TALLINNA TEHNIKAÜLIKOOL
Majandusteaduskond
Ärikorralduse instituut

Anastassia Bagnetova

ISIKUANDMETE KAITSE EESTI ETTEVÕTETE RAAMATUPIDAMISES

Magistritöö
Õppekava TARM, peaeriala majandusarvestus

Juhendaja: Natalie Aleksandra Gurvitš-Suits, PhD

Tallinn 2019

Deklareerin, et olen koostanud magistritöö 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 12 397 sõna sissejuhatusest kuni kokkuvõtte lõpuni.

Anastassia Bagnetova ……
(allkiri, kuupäev)
Üliõpilase kood: 176914TARM
Üliõpilase e-posti aadress: anastassia.bagnetova@gmail.com

Juhendaja: Natalie Aleksandra Gurvitš-Suits, PhD
Töö vastab kehtivatele nõuetele

……
(allkiri, kuupäev)

Kaitsmiskomisjoni esimees:
Lubatud kaitsmisele

……
(nimi, allkiri, kuupäev)

SISUKORD

LÜHIKOKKUVÕTE

Töö pealkiri on: Isikuandmete kaitse Eesti ettevõtete raamatupidamises

Magistritöö eesmärk oli selgitada välja raamatupidajate ja teiste arvestusala spetsialistide teadlikkus isikuandmete kaitsest ja seda puudutavast üldmäärusest. Samas oli autori jaoks oluline uurida, milliseid peamisi muudatusi on toonud üldmäärus isikuandmete kaitse suhtes ning milliseid meetmeid rakendatakse, et isikuandmed kaitsta. Uuringu tegemiseks koostati küsimustik, millega sooviti selgitada välja Eesti raamatupidajate ja teiste arvestusala spetsialistide teadmised andmekaitsest ja üldmäärusest.

Uuringu tulemused näitasid, et Eesti arvestusala spetsialistide teadlikkus üldmääruse nõuetest on pigem kõrge. Siiski selgus teadmiste nõrgem külg, mis ilmnes selles, et mõnel arvestusala spetsialistil puudus isikuandmete töötlemise mõistest täielik arusaam. Lisaks esines väike ebakindlus vastutava ja volitatud töötlejate kohustusi puudutavate väidete hindamisel. Teaduskirjanduse läbitöötamisega määrati kindlaks põhilisemad muudatused, mida üldmäärus on andmekaitset reguleerivatesse nõuetesse sisse viinud. Samuti tegi autor selgeks üldmääruse kitsaskohad, mida olid märganud teised üldmääruse uurijad.

Töö alusel võib järeldada, et isikuandmete kaitset reguleeriv üldmäärus on toonud ettevõtetele lisakohustusi, samal ajal laiendades isikute õigusi andmekaitse suhtes. Kuigi kõik ei ole üldmääruses praegu selge, peab otsima sobivaid lahendusi arusaamatuste vähendamiseks. Selleks on eelkõige töötajate teadlikkuse tõstmine koolitusprogrammide kaudu ning ettevõtetes tõhusama andmekaitse tagamiseks kvaliteetsemate kaitsetehnoloogiate loomine.

Võtmesõnad: isikuandmed, isikuandmete kaitse, isikuandmete kaitse üldmäärus, üldmäärus (EL) 2016/679, isikuandmete kaitsemeetmed, muudatused isikuandmete kaitse üldmääruses, GDPR

SISSEJUHATUS

Inimese üks tähtsamaid ressursse on tema isikuandmed. Need määravad isiku identiteedi, mis rõhutab tema erilisusi ja unikaalsust teiste isikute ees, kuid samal ajal võib viidata inimese elu ähvardamisele. Identiteedivargus on tänapäeval üsna oluline probleem, kuna sellega kaasnevad ohud võivad varastatud identiteedi omanikke negatiivselt mõjutada. Teise isiku nimel laenude võtmise, raha varastamiseks veebipõhiste petuskeemide rakendamise ja muude küber-kuritegevusega seotud pettuste juhtumite sagedus on aina kasvanud. Uute tehnoloogiate loomisega sooritatakse küberrünnakuid, mis omakorda suurendab vajadust tõhusamate kaitsevahendite sisseviimise järele. Ka andmekaitseregulatsioonide suhtes tekkis vajadus tõsiste muudatuste järele, täpsemalt kehtestada rangemad nõuded isikuandmete turvalisusele ning viia sisse nendest nõuetest mittekinnipidamise korral karmimad karistused kulukamate rahatrahvide näol.

Magistritöös uuritakse 25. mail 2018. aastal jõustunud isikuandmete kaitse üldmäärust. Isikuandmete kaitse nõuete muudatused on sisse viidud Euroopa Nõukogu ja Euroopa Parlamendi poolt heakskiidetud üldmääruse (EL) 2016/679 alusel, mille vastuvõtmine muutis kehtetuks andmekaitsedirektiivi 95/46/EÜ. Magistritöö raames püstitatakse eesmärk selgitada välja Eesti raamatupidajate ja teiste arvestusala spetsialistide teadlikkus isikuandmete kaitsest ja seda puudutavast üldmäärusest.

Uuringu tegemiseks esitatakse järgmised uurimisküsimused:

1. Kui teadlikud on Eesti raamatupidajad ja teised arvestusala spetsialistid isikuandmete kaitsest ja seda puudutavast üldmäärusest?
2. Millised muudatused on toonud üldmäärus isikuandmete kaitse suhtes?
3. Milliseid kaitsemeetmeid rakendatakse isikuandmete turvalisuse tagamiseks?

Uuringu raames antakse ülevaade isikuandmete olemusest ja neid puudutava üldmääruse peamistest nõuetest. Lisaks käsitletakse isikuandmete rikkumisest tulenevat vastutust ja rikkumiste vältimiseks võimalikke isikuandmete kaitsemeetmeid ning tehakse küsitlus, et selgitada välja arvestusala spetsialistide teadlikkus isikuandmete kaitsest ja üldmääruse nõuetest.

Magistritöö on jagatud kolmeks peatükiks. Esimeses peatükis vaadeldakse isikuandmete olemust ja nende kaitse tähtsust, üldmääruses (EL) 2016/679 ette nähtud isikuandmete kaitse põhimõtteid ja andmesubjekti õigusi ning antakse ülevaade üldmäärusest tulenevatest peamistest muudatustest ja teiste üldmääruse uurijate välja toodud kitsaskohtadest.

Teises peatükis on vaatluse all üldmääruse kajastamine raamatupidamises ja töösuhetes, selle rikkumisest tulenev vastutus, rikkumise vältimiseks isikuandmete võimalikud kaitsemeetmed ning 2017. aastal Rumeenias tehtud uuring kohalike arvestusala spetsialistide teadmistest üldmääruse kohta.

Kolmas peatükk sisaldab autori tehtud uuringut, mille raames koostati Eesti arvestusala spetsialistidele suunatud küsimustik, millega selgitati välja nende teadlikkus isikuandmete kaitsest ja seda puudutava üldmääruse nõuetest. Lisaks võrreldakse selles peatükis Eesti ja Rumeenia uuringute tulemusi ning tehakse järeldused, tuginedes kõigile magistritöö osadele.

Magistritöö koostamisel töötatakse läbi nii inglise- kui ka eestikeelne teaduskirjandus, üldmääruse ja Eesti isikuandmete kaitse seaduse artiklid ning veebipõhised allikad.

Autor soovib avaldada tänu kõigile, kes uuringusse panustasid.

1. ISIKUANDMETE KAITSE

Peatükk sisaldab teoreetilist käsitlust isikuandmete kaitse üldmäärusest. Siin antakse ülevaade isikuandmete liikidest ja nende kaitse olulisusest, üldmääruse (EL) 2016/679 põhilisematest nõuetest, sh isikuandmete kaitse põhimõtted ja andmesubjektile suunatud õigused ning lisaks vaadeldakse üldmäärusest tulenevad põhilisemad muudatused ja mõnede nõuete kitsaskohad.

1.1. Isikuandmed ja nende kaitse olulisus

Tänapäeva ühiskonnas väärtustatakse olulisel määral isiku privaatsust. Üha vähem jagatakse enda kohta käivat infot teistega, ka sotsiaalvõrgustikes luuakse võimalused oma isikuandmetele juurdepääsu piiramiseks. Inimeste soov teha eraelu teistele vähem kättesaadavaks on loomulik ja selge ning selleks on oluline põhjus. Isikuandmed on igale inimesele kuuluv väärtuslik vara, mille sattumine valedesse kätesse võib tekitada selle omanikule märkimisväärset kahju. Isikuandmete ja nende kaitse tähtsusest põhjalikuma ülevaate saamiseks peab eraldi käsitlema isikuandmeid liigiti ning nende kaitse vajadust kinnitavaid asjaolusid.

Igasuguse informatsiooni osad, mille abil võib jõuda isiku identifitseerimisele on isikuandmed. Need liigitatakse lähtuvalt nende kaitsetaseme vajadusest. On teada kaks põhilist isikuandmete liiki: tavalised ja tundlikud isikuandmed.

Tavalisteks andmeteks peetakse selliseid isikuandmeid, mille puhul on võimalik mitte ainult otsene isiku tuvastamine näiteks tema nime või ID-kaardi numbri järgi, vaid ka tema kaudsel viisil kindlaksmääramine näiteks asukohateabe või pildi abil (Gruschka *et al.* 2018, 2). Erinevalt kehtetuks tunnistatud direktiivist 95/46/EÜ (EÜ – Euroopa Ühendus) peetakse 2018. aastast isiku asukohale viitavaid andmeid isikuandmeteks, mis tähendab, et need alluvad üldmääruse regulatsioonile (Gheorghiu, Spătariu 2018, 89). Peab märkima, et isikuandmeid võivad omada ainult füüsilised isikud, kuna juriidilistel isikutel ei ole eraelu, seega puuduvad ka isikuandmed.

Tundlikud isikuandmed on üldjuhul andmed, mille avalikustamine võib kahjustada inimese elu ja tervist ning aidata kaasa identiteedi varastamisele. Sellist liiki isikuandmed on andmed, mis on seotud makseteenustega (makseandmed, pangakonto number, pangakaardil olevad andmed jm), digiallkirjastamiseks vajalikud andmed, avalikult kättesaamatu informatsioon isiku vara kohta jm (Andmekaitse Inspektsioon).

Samuti on olemas ka eriliigilised isikuandmed. Need hõlmavad isikule kuuluvaid geneetilisi andmeid, filosoofilisi ja usulisi veendumusi, poliitilisi vaateid, teavet seksuaalse sättumuse kohta jne. Enne töös käsitletava üldmääruse jõustumist kandsid need nimetust delikaatsed isikuandmed (Lee 2018, 4). Delikaatsete isikuandmete töötlemise registreerimine lõpetati 25. mail 2018 aastal ehk üldmääruse jõustumise päevast. Enne seda oli kohustuslik saada delikaatsete isikuandmete töötlemisele luba, mida oli võimalik taotleda delikaatsete isikuandmete töötlemise registri (DIAT) kaudu (Kaob delikaatsete isikuandmete ... 2018). Eriliigiliste isikuandmete hulka kuuluvad ka varem mainimata jäänud biomeetrilised andmed, mida kogutakse eritehnoloogiate abil (nt skaneerimisvahendid), mis võimaldavad saada inimesele kuuluva unikaalse materjali, milleks on näiteks digitaalne sõrmejälg (Savić, Veinović 2018, 28).

Viimaste kümnendite jooksul toimunud tehnoloogiline läbimurre on teinud inimese elu palju lihtsamaks. Tänapäeval on muutunud võimalikuks teostada veebikeskkonna kaudu teatud isikuandmete edastamisel paljusid elutähtsaid protsesse kiirelt ja hõlpsalt. Vaatamata sellele, et innovaatilised lahendused on toonud inimestele palju võimalusi, on need põhjustanud ka muresid.

Isikuandmete kaitse on tänapäeval üsna oluline probleem, kuna tehnoloogia kiire arenguga kaasneb ka suurem küberpettuste arv. Iga aastaga sagenenud süsteemide häkkimise juhtumid ja väärtusliku teabe lekked põhjustavad teabeomanikele märkimisväärset kahju. Suuremad ettevõtted võivad kannatada kahju tuhandetes või isegi miljonites eurodes. Tihti saavad küberpetturite varastamise objektiks ka isikuandmed. Selleks kasutatakse igasuguseid petuskeeme, tihti tegutsevad petturid mõne tuntud ettevõtte nime alt. Näiteks hoiatati 2019. aasta suvel petuskeemist, kus SEB Pank AS-i nime alt saadeti selle panga klientidele kirjad lingiga, millele vajutamisel ja sisselogimisel varastati klientide paroolid. Samal suvel saadi teada ettevõtte Charlot veebipoe suurest andmelekkest, millega lekkisid 14 tuhat kliendi andmed, sh nimed, isikukoodid ja kontode paroolid (Liive 2019). Sellised juhtumid ei ole ainukordsed, neid juhtub üle maailma üsna palju. Ka Riigi Infosüsteemi Ameti 2018. aasta aruandes on toodud, et 2018. aastal registreeriti 17 tuhat küberpettuste kaebust, mis on rohkem, kui aastal 2017. Küberpetturite ohvriks

on langenud nii väikeettevõtted kui ka kesk- ja suurettevõtted, k.a. avaliku sektori asutused. On olnud juhtu-meid, mille puhul varastati ka delikaatseid isikuandmeid (Ahas 2019).

Eelnimetatud asjaolud viitavad ettevõtete vajadusele luua infosüsteemidele ja andmebaasides hoitavale teabele tugevam kaitse ning kehtestada sisemises privaatsuseeskirjas karmimad nõuded. Küberturvalisuse tagamine eeldab ettevõttepoolseid investeeringuid, kuid samal ajal ka isiku-andmete kaitse nõuete põhjalikku uurimist.

1.2. Üldmääruse (EL) 2016/679 kohaldamine, isikuandmete kaitse põhimõtted ja andmesubjekti õigused

Tänapäeval peetakse andmekaitset väga oluliseks teemaks. Euroopa Liidul on siin eriline roll, sest omades maailmas üht suurimat tarbijaturgu püüeldakse eraelu puutumatuse õigusest lähtudes tagada oma kodanikele piisaval määral andmekaitsealaseid õigusi ja vabadusi (Bendiek, Römer 2019, 40).

Andmekaitse ajaloo alguseks võib Euroopa Liidus pidada 1970-aid aastaid. Tol ajal hakati populariseerima arvutikasutamist, mis pani omakorda mõtlema küberkaitse tagamise peale. 11. mail 1973 võeti Rootsis vastu maailma esimene andmekaitse õigusakt. Selle vastuvõtmise eesmärk oli tagada isikutele kuuluvate andmete privaatsus nende töötlemisel arvutis (Öman 2004, 390).

Veel üks tähtis sündmus, mis avaldas mõju andmekaitseregulatsiooni loomisele oli 1981. aastal Euroopa Nõukogu poolt Strasbourgis koostatud andmekaitse konventsioon, millele eelnes 1980. aastal Majandusliku Koostöö ja Arengu Organisatsiooni (OECD – *Organisation for Economic Co-operation and Development*) mitteametlike andmekaitsesuuniste väljaandmine (Fuster 2014, 104).

Interneti kiire levimisega 1990. aastatel on kasvanud andmekaitse tähtsus. See asjaolu sai aluseks samal kümnendil, nimelt 1995. aastal Euroopa Liidus andmekaitsedirektiivi 95/46/EÜ vastuvõtmisele. Direktiivi eesmärk oli reguleerida kaitse isikuandmete töötlemisel ja nende vaba liikumine veebikeskkonnas.

21. sajandil on pidevast tehnoloogilisest arengust tulenenud vajadus tõhusama andmekaitse tagamisele sundinud hakkama mõtlema andmekaitsenõuete kohandamisele tänapäevastele

tingimustele. Andmekaitsedirektiiv 95/46/EÜ, mis oli jõus rohkem kui 20 aastat, ei olnud enam oma nõuete poolest aktuaalne ning seetõttu oli vaja viia sisse muudatused. Seega hakkas 25. mail 2018 kõigis Euroopa Liidu liikmesriikides kehtima uus isikuandmete kaitse üldmäärus (GDPR – *General Data Protection Regulation*, edaspidi üldmäärus), mille vastuvõtmisele eelnes 14. aprillil 2016 Euroopa Parlamendi ja Euroopa Nõukogu poolt üldmääruse (EL) 2016/679 heakskiitmine. Selle jõustumisega muutus kehtetuks eespool mainitud andmekaitsedirektiiv 95/46/EÜ. Üldmääruse otsekohaldatavuse tõttu muutus ka Eesti kohalik isikuandmete kaitse seadus. Viimane jõustus 15. jaanuaril 2019.

Üldmääruse vastuvõtmine oli suunatud eelkõige üksikisiku õiguste ja vabaduste laiendamisele, mis ilmneb õiguses läbipaistvamale teabele tema kohta käivate isikuandmete töötlemise eesmärkidest ja vahenditest. Üldmääruse prioriteedina tagatakse tõhusam andmekaitse. Selle kasutusele võtmise üks eesmärke on olnud ühtlustada ka isikuandmete kaitset käsitlevad nõuded kõigis EL-i liikmesriikides (Lee 2018, 4). Igal liikmesriigil on õigus täiendada kohalikku isikuandmete kaitse seadust oma nõuetega (sh need, mis määravad kindlaks vastavad riiklikud järelevalveorganid), mis peavad omakorda olema üldmäärusega kooskõlas. Üldmäärus annab järelevalveorganitele õiguse iseseisvalt määrata ettevõtetele trahvisummad seaduse rikkumise eest (Loveday, Abraham 2018, 2).

Võimalikult turvalisema andmetöötluse tagamiseks peab lähtuma isikuandmete töötlemise põhimõtetest, mis on esitatud üldmääruse artikli 5 lõikes 1:

- seaduslikkus, õiglus, läbipaistvus;
- eesmärgi piiramine;
- võimalikult väheste andmete kogumine;
- õigsus;
- säilitamise piiramine;
- usaldusväärsus ja konfidentsiaalsus.

Läbipaistvust rõhutatakse kui andmetöötluse olulisemat põhimõtet, sest see toetab üldmäärusest tulenevat eesmärki anda isikutele võimalus teada nende isikuandmete töötlemisest võimalikult palju (sh andmetöötluse eesmärgid ja vahendid). Eesmärgi piiramine tähendab üldmääruse kontekstis inimesele kuuluvate andmete töötlemist vaid selleks püstitatud eesmärgi raames, mis peab olema talle selge ja arusaadav (Männiko 2011, 45).

Andmesubjektile kuuluva teabe tugevama kaitse tagamiseks peab koguma tema kohta käivaid isikuandmeid piiratud ulatuses (*Ibid.* 2011, 45). See tingimus on ette nähtud võimalikult väheste andmete kogumise põhimõttena. Seega peab vältima igasugust andmetöötlust, millel ei ole seost selleks püstitatud eesmärgiga. Õigsuse põhimõte eeldab, et töödeldavad isikuandmed oleksid aktuaalsed ja vastaksid tõele. Nende aktuaalsuse kaotamise tuvastamisel peab isikuandmeid kas uuendama või need kustutama.

Üldmääruse nõuded ei luba ettevõtetel hoida isikuandmeid infosüsteemides igavesti. Selline tingimus kajastub säilitamise piiramise põhimõttes. Vastavalt sellele põhimõttele on võimalik isikuandmed töödelda kuni selle hetkeni, mil see jõuab andmetöötluse eesmärgi saavutamiseni. Pärast eesmärgile jõudmist peab need andmebaasist maha võtma. Küll aga võib isikuandmeid hoida pikema aja jooksul tingimusel, et nende töötlemine toimub avalikes huvides kas teaduslikes, ajaloolistes või statistilistes uuringutes (Kaul 2017, 17-18).

Usaldusväärsuse ja konfidentsiaalsuse põhimõttest tuleneb nõue hoida isikuandmed turvalisena, mis tähendab nende töötlemist kvaliteetse töötlemistarkvaraga ja andmetöötluse nõuete arvesse võtmist, et välistada igasugune isikuandmete juhusliku kaotamise või hävitamise võimalus.

Üldmääruse jõustumine kehtestas ettevõtetele mõne piirangu ja lisas kohustused andmekaitse suhtes. Samal ajal mõjutas see üksikisikuid otse vastupidi, pakkudes neile rohkem isikuandmete töötlemist puudutavaid õigusi. Kõik andmesubjektile tagatavad õigused on kajastatud üldmääruse peatükis III.

Esimese õigusena mainitakse peatükis õigust läbipaistvusele, millega võimaldatakse inimesel tutvuda tema isikuandmete töötlemise eesmärke, meetmeid ja vahendeid puudutava teabega. Tasub rõhutada, et info selle kohta peab olema kättesaadav ja selgelt sõnastatud. Sellele järgnev juurdepääsuõigus tagab inimesele võimaluse tema isikuandmetele ligi saada. Tulenevalt isikuandmetega tutvumise õigusest on isikul võimalik saada ülevaade selle kohta, milliseid tema isikuandmed töödeldakse, kellele need avalikuks tehakse ja millised on isiku õigused seoses võimaliku isikuandmete parandamise või kustutamise või kaebuste esitamise vajaduse tekkimisega. Vajaduse korral võib andmesubjekt nõuda andmetöötlejalt talle kuuluvate isikuandmete parandamist. See tingimus tuleneb õigsuse põhimõttest, mille puhul peavad andmesubjekti isikuandmed olema aktuaalsed ja usaldusväärsed. Inimene võib igal ajal nõuda oma isikuandmete kustutamist. Selline õigus sai nimeks „õigus olla unustatud“ *(The Right to be*

Forgotten). Isik võib seda õigust kasutada, kui ta leiab, et tema isikuandmeid töödeldakse ebaseaduslikult või nende töötlemise eesmärk on juba saavutatud. Sellise nõude esitamisel peab andmetöötleja rollis olev ettevõte andmetöötluse lõpetama ja isikuandmed kustutama ning nende edastamisel kolmandatele ettevõtetele nõuda neilt sama (Deac 2018, 155). Isikuandmete süsteemist mahavõtmine peaks olema tehtud 48 tunni jooksul ilma selle eest tasu võtmata (9 Ways Accountants can ... 2018, 3). Peale eespool nimetatud õiguste võib isik nõuda isikuandmete töötlemise piiramist, kui talle tundub, et tegemist on tema aktuaalsust kaotanud isikuandmete töötlemisega või ta ei leia nende töötlemiseks õiguslikku alust. Õigus andmete ülekandmisele on nii-öelda värske ja ainult sellest üldmäärusest tulenev ning näeb ette inimese nõudmisel tema isikuandmete edastamist ühelt ettevõttelt teisele, kui andmetöötlus teostatakse automaatselt või kui see toimub kas nõusoleku või lepingu alusel (*Ibid.* 2018, 155). Üldmäärus lubab isikul esitada isikuandmete töötlemisega kaasnevaid vastuväiteid. Seda on võimalik teha otseturunduse puhul, näiteks profiilianalüüsil. Profiilianalüüs tehakse peamiselt turunduslikel eesmärkidel, et selgitada välja isiku asjaolud, näiteks tema tarbijana käitumine, eelistused ja hoiakud, mille alusel langetatakse tema kohta otsused ning tulenevalt tema poolt kõige sagedamini külastatavatest linkidest pakutakse vastav reklaam. Selleks kasutatakse veebilehtedel küpsiseid. Küpsiste kasutamisel automatiseeritakse ja salvestatakse kasutaja eelistused.

