1784.

- Bergerson, J. (2016) "Data Collection: Embracing New Technology and Abandoning Old Paradigms." ILTA Publications.
- Bianco, M., Bripi, F. (2010) "Administrative burdens on business activities: regional disparities." *Giornale degli Economisti e Annali di Economia*. Vol. 69, No. 2, 37-79.
- Brouthers, K. (2013) "Institutional, cultural and transaction cost influences on entry mode choice and performance." *Journal of International Business Studies*. Vol. 44 (1), 1-13.
- Bridge, P. (2014) "EU puts pressure on businesses to erase data." *Network Security*. No. 8, 5-8.
- Boylaud, O. Nicoletti, G., Scarpetta, S. (2000) "Summary Indicators of Product Market Regulation with an Extension to Employment Protection Legislation". *OECD Working Paper*. No. 226, 1-86.
- Borgesius, Z. F. (2013) "Consent to Behavioural Targeting in European Law - What are the Policy Implications of Insights from Behavioural Economics?" *Amsterdam Law School Research Paper*. No. 2013-43, 1-59.
- Bradford, C. S. (2015) "Does Size Matter? An Economic Analysis of Small Business Exemptions from Regulation" (2004). *Journal of Small and Emerging Business Law Publications*. No. 8, 1-37.
- Butter, F., de Graaf, M., Nijssen, A. (2009) "The Transaction Costs Perspective on Costs and Benefits of Government Regulation: Extending the Standard Cost Model." *Tinbergen Institute Discussion Paper*. No. 09-013/3, 1-32.
- Butter, F. A. G., Hudson J. (2009) "Standardization and Compliance Costs: Relevant Developments at EU Level." *Business Regulation and Public Policy*. Vol 20. New York: Springer, 1-15.
- Böröcz, I. (2016) "Risk to the Right to the Protection of Personal Data." *European Data Protection Law Review*. Vol. 2, No. 4, 467 – 480.
- Carroll, G. R., Teece, D. J. (1999) "Firms, markets, and hierarchies: introduction and overview." *Firms, Markets, and Hierarchies: The Transaction Cost Economics Perspectiv*. London: Oxford University Press, 3–13.
- Carter, R., Hodgson, G. M. (2006) "The impact of empirical tests of transaction cost economics on the debate on the nature of the firm." *Strategic Management Journal*, Vol. 27(5), 461-476.
- Ciriani, S. (2015) "The Economic Impact of the European Reform of Data Protection." *Communications & Strategies*. Mo.97, 41-58.
- Civita, P., Downs, A., MacDonald, A. (2011) "Contribution of Behavioural Economics to Regulatory and Policy Impact Analysis." *Policy Research Initiative*. Canada: Government of Canada, 1-9.

