

TALLINNA TEHNIKAÜLIKOOL

Majandusteaduskond

Ärikorralduse instituut

Anna Bogdanskaja

**ISIKUANDMETE KAITSE ÜLDMÄÄRUSE NÕUDED
RAAMATUPIDAMISES**

Lõputöö

Õppekava MAJANDUSARVESTUS JA ETTEVÕTLUSE JUHTIMINE,
Peeriala majandusarvestus

Juhendaja: Margit Pado, MA

Tallinn 2019

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 8559 sõna sissejuhatusest kuni kokkuvõtte lõpuni.

Anna Bogdanskaja

(allkiri, kuupäev)

Üliõpilase kood: 166059BDMR

Üliõpilase e-posti aadress: annabogdanskaja@gmail.com

Juhendaja: Margit Pado, MA:

Töö vastab kehtivatele nõuetele

.....

(allkiri, kuupäev)

Kaitsmiskomisjoni esimees:

Lubatud kaitsmisele

.....

(nimi, allkiri, kuupäev)

SISUKORD

LÜHIKOKKUVÕTE	3
SISSEJUHATUS	4
1. UUE ISIKUANDMETE KAITSE ÜLDMÄÄRUSE NÕUDED	6
1.1. Privaatsus ja isikuandmed	7
1.2. Isikuandmete kaitse üldmääruse olemus ja definitsioon	9
1.3. Kaasnevad ja olulised muudatused üldmääruses.....	11
2. ÜLDMÄÄRUSE RAKENDAMINE RAAMATUPIDAMISES	17
2.1. Üldmääruse kasutamine raamatupidamises igapäevatöös.....	17
2.2. Üldmääruse rikkumise tagajärjed	21
2.3. Olulised turvameetmed raamatupidajate ja kogu ettevõtte jaoks	22
3. EESTI ETTEVÕTETE RAAMATUPIDAJATE TEADMISTE HINNANG JA ANALÜÜS	26
3.1. Uuringu metoodika ja valimi kriteeriumid	26
3.2. Interneti uuringu tulemused.....	27
3.3. Intervjuu uuringu tulemused.....	34
3.4. Arutelu, järeldused ja ettepanekud	37
KOKKUVÕTE	39
SUMMARY	41
VIIDETUD ALLIKATE LOETELU	43
LISAD	46
Lisa 1. Intervjuu küsimuste transkriptsioon: vastaja 1 (väikeettevõte)	46
Lisa 2. Intervjuu küsimuste transkriptsioon: vastaja 2 (väikeettevõte)	48
Lisa 3. Intervjuu küsimuste transkriptsioon: vastaja 3 (keskettevõte).....	51
Lisa 4. Intervjuu küsimuste transkriptsioon: vastaja 4 (keskettevõte).....	53
Lisa 5. Intervjuu küsimuste transkriptsioon: vastaja 5 (suurettevõte).....	56
Lisa 6. Intervjuu küsimuste transkriptsioon: vastaja 6 (suurettevõte).....	59
Lisa 7. Google Forms küsimustik.....	62
Lisa 8. Raamatupidajate teadmiste tase tabel	65

LÜHIKOKKUVÕTE

25. mail 2018. aastal jõustus Euroopa Parlamendi ja nõukogu isikuandmete kaitse üldmäärus (GDPR – General Data Protection Regulation), mille eesmärk on tagada suurem kaitse isikuandmete töötlemisel ja anda füüsilisele isikule rohkem kontrolli oma andmete üle (Isikuandmete kaitse seaduse eelnõu seletuskiri). Selle seaduse jõustumine tõi kaasa mitmeid muudatusi raamatupidajate töökorralduses. Lõputöö eesmärk on välja selgitada Euroopa Parlamendi ja nõukogu isikuandmete kaitse üldmääruse muutuste mõju ja uurida, mil määral on Eesti ettevõtete raamatupidajad kursis kõikide isikuandmete kaitse nõuetega. Käesoleva lõputöö uurimisprobleemiks on raamatupidajate teadmised isikuandmete kaitse üldmääruse mõjust ja võimekus kohaldada üldmäärust igapäevatoös.

Töö koostamisel lähtuti küsitluste ja intervjuude vastustest, vastajaid intervjuueriti oktoobrist kuni novembrini 2018. aastal. Uurimisküsimusi oli kokku viis:

- Milline on olnud üldmääruse muudatuste mõju?
- Kas üldmääruse muudatused saaksid lihtustada ettevõtte tööd?
- Kas raamatupidajad saavad täita kõiki isikuandmetega seotud nõudeid?
- Mida peab raamatupidamises arvesse võtma isikuandmete töötlemisel?
- Milliseid reegleid on isikuandmete kaitsega seoses vaja organisatsioonis kehtestada ja järgida?
- Mis juhtub, kui raamatupidamises rikutakse isikuandmete kaitset?

Lõputöö tulemusena anti hinnang, milline on raamatupidajate võimekus kohandada üldmäärusega kaasnevat muudatusi igapäevatoöga ning muudatuste mõju raamatupidajate tööle.