Näiteks mõne e-poe korduval külastamisel hakatakse inimese enim vaadatud tooteid mõne aja pärast kajastama sotsiaalvõrgustikes reklaamina või samal veebilehel viimati külastatud toodet selle leidmise lihtsustamiseks vihjena. Kui inimene esitab ettevõttele, kes tegeleb tema profiilianalüüsiga vastuväiteid, peab viimane tema isikuandmete töötlemise kahe ööpäeva jooksul lõpetama.

Siinses alapeatükis käsitleti üldmäärusest tulenevad andmesubjektidele suunatud õigusi ja põhimõtteid, mis toetavad Euroopa Liidus valitsevaid inimõigusi ja vabadusi. Igal füüsilisel isikul peab olema õigus teada teda puudutavate isikuandmete töötlemise eesmärkidest, andmetöötlejatest ja rakendatavatest meetmetest ning teatud juhtudel nende töötlemist piirata. Sellega tagatakse isikutele õigus eraelu puutumatusele, mis on Euroopa Liidus üks võtmeõigusi, mille piiramine ei peaks lubatud olema.

1.3. Üldmääruse jõustumisega kaasnevad peamised muudatused

Üldmääruse jõustumine on toonud kaasa rangemad isikuandmete töötlemise nõuded. Rangemaks on need muutunud eelkõige juriidiliste isikute jaoks, sest isikuandmete töötlemine toimub peamiselt ärilistel eesmärkidel. Siinses alapeatükis tuuakse välja autori hinnangul kõige põhilisemad muudatused üldmääruses.

Esimene oluline aspekt oli kõigil ettevõtetel tekkinud kohustus alates 25. maist 2018 teavitada kõiki isikuid, peamiselt kliente jõustunud üldmäärusest ning sellest tulenevast nõudest anda neile edaspidi põhjalik info nende õigustest isikuandmete töötlemise suhtes. See tähendas ettevõtete jaoks kohustuslikus korras klientidele teate suunamist, mis hõlmaks eelkõige isikuandmete töötlemise tingimused (sh eesmärgid) ning pakuks neile võimaluse kas lubada nende töötlemist või sellest loobuda.

Ettevõtteid puudutas ka vajadus määrata kindlaks, kas nad kuuluvad vastutavasse või volitatud töötleja liiki. Vastutava ja volitatud töötleja kohustused on kindlaks määratud artiklites 24 ja 28. Vastutavat töötlejat võib pidada mõjukaks figuuriks andmekaitse suhtes, sest ta määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid ning otsustab, milliseid isikuandmeid koguda ja milliseid nendega kaasnevaid toiminguid teostada. Volitatud töötleja tegutseb ainult vastutava töötleja nime all, mis tähendab, et ta peab järgima kõiki vastutava töötleja antud juhiseid. Erinevalt vastutavast töötlejast ei tohi volitatud töötleja iseiseisvalt määrata isikuandmete töötlemise eesmärki, kuid ta võib omal soovil valida, milliseid korralduslikke ja tehnilisi vahendeid (nt töötlemistarkvara) andmetöötlusel kasutada.

Järgmisena tuuakse näide, mille korral on ühel ja samal ettevõttel mõlema andmetöötleja roll. Raamatupidamisbüroo osutab teenuseid väikeettevõttele. Väikeettevõte on selle näite kohaselt vastutav töötleja, kuna ta ise otsustab, millised töötajate isikuandmed raamatupidamisbüroole üle anda. Raamatupidamisbüroo on volitatud töötleja, kes töötleb töötajate isikuandmeid (nt töötaja nimi ja pangakonto number) tulenevalt väikeettevõtte poolt püstitatud eesmärkidest (nt palgaarvestus). Samal ajal võib see raamatupidamisbüroo olla ka vastutav töötleja näiteks ettevõtte suhtes, kellelt ta raamatupidamistarkvara rendib. Raamatupidamistarkvara pakkuv ettevõte esineb selles näites volitatud töötlejana, kuna ta hoiab ja töötleb raamatupidamisbüroo poolt usaldatud isikuandmeid.

Samuti on tähtis mainida, et tulenevalt ariklist 30 on vastutava töötleja kohustus dokumenteerida isikuandmete töötlemisega kaasnevaid toiminguid (sh tehnilised ja korralduslikud kaitsemeetmed). See nõue laieneb ettevõtetele, kus töötab üle 250 töötaja ehk suurettevõtetele. Toimingute registreerimine on oluline abivahend isikuandmete võimalike rikkumiste leevendamiseks (Accountancy Europe ... 2017, 4). Samas on dokumentatsiooni pidamine vajalik selleks, et lähtuvalt juurdepääsuõigusest tagada andmesubjektile võimalus tutvuda talle kuuluvate iskuandmete töötlemist puudutava informatsiooniga.

Artikli 33 lõige 1 sätestab, et vastutava töötleja pädevuses seoses uue üldmäärusega on teavitada 72 tunni jooksul isikuandmete rikkumisest nii Andmekaitse Inspektsiooni kui ka nende omanikku, kui sellega kaasneb suur oht isikuandmetele ning kui vastutaval töötlejal ei õnnestunud rikkumist iseseisvalt kõrvaldada. Juhul kui vastutaval töötlejal tekivad kahtlused isikuandmete rikkumise esinemise kohta, peab ta igal juhul pöörduma järelevalveasutusse ja edastama sinna aruande, kus peab kirjeldama võimalike isikuandmete rikkumiste iseloomu (Petersen 2018, 14). See on oluline aspekt, sest aruande kaasamine võimaldab isikuandmete rikkumise likvideerimist või vähemalt negatiivsete tagajärgede minimeerimist ning lisaks on võimalik aruannet kasutada vihjena vastutava töötleja poolt märkamata rikkumiste tuvastamisel.

Teatud juhtudel võib ettevõte määrata kaks või enam vastutavat töötlejat. Kui määratakse enam kui üks vastutav töötleja, siis on tegemist kaasvastutavate töötlejatega. Kaasvastutavate töötlejate vahel peab olema sõlmitud kokkulepe, mis määrab iga osapoole vastutuse määra andmesubjekti teavitamisel isikuandmete töötlemisest ning nendega kaasnevatest ohtudest ja rikkumistest (Hintze 2018, 25). Kaasvastutavate töötlejatega võib olla tegu siis, kui näiteks ettevõte müüb teisele ettevõttele frantsiisi. Sellisel juhul täidavad mõlemad vastutava töötleja ülesandeid.

Ettevõttele, kes tegeleb suurema riskiga isikuandmete töötlemisega või kes soovib välja vahetada töötlemistarkvara, määratakse kohustus teha kirjalik andmekaitsealane mõjuhinnang. Kirjaliku mõjuhinnangu tegemine on mõeldud eelkõige ettevõtetele, kes teostavad profiilianalüüsi ehk tegelevad suures ulatuses isiklike aspektide automatiseeritud töötlemisega ning haiglatele ja tervisekeskustele, kes töötlevad terviseandmeid (nt patsientide haiguslood), mille võimalik leke võib tekitada inimese elule ja tervisele olulist kahju (Isikuandmete töötleja üldjuhend).

Üldmääruses kehtestatud nõuded laienevad ka Euroopa Liitu mittekuuluvates riikides tegutsevatele ettevõtetele, kui viimased koguvad ärilistel eesmärkidel Euroopa Liidu kodanike isiklikku

informatsiooni läbi kaupade müügile või teenuste osutamisele suunatud veebilehtede või tarbimisharjumuste monitoorimise vahendite (Chabinsky 2018, 30). Isikuandmete edastamine väljaspool Euroopa Liitu tegutsevale ettevõttele on võimalik, kui selle riigis kehtivad isikuandmete kaitse reeglid, mida on võimalik seostada üldmäärusega ettenähtud nõuetega või kui Euroopa Liitu mittekuuluva ettevõtte vastutav töötleja tagab isikuandmete töötlemisel piisava turvalisuse (Accountancy Europe ... 2017, 6). Näiteks Euroopa Majanduspiirkonda kuuluval Islandil, samuti Norras ja Liechtensteinis on kehtestatud nõuded isikuandmete kaitsele sarnased Euroopa Liidus kehtivate nõuetega, millest tuleneb, et nendes riikides on tagatud samaväärne turvalisuse tase (Kirss 2019). Samas on sõlmitud Euroopa Liidu ja Ameerika Ühendriikide vahel kokkulepe, mis sai nimeks Privacy Shield. Selle sõlmimise eesmärk oli jälgida USA ettevõtteid, kes teevad koostööd Euroopa Liidu ettevõtetega ning nendevahelise andmevahetuse ja -töötluse seaduslikkust (Voss 2017, 231).

Muudatused üldmääruses sundisid teatud ettevõtete ja asutuste liike määrama ametisse andmekaitsespetsialisti. Andmekaitsespetsialisti kontseptsioon ei ole uus ja kuigi andmekaitse-direktiivist 95/46/EÜ ei tulenenud kohustust määrata nimetatud spetsialisti teatud asutuste liikidele, on mõne Euroopa Liidu liikmesriigi ettevõtetes andmekaitsespetsialist kohale määratud juba ammu (Cliza, Spataru-Negura 2018, 492). Käesoleva üldmääruse artikliga 37 ette nähtud kohustuslik andmespetsialisti määramine puudutab eelkõige avaliku sektori asutusi ning neid ettevõtteid või asutusi, kes tegelevad inimeste monitoorimisega või töötlevad kriminaalasjadega kaasnevaid isikuandmeid.

Tänapäeval saavad kõik isikud, kes on määratud ettevõttes andmekaitsespetsialistiks, läbida vastavad koolitused. Andmekaitsespetsialisti koolitusi pakuvad näiteks Tartu Ülikool ja Tallinna Ülikool ning koolitusettevõtted. Samas on võimalik läbida isikuandmete kaitset puudutavad temaatilised koolitused TalTechis. Koolituste läbimine on kasulik ja võimaldab andmekaitsespetsialistil õppida paremini tundma oma kohustusi ja ülesandeid. Samal ajal ei ole koolituste läbimine ega vastava tunnistuse omandamine kohustuslik, kuna see ei ole üldmääruse ega Andmekaitse Inspektsiooni nõuetega ette nähtud. Andmekaitse Inspektsiooni peadirektori Viljar Peebu arvates on peamine, mida andmekaitsespetsialist peab tundma, andmekaitse nõuded ning ettevõttesised tööprotsessid, tehnoloogiad ja töökorralduse reeglid. Peebu sõnul peab ta oskama eespool mainitud küljed omavahel siduda. Samuti peab andmekaitsespetsialisti ülesandeid täitev töötaja olema teadlik andmekaitse põhimõtetest ning oskama rakendada asjakohaseid turvameetmeid (Andmekaitse spetsialist ... 2018).

Kuigi üldmääruse nõuded näitasid end juriidiliste isikute suhtes pigem rangemast küljest, laiendasid need samal ajal füüsiliste isikute õigusi. Peale õiguse läbipaistvamale teabele isikuandmete töötlemise kohta said füüsilised isikud ehk üldmääruse kontekstis andmesubjektid lähtuvalt artiklist 17 „õiguse olla unustatud“ ehk õiguse, mille korral on neil võimalik igal ajal nõuda nende isikuandmete kustutamist, mis peab olema tehtud 48 tunni jooksul selle eest tasu küsimata. Samas jäetakse isikutele õigus esitada vastuväiteid näiteks otseturunduse puhul või nende arvates isikuandmete ebaseadusliku töötlemise kohta.

Näitena andmete kustutamise õigusest võib tuua olukorra, kui inimene ostab tehnikat müüva poe veebilehelt nutiseadme ning pärast ostu sooritamist hakatakse tema e-posti aadressile saatma poe sooduspakkumisi. Kui ta ei soovi uudiskirja saada, on tal õigus pöörduda sellest loobumise nõudega e-poe poole, mille korral viimane peab uudiskirja saatmise kahe ööpäeva jooksul lõpetama.

Andmesubjektid said tänu üldmäärusele õiguse andmete ülekandmisele. Lähtuvalt sellest õigusest võib isik nõuda ettevõttelt talle kuuluvate isikuandmete edastamist teisele ettevõttele (üldmäärus (EL) 2016/679 art 20 lg 1). Selle õiguse raames antakse andmed üle põhimõtteliselt ilma andmesubjekti osaluseta, mis tähendab, et inimene ei pea ise tegelema enda kohta käivate andmete üleandmisega.

Selle õiguse kasutamist päriselus võib näha näiteks teleoperaatori vahetamisel. Inimene lõpetab koostööd ühe operaatoriga ja sõlmib lepingu teisega. Samal ajal toimub nende operaatorite vahel kliendi isikuandmete ülekandmine endise operaatori andmebaasist uue operaatori omasse.

Magistritöö siinses osas toodi välja autori arvates peamised üldmäärusega kaasnevad muudatused. Nende alusel võib järeldada, et üldmäärus on toonud ettevõtetele täiendava töömahu ning samal ajal andnud inimestele suuremad õigused, mis väljenduvad võimaluses teada enda väärtusliku vara ehk isikuandmete töötlemisega seonduvast nii palju, kui võimalik. Samas aga ei saa väita, et kõik üldmääruses on selge. Ebaselgeid nüansse vaadeldakse järgmises alapeatükis.

1.4. Üldmääruse kitsaskohad

Tööst selgub, et inimeste õigused andmetöötluse suhtes on märkimisväärselt laienenud. Siiski näeb mõni üldmääruse uurija selles kitsaskohti, mis teevad andmetöötluse raskemaks. See seisneb eelkõige mõne üldmääruse nõude määramatuses. Michelle Goddard (2017, 704-705) on arvamusel, et üldmäärusega ette nähtud paindlikkus, mis ilmneb kõigi liikmesriikide võimaluses täiendada kohalikku isikuandmete kaitse seadust, võib oma nõuetega määramatust suurendada. Näiteks artikli 8 lõike 1 järgi võimaldab üldmäärus kõigil EL-i kuuluvatel riikidel iseseisvalt määrata vanusepiirang lapse isikuandmete töötlemise jaoks, mis peab jääma vahemikku 13-16 aastat. Eri riikides erinevate nõuete kehtestamine raskendab koostööd rahvusvaheliste ettevõtete vahel, sest teise riigi sama nõude erinevuse arvestamata jätmine võib põhjustada isikuandmete töötlemise nõuete rikkumist, millest tuleneb ka rahalise karistuse võimaluse teke.

Iga andmetöötlusega tegelev ettevõte peab teadma, kas ta täidab isikuandmete töötlemisel teiste ettevõtete suhtes vastutava või volitatud töötleja kohustusi. Selle kindlaksmääramine on tähtis, sest mõlemal andmetöötlejaliigil on eri ülesanded ja vastutuse tase. Mike Hintze (2018, 18) märgib, et tihti saadakse vastutava ja volitatud töötleja mõistest valesti aru, mis võib põhjustada üldmääruse nõuete rikkumise. Ta toob oma uuringus näite, kus termin „vastutav töötleja“ seostatakse tihti mõistega „andmete omanik“, mis on aga täiesti vale lähenemine. Need ei ole samad asjad, kuna tavaliselt esineb vastutava töötlejana ettevõte, kes saab näiteks tööandjana isikuandmed andmesubjektidelt ehk töötajatelt ja usaldab nende töötlemist teisele ettevõttele, näiteks raamatupidamisbüroole. Arusaamatust võib tema sõnul tekitada ka selline asjaolu, et iga ettevõte võib teiste ettevõtete suhtes täita nii vastutava kui ka volitatud töötleja ülesandeid. Ettevõtted peavad meeles pidama, et vastutus isikuandmete töötlemise, sh nende kogumise, kasutamise, säilitamise, kustutamise, edastamise kaudu avalikustamise ja muude isikuandmete töötlemisega kaasnevate toimingute üle langeb eelkõige vastutavale töötlejale, kuid mitte volitatud töötlejale (Fazlioglu 2019, 277). Volitatud isik või asutus töötleb isikuandmeid lähtuvalt vastutava töötleja juhistest ning rikkumiste tuvastamise korral pöördub ta vastutava töötleja poole. Peab ka rõhutama, et mõlemal andmetöötlejal peab olema piisavalt kompetentse ning nad peavad turvalise andmetöötluse tagamiseks rakendama kvaliteetseid töötlemisvahendeid.

Üldmääruse nõuete mõju alla satuvad ka kolmandad osapooled, kellega EL-is tegutsevad ettevõtted koostööd teevad. See tekitab mõlemale osapoolele täiendavat töömahtu, sest koostöö loomiseks või jätkamiseks peavad kolmanda riigi ettevõttel olema kasutuses üldmääruse nõuetele

vastavad andmekaitse vahendid ning samas peab ta jagama andmetöötluse turvalisust tunnistavaid aruandeid. Arvestusspetsialist Mark Lee (2018, 7-8) arvates peab iga liikmesriigi ettevõte pidama nimestikku kolmandatest riikidest ettevõtete kohta, kellega ta koostööd teeb. Ettevõttel, kes on usaldanud isikuandmed kolmandatele osapooltele, on vastutus nende üle, seega on nad vastutavad töötlejad. Isikuandmeid töötlevad kolmandad osapooled täidavad tavaliselt volitatud töötleja ülesandeid. Isikuandmeid edastavad ettevõtted võiksid katsetada kolmandate osapoolte poolt kasutatavaid töötlemisvahendeid ning hinnata katsete alusel nende sobivust. See on eriti oluline Euroopa Liidu ettevõtete jaoks, sest nad peavad olema suutelised tõendama isikuandmete töötlemise vastavust üldmääruse nõuetele. Seega peavad liikmesriigi ettevõtted koguma nii palju tõendusmaterjale kui võimalik. Tõendusmaterjaliks sobib näiteks vastutava töötleja ja volitatud töötleja rolliga ettevõtete vaheline kirjavahetus, kolmanda osapoole tehtavad isikuandmetele piisava kaitse tagamise kirjalikud kinnitused ning vastutava töötleja teostatavate isikuandmete töötlemismeetmete sobivuse testimise aruanded.

Probleemi näevad Shastri *et al.* (2019) veel selles, et üldmäärusest tuleneva nõude täitmine – kustutada isikuandmeid lühikese aja jooksul – võib tegelikkuses rohkem aega võtta. Näiteks pilvetarkvaras on ette nähtud osa andmeid salvestada alamsüsteemidesse, milleks on mälu, vahemälu, kettad ja võrgusalvestus, mis loob mitu andmete koopiat. Nende kustutamise vajaduse tekkimisel tuleb kustutada kõik andmete koopiad, mis võib tingida üldmäärusega ette nähtud ajast pikema ajakulu.

Üldmääruse üks põhimõtteid on võimalikult väheste andmete kogumise põhimõte, mis eeldab, et ettevõtte toimimiseks hoitakse andmebaasis ainult kõige olulisemat füüsiliste isikute kohta käivat teavet. Ühest küljest on see hea selle poolest, et kuna kaitset vajavaid andmeid on vähem, on väiksem ka andmete kaotamise või varastamise võimalus. Teisest küljest peaks aga ettevõttel, kes kasutab üksikisikute andmeid enda tarbeks, olema täpne ettekujutus konkreetsetest andmetest, nimelt milliseid andmeid vajatakse, kust need kogutakse ja kus säilitatakse. Sageli on keeruline ennustada, milline teave klientide ja tarnijate kohta on tulevikus ettevõtte jaoks oluline, eriti kui tegemist on pooltevaheliste vaidluste lahendamisega. Näiteks kui ettevõttes kasutatakse kirjavahetuse piiratud säilitamise meetodit (nt 30 või 60 päeva), võib tulevikus tekkida kas tarnija või kliendiga seotud vaidluse lahendamiseks vajalike üksikasjade puudumise probleem, kuna kirjad kustutatakse teatud aja möödumisel (Sipes *et al.* 2016, 56).

Uuendatud isikuandmete töötlemise nõuetele kohandamine võib osutuda ettevõtetele kulukas. Üldmääruse jõustumine nõuab neilt tõhusama andmekaitse tagamist, mis tähendab mõne ettevõtte jaoks uude tarkvarasse täiendavate investeeringute tegemist. Sama oluline on töötajate andmekaitseteadlikkuse tõstmine, milleks peab ettevõte korraldama vastavaid tasulisi koolitusi. Küll aga ei kujune investeerimine kaitsesüsteemidesse ega töötajate teadmistesse probleemiks, kui isikuandmed tõeliselt väärtustatakse.

Töö sellest osast järeldub, et üldmääruses peituvad ka kitsaskohad, mis jäävad paljudele arusaamatuks. Peab märkima, et kõik maailmas ei ole laitmatus korras, kuid jääb üle loota, et üldmäärusest tulenevad puudused saavad parandatud või arusaamatust tekitavad nõuded vähemalt põhjalikult lahti seletatud. Autori arvates peab looma rohkem selges keeles koostatud praktilisi juhendmaterjale ja korraldama koolitusi, mis aitavad ettevõtetel üldmääruse kohaselt korrektselt andmeid töödelda.

2. ISIKUANDMETE KAITSE SEOS RAAMATUPIDAMISEGA

Selles peatükis tuuakse välja üldmääruse mõju raamatupidamisele ja töösuhetele, üldmääruse nõuete rikkumisest tuleneva vastutuse käsitlus ning antakse selle vältimiseks ülevaade võimalikest andmekaitsemeetmetest. Lisaks käsitletakse siin 2017. aasta uuringu tulemusi Rumeenia arvestusala spetsialistide teadlikkusest üldmääruse kohta, et edaspidi võrrelda neid andmeid autori uuringu tulemustega.