- Chittenden, F., Kauser, S., Panikkos, P. (2002) "Regulatory burdens of small business: A literature review." *SBS Research Directorate*, 1-79.
- Christensen, L., Colciago, A., Etro, F., Rafert G. (2013). "The impact of the data protection regulation in the eu". *Intertic Policy Paper*, 1-51.
- Christensen, J., Kent, P. (2011) "The decision to internally generate or outsource risk management activities." *23rd Asian-Pacific conference on international accounting issues*, 16.10. 2011, Beijing, China. Bond Business School Publications, 1-35.
- Coglianesi, C. (2012) "Measuring Regulatory Performance evaluating the impact of regulation and regulatory policy." *OECD Expert Paper*. No. 1, 1-59.
- Cooper, D. (2010) "The Lisbon Treaty and data protection: What's next for Europe's privacy rules?" *Covington & Burling LLP Privacy & Data Protection Advisory*, 01.12.2009, 18
- Croxson, B. (2000) "Organisational Costs in the New NHS: An introduction to the transaction costs and internal costs of delivering health care." *Monographs*. London: Office of Health Economics, 1-63.
- Dixon, L., Gates, S. M., Kapur, K., Seabury, S. A., Talley, E. (2006) "The Impact of Regulation and Litigation on Small Business and Entrepreneurship." *Kauffman-RAND Center for the Study of Small Business and Regulation Working Paper*. Rand Publications, 17-68.
- Ducos, G., Dupraz, P. (2007) "The Asset Specificity Issue in the Private Provision of Environmental Services: Evidence from Agri-Environmental Contracts". *Documento de trabajo*. Rennes Cedex: Institut National de la recherche Agronomique, 1-31.
- Elder, T., Yarrison, F. W., Long, B. L. (2015) An Empirical Investigation of Privacy: The Impact of Multiple Levels of Trust. *Paper prepared for the American Sociological Association Annual Meeting*, 2009. Ohio: Kent State University, 1-24.
- Elgammal, A., Turetken, O., van den Heuvel, W., Papazoglou, M. (2016) "Formalizing and applying compliance patterns for business process compliance." *Software and Systems Modeling*, No. 15(1), 119-146.
- European Commission (2009) "Implementation of Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises." *Commission staff working document*, European Commission, 1-5.
- Fenn, P., Veljanovski C. G. (1988) "A Positive Economic Theory of Regulatory Enforcement." *The Economic Journal*, Vol. 98, No. 393, 1055-1070.
- Fitzgerald, G., Mendo, A. (2005) "Theoretical approaches to study SMEs ebusiness progression." *Journal of computing and information technology*, No. 13 (2), 123 -136.
- Flett, E. L., Wilson, J. F. (2017) "EU General Data Protection Regulation." *Kirkland & Ellis International LLP*, 1-8.

- Hampton, P. (2005) "Reducing administrative burdens: effective inspection and enforcement." *Report by Philip Hampton for the UK Government Treasury*, London: HM Treasury, 1-140.
- Hart, M., Kitching, J., Wilson, N. (2015) "Burden or benefit? Regulation as a dynamic influence on small business performance." *International Small Business Journal*, Vol. 33(2), 130-147.
- Harvey, H., Herd, P., Moynihan, D. (2014) "Administrative Burden: Learning, Psychological, and Compliance Costs in Citizen-State Interactions." *Oxford University Press on behalf of the Journal of Public Administration Research and Theory*, Vol. 25, 43-69
- Heinrich, C. J. (2015) "The Bite of Administrative Burden: A Theoretical and Empirical Investigation." *Journal of Public Administration Research and Theory*, Vol. 26, No. 3, 403-420
- Herath, T., Rao, H. R. (2009) "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness." *Decision Support Systems*, Vol. 47, No. 2, 154-165.
- Hornung, G. (2012) "A General Data Protection Regulation for Europe? Light and Shade in The Commission's Draft Of 25 January 2012", *SCRIPTed*, Vol. 9, No. 1, 64-81
- Hopkins, T. D. (1998) "Regulatory Costs in Profile." *Policy Sciences*, Vol. 31, No. 4, 301-320
- Kahneman, D. (2002) "Maps of Bounded Rationality: A Perspective on Intuitive Judgment and Choice." *Nobel Prize Lecture*, 449-489.
- Kirkpatrick, C., Parker, D. (2012) "Measuring Regulatory Performance. The Economic Impact of Regulatory Policy: Literature review of quantitative evidence." *OECD. Expert Paper*, No. 3, 1-48
- Kitching, J. (2006). A burden on business? Reviewing the evidence base on regulation and small-business performance. *Environment and planning C: government and policy*, Vol. 24, No. 6, 799-814.
- Klinke, A., Renn, O. (2002) "A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies." *Risk Analysis*, Vol. 22, No. 6, 1071-1094
- Kljucnikov, A., Sobeková, M. M. (2016) "Impact of Gender in the Perception of Administrative Burdens among Young Entrepreneurs - Evidence from Slovakia." *Journal of Competitiveness*, Vol. 8, No. 2, 17-30.
- Kox, H. (2005) "Intra-EU differences in regulation-caused administrative burden for companies." *CPB Netherlands Bureau for Economic Policy Analysis*, No. 136, 1-19
- Koops, B. J. (2014) "The trouble with European data protection law." *International Data Privacy Law*, Vol. 4, No. 4, 250-261.