Võtmesõnad: isikuandmete kaitse üldmäärus, privaatsus, andmekaitse, rikkumise tagajärjed, kasutamine ja rakendamine igapäevatoös.

SISSEJUHATUS

Privaatsus ja üksikisiku andmete kaitse on inimeste jaoks väga olulised mõisted. Privaatsust seostatakse eraelu kaitsmisega ja õigusega puutumatusel. Tänapäeval omavad kõik ettevõtted informatsiooni füüsiliste isikute kohta – oma klientide ja töötajate andmeid. Väga oluline on tagada selle informatsiooni töötlemine, säilimine ja ringlus vastavalt kehtivale isikuandmete kaitse üldmäärusele (Isikuandmete kaitse seaduse eelnõu seletuskiri).

25. mail 2018. aastal jõustus Euroopa Parlamendi ja nõukogu isikuandmete kaitse üldmäärus (GDPR – General Data Protection Regulation). Isikuandmete kaitse üldmääruse eesmärk on tagada parem kaitse isikuandmete töötlemisel ja anda füüsilise isikule rohkem kontrolli oma andmete üle (Isikuandmete kaitse seaduse eelnõu seletuskiri). Kuna määrus puudutas kõiki ettevõtteid, kes tegutsevad Euroopa Liidus ja kes osutavad teenuseid Euroopa Liidu kodanikele, toimusid määruse jõustumisega mitmed muudatused nendes ametites, mis puutuvad kaudselt või otseselt kokku isikuandmete ning nende töötlemisega.

Lõputöö eesmärk on välja selgitada Euroopa Parlamendi ja nõukogu isikuandmete kaitse üldmääruse muutuste mõju ja anda hinnang, millisel määral on Eesti ettevõtete raamatupidajad kursis kõikide isikuandmete kaitse nõuetega. Uurimisprobleemiks on raamatupidajate teadmised üldmääruse mõjust ja võimekus kohaldada üldmäärust igapäevatoös. Lõputöö uurimisküsimused on:

- Milline on olnud üldmääruse muudatuste mõju?
- Kas üldmääruse muudatused saaksid lihtustada ettevõtte tööd?
- Kas raamatupidajad saavad täita kõiki isikuandmetega seotud nõudeid?
- Mida peab raamatupidamises arvesse võtma isikuandmete töötlemisel?
- Milliseid reegleid on isikuandmete kaitsega seoses vaja organisatsioonis kehtestada ja järgida?
- Mis juhtub, kui raamatupidamises rikutakse isikuandmete kaitset?

Lõputöö on jaotatud kolmeks peatükiks. Esimene peatükk annab ülevaate isikuandmete kaitse üldmäärusest: selle olemusest, definitsioonist ja olulisematest muudatustest töökorralduses seoses

määruse jõustumisega. Teises peatükis keskendutakse isikuandmete kaitse üldmääruse kasutamisele raamatupidamises ja üldmääruse rikkumise tagajärgedele; seehulgas annab peatükk ülevaate erinevatest meetoditest, mida ettevõtted ja raamatupidajad peaksid kasutama igapäevastöös, et tagada isikuandmete kaitse ettevõttes. Kolmas peatükk keskendub lõputöös kasutatatud metoodikale, annab vastused uurimisküsimustele ning sisaldab autori järeldusi ja ettepanekuid.

Lõputöö eesmärk hõlmab küsitlust ja intervjuude läbiviimist, et selgitada välja, millisel määral Eesti ettevõtete raamatupidajad on kursis isikuandmete kaitse üldmääruse nõuetega. Samuti töös küsitluse ja intervjuu vastuste töötlemine ning grupeerimine, selgitamaks välja, mis määral on Eesti ettevõtete raamatupidajad kursis isikuandmete kaitse kõigi nõuetega. Esimese sammuna viidi läbi internetiküsitlus, mille eesmärk oli saada üldised statistilised andmed raamatupidajate teadmistest. Teise sammuna valiti kuus raamatupidajat erineva suurustega ettevõttest ja viidi läbi intervjuud. Intervjuude abil sai autor teada valdkonna nõrkused ja uurida, kas valitud ettevõtete raamatupidajatel on samad teadmised.

Lõputöö koostamisel on kasutatud võõrkeelset ja eestikeelset kirjandust, seadusi, internetiartikleid ja -teavet.

1. UUE ISIKUANDMETE KAITSE ÜLDMÄÄRUSE NÕUDED

Isikuandmete kaitse oli, on ja jääb väga aktuaalseks teemaks kogu ajani. Seda kinnitab tõsiasi, et juba 1995. aastal võttis Euroopa Komisjon vastu direktiivi 95/46/EC (EC-European Council), mis käsitleb üksikisiku kaitset isikuandmete töötlemisel ja selliste andmete vaba liikumist (Timeline. The History of the General Data Protection Regulation 2018). Üheks väga oluliseks eesmärgiks oli luua ühised reeglid kõikidele riikidele, kes on liitunud Euroopa Liiduga. Maailma kõige esimene andmete kaitse seadus võeti vastu Hesseni liidumaal Saksamaa Liitvabariigis 1970. aastal. 1970. aastatel ei olnud see seadus siiski uus, sest 1820. aastal keelas lord Eldon arstidel avaldada märkmeid oma patsientide kohta. 1868. aasta Prantsuse seadus nägi ette rahalise karistuse eraelu puudutavate andmete avaldamise eest (Isikuandmete kaitse ja E-Riik).