2.1. Üldmääruse nõuete kajastamine raamatupidamises ja töösuhetes

Ehkki kõigis ettevõtetes sõltuvalt suurusest, tegevusalast või muust põhjusest pole eraldi raamatupidamisosakonda või raamatupidajat, on raamatupidamine iga ettevõtte oluline osa. Raamatupidamine aitab võtta vastu otsuseid ettevõttele tähtsates küsimustes, täita administratiivseid funktsioone ning tõsta tootlikkuse taset ettevõtte eesmärkide täitmiseks (El-Dalabeeh, Alshebeil 2012, 893-900). Raamatupidamise oluliste funktsoonide hulka kuulub finantsandmete ja -tehingute töötlemine ning finantsinfo ja -aruannete edastamine juhtkonnale, mis on tähtis käesoleva ja tulevase tegevuse planeerimiseks ja kontrollimiseks. Viimane aitab huvitatud osapooltel saada ratsionaalseks otsuste langetamiseks kasulikku informatsiooni (Bansah 2018, 445). Igapäevaselt puututakse raamatupidamises kokku mitmesuguste isikuandmetega, mis eeldab raamatupidajate kursisolekut üldmääruse nõuetega. Autori arvates on tähtis rõhutada üldmääruse nõuete kajastamist raamatupidaja igapäevastes tööülesannetes ning lisaks tuua välja ka näited selle mõjust töösuhetele, kuna need moodustavad olulise osa ettevõtte tegevuses.

Iga ettevõtte üks tähtsamaid ressursse on töötajad. Tööandja ja töötaja vaheliste töösuhete loomise aluseks on töölepingu sõlmimine. Töölepingu sõlmimine eeldab füüsiliselt isikult (töötaja) tööde teostamist teisele isikule (tööandja), mille eest kohustatakse tööandjat töötajale palka maksma (TLS §1). Eelmises töölepingu sõlmimise olemust käsitlevas mõistes rõhutatakse töötaja kui füüsilise isiku olekut. Vastavalt isikuandmete definitsioonile nimetatakse isikuandmeid igasuguseks teabeks, mis viitab füüsilise isiku kas otsesele või kaudsele tuvastamisele. Füüsilisel

isikul olev alus isikuandmetele tuleneb tema eraelu olemasolust, mida näiteks juriidilise isiku puhul olla ei saa.

Töösuhete loomine põhineb töötaja kohta käiva info kogumisel ja töötlemisel. Siia kuulub näiteks värbamisprotsessi käigus töövõtjalt saadud isiklik informatsioon, k.a töövõtja intervjueerimisel ja testimisel saadud vastused ning tema CV-s toodud info, mille alusel tehakse tema sobivuse hinnang kandideeritavale ametikohale (Tiits 2019). Tööle kandideeriva isiku kohta informatsiooni kogumisel otsingumootori või sotsiaalvõrgustike kaudu peab töövõtjat selle kohta teavitama ning vestlusel pakkuma talle võimalust kogutud infot kas täpsustada või parandada (Miidla-Vanatalu 2012). Isikuandmete töötlemisel töösuhetes lähtutakse mõlema osapoole põhiõigustest ja huvidest, samas ka seaduses määratud õiguslikest normidest. Usalduslike töösuhete loomine tööandja ja töövõtja vahel on väga oluline, sest see avaldab positiivset mõju mõlema osapoole eesmärkide täitmisele töösuhetes. Üldmääruse seaduslikkuse ja läbipaistvuse põhimõttest tulenevalt on andmesubjektil, kelleks on töösuhetes töövõtja, õigus tutvuda tööandja poolt töödeldavate talle kuuluvate isikuandmetega ning nende töötlemiseks oleva õigusliku aluse ja eesmärgiga. Kõik töölepingus sätestatud tingimused, k.a need, mis puudutavad isikuandmete töötlemist peavad olema sõnastatud lihtsas ja selges keeles ning vajaduse korral töölepingu sõlmimisel töövõtjale põhjalikumalt lahti seletatud.

Näiteks kontorisse sisenemiseks ja väljumiseks vajaliku uksekaardi registreerimine on mingil määral isikuandmete kogumine ja töötlemine, kuna selle logisid kasutatakse töötaja reaalse kontoris viibimise aja kontrollimiseks ning võimalike hilinemiste ja töökohalt puudumise tõendamiseks. Nii peab olema ka sõnastatud eesmärk, mis võib kõlada järgmiselt: „Uksekaarte kasutatakse nii võõrastele isikutele kontorisse juurdepääsu piiramiseks kui ka töötajapoolse tööajast kinnipidamise kontrollimiseks“ (Miidla-Vanatalu 2014, 5). Eespool toodud näites vaadeldud tingimus ja selle sisseviimise eesmärk on selge ja arusaadav, mis vastab üldmääruse põhimõttele isikuandmete töötlemise läbipaistvuse kohta.

Teiste ettevõtetega koostöösuhete loomine on ettevõtluses üks olulisi tegevusi, milleta ei saaks toimida ükski ettevõte. Koostöö tegemise puhul sõlmitakse osapoolte vahel alati leping, millest tekib ka vajadus koguda andmeid. Mikro- ja väikeettevõtete seas on levinud kasutada isikliku raamatupidaja ametikoha või raamatupidamisosakonna asemel raamatupidamisbüroode teenuseid. See on tänapäeval üsna mugav viis äri raamatupidamise tegemiseks. Selliseid büroosid on Eestis piisavalt palju ning nende seast on võimalik valida sobivaim lähtuvalt pakutavatest teenustest,

raamatupidaja pädevusest, sh välisriikide raamatupidamisseaduste tundmisest, keelteoskusest ja muudest teguritest. Raamatupidamisbürooga koostöö tegemisel on vastutavaks töötlejaks tööandja ning volitatud töötlejaks raamatupidamisbüroo. Tööandja usaldab raamatupidamisbüroole töötajatelt saadud isikuandmed, mida viimane töötleb ja kasutab igasuguste väljamaksete tegemiseks. Tavaliselt kuuluvad nende andmete hulka tundlikud isikuandmed (nt töötaja pangaandmed). Üldmäärus kohustub tööandjat kinni pidama võimalikult väheste andmete kogumise põhimõttest, mille kohaselt peab töötaja kohta koguma piiratud koguses isikuandmeid ehk ainult neid, mille kogumine ja töötlemine on vajalik töövõtja poolt kandideeritava ametikoha ülesannete täitmiseks. Alati peab töötajal olema õigus teada, milliseid tema isikuandmeid töödeldakse, samuti nende töötlemise eesmärki.

Töölepingusse märgitud töötaja isikuandmeid kasutab raamatupidaja eelkõige töötajale palga arvestamiseks. Peale isikut tuvastavate andmete (nagu ees- ja perekonnanimi ning isikukood) ja palgaarvestust puudutava teabe (sh palgainfo, kinnipeetavad makse- ja maksumäärad ning pangakonto number), on raamatupidajal vajalik saada töötajalt tema terviseseisundi andmed ja laste olemasolul nende kohta käiv informatsioon (sh ees- ja perekonnanimi, sünniaeg või isikukood).

Terviseandmed kuuluvad eriliigiliste andmete hulka. Nende kogumisele on üldmäärusega ette nähtud ka piirangud. Näiteks ei tohi tööandja küsida tervishoiuasutuselt töötaja kohta selliseid andmeid nagu töötaja haiguslugu, arstitõendisse märgitud diagnoos, seadusega ette nägemata andmed tervisekontrolli tulemustest või tööõnnetuse kohta saadud arsti järeldusest (*Ibid.* 2014, 6). Töötaja peab ise edastama tema terviseseisundi kohta käivad andmed, kui nende edastamisel on seaduslik alus. Töötajalt kogutud terviseandmete alusel maksab raamatupidaja töötajale välja tervisehüvitise. Tervisega seotud hüvitiste väljamaksmiseks peab töötaja esitama vastavad tervisetõendid.

Näiteks kui tuvastatakse töö käigus nägemisteravuse halvenemise tõttu vajadus kasutada kuvariga töötamisel prille, esitab töötaja silmaarsti otsuse prillide vajaduse kohta, prillide hüvitamise avalduse, prilliretsepti ning prillide eest raha tasumist tõendavad tšekid. Hüvitise suurus sõltub tööandja sisemise korraga määratud summast, kuid see peaks olema piisav töötajale prillide soetamiseks. Töötajal on võimalik soetada ka hüvitise summast kallimad prillid, kuid vahe peab ta ise juurde maksma.

Üldmäärus on kehtestanud laste isikuandmete töötlemist puudutavaid nõudeid, mille kohaselt ei ole võimalik alla 13 aastase lapse isikuandmeid töödelda, kui tema vanemad sellega ei nõustu. Töösuhetes on tavaliselt ette nähtud töötaja laste kohta info küsimine. Töötaja lapsi puudutav informatsioon on raamatupidajale vajalik näiteks lapsepuhkuse arvestamisel, mis makstakse välja kuni 14 aasta lapse olemasolul. Eesti Vabariigi õigusaktidega on ette nähtud erinevad lapsepuhkused, millel viibimise aeg ja tingimused varieeruvad sõltuvalt puhkuse liigist (Sotsiaalkindlustusamet). Töötaja laste kohta käivat informatsiooni, täpselt nende sünniajad kogutakse ka muudel eesmärkidel, näiteks lastele jõuludeks kinkide organiseerimisel ja igasuguste boonusprogrammide läbiviimisel.

Eelpool toodud näited puudutavad kas delikaatsete või tundlike isikuandmete töötlemist. Mõlema liigi isikuandmete töötlemine ei ole üldmäärusega lubatud, kui andmesubjekt ehk siinses näites töötaja ei ole andnud sellele vastavat nõusolekut. Selline nõue tuleneb nende andmeliikide tugevamast vastuvõtlikkusest rikkumistele, millega võivad kaasneda riskid isikuandmete omaniku eraelule ja tervisele.

Paljudel, peamiselt suure töötajate arvuga ettevõtetel on kasutusel siseveeb, mis on mõeldud töötajatele ettevõttesiseste uudiste, ürituste ja muu ettevõtet puudutava informatsiooni vahendamiseks. Tavaliselt sisaldab see ettevõtte kohta käivat teavet, mis ei ole mõeldud suuremale isikuteringile avalikustamiseks. Selleks infoks on näiteks ettevõtte strateegiad, ärisaladus ning töötajate andmed. Siseveebis kajastuv töötajate info peab olema toodud selles ulatuses, mis on piisav töölepingus sätestatud tööülesannete täitmiseks, näiteks töötaja ees- ja perekonnanimi, amet ning töötajaga ühenduse võtmiseks vajalikud andmed, milleks on e-posti aadress ja töötelefoni number. Muu töötajat puudutav teave, nagu sünniaeg või lapsehoolduspuhkusel viibimise aeg, võib siseveebis kajastuda ainult töötaja nõusolekul. Peab mainima, et igasugusele töötajale kuuluvale isiklikule informatsioonile, mis on ettevõtte käsutuses, peab olema tagatud juurdepääs ainult nendel kaastöötajatel, kelle töölepingus määratud tööülesanded eeldavad neile juurdepääsu. Näiteks raamatupidajale peavad olema kättesaadavad töötajate pangaandmed, kuna palga- ja muude hüvitiste arvestamine ja väljamaksmine kuulub raamatupidaja tööülesannete hulka.

Tööülesannete täitmiseks vajaliku töötajate vahelise suhtluse tagamiseks pakutakse igas ettevõttes vastavate kommunikatsioonivahendite kasutamise võimalus. Suhtlusvahendina kasutatakse eelkõige internetti, e-posti ja telefoni. Internetikasutus peab olema tagatud igas ettevõttes, kuna selle puudumisel muutuks võimatuks peaaegu kõikide tööülesannete täitmine. Interneti

kasutamine töökohal peab vastama tööülesannete täitmiseks püstitatud eesmärkidele. Töötaja internetikasutuse kohta andmete kogumise aluseks on eelkõige arvutisüsteemi turvalisus ja töötaja kontrollimine (Miidla-Vanatalu 2014, 9). Tööülesannete täitmist mittepuudutavate veebilinkide kasutamisel peab olema kõrvaldatud igasugune küberrünnakute võimalus. Eriti puudutab see raamatupidamist, kuna raamatupidaja tööülesannete hulka kuuluvad ka internetipangaga seotud toimingud ning tavaliselt on tegemist pangakontodel olevate suurte summadega, mida küberpetturid kalduvad petuskeemide abil aeg-ajalt omastama. Petuskeemide rakendamine on üsna levinud isiku- ja rahaliste andmete varastamise viis, milleks petturid kasutavad tihti e-posti. E-postiga saadetakse ohvritele linke mõne riigis tuntud asutuse nimel, nt pangalt ning palutakse seda vajutada ja sisse logida. Sisselogimisel varastatakse ohvri poolt sisestatud andmed, mida edaspidi kasutatakse tema kontolt raha äravõtmiseks. Seega on tähtis enne e-kirjas olevale lingile vajutamist kontrollida saatja e-posti aadressi ja vajaduse korral küsida eeldatavalt saatjalt kinnitust.

Põhiliselt toimub töötajate vaheline suhtlus e-posti teel. E-postiga saadetakse tööks vajalikke dokumente, infot ettevõttes käivatest muudatustest ja toimuvatest üritustest ning muud tööalast teavet. Raamatupidaja igapäeva töö hõlmab igasuguste andmete kogumist, töötlemist ja edasiandmist. Eriti tihti puutub ta kokku tundlike isikuandmetega, mille edastamine käib tavaliselt e-posti teel. Selliste andmete edastamiseks peab ettevõttes olema loodud kõrgtasemel andmekaitset tagav infosüsteem, et vältida igasugust väärtuslike andmete leket. E-postiga isikuandmete turvalisemaks edastamiseks nähakse üldmäärusega ette andmete krüpteerimine, mis tähendab andmete kindla algoritmiga salastamist ja loetavaks tegemist ainult piiratud isikuteringile, kes on omandanud õiguse nende töötlemisele. Ka tähtsamate dokumentide edastamisel rakendatakse mõningates ettevõtetes piiratud säilitamisega kirjade saatmist. Kiri koos tugevamat kaitset nõudva dokumendiga laekub postkasti ja säilib seal piiratud ajaks, näiteks kolmeks tunniks. Kirjas sisalduv dokument peab olema saaja poolt salvestatud selle aja jooksul, vastasel juhul ei ole see talle kättesaadav, kuna kiri kustutatakse kolme tunni möödumisel automaatselt.

Telefoni kasutamine on mugav ja lihtne viis tööalaste küsimuste lahendamiseks. Telefonikõnesid puudutavate andmete kogumine ja töötlemine on vajalik eelkõige telefoniarvete puhul. Telefoni isiklikes huvides kasutamisel peab töötaja hüvitama erakõnedele kulutatud summa, tööalaste kõnede eest maksab tööandja ise (*Ibid.* 2014, 8). Erakõnede maksumuse hüvitamiseks võib raamatupidaja töötajale kas arve väljastada või pidada kuupalgast kinni mittetööalastele kõnedele kulutatud summa. Tavaliselt on kasutusel teine variant.

Tänapäeval on üsna levinud kaugtöö kontseptsioon, mõni ettevõte võimaldab sellist tööviisi ka raamatupidajatele. Aeg-ajalt kodust või mujalt kui ettevõtte kontorist töötamine eeldab, et ettevõte tagab töötajale tööülesannete täitmiseks sülearvuti. Tavaliselt sisaldavad ettevõtte poolt välja antud tehnilised seadmed erinevaid kaitse- ja jälgimistarkvarasid, mis võimaldab hoida arvutisse salvestatud dokumendid ja andmed võimalikult turvalisena. Hoolimata sellest, kus asukohas töötaja oma tööd teeb, kas kontoris või kodus, peab ta igal juhul järgima ettevõtte sisse-eeskirjaga ettenähtud reegleid ja täitma töölepingusse märgitud kohustusi. Tööandja peab omakorda meeles pidama, et kui ta rakendab alluvate suhtes tehnoloogiaid, mis võimaldavad inimest jälgida (k.a videokaamerad), peab ta enne töösuhete loomist tulevast töötajat sellest teavitama ja jälgimist käsitletavad tingimused töölepingusse märkima.

Töötajaga töösuhete lõpetamisel on tööandjal lubatud hoida tema isikuandmed ettevõtte andmebaasis kümme aastat alates töösuhete lõpetamise kuupäevast. Kümne aasta möödumisel on tööandja kohustatud igasugune lahkunud töötajale kuuluv teave andmebaasist ära kustutama (TLS §5). Endisele töötajale kuuluv ettevõtte domeeniga e-post peab olema samuti kustutatud kas kohe pärast töölepingu lõppemist või teatud aja möödumisel, kui ettevõtte sisereeglitega on see ette nähtud. Lisaks ei ole tööandjal lubatud tutvuda lahkunud töötaja postkastis olevate e-kirjade sisuga, kuna see rikub töötaja õigusi eraelu puutumatusele.

Siinses alapeatükis käsitleti üldmääruse nõuete kajastamist raamatupidamises ja töösuhetes. Üldmääruse nõuete mõju raamatupidamisele tuleneb eelkõige sellest, et raamatupidaja ülesanded hõlmavad väärtuslike dokumentidega töötamist ning igasuguste rahaliste toimingute teostamist, milleks on nõutav isikuandmete töötlemine. Töösuhete loomine eeldab isikult ka tema isikuandmete kogumist ja töötlemist tulevasest töötajast pildi kujunemiseks, tema ametikohale sobivuse hindamiseks, tööülesannetest ja töökorralduslikest reeglitest kinnipidamise kontrollimiseks, palkade ja hüvitiste väljamaksmiseks jm, seega alluvad kõik need toimingud isikuandmete kaitse õigusaktidele. Isikuandmete turvalisuse tagamine on sama oluline nii raamatupidamises kui ka töösuhetes, kuna igal juhul ei tohi isikule kuuluvat konfidentsiaalset infot rikkuda ja ilma omaniku nõusolekuta teistele avalikuks teha.

2.2. Isikuandmete rikkumisest tulenev vastutus ja rikkumiste vältimiseks rakendatavad andmekaitsemeetmed

Üldmääruses on oluline koht isikuandmete rikkumist käsitletavatel punktidel. Isikuandmete rikkumise küsimus nõuab erilist tähelepanu, kuna nii rikutakse inimese õigust privaatsusele ja eraelu puutumatusele. Mõni ettevõte eirab isikuandmete kaitset puudutavaid nõudeid, mis tihti põhjustab andmete leket või muid rikkumisi. Magistritöö selles osas tuuakse välja info selle kohta, kuidas peavad andmetöötlejad käituma isikuandmete rikkumise korral, millised on trahvid seoses rikkumiste eiramisega ning milliseid kaitsemeetmeid on oluline rakendada nende vältimiseks tulevikus.

2.2.1. Isikuandmete rikkumisest teavitamine

Kõige suurem vastutus andmekaitseküsimustes on vastutava töötlejana esinevatel ettevõtetel. See on tingitud muuhulgas sellepärast, et lisaks isikuandmete töötlemise eesmärgi ja turvameetmete määramisele peavad nad tundma ka volitatud töötlejate kohustusi. Peab mainima, et volitatud töötlejate peamine kohustus on teostada seadusega kooskõlas olevat andmetöötlust ja teavitada õigeaegselt vastutava töötleja võimalikest rikkumistest.

Eestis kehtiva isikuandmete kaitse seaduse (edaspidi IKS) paragrahv 44 sätestab, et kui isikul, keda volitati tegema andmetöötlust, tundub, et tegemist on andmesubjektile võimalikku ohtu tekitava isikuandmete rikkumistega, peab ta kohe vastutavale töötlejale selle kohta teada andma. Vastutav töötleja on kohustatud omakorda teavitama sellest Andmekaitse Inspektsiooni 72 tunni jooksul. Enne teavitamist peab vastutav töötleja hindama isikuandmete rikkumisega kaasneva riski taset andmesubjekti suhtes. Kui tegemist on madala riskiga isiku õigustele ja vabadustele, siis pole Andmekaitse Inspektsiooni rikkumisest teavitamine kohustuslik. Kui aga vastutava töötleja hinnangul võib isikuandmete rikkumine oluliselt ähvardada omaniku elu, siis peavad nii Andmekaitse Inspektsioon kui ka andmesubjekt olema kohustuslikus korras rikkumisest teavitatud. Rikkumisest teavitamisel peab vastutav töötleja edastama infot isikuandmete rikkumise asjaoludest, rikkumiste võimalikest tagajärgedest ning nende leevendamiseks rakendatud meetmetest (Turk 2018). Hilisemal teavitamisel peab Andmekaitse Inspektsioonile esitama selle kohta põhjenduse.

Mõlema, st nii madalama kui ka suurema riskiga isikuandmete rikkumise puhul peavad olema rakendatud rikkumise kõrvaldamismeetmed. Kui vastutaval töötlejal ei õnnestunud iseseisvalt,

kasutades tema arvates sobivaid korralduslikke ja tehnoloogilisi meetmeid, parandada olukorda ehk isikuandmete rikkumist leevendada, siis on ta kohustatud andmesubjekti isikuandmete rikkumistest teavitama. Samas võib pöörduda Andmekaitse Inspekstisooni, kes hindab isikuandmete rikkumise raskust ja otsustab selle alusel, kas andmesubjekti teavitamine on vajalik või mitte.

Vastavalt IKS-i paragrahvile 45 võib isikuandmete rikkumistest teada anda kas hiljem või piiratud ulatuses või jätta üldse teavitamata, näiteks kui on tegemist võimaliku kuriteoga. Sel juhul ei ole isikuandmete rikkumisest teavitamine asjakohane, kuna see võib takistada kuriteo uurimist, avastamist ja kurjategija kinnipidamist. Sama tingimus kehtib, kui isikuandmete rikkumisest teadaandmine toob kaasa teisele isikule kuuluvate andmete rikkumist, ohtu riigi julgeolekule või avaliku korra kaitsele.

2.2.2. Üldmääruse rikkumise eest määratavad trahvid

Isikuandmete rikkumisega kaasneb üldmääruse nõuete rikkumine. Rikkumiste tähelepanuta jätmine ning nende kõrvaldamiseks vajalike meetmete mitterakendamine toob seaduse rikkujatele kaasa karistuse. Üldmäärus lubab liikmesriikides tegutsevatel järelevalveasutustel määrata trahvisumma ise. Eesti ettevõtetele laienevaid trahvi määramise tingimusi käsitletakse IKS-i paragrahvides 62, 67-69, 71 ja 72.

