TALLINNA TEHNIKAÜLIKOOL
Majandusteaduskond
Ärikorralduse instituut

Anette Sutt

FINANTSAUDIITORI KOHUSTUSED TULENEVALT ISIKUANDMETE KAITSE ÜLDMÄÄRUSEST

Lõputöö

Õppekava MAJANDUSARVESTUS JA ETTEVÕTLUSE JUHTIMINE,
peaeriala majandusarvestus

Juhendaja: Ester Vahtre, *EMBA*

Tallinn 2020

Deklareerin, et olen koostanud töö iseseisvalt ja
olen viidanud kõikidele töö koostamisel kasutatud
teiste autorite töödele, olulistele seisukohtadele ja andmetele,
ning ei ole esitanud sama tööd varasemalt ainepunktide saamiseks.
Töö pikkuseks on 8 970 sõna sissejuhatusest kuni kokkuvõtte lõpuni.

Anette Sutt ……
(allkiri, kuupäev)
Üliõpilase kood: BDMR166067
Üliõpilase e-posti aadress: anettesutt@gmail.com

Juhendaja: Ester Vahtre, *EMBA*:
Töö vastab kehtivatele nõuetele

……
(allkiri, kuupäev)

Kaitsmiskomisjoni esimees:
Lubatud kaitsmisele

……
(nimi, allkiri, kuupäev)

SISUKORD

LÜHIKOKKUVÕTE

Lõputöö eesmärgiks on hinnata finantsaudiitorite teadlikkust isikuandmete kaitse üldmääruse ja sellega kaasnevate kohustuste osas. Eesmärgi saavutamise jaoks tõlgendatakse lahti isikuandmete kaitse üldmääruse metodoloogia ning seos finantsauditiga. Seejärel viiakse läbi veebipõhine küsitlus Eestis tegutsevate finantsauditi praktikantide, konsultantide, projektijuhtide ning *manager*'idega, et hinnata nende pädevust.

Uuringu käigus hindas autor audiitorite mõistmist isikuandmete kaitse üldmääruse põhilistest definitsioonidest, nagu isikuandmed, andmesubjekt ja töötlemine, ning teadlikkust üldmäärusest tulenevatest kohustustest. Tulemustest ilmnes, et audiitorid ei suuda korrektselt tõlgendada põhilisi definitsioone nagu isikuandmed ja andmesubjekt. Kõrgemate ametikohtade töötajad teavad, et nad on vastutavad töötlejad, seega pööravad nad ka rohkem tähelepanu andmete töötlemise protsessile. Konsultandid ning praktikandid pigem leiavad, et nemad ei otsusta, kuidas ja milliseid kliendi andmeid töödeldakse ja on üldmääruse mõistes volitatud töötlejad.

Mida madalam ametikoht, seda vähem rakendatakse ka üldmäärusest tulenevaid andmetöötlemise põhimõtteid. Kui audiitoritelt uuriti, kas nad kasutavad kohustusi vähendavaid üldmääruse poolt väljapakutavaid meetodeid, oli vastus pigem eitav. Kui üldse, siis teevad seda kõrgemate ametikohtade töötajad.

Kuigi audiitorite teadmised isikuandmete kaitse üldmäärusest tulenevatest kohustustest on puudulikud, ei olnud vastanutel esinenud olulisi rikkumisi. Kõik rikkumised olid lahendatud ettevõttesiseselt kaasamata järelevalveasutust. Rikkumise esinemisel teavad audiitorid, kelle poole pöörduda vastavalt üldmääruse nõuetele.

Võtmesõnad: Euroopa Liidu isikuandmete kaitse üldmäärus, GDPR, andmekaitse, finantsaudit, audit

SISSEJUHATUS

2016. aasta aprillis võttis Euroopa Parlament vastu otsuse asendada seni kehtinud andmekaitse raamistik uue isikuandmete kaitse üldmäärusega ning alates 2018. aastast on see olnud esmane seadus, mis reguleerib ettevõtete kohustust kaitsta Euroopa Liidu kodanike isikuandmeid. Võrreldes eelnevalt 21 aastat kehtinud direktiiviga, ühtlustab uus määrus Euroopa Liidu liikmesriikide vahelist seadusandlust ning suurendab järelevalvet isikuandmete töötlemise üle.

Finantsaudiitorite jaoks on olulise tähtsusega oma klientide isikuandmete kaitsmine, sest auditikliendi finantsaruannete kohta arvamuse kujundamisel töötlevad audiitorid neid isikuandmeid igapäevaselt. Hooletusest või teadmatusest tekkinud eksimused mõjutavad nii kliendi kui ka audiitorbüroo mainet, mis seab ohtu ettevõtluskeskkonna usaldusväärsuse ja koostöösuhted klientidega.

Lõputöö teema valikul lähtus autor uue määruse aktuaalsusest ning olulisusest finantssektori jaoks. Valitud teemat pole varasemalt uuritud, seega pole veel teada, kas Eesti finantsaudiitorid on piisavalt pädevad uue üldmääruse rakendamisel. Kuna tegemist on hiljuti toimunud reformiga, mis mõjutab ka Eesti Vabariigi kodanikke, tekib küsimus, kui pädevad on Eesti finantsaudiitorid uue isikuandmete kaitse üldmäärusega kaasnevate kohustuste mõistmises ning määruse korrektses tõlgendamises?

See küsimus on ka antud lõputöö uurimisprobleemiks ning sellest tulenevalt on autor seadnud eesmärgiks hinnata finantsaudiitorite teadlikkust isikuandmete kaitse üldmääruse ja sellega kaasnevate kohustuste osas. Selle saavutamiseks on autor püstitanud järgmised uurimisülesanded:

1. analüüsida isikuandmete kaitse üldmäärust ning selle teket;
2. tuvastada isikuandmete kaitse üldmäärusest tulenevad kohustused finantsaudiitorile;
3. uurida Eesti finantsaudiitorite teadmisi määruse põhiaspektidest ja kohustustest;
4. analüüsida Eesti finantsaudiitorite hinnangut määruse põhiaspektidele ja kohustustele.

Lõputöö eesmärk saavutati läbi kvantitatiivse uuringu. mille jaoks koguti andmeid ankeetküsitluse teel. Küsitlus viidi läbi Eesti suurimate audiitorettevõtete finantsaudiitorite seas. Sihtrühmadeks olid büroodes töötavad konsultandid, projektijuhid ja *manager*'id, kes tegelevad igapäevaselt kliendisuhtluse ning auditi tõendusmaterjali ehk andmete töötlemisega.

Lõputöö on jaotatud kolmeks osaks. Esimene osa on metodoloogiline ülevaade andmekaitsest ning selle põhikomponentidest. Viimastest on süvitsi välja toodud isikuandmed ning nende töötlemine uuest määrusest lähtuvalt. Teises osas seostatakse isikuandmete kaitse üldmääruse sisu finantsaudiitori ametiga lähtudes metodoloogiast. Töö kolmas osa on analüüs finantsaudiitorite seas läbi viidud küsitluse tulemustest. Tulemuste põhjal hindab autor Eesti finantsaudiitorite pädevust ja teadlikkust uuest isikuandmete kaitse üldmäärusest.

Töö koostamisel on peamiselt lähtutud Euroopa Parlamendi ja Euroopa Liidu Nõukogu määrusest (EL) 2016/679, mille sisu tõlgendamiseks on kasutatud erinevaid erialaseid allikaid ning teadusartikleid. Neist kõige olulisemad on raamatud A. Nõmper ja E. Tikk „Informatsioon ja õigus" (A. Nõmper, E. Tikk) ning „*The EU General Data Protection Regulation (GDPR): A Practical Guide*" (A. Buscche, P. Voigt). Lisaks on kasutatud erinevaid auditi standardeid ning suuremate audiitorettevõtete isikuandmete kaitset käsitlevaid avaldusi.

Töö pakub huvi Eestis tegutsevatele audiitorettevõtjatele ning auditi või ülevaatuse kohustusega ettevõtetele, kes soovivad teada, mil määral vastab Eesti audiitorite pädevus uuele isikuandmete kaitse üldmäärusele, et hinnata selle põhjal nende kvaliteeditaset. Lisaks saavad audiitorettevõtjad selle põhjal hinnata, milline on audituturu valmidus uue määruse täielikuks järgimiseks ning kus on murekohad, millele oma ettevõttes tähelepanu pöörata.

1. ISIKUANDMETE KAITSE ÜLDMÄÄRUS

Euroopa Liidu (edaspidi: EL) majandus- ja ühiskondliku elu eri valdkondades kasutatakse üha sagedamini isikuandmeid. Isikuandmete igapäevane töötlemine ja vahetamine on muutunud märkimisväärselt lihtsamaks tänu infotehnoloogia arengule. (EN direktiiv 95/46/EÜ põhjenduspunkt 4) Standardinõuded andmekaitse suhtes muutuvad läbi aja aina keerukamaks ning aktuaalsemaks, millest tulenevalt seisavad ettevõtted vastamisi üha raskemate ülesannetega, et tagada andmetöötlustoimingute vastavust seadustega (Bussche, Voigt 2017, 1).

Selleks, et tagada liikmesriikide vahel ühtne arusaam isikuandmete kaitsest ning tõsta füüsiliste isikute privaatsustaset, võttis Euroopa Liit 2016. aastal vastu isikuandmete kaitse üldmääruse (edaspidi: GDPR – *General Data Protection Regulation*), mida hakati kohaldama alates 25. maist 2018. GDPR kehtestab eeskirjad füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EN direktiiv (EL)2016/679).

1.1. Andmekaitse areng Euroopa Liidus

Teise maailmasõja tagajärgedest taastumisel tekkis vajadus riikidevaheliste suhete korrastamiseks. Teine maailmasõda pani maailma riike mõistma koostöö vajalikkust ning vajadust üldiselt tunnustatavate põhiõiguste ning vabaduste järgi. (Männiko 2011, 15)

7. detsembril 2000. a kuulutati välja esimene EL-i põhiõiguste harta, mille 8. artikkel sätestas andmekaitse iseseisva põhiõigusena. Eelmainitud artikli kohaselt (*Ibid.*, 71):

1) Igaühel on õigus oma isikuandmete kaitsele.
2) Isikuandmeid tuleb töödelda seotud isiku nõusolekul asjakohaselt ning kindlaksmääratud eesmärkidel või muul seaduses ettenähtud õiguslikul alusel. Igaühel on õigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist.
3) Nende sätete täitmise kontrollimise eest vastutab sõltumatu asutus.

Selleks, et tunnustada isikuandmete kaitset EL-i kodanike põhiõigusena, tuli vastu võtta terve rida andmekaitsealaseid regulatsioone ning defineerida privaatsus inimõigusena (*Ibid.*, 71).

Paar aastat pärast Teise maailmasõja lõppu, 10. detsembril 1948. a, võttis ÜRO vastu inimõiguste ülddeklaratsiooni, mille artikkel 12 sätestab isiku õiguse privaatsusele. Arvestades ÜRO inimõiguste ülddeklaratsiooni, võttis Euroopa Nõukogu 4. novembril 1950. a vastu Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni (edaspidi: konventsioon, EIÕK), millega on tänaseks ühinenud kõik Euroopa Nõukogu 47 liiget, sh Eesti aastal 1993. Konventsiooni artikkel 8 sätestab privaatsusõiguse kaitse igaühele. (EIÕK 1950 art 8 viidatud *Ibid.*, 15) Kuigi artikkel 8 ei kasuta termineid „andmed“ või „informatsioon“, siis Euroopa Inimõiguste Kohtu praktikas käsitletakse artikkel 8 kohaselt ka õigust isikuandmete kaitsele. Sellest tulenevalt on artiklit edaspidi kasutatud ka andmekaitse ühe põhilise alustalana. (Tikk, Nõmper 2007, 39)

Edasi mõjutasid nii EL-i kui ka liikmesriikide andmekaitse õigusaktide väljakujunemist kolm olulist allikat (*Ibid.*, 67):

1) Majandusliku Koostöö ja Arengu Organisatsiooni (OECD – *Organization for Economic Co-operation and Development*) 1980. aastal koostatud juhend privaatsuse ja piiriüleselt edastatavate isikuandmete kaitse kohta (edaspidi: OECD juhend);
2) Euroopa Nõukogu poolt 1981. aastal vastu võetud isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (edaspidi: ETS nr 108);
3) Euroopa Ühenduse direktiiv 95/46/EÜ üksisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (edaspidi: isikuandmete direktiiv).

OECD juhendi eesmärgiks oli koostada riikidele mittesiduvad juhised siseriikliku andmekaitseõiguse regulatsiooni loomiseks. (*Ibid.*, 68) Kuni tänaseni on OECD juhend sätestanud andmekaitse seisukohast olulised definitsioonid (nt andmete töötleja, isikuandmed ja isikuandmete piiriülene levik) ning õiguspärased andmetöötluse üldpõhimõtted. (Männiko 2011, 57)

Kuna tegemist oli mittesiduva juhisega, mis jättis riikidele võrdlemisi vabad käed otsustamaks, kuidas neid üldpõhimõtteid siduda riigisisese õigusega, võeti vastu ETS nr 108. ETS nr 108 oli esimene õiguslikult siduv rahvusvaheline instrument, mille eesmärgiks oli ühtlustada eri riikides vastuvõetud isikuandmete automatiseeritud töötlemise reegleid ning olla ühtsete põhimõtete rajaja. ETS nr 108 kohustab ühinenud riike oma riigisiseses andmekaitse seadusandluses arvesse võtma ausat isikuandmete kogumist, automaatset töötlemist, säilitamist ja kasutamist üksnes seaduslikel ja kogumise aluseks olnud eesmärkidel. (*Ibid.*, 59)

Andmekaitse arengu üheks olulisemaks raamdokumendiks võib pidada 1995. aasta isikuandmete direktiivi. Kuni 1995. aastani määrasid andmekaitsealased regulatsioonid väga erineval tasemel juriidilist kaitset ning ei suutnud pakkuda täielikku kindlust – ei eraisikule, vastutavale töötlejale ega volitatud töötlejale (Bussche, Voigt 2017, 2). Isikuandmete direktiivi reguleerimisala oli võrreldes ETS nr 108 ja OECD juhendiga oluliselt laiem. Kui varem oli reguleeritud automatiseeritud isikuandmete töötlemine, siis isikuandmete direktiiv laienes igasugusele töötlemisele (Männiko 2011, 72). Direktiivis määratleti detailselt isikuandmete kaitse põhimõtted ja eesmärgid, defineeriti õigusmõisted ning anti üldine raamistik asjakohastele menetlustele ja järelevalvele. EL-i liikmesriigid pidid direktiivi kooskõlastama siseriikliku õigusega 1998. aastaks eesmärgiga ühtlustada üksikisikute põhiõiguste kaitse seoses andmetöötlusega ja tagada isikuandmete vaba liikumine liikmesriikide vahel. (*Ibid.*, 71–72; Bussche, Voigt 2017, 2)

Isikuandmete direktiiv ei suutnud oma eesmärke täita ega viia andmekaitset EL-is ühtsele tasemele. Liikmesriikide rakendusmeetmete erinevused tõstsid esile õiguslikke ebakõlasid – ühes liikmesriigis lubatud andmetöötlustoimingud võisid olla teises ebaseaduslikud. Andmekaitse killustatust liikmesriikides ning sellest tulenevat õiguslikku ebakindlust nähti takistusena EL-i majandustegevusele. 2016. aastal võeti vastu GDPR, et asendada 21 aasta vanune isikuandmete direktiiv, ning seekord oli määrus suunatud kõigile EL-i liikmesriikidele. (Bussche, Voigt 2017, 2)

Siinkohal on oluline defineerida direktiivi ja määruse erinevus. Direktiiv on õigusakt, milles sätestatakse eesmärk, mida kõik EL-i liikmesriigid peavad saavutama, otsustades ise selle üle, milliseid õigusakte kehtestada eesmärgi saavutamiseks. Määrus see-eest on siduv õigusakt, mida tuleb tervikuna kohaldada kogu EL-is eranditult. (Määrused … 2019)

1996. aastal ilmus Eestis isikuandmete kaitset reguleeriva isikuandmete kaitse seaduse (edaspidi: IKS) esimene redaktsioon. 2003. aastal, kui toimusid läbirääkimised EL-iga ühinemiseks, läbis IKS sisulise uuenduse ja viidi osaliselt vastavusse isikuandmete direktiiviga. Aja jooksul ilmnes seaduse rakendamisel sisulisi probleeme, millest tulenevalt on aastate jooksul seadust reformitud (Nõmper, Tikk 2007, 69), viimati 2019. aasta alguses. Eesti, kuuludes Euroopa andmekaitseõiguse süsteemi, pidi viima ka IKS-i vastavusse GDPR-iga, kuid GDPR-ist tulenevad regulatsioonid kehtisid juba 2018. aasta mai lõpust. (Uue isikuandmete … 2019)

1.2. Andmekaitse olemus

Andmekaitse tagab isikule informatsioonilise enesemääratlusõiguse. Tegemist on põhiõiguse ja -vabadusega ise valida ja otsustada, kellele ning milliseid endaga seotud andmeid isik jagab. Andmeliik, mis on kaetud andmekaitsega, on informatsioon kellegi kohta ehk isikuandmed. Oluline on, et andmed oleksid seonduvad identifitseeritava isikuga, sest ilma informatsioonilise enesemääratlusõiguseta ei ole andmetel iseseisvalt väärtust ega vaja sellest tulenevalt eraldi õiguskaitset. (Männiko 2011, 42)

Andmekaitsest lähtuvalt on füüsiline isik, kelle isikuandmeid töödeldakse, andmesubjekt. Andmesubjekti isikuandmete olemasolu ei lisa ega võta ära subjekti põhiõigusi, seni kuni neid ei töödelda kolmanda isiku poolt. Lihtsamalt öeldes on andmesubjekt iga inimene, kelle kohta on olemas otseselt temaga seotud informatsioon, mida teab, omab, avaldab või kasutab mõni kolmas isik. (*Ibid.*, 43; Lloyd 2017, 71)

Põhinedes eelnevalt välja toodud definitsioonidele, võib kokkuvõtvalt öelda, et andmekaitsest saab rääkida, kui on täidetud järgmised tingimused (Männiko 2011, 44):

1) andmesubjekti olemasolu;
2) andmesubjektil on isikuandmeid;
3) toimub isikuandmete töötlemine kolmanda isiku poolt;
4) töödeldavad andmed on sellised, mille järgi andmesubjekt on tuvastatav.

Antud tingimused seavad üldraamistiku andmekaitsele ning GDPR mõtestab lahti iga tingimusega kaasnevad kohustused ning õigused.

1.3. Isikuandmed ning nende töötlemine

GDPR-i järgi on isikuandmed igasugune teave tuvastatud või tuvastatava andmesubjekti kohta ehk andmeid ei loeta isikuandmeteks, kui neid pole võimalik seostada füüsilise isikuga (EU General… 2017, 20). Füüsiliseks isikuks loetakse hetkel elavat isikut tema sünnist kuni surmani. GDPR ei rakendu surnud või sündimata füüsilistele isikutele. (Öqvist, Johnssen 2018, 33) Füüsiline isik peab olema kas otseselt või kaudselt tuvastatud selliste identifitseerimistunnuste põhjal nagu nimi,

isikukood, asukohateave, võrguidentifikaator või tema mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal (EU General… 2017, 20).