- Kooreman, P., Prast, H. (2007) "What does behavioral economics mean for policy? Challenges to savings and health policies in the Netherlands." *De Economist*, Vol. 158, No. 2, 101-122.
- Likert, R. (1932) "A technique for the measurement of attitudes." *Archives of Psychology*, Vol. 22, No. 140. (1932), 1-55.
- Lohmann, N. (2012) "Compliance by design for artifact-centric business processes." *Information Systems*, Vol. 38, No. 4, 606-618
- Hofheinz, P., Mandel M. (2014) "Bridging the Data Gap: How Digital Innovation Can Drive Growth and Create Jobs", *Lisbon Council-Progressive Policy Institute policy brief*, No. 15/2014, 1-16.
- Manne, G. A. (2016) "Data Regulation and Its Effect on Business Models & Corporate Organization in The New Economy." *Innovation & the New Economy Research Program White Paper*, 1-23.
- Martin, K. (2013) "Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online." *First Monday*, Vol. 18, No. 12.
- Meyer, K. (2001) "Institutions, Transaction Costs, and Entry Mode Choice in Eastern Europe." *Journal of International Business Studies*, Vol. 32, No. 2, 357-367.
- Munnich, M. (2004) The regulatory burden and administrative compliance costs for companies. *The Confederation of Swedish Enterprise*, 1-21.
- Nijssen, A. (2000) "Information obligations in the Dutch constitutional state." *EIM Business and Policy Research*, No. B200001, 1-149.
- Nooteboom, B. (1993) "Firm size effects on transaction costs." *Small Business Economics*, Vol. 5, No. 4, 283-295.
- Oprysk, L. (2016) "The Forthcoming General Data Protection Regulation in the EU: Higher Compliance Costs Might Slow Down Small and Medium-Sized Enterprises." *Juridica International*, Vol. 24, 23-31.
- Pham, H-C., Brennan, L., Richardson, J. (2017) "Review of behavioural theories in security compliance and research challenges." *Proceedings of the Informing Science and Information Technology Education Conference*, Vietnam. Santa Rosa. Informing Science Institute, 65-76.
- Pollitt, C. (2008) "Timeship – Navigating the Past. Time, Policy, Management: Governing with the Past." *International Review of Administrative Sciences*, Vol 74, no. 4, 703 – 706.
- Posner, R.A. (1978) "Economic theory of privacy." *Aei Journal on Government and Society*, Vol. 2. 19-26.
- Pyykko, E. (2012) "Data Protection at the Cost of Economic Growth?" *European Credit Research Institute ECRI Commentary*, No. 1, 1-7.