Vastavalt neis paragrahvides toodud tingimustele on võimalik vastutava ja volitatud töötleja kohustuste rikkumisel karistada nende ülesandeid täitvaid isikuid trahviga summas kuni 10 miljonit eurot. Sarnase rikkumise eest on juriidilisele isikule trahvisumma määramise tingimus sama või kuni 2% tema eelmise majandusaasta aastasest maailma kogukäibest sõltuvalt sellest, kumb summa on suurem. Isikuandmete töötlemise põhimõtete rikkumise puhul karistatakse veelgi suurema trahviga, mille summa võib olla kuni 20 miljonit eurot. Juriidilise isiku poolt andmetöötluse põhimõtete rikkumine võimaldab määrata talle trahvi summas, mis kujutab kuni 4% tema eelmise majandusaasta aastasest maailma kogukäibest. Sama trahvisumma määratakse, kui rikutakse isikuandmete edastamise korda, piiratakse Andmekaitse Inspektsioonile juurdepääsu rikutud andmetele või kui ignoreeritakse viimase korraldusi. Isikuandmete töötlemisel, mis ei ole aga üldmääruse nõuetega vastavuses karistatakse trahviga summas kuni 200 rahaühikut.

Üldmääruse jõustumisest möödunud pooleteise aasta jooksul on juba toimunud mõned trahvide määramise juhtumid. Neist kõige markantsemaks võib pidada Google-i juhtumit, keda 2019. aastal

Prantsusmaal tegutsev andmekaitseasutus karistas trahviga summas 50 miljonit eurot. Selle aluseks oli Google-i poolt inimestele ebapiisaval määral selgitatud andmetöötluse tingimused, k.a selle kohta, kuidas toimub andmete kogumine personaliseeritud reklaami kajastamiseks (Google hit with ... 2019).

2.2.3. Rikkumiste vältimist tagavad andmekaitsemeetmed

Üheks nõudeks, mis on kehtestatud vastutavale töötlejale seoses tema isikuandmete töötlemisega kaasneva laia vastutusalaga, on andmete turvalist töötlemist tagavate meetmete ja protseduuride kindlaksmääramine. Enne nende kasutusele võtmist tuleb kindlaks teha kaitseobjektid ja nende ulatus, teisisõnu andmed, mida tuleb kaitsta (Grove *et al.* 2018, 13). Eelkõige on tähtis tuvastada ettevõtte infosüsteemi salvestatud kriitilised andmed. Kriitilisteks andmeteks peetakse selliseid andmeid, mille võimalik leke tekitab ettevõttele suure rahalise kahju või isegi pankrotistumise ohu. Tavaliselt eristatakse kriitiliste andmetena sellist teavet, mis rõhutab ettevõtte ainulaadsust ja identiteeti, mis annab eelise konkurentide ees. Sellised andmed hõlmavad ka ettevõtte rahalisi ressursse (Pendley 2018, 54).

Igas ettevõttes on oluline tagada tõhus riskide jälgimine ning määrata terves ettevõttes kaitse tagamiseks vajalikke turvameetmeid rakendavad spetsialistid (*Ibid.* 2018, 13). Suuremates ettevõtetes luuakse tihti siseauditi osakond. Siseaudiitori ülesanne on olla objektiivne ja sõltumatu nõustaja küsimustes, mis puudutavad ettevõtte tegevust mõjutavate riskide analüüsimist ja maandamist (Aruste 2006, 15). Siseauditi abil määratakse ettevõtte eesmärkide saavutamiseks vajalikud juhtimis- ja kontrollimeetmed, antakse hinnangud nende efektiivsusele ja tulemuslikkusele ning hinnangute alusel tehakse järeldused meetmete sobivuse ja töökindluse kohta. Siseaudiitori pädevuses on esitada juhtkonnale aruanne koos oma hinnangutega ja nende alusel tehtud tähelepanekute ja järeldustega ning pakkuda olukorra paremaks muutmiseks vajalikke soovitusi (Eesti Siseaudiitorite Ühing ... 2002, 17). Kuna siseaudit mängib olulist rolli võimalike ettevõtte tegevusele kahju tekitavate riskide tuvastamisel ja nende kõrvaldamisel, on võimalik, et siseaudiitorid võiksid olla nõustajad andmetöötlusega tegelevate kaastöötajate jaoks.

Andmekaitsespetsialisti ja siseaudiitori Donna Gracey arvates võib siseaudit olla abikäsi üldmääruse nõuete mõistmisel. Samas võib see aidata tuvastada võimalikke ettevõtte tegevust ähvardavaid riske. Nende tuvastamiseks peab siseaudiitor teostama isikuandmete töötlemise ekspertiisi. Gracey sõnul on tähtis, et siseaudiitoril tekiks arusaam üldmääruse nõuetest, samuti peab ta oluliseks selgitada ettevõtte kõigile osakondadele üldmääruse nõudeid ja võimalikke kaasnevaid

riske (Internal Auditor ... 2018, 13). Siseaudiitoril on tähtis olla kursis kõigi isikuandmete kaitsega seotud uudistega, et võimalusel võiks ta aidata andmetöötlust teostavaid isikuid. Terve ettevõtte teadlikkus seaduslikust andmetöötlusest soodustab isikuandmete rikkumiste minimeermist.

Töötajate teadlikkuse tähtsust rõhutab ka Eestis tegutseva ettevõtte Grant Thornton Baltic IT-juht Arko Kurg (2019). Tema on seisukohal, et väärtuslike andmete kaitse tagamiseks ei peaks ettevõtted piirduma küberkaitset tagavatesse vahenditesse investeerimisega, nagu paljud kalduvad tegema. Seda kinnitavad ka Grant Thornton Baltic-u tehtud uuringu tulemused, millest selgub, et andmekaitse põhirõhk ainult uute küberturvalisuse tehnoloogiate sisseviimisele ei ole tegelikult efektiivne. Tema arvates peab töötajate andmekaitsealane ettevalmistus ja ettevõttes rakendatavad kaitsetehnoloogiad olema tasakaalus. Kurg pakkus võimalikuks lahenduseks lühikoolitusi. Siia võivad kuuluda näiteks kuni kaheminutiliste videote vaatamine andmekaitse teemal ning igasugused meeldetuletused andmekaitse tähtsusest (nt temaatilised postrid seintel, lühisõnumid arvutisse sisselogimisel jm), mis võimaldaksid töötajatel andmekaitse kohta käivat informatsiooni paremini meelde jätta.

IKS-i paragrahvis 43, mis on suunatud eelkõige vastutavale ja volitatud töötlejale, käsitletakse isikuandmete turvameetmeid, mida tasub rakendada võimalike rikkumiste vältimiseks. Selles paragrahvis sätestatu põhjal peavad mõlemad andmetöötlejad olema võimelised piirama juurdepääsu isikuandmetele kõigile, kes ei oma õigust nende töötlemisele, samas ära hoidma ükskõik millised isikuandmetega seotud omavolilised toimingud, sh isikuandmete sisestamine, nendega tutvumine ja muutmine. Lisaks on nende pädevuses tagada juurdepääs automatiseeritud töötlemistarkvara kasutajale ainult nende isikuandmete suhtes, mille puhul on lubatud automaatne andmetöötlus. Vastutav ja volitatud töötleja peavad olema võimelised tõendama ja kindlaks määrama isikud või asutused, kellele isikuandmete edastamine andmesidevahendite kaudu on tehtud ja/või lubatud teha. Peale selle peavad nad oskama tõendada ja tuvastada automatiseeritud andmetöötlussüsteemi sisestatud isikuandmeid ning nende sisestajaid. Väga oluline aspekt on andmetöötlussüsteemi korralik toimimine ning võimalike toimimisvigade esinemisel on kohustatud mõlemad andmetöötlejad operatiivselt nendest teada andma ja tagama nende kõrvaldamise. Ei tohi ka lubada isikuandmete moonutamist andmetöötlussüsteemi rikete tekkimisel.

Eespool mainitud asjaolud viitavad sellele, et inimesel on oluline roll turvalise andmetöötluse tagamisel. Töötajatel peab tekkima kindel arusaam võimalikest ohtudest, mis võivad kaasneda

näiteks e-kirjas oleva kahtlase manuse avamisega või kaitsmata faili allalaadimisega. Ettevõtted peavad tagama oma töötajatele soodsad tingimused andmekaitsealaste teadmiste omandamiseks. Viimased peavad omakorda kinni pidama ettevõttes kehtivatest sisemistest andmekaitse ja privaatsuse nõuetest. Vaatamata sellele, et inimfaktor avaldab märkimisväärset mõju isikuandmete korralikule töötlemisele, jäävad andmekaitse tagamisel oluliseks ka tehnilised vahendid.

Andmekaitse eeldab igas ettevõttes kvaliteetse infosüsteemi loomist. Peale selle on tähtis selle kõrgtasemel toimimine, millele aitavad kaasa pidevad uuendamised. Vananenud tarkvara versioonide kasutamine takistab tarkvara korrektset toimimist ning suurendab võimalusi sattuda küberrünnakute ohtu. Regulaarsed tarkvarauuendused aitavad analüüsida nii praeguseid kui ka võimalikke tulevasi isikuandmete lekke riske.

Kui ettevõte on otsustanud vahetada isikuandmete töötlemise laadi, nimelt võtta kasutusele uus töötlemistarkvara, soovitab Andmekaitse Inspektsioon sellisel juhul koostada kirjalik andmekaitsealane mõjuhinnang (Toomela *et al*. 2019). Mõjuhinnang on mõeldud eelkõige suurema riskiga isikuandmete töötlemise puhul. Selle läbiviimise vajadus on käsitletud üldmääruse artiklis 35. Andmekaitsealase mõjuhinnangu eesmärk on hinnata enne isikuandmete töötlemist kavandatavate andmetöötlustoimingute mõju isikuandmete kaitsele. Kirjalikus andmekaitsealases mõjuhinnangus peab olema toodud järgmine teave: kavandatud isikuandmete töötlemise eesmärgid ja toimingud, hinnang isiku õigusi ja vabadusi ohustavate võimalike riskide kohta ning nende käsitlemiseks kavandatud meetmed. Kui mõjuhinnangust selgub, et riskantsemate isikuandmete töötlemise toimingud võivad kujutada viimastele suurt ohtu, mida ei oleks võimalik kõrvaldada asjakohaste meetmetega, peab enne töötlemist nõu pidama Andmekaitse Inspektsiooniga (Isikuandmete töötleja üldjuhend).

Selleks, et inimese nõusolekust tuleneval isikuandmete edastamisel ei satuks need küberpetturite kätte, rakendatakse sellist kaitsemeedet nagu krüpteerimine. Andmete krüpteerimine kujutab endast protsessi, mille korral tehakse andmed kindla algoritmi abil suuremale isikuteringile loetamatuks ja kättesaadavaks ainult nende saajale. Isikuandmeid ei ole võimalik võõral isikul lugeda, kuna need on salastatud suvaliste sümbolitega. Andmete krüpteerimisel ning nende edaspidisel edastamisel kontrollitakse seda, et krüpteeritud andmed oleksid üleandmise käigus kättesaadavad ainult tegelikule saajale. Samuti vaadatakse üle parameetrid, mis määravad kindla rakendatava algoritmi. Sellega tagatakse tegeliku saaja arusaam krüpteeritud andmete sisust

(Pendley 2018, 54-55). Tihti krüpteeritakse tundlikke isikuandmeid nagu makseandmed, isikut tuvastavad andmed või klientide, hankijate ja töötajate isiklik teave.

Lisaks krüpteerimisele mainitakse üldmääruses sellist turvameedet nagu andmete pseudonümiseerimine. Pseudonümiseerimisega on võimalik määrata isikuandmete seos konkreetse isikuga vaid juhul, kui on olemas isiku kohta käiv lisateave, mis peab olema kaitstud ja avalikult kättesaamatu. Praegu muutub pseudonümiseerimine tänapäevaste elektrooniliste tuvastamissüsteemide seas kui konfidentsiaalsuse suurendamise meetod üha populaarsemaks, mis võib märkimisväärselt vähendada isikunandmete kuritarvitamise riske (Salmony 2018, 42-43).

Parooliga kaitsmise vajadust peetakse oluliseks kasutaja autentimise vormiks nii internetis kui ka ettevõtte sisemistes arvutisüsteemides. Paroolid peavad olema keerulised ja sisaldama tähtede kombinatsiooni (suur- ja väiketähed) ning numbreid, võimaluse korral ka tähemärke. Identiteedivarguse ohu minimeerimiseks tuleb vahetada paroole vähemalt iga kolme kuu tagant.

Paljud ettevõtted kasutavad dokumentide salvestamiseks ja edastamiseks pilvehoidlat. Failide salvestamine pilvehoidlasse on mugav, kuna see tagab ettevõttele märkimisväärse aja ja kulude kokkuhoiu. Lisaks annab pilvehoidla kasutamine isikuandmetele juurdepääsuga töötajatele võimaluse kasutada ühiseid ressursse. Paraku ei taga pilvehoidlate kasutamine dokumentide hoidmisel 100% turvalisust. Seega peavad nende kasutajad arvestama võimaliku andmete kadumise riskiga. Andmete lekke ohu vähendamiseks on vaja piirata administraatoriõigusi ja kasutada administratiivkontosid ainult vastavalt vajadusele. On väga oluline, et pilvehoidlas olevate dokumentide kättesaadavus oleks kontrollitud ja tagatud ainult neile, kel on õigus nendes sisalduvaid andmeid kasutada ja töödelda. Pilvehoidlasse salvestatud andmed peaksid võimalikult sageli läbima automaatse varundamise protseduuri. Võimalikult suurema turvalisuse tagamiseks peab kaitsemeetmena rakendama isikuandmete krüpteerimist, autoriseerimist ja autentimist. VPN-iga serveri sisslogimisel on soovitav kasutada kahe-astmelist autentimist. Kõiki eelnimetatud meetmeid tuleb iga aasta uuesti hinnata, et kõrvaldada igasugune andmete lekke risk (Jakimoski 2016, 49, 53, 54).

Nagu sellest magistritöö osast järeldub, on olemas palju andmekaitsemeetmeid. Nende kombineerimisel on võimalik saavutada andmete võimalikult suurem ohutu kasutamine ja minimaalsem andmete lekke risk. Samuti on oluline meeles pidada, et isikuandmete kasutamist ja edastamist tuleks teostada ainult vajaduse korral ning nende töötlemine peaks vastama

konkreetsele eesmärgile. Kõigi nende aspektide arvestamine suurendab võimalusi vältida isikuandmetega seotud rikkumisi.

2.3. Uuring Rumeenia arvestusala spetsialistide teadlikkusest üldmääruse nõuetest

Muudatused isikuandmete kaitse nõuetes puudutavad kõiki Euroopa Liidu liikmesriike. Selleks riigiks on ka Rumeenia, kes on Euroopa Liidu liikmesriik alates 2007. aastast. Üldmääruse vastuvõtmisega tehti 2017. aastal läbiviidud uuring, mille eesmärk oli teha selgeks Rumeenia raamatupidajate ja audiitorite (edaspidi arvestusala spetsialistid) teadlikkus 2018. aastal Euroopas kasutusele võetava üldmääruse nõuetest (Stanciu, Rîndaşu 2018, 5-8). Uuringu tegemiseks kasutati kvantitatiivset uurimismeetodit ehk koostati küsimustik. Küsitlusest võttis osa 109 arvestusala spetsialisti.

Siinses alapeatükis käsitletakse Rumeenias tehtud uuringu käigus esitatud küsimusi ning nende vastustest saadud tulemusi, mida edaspidi võrreldakse magistritöö autori uuringu tulemustega, et saada ülevaade teadlikkuse muutustest.

Tulemuste võrdlemiseks võttis autor uuringust aluseks viis küsimust, mille sõnastus oli järgmine:

1. Kas Teie puutute isikuandmete töötlemisega kokku igapäevaste tööülesannete täitmisel?
2. Kas Teie teate uue üldmääruse kasutuselevõtmisest?
3. Kas ettevõtte juhtkond teavitas Teid uue üldmääruse jõustumisest?
4. Kas Teie olete seoses üldmääruse vastuvõtmisega oma igapäevased toimingud üle vaadanud ja ära parandanud?
5. Milliseid andmekaitsemeetmeid rakendatakse Teie ettevõtetes?

Kõigepealt küsiti Rumeenia arvestusala spetsialistide käest teiste isikute isiklike andmete (ees- ja perekonnanimi, panga- ja isikut tõendavad andmed) töötlemisega kokkupuute kohta. Selgus, et 83% vastanuid tegelevad iga päev isikuandmete töötlemisega.

Üks tähtsamaid küsimusi oli Rumeenia arvestusala spetsialistide teadlikkus uuest regulatsioonist. Uuringust selgus, et vaid 61,5% vastanuid olid sellest muudatusest teadlikud. Samuti selgus, et 35% vastanutest, kes tegelevad oma igapäevases töös isikuandmete töötlemisega, ei olnud

üldmäärusest enne uuringust osavõtmist üldse teadlikud. Samal ajal 44% vastanuid, kelle igapäevased tööülesanded ei hõlma isikuandmete kasutamist, näitasid oma teadlikkust.

Vastanutele esitati küsimus, millega sooviti selgeks teha ettevõtte juhi panus Rumeenia arvestusala spetsialistide teadlikkusesse uue üldmääruse rakendamisest. Vastused näitasid, et enamik uuringus osalejaid ei tea, kas neid informeeritakse selle kohta või mitte (*ca* 41%), ligikaudu 35% on sellest juba teavitatud ning ülejäänud 24% arvavad, et neid viiakse selles küsimuses kurssi varsti. Selline vastuste jagunemine viitab ettevõtete juhatuse mittetõsisele suhtumisele andmekaitsenõuete muudatustesse. Juhid peaksid mõistma, milliseid probleeme võib tuua nõuete eiramine. Üldmääruse rikkumine näeb ette suuri trahvisummasid.

Rumeenia arvestusala spetsialistidele esitati küsimus ka selle kohta, kas nad on juba hakanud tuvastama igapäevastesse tööülesannetesse kuuluvaid toiminguid, mis lähevad hiljuti jõustunud üldmääruse reguleerimise alla. Vastustest selgus, et umbes 53% vastanuid on juba alustanud uutele nõuetele alluvate toimingute tuvastamist, ülejäänud sellega veel tegelenud ei ole.

Uuringu raames küsiti meetmete kohta, mida arvestusala spetsialistid rakendavad tööülesannete turvalisemaks täitmiseks. Enamus märkis vastuseks sagedast paroolide vahetamist, teiseks levinud valikuks osutus erinevate paroolide loomine. Väiksem osa vastanuid skaneerib e-postiga saadetud dokumente ja faile ning kõige vähem märgiti, et krüpteeritakse e-posti teel saadetavad failid. Uuringu autorid leidsid, et Rumeenia arvestusala spetsialistidel puudub täielik arusaam isikuandmete kaitse olulisusest.

Alapeatükis käsitletud uuringu tulemustest võib järeldada, et Rumeenia arvestusala spetsialistid ei olnud kõrgel tasemel teadlikud 2018. aasta maikuus kasutusele võetud üldmääruse muudatustest. See on tingitud eelkõige ettevõtete juhtide passiivsusest personali informeerimisel. Juhid avaldavad olulist mõju ettevõtte töötajatele ning peavad olema pädevad ettevõtlusega seotud muudatuste suhtes ning valmis neist muudatustest alluvaid teavitama. Ettevõte on nagu inimorganism, mille organid ehk allüksused ja organite rakud ehk seal töötavad inimesed on omavahel seotud, sest nad teevad tööd ühiste eesmärkide täitmiseks. Seega iga ettevõtte koosseisu kuuluv inimene peab olema kursis ettevõttes toimuvaga ning ettevõtet ja oma tööülesandeid puudutavate tahkudega. Uuring korraldati Rumeenias mitu kuud enne muudetud üldmääruse vastuvõtmist, seega oli uuringu tegijatel lootus, et Rumeenias töötavatel arvestusala spetsialistidel

on veel aega uute andmekaitsenõuete õppimiseks ja juhtidel jõustunud muudatustest personali teavitamiseks.

3. ISIKUANDMETE KAITSE EESTI RAAMATUPIDAJATE JA TEISTE ARVESTUSALA SPETSIALISTIDE PILGU LÄBI

Magistritöö selles osas vaadeldakse autoripoolse uuringuga Eesti arvestusala spetsialistide teadlikkust üldmääruse kohta. Siia kuulub küsimustiku vastuste analüüsimine, tulemuste tabelitena/joonistena esitamine ja nende tõlgendamine. Peale selle võrreldakse arvestusala spetsialistide üldmäärusest informeerituse taset kaks aastat tagasi (Rumeenias 2017) ja praegusel hetkel (Eestis 2019).

3.1. Kvantitatiivne uuring

3.1.1. Ülevaade kvantitatiivsest uuringust

Uuringu praktilise osa jaoks loodi küsimustik, mis hõlmas isikuandmete kaitset ja seda puudutavat üldmäärust käsitlevaid küsimusi. Küsimused koostati magistritöö teoreetilise osa põhjal, samas mõni neist võeti Rumeenias tehtud uuringust, et edaspidi tulemusi võrrelda. Autori uuringust võttis osa 68 inimest. Uuringu sihtrühmaks märkis autor inimesed, kelle ametiks oli kas raamatupidaja või muu arvestusala spetsialist (edaspidi arvestusala spetsialist). Muudeks arvestusala spetsialistideks on uuringu raames näiteks finantsjuht, kontroller, arvelduspetsialist, raamatupidamisassistent, lisaks arvestuse erialal õppivad üliõpilased või praktikandid. Uuringusse panustasid ka teised spetsialistid, kel on arvestusega kas vähem kokkupuudet võrreldes eespool nimetatud uuringus osalejatega või nende amet ei ole küsimustikus olevate ametinimetuste hulgas mainitud. Küsitlus oli avatud ajavahemikus 5. november kuni 30. november 2019. Küsimustikuks kasutati veebipõhist küsitluste koostamise vahendit Google Forms nii eesti keeles kui ka tõlkes vene keelde, seda levitati sotsiaalvõrgustike kaudu ning saadeti ettevõtetele e-posti teel. Küsimustik on toodud lisas 1.

Küsimustikus on kuus taustaküsimust (vt lisa 3) ning 11 teemakohast küsimust. Küsimustik oli anonüümne ning vastusevariantidega, vastamisel oli võimalik valida kas üks või mitu vastust. Lisaks paluti uuringus osalejaid hinnata viiepalliskaalal, mis uuringu tulemuste analüüsimise

käigus kohandati Likerti viiepalliskaalale, kui nõus on nad küsimustikus toodud 15 väitega. Esimene osa väiteid puudutas üldmääruse põhilisemaid nõudeid, teise ossa kuuluvad väited olid seotud vastutava ja volitatud töötleja kohustustega.