Igasugust teavet isiku kohta, ükskõik kui kõrge olulisusega, on võimalik klassifitseerida isikuandmeteks. Isikuandmete sisu ning sisust tuleneva riive intensiivsuse järgi jagunevad isikuandmed üldisteks isikuandmeteks ning eriliiki isikuandmeteks. (Feiler *et al.* 2018, 14) Eriliiki isikuandmed on andmed, millest ilmneb andmesubjekti rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused, geneetilised andmed, isiku kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed, terviseandmed ja andmed seksuaalelu ja seksuaalse sättumuse kohta (EN direktiiv (EL)2016/679 art 9 lg 1).

See, kuivõrd teatavaid andmevorme saab liigitada eriliiki isikuandmeteks, on pikka aega olnud vaidluse all. Tekib küsimus, millist teavet peetakse tundlikuks ja mis määrab selle tundlikkuse tajumise, kuna teabe tundlikkust tajub iga inimene erinevalt ja see on ka riigiti erinev. GDPR-i definitsioon on üpris lai ning seda suuresti tulenevalt liikmesriikide probleemidest, mida on põhjustanud puudulik ühtselt reguleeriv andmekaitse normide kogu (Lloyd 2017, 59). Liikmesriikide ühiskonnad on muutunud mitmekülgsemaks ning lai definitsioon kindlustab, et iga füüsilise isiku õigused on tagatud sõltumata tema päritolust.

Ühendkuningriikide teabevoliniku kantselei poolt 2006. aastal läbi viidud uuringus selgitati välja uuringus osalenud inimeste hinnangud konkreetset tüüpi teabe tundlikkuse suhtes. Esindatud olid kõik peamised andmetüübid, mis on loetletud ka GDPR-i definitsioonis ning lisaks veel finantsandmed, kriminaalteave isiku kohta ning klikivoo andmed. Uuringu subjektid hindasid kõige tundlikumaks finantsandmeid (88% kogu valimist). (Lloyd 2017, 59) 2019. aastal viidi Saksamaal läbi sama eesmärgiga uuring, mille tulemused olid sarnased – uuringu valim hindas finantsandmeid teiseks kõige tundlikumaks andmetüübiks (Schomakers *et al*. 2019, 146). Huvitav on, et GDPR-i alusel ei kuulu finantsandmed eriliiki andmete kohustuslikku loendisse.

GDPR ütleb, et töötlemine on isikuandmetega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum. Toimingud, mida loetakse töötlemiseks, on kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühendamine, piiramine, kustutamine või hävitamine. (EN direktiiv (EL)2016/679 art 4 lg 1) Avatud sõnastus tuleneb seadusandja tahtest vältida normide täitmisest

kõrvalehoidumise märkimisväärset ohtu, mille jaoks peaks füüsiliste isikute kaitse olema tehnoloogiliselt neutraalne ega tohiks sõltuda kasutatud meetoditest (*Ibid.* põhjenduspunkt 15).

GDPR-i 5. artikkel sätestab isikuandmete töötlemise seitse põhimõtet, mille alusel isikuandmete töötlemisel tagatakse, et (*Ibid.* art 5; Feiler *et al*. 2018, 75):

1) töötleja on vastutav ja on võimeline põhimõtete täitmist tõendama;
2) töötlemine on seaduslik, õiglane ja andmesubjektile läbipaistev;
3) isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel, mis on sätestatud eelnevalt andmete omandamisele ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus;
4) isikuandmed on asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt;
5) isikuandmed on õiged ja vajaduse korral ajakohastatud ning et võetakse kõik mõistlikud meetmed, et töötlemise eesmärgi seisukohast ebaõiged isikuandmed kustutataks või parandataks viivitamata;
6) isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse ning sellele järgnevalt tuleb andmed kas pseudonümiseerida või anonümiseerida;
7) isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid.

Isikuandmeid ei peeta GDPR-i mõistes isikuandmeteks, kui need on turvaliselt modifitseerimise kaudu anonümiseeritud. Anonümiseeritud andmed on isikuandmed, mille kaudu ei saa füüsilist isikut tuvastada ega seostada. (Öqvist, Johnssen 2018, 34) Anonümiseerimise meetodid jagunevad kahte suuremasse kategooriasse (Voigt, Bussche 2017, 13):

1) Juhuslikustamine (*randomisation*) saavutatakse andmete täpsuse muutmisel nii, et kõrvaldatakse tugev seos andmete ja andmesubjekti vahel. Kui andmed on muudetud piisavalt ebamääraseks, ei saa need enam viidata konkreetsele isikule.
2) Üldistamine (*generalisation*) saavutatakse andmesubjektide andmete tunnusmärkide üldistamisel, muutes andmetetunnuse vastavat skaalat või järjekorda (nt asukoht muudetakse linna täpsuselt maakonna täpsusele või kasutatakse nädala täpsuse asemel kuu täpsust).

Anonüümseks muutmine pakub töötlejale mitmeid eeliseid. Üksused salvestavad ja koguvad sageli väga suures koguses andmeid, kuigi töötlemiseks vajavad nad sellest ainult väikest osa. Liigsete andmete kustutamine võib muuta andmed anonüümseks, mis hoiab ära GDPR-ist tulenevaid mitmeid andmekaitsekohustusi. See tähendab, et juhul, kui töötleja suudab anonüümseks muudetud teabe taastada nii, et see on kõrge tõenäosusega seondatav füüsilise isikuga, loetakse seda GDPR-i mõistes isikuandmeteks. (Voigt, Bussche 2017, 14)

Kui anonümiseeritud andmete kaudu on võimalik tagasiulatuvalt andmesubjekti tuvastada, siis pole tegemist anonümiseerimise vaid pseudonümiseerimisega. Pseudonümiseeritud andmeid peetakse endiselt GDPR-i mõistes isikuandmeteks ja pseudonümiseeritud andmete suhtes kehtivad samad nõuded kui isikuandmete suhtes, sest risk tuvastada selliste andmete kaudu füüsiline isik on oluliselt suurem. (Öqvist, Johnssen 2018, 34)

Pseudonümiseerimine on enim levinud viis, kuidas hoida ära füüsilise isiku tuvastamist läbi isikuandmete. Pseudonümiseerimine on isikuandmete töötlemine sellisel viisil, et neid ei saa enam täiendavat teavet kasutamata seostada konkreetse andmesubjektiga. Seda saavutatakse läbi andmete kodeerimise, vahetades näiteks isiku nime või muu tunnuse kindlate näitajatega (nt koodiga). Pseudonümiseerimine on efektiivne ainult juhul, kui kodeerimisel kasutatud tunnuseid või sellega seotud teavet hoitakse eraldi. Kõik pseudonümiseerimise tegevused peavad olema tagatud tehniliste ja korralduslike meetmetega nagu näiteks eelnevalt välja toodud kodeerimine ning kodeerimise võtme jagamine väheste töötlejate seas. (Voigt, Bussche 2017, 15)

Isikuandmete pseudonüümiseerimine on töötlejate jaoks üks võimalus täita GDPR-ist tulenevaid andmekaitse kohustusi ning tagada määruse jälgimise vastavust. Isikuandmete pseudonümiseerimine võib vähendada asjaomaste andmesubjektide jaoks ohte ning aidata vastutavatel töötlejatel ja volitatud töötlejatel täita oma andmekaitse kohustusi. Efektiivse pseudonümiseerimise rakendamisel võib riskipotentsiaali vähendada nii, et töötleja ei ole kohustatud pseudonümiseeritud andmetega seotud andmesubjekti isikuandmetega seotud rikkumisest teatama. (*Ibid*., 15)

2. ISIKUANDMETE KAITSE ÜLDMÄÄRUSE SEOS FINANTSAUDITIGA

Finantsaudiitorid vastutavad selle eest, et klienditööd tehtaks ausalt, kvaliteetselt ja professionaalselt, sealhulgas austades ja kaitstes ettevõtte ja nende klientide konfidentsiaalset teavet. Üks eksimus võib hävitada kliendi maine või koostöösuhte kliendiga, mistõttu on väga oluline, et finantsaudiitorid võtaksid konfidentsiaalsust tõsiselt. Neil tuleb koguda ja käsitleda konfidentsiaalset teavet vastavalt kehtivatele seadustele, ametialastele kohustustele ja sisemistele andmehaldustavadele. Auditikliendid usaldavad ja loodavad, et audiitorid kaitsevad ja kasutavad neile usaldatud konfidentsiaalset teavet ainult sihtotstarbeliselt ning kehtestavad konfidentsiaalsuse rikkumiste vältimiseks sobivad ja tõhusad kaitsemeetmed. Selleks, et tagada kõigi eelnevalt nimetatud ootuste ning kohustuste täitmine, on oluline mõista finantsaudiitorite seost GDPR-iga.

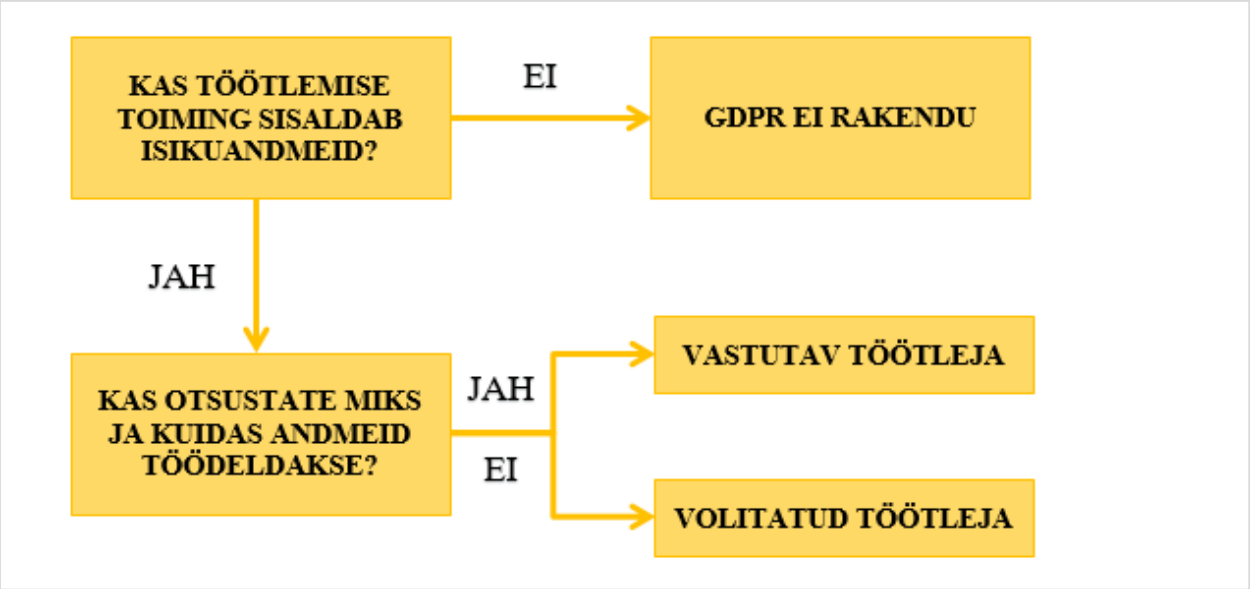
2.1. Vastutav töötleja ja volitatud töötleja

Töötlejale on oluline kindlaks teha, kas ta tegutseb GDPR-i alusel vastutava või volitatud töötlejana (vt Joonis 1). Kahe töötleja tüübi eristamine on oluline, sest neile rakendatavad kohustused erinevad omavahel.

Vastutav töötleja on füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes määrab üksi või koos teistega kindlaks isikuandmete töötlemise eesmärgid ja vahendid (EN direktiiv (EL) 2016/679 art 4 lg 7). Seega on vastutav töötleja isik, kes otsustab, kuidas isikuandmeid töödelda, miks andmeid kasutatakse ning tagab ja vastutab selle eest, et töötlemine toimuks kooskõlas GDPR-iga.

Lisaks töötlemistoimingute määratlemisele peab vastutav töötleja otsustama, kas tal on GDPR-ist tulenevalt kohustus andmesubjekte teavitada või neilt nõusolekut taotleda, kui kaua peab andmeid säilitama ja kas on vaja kaasata kolmanda osapoolena ka volitatud töötlejat (EU General… 2017,

236-237). Viimane on määratletud kui füüsiline või juriidiline isik, riigiasutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötleja nimel (EN direktiiv (EL) 2016/679 art 4 lg 8).



Joonis 1. Vastutava töötleja ja volitatud töötleja määramine GDPR-i alusel
Allikas: GDPR: implications… (2018, 4)

Seega sõltub volitatud töötleja olemasolu vastutava töötleja otsusest, kes võib töödelda andmeid oma organisatsioonis või delegeerida kogu töötlemistegevuse või osa sellest kolmandale osapoolele, muutes viimase volitatud töötlejaks (Voigt, Bussche 2017, 20). GDPR-i artikkel 28 lõige 1 sätestab, et juhul, kui vastutav töötleja kaasab volitatud töötleja, tohib ta kaasata ainult selliseid töötlejaid, kes rakendavad asjakohaseid tehnilisi ja korralduslikke meetmeid sellisel viisil, et töötlemine on kooskõlas määrusega ja tagab andmesubjekti õiguste kaitse (EN direktiiv (EL) 2016/679).

Vastutav töötleja ei pea määratlema andmete töötlemise kõiki elemente ja tihti tugineb volitatud töötleja kinnitusele, et töötlemine toimub turvaliselt. Sellisteks elementideks on peamiselt kasutatavad IT-süsteemid ja meetodid, millega tagatakse andmete töötlemine GDPR-i mõistes. Kõige olulisem piirang, mida vastutav töötleja peab jälgima on, et volitatud töötleja ei kaasaks teist volitatud töötlejat ilma vastutava töötleja nõusolekuta. See tagab, et vastutav töötleja rakendab järelevalvet isikuandmete töötlemise ahela üle ning et iga ahela etapi juures järgitakse vastavaid turvameetmeid. (EU General… 2017, 239–240)

Põhjalike aruteludetulemusel on *Accountancy Europe*, mille liige on ka Eesti Audiitorkogu, jõudnud seisukohale, et GDPR-ist tulenevalt on finantsaudiitorid vastutavad andmetöötlejad. Kohustuslikku auditit käsitlevad õigusaktid kohustavad audiitoreid olema sõltumatud ja seepärast otsustavad audiitorid, milliseid andmeid nad auditi tegemiseks vajavad ja kuidas andmeid kasutatakse. Lisaks ei määra audiitor ega klient ühiselt töötlemise eesmärke ega meetmeid. Auditi eesmärgid ja protseduurid on kindlaks määratud seaduste ja määrustega. (GDPR: implications... 2018, 3).

Sellest tulenevalt ei peaks audiitorid sõlmima auditiklientidega andmetöötluslepingut, vaid on kohustatud looma klientide teavitamiseks isikuandmete kaitse avalduse (*Privacy Statement*) ja teavitama oma kliente, lisades auditilepingusse andmekaitse klausli. Isikuandmete kaitse avaldus peaks selgitama audiitori rolli ja kohustusi vastutava töötlejana. (*Ibid.*)

2.2. Vastutava töötleja peamised kohustused

GDPR-i 24. artikliga kehtestatakse vastutava töötleja kohustused ning vastutused isikuandmete töötlemisel, mida ta ise või kolmas osapool tema nimel teeb. Sellest tulenevalt on töötleja kohustatud rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada ja suuta näidata, et töötlemine toimub vastavalt määrusele. Sama artikli lõikes 1 nimetatud meetmed peavad võtma arvesse andmetöötluse laadi, ulatust, konteksti ja eesmärke ning üksikisikute õiguseid ja vabadust ähvardavaid ohte. (EN direktiiv (EL) 2016/679 art 24)

Suuniseid asjakohaste meetmete rakendamiseks ja nõuete täitmise tõendamiseks vastutava töötleja poolt võib anda andmekaitsenõukogu esitatud juhistega (*Ibid.* põhjenduspunkt 77). Eesti Andmekaitse Inspektsioon on Euroopa Andmekaitsenõukogu liige, mis on omapoolt andnud välja juhendmaterjali, kus on välja toodud andmetöötleja peamised kohustused (Isikuandmete töötleja… 2019, 9–10):

- Töötleja rakendab kõikides oma töötlustoimingutes isikuandmete töötlemise seitset põhimõtet (vt ptk 1.3.).
- Töötleja rakendab andmetele vastava turvalisuse taseme tagamiseks asjakohaseid korralduslikke ja tehnilisi meetmeid.

- Andmetöötleja määrab andmekaitsespetsialisti juhul, kui tema põhitegevuseks on andmesubjektide korrapärane jälgimine või eriliiki isikuandmete või süüteoandmete ulatuslik töötlemine.
- Vastutav töötleja esitab andmesubjektidele kogu vajaliku teabe nende isikuandmete töötlemise tingimuste kohta.
- Vastutavad töötlejad koostavad isikuandmete töötlemise ülevaate, mille käigus kaardistatakse kõik andmetöötlustoimingud.
- Isikuandmetega seotud rikkumise korral dokumenteerib vastutav töötleja rikkumise asjaolud, mõjud, parandusmeetmed ning teatab rikkumisest järelevalveasutusele 72 tunni jooksul pärast sellest teadasaamist. Andmekaitse subjekti tuleb rikkumisest teavitada juhul, kui rikkumisega kaasneb suur oht subjekti õigustele ja vabadustele.
- Enne tõenäoliselt suurt ohtu põhjustava andmetöötlusega alustamist peab vastutav töötleja hindama ja dokumenteerima selle mõju ning enda tegevuse. Suure ohuga on tegemist, kui toimub eriliiki või süüteo andmete ulatuslik töötlemine, avalike alade jälgimine või süsteemne ulatuslik automatiseeritud hindamine, millel on subjekti jaoks õiguslikud tagajärjed.
- Vastutav töötleja teeb oma ülesannete täitmisel koostööd järelevalveasutusega juhul, kui mõjuhinnangust selgub, et meetmete rakendamisest sõltumata jääb suur oht isiku õigustele ja vabadustele.
- Kui andmesubjekt soovib, annab vastutav töötleja andmesubjektiga seotud isikuandmed üle teisele ettevõttele.

Lisaks on juhendis toodud välja GDPR-ist tulenevad kohustused kolmandatesse riikidesse isikuandmete edastamisel, kuid sellistest toimingutest tulenevaid kohustusi antud lõputöö raames ei käsitleta.

2.3. Finantsauditis kasutatavad isikuandmed

Vastutava töötlejana töötlevad audiitorid otseselt auditiklientideks mitteolevate füüsiliste isikute isikuandmeid. Sinna hulka kuuluvad kliendi töötajad, lepingulised partnerid, tarnijad ning juhatus ja isikud, kelle ülesandeks on valitsemine. Audititeenuse olemusest tulenevalt võib see puudutada ka viimaste pereliikmeid ja ülalpeetavaid. Üldiselt esitatakse sellised isikuandmed auditiklientide või auditiga seotud kolmandate osapoolte, mitte andmesubjekti poolt. (Deloitte Central… 2019; EY Privacy Statement 2019)

Audiitorite peamine eesmärk isikuandmete töötlemisel on kokkulepitud auditiprotseduuride läbiviimine. Isikuandmete selline töötlemine audititeenuse osutamisel on vajalik auditikliendi õigustatud huvide tagamiseks ning tuleneb mõnel juhul ka seadusest (näiteks kui klient on auditikohuslane). Audiitorid peavad oma töös jälgima, et vajalikke isikuandmeid kogutaks ainult kokkulepitud eesmärkidel. (Individuals whose… 2019)

Hea tava järgi paluvad audiitorid klientidel pseudonümiseerida esitatavad tõendusmaterjalid, mis sisaldavad isikuandmeid, et maandada GDPR-ist tulenevate kohustustega kaasnevaid riske. Kui teenuse osutamiseks on vajalik isikuandmete töötlemine, peaksid auditikliendid edastama asjaomastele andmesubjektidele audiitorilt saadud teabe nende isikuandmete kasutamise kohta või audiitorettevõtja isikuandmete kaitse avalduse.