- Rantaša, K. Š. (2004) "Recruitment of employees: Administrative burdens on Slovenian SMEs in comparison with Europe." *Journal of East European Management Studies*. Vol. 9, No. 3, 278-312.
- Rubinstein, I. S. (2013) "Big Data: The End of Privacy or a New Beginning?" *International Data Privacy Law*, Vol. 3, No. 2, 74–87.
- Rohtmets, E., Kanger, L. (2013) Eesti andmekaitse Euroopa Kohtu praktika peeglis. *Riigikogu toimetised 2013/28*.
- Rohtmets, E. (2013) Isikuandmete kaitse küsimused Euroopa Kohtu eelotsustes. *Kohtupraktika analüüs*. Tartu: Riigikohus.
- Sadovnik, A. R. (2007). Qualitative research and public policy. *Handbook of public policy analysis: Theory, politics, and methods*, Vol. 125, 417-427.
- Shekhovtsev, N. (2018) "One More Thought on the Issue of Tax Compliance Cost Burden for Large Enterprises in New Zealand: An Application of Rational Choice Model to Tax Compliance Administration." *University of Canterbury*, 1-29.
- Sholtz, P. (2001) "Transaction Costs and the Social Costs of Online Privacy." *First Monday*, Vol. 6, No. 5.
- Simon, H. A. (1985) "Human Nature in Politics: The Dialogue of Psychology with Political Science." *American Political Science Review*, Vol. 79, 293–304.
- Simon, H. A. (1955) "A Behavioral Model of Rational Choice." *Quarterly Journal of Economics*. Vol. 69. 99-118.
- Simon, H. (1959) "Theories of Decision-Making in Economics and Behavioral Science." *The American Economic Review*, Vol. 49, No. 3, 253-283.
- Solove, D. J., Schwartz, P. M. (2013) "Reconciling Personal Information in the United States and European Union." *GW Law Faculty Publications*, Vol. 102, No. 877.
- Solove, D. J. (2002) "Identity theft, privacy, and the architecture of vulnerability." *Hastings Law Journal*, Vol. 54, 1227-1275.
- Stiglitz, J. (2009) "Government Failure vs. Market Failure: Principles of Regulation." In E. Balleisen & D. Moss (Eds.), *Government and Markets: Toward a New Theory of Regulation*. *Cambridge University Press*, 13-51.
- Stigler, G. J. (1971) "Theory of Economic Regulation." *The Bell Journal of Economics and Management Science*. Vol. 2, No. 1, 3-21.
- Tisdell, C. A. (2004) "Transaction Costs and Bounded Rationality-Implications for Public Administration and Economic Policy." *University of Queensland, School of Economics*, 1-24.
- Tzanou, M. (2013) "Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right." *International Data Privacy Law*, Vol. 3, No. 2, 88-99.

- Tănase, G. C. (2016) "The Future of Marketing in 2016: Trends in the New Digital Age." *Romanian Distribution Committee Magazine, Romanian Distribution Committee*, Vol. 7, No. 2, 20-25.
- Voermans, W. (2015) "The Achilles Heel of European Integration." *The Theory and Practice of Legislation*, Vol. 2, No. 3, 343-359.
- Wegrich, K. (2009) "The administrative burden reduction policy boom in Europe: comparing mechanisms of policy diffusion." *London School of Economics and Political Science*, No. 52, 1-24.
- Williamson, O. E. (1985) "The economic institutions of capitalism." *New York: The Free Press*, 385-387.
- Williamson, O. E. (1976) "Franchise bidding for natural monopolies in general and with respect to CATV." *Bell Journal of Economics*, Vol. 7 (1), 73-104.
- Williamson, O. E. (1979) "Transaction-Cost Economics: The Governance of Contractual Relations." *The Journal of Law & Economics*, Vol. 22, No. 2, 233-261.

Elektroonilised allikad

- Berkeley, R. (2018) How the Creative Industry can Prepare for GDPR. Kättesaadav: <http://digitalmarketingmagazine.co.uk/gdpr/how-the-creative-industry-can-prepare-for-gdpr/4787>, 24.04.2018
- Brown, D. (2017) Ready or Not? GDPR Maturity Across Vertical Industries. IDC Analyze the Future. Kättesaadav: <https://www.bankinfosecurity.com/whitepapers/ready-or-not-gdpr-maturity-across-vertical-industries-w-3459#dynamic-popup>, 28.04.2018
- EBA and RSM (2017) 92% of European Businesses are Unprepared for GDPR. London, PRNewswire. Kättesaadav: <https://www.prnewswire.com/news-releases/92-of-european-businesses-are-unprepared-for-gdpr-658099083.html>, 04.04.2018
- Eesti Statistikaamet (2018) Majanduslikult aktiivsed ettevõtted töötajate arvu järgi, 19.04.2018. Kättesaadav: <https://www.stat.ee/68771>, 12. 05.2018
- Fearn, N. (2018) Small businesses "worryingly unprepared" for GDPR, warns Federation of Small Businesses. Incisive Business Media Limited. Kättesaadav: <https://www.computing.co.uk/ctg/news/3027321/small-businesses-worryingly-unprepared-for-gdpr-warns-federation-of-small-businesses>