Enamik küsimustele vastanuid kuulus pea- või vanemraamatupidaja ametisse (34%), järgnesid raamatupidajad (32%), arveldusspetsialistid (9%), finantsjuhid või kontrollerid (6%), raamatupidamisassistendid (4%) ning arvestusala üliõpilased või praktikandid (1%). Lisaks osalesid uuringus ka muud spetsialistid, kelleks olid finantsanalüütikud, audiitor, arvestusala osakonnajuht, kontoriassistent, arveldussüsteemi spetsialist, personali peaspetsialist ning tegev- ja firmajuht. Viimased moodustasid 14% kogu vastanute arvust. Kõigi eelnimetatud spetsialistide arvamus, k.a nende, kel on arvestusega vähem seost, on autori jaoks väga tähtis, kuna nende ülesannetesse kuuluvad üldjuhul ka igasugused isikuandmetega seotud toimingud.

Küsimustikule vastanute seas oli naisi 96% ning mehi 4%. Küsimustiku täitis 1% inimest vanuses kuni 20 aastat, 22% vanuses 21–30 aastat, 25% vanuses 31–40 aastat, kõige rohkem vastajaid ehk 34% oli vanuses 41–50 aastat ning 18% olid üle 51-aastased. Uuringust osavõtjatel paluti märkida ka haridustase. Vastustest selgus, et 21% vastanuid oli kutseharidusega, peaaegu pool (49%) bakalaureusekraadiga ning 31% magistrikraadiga. Vastanute seas doktorikraadiga spetsialiste ei olnud.

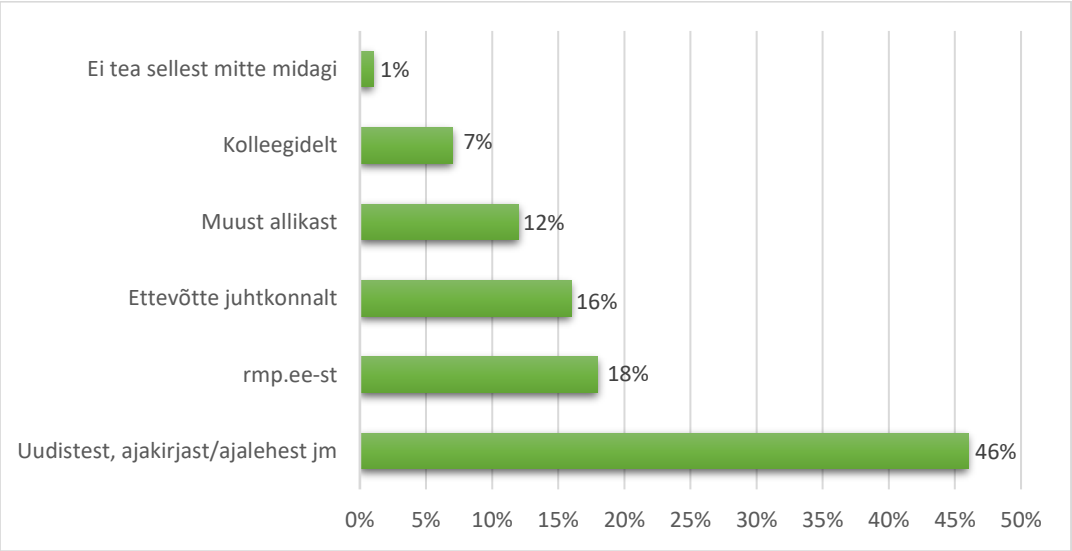
Vastanute käest küsiti ka nende tööstaaži arvestusala spetsialistina. Kõige rohkem ehk 33% oli kuni 4-aastase tööstaažiga, 19% on töötanud 5–10 aastat, 13% 11–14 aastat, 10% 15–20 aastat ning neljandiku ehk 25% vastanute tööstaaž oli enam kui 20 aastat.

Lisaks paluti uuringust osavõtjail märkida ettevõtte suurus, kus nad hetkel töötavad. Nendest 26% kuuluvad mikro-, 32% väike-, 18% kesk- ning 24% suurettevõtete hulka.

3.1.2. Küsitluse kaudu saadud vastuste analüüs ja tulemuste tõlgendamine

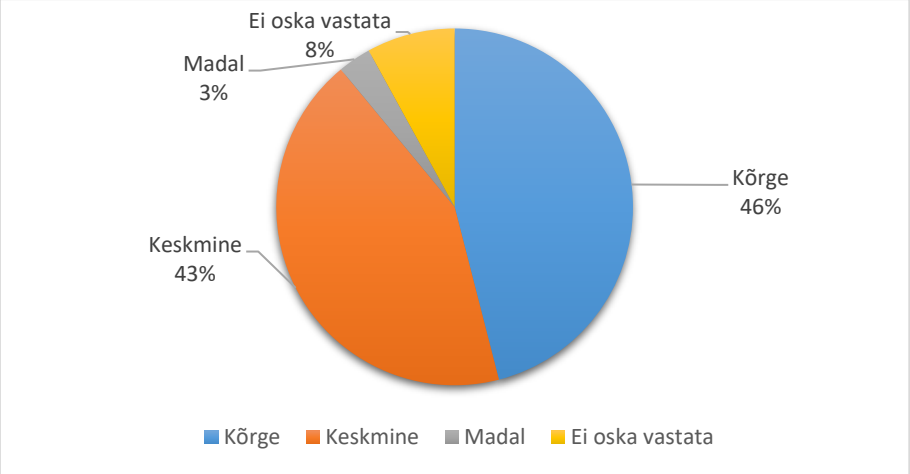
Küsitluse esimese küsimusega soovis autor teada saada, kas uuringust osavõtjad on teadlikud 25. mail 2018 jõustunud üldmäärusest või mitte. Vastused näitasid, et enamik ehk 99% on selle kohta kuulnud ning vaid 1% ei olnud. Järgnev küsimus käsitles allikaid, kust saadi teada uue üldmääruse kasutusele võtmisest. Selgus, et suurem osa vastanuid ehk 46% said infot uudistest või ajakirjast-ajalehest, 18% lugesid sellest raamatupidamis- ja maksuinfoportaalist (rmp.ee), 16% teavitas

juhtkond, 12% said teada muust allikast, 7% kolleegide käest ning 1% märkis, et ei tea üldmääruse kohta mitte midagi. Vastuste jaotus on toodud joonisel 1.



Joonis 1. „Kuidas Teie saite teada uue isikuandmete kaitse seaduse vastuvõtmisest?“
Allikas: Autori koostatud Lisa 2 alusel

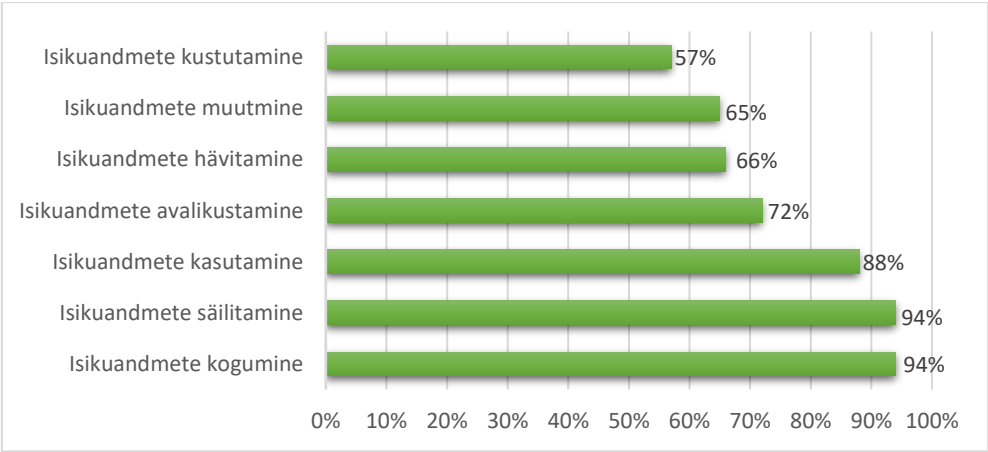
Autor esitas uuringus osalejatele küsimuse, mis puudutas nende arvamust andmekaitse taseme kohta ettevõtetes, kus nad töötavad. Enamik vastanuid ehk 46% hindab andmekaitse taset oma ettevõttes kõrgelt, 43% hindab olukorda keskmise tasemega, 3% vastanute arvates on tase madal ning 8% ei osanud sellele küsimusele vastata. Vastuste alusel võib järeldada, et suurem osa Eesti ettevõtteid on kas kõrge või keskmise andmekaitsetasemega, mis on üsna positiivne näitaja, kuna see viitab Eesti ettevõtete hoolivale suhtumisele andmekaitsesse (vt joonis 2).



Joonis 2. „Milline on Teie arvates andmekaitse tase Teie ettevõttes?“
Allikas: Autori koostatud Lisa 2 alusel

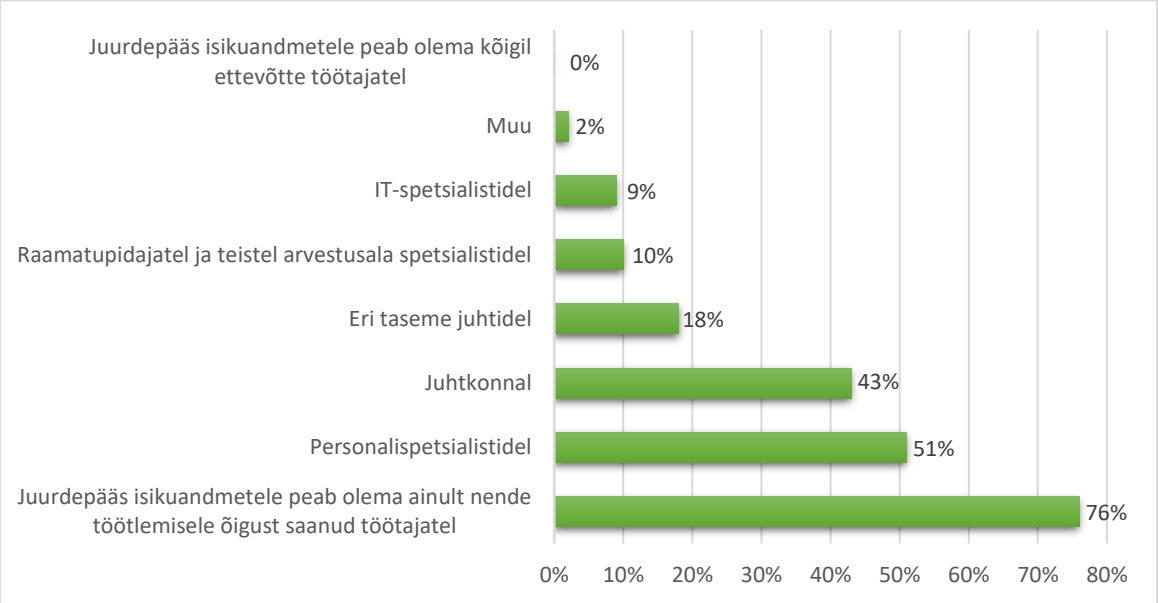
Üldmääruse nõuded avaldavad suurt mõju isikuandmete töötlemisele, mis on enamiku arvestusala spetsialistide ülesannete lahutamatu osa. Seetõttu küsis autor uuringus osalejatelt, kuidas mõistavad nad definitsiooni „isikuandmete töötlemine“. Sellele küsimusele vastamisel oli võimalik valida mitu vastusevarianti, milleks oli isikuandmete kogumine, säilitamine, hävitamine, kasutamine, avalikustamine, muutmine ja kustutamine. Vastuste protsentuaalne jaotus on toodud joonisel 3. Sellest on näha, et enamik vastanuid nimetas kolme põhilise isikuandmete töötlemise teguri seas isikuandmete kogumist (94%), säilitamist (94%) ja kasutamist (88%). Uuringust osavõtjatest 72% valisid vastuseks isikuandmete avalikustamise, 66% isikuandmete hävitamise, 65% isikuandmete muutmise ning 57% isikuandmete kustutamise. Tegelikkuses iseloomustavad kõik eespool nimetatud tegurid isikuandmete töötlemist. Peab mainima, et kõik seitse vastusevarianti valisid 68 vastanust 33, mis moodustab ligikaudu 49% vastanute osakaalust.

Osalejatel paluti ka märkida, kui tihti nad isikuandmete töötlemisega tegelevad. Selgus, et 44% spetsialistidest teevad seda iga päev, suurem osa ehk 50% tegelevad isikuandmete töötlemisega aeg-ajalt ning 6% märkis, et nad ei puutu isikuandmete töötlemisega kokku. Autori arvates sai eelmisele küsimusele vastuste jagunemise põhjuseks arvestusala spetsialistide ebaõige arusaam isikuandmete töötlemise mõistest. Sellele viitas ka asjaolu, et 6% neid, kes vastasid küsimusele isikuandmete töötlemissageduse kohta, et nad ei puutu isikuandmete töötlemisega üldse kokku, kuigi kõigi nende ametiks on kas raamatupidaja või pea/vanemraamatupidaja, kes üldjuhul töötlevad isikuandmeid mõningate tööülesannete täitmiseks. Vaatamata isikuandmete töötlemise definitsiooni ebatäielikule mõistmisele, hindasid kõik uuringus osalejad isikuandmete töötlemise turvalisust piisavalt kõrgelt. Nende keskmiseks hinnanguks kujunes 3,65 palli.



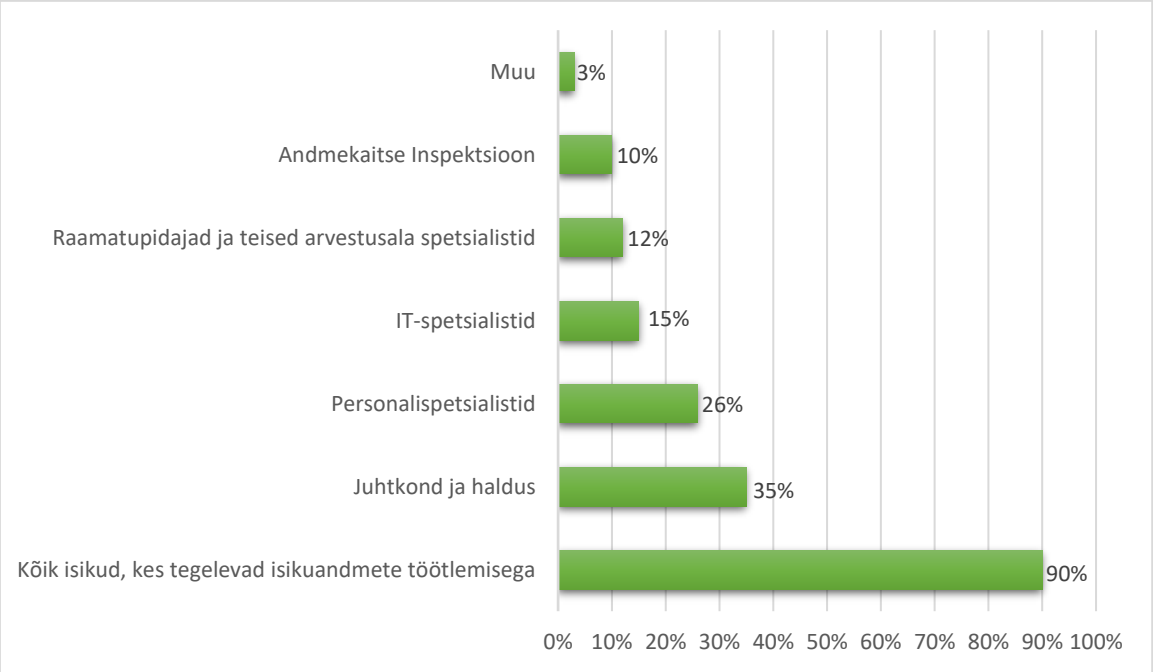
Joonis 3. „Mis hõlmab Teie arvates isikuandmete töötlemist?“
Allikas: Autori koostatud Lisa 2 alusel

Arvestusala spetsialistidelt küsiti nende arvamust selle kohta, kellele peaks olema tagatud juurdepääs ettevõtte kasutuses olevatele isikuandmetele – kas juhtkonnale, eri taseme juhtidele, personalispetsialistidele, IT-spetsialistidele, arvestusala spetsialistidele, kõigile töötajatele või ainult neile, kes sai õiguse isikuandmete töötlemiseks. Vastamisel oli võimalik märkida mitu varianti ning lisaks pakkuda oma vastus. Tulemused on esitatud joonisel 4, kust on näha, et enamik ehk 76% arvab, et isikuandmed peavad olema kättesaadavad ainult nende töötlemisele õiguse saanud isikutele, mis on õige ka üldmääruse kohaselt. Natuke rohkem kui 50% vastanuid on arvamusel, et isikuandmetele saavad ligi pääseda personalispetsialistid, 43% märkisid vastuseks juhtkonna, 18% eri taseme juhid, 10% raamatupidajad ja muud arvestusala spetsialistid ning 9% IT-spetsialistid. Väga positiivseks näitajaks peab autor seda, et mitte keegi ei valinud vastust „Juurdepääs peab olema kõigil ettevõtte töötajatel“, mis oleks olnud täiesti vale. Muu variandina pakuti andmekaitsespetsialisti ning üks uuringus osaleja märkis, et see sõltub sellest, kellele isikuandmed kuuluvad, kas töötajatele või klientidele. Selle küsimuse esitamisel eeldas autor, et valdav osa valib vastusena „Juurdepääs isikuandmetele peab olema ainult nende töötlemisele õigust saanud töötajatel“, mis tegelikkuses vastas tema ootustele, kuna see on päris õige. Nendel, kes märkisid vastuseks juhtkonna, eri taseme juhid või kellegi eelnimetatud spetsialistidest, on tegelikult samuti mingil määral õigus, kuid tulenevalt üldmääruse nõuetest nendele, nagu igale teisele ettevõtte töötajale, peab olema tagatud juurdepääs isikuandmetele sellel määral, mis on ette nähtud töölepingus sätestatud tööülesannete täitmiseks.



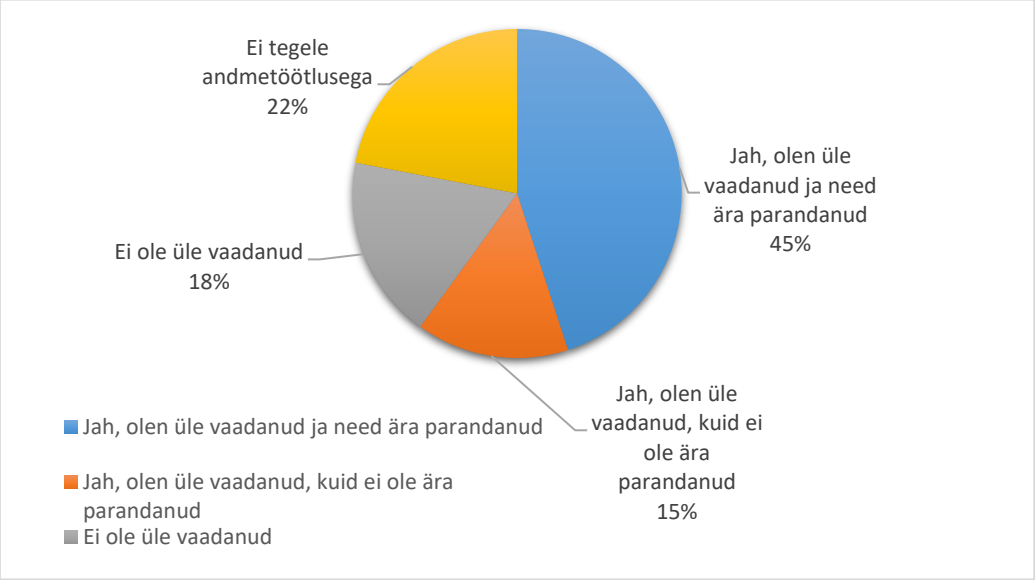
Joonis 4. „Kellel Teie arvates peab olema juurdepääs isikuandmetele ettevõttes?“
Allikas: Autori koostatud Lisa 2 alusel

Uuringus osalejatelt küsiti isikuandmete turvalise töötlemise eest vastutava isiku kohta. Vastusevariantideks pakkus autor raamatupidajaid ja teisi arvestusala spetsialiste, IT-spetsialiste, juhtkonda ja haldust, personalispetsialiste, Andmekaitse Inspektsiooni ning isikuid, kes tegelevad andmetöötlusega ettevõttes. Vastanutel oli lubatud märkida mitu vastust ning lisaks oli võimalik pakkuda midagi ka ise. Uuringus osalejatest 90% on arvamusel, et isikuandmete turvalise töötlemise eest peavad vastutama kõik ettevõtte töötajad, kes tegelevad isikuandmete töötlemisega, 35% vastanutest tundub, et vastutavad juhtkond ja haldus, 26% valisid vastuseks personalispetsialistid, 15% IT-spetsialistid, 10% Andmekaitse Inspektsiooni ning 3% pakkusid oma varianti, milleks oli andmekaitsespetsialist (vt joonis 5). Nagu eelmise küsimuse puhul, valis valdav osa vastanuid tõele kõige lähedasema variandi. Isikuandmete turvaline töötlemine tähendab igasuguste isikuandmetega kaasnevate toimingute teostamist, mis on vastavuses üldmääruse nõuetega ning mille puhul rakendatakse asjakohaseid turvameetmeid. Kõik vastusevariantidena toodud spetsialistid puutuvad kas aeg-ajalt või iga päev isikuandmetega kokku, seega on nende kohustus tagada andmete turvaline töötlemine. Ainult Andmekaitse Inspektsiooni roll andmetöötluses on erinev. Andmekaitse Inspektsiooni üks peamisi kohustusi isikuandmete kaitse suhtes on jälgida, et kõik need, kel on isikuandmetega pidev kokkupuude, tagaksid isikuandmete töötlemise viisil, mis on kooskõlas üldmääruse nõuetega.