Rahvusvaheline auditeerimise standard ISA 500 sätestab audiitorile kohustuse välja töötada ja läbi viia auditiprotseduure piisava asjakohase auditi tõendusmaterjali põhjal, et olla võimeline tegema põhjendatud järeldusi, mis on aluseks audiitori arvamusele. Auditi tõendusmaterjali hangitakse peamiselt auditiprotseduuride jaoks või ka kvaliteedikontrolli protseduurides kliendi aktsepteerimise ja kliendiga jätkamise käigus. (ISA 500 A1)
Auditi tõendusmaterjal on audiitori poolt järelduste ning audiitori arvamuse tegemiseks kasutatav informatsioon. Tõendusmaterjal hõlmab nii finantsaruannete aluseks olevat arvestusandmetes sisalduvat informatsiooni kui ka informatsiooni, mis on hangitud muudest allikatest. (ISA 200 § 6 p (c)) Arvestusandmeteks on esialgsete raamatupidamiskannete andmed ja neid toetavad andmed, nagu näiteks rahaülekannete andmed, arved, lepingud, pearaamatud ja alamregistrid ning sellised andmed, mis toetavad kulude jaotamisi, arvutusi, kooskõlastavad võrdlusi ja avalikustatavat informatsiooni, nagu näiteks töölehed ja tabelarvutused (*Ibid.* p (a)).

Suuremad auditiprotseduuride teostamisel ja tõendusmaterjalide töötlemisel esinevad isikuandmete kategooriad jagunevad (Individuals whose… 2019; EY Privacy Statement 2019):

1. isikuandmed: nimi, isikukood, sünnikuupäev, sugu, elukohariik;
2. teave pereliikmete kohta: pereliikmete nimed, sünniaeg ning laste arv;
3. kontaktandmed: e-posti aadress, telefoninumber, kodune aadress;
4. finantsandmed: pangakonto number, krediidihinnang, pensionialane teave, kindlustusandmed, palgaga seotud andmed ning muud rahalised üksiknäitajad, nagu sissetulek, investeeringud, hüvitised, maksustaatus;

5. kutsealased üksikasjad: hariduslik taust, ametinimetus, tööaeg, tööalane teave ja muu teave juhtkonna ja töötajate kohta;
6. tervise ja töölt puudumise andmed: arstitõendid, haiguspuhkustega või muude puhkustega seotud teave.

Antud loetelu pole ammendav, sest võib esineda ka muude kategooriate isikuandmeid, nagu eriliiki isikuandmed, mida võib olla vaja auditi läbiviimiseks vastavalt audiitorite heale tavale ja auditeerimisstandarditele (*Ibid.*).

Lisaks töötlevad audiitorid kliendi aktsepteerimise käigus ka tuvastamis- ja taustteavet. See töötlemine on vajalik auditikliendi ehk juriidilise isikuga sõlmitud töövõtulepingu täitmiseks, kus audiitor töötleb audiitorteenuste osutamiseks kliendiettevõttega seotud eraisikute (nagu juhtkond ja nendega seotud isikud) isikuandmeid. (Individuals whose… 2019)
Audiitorettevõtja peab enne uue kliendiga töövõtu aktsepteerimist või olemasoleva töövõtu jätkamist koguma vajaliku informatsiooni, millega rakendada töövõtu tasemel kvaliteedikontrolli protseduure (ISA 220 § 6). Kvaliteedikontrolli peamised protseduurid on (EY Privacy Statement 2019):

- tegelike tulusaajate tuvastamine;
- ettevõtte ning isikute, kelle ülesandeks on juhtimine ja valitsemine, identiteedi kontrollimine;
- kliendi meedias kajastumine ehk maine kontroll;
- auditi sõltumatuse tagamiseks vajalikud kontrollprotseduurid;
- rahapesu ja terrorismi rahastamise tuvastamise kontrollid;
- huvide konflikti kontrollprotseduurid ja finantskontroll.

Need kontrollid annavad audiitorile põhjendatud kindluse, et audit on vastavuses kutsestandarditega ning kohaldatavate seadustest ja regulatioonidest tulenevate nõuetega ja audiitori väljaantud aruanne on nendes tingimustes asjakohane (ISA 220 § 6). Samuti aitavad kontrollide protseduurid audiitoril planeerida auditi töövõttu nii, et (ISA 300 A6):

- audiitor säilitab vajaliku sõltumatuse ja võime viia läbi töövõtt;
- juhtkonna aususe osas ei eksisteeri probleeme, mis võivad mõjutada audiitori valmisolekut klienditööd jätkata;
- kokkulepitud töö tingimuste osas ei eksisteeri arusaamatusi kliendiga.

Seega tulenevalt standarditest on audiitoritel olemas seaduslik alus isikuandmete töötlemiseks.

3. EESTI FINANTSAUDIITORITE PÄDEVUS ISIKUANDMETE KAITSE ÜLDMÄÄRUSE RAKENDAMISEL

Antud peatükis kirjeldab autor töös kasutatud uurimismetoodikat, uuringu tulemusi ning tulemuste põhjal tehtud järeldusi. Uurimine on protsess, mille käigus kogutakse, analüüsitakse ja tõlgendatakse uuringu käigus saadud andmeid, et mõista kindlat nähtust. Uuring saab alguse vähemalt ühest küsimusest või probleemist, mis on seotud huvipakkuva nähtusega. Antud töö uurimisprobleemiks on isikuandmete kaitse üldmääruse laienemine audiitortegevusele Eestis ning teadmatus, kui pädevad on Eesti finantsaudiitorid sellega kaasnevate kohustuste mõistmises ning määruse korrektses tõlgendamises. Uurimisprobleemist tulenevalt on töö eesmärgiks hinnata finantsaudiitorite teadlikkust isikuandmete kaitse üldmäärusest.

3.1. Kasutatud uurimismeetodid

Töös püstitatud probleemi lahendamiseks valis autor kvantitatiivse meetodi. Kvantitatiivne uurimismeetod on uurimisprobleemi ja sellega seotud nähtuse selgitamine, kogudes selleks arvulisi andmeid ja analüüsides saadud andmeid matemaatiliste meetodite abil. Antud meetodi tulemusel tehakse järeldusi ja ettepanekuid numbriliste tulemuste põhjal, saades nii objektiivsemad vastused kui kvalitatiivse meetodi kasutamisel. Kvalitatiivne meetod kasutab andmetena pigem kirjeldavaid vastuseid ning aitab otsida uusi probleeme ja võimalusi, mille abil oleks uuringu üksikasjadesse parem süvitsi laskuda. (Williams 2007, 65–68) Arvestades antud töö mahupiiranguid, on autori hinnangul targem kasutada kvantitatiivset meetodit, et leida üldistatavad vastused uurimisprobleemile ning teha järeldusi, lähtudes numbrilistest andmetest.

Kvantitatiivsetest uurimismeetoditest valis autor küsitlusuuringu. Küsitlusuuringud hõlmavad endas kogu populatsioonist valimi kasutamist koos kavandatud küsimustikuga, et mõõta konkreetse populatsiooni tunnuseid statistiliste meetodite abil. Andmed saadakse otse valimisse sattunud füüsilistelt isikutelt ning valimi vastused üldistatakse kogu populatsioonile. (Apuke 2017, 43–44) Andmete kogumiseks kasutas autor veebipõhist küsitluskeskkonda Ankeet.ee, et tagada

kiire andmete kogumine ning kerge töötlemine. Antud keskkonna lihtne lahendus ja rohked võimalused tegid selle kasutamise mugavaks nii autori kui ka vastajate jaoks.

Küsimustik koosnes 18 kohustuslikust küsimusest, millele lisandus sõltuvalt uurimisobjekti vastusest üks täiendav küsimus (vt Lisa 1). Enamus küsimusi olid kinnised (vastaja ei pidanud kirjeldama vastuseid), et küsimustik oleks vastajale võimalikult lihtsasti arusaadav ning täitmine kiire ja mugav. Peamised küsimuste liigid olid binaarsed ja mitme vastusevariandiga küsimused, järjestamisega reitinguskaala küsimused ning reitinguskaala küsimused 10-palli skaalal.

Küsimustiku koostamisel lähtus autor töö metodoloogilisest osast ning küsimustik koosnes neljast osast. Esimeses osas kaardistati vastaja ametikoht ning kokkupuude isikuandmetega. Teine osa puudutas GDPR-i põhilisi definitsioone ning küsimused aitasid autoril aru saada, kas vastaja tõlgendab määrust korrektselt ning omab arusaama selle sisust. Kolmas osa aitas autoril hinnata, kas töökeskkond avaldab mõju vastaja pädevusele. Neljanda küsimuste ploki eesmärk oli hinnata audiitori teadlikkust oma kohustustest ning seda, kui palju audiitor rakendab erinevaid meetmeid vastavuse tagamiseks.

3.2. Valimi kirjeldus ning analüüs

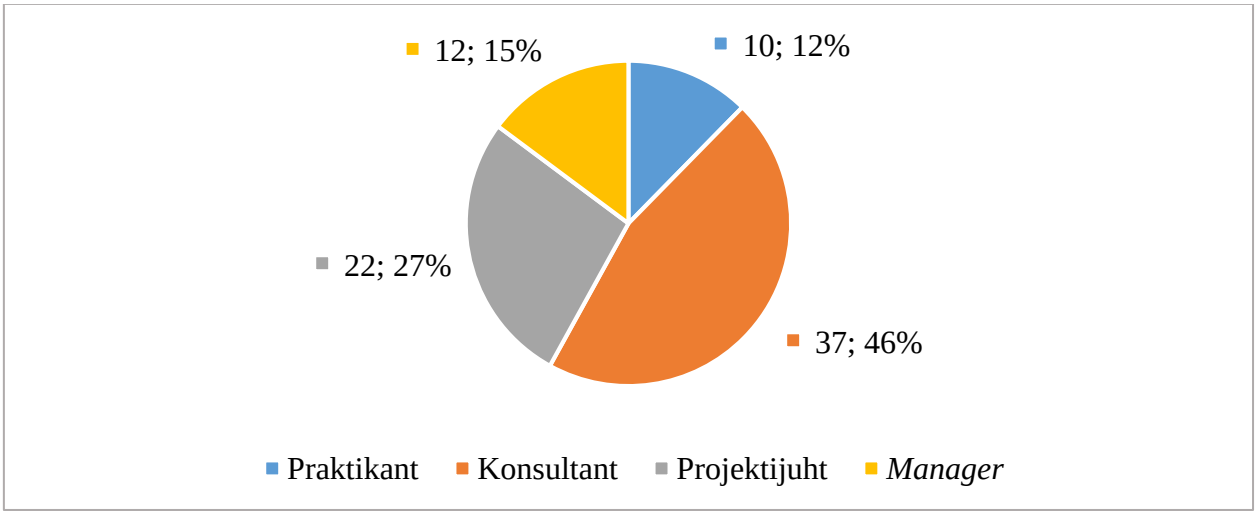
Küsimustiku sihtgrupiks olid Eesti audiitorettevõtjate finantsaudiitorid, kes puutuvad kokku isikuandmete töötlemisega. Väga suur uurimisobjektide hulk teeb uurimise keerukaks ning tihti on vaja kogu populatsiooni kitsendada ka piiratud aja tõttu (Õunapuu 2014, 139). Selleks, et piirata üldkogumit, moodustas autor audiitorite ametikohtadest lähtuvalt järgnevad osakogumid: praktikandid, konsultandid, projektijuhid ning *manager*'id.

Esimese kahe ametikoha peamisteks tööülesanneteks on auditi tööpaberite täitmine ning muude vahetu juhi poolt antud ülesannete täitmine. Ülesannete täitmiseks on vaja töödelda ning analüüsida auditite käigus kogutud tõendusmaterjali, mistõttu puutuvad nad oma igapäevatöös pidevalt kokku isikuandmetega.
Projektijuhi ülesandeks on auditi tööplaani koostamine ning auditi protseduuride läbiviimine. Kuigi täitev funktsioon on praktikantidel ning konsultantidel, siis projektijuhid kordineerivad ning kontrollivad nende poolt tehtud tööd. Juhtiv funktsioon on *manager*'idel, kelle tööülesandeks on juhendada projektijuhte ning jälgida, et auditi strateegia oleks vastavuses ettevõtte metodoloogia

ja auditistandarditega ning töövõtt saaks lõpetatud. Sageli otsustavad projektijuhid koos *manager*'idega, milliseid tõendusmaterjale on vaja auditi läbiviimiseks. Nende tööülesandeks on ka kontrollida üle kasutatud tõendusmaterjalide dokumentatsioon tööpaberites, mistõttu on nende tööülesandeks isikuandmete töötlemine.

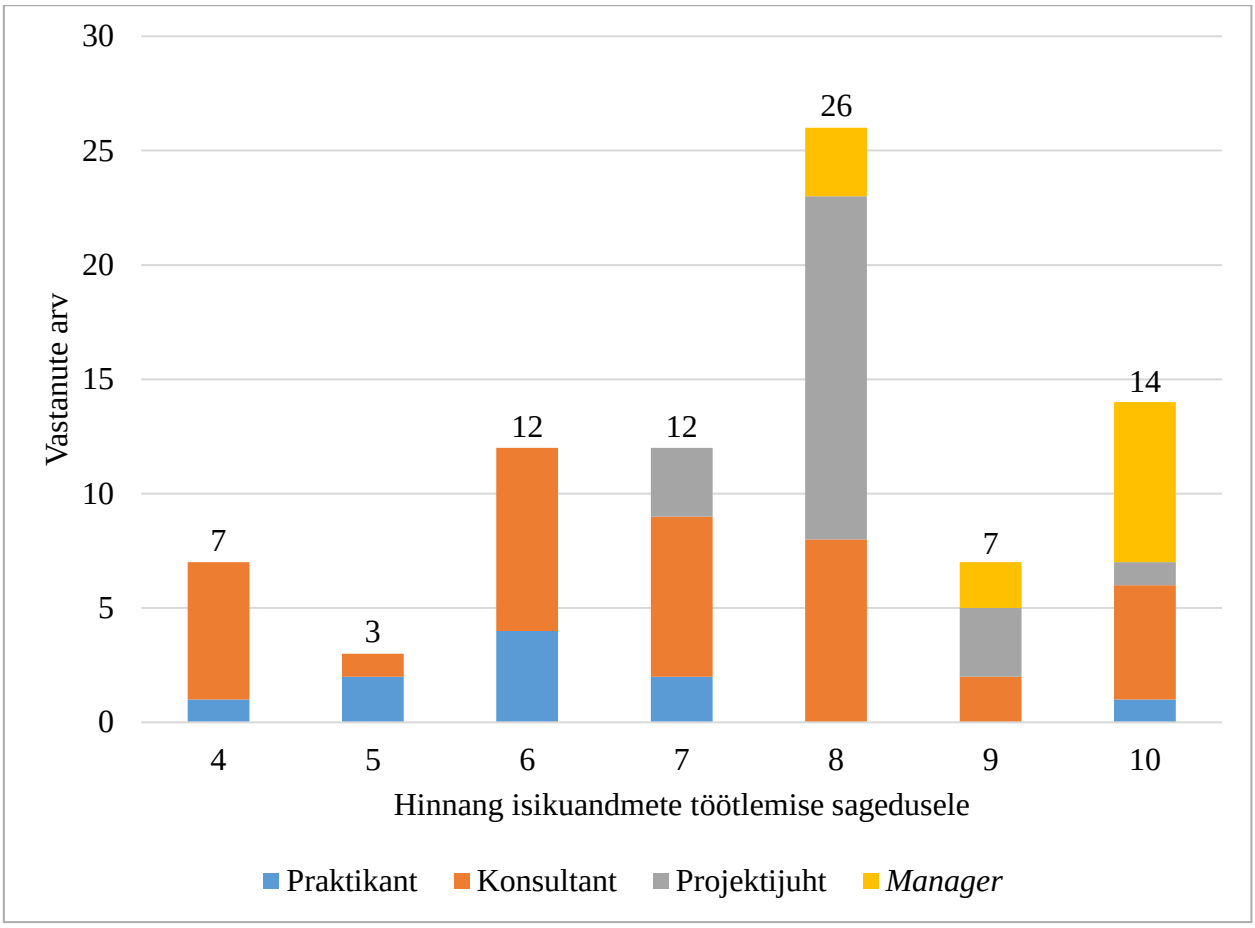
Autor kasutas valimi moodustamisel empiirilist valikut, mille korral ei ole objektide valimisse sattumise tõenäosused teada, kuid valimi moodustamise eesmärgiks on saada valim, mille strukuur langeb kokku üldkogumi struktuuriga (Sauga 2017, 241).
Empiirilise valiku meetodina kasutati sobivusvalimit, kus küsimustik saadeti Eesti suurimatesse audiitorbüroodesse, et korraga levitada küsimustikku erinevate ametikohtade hulgas ning samas katta ka suurem osa Eesti audititurust. Antud kriteeriumid aitasid populatsioonist eraldada väiksema hulga ehk valimi nii, et valimi uurimisel saadavad tulemused on nende struktuurist lähtuvalt üldistatavad üldkogumile (Õunapuu 2014, 139).

Kokku laekus vastuseid 93 finantsaudiitorilt, kellest 12 vastasid, et oma töö iseloomu tõttu nad ei töötle isikuandmeid (vt Lisa 2 Tabel 4). Nende vastused jäeti valimist välja ning lõplikuks valimi suuruseks jäi 81 vastanut. Vastanutest suurema osa moodustasid konsultandid ning kõige väiksema osalusega olid *manager*'id, mis oli oodatav tulemus. Kuna audiitorbüroodes on kõige rohkem just madalama taseme spetsialiste (praktikandid, konsultandid), siis iga kõrgema tasemega (projektijuhid, *manager*'id) väheneb spetsialistide osakaal ettevõttes ning seega peegeldab antud tulemus audiitorettevõtete struktuuri usaldusväärselt. (vt Joonis 2)



Joonis 2. Vastanute jaotus ametikoha alusel
Allikas: Autori koostatud lisa 2 tabelis 5 toodud andmete alusel

Selleks, et paremini mõista, kuidas audiitorid ise tunnetavad enda igapäevatöös kokkupuudet isikuandmetega, palus autor vastajatel hinnata, kui tihti nad isikuandmeid töötlevad. Antud küsimusele pidid vastajad andma hinnangu 10-palli skaalal, kus 1 väärtuseks oli „väga harva“ ning 10 väärtuseks „igapäevaselt“ (vt Joonis 3).