- Hon, W. K. (2017) What's wrong with the ICO's draft guidance on controller-processor contracts? International Association of Privacy Professionals, 10.10.2017. Kättesaadav: <https://iapp.org/news/a/controllers-processors-contracts-liability-the-ico-draft-guidance/>
- Justiitsministeerium (2018) Isikuandmete kaitse seaduse eelnõu seletuskiri. Kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/iks_sk_21.03.18.pdf
- Kennedy, J. (2018) Privacy by default: GDPR will change the rules of marketing forever. Silicon Republic, 13.03.2018. Kättesaadav: <https://www.siliconrepublic.com/enterprise/marketing-gdpr-consent-privacy>
- Mayers, C. (2017) One Poll: Three Major GDPR Obstacles Facing British Businesses. 06.09.2017. Kättesaadav: <https://www.citrix.com/blogs/2017/09/06/three-major-gdpr-obstacles-facing-british-businesses/>
- Myers, A. (2016) Top 10 operational impacts of the GDPR: Part 7. Vendor Management. International Association of Privacy Professional, 04.03.2016. Kättesaadav: <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-7-vendor-management/>
- OECD (2006) Outline of principles of impact evaluation. Kättesaadav: <http://www.oecd.org/dac/evaluation/dcdndep/37671602.pdf>
- PWC (2017) Privacy governance survey. The state of privacy management in Belgian organisations. Kättesaadav: <https://www.pwc.be/en/news-publications/publications/2017/belgian-privacy-survey.html>
- PWC (2017) Technology's role in data protection – the missing link in GDPR transformation. 10.2017. Kättesaadav: <https://www.pwc.co.uk/legal/pdf/technologys-role-in-data-protection-the-missing-link-gdpr-transformation.pdf>
- Sherman, C. (2016) Forrester's 2016 Data Privacy Heatmap points to continued European influence on global regulations. Forrester Research, 15.11.2016. Kättesaadav: <https://www.zdnet.com/article/forrester-highlights-the-data-protection-guidelines-and-practices-for-54-different-countries-with/>
- Weissbrot, A. (2018) The Media Agency's Guide to GDPR And EPrivacy. Ad Exchanger, 06.03.2018. Kättesaadav: <https://adexchanger.com/agencies/media-agencys-guide-gdpr-eprivacy/>, 06.05.2018

Muud allikad

- Berg-Larsen, E. (2015) The Issue of Privacy in the European Union. Controversies of the General Data Protection Regulation. (Master's thesis). University of Oslo. Oslo.
- Business Europe (2015) BusinessEurope Input for Trilogue Discussions on The General Data Protection Regulation. Position Paper. Brussels.

- Department of Public Expenditure and Reform (2014) Department of Public Expenditure and Reform. Central Expenditure Evaluation Unit.
- Engan, M. (2017) Big Data and GDPR. A study of how the the new EU data protection regulation impact the value of data. (Master's thesis). University of Stavanger. Stavanger.
- Irish SME Association (2018) Report: Business Unprepared for GDPR, 12.01.2018
- Jonas, J. (2018) Finding the missing link in GDPR compliance. Senzing report, 19.01.2018
- Government of Canada (2010) Analysis of Regulatory Compliance Costs: Part II. Paperwork time burden, costs of paperwork compliance and paperwork simplification, 01.01.2010.
- Lindberg, S. (2017) *GDPR – A handbook for digital marketer*. (Bachelor's thesis). Haaga-Helia University. Helsinki.
- London Economics (2013) Implications of the European Commission's proposal for a general data protection regulation for business. Final report to the Information Commissioner's Office, 01.05.2013
- Magnusson, W. (2017) The EU General Data Protection Regulations and their consequences on computer system design. (Master's thesis) KTH Institute of Technology School of Computer Science and Communication. Sweden.
- Sillaots, S. (2014) "Isikuandmete kaitse regulatsiooni ühtlustamine isikuandmete kaitse üldmääruse eelnõus ja selle mõju Eestile." (Magistritöö). Tartu Ülikool.