Joonis 5. „Kes Teie arvates peab vastutama turvalise isikuandmete töötlemise eest?“
Allikas: Autori koostatud Lisa 2 alusel

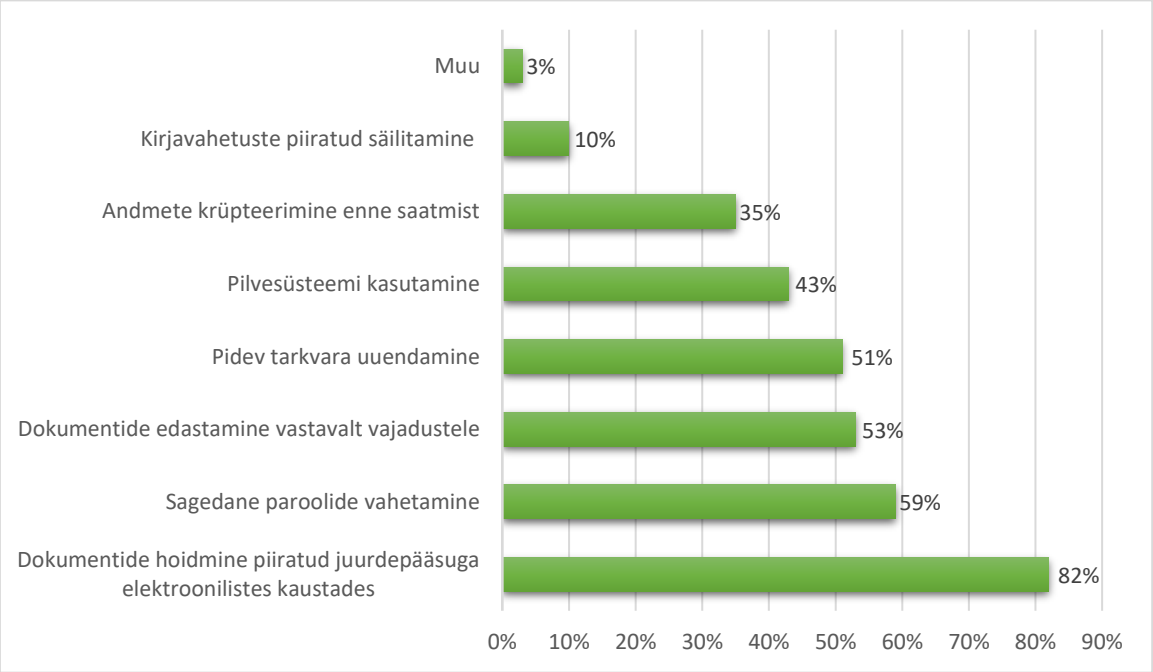
2018. aastal muutusid üldmääruse jõustumisega isikuandmete kaitset puudutavad nõuded rangemaks, mis sundis isikuandmete töötlemisele vaatama nii-öelda teise nurga alt. Seetõttu esitati uuringu raames arvestusala spetsialistidele küsimus „Kas Te olete seoses uue isikuandmete seaduse vastuvõtmisega oma andmetöötlusega seotud toimingud üle vaadanud?“. Vastanutest suurem osa (45%) oli isikuandmeid puudutavad toimingud üle vaadanud ja neid parandanud, 15% vastanuid ainult vaatasid üle, kuid ei parandanud, 18% uuringus osalejaid ei ole neid üle vaadanud ega parandanud ning 22% vastasid, et ei tegele andmetöötlusega (vt joonis 6). Vastustest on näha päris suur andmetöötlusega mittetegelevate spetsialistide osakaal, mis tundus eelmiste küsimuste vastuste analüüsimisel olevat madalam. Nagu juba varem mainitud, võib see olla tingitud arvestusala spetsialistide ebapiisavast arusaamast isikuandmete töötlemise definitsiooni kohta, mistõttu ei saa nad tõenäoliselt objektiivselt oma tööülesannete seas isikuandmete töötlemist hõlmavaid toiminguid tuvastada. Samas peab rõhutama, et kuigi isikuandmetega kaasnevate toimingute ülevaatamise ja parandamisega tegeles enamik ehk peaaegu pool vastanutest, tundub, et Eesti arvestusala spetsialistid ei suhtu isikuandmete turvalisusesse ega üldmääruse nõuetesse tarviliku tõsisusega. Autori arvates võiks toimingute ülevaatamise ja parandamisega tegelenud spetsialiste olla rohkem.



Joonis 6. „Kas Teie olete seoses uue isikuandmete seaduse vastuvõtmisega oma andmetöötlusega seotud toimingud üle vaadanud?“
Allikas: Autori koostatud Lisa 2 alusel

Liikudes isikuandmete turvalisuse teema juurde, oli uuringu raames tähtis välja selgitada, milliseid isikuandmete kaitse meetmeid rakendatakse vastanute ettevõtetes (tulemused on toodud joonisel 7). Vastusevariandid ja osakaalud olid järgmised: sagedane paroolide vahetamine (59%), pidev

tarkvarauuendamine (51%), dokumentide edastamine vastavalt vajadusele (53%), pilvesüsteemi kasutamine (43%), andmete krüpteerimine enne saatmist (35%), dokumentide hoidmine piiratud juurdepääsuga elektroonilistes kaustades (82%) ning kirjavahetuste piiratud säilitamine (10%). Uuringus osalejatel pakuti märkida ka oma vastusevariandid (3%). Muudeks variantideks pakuti töötajate nimede asemel koodide kasutamist, vajaduspõhiste dokumentide ja andmete krüpteerimist enne edastamist (mis on põhimõtteliselt seotud vastusevariandiga „andmete krüpteerimine enne saatmist“) ning üks vastanu märkis, et see on salastatud info, mis ei kuulu jagamisele. Kõige suurem osa vastanuid valis variandiks dokumentide hoidmise piiratud juurdepääsuga elektroonilistes kaustades, mis on tegelikult üsna turvaline, sest ei luba võõrastel tähtsatele andmetele ja dokumentidele ligi pääseda. Paroolide sagedast vahetamist peetakse samuti heaks kaitsemeetmeks ning soovitatakse seda teha vähemalt iga kolme kuu tagant ning nende vahetamisel kasutada keerulisi, kuid samal ajal kasutajale meeldejäävaid kombinatsioone. Kvaliteetne ja pidevalt uuendatav tarkvara on üks võtmetegureid isikuandmete kaitses, sest kiirest tehnoloogiaarengust tulenev kasvav vajadus tõhusamale kaitsele nõuab ettevõtete infosüsteemidelt enam läbimõeldud andmekaitselahendusi.



Joonis 7. „Millised andmekaitse meetmed Teie ettevõttes rakendatakse?“
Allikas: Autori koostatud Lisa 2 alusel

Lisaküsimusena esitati küsimus andmete kohta, mis kuuluvad tundlike isikuandmete hulka. Variantideks oli isikuandmed, mille avalikustamine võib kahjustada isiku elu ja tervist, poliitilised vaated ja usulised veendumused, terviseandmed, makse- ja krediitkaardiandmed ning isiku

tuvastamiseks vajalikud biomeetrilised andmed. Enamus (96%) märkis vastuseks esimese variandi, 93% valis terviseandmed ning 82% makse- ja krediitkaardiandmed. Andmekaitse Inspektsiooni veebilehel oleva isikuandmete liigituse kohaselt ongi kõik eelnimetatud andmed tundlikud isikuandmed. Vastusevariandid „poliitilised vaated ja usulised veendumused“ ning „isiku tuvastamiseks vajalikud biomeetrilised andmed“ valis uuringust osavõtjatest vastavalt 53% ja 72%. Neid andmeid ei peeta tundlikeks isikuandmeteks, vaid neid seostatakse eriliigiliste isikuandmetega.

Magistritöö eesmärk on selgeks teha raamatupidajate ja teiste arvestusala spetsialistide teadlikkus isikuandmete kaitsest ja seda puudutava üldmääruse nõuetest. Eesmärgi saavutamiseks palus autor uuringus osalejatel hinnata, mil määral on nad nõus küsimustikus toodud 15 väitega, millest üheksa puudutasid üldmääruse nõudeid ning kuus käsitlesid vastutava ja volitatud töötleja kohustusi. Need väited ja neile antud hinnangud on toodud lisades 4 ja 5. Vastuste analüüsimisel kohandati küsitluses kasutatud skaala Likerti viiepalliskaalale, kus 1 – „ei ole üldse nõus“ , 2 – „pigem ei ole nõus“, 3 – „pigem olen nõus“, 4 – „olen täiesti nõus“ ning 5 – „ei oska vastata“.

Esimene väide puudutas üldmääruse eesmärki, mis seisneb andmesubjektile isikuandmete töötlemise eesmärkidest teabe kättesaadavuses. Uuringus osalejad hindasid seda kõrgelt (3,38), mis tähendab, et selle väitega ollakse pigem nõus. Tegelikkuses on neil õigus, kuna üldmääruse vastuvõtmise üks peamisi eesmärke ongi tagada andmesubjektidele õigus tutvuda enda kohta käivate isikuandmete töötlemise eesmärkide, andmetöötlejat puudutava info ning meetmetega. Sellele toetub ka üks isikuandmete kaitse põhimõtteid, milleks on läbipaistvus.

Järgmisena esitatud väide käsitles isikuandmete dokumenteerimise kohustuse puudumist. Keskmine hinnang sellele kujunes 1,58 ehk vastanud ei ole sellega nõus. See on õige, kuid selline tingimus puudutab eelkõige ettevõtteid, kus töötab üle 250 inimese. Isikuandmete töötlemise dokumenteerimine on nõutav, sest isikuandmete võimalike rikkumiste puhul võib see osutuda abivahendiks rikkumiste leevendamisel. Samuti peavad andmetöötlejad olema valmis esitama Andmekaitse Inspektsioonile isikuandmete töötlemise dokumentatsiooni, ka on andmesubjektidel õigus neilt küsida enda kohta käivate isikuandmete töötlemist puudutavaid dokumente.

Autor palus vastanuid hinnata väidet „Enne isikuandmete töötlemist peab saama sellele nõusoleku andmesubjektilt“. Väide sai hinnangu 3,64, mis pigem vastab vastusevariandile „Olen täiesti nõus“. Selleks, et isikuandmete töötlemine omaks seaduslikku alust, peab üldmääruse artiklis 6

toodud tingimustest olema täidetud vähemalt üks, mille hulka kuulub ka andmesubjektilt isikuandmete töötlemisele nõusoleku saamine. Nõusolekut isikuandmete töötlemisele küsitakse üldjuhul veebilehtede külastamisel. See näeb tavaliselt välja kui teade, mis tutvustab veebilehe külastajale selle kasutamistingimusi, millele järgneb teade nendega nõustumisest või mittenõustumisest. Tingimustega nõustumisel annab andmesubjekt loa isikuandmete töötlemisele. Tasub mainida, et andmetöötleja peab vajaduse korral olema alati valmis tõestama andmesubjektilt isikuandmete töötlemisele nõusoleku saamist.

Väide kõigile töötajatele isikuandmetele juurdepääsu tagamise kohta sai keskmiseks hinnanguks 1,05, mis tähendab, et vastanud ei nõustu sellega. Nende mittenõustumine on arusaadav, sest vastavalt üldmäärusele peab ligipääs isikuandmetele olema ainult nendel isikutel, kes tegelevad andmetöötlusega tulenevalt töölepingus toodud tööülesannetest. Ka neile ei pea olema päris kõik ettevõtte kasutuses olevad isikuandmed kättesaadavad, vaid ainult selles ulatuses, mis on nõutav tööülesannete täitmiseks.

Isikuandmete rikkumine on üks kitsaskohti, mille eiramine võib tuua rikkujatele tõsiseid probleeme. Nende vältimiseks on kehtestatud üldmäärusega nõue, mille kohaselt peab isikuandmete rikkumisel teavitama 72 tunni jooksul, seega vastanute antud üsna kõrge hinnang (3,72) väitele operatiivsest teavitamisest isikuandmete rikkumise korral on põhjendatud. Volitatud töötleja poolt rikkumise tuvastamisel peab ta selle kohta vastutavale töötlejale teada andma ning viimane peab omakorda rakendama nende rikkumiste kõrvaldamiseks asjakohaseid meetmeid. Kui tal ei õnnestu iseseisvalt probleemi lahendada, pöördub ta nende kolme ööpäeva jooksul Andmekaitse Inspektsiooni poole, samas teavitab ka andmesubjekti. Rikkumisest teavitada ei ole kohustuslik, kui see oluliselt ei ohusta andmesubjekti isikuandmeid ning kui rikkumine sai juba leevendatud.

Autori esitatud väide, mis käsitleb turvalise isikuandmete töötlemise eest vastutava isiku määramise olulisust, millest tuleneb rikkumiste eest määratavate karistuste ja trahvide vältimine, sai hinnangu 3,55 ehk uuringus osalejad nõustuvad väitega. Turvalise isikuandmete töötlemise tagamine on oluline mitte ainult selle poolest, et see aitab kaasa isikuandmete kaitstud hoidmisele, vaid ka selle poolest, et see võimaldab isikuandmeid töötlevatel ettevõtetel hoiduda seaduse rikkumisest tulenevatest rahakulukatest trahvidest, mis võivad ulatuda miljonite eurodeni.

Isikuandmete piiramatu hoidmisega ettevõtte andmebaasis uuringust osavõtjad pigem ei nõustunud, kuna nende hinnanguks kujunes 2,22. Autor on vastanutega ühel meelel, ka viitab sellele isikuandmete kaitse piiratud säilitamise põhimõte. Lähtuvalt sellest põhimõttest ei ole isikuandmeid võimalik säilitada kauem, kui on nõutud nende töötlemise eesmärgi saavutamiseks.

Väitele avaliku sektori asutustele andmekaitsespetsialisti määramise kohustuse puudumise kohta andsid uuringus osalejad hinnangu 1,50, mis näitab, et nad ei ole selle väitega nõus. Neil on õigus, kuna andmekaitsespetsialisti on kohustatud määrama kõik avalikus sektoris tegutsevad asutused ja organid. Lisaks peavad ta määrama ka need, kes tegelevad põhitegevuse raames isikute jälgimisega, ning need, kes töötlevad põhitegevuse raames kas eriliigilisi või süütegude ja kohtuotsustega seotud isikuandmeid.

Viimane üldmääruse nõudeid puudutav väide oli isikuandmete edastamise kohta kolmandale osapoolele. Vastavalt väitele võib isikuandmeid edastada kolmandale osapoolele, kui selles riigis kehtivad üldmäärusega ette nähtud nõuetega samaväärsed nõuded. Seda väidet hinnati 2,64-ga, mis tähendab, et uuringus osalejad pigem kalduvad sellega nõustuma. Isikuandmete edastamise aluseks kolmandale osapoolele ongi üldmääruses kehtestatud nõuetele vastavus. Riigis, kuhu isikuandmed kavatsetakse edastada, peab olema tagatud samatasemeline isikuandmete töötlemise turvalisus. Isikuandmete edastamisel Euroopa Liidus kehtestatud madalama andmekaitsetasemega riikidele tuleb rakendada täiendavaid kaitsemeetmeid.

Järgmised kuus väidet käsitlevad isikuandmete töötlemisse mõjukamat suhtumist omavate isikute ehk vastutava ja volitatud töötleja kohustusi. Esimene väide sel teemal oli „Isikuandmete töötlemise eesmärki võib määrata nii vastutav kui ka volitatud töötleja“, millele anti hinnang 2,51. Selline tulemus viitab arvestusala spetsialistide ebakindlusele väite suhtes. Kahtluste hajutamiseks peab meelde tuletama, et üldmääruse kohaselt on vastutava töötleja pädevuses püstitada andmetöötluse eesmärgid ja sellega kaasnevad toimingud, mida volitatud töötlejal ei ole lubatud teha. Volitatud töötleja ülesanne on teostada andmetöötlus vastutava töötleja nimel.

Väidet volitatud töötleja õiguse kohta valida isikuandmete töötlemismeetmed hinnati palliga 2,98, mis näitab, et uuringus osalejad on sellega pigem nõus. Volitatud töötlejal on õigus iseseisvalt valida enda arvates sobivad isikuandmete töötlemisvahendid ning nagu eelmisest väitest tulenes, ei saa andmetöötluse eesmärki määrata.

Uuringus osalejad nõustusid väitega vastutava töötleja teadlikkuse vajadusest volitatud töötleja kohustuse kohta, mille keskmiseks hinnanguks kujunes 3,85. Nende arvamus on kooskõlas üldmääruse nõuetega, sest lisaks oma kohustuste tundmisele on vastutava töötleja kui nii-öelda ülemuse pädevuses olla kursis volitatud töötleja kui tema alluva ülesannete ja kohustusega.

Väide vastutava töötleja kohustusest teavitada järelevalveasutust ja andmesubjekti sai samuti kõrge hinnangu (3,63). Selline tingimus tuleneb üldmääruse artiklist 33. Nagu eespool käsitletud, ei pea seda kohustuslikus korras tegema kas madalama riskiga isikuandmete puhul või rikkumiste iseseisval kõrvaldamisel kolme ööpäeva jooksul.

Vastanud andsid madala hinnangu (2,18) väitele, mille kohaselt ei saa isikuandmete töötlemise eesmärke ega vahendeid üheselt kindlaks määrata enam kui üks vastutav töötleja. Artikkel 26 sätestab, et kahe või enama vastutava töötleja määramine on võimalik ning sel juhul on tegemist kaasvastutavate töötlejatega. Nende vahel peab olema sõlmitud kokkulepe, kus tuuakse mõlema osapoole ülesanded ja kohustused isikuandmete turvalise töötlemise suhtes.

Nii vastutava kui ka volitatud töötleja poolse isikuandmete töötlemise toimingute registreerimise kohustust käsitletav väide hinnati palliga 3,37, mis tähendab, et vastanud on sellega nõus. Autor on samal arvamusel, sest tulenevalt artiklist 30 peab vastutav töötleja registreerima isikuandmete töötlemise toimingud, samal ajal on volitatud töötleja ülesanne pidada isikuandmete töötlemise toimingute kategooriate registrit. Peab aga meeles pidama, et nimetatud kohustus puudutab eelkõige suurettevõtteid.

Uuringu selles osas selgitas autor, et Eesti arvestusala spetsialistide teadlikkus üldmäärusest tulenevatest nõuetest on pigem kõrge. Ainult ühe vastutava ja volitatud töötleja kohustusi puudutava väite suhtes ilmnes ebakindlus. Ka uuringu tulemuste analüüsi käigus sai selgeks, et mõnel arvestusala spetsialistil on tekkinud ebatäielik arusaam isikuandmete töötlemise mõistest. Autori arvates võiks ettevõtete juhtkond rohkem panustada töötajate teadlikkuse tõstmisse isikuandmete kaitse teemal, näiteks infotundide või koolituste kaudu. See aitab kogu ettevõtte kollektiivil saada tuge seista vastu isikuandmete töötlemisel tekkivatele võimalikele kaasnevatele rikkumistele.

3.2. Eestis ja Rumeenias tehtud uuringute tulemuste võrdlemine

Üldmääruse teemal hakati rääkima ja selleks valmidust uurima vähemalt pool aastat enne selle kasutusele võtmist. Nii ka Rumeenias, kus 2017. aastal korraldati kohalike arvestusala spetsialistide teadlikkuse kohta uuring 25. mail 2018 kasutusele võetava üldmääruse nõuetest. Selles alapeatükis võrreldakse olukorda enne üldmääruse jõustumist (Rumeenias) ning poolteist aastat pärast selle kasutusele võtmist (Eestis).

Rumeenia arvestusala spetsialistide teadlikkus üldmäärusest enne selle jõustumist oli üsna madal ehk ligikaudu 62%. Eestis tehtud uuringus osalejate seas oli see 30. novembri 2019 seisuga 99%. Suure vahe põhjuseks võib olla see, et eeldatavasti ei räägitud üldmäärusest nii palju enne selle kohaldamist, seega sellest informeerimise tase osutus madalaks. Eestis valgustati üldmääruse jõustumist piisaval määral meedias. Lisaks hakati aktiivselt looma juhendmaterjale.

2017. aasta uuringu läbiviijad küsisid vastanutelt juhipoolse teavitamise kohta uue üldmääruse jõustumisest. Tulemused näitasid, et 35% vastanuid said muudatustest teavitatud. Eestis sai aga ainult 16% uuringus osalejaid üldmääruse kohta teada tänu juhtkonnale. Mõlemad juhtumid näitavad päris madalat juhipoolset huvi töötajate teadlikkuse tõstmise suhtes, mis on aga tõsine möödalask, sest ettevõttes sõltub palju töötajatest ning nende teadmistest ja oskustest, puudulikud andmekaitseteadmised võivad osutuda tõsiseks probleemiks kogu ettevõtte tegevusele.

Mõlema riigi arvestusala spetsialistidele esitati küsimus isikuandmete töötlemisega kaasnevate toimingute ülevaatamise kohta. Rumeenias vaatasid 2017. aastal need üle 53% vastanuid. Eesti arvestusala spetsialistidest tegeles toimingute ülevaatamisega 60%. Vahe ei ole suur, mis viitab sellele, et praktikas ei pöörata mõlemal juhul piisavat tähelepanu isikuandmete kaitsele vaatamata sellele, et Eesti arvestusala spetsialistid näitasid üsna heal tasemel teoreetilisi teadmisi. See võib olla tingitud ka juhipoolsest madalast motiveerimisest olla tähelepanelikum andmekaitse suhtes.

Arvestusala spetsialistidel paluti nimetada nende ettevõtetes kasutatavaid turvameetmeid. Rumeenia spetsialistid märkisid ära sagedase paroolide vahetamise, erinevate paroolide loomise, e-postiga saadetud dokumentide skannimise ning nende krüpteerimise enne edastamist. Eesti arvestusala spetsialistid rakendavad aga palju enam turvameetmeid, milleks on lisaks paroolide sagedasele vahetamisele ja dokumentide krüpteerimisele pidev tarkvarauuendamine, dokumentide hoidmine piiratud juurdepääsuga elektroonilistes kaustades, kirjavahetuste piiratud säilitamine,

pilvesüsteemi kasutamine, dokumentide edastamine vastavalt vajadusele, isikuandmete koodidega salastamine jm. Tundub, et Eesti ettevõtetes valitseb isikuandmete kaitsele tõsisem lähenemine. Sellele võib mõju avaldada näiteks Eesti kui e-riigi kuvand. Eesti sai infotehnoloogia riigi maine tänu pidevate tehnoloogiliste lahenduste loomisele, millega tegeldakse olulisel määral ka TalTechis ning tõenäoliselt on Eestis tehnoloogiad võrreldes Rumeeniaga palju paremini arenenud.

Uuringute tulemuste võrdlus näitas olukorra märkimisväärset paranemist nende kahe aasta jooksul. Loodetavasti said Rumeenia arvestusala spetsialistid teadlikumaks isikuandmete kaitse suhtes. Autori arvates vajavad mõlema riigi spetsialistid suuremat valmidust isikuandmete turvalisuse tagamisele praktikas, sest ainult teoreetilistest teadmistest üldmääruse nõuete kohta ei piisa.

3.3. Arutelu ja järeldused

Uuringu raames käsitleti üldmääruse põhilisemaid nõudeid ning sai selgeks, et need on muutunud rangemaks. Esiteks tekkis vajadus vastutava ja volitatud töötleja määramisele. Kuigi nende olemasolu aitab minimeerida isikuandmetega kaasnevaid rikkumisi, paneb see nõue (suur)ettevõtetele täiendavad kohustused näiteks isikuandmete töötlemise kohustusliku dokumenteerimise näol. Lisaks said teatud ettevõtted-asutused kohustuse määrata ametisse andmekaitsespetsialist. Liikmesriigis mittetegutsevatele ettevõtetele isikuandmete edastamine muutus võimalikuks ainult tingimusel, et nendes riikides tagatakse üldmääruse nõuetele vastav andmekaitse või selle madalama taseme korra rakendatakse täiendavaid turvameetmeid. Üldmääruse jõustumine tõi kaasa isikuandmete rikkumistest 72 tunni jooksul teavitamise nõude. Samas näeb see ette isikuandmete nõuete rikkumisel trahvisummade määramise kuni 20 miljonit eurot või 4% ettevõtte eelmise majandusaasta maailma kogukäibest. Kõik eeltoodud nõuded on suunatud eelkõige ettevõtetele, millest selgub, et üldmääruse nii-öelda karmim külg puudutab eelkõige juriidilisi isikuid.