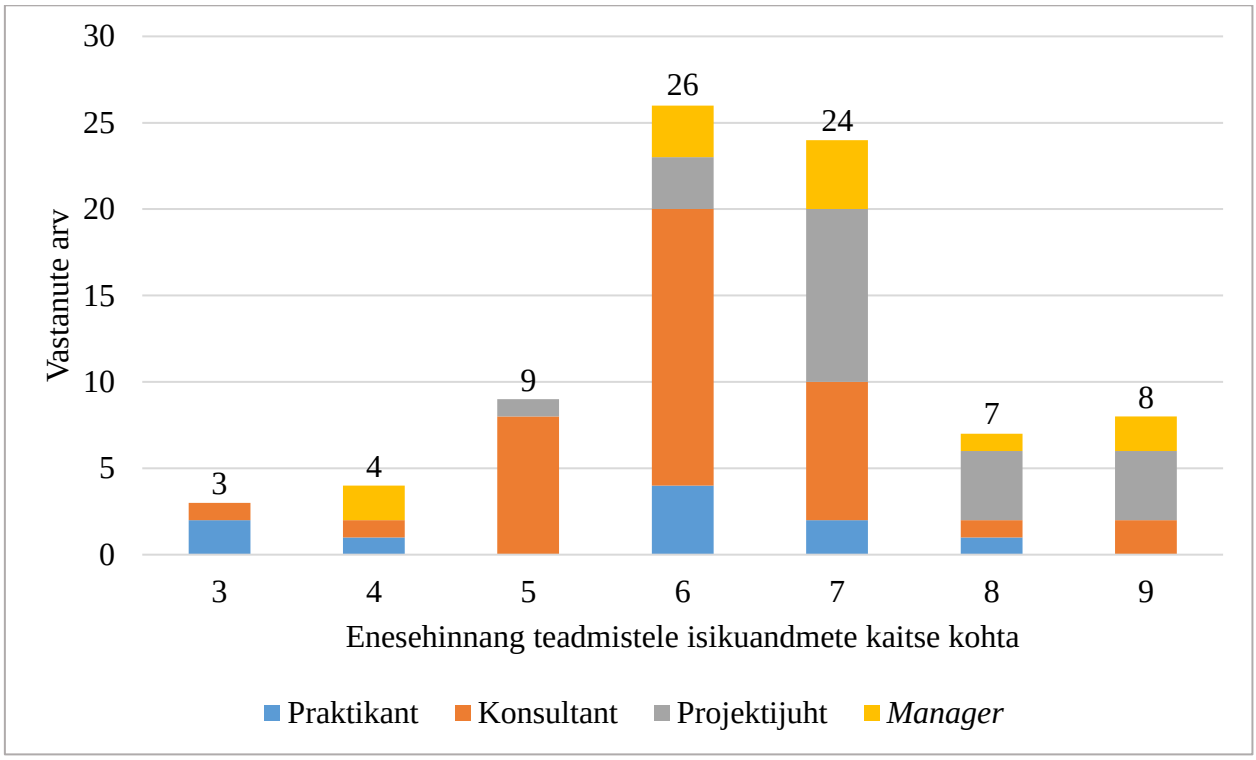


Joonis 3. Vastanute hinnang isikuandmete töötlemise sagedusele
Allikas: Autori koostatud lisa 2 tabelis 6 toodud andmete alusel

Tulemuste hindamiseks ametikohtade lõikes kasutas autor statistilisi keskmisi (vt Lisa 2 Tabel 6). Kogu valimi peale olid valimi mood ja kaalutud aritmeetiline keskmine 8, mis on võrdväärne iganädalaselt isikuandmete töötlemisega. Valimi alumiseks piiriks oli 4 ehk „kvartaalselt“ ning antud hinnangu valisid madalama taseme ametikohad. Valimi ülemiseks piiriks oli 10, mida valisid iga ametikoha esindajad, kuid kõige enam *manager*’id (58% kõikidest *manager*’idest).
Kaalutud aritmeetiliste keskmiste alumiseks piiriks oli 6, mis oli praktikantide kaalutud keskmine. Iga järgneva ametikohaga suurenes kaalutud keskmine ühe võrra ning ülemiseks piiriks oli 9, mis oli *manager*’ide kaalutud keskmine.

Tulemusi võib mõjutada fakt, et sageli ei tööta madalama ametikoha audiitorid täisajaga ning sellest tulenevalt ei saa ka hinnata sagedust maksimaalse väärtusega. Siiski oleks oodatav, et madalama ametikoha audiitorid hindaksid, et nad töötlevad isikuandmeid iganädalaselt, kuid antud tulemuste põhjal on hinnang pigem üks või mitu korda kuus. Kõrgema ametikoha audiitorid aga hindasid, et töötlemine toimub nädalas üks kuni mitu korda.

Analüüsides valimiobjektide hinnangut enda teadmistele isikuandmete kaitse kohta 10-palli skaalal, kus 1 oli võrdväärne „teadmised puuduvad“ ja 10 „teadmised on täielikud“, sai autor alumiseks piiriks 3 ning ülemiseks piiriks 9 (vt Joonis 4).



Joonis 4. Vastanute enesehinnang teadmistele isikuandmete kaitse kohta
Allikas: Autori koostatud lisa 2 tabelis 7 toodud andmete alusel

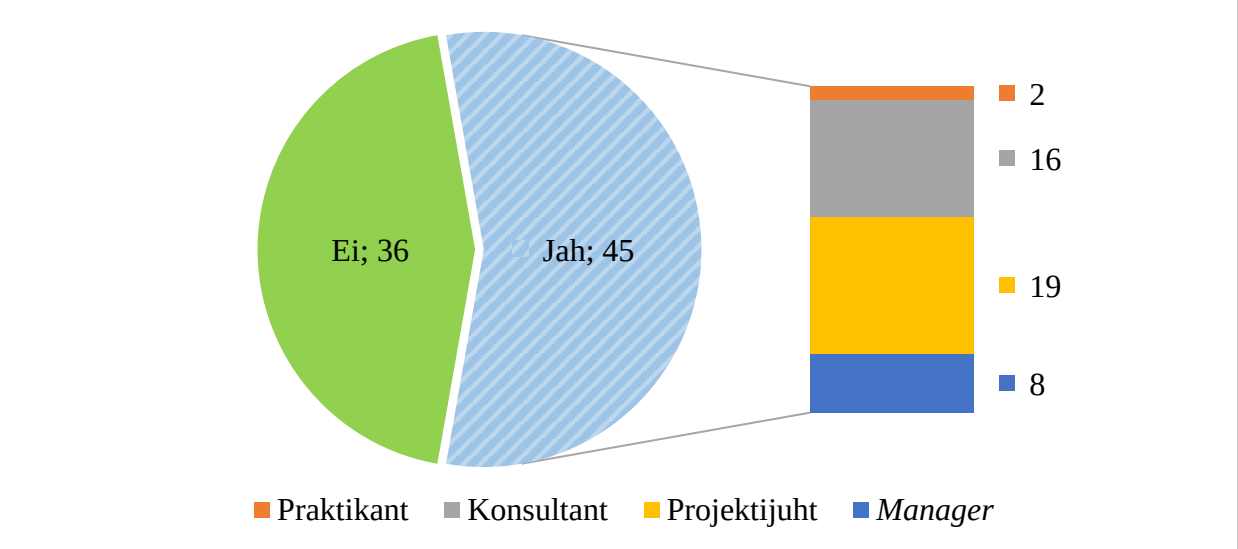
Mitte ükski vastanutest ei hinnanud enda teadmisi täielikuks ega polnud ka neid, kes leidsid, et teadmised puuduvad. Nii *manager*'id kui ka projektijuhid hindasid keskmiselt oma teadmisi pigem heaks. Kaalutud keskmisest lähtudes on praktikantide ning konsultantide hinnang oma teadmistele rahuldav. (vt Lisa 2 Tabel 7)

3.3. Eesti finantsaudiitorite teadmised isikuandmete kaitse üldmääruse põhiaspektidest

GDPR-i raamistikust lähtudes on finantsaudiitor vastutav töötleja, kellel on õigus otsustada, kuidas ja mis andmeid töödeldakse ning kes vastutab selle eest, et kõikide andmesubjektide isikuandmete töötlemine toimuks vastavuses GDPR-iga.

Küsitluses osalejad pidid märkima, kas nende hinnangul nad otsustavad, miks ja kuidas kliendi andmeid töödeldakse. Antud väitega nõustus 56% vastanutest (vt Joonis 5). Suurem osa projektijuhtidest (19; 86% kõikidest projektijuhtidest) ning *manager*'idest (8; 67% kõikidest *manager*'idest) hindasid end vastutavaks töötlejaks, moodustades 60% kõikidest nõustunud audiitoritest.

Vähem nõustusid konsultandid (16; 43% kõikidest konsultantidest) ning praktikandid (2; 20% kõikidest praktikantidest). Madalama ametikoha audiitorid hindasid pigem, et nemad ei ole vastutavad töötlejad, moodustades 81% kõikidest vastanutest, kes ei nõustunud küsimusega. (vt Lisa 3 Tabel 8).



Joonis 5. Vastus küsimusele: „Kas Te otsustate kuidas ja milliseid kliendi andmeid töödeldakse?"
Allikas: Autori koostatud lisa 3 tabelis 8 toodud andmete alusel

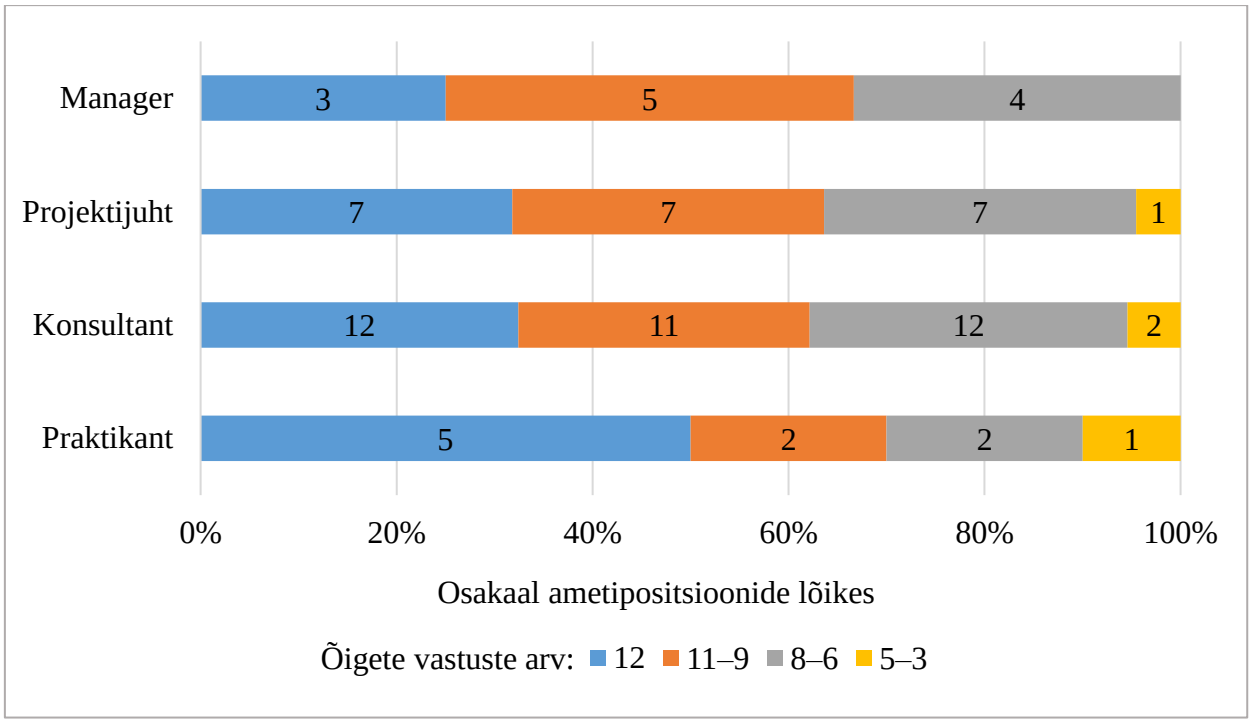
Antud tulemust mõjutab tööjaotus audiitorbüroodes. Üldiselt on büroodes püramiidne personali struktuur, kus igaüks saab enda tööülesanded tase kõrgemalt isikult, ning samamoodi toimib ka tehtud töö kontrollimine. Madalamate ametikohade töötajad saavad üldiselt projektijuhtidelt nii

tööjuhised kui ka sisendi, milliseid tõendusmaterjale on vaja küsida, seega on nad GDPR-i mõistes volitatud töötlejad. GDPR-i artikkel 82 lõike 2 kohaselt vastutab ka volitatud töötleja töötlemise käigus määruse nõuete täitmise eest ning on kohustatud jälgima vastutava töötleja juhiseid (EN direktiiv (EL) 2016/679).

Küsitluse käigus pidid vastanud tuvastama õige definitsiooni isikuandmetele. Vastusevariante oli kokku neli ja neist õige üks („Isikuandmed on igasugune teave tuvastatud või tuvastatava elava füüsilise isiku kohta.“) ning selle valis 46% kogu valimist (vt Lisa 3 Tabel 9). Vastanutest 10% valis teise definitsiooni, milles oli välja jäetud tunnus, mille kohaselt andmesubjekt peab olema elav isik. GDPR-i põhjenduspunkt 27 aga näeb ette, et antud määrust ei kohaldata surnuid puudutavatele isikuandmetele (EN direktiiv (EL) 2016/679).
Vastanutest 44% valis aga definitsiooni, kus oli märgitud andmesubjektiks ka juriidiline isik. Antud vastuseid valisid peamiselt konsultandid (43% kõikidest konsultantidest), kuid kõrge osakaaluga olid ka projektijuhid (46% kõikidest projektijuhtidest) ning *manager*'id (50% kõikidest *manager*'idest).

Autor palus vastanutel valida, mis on nende hinnangul isikuandmed (vt Lisa 3 Tabel 10). Küsimuses oli loetletud 12 põhilist isikuandmete liiki, millest kõige populaarsemateks valikuteks osutusid finantsandmed, isikukood, kontaktandmed ning teave terviseseisundi ja pereliikmete kohta. Antud vastused valis pea 90% kogu valimist. Võrguidentifikaator oli ainuke vastuse valik, mille valisid vähem kui pooled valimist (48%) ning ei esinenud ühtegi valikut, mida ükski vastanutest ei pidanud isikuandmeteks. Teised vähem populaarsed vastused olid ühingusse kuuluvuse teave (59%) ning ametialane teave (58%).

Kui hinnata õigete vastuste osakaalu ametikohtade lõikes, siis enim valisid kõik valikuvariandid konsultandid (43% kõikidest konsultantidest) (vt Joonis 6). Ka projektijuhtidest valis kõige suurem osa (36% kõikidest projektijuhtidest) kõik 12 vastusevarianti. *Manager*'i tasemel oli kõige suurema osakaaluga (42% kõikidest *manager*'idest) valik 9–11 vastusevarianti ning praktikantide puhul (60%) 6–8 vastust.



Joonis 6. Küsimusele 7 vastanute õigete vastuste jaotus ametikohtade lõikes
Allikas: Autori koostatud lisas 1 toodud küsimustiku ja lisa 3 tabelis 10 andmete alusel

Audiitoritel palus valida ka loetelust, kes on nende hinnangul andmesubjekt (vt Lisa 3 Tabel 12). Loetelus olid nimetatud peamised auditikliendiga seotud füüsilised (4 vastusevarianti) ja juriidilised isikud (2 vastusevarianti). Kõige populaarsemaks (89%) osutus vastus „ettevõtte töötajad“ ehk peamised eraisikud, kelle isikuandmeid auditi käigus töödeldakse. Samuti valis üle 80% valimist andmesubjektiks juhatuse ja valitsejad ning auditikliendi eraisikust kliendi või koostööpartneri. Vastanutest 67% hindas andmesubjektiks ka ettevõtte, kuigi tegemist on juriidilise isikuga. See oli ka enim valitud vale vastus kõikide ametikohtade seas.

Andmeid analüüsides selgus, et 53% vastanutest märkis kõik juriidilised isikud andmesubjektideks (vt Tabel 1). Antud arvamust esines igal ametikohal vähemalt poolte seas. Kõigest 21% ei märkinud ühtegi juriidilist isikut andmesubjektiks, kuid jätsid see-eest mõne füüsilise isiku märkimata. Leidus ka üksikuid vastanuid madalamatelt ametikohtadelt, kes ei hinnanud ühtegi füüsilist isikut andmesubjektiks (2; 2% kogu valimist) Peaaegu pooled vastanutest (48%) suutsid valida kõik eraisikud, kelle andmeid auditite käigus võidakse töödelda.

Tabel 1. Andmesubjekti loetelu õigete ja väärate vastuste jaotus ametikohtade lõikes

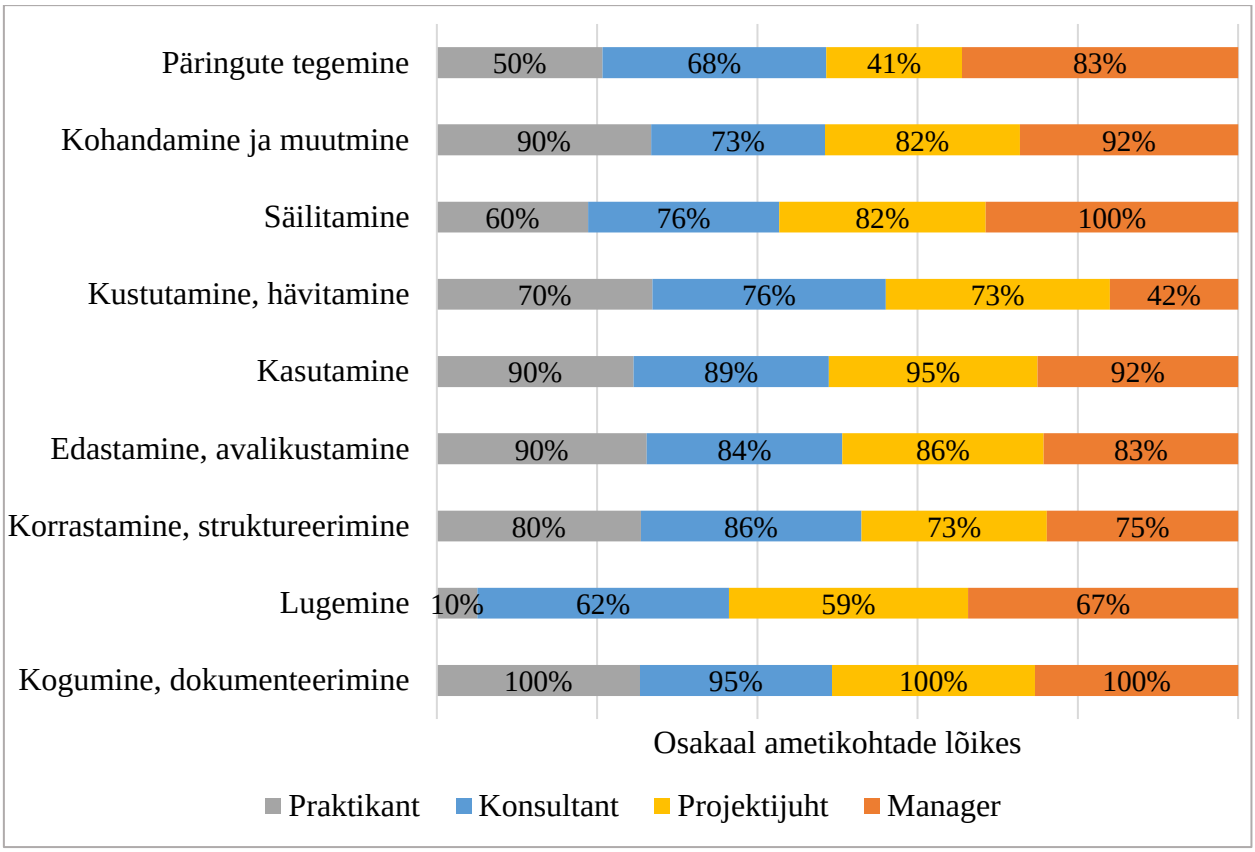
	Väärate vastuste arv				Õigete vastuste arv					
	2	1	0	**Kokku**	0	1	2	3	4	**Kokku**
Praktikant	6	3	1	**10**	1	2	1	3	3	**10**
	60%	30%	10%	**100%**	10%	20%	10%	30%	30%	**100%**
Konsultant	20	8	9	**37**	1	-	6	15	15	**37**
	54%	22%	24%	**100%**	3%	-	16%	41%	41%	**100%**
Projektijuht	11	9	2	**22**	-	2	2	6	12	**22**
	50%	41%	9%	**100%**	-	9%	9%	27%	55%	**100%**
Manager	6	1	5	**12**	-	1	-	2	9	**12**
	50%	8%	42%	**100%**	-	8%	-	17%	75%	**100%**
Kokku	**43**	**21**	**17**	**81**	**2**	**5**	**9**	**26**	**39**	**81**
	53%	**26%**	**21%**	**100%**	**2%**	**6%**	**11%**	**32%**	**48%**	**100%**

Allikas: Autori koostatud lisas 1 toodud küsimustiku ja lisa 3 tabelis 12 andmete alusel

Autor analüüsis ka, kui paljud õige isikuandme definitsiooni valinud vastajatest märkisid valikust kõik andmesubjektid korrektselt. Õige definitsiooni valinud 37 vastanust kõigest 6 (16%; 7% kogu valimist) vastasid õigesti ka andmesubjekti küsimusele. Kokku oli kogu valimi peale õigeid vastuseid 10 (12%). Ülejäänud 4 vastajat valisid andmesubjekti definitsiooni, kus puudus tunnus, mille alusel on andmesubjekt elav füüsiline isik. Seega kuigi pea pooled vastanud suutsid märkida ära kõik eraisikud, märkisid nad samas ka juriidilisi isikuid ehk ei saa järeldada, et audiitoritel oleks ülevaadet, kes on nende igapäevatöös GDPR-i mõistes andmesubjekt.