Normdokumendid

Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679

Isikuandmete kaitse seadus. RT I 2007, 24, 127

LISAD

Lisa 1. Intervjuude loetelu

Kõik intervjuud viis läbi magistritöö autor.

1. Intervjuu A. Intervjueerija märkmed. Tallinn: 07.04.2018
2. Intervjuu B. Intervjueerija märkmed. Tallinn: 07.04.2018
3. Intervjuu C. Intervjueerija märkmed. Tallinn: 07.04.2018
4. Intervjuu D. Intervjueerija märkmed. Tallinn: 26.04.2018
5. Intervjuu E. Intervjueerija märkmed. Tallinn: 03.05.2018
6. Intervjuu F. Intervjueerija märkmed. Tallinn: 07.05.2018

Lisa 2. Poolstruktureeritud intervjuu küsimused

1. Missuguseid isikuandmeid Teie ettevõtte töötleb?
2. Kui suur on ettevõtte isikuandmete andmebaas? Töötajate oma? Ülejäänud (kliendid, klientide kliendid jne)?
3. Teie ettevõttes on enne isikuandmete töötlemist kaardistatud ära isikuandmed?
4. Kas eesmärgipärase töötlemise põhimõte piirab isikuandmetega tehtavaid toiminguid Teie ettevõttes?
5. Kas Teil on ettevõttes isikuandmeid, mis ei järgi eesmärgipärase töötlemise põhimõtet?
6. Kas Te peate tegema enda ettevõttes muudatusi, et järgida võimalikult väheste andmete

kogumise printsiipi? Milliseid oleksid antud muudatused?

7. Kuidas toimub isikuandmete säilitamine Teie ettevõttes? Kas Teil on määratud isikuandmete säilitamistähtajad? Mille alusel olete määranud isikuandmete säilitamise tähtajad?
8. Kuidas antud nõue mõjutab Teie ettevõtte isikuandmetega seotud toiminguid?
9. Kas Te olete läbi viinud andmete kaardistuse, mis võimaldab saada parema ülevaate andmetest ja nende asukohtadest ettevõttes? Juhul, kui Teie ettevõttes ei ole veel viidud andmete kaardistust läbi, siis kas Te näete selle vajalikkust?
10. Kas Teie ettevõttes on määratud isikuandmete kaitse eest vastutav isik? Kui jah, siis kas Te olete määranud antud isiku oma töötajate seast? Kui ei, siis kas Te plaanite määrata isikuandmete kaitse eest vastutava isiku? Kas vastutava isiku määramine mõjutab kulutusi tööjõule?
11. Kas Te dokumenteerite isikuandmetega seotud toimingud? Kuidas see protsess Teie ettevõttes toimub? Kellel on Teie ettevõttes andmetele ligipääs? Kas Te peate või plaanite pidada andmetöötlustoimingute kohta logifaile?
12. Kas Te tõhustate turvalisuse meetmeid, et vältida andmete lekkimist? Mis on kõige olulisemad meetmed, mida on vaja sisse viia andmete lekkimise vältimiseks? Kas plaanite kulutusi turvameetmete tugevdamiseks andmete kaitsmisel?
13. Kas ja kui palju Te koolitate oma töötajaid, et tõsta teadlikkust andmekaitse teema? Kas Teie ettevõttes on viidud teadlikkuse tõstmiseks läbi siseseid koolitusi? Kas ettevõtte töötajad on osalenud välistel koolitustel?
14. Kas planeerite tuleviku kulutusi teadlikkuse tõstmiseks? Kas koolitustelt saadav info on olnud piisav isikuandmete valdkonnas teadlikkuse tõstmiseks ja ettevõtte vastavusse viimiseks?