Füüsiliste isikute suhtes on üldmäärus leebem. Enamgi veel, selle peamisi eesmärke ongi füüsilistele isikutele isikuandmete töötlemise kohta käiva teabe kättesaadavamaks muutmine, mis omakorda laiendab viimaste õiguste ja vabaduste piire. Inimestel tekkis võimalus omada suuremat kontrolli neile kuuluvate töödeldavate isikuandmete üle, nimelt otsustada, milliseid isikuandmeid

edastada, kas anda nende töötlemisele nõusolek jm. Samuti võimaldab üldmäärus neil nõuda oma isikuandmete viivitamata kustutamist, mida näeb ette „õigus olla unustatud“.

Üldmäärus avaldab olulist mõju nii raamatupidamisele kui ka ettevõtte tegevusele tervikuna. Töödeldes iga päev erinevaid isikuandmeid, peavad arvestusala spetsialistid ja kõik isikud, kelle tööülesanded eeldavad isikuandmetega igasuguste seonduvate toimingute tegemist, olema teadlikud üldmääruse nõuetest. Novembris 2019 tehtud küsitlus näitas, et Eesti arvestusala spetsialistid tunnevad üldmääruse nõudeid pigem kõrgel tasemel. Ebakindlust on tekkinud vastutava ja volitatud töötleja kohustusi käsitletud väidete hindamisel. Samas selgus, et mõni arvestusala spetsialist ei saa täielikult aru sellest, mis kuulub isikuandmete töötlemise alla. Autor võrdles Eesti arvestusala spetsialistide teadlikkust üldmäärusest Rumeenia spetsialistide omaga, mis selgitati välja 2017. aastal tehtud uuringuga. Selgus, et kahe aasta jooksul on arvestusala spetsialistide teadlikkus märkimisväärselt kasvanud. Siiski märgiti mõlema uuringu puhul vähest juhipoolset huvi töötajate teadmistesse panustamise vastu. Ka näitasid arvestusala spetsialistide vastused andmetöötlusega kaasnevate toimingute ülevaatamise kohta, et nad pigem ei suhtu andmekaitsesse tarviliku tõsisusega. Töötajate arusaama loomine andmekaitse tähtsusest on väga oluline, sest nende ebapiisavad teadmised võivad osutuda ettevõttele tõsiseks probleemiks. Seega on tähtis töötajaid kurssi viia näiteks koolitustega andmekaitse teemal, kasutades paremaks meeldejätmiseks mitmesuguseid meeldetuletusi arvutis ja muid motiveerivaid vahendeid.

Positiivse näitajana märkis autor ära selle, et enamik Eesti arvestusala spetsialistidest hindas nende ettevõtetes oleva andmekaitse taset kõrgeks. Lisaks selgitati uuringu käigus välja Eestis rakendatavad isikuandmete turvameetmed. Nendest kõige levinumad olid piiratud juurdepääsuga elektroonilised kaustad, sagedane paroolide vahetamine ja dokumentide edastamine vastavalt vajadusele. Need meetmed on päris turvalised, kuid neid oleks võimalik kombineerida ka muude meetmega, näiteks pidev tarkvarauuendamine või dokumentide krüpteerimine enne edastamist.

Isikuandmed kui vara on väga väärtuslik ressurss, millesse on vaja suhtuda hoolivalt. Seega peavad kõik isikuandmete töötlemisega tegelevad isikud tundma isikuandmete töötlemise põhimõtteid ning andmesubjektid pidama meeles oma õigusi isikuandmete töötlemise suhtes. Tõhusama andmekaitse saavutamiseks peavad olema tasakaalus nii töötajate valmidus kui ka ettevõtetes rakendatavad kaitsetehnoloogiad.

KOKKUVÕTE

Magistritöö eesmärk oli selgitada välja Eesti raamatupidajate ja teiste arvestusala spetsialistide teadlikkus isikuandmete kaitse ja seda puudutava üldmääruse kohta.

Esimeses peatükis käsitleti isikuandmete liike ja nende kaitse olulisust, üldmääruse põhilisemaid nõudeid, isikuandmete kaitse põhimõtteid ning andmesubjektile tagatavaid õigusi. Samuti vaadeldi üldmääruse jõustumisega kaasnenud peamisi muudatusi ja toodi välja selle nõuetest tulenevad kitsaskohad.

Teine peatükk puudutas üldmääruse kajastamist raamatupidamises ja töösuhetes, isikuandmete rikkumisega tekkivat vastutust ning rikkumiste vältimiseks võimalike turvameetmete käsitlemist. Lisaks anti ülevaade 2017. aastal Rumeenias tehtud uuringust arvestusala spetsialistide teadlikkusest üldmäärusest.

Kolmandas peatükis esitas autor oma kvantitatiivse uuringu. Selle raames tehti küsitlus, et selgitada välja, kui hästi tunnevad Eesti arvestusala spetsialistid isikuandmete kaitset ja seda puudutavaid nõudeid. Peale selle võrdles autor oma uuringuga saadud tulemusi Rumeenia uuringu tulemustega, et selgitada välja kahe aasta jooksul toimunud teadlikkuse muutus.

Uuringu läbiviimiseks esitati kolm uurimisküsimust. Esimene küsimus oli „Kui teadlikud on Eesti raamatupidajad ja teised arvestusala spetsialistid isikuandmete kaitsest ja seda puudutavast üldmäärusest?“. Küsitluse käigus selgus, et enamiku Eesti arvestusala spetsialistide teadmised sellest on pigem head. Ainult ühe väite hindamisel, mis puudutas vastutava ja volitatud töötleja kohustusi, olid nende vastused ebakindlad. Lisaks sellele tuvastati mõne uuringus osalenu puhul ebatäielik arusaam isikuandmete töötlemise definitsioonist.

Teise uurimisküsimuse esitamisel sooviti teada saada üldmääruse jõustumisega põhjustatud peamised muudatused isikuandmete kaitse suhtes. Selgus, et uue üldmääruse kasutusele võtmine suurendas ettevõtete jaoks andmekaitsealaseid kohustusi ning lisas isikute puhul täiendavaid

õigusi. Peamine muudatus üldmääruses seisnes näiteks isikuandmete töötlemisest avalikuma teabe suunamises nende omanikele, inimestel tekkinud õiguses nõuda oma andmete kustutamist ja õiguses esitada vastuväiteid seoses nende töötlemisega mittenõustumisega ning lisakohustustes ettevõtetele, kes teevad aktiivselt koostööd rahvusvaheliste ettevõtetega.

Kolmas uurimisküsimus käsitles isikuandmete kaitseks rakendatavaid meetmeid. Enam levinud kaitsemeetmed on piiratud juurdepääsuga elektroonilistes kaustades dokumentide hoidmine, sagedane paroolide vahetamine ning vajaduspõhine dokumentide edastamine. Suurema osa uuringus osalejate hinnang andmekaitsele nende ettevõtetes oli kõrge, millest järeldub, et eelmainitud meetmed tagavad piisava turvalisuse. Autori arvates võib lisaks nendele rakendada ka teisi turvameetmeid, näiteks andmete krüpteerimist, tarkvara uuemate versioonide ja pilvesüsteemide kasutamist. Oluline aspekt on ka ettevõtte töötajate nii teoreetiliste kui ka praktiliste andmekaitseteadmiste arendamine.

Autori arvates saavutas magistritöö püstitatud eesmärgi. Arvestusala spetsialistide vastused küsimustele näitasid nende teadmiste taset, mis osutus pigem positiivseks, kuid samal ajal selgitati välja mõni teadmiste kitsaskoht. Tasub meeles pidada, et peale üldmääruse hoolika läbilugemise peab uurima ka sellega seonduvat praktilist külge.

SUMMARY

PERSONAL DATA PROTECTION IN ACCOUNTING OF ESTONIAN COMPANIES

Anastassia Bagnetova

With the development of information technology in the world, cases of cyberattacks have become more frequent. When applying various schemes, fraudsters seek to obtain important information about people, including personal data. Current circumstances prompted to start thinking about the introduction of more effective protective technologies. In addition, there was a need for amendments to the laws governing the protection of personal data, namely, to establish stricter requirements for the security of personal data and to impose stricter penalties in the form of larger fines for not following them. Thus, on 25th of May 2018, the General Data Protection Regulation (GDPR) came into force.

The aim of this Master's Thesis was to determine the awareness of Estonian accountants and other accounting professionals about the protection of personal data and the GDPR.

The first chapter dealt with the categories of personal data and the importance of their protection, the basic requirements of the GDPR, the principles of personal data protection and the rights guaranteed to the data subject. It also examined the main changes brought about by the entry into force of the GDPR and highlighted the shortcomings of its requirements.

The second chapter considered the reflection of the GDPR in accounting and employment relationships, liability for personal data breaches and consideration of possible security measures to prevent breaches. Furthermore, the results of a study conducted in Romania in 2017 on the awareness of accounting professionals about the GDPR were reviewed.

In the third chapter, the author presented quantitative study. As part of this, a survey was conducted to determine how well Estonian accounting professionals are familiar with personal data protection

and the requirements that apply to it. In addition, the author compared the results of current study with the results of a Romanian study to identify changes in awareness over two years.

To conduct the study, three research questions were asked:

1. How aware are Estonian accountants and other accounting professionals of the protection of personal data and the GDPR?
2. What changes were brought by the introduction of the GDPR?
3. Which methods are used to protect personal data?

The survey has shown that the majority of Estonian accounting professionals have rather good knowledge of the GDPR requirements. Only when evaluating one statement regarding the responsibilities of the data controller and data processor, their answers were uncertain. Also, in the case of some survey participants, an incomplete understanding of the meaning of the concept of personal data processing was revealed.

There was also made a comparison of the awareness of Estonian and Romanian accounting professionals about the GDPR. It appeared that the awareness of accounting professionals has increased significantly over the two years. However, in both studies, little managerial interest in contributing to the knowledge of the employees was identified. Also, the answers of accounting professionals to the question about the review of data processing operations show that they tend not to take data protection seriously. Developing employees' awareness of the importance of data protection is very significant as their lack of knowledge can be a serious problem for the company. Therefore, it is necessary to bring employees up to date, for example, through training on data protection, as well as using various reminders on a computer or other motivational tools for the better memorization.

The entry into force of the GDPR imposed more responsibilities on companies, but also provided individuals with additional rights. The main changes related to the new regulation were, for example, the providing more transparent information on the processing of personal data to their owners, the right to demand the deletion of personal data and, in certain circumstances, the right to object to the processing of personal data, as well as the increased responsibilities for those companies that are actively cooperating with international enterprises.

In connection with the stricter requirements for data protection, it was important to consider methods that ensure the security of personal data. The most common methods are storing documents in restricted electronic folders, changing passwords frequently, and transferring documents as needed. Most of the respondents rated the level of data protection in the companies where they work highly, which implies that the methods mentioned above provide sufficient security. According to the author, other security measures, such as data encryption, use of newer versions of software, and cloud systems, can also be applied. An important aspect is the ability of employees to apply knowledge about the protection of personal data in practice.

In conclusion, personal data as an asset is very valuable and needs to be treated with care. Therefore, all individuals involved in the processing of personal data must be aware of the data protection principles and data subjects should know their rights regarding the processing of personal data. In order to achieve more effective data protection, there must be a balance between the knowledge of employees and the security technologies used in companies.

KASUTATUD ALLIKATE LOETELU

Accountancy Europe. (2017). What do the New EU Data Protection Rules mean for You? – *SME Infopack*, 4, 6.

Ahas, E. (2019). *Raamatupidaja roll küberkahju ärahoidmisel*. Kättesaadav: https://www.rup.ee/uudised/maksud-ja-raamatupidamine/raamatupidaja-roll-kuberkahju-arahoidmisel, 24. oktoober 2019.

Andmekaitse Inspektsioon. (2019). *Isikuandmed ja töötlemine.* Kättesaadav: https://www.aki.ee/et/eraelu-kaitse/isikuandmed-ja-tootlemine, 10. oktoober 2019.

Andmekaitse Inspektsioon. *Isikuandmete töötleja üldjuhend.* Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf, 18. november 2019.

Aruste, V. (2006). *Siseaudit ja Revisjon*. Tallinn: Ferdida.

Bansah, E.A. (2018). The Threats of Using Computerized Accounting Information Systems in the Banking Industry. – *Accounting and Management Information Systems*, 17(3), 445.

Bendiek, A., Römer, M. (2019). Externalizing Europe: the global effects of European data protection. – *Digital Policy, Regulation and Governance*, 21(1), 40.

Chabinsky, S. (2018). GDPR: Will Your Company Be Fine or Fined?. *Security Magazine*, 30.

Cliza, M., Spataru-Negura, L. (2018). The General Data Protection Regulation: what does the public authorities and bodies need to know and to do? The rise of the data protection officer. – *Juridical Tribune*, 8(2), 492.

Deac, A. (2018). Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of These Data. – *Perspectives of Law and Public Administration*, 7(2), 155.

El-Dalabeeh, R., Alshebeil, S.O. (2012). The Role of Computerized Accounting Information Systems in Reducing the Costs of Medical Services at King Abdullah University Hospital. *Interdisciplinary Journal of Contemporary Research in Business*, 4(6), 893-900.

Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679. (2016). Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32016R0679, 06. detsember 2019.

Fazlioglu, M. (2019). Beyond the „Nature“ of Data: Obstacles to Protecting Sensitive Information in European Union and The United States. – *Fordham Urban Law Journal*, XLVI, 277.

Fuster, G.G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (16th ed). Switzerland: Springer International Publishing.

Gheorghiu, G., Spătariu, E.C. (2018). The EU General Data Protection Regulation Implications for Romanian Small and Medium-Sized Entreprises. – *Economic Sciences Series*, 18(1),89.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. – *International Journal of Market Research*, 59(6), 704-705.

Grove, H., Holder, A.D., Schaffner, L.G., Clouse, M. (2018). *Cybersecurity Guidance for Accountants and Executives, 13.* Kättesaadav: https://www.researchgate.net/publication/330199422_Cybersecurity_Guidance_for_Accountants_and_Executives, 15. oktoober 2019.

Gruschka, N., Mavroeidis, V., Vishi, K., Jensen, M. (2018). Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. 2.

Hintze, M. (2018). Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR. *Journal of Internet Law*, 18, 25.

Internal Auditor. (2018). *Regulation Ready?*, 13.

IRIS. (2017). *9 Ways Accountants Can Prepare for GDPR*, 3.

Isikuandmete kaitse seadus. RT I, 04.01.2019, 11.

IT uudised. (2018). *Andmekaitse spetsialist ei pea läbima koolitust*. Kättesaadav: https://www.ituudised.ee/uudised/2018/04/23/andmekaitse-spetsialist-ei-pea-labima koolitust, 25. november 2019.

Jakimoski, K. (2016). Security Techniques for Data Protection in Cloud Computing. *International Journal of Grid and Distributed Computing*, 9(1), 49, 53, 54.

Kaul, R. (2017). *Andmesubjekti õigus andmete kustutamisele vs väljendusvabadus ja ettevõtlusvabadus.* (Magistritöö) TÜ Avaliku õiguse osakond, Tartu.

Kirss, M. (2019). *Isikuandmete edastamisest kolmandatesse riikidesse*. Kättesaadav: https://www.rmp.ee/ettevotlus/andmekaitse/isikuandmete-edastamisest-kolmandatesse-riikidesse, 02. november 2019.

Kurg, A. (2019). *Miks ettevõtted ikka veel õngitsuskirjade õnge lähevad.* Kättesaadav: https://www.raamatupidaja.ee/uudised/2019/10/08/miks-ettevotted-ikka-veel-ongitsuskirjade-onge-lahevad, 06. november 2019.

Lee, M. (2018). GDPR: A Guide for Accountants in Practice. – *ICPA*, 4, 7-8.

Liive, R. (2019). *Toimus Eesti ajaloo suurim e-poe andmeleke: ripakil olid 14 000 eestlase isikuandmed.* Kättesaadav: https://digi.geenius.ee/rubriik/uudis/toimus-eesti-ajaloo suurim-e-poe-andmeleke-ripakil-olid-14-000-eestlase-isikuandmed/, 04. detsember 2019.

Loveday, C., Abraham, R. (2018). The General Data Protection Regulation – Another Key Compliance Area for Global Business. – *Defense Counsel Journal*, 85(3), 2.

Miidla-Vanatalu, M. (2012). *Kuidas on andmete kaitse seotud töösuhetega?* Tallinn: Tööinspektsioon.

Miidla-Vanatalu, M. (2014). *Isikuandmed töösuhetes ja reeglid töökorraldusele.* 2 tr. Tallinn: Tööinspektsioon.

Männiko, M. (2011). *Õigus privaatsusele ja andmekaitse*. Tallinn: Tallinna Raamatutrükikoda.

Pendley, J.A. (2018). Finance and Accounting Professionals and Cybersecurity Awareness. – *The Journal of Corporate Accounting & Finance*, 29(1), 54-55.

Petersen, K. (2018). GDPR: What (and Why) You Need to Know About EU Data Protection Law. – *Utah Bar Journal*, 31(4), 14.

Raamatupidaja.ee 12 käsiraamat. (2002). Tallinn: Eesti Siseaudiitorite Ühing.

Salmony, M. (2018). Rethinking Digital Identity. – *Journal of Payments Strategy & Systems*, 12(1), 42-43.

Savić, D., Veinović, M. (2018). Challenges of General Data Protection Regulation (GDPR). Conference: Sinteza 2018, 28.

Shastri, S., Wasserman, M., Chidambaram, V. (2019). *The Seven Sins of Personal-DataProcessing Systems under GDPR.* Kättesaadav: https://papers.ssrn.com/sol3/papers.cfm?abstract_id =3425860, 01. detsember 2019.

Sipes, E., James, J., Zetoony, D. (2016). Current Data Security Issues for Financial Services Firms. *Journal of Investment Compliance*, 17(3), 56.

Sotsiaalkindlustusamet. *Lisapuhkepäevad isale, puudega lapse vanemale ja lapse rinnaga toitmise vaheaegade hüvitamine.* Kättesaadav: https://www.sotsiaalkindlustusamet.ee/et/lapsed-ja pere/perehuvitiste-liigid/lisapuhkepaevad-isale-puudega-lapse-vanemale-ja-lapse-rinnaga, 29. oktoober 2019.

Stanciu, V., Rîndașu, S. (2018). The Impact of General Data Protection Regulation in The Accounting Profession – Evidences from Romania. – *Journal of Information Assurance & Cyber Security*, 2018, 5-8.

Tiits, K. (2019). *Isikuandmete töötlemine töösuhetes.* Kättesaadav: https://www.rmp.ee/ toooigus/tls/isikuandmete-tootlemine-toosuhetes, 10. november 2019.

Toomela, T., Tuvike, E., Saaliste, M.S. (2019). *Kaameratega jälgimine töökeskkonnas eeldab hoolikat planeerimist ja rangete nõuete täitmist.* Kättesaadav: https://www.rmp.ee/ettevotlus/kasulikteada/kaameratega-jalgimine-tookeskkonnas eeldab-hoolikat-planeerimist-ja-rangete-nouete-taitmist, 10. november 2019.

Turk, K. (2018). *Andmekaitse tegevuste TOP 10: 8. Käitumine isikuandmetega seotud rikkumiste korral.* Kättesaadav: https://triniti.ee/andmekaitsemaaruse-tegevuste-top-10-8-kaitumine-isikuandmetega-seotud-rikkumise-korral/, 11. november 2019.

Töölepingu seadus. RT I 2009, 5, 35.

Voss, W.G. (2017). European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting. – *Business Lawyer*, 72(1), 231.

Äripäev. (2018). *Kaob delikaatsete isikuandmete töötlemise register.* Kättesaadav: https://www.aripaev.ee/uudised/2018/03/27/kaob-delikaatsete-isikuandmete-tootlemise-register, 23. oktoober 2019.

Öman., S. (2004). Implementing Data Protection in Law. – *Stockholm Institute for Scandianvian Law*, 390.

LISAD

Lisa 1. Veebipõhise küsitluse küsimused

Lugupeetud vastaja!

Olen Tallinna Tehnikaülikooli magistriõppe majandusarvestuse eriala üliõpilane ja viin läbi magistritöö raames uuringu. Magistritöö töö eesmärk on välja selgitada raamatupidajate ja teiste arvestusala spetsialistide teadlikkus isikuandmete kaitsest ja 25. mail 2018. aastal jõustunud isikuandmete kaitse üldmäärusest.

Oleksin Teile väga tänulik, kui leiate umbes 10 minutit küsitluse täitmiseks. Küsimustele vastamine on anonüümne ning Teie vastuseid kasutatakse üldistatud kujul.

Küsitluse täitmisel tekkinud küsimuste ja ettepanekute korral palun võtke minuga ühendust e-maili teel anastassia.bagnetova@gmail.com.

Tänan Teid küsitluse täitmisele kulutatud aja eest, Teie panus uuringusse on väga tähtis!