Isikuandmete kaitse rakendumisest ei saa rääkida enne, kui pole toimunud isikuandmete töötlemist. Selleks peab vastutav töötleja aru saama, millised toimingud on GDPR-i mõistes töötlemisprotsessid. Vastajad pidid märkima loetelust kõik toimingud, mis on nende hinnangul töötlemistegevused. Vastuse variandid olid määratud lähtudes GDPR-i artikli 4 isikuandmete töötlemise definitsioonist ning loetelus polnud valet vastust (EN direktiiv (EL) 2016/679).

Kui vaadata enim hinnatud valikuid ametikohtade lõikes, siis esines kogu valimiga võrreldes paar erinevust (vt Joonis 7). Kõik *manager*'id märkisid ära säilitamise, mis teiste tasemete puhul polnud kõige populaarsem vastus. *Manager*'id üldiselt vastutavad lõpliku töövõtu ülevaatamise eest ning ka tihtipeale töövõtu arhiveerimise eest. Teine erinevus oli konsultantide hinnangus, kellest 86% (32) leidis, et korrastamine ja struktureerimine on andmete töötlemine (teiste tasemete puhul jäi see osakaal keskmiselt 76% juurde). Jällegi saab seostada seda ametikohtade kohustustega, sest üldiselt on konsultandid need, kes tegelevad enim ettevõtete süsteemides suurte andmemahtude töötlemise ja struktureerimisega.



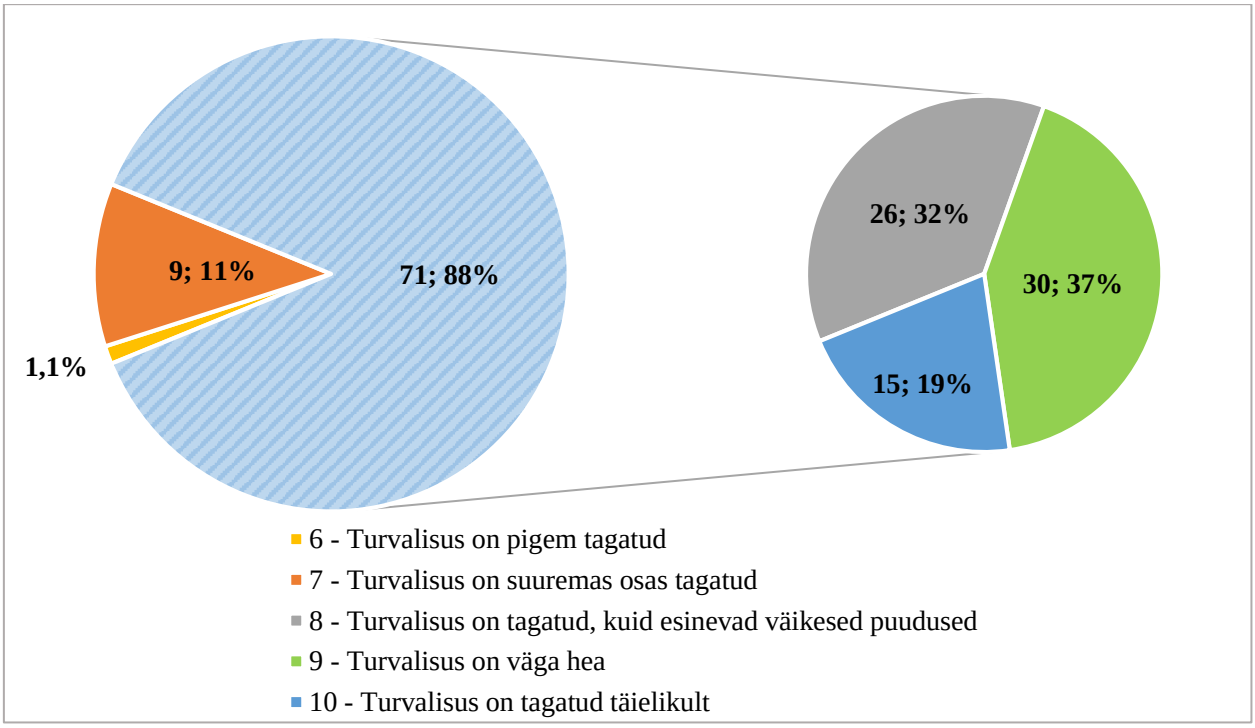
Joonis 7. Töötlemise loetelu vastuste jaotus ametikohtade lõikes
Allikas: Autori koostatud lisas 1 toodud küsimustiku ja lisa 3 tabelis 11 andmete alusel

Pea kõik vastanud (98%) märkisid, et nende hinnangul on andmete kogumine ning dokumenteerimine isikuandmete töötlemine (vt Lisa 3 Tabel 11). Antud tulemus oli oodatav, sest auditi käigus koguvad audiitorid kliendilt tõendusmaterjale, mille dokumenteerimine on standarditest tulenevalt kohustuslik. Teised kõige enim valitud vastused olid veel andmete kasutamine (91%) ning andmete edastamine ja levitamine (85%). 30% valimist märkis kõik loetletud toimingud töötlemiseks ja neid, kes jätsid ühe valimata, oli 25%. Kõige vähem (56%) pidasid vastajad töötlemiseks lugemist. Vastanutest 4% (3 kogu valimist) valisid ainult kolm varianti üheksast, milleks peamiselt olid kogumine, kohandamine ning korrastamine, struktureerimine.

3.4. Eesti audiitorettevõtjate vastavus isikuandmete kaitse üldmäärusega

Töötaja pädevust mõjutab suures osas ka tööandja vastavus GDPR-i nõuete rakendamisel. 2018. aastal ennustati, et suurem osa ettevõtetest ei suuda viia end vastavusse GDPR-i nõuetega enne üldmääruse jõustumist 2018 kevadel. 2019. aastal viidi läbi uuring, mille kohaselt 31% vastanutest saavutasid vastavuse 2018. aasta lõpuks ja 30% vastanutest saavutavad vastavuse alles 2019. aasta jooksul. Suurem osa vastanutest (80%) nentisid, et võrreldes teiste ettevõtetele kehtivate privaatsuse ja turvalisuse nõuetega oli vastavust raskem saavutada ning sellest tulenevalt võttis vastavuse tagamine ka oodatust kauem aega. (Keeping pace … 2019, 16)

Kui valimil paluti hinnata 10-palli skaalal oma ettevõtte vastavust, olid tulemused väga head (vt Joonis 8). See näitab, et vastanud hindavad ettevõtte poolt isikuandmete kaitse jaoks rakendavaid turvameetmeid efektiivseks. Vastanutest 88% leidis, et nende ettevõttes on turvalisus tagatud täielikult või esineb väiksemaid puuduseid. Kõige madalam antud hinnang oli võrdne 6 palliga („turvalisus on pigem tagatud“) ning seda ainult ühe vastaja poolt.



Joonis 8. Vastanute hinnang tööandja isikuandmete kaitse turvameetmetele
Allikas: Autori koostatud lisa 4 tabelis 13 toodud andmete alusel

Autor koostas isikuandmete töötlemise põhimõtetest lähtuvalt loetelu erinevatest meetmetest, mille rakendamisel on tööandja vastavuses GDPR-iga. Esiteks peab iga ettevõte kehtestama juhendid, sisekorrad ja eeskirjad isikuandmete töötlemise kohta. Tervelt 95% valimist kinnitas, et nende tööandja on koostanud vastavad dokumendid (vt Lisa 4 Tabel 14).
Teiseks peavad ettevõtte töötlemissüsteemid vastama turvalisuse nõuetele. Vastanutest 81% leidis, et nende IT-süsteemid on viidud nõuetega vastavusse, kuid ainult poolte (53%) vastanute tööandjad hindavad regulaarselt turvameetmete vastavust ning rakendamist.
Vastavuse tagamiseks peavad töötajad esmalt mõistma, et nad on vastutavad töötlejad. Selleks saavad tööandjad korraldada koolitusi ning määrata andmekaitsespetsialisti, kes jälgib ettevõtte GDPR-i vastavust. 2019. aastal korraldatud uuringu andmetel on 2019. aasta juuli seisuga 90% vastanutest määranud endale andmekaitsespetsialisti, mis on väga kõrge saavutus, arvestades, et tegemist on eeldustega nõudega, mis ei rakendu kõikidele ettevõtetele (Keeping pace … 2019, 21). Sarnaselt mainitud uuringu tulemustele on 85% lõputöö küsitluses osalenute tööandja määranud andmekaitsespetsialisti ning 84% osalenu tööandja on organiseerinud andmekaitseteemalisi koolitusi.

Autor uuris ka turvalisuse hinnangu seost ettevõtte poolt vastanute arvates rakendatavate turvameetmetega (vt Tabel 2).

Tabel 2. Tööandja turvalisuse hinnangu seos ettevõtte poolt rakendavate turvameetmega

	Tööandja poolt rakendatud meetmed turvalisuse tagamiseks:				
	GDPR koolitused	Juhendid, sisekorrad ja eeskirjad	Andmekaitse-spetsialist	GDPR-iga vastavuses IT-süsteemid	GDPR audit
Hinnang 10	12	15	15	15	15
Osakaal vastanutest	80%	100%	100%	100%	100%
Hinnang 9	25	30	23	23	12
Osakaal vastanutest	83%	100%	77%	77%	40%
Hinnang 8	24	25	21	20	14
Osakaal vastanutest	92%	96%	81%	77%	54%
Hinnang 7	6	6	9	7	1
Osakaal vastanutest	67%	67%	100%	78%	11%
Hinnang 6	1	1	1	1	1
Osakaal vastanutest	100%	100%	100%	100%	100%

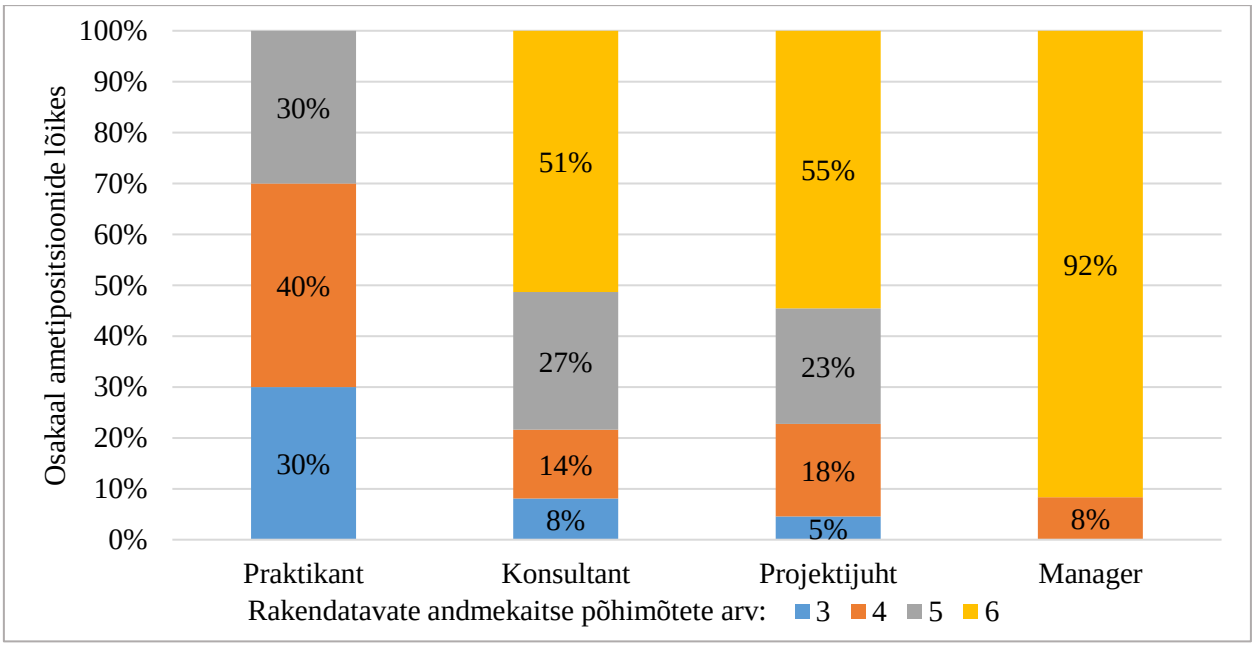
Allikas: Autori koostatud lisas 1 toodud küsimustiku ja lisa 4 andmete alusel

80% neist, kes hindas ettevõttes turvalisuse täielikult tagatuks, märkis, et ettevõttes on kõik nõuded täidetud. Ülejäänud 20% jättis loetelus märkimata ainult GDPR-i teemadlised koolitused.
Nende vastanute seas, kes hindasid ettevõtte turvalisust kas väga heaks või osaliselt puudulikuks, ei viida regulaarselt läbi turvameetmete vastavuse hinnanguid ehk GDPR auditeid.
Vastaja, kes hindas, et turvalisus on pigem tagatud, märkis ära kõik tööandja poolt rakendatud turvalisuse meetmed. Madalam hinnang ettevõtte turvalisusele võib peegelduda rakendatud meetmete ebaefektiivsuses või muudes asjaoludes, mida antud loetelus polnud välja toodud.

3.5. Eesti finantsaudiitorite teadmised isikuandmete kaitse üldmääruse kohustustest

Töötleja peamiseks kohustuseks on jälgida töötlemisprotsesside käigus andmete töötlemise kuut põhimõtet, mis on sätestatud GDPR-i artikkel 5-ga. Osalejad pidid märkima, milliseid töötlemise põhimõtteid nad andmete töötlemisel järgivad (vt Lisa 5 Tabel 16).
Kõige enam (93% kogu valimist) koguvad audiitorid ainult andmeid, mis on vajalikud töötlemise eesmärkide täitmiseks. Kogu valimist 91% väitis, et nemad töötlevad andmeid turvaliselt ning andmed, mida kasutatakse töötlemiseks, on aja- ja asjakohased. Põhimõtetest kõige ebapopulaarsem (69% kogu valimist) oli andmete säilitamise tähtaegade järgimine. Ainult kõik *manager*'id nõustusid sellega täielikult, teistel tasemetel oli nõustujaid 64%. Teine ebapopulaarne vastus oli andmete seaduslik ja õiglane töötlemine (79% kogu valimist), millega nõustus 30% praktikantidest ja 86% teiste tasemete töötajatest.

Mida madalam on tase organisatsiooni hierarhias, seda vähem rakendatakse kõiki põhimõtteid (vt Joonis 9). Kui vaadata ametikohtade lõikes, siis 92% *manager*'idest rakendavad kõiki põhimõtteid andmete töötlemisel. Projektijuhtidest rakendab kõiki põhimõtteid 55% ning 23% vähemalt viit põhimõtet. Konsultantidest rakendab 51% kõiki põhimõtteid, 27% viit põhimõtet ning ülejäänud 22% nelja või kolme põhimõtet. Praktikantide seas rakendatakse kõige rohkem (40% kõikidest praktikantidest) nelja põhimõtet ning mitte ükski praktikant ei märkinud ära kõiki põhimõtteid.



Joonis 9. Rakendatavate andmekaitse põhimõtete arv ametikohtade lõikes
Allikas: Autori koostatud lisas 1 toodud küsimustiku ja lisa 5 tabeli 16 andmete alusel

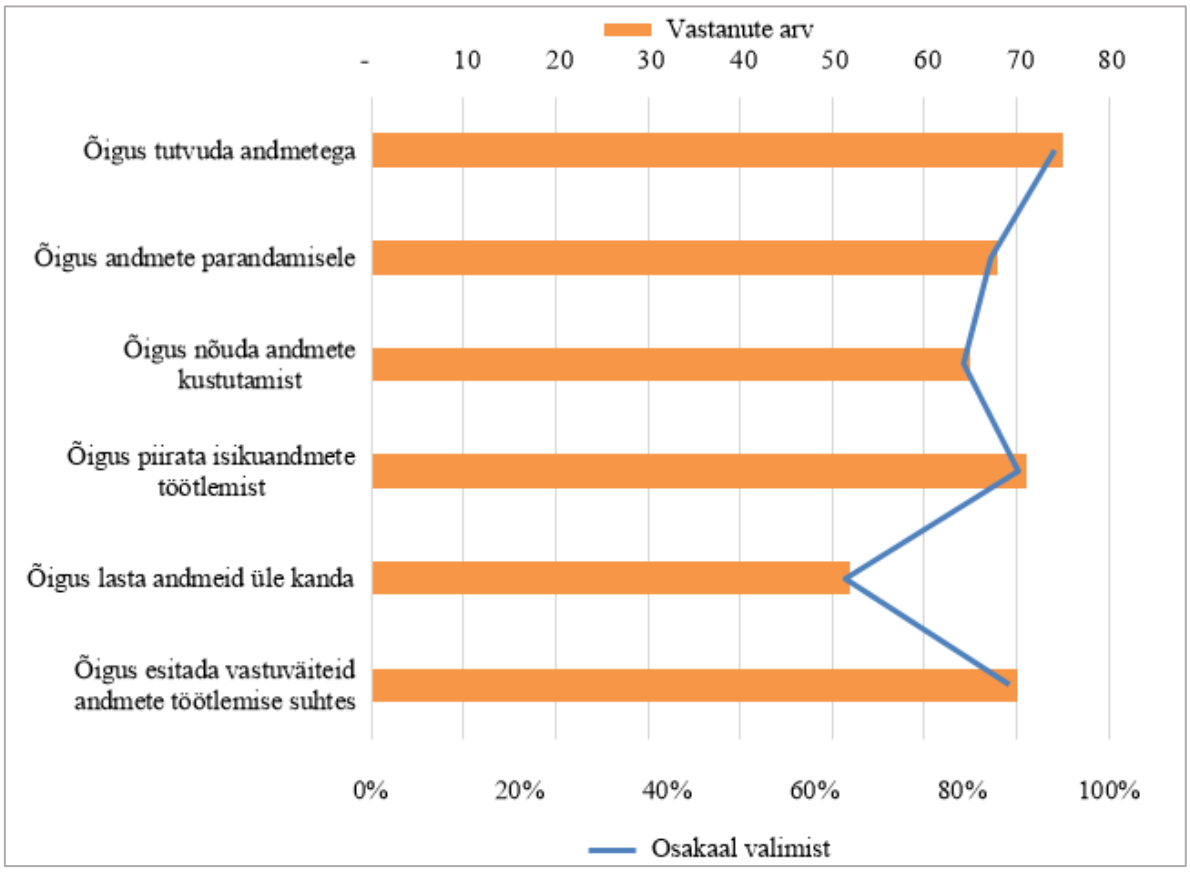
Selleks, et vähendada määruse rakendumise ulatust, on töötlejatel õigus isikuandmeid pseudonümiseerida ning anonümiseerida. Auditi tõendusmaterjalide omavahelise kokkuviidavuse vajaduse tõttu pole anonümiseerimine alati võimalik, kuid ka efektiivne pseudonümiseerimine tagab andmesubjektile tema õigused. Autor palus vastajatel hinnata 10-palli skaalal, kui tihti nad antud meetodeid rakendavad või paluvad kliendil rakendada.