- **Üldised küsimused**

1. Kas Teie hinnangul annab GDPR Teie ettevõttele võimaluse konkurentidest eristuda, saavutada tugevam side Teie ettevõtte ja andmesubjektide vahel või näete seda kui takistusena ettevõtluse arendamisel?
2. Kategoriseerudes väikese- ja keskmise suurusega ettevõtte alla, kas Te leiate, et mõni GDPR-st tulenev nõue on ebaproportsionaalselt koormavam? Milline?
3. Mis kulud Teie hinnangul kõige rohkem suurenevad ettevõtte GDPR reeglitega vastavusse viimisel?
4. Kuidas hindate selle GDPR rakendamise mõju ettevõtte kuludele? (1-5 palli skaalal)? (1 – mõju puudub, 2- vähene mõju, 3- keskmine mõju, 4- suur mõju, 5- täielik mõju, 0- ei oska hinnata).
5. Kuidas hindate selle GDPR rakendamise mõju ettevõtte halduskoormusele? (1-5 palli skaalal)? (1 – mõju puudub, 2- vähene mõju, 3- keskmine mõju, 4- suur mõju, 5- täielik mõju, 0- ei oska hinnata).
6. Kas ja kuidas koostöö tegemine suurettevõtetega mõjutab isikuandmete töötlemise protsessi Teie ettevõttes?
7. Kas ja kui palju mõjutavad GDPR trahvimäärad seda, kuidas isikuandmetega seonduvad toimingud teostate (kuni 20 miljonit või 4% globaalsest käibest)? (1 – mõju puudub, 2- vähene mõju, 3- keskmine mõju, 4- suur mõju, 5- täielik mõju, 0- ei oska hinnata).

Lisa 2. Isikuandmete tööstustoimingute kaardistamine ja võrdlus GDPR ja IKS põhjal

Kohustused	Allikas IKS-is	GDPR	Rakendusseadus	Kommentaar
Seadusega tutvumine				
Vastutava töötleja kohustus määrata kindlaks töötlemise eesmärgid, andmete koosseis, töötlemise kord ja viis ning kolmandatele isikutele edastamise lubatavus.	§7 lg 2	Artikkel 24, 26, 30		
Vastutava töötleja kohustus anda juhised volitatud töötlejale isikuandmete töötlemiseks	§7 lg 4	Artikkel 28		
Volitatud töötleja kohustus küsida töötlemise edasi volitamiseks vastutava töötleja kirjalik nõusolek	§7 lg 5	Artikkel 28		
Vastutava töötleja kohustus küsida andmesubjektilt luba tema andmete töötlemiseks (sh selgitada andmesubjektile, mis andmetega ja mida plaanitakse teha ning kuidas saab andmetöötlejaga kontakteeruda)	§10 lg 1	Artikkel 6, 13		

Vastutava töötleja kohustus teavitada andmesubjekti isikuandmete töötlemisest, kui andmed ei ole saadud otse andmesubjektilt	§15 lg 1	Artikkel 14		
Vastutava töötleja kohustus teavitada automaatse otsustusprotsessi kasutamisel andmesubjekti otsustusprotsessi olemusest ja protsessi tingimustest	§17 lg 2	Artikkel 13, p 2f		
Vastutava töötleja kohustus kontrollida andmete edastamisel välisriiki, kas andmekaitse tase välisriigis, kuhu andmed edastatakse, on piisav	§18 lg 1	Artikkel 45		
Vastutava töötleja kohustus küsida andmete saatmiseks välisriiki, mille isikuandmete kaitse taset ei ole Euroopa Komisjon hinnanud piisavaks	§18 lg 3	Artikkel 45		
Vastutava töötleja kohustus väljastada andmesubjektile andmesubjekti soovil tema isikuandmeid või selgitada, miks isikuandmeid ei saa väljastada	§19 lg 1	Artikkel 15	§ 24	
Vastutava töötleja kohustus parandada andmesubjekti andmed	§21 lg 1	Artikkel 5, 16	§ 24, § 25	