Anastassia Bagnetova

Vastaja profiil

1. Teie sugu:
    - Mees
    - Naine
2. Teie vanus:
    - Kuni 20 aastat
    - 21-30 aastat
    - 31-40 aastat
    - 41-50 aastat

- Üle 51 aasta

3. Teie haridustase:
    - Kutseharidus
    - Kõrgharidus (bakalaureus või rakenduskõrgharidus)
    - Kõrgharidus (magister)
    - Kõrgharidus (doktor)
4. Teie amet:
    - Raamatupidaja
    - Pearaamatupidaja/vanemraamatupidaja
    - Arvelduspetsialist
    - Finantsjuht/kontroller
    - Raamatupidamisassistent
    - Arvestusala üliõpilane/praktikant
    - Muu
5. Teie tööstaaž arvestusala spetsialistina:
    - Kuni 4 aastat
    - 5-10 aastat
    - 11-15 aastat
    - 15-19 aastat
    - Üle 20 aasta
6. Ettevõtte suurus:
    - Mikroettevõte (0-9 töötajat)
    - Väike ettevõte (10-49 töötajat)
    - Keskkettevõte (50-249 töötajat)
    - Suurettevõte (üle 250 töötaja)

Lisa 1. järg

Isikuandmete kaitse raamatupidamises

7. Kas Teie olete kuulnud 25. mail 2018. aastal jõustunud isikuandmete kaitse seadusest?
    - Jah, olen kuulnud
    - Ei, ei ole kuulnud
8. Kuidas Teie saite teada uue isikuandmete kaitse seaduse vastuvõtmisest?
    - Uudistest, ajakirjast vms
    - Ettevõtte juhtkonnalt
    - Kolleegide käest
    - Raamatupidamis- ja maksuinfoportaalist (rmp.ee)
    - Muust allikast
    - Ei tea sellest midagi
9. Milline on Teie arvates andmekaitse tase Teie ettevõttes?
    - Kõrge
    - Keskmine
    - Madal
    - Ei oska vastata
10. Mis hõlmab Teie arvates isikuandmete töötlemine? (võib valida mitu varianti)
    - Isikuandmete kogumine
    - Isikuandmete säilitamine
    - Isikuandmete hävitamine
    - Isikuandmete kasutamine
    - Isikuandmete avalikustamine
    - Isikuandmete muutmine
    - Isikuandmete kustutamine
    - Muu
11. Kui tihti Teie puutute kokku enda töös isikuandmete töötlemisega?
        - Igapäevaselt
        - Aeg-ajalt
        - Ei puutu üldse kokku

12. Kui oluline on Teie arvates isikuandmete töötlemise turvalisus? (1 - ei ole üldse oluline; 2 - pigem ei ole oluline; 3 - pigem on oluline; 4 - on väga oluline; 5 - ei oska vastata)
13. Kellel Teie arvates peab olema juurdepääs isikuandmetele ettevõttes? (võib valida mitu varianti)
    - Juhtkonnal
    - Eri taseme juhtidel
    - Personalispetsialistidel
    - IT-spetsialistidel
    - Raamatupidajatel ja teistel arvestusala spetsialistidel
    - Juurdepääs isikuandmetele peab olema kõigil ettevõtte töötajatel
    - Juurdepääs isikuandmetele peab olema ainult nende töötlemisele õigust saanud töötajatel
    - Muu
14. Kas Teie olete seoses uue isikuandmete seaduse vastuvõtmisega oma andmetöötlusega seotud toimingud üle vaadanud?
    - Jah, olen üle vaadanud ja need ära parandanud
    - Jah, olen üle vaadanud, kuid ei ole ära parandanud
    - Ei ole üle vaadanud
    - Ei tegele andmetöötlusega
15. Kes Teie arvates peab vastutama turvalise isikuandmete töötlemise eest? (võib valida mitu varianti)
    - Raamatupidajad ja teised arvestusala spetsialistid
    - IT-spetsialstid
    - Juhtkond ja haldus
    - Personalispetsialistid
    - Kõik isikud, kes tegelevad isikuandmete töötlemisega
    - Andmekaitse Inspektsioon
    - Muu
16. Millised andmekaitse meetmed Teie ettevõttes rakendatakse? (võib valida mitu varianti)
    - Sagedane paroolide vahetamine (nt iga 3-6 kuu tagant)
    - Pidev tarkvara uuendamine

- Dokumentide edastamine vastavalt vajadustele
- Pilvesüsteemi kasutamine
- Andmete krüpteerimine enne saatmist
- Dokumentide hoidmine piiratud juurdepääsuga elektroonilistes kaustades
- Kirjavahetuste piiratud säilitamine (nt e-kirjade automaatne kustutamine 30 päeva möödumisel)
- Muu

17. Millised allpool olevatest väidetest iseloomustavad Teie arvates tundlikke andmeid? (võib valida mitu varianti)
    - Isikuandmed, mille avalikustamine võib kahjustada nende omaniku elu ja tervist
    - Poliitilised vaated ja usulised veendumused
    - Terviseandmed
    - Makseandmed, krediitkaardi andmed
    - Isiku tuvastamiseks vajalikud biomeetrilised andmed

Palun hinnake 5-palli skaalal, kui nõus Teie olete järgmiste väidetega:

(1 – „ei ole üldse nõus“; 2 – „pigem ei ole nõus“; 3 – „pigem olen nõus“; 4 – „olen täiesti nõus“; 5 – „ei oska vastata“)

- Isikuandmete kaitse seaduse eesmärk on tagada andmesubjektile läbipaistvam teave tema isikuandmete töötlemise eesmärkidest;
- Isikuandmete töötlemise dokumenteerimine ei ole kohustuslik;
- Enne isikuandmete töötlemist peab saama sellele nõusoleku andmesubjektilt;
- Juurdepääs ettevõtte andmebaasis olevatele isikuandmetele peab olema tagatud kõigile töötajatele;
- Isikuandmete rikkumisest peab teavitama nii kiiresti kui võimalik;
- Turvalise isikuandmete töötlemise eest vastutava isiku määramine on oluline, kuna see võimaldab vältida rikkumiste eest määratavaid karistusi ja trahve;
- Isikuandmete hoidmine ettevõtte andmebaasis ei pea olema ajaliselt piiratud;
- Avalikus sektoris tegutsevatel asutustel ei ole kohustulik määrata andmekaitsespetsialisti;
- Isikuandmete edastamine kolmandale osapoolele on võimalik, kui selle riigis tagatakse selline isikuandmete kaitse tase, mis on vastavuses IKS-s toodud nõuetega.

Lisa 1. järg

Isikuandmete kaitse seadus näeb ette vastutava töötleja (ing.k. controller) ja volitatud töötleja (ing.k. processor) määramise. Palun hinnake 5-palli skaalal, kui nõus Teie olete alljärgnevate vastutava ja volitatud töötleja kohustusi ja õigusi käsitletavate väidetega:
(1 – „ei ole üldse nõus“; 2 – „pigem ei ole nõus“; 3 – „pigem olen nõus“; 4 – „olen täiesti nõus“; 5 – „ei oska vastata“)

- Isikuandmete töötlemise eesmärki võib määrata nii vastutav kui ka volitatud töötleja;
- Volitatud töötlejal on lubatud valida isikuandmete töötlemise tehnilised meetmed (nt töötlemistarkvara), kuid ei ole lubatud määrata töötlemise eesmärki;
- Vastutav töötleja peab olema teadlik nii enda kui ka volitatud töötleja kohustustest;
- Vastutav töötleja peab isikuandmetega seotud rikkumistest teavitama nii järelevalveasutust kui ka andmesubjekti;
- Isikuandmete töötlemise eesmärke ja vahendeid ei saa ühiselt kindlaks määrata rohkem kui üks vastutav töötleja;
- Isikuandmete töötlemise toimingute kohta käivat infot peab registreerima nii vastutav kui ka volitatud töötleja.

Lisa 2. Uuringus osalejate vastused

Vastaja profiil

Teie sugu:

- Mees – 3 (4%)
- Naine – 65 (96%)

Teie vanus:

- Kuni 20 aastat – 1 (1%)
- 21-30 aastat – 15 (22%)
- 31-40 aastat – 17 (25%)
- 41-50 aastat – 23 (34%)
- Üle 51 aasta – 12 (18%)

Teie haridustase:

- Kutseharidus – 14 (21%)
- Kõrgharidus (bakalaureus või rakenduskõrgharidus) – 33 (48%)
- Kõrgharidus (magister) – 21 (31%)
- Kõrgharidus (doktor) – 0 (0%)

Teie amet:

- Raamatupidaja – 22 (32%)
- Pearaamatupidaja/vanemraamatupidaja – 23 (34%)
- Arveldusspetsialist – 6 (9%)
- Finantsjuht/kontroller 4 (6%)
- Raamatupidamisassistent – 3 (4%)
- Arvestusala üliõpilane/praktikant – 1 (1%)
- Muu – 8 (14%)

Teie tööstaaž arvestusala spetsialistina:

- Kuni 4 aastat – 22 (33%)
- 5-10 aastat – 13 (19%)
- 11-15 aastat – 9 (13%)
- 15-19 aastat – 7 (10%)
- Üle 20 aasta – 17 (25%)

Ettevõtte suurus:

- Mikroettevõte (0-9 töötajat) – 18 (26%)

- Väike ettevõte (10-49 töötajat) – 22 (32%)
- Keskkettevõte (50-249 töötajat) – 12 (18%)
- Suurettevõte (üle 250 töötaja) – 16 (24%)

Isikuandmete kaitse raamatupidamises

Kas Teie olete kuulnud 25. mail 2018. aastal jõustunud isikuandmete kaitse seadusest?

- Jah, olen kuulnud – 67 (99%)
- Ei, ei ole kuulnud – 1 (1%)

Kuidas Teie saite teada uue isikuandmete kaitse seaduse vastuvõtmisest?

- Uudistest, ajakirjast vms – 31 (46%)
- Ettevõtte juhtkonnalt – 11 (16%)
- Kolleegide käest – 5 (7%)
- Raamatupidamis- ja maksuinfoportaalist (rmp.ee) – 12 (18%)
- Muust allikast – 8 (12%)
- Ei tea sellest midagi – 1 (1%)

Milline on Teie arvates andmekaitse tase Teie ettevõttes?

- Kõrge – 31 (46%)
- Keskmine – 29 (43%)
- Madal – 2 (3%)
- Ei oska vastata – 5 (8%)

Mis hõlmab Teie arvates isikuandmete töötlemine? (võib valida mitu varianti)

- Isikuandmete kogumine – 64 (94%)
- Isikuandmete säilitamine – 64 (94%)
- Isikuandmete hävitamine – 45 (66%)
- Isikuandmete kasutamine – 60 (88%)
- Isikuandmete avalikustamine – 49 (72%)
- Isikuandmete muutmine – 44 (65%)
- Isikuandmete kustutamine – 39 (57%)
- Muu – 0 (0%)

Kui tihti Teie puutute kokku enda töös isikuandmete töötlemisega?

- Igapäevaselt – 30 (44%)

- Aeg-ajalt – 34 (50%)
- Ei puutu üldse kokku – 4 (6%)

Kui oluline on Teie arvates isikuandmete töötlemise turvalisus? (1 - ei ole üldse oluline; 2 - pigem ei ole oluline; 3 - pigem on oluline; 4 - on väga oluline; 5 - ei oska vastata)

- 1 – 1 (1%)
- 2 – 0 (0%)
- 3 – 19 (28%)
- 4 – 43 (63%)
- 5 – 5 (7%)

Kellel Teie arvates peab olema juurdepääs isikuandmetele ettevõttes? (võib valida mitu varianti)

- Juhtkonnal – 29 (43%)
- Eri taseme juhtidel – 12 (18%)
- Personalispetsialistidel – 35 (51%)
- IT-spetsialistidel – 6 (9%)
- Raamatupidajatel ja teistel arvestusala spetsialistidel – 7 (10%)
- Juurdepääs isikuandmetele peab olema kõigil ettevõtte töötajatel – 0 (0%)
- Juurdepääs isikuandmetele peab olema ainult nende töötlemisele õigust saanud töötajatel – 52 (76%)
- Muu – 2 (2%)

Kas Teie olete seoses uue isikuandmete seaduse vastuvõtmisega oma andmetöötlusega seotud toimingud üle vaadanud?

- Jah, olen üle vaadanud ja need ära parandanud – 31 (45%)
- Jah, olen üle vaadanud, kuid ei ole ära parandanud – 10 (15%)
- Ei ole üle vaadanud – 12 (18%)
- Ei tegele andmetöötlusega – 15 (22%)

Kes Teie arvates peab vastutama turvalise isikuandmete töötlemise eest? (võib valida mitu varianti)

- Raamatupidajad ja teised arvestusala spetsialistid – 8 (12%)
- IT-spetsialstid – 10 (15%)
- Juhtkond ja haldus – 24 (35%)
- Personalispetsialistid – 18 (26%)

- Kõik isikud, kes tegelevad isikuandmete töötlemisega – 61 (90%)
- Andmekaitse Inspektsioon – 7 (10%)
- Muu – 2 (3%)

Millised andmekaitse meetmed Teie ettevõttes rakendatakse? (võib valida mitu varianti)

- Sagedane paroolide vahetamine (nt iga 3-6 kuu tagant) – 40 (59%)
- Pidev tarkvara uuendamine – 35 (51%)
- Dokumentide edastamine vastavalt vajadustele – 36 (53%)
- Pilvesüsteemi kasutamine – 29 (43%)
- Andmete krüpteerimine enne saatmist – 24 (35%)
- Dokumentide hoidmine piiratud juurdepääsuga elektroonilistes kaustades – 56 (82%)
- Kirjavahetuste piiratud säilitamine (nt e-kirjade automaatne kustutamine 30 päeva möödumisel) – 7 (10%)
- Muu – 3 (3%)

Millised allpool olevatest väidetest iseloomustavad Teie arvates tundlikke andmeid? (võib valida mitu varianti)

- Isikuandmed, mille avalikustamine võib kahjustada nende omaniku elu ja tervist – 65 (96%)
- Poliitilised vaated ja usulised veendumused – 36 (53%)
- Terviseandmed – 63 (93%)
- Makseandmed, krediitkaardi andmed – 56 (82%)
- Isiku tuvastamiseks vajalikud biomeetrilised andmed – 49 (72%)

Palun hinnake 5-palli skaalal, kui nõus Teie olete järgmiste väidetega:
(1 – „ei ole üldse nõus“; 2 – „pigem ei ole nõus“; 3 – „pigem olen nõus“; 4 – „olen täiesti nõus“; 5 – „ei oska vastata“)

1. Isikuandmete kaitse seaduse eesmärk on tagada andmesubjektile läbipaistvam teave tema isikuandmete töötlemise eesmärkidest;
    - 1 – 3 (4%)
    - 2 – 0 (0%)
    - 3 – 13 (19%)
    - 4 – 25 (37%)
    - 5 – 27 (40%)

2. Isikuandmete töötlemise dokumenteerimine ei ole kohustuslik;
    - 1 – 27 (40%)
    - 2 – 21 (31%)
    - 3 – 16 (24%)
    - 4 – 3 (4%)
    - 5 – 1 (1%)
3. Enne isikuandmete töötlemist peab saama sellele nõusoleku andmesubjektilt;
    - 1 – 3 (5%)
    - 2 – 2 (3%)
    - 3 – 7 (10%)
    - 4 – 9 (13%)
    - 5 – 47 (69%)
4. Juurdepääs ettevõtte andmebaasis olevatele isikuandmetele peab olema tagatud kõigile töötajatele;
    - 1 – 58 (86%)
    - 2 – 3 (4%)
    - 3 – 7 (10%)
    - 4 – 0 (0%)
    - 5 – 0 (0%)
5. Isikuandmete rikkumisest peab teavitama nii kiiresti kui võimalik;
    - 1 – 0 (0%)
    - 2 – 1 (1%)
    - 3 – 8 (12%)
    - 4 – 15 (22%)
    - 5 – 44 (65%)
6. Turvalise isikuandmete töötlemise eest vastutava isiku määramine on oluline, kuna see võimaldab vältida rikkumiste eest määratavaid karistusi ja trahve;
    - 1 – 2 (2%)
    - 2 – 2 (2%)
    - 3 – 21 (18%)
    - 4 – 11 (16%)

- 5 – 32 (47%)

7. Isikuandmete hoidmine ettevõtte andmebaasis ei pea olema ajaliselt piiratud;
    - 1 – 16 (23%)
    - 2 – 12 (18%)
    - 3 – 22 (32%)
    - 4 – 10 (15%)
    - 5 – 8 (12%)
8. Avalikus sektoris tegutsevatel asutustel ei ole kohustulik määrata andmekaitsespetsialisti;
    - 1 – 39 (57%)
    - 2 – 10 (15%)
    - 3 – 12 (18%)
    - 4 – 3 (4%)
    - 5 – 4 (6%)
9. Isikuandmete edastamine kolmandale osapoolele on võimalik, kui selle riigis tagatakse selline isikuandmete kaitse tase, mis on vastavuses IKS-s toodud nõuetega.
    - 1 – 11 (16%)
    - 2 – 4 (6%)
    - 3 – 29 (42%)
    - 4 – 12 (18%)
    - 5 – 12 (18%)

Isikuandmete kaitse seadus näeb ette vastutava töötleja (ing.k. controller) ja volitatud töötleja (ing.k. processor) määramise. Palun hinnake 5-palli skaalal, kui nõus Teie olete alljärgnevate vastutava ja volitatud töötleja kohustusi ja õigusi käsitletavate väidetega:

(1 – „ei ole üldse nõus“; 2 – „pigem ei ole nõus“; 3 – „pigem olen nõus“; 4 – „olen täiesti nõus“; 5 – „ei oska vastata“)

1. Isikuandmete töötlemise eesmärki võib määrata nii vastutav kui ka volitatud töötleja;
    - 1 – 10 (15%)
    - 2 – 14 (21%)
    - 3 – 9 (13%)
    - 4 – 17 (25%)
    - 5 – 18 (26%)

2. Volitatud töötlejal on lubatud valida isikuandmete töötlemise tehnilised meetmed (nt töötlemistarkvara), kuid ei ole lubatud määrata töötlemise eesmärki;
    - 1 – 7 (10%)
    - 2 – 6 (9%)
    - 3 – 19 (28%)
    - 4 – 17 (25%)
    - 5 – 19 (28%)
3. Vastutav töötleja peab olema teadlik nii enda kui ka volitatud töötleja kohustustest;
    - 1 – 0 (0%)
    - 2 – 0 (0%)
    - 3 – 53 (78%)
    - 4 – 6 (9%)
    - 5 – 9 (13%)
4. Vastutav töötleja peab isikuandmetega seotud rikkumistest teavitama nii järelevalveasutust kui ka andmesubjekti;
    - 1 – 1 (1%)
    - 2 – 3 (4%)
    - 3 – 42 (63%)
    - 4 – 9 (13%)
    - 5 – 13 (19%)
5. Isikuandmete töötlemise eesmärke ja vahendeid ei saa ühiselt kindlaks määrata rohkem kui üks vastutav töötleja;
    - 1 – 15 (22%)
    - 2 – 9 (13%)
    - 3 – 7 (10%)
    - 4 – 29 (43%)
    - 5 – 8 (12%)
6. Isikuandmete töötlemise toimingute kohta käivat infot peab registreerima nii vastutav kui ka volitatud töötleja.
    - 1 – 1 (1%)
    - 2 – 6 (9%)

- 3 – 28 (41%)
- 4 – 14 (21%)
- 5 – 19 (28%)

Lisa 3. Vastanute profiil

Sugu	
Mees	3 (4%)
Naine	65 (96%)
Kokku	**68 (100%)**
Vanus	
<20	1 (1%)
21-30	15 (22%)
31-40	17 (25%)
41-50	23 (34%)
51<	12 (18%)
Kokku	**68 (100%)**
Haridus	
Kutseharidus	14 (21%)
Bakalaureus või rakenduskõrgharidus	33 (48%)
Magister	21 (31%)
Doktor	0 (0%)
Kokku	**68 (100%)**
Amet	
Raamatupidaja	22 (32%)
Pea- või vanemraamatupidaja	23 (34%)
Arvelduspetsialist	6 (9%)
Finantsjuht või kontroller	4 (6%)
Raamatupidamisassistent	3 (4%)
Üliõpilane või praktikant	1 (1%)
Muu	8 (14%)
Kokku	**68 (100%)**

Allikas: autori koostatud Lisa 2 alusel

Lisa 3. järg

Tööstaaž	
<4	22 (33%)
5-10	13 (19%)
11-14	9 (13%)
15-19	7 (10%)
>20	17 (25%)
Kokku	**68 (100%)**
Ettevõtte suurus	
Mikro	18 (26%)
Väike	22 (32%)
Keskmine	12 (18%)
Suur	16 (24%)
Kokku	**68 (100%)**

Allikas: autori koostatud Lisa 2 alusel

Lisa 4. Isikuandmete kaitse üldmääruse nõudeid puudutavad väited

Väide	**Keskmine hinnang**
Isikuandmete kaitse määruse eesmärk on tagada andmesubjektile läbipaistvam teave tema isikuandmete töötlemise eesmärkidest;	3,38
Isikuandmete töötlemise dokumenteerimine ei ole kohustuslik;	1,58
Enne isikuandmete töötlemist peab saama sellele nõusoleku andmesubjektilt;	3,64
Juurdepääs ettevõtte andmebaasis olevatele isikuandmetele peab olema tagatud kõigile töötajatele;	1,05
Isikuandmete rikkumisest peab teavitama nii kiiresti kui võimalik;	3,72
Turvalise isikuandmete töötlemise eest vastutava isiku määramine on oluline, kuna see võimaldab vältida rikkumiste eest määratavaid karistusi ja trahve;	3,55
Isikuandmete hoidmine ettevõtte andmebaasis ei pea olema ajaliselt piiratud;	2,22
Avalikus sektoris tegutsevatel asutustel ei ole kohustulik määrata andme-kaitsespetsialisti;	1,50
Isikuandmete edastamine kolmandale osapoolele on võimalik, kui selle riigis tagatakse selline isikuandmete kaitse tase, mis on vastavuses isikuandmete kaitse üldmääruse toodud nõuetega.	2,64

Allikas: Autori koostatud Lisa 2 alusel

Lisa 5. Vastutava ja volitatud töötleja kohustusi käsitlevad väited

Väide	**Keskmine hinnang**
Isikuandmete töötlemise eesmärki võib määrata nii vastutav kui ka volitatud töötleja;	2,51
Volitatud töötlejal on lubatud valida isikuandmete töötlemise tehnilised meetmed (nt töötlemistarkvara), kuid ei ole lubatud määrata töötlemise eesmärki;	2,98
Vastutav töötleja peab olema teadlik nii enda kui ka volitatud töötleja kohustustest;	3,85
Vastutav töötleja peab isikuandmetega seotud rikkumistest teavitama nii järelevalveasutust kui ka andmesubjekti;	3,63
Isikuandmete töötlemise eesmärke ja vahendeid ei saa ühiselt kindlaks määrata rohkem kui üks vastutav töötleja;	2,18
Isikuandmete töötlemise toimingute kohta käivat infot peab registreerima nii vastutav kui ka volitatud töötleja;	3,37

Allikas: Autori koostatud Lisa 2 alusel

Lisa 6. Lihtlitsents

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina Anastassia Bagnetova *(autori nimi)* (sünnikuupäev: 08.07.1995)

1. annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

Isikuandmete kaitse Eesti ettevõtete raamatupidamises,
(lõputöö pealkiri)

mille juhendaja on Natalie Aleksandra Gurvitš-Suits,
(juhendaja nimi)

1.1 reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh TalTechi raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2 üldsusele kättesaadavaks tegemiseks TalTechi veebikeskkonna kaudu, sealhulgas TalTechi raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.

3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

---

[1]*Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil.*