Sõltumata ametikohast on audiitorite huvi vähendada GDPR-ist tulenevaid kohustusi läbi pseudonümiseerimise ja anonümiseerimise pigem minimaalne (vt Lisa 5 Tabel 17). Kogu valimist 21% ei palu kliendil kunagi andmeid muuta ning 30% palub seda teha üksikutel kordadel või harva. Pseduonümiseerimist ja anonümiseerimist rakendavad kõige rohkem projektijuhid ja *manager*'id, kellest üle poole (51%; 67% vastavalt) paluvad sageli klientidel andmeid muuta.
Samuti ei töötle audiitorid saadud tõendusmaterjali ise nii, et vähendada määrusest tulenevaid kohustusi (vt Lisa 5 Tabel 18). Nimelt ei pseudonümiseeri ega anonümiseeri 31% audiitoritest kunagi kliendilt saadud andmeid ning neid, kes teevad seda sageli kuni enamasti, on kokku kõigest 22%.
Vastanute seas ei olnud audiitoreid, kes muudaks andmeid alati või peaaegu alati. Neid, kes lasevad andmeid enamasti või peaaegu alati kohandada, on kõigest 9% kogu valimist. Seda kinnitab ka tugev korrelatsioon (r = 0,84) audiitorite vastuste vahel. Audiitorid, kes ei palu klientidel

pseudonümiseerida või anonümiseerida andmeid, ei tee seda ka ise ning need üksikud, kes paluvad, kohandavad ka vajadusel andmeid ise.

Määruse artiklite 15–21 kohaselt peab töötleja teavitama andmesubjekti isikuandmete töötlemisest kokkuvõtlikult ja arusaadavalt, juhul kui andmesubjekt seda taotleb. Vastanutest 35% ei palu kunagi kliendil informeerida andmesubjekti isikuandmete töötlemise kohta (vt Lisa 5 Tabel 19). Neid, kes teeksid seda vähemalt sageli või alati, on 26% kogu valimist.

Autor palus küsitluses osalejatel hinnata ka, mis on nende arvates andmesubjekti õigused (vt Joonis 10). Valimist 53% leidis, et kõik loetletud õigused on andmesubjekti õigused. Neid, kes märkisid valikust viis õigust, oli kokku 15% ning üldjuhul jäeti märkimata andmesubjekti õigus andmeid üle kanda. Samamoodi arvasid ka need, kes märkisid kokku neli õigust (14% kogu valimist), kuid ei leidnud, et andmesubjektil on õigus nõuda andmete kustutamist. Seda peegeldab Joonis 10, millel on näha, et kaks kõige vähem valitud vastust olid õigus lasta andmeid üle kanda (64% kogu valimist) ning õigus nõuda andmete kustutamist (80% kogu valimist).



Joonis 10. Vastanute hinnang andmesubjekti õigustele
Allikas: Autori koostatud lisa 5 tabelis 15 toodud andmete alusel

Üheks andmete töötleja kohustuseks on raporteerida kõik isikuandmete kaitsega seotud rikkumised. Sõltuvalt rikkumise ulatusest pole töötlejal alati andmesubjekti kohese teavitamise kohustust.

Joonisel 11 on näidatud, milline peaks olema info liikumine isikuandmetega seotud rikkumise korral. Esmalt peaks töötleja pöörduma audiitorettevõtte andmekaitsespetsialisti poole ning viimase puudumisel tööandja poole, et arutada, kas toimunud rikkumine on ka GDPR-i mõistes isikuandmetega seotud rikkumine. Kontakteerumine andmekaitsespetsialisti või tööandjaga peab toimuma kohe rikkumise ilmnemisel, sest juhul, kui tegemist on GDPR-i mõistes rikkumisega, peab kas andmekaitsespetsialist või rikkuja võtma ühendust järelevalveasutusega 72 tunni jooksul (EN direktiiv (EL) 2016/679 33 lg 1). Sõltuvalt järelevalveasutuse hinnangust võib rikkujal tekkida ka kohustus teavitada andmesubjekti. Kuna üldiselt ei töötle audiitorid otsese auditikliendi kontaktisiku andmeid vaid ettevõttega seotud füüsiliste isikute andmeid, peab audiitor võtma ühendust auditi kontaktisikuga, et tema kaudu informeerida rikkumisest andmesubjekti.

Joonis 11. Info liikumine isikuandmetega seotud rikkumise korral
Allikas: EN direktiiv (EL) 2016/679, autori koostatud

Vastajad pidid järjestama olulisuse järjekorras, keda nemad isikuandmete rikkumise korral esmalt informeeriksid (vt Tabel 3). Madalama taseme töötajad informeeriksid esmalt tööandjat ning andmekaitsespetsialisti, siis auditiklienti, kelle kaudu informeeritaks ka andmesubjekti, ning kõige viimasena järelevalveasutust. Arvestades, et kõikides ettevõtetes pole andmekaitsespetsialisti, ei ole järjestuse algus vale. Madalama taseme töötajad eeldavad, et järelevalveasutusega suhtlemise eest vastutab tööandja ning sellest tulenevalt on see ka viimane lüli, keda nad ise informeeriksid.

Seevastu kõrgematel ametikohtadel olevad spetsialistid, kellel on ka kõrgem vastutus, informeeriksid esmalt ise järelevalveasutust, siis kas tööandjat või andmekaitsespetsialisti ning seejärel klienti ja kliendiga seotud andmesubjekti. Antud järjekord pole vale, sest rikkuja võib ka kohe kontakteeruda järelevalveasutusega, kuid samuti peab ta informeerima tööandjat.

Kuigi vastuste järjestused erinesid ametikohtade lõikes, ei saa lugeda ühtegi neist valeks. Oluline on, et audiitorid teaksid, et rikkumise korral on nad kohustatud esmalt teavitama järelevalveasutust või andmekaitsespetsialisti ning viimase puudumisel tööandjat.

Tabel 3. Isikuandmetega seotud rikkumise korral infoliikuvuse järjestus ametikohtade lõikes

	Järjestus				
	1	**2**	**3**	**4**	**5**
Valim	Tööandja	Andmekaitse-spetsialist	Auditikliendi kontaktisik	Andmesubjekt	Järelevalve-asutus
Praktikant	Tööandja	Andmekaitse-spetsialist	Auditikliendi kontaktisik	Andmesubjekt	Järelevalve-asutus
Konsultant	Tööandja	Andmekaitse-spetsialist	Auditikliendi kontaktisik	Andmesubjekt	Järelevalve-asutus
Projektijuht	Järelevalve-asutus	Tööandja	Andmekaitse-spetsialist	Auditikliendi kontaktisik	Andmesubjekt
Manager	Järelevalve-asutus	Tööandja	Andmekaitse-spetsialist	Auditikliendi kontaktisik	Andmesubjekt

Allikas: Autori koostatud lisas 1 toodud küsimustiku ja lisa 5 tabelis 20 andmete alusel

Viiel protsendil vastanutest on esinenud GDPR-i mõistes rikkumisi (vt Lisa 5 Tabel 21). Vastanutel paluti kirjeldada rikkumise sisu ning selle lahendamiseks kasutatud meetmeid. Peamiseks põhjuseks oli kliendiandmete saatmine valele adressaadile. Kliendiandmeid saadeti enda ettevõtte siseselt teistele audiitoritele, kes polnud antud kliendiga seotud, ning neil paluti saadud kiri ära kustutada. Ühel juhul saadeti teisele kliendile auditikliendi andmeid, mille puhul läheneti samamoodi ning paluti kolmandal osapoolel kiri ära kustutada.

Ühe rikkumisena tõi projektijuht välja, et süsteemides oli jäetud auditikliendi töövõtuga mitteseotud töötajatele ligipääs kõikidele tõendusmaterjalidele. Antud probleem lahendati koostöös tööandjaga ning süsteemis vaadati riskide vähendamiseks üle iga kliendiga seotud ligipääsud.

3.6. Järeldused ja ettepanekud

Lõputöös uuriti, millised on Eesti finantsaudiitorite teadmised neile kohalduvatest isikuandmete kaitse kohustustest ning kui hästi on nad kursis uue isikuandmete kaitse üldmäärusega. Töö eesmärgiks oli välja selgitada, kui pädevad on Eesti finantsaudiitorid GDPR-i rakendamisel. Töö tulemused on välja toodud töö kolmandas peatükis ning nende põhjal on esitatud lõputöö järeldused ja ettepanekud.

Uuringust selgus, et kõrgematel ametikohtadel töötavad audiitorid hindavad oma teadmisi määruse kohta pigem heaks ning madalama taseme töötajad rahuldavaks. Keskmiselt puutuvad audiitorid isikuandmete töötlemisega kokku vastanute hinnangul iganädalaselt.

Küsimustikule vastanud erinevate audiitorbüroode töötajad hindavad, et nende tööandja on taganud turvalisuse suuremas osas või täielikult. Enim rakendatud turvameetmeteks on töötlemiseks vajalike juhendmaterjalide olemasolu, IT-süsteemide nõuetele vastavus ning andmekaitsespetsialisti olemasolu ettevõttes. Lisaks hindavad pooled tööandjad regulaarselt turvameetmete vastavust läbi GDPR-i auditite.

Kui audiitorid pidid hindama, mis on nende arvates isikuandmete definitsioon, jagunesid vastused võrdlemisi pooleks. Sõltumata ametikohast mõistab natuke alla poole (44%) audiitoritest, et isikuandmed on nii füüsiliste kui ka juriidiliste isikutega seotud andmed. Ülejäänud (56%) leiavad, et isikuandmed on ainult füüsiliste isikutega seonduv teave.
Poolikuid teadmisi kinnitas ka audiitorite poolt antud hinnang sellele, kes on töövõtu käigus GDPR-i mõistes andmesubjekt. Audiitorid märkisid andmesubjektideks nii juriidilisi kui ka füüsilisi isikuid. Viga esines ka nende seas, kes märkisid isikuandmete definitsiooni õigesti. Seega saab järeldada, et audiitorid hindavad kõiki auditikliendiga seotud isikuid andmesubjektideks.

Antud tulemused viitavad, miks ei suutnud audiitorid tuvastada neile esitatud isikuandmete loetelust kõiki andmeliike isikuandmetena. Keskmiselt tuvastasid audiitorid üheksa peamist andmeliiki kaheteistkümnest. Audiitorid ei hinnanud peamiselt isikuandmeteks võrguidentifikaatorit, ühingusse kuuluvuse ja ametialast teavet. Sellegipoolest mõistab 90% valimist, et auditites kõige enam tõendusmaterjalina kasutatavad finantsandmed on isikuandmed ning samuti isikute kontaktandmed ja isikukood.

Kogu valimist on pooled (53%) audiitorid teadlikud kõikidest andmesubjekti õigustest. Enamus audiitoreid on teadlikud, et andmesubjektil on õigus tutvuda töödeldavate andmetega ja vajadusel piirata või esitada vastuväiteid andmete korrektsusele. Esines ka neid (19%), peamiselt konsultantide seas, kes ei suutnud tuvastada üle poolte õigustest.
Üks peamine andmesubjektiga seotud kohustus on andmesubjekti teavitamine isikuandmete töötlemisest. Kõigest veerand (26%) kogu valimist palub auditikliendil informeerida andmesubjekte nende andmete töötlemisest. Hinnanguliselt on tegemist olulise GDPR-i rikkumisega, kuid arvestades, et vastajad töötavad suurtes audiitorbüroodes, on nende tööandjal kohustus koostada isikuandmete kaitse avaldus ning võimaldada kõikidel auditiklientidega seotud andmesubjektidel sellega tutvuda. Sellest tulenevalt ei tunne audiitorid kohustust andmesubjekte teavitada.

Kõrgemate ametikohtade töötajad on teadlikud, et nad on GDPR-i mõistes vastutavad töötlejad. Konsultandid ning praktikandid leidsid, et nemad ei otsusta kuidas ja milliseid kliendi andmeid töödeldakse.

Uuringust selgus, et enim peavad audiitorid töötlemiseks isikuandmete kogumist, dokumenteerimist või kasutamist. Natuke üle poole valimist (55%) on teadlik, et igasugune tegevus isikuandmetega klassifitseerub töötlemisena. Kõige vähem peetakse isikuandmete töötlemiseks lugemist ja päringute tegemist.
Mida madalamal tasemel organisatsiooni hierarhias paiknetakse, seda vähem rakendatakse ka GDPR-ist tulenevaid andmetöötluse põhimõtteid. Pea kõik *manager*'id ning pooled projektijuhid rakendavad kõiki põhimõtteid, kuid konsultandid ja praktikandid pigem osasid. Seda mõjutab ka tööjaotus ettevõtetes, sest osad põhimõtted on rohkem seotud tõendusmaterjalide kasutamisega pikemas perspektiivis ning arhiveerimine ja säilitamisaegade jälgimine on pigem kõrgema taseme töötajate kohustus.

Kui audiitoritelt uuriti, kas nad kasutavad GDPR-ist tulenevate kohustuste vähendamiseks pseudonümiseerimist või anonümiseerimist, oli vastus pigem eitav. Ainult osa kõrgema ametikoha töötajatest palub auditikliendil saata andmeid töödelduna, kuid isegi nemad ei pseudonümiseeriks ega anonümiseeriks kliendilt saadud andmeid ise.

Vajadust pseudonümiseerida või anonümiseerida võib mõjutada ka fakt, et enamusel audiitoritest pole veel siiani esinenud GDPR-i mõistes rikkumisi. Küsitlusele vastanutest oli vaid mõnel esinenud rikkumisi, mille käigus tekkis kolleegidel ligipääs kliendiandmetele või edastati kliendiandmed meili teel valele adressaadile. Rikkujate enda hinnangul polnud tegemist oluliste rikkumistega ning probleemid lahendati ettevõttesiseselt. Audiitorid küll teavad, kelle poole pöörduda rikkumise esinemisel, kuid nende arusaam rikkumise lahendamisest pole täielik ning sellest tulenevalt ei pruugi nad hinnata ohte piisava tõsidusega.

Kokkuvõtvalt leiab autor, et audiitorite teadmised GDPR-ist ja sellega kaasnevatest kohustustest võiksid olla paremad ning seda kõigil ametikohtadel. Üldiselt teadsid vastanud kõigil tasemetel üksikuid GDPR-i aspekte täielikult, mitmete aspektide puhul esines aga põhimõttelisi vigu.

Esiteks soovitab autor audiitorettevõtjatel pöörata lisaks ettevõtte GDPR-i vastavusele tähelepanu ka töötajate kompetentsile, sest uuringust selgus, et oma kohustuste teadmine ja metoodika

tundmine on enamasti puudulik. Audiitorid tunnetavad, et GDPR-i vastavuse tagamine on tööandja kohustus ning sellest tulenevalt ei erista töötleja kohustusi ettevõtte omadest. Küsitluses osalenute seas polnud ühtegi vastajat, kes oleks tõlgendanud isikuandmete kaitse üldmäärust täies ulatuses korrektselt või teadnud kõiki kohustusi. Tööandjad peaksid vaatama üle töötajatele koostatud juhendmaterjalid ning hindama, kas need on lihtsasti arusaadavad ning edastavad piisavalt vajalikku informatsiooni töötlemistoimingute korrektseks läbiviimiseks.

Teiseks soovitab autor audiitoritel paluda tööandjalt vastavate koolituste korraldamist. Tegemist on keerulise määrusega, mille mõju ei pruugita tunda enne, kui on toimunud rikkumine. Selleks, et tagada kliendi usaldus ning ettevõtte kvaliteedistandardid, peavad audiitorid mõistma, kelle suhtes, milliste andmete osas ja miks GDPR-i nõuded kehtivad. Koolituste läbiviimise kohustus võiks olla ka järelevalveasutusel või Audiitorkogul, et tagada audituri kompetents.

Samuti soovitab autor audiitoritel rõhutada ka klientidele isikuandmete kaitse olulisust. Auditite käigus tuleks hinnata auditikliendi vastavust määrusega ning auditikliendi ettevõttesiseste töötlejate pädevust. Pädevuse hindamiseks võib lasta kliendil auditi tõendusmaterjali pseudonümiseerida või anonümiseerida. Nii saavad audiitorid vähendada ka GDPR-i mittevastavusest tulenevaid riske.

KOKKUVÕTE

Uus keerukas Euroopa Liidu isikuandmete kaitse üldmäärus jõustus 25. mail 2018. aastal, muutes seda, kuidas igas tööstusharus tegutsevad ettevõtted käitlevad isikuandmeid. GDPR mõjutab ka Eestis tegutsevaid finantsaudiitoreid. Neil tuleb koguda ja käsitleda saadud andmeid vastavalt kehtivatele seadustele. Finantsaudiitorid vastutavad selle eest, et kliendiandmeid töödeldaks austades ja kaitstes kliendi konfidentsiaalset teavet.

Lõputöö eesmärgiks oli hinnata finantsaudiitorite teadlikkust isikuandmete kaitse üldmääruse ja sellega kaasnevate kohustuste kohta. Eesmärgi saavutamiseks viidi läbi kvantitatiivne uuring. Andmete kogumiseks kasutas autor veebipõhist küsitlusuuringut ning küsimustiku sihtgrupiks olid Eesti audiitorettevõtjate all tegutsevad finantsaudiitorid, kes puutuvad kokku isikuandmete töötlemisega. Vastuseid laekus kokku 81 audiitorilt, kes jagunesid nelja osakogumisse: praktikandid, konsultandid, projektijuhid ning *manager*'id.