andmesubjekti soovil või põhjendada sellest keeldumist				
Vastutava töötleja kohustus lõpetada andmesubjekti soovil andmete töötlemine tarbijaharjumuste uurimiseks või otseturunduseks	§12 lg 5	Artikkel 21		
Vastutava töötleja kohustus lõpetada andmesubjekti soovil andmete avalikustamine	§11 lg 3	Artikkel 17 p 2		
Vastutava töötleja kohustus teavitada andmete parandamisel sellest viivitamatult kolmandaid isikuid, kellele andmed saadeti või kellelt neid saadi	§24 p 6	Artikkel 19	§ 25	GDPR Artikkel 19 - Vastutava töötleja kohustus teavitada isikuandmete parandamisest, kustutamisest või isikuandmete töötlemise piiramisest kõiki vastuvõtjaid, kellele isikuandmed on avaldatud
Vastutava töötleja kohustus võtta isikuandmete töötlemisel kasutusele organisatsioonilised turvameetmed	§25 lg 1	Artikkel 24, 32		
Vastutava töötleja kohustus võtta isikuandmete töötlemisel	§25 lg 1	Artikkel 24, 25, 32		

kasutusele infotehnoloogilised turvameetmed				
Vastutava töötaja kohustus võtta isikuandmete töötlemisel kasutusele füüsilised turvameetmed	§25 lg 1	Artikkel 24, 25,32		
Vastutava töötaja kohustus tagada oma alluvuses isikuandmeid töötlevatele töötajatele väljaõpe isikuandmete kaitse alal	§26 lg 3	Artikkel 39 – koolituse säte andmekaitseametniku määramisel	§40- koolituse säte andmekaitseametniku määramisel	
Vastutava töötaja kohustus registreerida AKIs delikaatsete isikuandmete töötlemine	§27 lg 1	Kohustus kehtib kuni 24.05.2018	Kohustus kehtib kuni 24.05.2018	
Isikuandmete kaitse eest vastutava isiku kohustus pidada andmetöötlemise registrit, kontrollida vastutava töötaja tegevust ja teavitada AKIt vastutava töötaja poolsetest rikkumistest	§30	Artikkel 30 p 2, Artikkel 33		Isikuandmete töötlemise toimingute registri pidamise kohustus ja registri AKIle ligipääsetavaks tegemine.
Vastutava töötaja kohustus teavitada andmesubjekti isikuandmetega seotud rikkumisest		Artikkel 34	§44	
Andmekaitseametniku määramine		Artikkel 39		
Organisatsioonisisese mõjuhinna koostamine		Artikkel 35		

isikuandmete ohutaseme määratlemiseks				
Alla 13 aastaste isikuandmete töötlemise nõusoleku või loa andnud isiku vanemliku vastutuse kontrollimine (kättesaadavat tehnoloogiat arvesse võttes) seoses infoühiskonna teenuste pakkumisega otse lapsele		Artikkel 8 – GDPR toob ära vanusepiiranguks 16 eluaastat.	§8	
Vastutava töötaja kohustus kustutada põhjendamatu viividuseta andmesubjekti puudutavad isikuandmed			Artikkel 17	
Vastutava töötleja kohustus edastada andmesubjektile teda puudutavad isikuandmeid üldkasutavas, masinloetava kujul, mis võimaldab andmete ülekandmist teisele vastutavale töötlejale			Artikkel 20	
Toimimisjuhendite koostamine			Artikkel 40	
Sertifitseerimise mehhanismide kasutuselevõtmine			Artikkel 42	
Vastutava töötleja kohustus dokumenteerida kõik isikuandmetega seotud rikkumised		Artikkel 33, p 5	§43	

Vastutava töötleja kohustus registreerida isikuandmete töötlemise toimingud		Artikkel 30	§30	
Töödeldavatele isikuandmetele tähtaegade kehtestamine			§ 16	
Volitatud töötleja kohustus registreerida isikuandmete töötlemise toimingud		Artikkel 30	§30	
Vastutus rikkumise eest rahaline trahv kuni 20 000 000 eurot.		Artikkel 83	§61, §62, §63, §64, §65, §66, §67, §68, §69	

Allikas: Anspal *et al.* (2009, 8-11); autori täiendused