Uuringust selgus, et vastanute hinnangul puutuvad audiitorid isikuandmete töötlemisega keskmiselt kokku iganädalaselt. Kõrgematel ametikohtadel töötavad audiitorid hindavad oma teadmisi määruse kohta pigem heaks ning madalama taseme töötajad rahuldavaks. Audiitorite hinnangul on nende tööandjad taganud GDPR-i kohustustest tulenevad turvalisuse nõuded suuremas osas või täielikult.

Uuringu käigus hindas autor audiitorite mõistmist GDPR-i põhilistest definitsioonidest, nagu isikuandmed, andmesubjekt ja töötlemine. Tulemustest ilmnes, et audiitorid leiavad, et nii füüsiline kui ka juriidiline isik on GDPR-i mõistes andmesubjekt. Suutmata korrektselt defineerida andmesubjekti ei osanud ka audiitorid tuvastada kõiki isikuandmeid etteantud loetelust. Suurem osa valimist on teadlik, et igasugune tegevus isikuandmetega klassifitseerub töötlemisena.

Samuti on audiitorid teadlikud peamistest andmesubjekti õigustest, nagu õigus tutvuda nende töödeldavate isikuandmetega ning vajadusel on neil õigus ka piirata või esitada vastuväiteid

andmete korrektusele. Kuigi audiitorite teadlikkus andmesubjekti õigustest on pädev, ei teavita enamus audiitoreid andmesubjekte nende andmete töötlemisest.

Mida madalama taseme ametikoha töötajaga on tegemist, seda vähem rakendatakse ka GDPR-ist tulenevaid andmetöötlemise põhimõtteid. Antud tulemust saab seostada audiitorite tõlgendusest, kas nad on GDPR-i mõistes vastutavad või volitatud töötlejad. Kõrgemate ametikohtade töötajad on teadlikud, et nad on vastutavad töötlejad, mistõttu pööravad nad ka rohkem tähelepanu andmete töötlemise protsessile. Konsultandid ning praktikandid leiavad pigem, et nemad ei otsusta, kuidas ja milliseid kliendi andmeid töödeldakse ja on GDPR-i mõistes volitatud töötlejad.

GDPR-ist tulenevate kohustuste vähendamiseks on audiitoritel võimalus andmeid kas pseudonümiseerida või anonümiseerida. Kui audiitoritelt uuriti, kas nad antud meetodeid rakendavad, oli vastus pigem eitav. Kui üldse, siis teevad seda kõrgemate ametikohtade töötajad. Kuigi audiitorite teadmised GDPR-ist tulenevatest kohustustest on puudulikud, ei olnud vastanutel esinenud olulisi rikkumisi. Kõik rikkumised olid lahendatud ettevõttesiseselt ilma järelevalveasutust kaasamata. Juhul, kui peaks esinema rikkumine, teavad audiitorid kelle poole pöörduda vastavalt GDPR-i nõuetele.

Analüüsi tulemuste põhjal järeldas autor, et audiitoritel puudub terviklik ülevaade kõikidest GDPR-ist tulenevatest kohustustest, mis mõjutavad nende igapäevatööd. Tegemist on keeruka ning alles vähe aega tagasi jõustunud määrusega, mille mõju ei osata veel korrektselt tõlgendada. Selleks, et vältida ebapädevusest tulenevaid rikkumisi, soovitab autor järgmisi lahendusi:

1) Audiitorettevõtjad peaksid pöörama tähelepanu lisaks ettevõtte GDPR-i vastavusele ka töötajate kompetentsile. Audiitorid eeldavad, et vastavuse tagamine on pigem tööandja kui nende kohustus. Sellest tulenevalt ei oska audiitorid eristada töötleja kohustusi ettevõtte omadest. Tööandjad peaksid ülevaatama nende poolt koostatud juhendmaterjalid ning hindama kas need on lugejale arusaadavad ning sisaldavad kõige olulisemaid GDPR-i aspekte.
2) GDPR-i korrektse rakendamise jaoks tuleb audiitorite seas viia läbi põhjalik koolitus, et tagada piisav pädevus. Juhul, kui antud koolitusi ei ole nõus korraldama tööandja, võiksid seda teha Audiitorkogu või järelevalveasutused, et tulevikus ennetada suuremaid andmekaitse rikkumisi.

3) Audiitorid võiksid isikuandmete kaitse olulisust rõhutada ka auditiklientidele. Juhul, kui auditikliendi töötleja oskab rakendada kohustuse vähendamiseks vastavaid meetmeid, vähendab see ka audiitorile GDPR-i mittevastavusest tulenevaid riske.

Autori hinnates saab antud lõputööd kasutada sisendiks ettepanekutes väljatoodud koolituste läbiviimiseks. Samuti saavad audiitorettevõtjad kasutada tööd töötajatele tehtud juhendite täiustamiseks. Töö analüüsi osas kaardistuvad välja peamised probleemsed kohad, mis võivad jääda audiitoritele arusaamatuks läbi vale tõlgendamise. Tõstes audiitorite teadlikkust, saavutavad ka audiitorettevõtjad kiiremini täieliku vastavuse ning tagatakse kvaliteetne audituturg.
Kuna tegemist on siiski alles vähe aega tagasi jõustunud reformiga, saab antud tööd tulevikus edasi arendada ka võrdlusanalüüsina. Edaspidi saab hinnata finantsaudiitorite GDPR-iga seonduva pädevuse dünaamikat ja jälgida, kas praeguseks selgunud murekohad on lahendatud või kas on tekkinud uusi.

SUMMARY

OBLIGATIONS OF A FINANCIAL AUDITOR UNDER THE GENERAL DATA PROTECTION REGULATION

Anette Sutt

The new complicated European Union General Data Protection Regulation (GDPR) came into force on May 25, 2018, changing how companies in every industry handle personal data. GDPR also has an impact on financial auditors in Estonia. Auditors must collect and process received client data in accordance with applicable laws. They are also responsible for ensuring that customer data is processed with respect and whilst doing so protect the customer's confidential information.

The purpose of this thesis was to assess the financial auditors' awareness of the GDPR and its related obligations. A quantitative survey was conducted to achieve this purpose. The author used a web-based survey to collect data and the target group of the questionnaire was financial auditors operating under Estonian audit firms who process personal data. Responses were received from a total of 81 auditors, divided into four subsets: interns, consultants, project managers and managers.

The survey found that on average auditors process personal data on a weekly basis. Auditors working in higher positions tend to rate their knowledge of the regulation as good and lower-level staff as satisfying. The auditors estimate that their employers have provided most or all of the security requirements according to their GDPR obligations.

During the survey, the author assessed the auditors' understanding of the basic definitions of the GDPR, such as personal data, data subject, and data processing. The results showed that auditors find that both a natural person and a legal entity are data subjects within the meaning of the GDPR. Without being able to define the data subject correctly, the auditors were also unable to identify all personal data from a given list. Most of the sample was aware that any activity involving personal data is classified as processing.

Auditors are also aware of the data subject's basic rights, such as the right of access to the personal data they process and, where appropriate, the right to limit or object to the correctness of the data. Although auditors are aware of the rights of the data subject, they rarely inform the data subjects when processing their data.

The lower the position in the organization hierarchy, the less the GDPR-based data processing principles are applied. This result can be attributed to the auditors' interpretation of whether they are controllers or processors within the meaning of the GDPR. Higher-level employees are aware that they are data controllers, so they also pay more attention to the process itself. Consultants and interns tend to find that they do not decide how and what customer data is processed and are authorized processors within the meaning of the GDPR.

To reduce obligations under the GDPR, auditors have the option of either pseudonymising or anonymising data. When auditors were asked whether they applied these methods, the answer was mostly negative. If at all, employees in higher positions do so. Although the auditors' knowledge of their obligations under the GDPR is incomplete, there had been no significant breaches among the respondents. All breaches were resolved internally without the involvement of the supervisory authority. In the event of a breach, the auditors knowwho to address in accordance with the GDPR.

Based on the results of the analysis, the author concluded that the auditors lack a comprehensive overview of all GDPR responsibilities that affects their daily work. It is a complex regulation that has been enforced for only a short period and the effects have not yet been properly interpreted. To avoid incompetence, the author recommends the following solutions:

1) Auditing firms should pay attention not only to the company's GDPR compliance but also to the competence of their employees. Auditors expect compliance to be the responsibility of the employer rather than theirs. As a result, auditors cannot distinguish the processor's responsibilities from those of the company. Employers should review their guidance material and assess whether it is comprehensible to the reader and contains the most important aspects of the GDPR.
2) Correct implementation of the GDPR requires in-depth training of auditors to prevent incompetence. In the event that the employers have no interest in organizing trainings, it could be done by the Estonian Auditors' Association or supervisory authorities in order to prevent future major data breaches.

3) Auditors could also emphasize the importance of personal data protection to audit clients. If the audit client's processor is able to implement appropriate mitigation measures, it will also reduce the auditor's risk of non-compliance with the GDPR.

Based on the evaluation of the author, this thesis can be used as an input for carrying out the training courses outlined in the solutions. Auditing firms can also use the thesis to improve guidance materials for staff. The analysis of the thesis maps out the main problem areas that may be misunderstood by auditors through misinterpretation. By raising awareness of auditors', auditing firms will also achieve full compliance more quickly and ensure a high quality audit market.

However, as this is a reform that has come into force recetly, this work can be further developed as a benchmarking exercise in the future. It is possible to compare how GDPR-related competencies have evolved over time among the auditors and whether previous concerns have been resolved or new ones have emerged.

KASUTATUD ALLIKATE LOETELU

Abuke, O.D. (2017). Quantitive Research Methods: A Synopsis Approach. *Kuwait Chapter of Arabian Journal of Business and Management Review*, 6 (11), 40–47.

Bussche, A., Voigt, P. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide.* Berliin: Springer International Publishing AG.

Deloitte Central Europe Service Specific Privacy Statement. Deloitte Touche Tohmatsu Ltd. Kättesaadav: https://www2.deloitte.com/ce/en/legal/deloitte-ce-privacy-statement-for-clients/deloitte-ce-entities-providing-services-as-data-controllers.html, 10.november 2019

EU General Data Protection Regulation (GDPR). An implementation and Compliance Guide. (2017). 2nd ed./Toim. IT Governance Privacy Team. Cambridgeshire: IT Governance Publishing.

Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, kehtetuks tunnistatud Euroopa Parlamendi ja nõukogu määrusega (EL) 2016/679, 27. aprill 2016

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

Feiler, L., Forgó, N., Weigl, M. (2018). *The EU General Data Protection (GDPR): A Commentary.* Surrey: Globe Law and Business Ltd.

GDPR: Implications for auditors: Position Paper. (2018). Accountancy Europe. Kättesaadav: https://www.accountancyeurope.eu/wp-content/uploads/181029_GDPR-and-its-implications-for-statutory-auditors_draft-publication.pdf, 1. november 2019

Individuals whose personal data we obtain in connection with providing services to our clients. PricewaterhouseCoopers LLP. Kättesaadav: https://www.pwc.co.uk/who-we-are/privacy-statement/individuals-whose-personal-data-we-obtain.html, 10. november 2019

Isikuandmete töötleja üldjuhend. (2019). Andmekaitse Inspektsioon Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf, 1. november 2019

Johnssén, F., Öqvist, K. L. (2018). *Hands-on guide to GDPR compliance: Privacy by Design, Privacy by Default.* Portsmouth: International Association of Privacy Professionals.

Keeping pace in the GDPR race: A global view of GDPR progress in the United States, Europe, China and Japan. (2019). Ponemont Institute. Kättesaadav: https://www.privacysecurityacademy.com/wp-content/uploads/2019/06/Keeping-Pace-in-the-GDPR-Race.pdf, 6. detsember 2019.

Lloyd, I. J. (2017). *Information Technology Law.* 8th ed. Oxford: Oxford University Press.

Männiko, M. (2011). *Õigus privaatsusele ja andmekaitse.* Tallinn: Kirjastus Juura.

Määrused, direktiivid ja muud õigusaktid. Euroopa Liit. Kättesaadav: https://europa.eu/european-union/eu-law/legal-acts_et, 17. oktoober 2019

Privacy Statement. (2019). Ernst & Young Global Ltd. Kättesaadav: https://www.ey.com/en_gl/privacy-statement, 10. november 2019

Rahvusvahelise auditeerimise standard (Eesti) 200 Sõltumatu audiitori üldised eesmärgid ja auditi läbiviimine kooskõlas rahvusvaheliste auditeerimise standarditega (Eesti).* Kättesaadav: https://audiitorkogu.ee/uploads/ISA-d%20alates%202016-12-15/ISA%20%28EE%29%20200.pdf, 10. november 2019

Rahvusvahelise auditeerimise standard (Eesti) 220 Finantsaruannete auditi kvaliteedikontroll.* Kättesaadav: https://www.audiitorkogu.ee/uploads/Standardid%20alates%2001.09.2018/ISA%20%28EE%29%20220.pdf, 10. november 2019

Rahvusvahelise auditeerimise standard (Eesti) 300 Finantsaruannete auditi planeerimine.* Kättesaadav: https://www.audiitorkogu.ee/uploads/ISA-d%20alates%202016-12-15/ISA%20%28EE%29%20300.pdf, 10. november 2019

Rahvusvaheline auditeerimise standard (Eesti) 500 Auditi tõendusmaterjal.* Kättesaadav: https://www.audiitorkogu.ee/uploads/Standardid%20alates%2001.09.2018/ISA%20%28EE%29%20500.pdf, 10. november 2019

Sauga, A. (2017). Statistika: *Statistika õpik majanduseriala üliõpilastele*. Tallinn: TTÜ Kirjastus

Schomakers, E.M., Lidynia, C., Müllmann, D., Ziefle, M. (2019). Internets users' perceptions of information of information sensitivity – insights from Germany. *International Journal of Information Management*, Vol. 46, Amsterdam: Elseiver Ltd., 142–150.

Tikk, E., Nõmper, A. (2007). *Informatisoon ja õigus*. Tallinn: Kirjastus Juura.

Uue isikuandmete kaitse seaduse lugemisel tuleb olla tähelepanelik. (2019). Andmekaitse Inspektsioon. Kättesaadav: https://www.aki.ee/et/uudised/pressiteated/uue-isikuandmete-kaitse-seaduse-lugemisel-tuleb-olla-tahelepanelik, 18. oktoober 2019

Williams, C. (2007). Research Methods. *Journal of Business & Economics Research (JBER)*, 5(3), 65–71.

Õunapuu, L. (2014). *Kvalitatiivne ja kvanitatiivne uurimisviis sotsiaalteadustes.* Tartu: Tartu Ülikool

LISAD

Lisa 1. Küsimustik

GDPR-ist tulenevad kohustused finantsaudiitorile

Lugupeetud vastaja!

Olen Anette Sutt ning õpin Tallinna Tehnikaülikooli majandusarvestuse eriala neljandal kursusel. Selleks, et kool saaks lõpetatud olen kirjutamas oma lõputööd, mis uurib finantsaudiitorite kohustusi uue isikuandme kaitse üldmääruse suhtes.

Lõputöö tegemiseks paluksin Teie abi ning olen väga tänulik, kui leiaksite aega vastata käesolevale küsimustikule. Küsimustele vastamine võtab aega mõne minuti. Vastused jäävad anonüümseks ning neid kasutatakse üksnes lõputöö empiirliseks analüüsiks, kokkuvõtete tegemiseks ning järelduste esitamiseks.

Tänan teid Teie aja eest ning head vastamist!

Kui tekib küsimusi või soovite võtta minuga ühendust: anettesutt@gmail.com

Lugupidamisega
Anette Sutt

1. Kas oma töö iseloomu tõttu töötlete isikuandmeid?

- ○ Jah
- ○ Ei

2. Millisel ametikohal Te hetkel töötate?

Konsultant on üldiselt 1-2 aastase töökogemusega audiitor
Projektijuht on üldiselt 3-4 aastase töökogemusega audiitor
Manager on üldiselt 5 või enama aastase töökogemusega audiitor

- ○ Praktikant
- ○ Konsultant
- ○ Projektijuht
- ○ *Manager*

3. Kui tihti Te töötlete isikuandmeid?

Palun hinnake skaalal 1-10, kus:
1 - Väga harva, 4 – Kvartaalselt, 6 – Igakuiselt, 8 - Iga nädalaselt, 10 – Igapäevaselt

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ 6
- ○ 7
- ○ 8
- ○ 9
- ○ 10

4. Kuidas hindate enda teadmisi isikuandmete kaitse kohta?

Palun hinnake skaalal 1-10, kus: 1 - Teadmised puuduvad, 4 - Teadmised on alla keskmise, 6 - Teadmised on rahuldavad, 8 - Teadmised on head, 10 - Teadmised on täielikud

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ 6
- ○ 7
- ○ 8
- ○ 9
- ○ 10

5. Kas Te otsustate kuidas ja milliseid kliendi andmeid töödeldakse?

- ○ Jah
- ○ Ei

6. Milline definitsioon selgitab Teie arvates kõige paremini isikuandmete olemust?

- ○ Isikuandmed on igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta
- ○ Isikuandmed on igasugune teave tuvastatud või tuvastatava füüsilise või juriidilise isiku kohta
- ○ Isikuandmed on igasugune teave elava füüsilise või juriidilise isiku kohta
- ○ Isikuandmed on igasugune teave tuvastatud või tuvastatava elava füüsilise isiku kohta

Muu (täpsusta)

---

7. Lähtudes isikuandmete definitsioonist, millised valikust klassifitseeruvad Teie hinnangul isikuandmeteks:

Palun valige üks või mitu vastust.

- ☐ Nimi
- ☐ Isikukood
- ☐ Sugu
- ☐ Asukohateave
- ☐ Teave perekonnaliikmete kohta
- ☐ Võrguidentifikaator
- ☐ Kontaktandmed
- ☐ Finantsandmed
- ☐ Teave terviseseisundi kohta
- ☐ Ametialane teave
- ☐ Hariduslik teave
- ☐ Ühingusse kuuluvuse teave

8. Mis on Teie arvates andmete töötlemine?

Palun valige loetelust üks või mitu vastust.

- ☐ Kogumine, dokumenteerimine
- ☐ Korrastamine, struktureerimine
- ☐ Säilitamine
- ☐ Kohandamine ja muutmine
- ☐ Päringute tegemine
- ☐ Lugemine
- ☐ Kasutamine
- ☐ Edastamine, levitamine, avalikustamine

- [ ] Kustutamine, hävitamine

Muu (täpsusta)

---

9. Kes on Teie hinnangul andmesubjekt finantsauditis?

Andmesubjekt on isik, kelle andmeid töödeldakse kolmanda isiku poolt. Loetelus on nimetatud auditikliendiga seotud füüsilised ja juriidilised isikud. Palun valige loetelust üks või mitu vastust.

- [ ] Ettevõte
- [ ] Ettevõtte töötajad
- [ ] Juhatus või need, kelle ülesandeks on valitsemine
- [ ] Juhatuse või nende, kelle ülesandeks on valitsemine pereliikmed ja ülalpeetavad
- [ ] Eraklient/koostööpartner
- [ ] Äriklient/koostööpartner

Muu (täpsusta)

---

10. Kuidas hindate Teie tööandja poolt tagatud turvalisuse meetmeid isikuandmete kaitse suhtes?

Palun hinnake skaalal 1-10, kus: 1 - Turvalisus puudub, 4 - Turvalisus on osaliselt tagatud, 6 - Turvalisus on pigem tagatud, 8 - Turvalisus on tagatud, kuid esinevad väikesed puudulikkused, 10 – Turvalisus on täielikult tagatud

- ( ) 1
- ( ) 2
- ( ) 3
- ( ) 4
- ( ) 5
- ( ) 6
- ( ) 7
- ( ) 8
- ( ) 9
- ( ) 10

11. Kuidas on Teie tööandja taganud ettevõtte vastavuse GDPR-iga?

Palun valige üks või mitu vastust.

- [ ] Organiseerinud andmekaitse teemadel koolitusi
- [ ] Juhendid, sisekorrad ja eeskirjad, mis reguleerivad isikuandmete töötlemise põhimõtteid

- [ ] Määranud andmekaitsespetsialisti
- [ ] IT süsteemid on viidud vastavusse turvalisuse nõuetega
- [ ] Hindab regulaarselt turvameetmete vastavust ning rakendamist

Muu (täpsusta)

---

12. Millised on Teie hinnangul andmesubjekti õigused?

Palun valige loetelust üks või mitu vastust.

- [ ] Õigus tutvuda andmetega
- [ ] Õigus andmete parandamisele
- [ ] Õigus nõuda andmete kustutamist
- [ ] Õigus piirata isikuandmete töötlemist
- [ ] Õigus lasta andmeid ülekanda
- [ ] Õigus esitada vastuväiteid andmete töötlemise suhtes

Muu (täpsusta)

---

13. Milliseid andmekaitse põhimõtteid järgite andmete töötlemisel?

Palun valige üks või mitu vastust.

- [ ] Töötlejana vastutate töötlemise eest
- [ ] Andmete töötlemine on seaduslik ja õiglane
- [ ] Kogute ainult andmeid, mis on vajalikud
- [ ] Andmed on aja- ja asjakohased
- [ ] Järgite andmete säilitamise tähtaegu
- [ ] Töötlete andmeid turvaliselt

14. Kui tihti palute kliendil andmeid pseudonümiseerida/anonümiseerida?

Anonümiseerimine on andmete modifitseerimine viisil, kus kaob igasugune andmete seos andmesubjektiga. Pseudonümiseerimine on andmete modifitseerimine viisil, kus isikuandmeid ei saa ilma täiendava teabeta seostada konkreetse andmesubjektiga (nt kodeerimine).
Palun hinnake skaalal 1-10, kus: 1 - Mitte kunagi 4 - Harva 6 - Sageli 8 - Enamasti 10 - Alati

- ( ) 1
- ( ) 2
- ( ) 3
- ( ) 4
- ( ) 5

- ○ 6
- ○ 7
- ○ 8
- ○ 9
- ○ 10

15. Kui tihti pseudonümiseerite/anonümiseerite kliendilt saadud andmeid ise?

Anonümiseerimine on andmete modifitseerimine viisil, kus kaob igasugune andmete seos andmesubjektiga. Pseudonümiseerimine on andmete modifitseerimine viisil, kus isikuandmeid ei saa ilma täiendava teabeta seostada konkreetse andmesubjektiga (nt kodeerimine).
Palun hinnake skaalal 1-10, kus: 1 - Mitte kunagi 4 - Harva 6 - Sageli 8 - Enamasti 10 - Alati

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ 6
- ○ 7
- ○ 8
- ○ 9
- ○ 10

16. Kui tihti palute kliendil informeerida andmesubjekte nende isikuandmete töötlemisest?

Palun hinnake skaalal 1-10, kus: 1 - Mitte kunagi 4 - Harva 6 - Sageli 8 - Enamasti 10 - Alati

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ 6
- ○ 7
- ○ 8
- ○ 9
- ○ 10

17. Juhul, kui esineks isikuandmete töötlemise rikkumine, siis keda Te informeeriksite?

Järjestage palun vastusevariandid Teie hinnangul olulisuse järjekorras.

- [ ] Auditikliendi kontaktisikut
- [ ] Andmesubjekti
- [ ] Järelvalveasutust (Andmekaitse Inspektsioon)
- [ ] Andmekaitsespetsialisti
- [ ] Tööandjat

18. Kas teil on esinenud isikuandmete töötlemisel rikkumisi?

- ○ Jah
- ○ Ei

19. Kui vastasite eelmisele küsimusele „Jah“ siis palun kirjeldage, mis oli rikkumise põhjus ning milliseid meetmeid rikkumise lahendamise jaoks kasutasite

_____

Lisa 2. Küsimuste 1–4 vastused

Tabel 4. Küsimus 1: „Kas oma töö iseloomu tõttu töötlete isikuandmeid?“

Vastus	Vastajate arv	Osakaal valimist
Jah	81	87%
Ei	12	13%
Kokku	**93**	**100%**

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Tabel 5. Küsimus 2: „Millisel ametikohal Te hetkel töötate?”

Ametikoht	Vastajate arv	Osakaal valimist
Praktikant	10	12%
Konsultant	37	46%
Projektijuht	22	27%
Manager	12	15%
Kokku	**81**	**100%**

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Tabel 6. Küsimus 3: „Kui tihti Te töötlete isikuandmeid?“

	Vastajate arv					Osakaal valimist				
	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**
1 - Väga harva	-	-	-	-	-	-	-	-	-	-
2 - Pigem harva	-	-	-	-	-	-	-	-	-	-
3 - Paar korda aastas	-	-	-	-	-	-	-	-	-	-
4 - Kvartaalselt	1	6	-	-	**7**	10%	16%	-	-	**9%**
5 - Peaaegu igakuiselt	2	1	-	-	**3**	20%	3%	-	-	**4%**
6 - Igakuiselt	4	8	-	-	**12**	40%	22%	-	-	**15%**
7 - Mitu korda kuus	2	7	3	-	**12**	20%	19%	14%	-	**15%**
8 - Iga nädalaselt	-	8	15	3	**26**	-	22%	68%	25%	**32%**
9 - Mitu korda nädalas	-	2	3	2	**7**	-	5%	14%	17%	**9%**
10 - Igapäevaselt	1	5	1	7	**14**	10%	14%	5%	58%	**17%**
Kokku	**10**	**37**	**22**	**12**	**81**	**100%**	**100%**	**100%**	**100%**	**100%**
Mood	6	6	8	10	8	-	-	-	-	-
Kaalutud aritmeetiline keskmine	6	7	8	9	8	-	-	-	-	-

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Tabel 7. Küsimus 4: „Kuidas hindate enda teadmisi isikuandmete kaitse kohta?“

Teadmised on: …	Vastajate arv					Osakaal valimist				
	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**
1 - puuduvad	-	-	-	-	-	-	-	-	-	-
2 - väga puudulikud	-	-	-	-	-	-	-	-	-	-
3 - pigem puudulikud	2	1	-	-	**3**	20%	3%	-	-	**4%**
4 - alla keskmise	1	1	-	2	**4**	10%	3%	-	17%	**5%**
5 - keskmised	-	8	1	-	**9**	-	22%	5%	-	**11%**
6 - rahuldavad	4	16	3	3	**26**	40%	43%	14%	25%	**32%**
7 - pigem head	2	8	10	4	**24**	20%	22%	45%	33%	**30%**
8 - head	1	1	4	1	**7**	10%	3%	18%	8%	**9%**
9 - väga head	-	2	4	2	**8**	-	5%	18%	17%	**10%**
10 - täielikud	-	-	-	-	-	-	-	-	-	-
Kokku	**10**	**37**	**22**	**12**	**81**	**100%**	**100%**	**100%**	**100%**	**100%**
Kaalutud aritmeetiline keskmine	6	6	7	7	6	-	-	-	-	-

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Lisa 3. Küsimuste 5–9 vastused

Tabel 8. Küsimus 5: „Kas Te otsustate kuidas ja milliseid kliendiandmeid töödeldakse?“

	Vastajate arv					Osakaal valimist				
	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**
Jah	2	16	19	8	**45**	20%	43%	86%	67%	**56%**
Ei	8	21	3	4	**36**	80%	57%	14%	33%	**44%**
Kokku	**10**	**37**	**22**	**12**	**81**	**100%**	**100%**	**100%**	**100%**	**100%**

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Tabel 9. Küsimus 6: „Milline definitsioon selgitab Teie arvates kõige paremini isikuandmete olemust?“

Vastus	Vastajate arv	Osakaal valimist
Isikuandmed on igasugune teave tuvastatud või tuvastatava elava füüsilise isiku kohta	37	46%
Isikuandmed on igasugune teave tuvastatud või tuvastatava füüsilise või juriidilise isiku kohta	31	38%
Isikuandmed on igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta	8	10%
Isikuandmed on igasugune teave elava füüsilise või juriidilise isiku kohta	5	6%
Muu (täpsusta)	-	0%
Kokku	**81**	**100%**

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Tabel 10. Küsimus 7: „Lähtudes isikuandme definitsioonist, millised valikust klassifitseeruvad Teie hinnangul isikuandmeteks?“

Vastus	Vastajate arv	Osakaal valimist
Isikukood	79	98%
Finantsandmed	78	96%
Teave terviseseisundi kohta	74	91%
Teave perekonnaliikmete kohta	72	89%
Kontaktandmed	72	89%
Nimi	68	84%
Asukohateave	66	81%
Hariduslik teave	55	68%
Sugu	54	67%
Ühingusse kuuluvuse teave	48	59%

Vastus	Vastajate arv	Osakaal valimist
Ametialane teave	47	58%
Võrguidentifikaator	39	48%

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Tabel 11. Küsimus 8: „Mis on teie arvates andmete töötlemine?“

Vastus	Vastajate arv	Osakaal valimist
Kogumine, dokumenteerimine	79	98%
Kasutamine	74	91%
Edastamine, levitamine, avalikustamine	69	85%
Korrastamine, struktureerimine	65	80%
Kohandamine ja muutmine	65	80%
Säilitamine	64	79%
Kustutamine, hävitamine	56	69%
Päringute tegemine	49	60%
Lugemine	45	56%
Muu	-	0%

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Tabel 12. Küsimus 9: „Kes on Teie hinnangul andmesubjekt finantsauditis?“

Vastus	Vastajate arv	Osakaal valimist
Ettevõtte töötajad	72	89%
Juhatus või need, kelle ülesandeks on valitsemine	67	83%
Eraklient/koostööpartner	66	81%
Ettevõte	54	67%
Äriklient/koostööpartner	53	65%
Juhatuse või nende, kelle ülesandeks on valitsemine pereliikmed ja ülalpeetavad	52	64%
Muu	-	0%

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Lisa 4. Küsimuste 10 ja 11 vastused

Tabel 13. Küsimus 10: „Kuidas hindate Teie tööandja poolt tagatud turvalisuse meetmeid isikuandmete kaitse suhtes?“

	Vastajate arv					Osakaal valimist				
	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**
1 - Turvalisus puudub	-	-	-	-	-	-	-	-	-	-
2 - Turvalisus on väga puudulik	-	-	-	-	-	-	-	-	-	-
3 - Turvalisus on pigem puudulik	-	-	-	-	-	-	-	-	-	-
4 - Turvalisus on osaliselt tagatud	-	-	-	-	-	-	-	-	-	-
5 - Turvalisus on pooleldi tagatud	-	-	-	-	-	-	-	-	-	-
6 - Turvalisus on pigem tagatud	-	-	-	1	**1**	-	-	-	8%	**1%**
7 - Turvalisus on suuremas osas tagatud	2	4	2	1	**9**	20%	11%	9%	8%	**11%**
8 - Turvalisus on tagatud, kuid esinevad väikesed puudused	4	14	4	4	**26**	40%	38%	18%	33%	**32%**
9 - Turvalisus on väga hea	4	13	10	3	**30**	40%	35%	45%	25%	**37%**
10 - Turvalisus on tagatud täielikult	-	6	6	3	**15**	-	16%	27%	25%	**19%**
Kokku	**10**	**37**	**22**	**12**	**81**	**100 %**	**100 %**	**100 %**	**100 %**	**100 %**
Kaalutud aritmeetiline keskmine	8	9	9	9	**9**	-	-	-	-	-
Mood	9	8	9	8	**9**	-	-	-	-	-

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Tabel 14. Küsimus 11: „Kuidas on Teie tööandja taganud ettevõtte vastavuse GDPR-iga?“

Vastus	Vastajate arv	Osakaal valimist
Juhendid, sisekorrad ja eeskirjad, mis reguleerivad isikuandmete töötlemise põhimõtteid	77	95%
Määranud andmekaitsespetsialisti	69	85%
Organiseerinud andmekaitse teemadel koolitusi	68	84%
IT süsteemid on viidud vastavusse turvalisuse nõuetega	66	81%
Hindab regulaarselt turvameetmete vastavust ning rakendamist	43	53%
Muu	-	0%

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Lisa 5. Küsimuste 12–18 vastused

Tabel 15. Küsimus 12: „Millised on Teie hinnangul andmesubjekti õigused?“

Vastus	Vastajate arv	Osakaal valimist
Õigus tutvuda andmetega	75	93%
Õigus andmete parandamisele	68	84%
Õigus nõuda andmete kustutamist	65	80%
Õigus piirata isikuandmete töötlemist	71	88%
Õigus lasta andmeid üle kanda	52	64%
Õigus esitada vastuväiteid andmete töötlemise suhtes	70	86%
Muu (täpsusta)	-	0%

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Tabel 16. Küsimused 13: „Milliseid andmekaitse põhimõtteid järgite andmete töötlemisel?“

	Vastajate arv					Osakaal ametikohast			
	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**	Praktikant	Konsultant	Projektijuht	*Manager*
Töötlejana vastutate töötlemise eest	6	33	19	12	**70**	60%	89%	86%	100%
Andmete töötlemine on seaduslik ja õiglane	3	31	18	12	**64**	30%	84%	82%	100%
Kogute ainult andmeid, mis on vajalikud	10	34	20	11	**75**	100%	92%	91%	92%
Andmed on aja- ja asjakohased	8	37	18	11	**74**	80%	100%	82%	92%
Järgite andmete säilitamise tähtaegu	5	24	15	12	**56**	50%	65%	68%	100%
Töötlete andmeid turvaliselt	8	34	20	12	**74**	80%	92%	91%	100%

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Tabel 17. Küsimus 14: „Kui tihti palute kliendil andmeid pseudonümiseerida/anonümiseerida?“

	Vastajate arv					Osakaal valimist				
	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**
1 - Mitte kunagi	5	9	3	-	**17**	50%	24%	14%	-	**21%**
2 - Üksikutel kordadel	-	2	3	1	**6**	-	5%	14%	8%	**7%**
3 - Pigem harva	1	8	1	-	**10**	10%	22%	5%	-	**12%**
4 - Harva	-	6	-	3	**9**	-	16%	-	25%	**11%**
5 - Pigem sageli	3	4	4	-	**11**	30%	11%	18%	-	**14%**
6 - Sageli	-	3	3	5	**11**	-	8%	14%	42%	**14%**
7 - Pigem enamasti	-	4	5	-	**9**	-	11%	23%	-	**11%**
8 - Enamasti	1	1	1	3	**6**	10%	3%	5%	25%	**7%**
9 - Peaaegu alati	-	-	2	-	**2**	-	-	9%	-	**2%**
10 - Alati	-	-	-	-	**-**	-	-	-	-	**-**
Kokku	**10**	**37**	**22**	**12**	**81**	100%	100%	100%	100%	**100%**

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Tabel 18. Küsimus 15: „Kui tihti pseudonümiseerite/anonümiseerite kliendilt saadud andmeid ise“?

	Vastajate arv					Osakaal valimist				
	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**
1 - Mitte kunagi	4	15	6	-	**25**	40%	41%	27%	-	**31%**
2 - Üksikutel kordadel	-	5	-	1	**6**	-	14%	-	8%	**7%**
3 - Pigem harva	1	2	5	5	**13**	10%	5%	23%	42%	**16%**
4 - Harva	2	1	-	2	**5**	20%	3%	-	17%	**6%**
5 - Pigem sageli	2	8	3	1	**14**	20%	22%	14%	8%	**17%**
6 - Sageli	-	2	2	-	**4**	-	5%	9%	-	**5%**
7 - Pigem enamasti	-	2	3	-	**5**	-	5%	14%	-	**6%**
8 - Enamasti	1	2	3	3	**9**	10%	5%	14%	25%	**11%**
9 - Peaaegu alati	-	-	-	-	**-**	-	-	-	-	**-**
10 - Alati	-	-	-	-	**-**	-	-	-	-	**-**
Kokku	**10**	**37**	**22**	**12**	**81**	100%	100%	100%	100%	**100%**

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Tabel 19. Küsimus 16: „Kui tihti palute kliendil informeerida andmesubjekte nende isikuandmete töötlemisest?“

	Vastajate arv					Osakaal valimist				
	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**	Praktikant	Konsultant	Projektijuht	*Manager*	**Kokku**
1 - Mitte kunagi	6	14	5	3	**28**	60%	38%	23%	25%	**35%**
2 - Üksikutel kordadel	2	9	5	1	**17**	20%	24%	23%	8%	**21%**
3 - Pigem harva	-	5	1	5	**11**	-	14%	5%	42%	**14%**
4 - Harva	-	2	-	2	**4**	-	5%	-	17%	**5%**
5 - Pigem sageli	-	-	-	-	**-**	-	-	-	-	**-**
6 - Sageli	-	1	9	-	**10**	-	3%	41%	-	**12%**
7 - Pigem enamasti	-	-	-	-	**-**	-	-	-	-	**-**
8 - Enamasti	1	1	1	1	**4**	10%	3%	5%	8%	**5%**
9 - Peaaegu alati	-	-	-	-	**-**	-	-	-	-	**-**
10 - Alati	1	5	1	-	**7**	10%	14%	5%	-	**9%**
Kokku	**10**	**37**	**22**	**12**	**81**	100%	100%	100%	100%	**100%**

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Tabel 20. Küsimus 17: „Juhul, kui esineks isikuandmete töötlemise rikkumine, siis keda Te informeeriksite?“

	Järjestus					
	1	2	3	4	5	**Kokku**
Auditikliendi kontaktisikut	5	23	29	16	8	**81**
Osakaal	6%	28%	**36%**	20%	10%	**100%**
Andmesubjekti	8	7	11	29	26	**81**
Osakaal	10%	9%	14%	**36%**	32%	**100%**
Järelevalveasutust	29	5	7	10	30	**81**
Osakaal	36%	6%	9%	12%	**37%**	**100%**
Andmekaitsespetsialisti	4	24	27	21	5	**81**
Osakaal	5%	**30%**	33%	26%	6%	**100%**
Tööandjat	35	22	7	5	12	**81**
Osakaal	**43%**	27%	9%	6%	15%	**100%**

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Tabel 21. Küsimus 18: „Kas teil on esinenud isikuandmete töötlemisel rikkumisi?“

	Vastajate arv					Osakaal valimist				
	Praktikant	Konsultant	Projektijuht	*Manager*	Kokku	Praktikant	Konsultant	Projektijuht	*Manager*	Kokku
Jah	**-**	2	2	**-**	**4**	**-**	5%	9%	**-**	**5%**
Ei	10	35	20	12	**77**	100%	95%	91%	100%	**95%**
Kokku	**10**	**37**	**22**	**12**	**81**	**100%**	**100%**	**100%**	**100%**	**100%**

Allikas: autori arvutused Lisa 1 küsimustiku tulemuste põhjal

Lisa 6. Lihtlitsents

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Anette Sutt (sünnikuupäev: 23.09.1996),

1. annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Finantsaudiitori kohustused tulenevalt isikuandmete kaitse üldmäärusest“, mille juhendaja on lektor Ester Vahtre,

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.