Kuna eelmise sajandi lõpu standardid ja reeglid ei ole täna päris asjakohased, võtsid Euroopa Liidu Parlament ja nõukogu 2016. aastal vastu üldise andmekaitse määruse (edaspidi: üldmäärus), mis on üks suurematest saavutustest viimastel aastatel. Infotehnoloogia kiire kasv on tekitanud vajaduse suurteks muudatusteks, sest umbes kakskümmend aastat tagasi oli Euroopas internet kättesaadav vaid ühele protsendile inimestest, kuid praegu on internet enamikul kodus ja mobiiltelefonis. „Üldmääruse eesmärgiks on ajakohastada kehtivad andmekaitsereglid, võttes arvesse majanduse digiteerimist, uute tehnoloogiate kasutuselevõttu ning piiriüleste tehingute arvu kasvu.“ (Isikuandmete kaitse seaduse eelnõu seletuskiri). Tänapäeva arenev tehnoloogia annab võimaluse otsida vastuseid küsimustele, suhelda sõpradega maailma teises otsas, hääletada ja valida seadusandliku võimu esindajaid, allkirjastada lepinguid, kuid kõik need võimalused toovad kaasa vajaduse olla kaitstud.

Uus isikuandmete kaitse üldmäärus asendab 1995. aasta andmekaitse direktiivi, mis võeti vastu ajal, mil internet oli alles arengusjärgus. Kõikidel Euroopa Liidu riikidel oli kaks aastat aega, et tagada oma riigis isikuandmete kaitse üldmääruse täielik rakendatavus 2018. aasta maist alates. Üldmäärus oli loodud selleks, et tagada suurem ühtsus liikmesriikide vahel. Isikuandmete kaitse üldmäärus asendab, täiendab ja täiustab Eestis kehtivat isikuandmete kaitse seadust.

1.1. Privaatsus ja isikuandmed

Privaatsuse üle arutletakse palju, aga siiski on see vähearusaadav ja raskesti juhitav. See on mitmemõõtmeline kontseptsioon, mis sõltub kontekstist ja kultuurist, tihti halvasti määratletud ja vaidlustatud (Marx 2007). Samas valib igaüks ise, mis tema privaatsuse kontseptsiooni kuulub ja kus tema privaatsuse piirid lõpevad. „Õigus privaatsusele on osa isiku üldistest vabadustest ja põhiõigustest vabale enesemääratlusele“ (Männiko 2011). „Igaühel on õigus perekonna- ja eraelu puutumatusse. Riigiasutused, kohalikud omavalitsused ja nende ametiisikud ei tohi kellegi perekonna- ega eraellu sekkuda muidu, kui seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks“ (Eesti Vabariigi põhiseadus § 26).

Isikuandmeteks loetakse kõiki andmeid tuvastatud või tuvastatava füüsilise isiku kohta, mis väljendavad isiku füüsilisi, psüühilisi, füsioloogilisi, majanduslikke, kultuurilisi või sotsiaalseid omadusi, suhteid ja kuuluvust (Andmekaitse inspeksioon. Mis on isikuandmed?). Isikuandmed on igasugune teave tuvastatud või tuvastatava füüsilise isiku (andmesubjekt) kohta. Tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal (Isikuandmete kaitse üldmäärus 2016/679 artikkel 4 p 1). Isikuandmed on mistahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on (Isikuandmete kaitse seadus (edaspidi IKS) § 4 lg 1). Isikuandmed on (Isikuandmete kaitse üldmäärus 2016/679 artikkel § p 1):

- eesnimi ja perekonnanimi
- asukohateave
- e-posti aadress, kui see sisaldab isiku nime ja perekonnanime
- isikukood
- asukoha andmed (näiteks mobiiltelefoni asukohaandmete funktsioon)
- võrguidentifikaatorid/ interneti-protokollid (IP) aadress
- küpsise ID
- telefoninumber reklaami jaoks
- geneetilised andmed
- haigla või arsti valduses olevad andmed, mis isikut eristavad.

Delikaatsed isikuandmed on (IKS § 4 lg 2):

- 1) poliitilisi vaateid, usulisi ja maailmavaatelisi veendumusi kirjeldavad andmed, välja arvatud andmed seadusega ettenähtud korras registreeritud eraõiguslike juriidiliste isikute liikmeks olemise kohta
- 2) etnilist päritolu ja rassilist kuuluvust kirjeldavad andmed
- 3) andmed tervises seisundi või puude kohta
- 4) andmed pärilikkuse informatsiooni kohta
- 5) biomeetrilised andmed (eelkõige sõrmejälje-, peopesajälje- ja silmaiirise kujutis ning geenandmed)
- 6) andmed seksuaalelu kohta
- 7) andmed ametiühingu liikmelisuse kohta
- 8) andmed süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist.

Kõik tundlikud andmed peavad olema hästi kaitstud ja töödeldud. Isikuandmete töötlemine on andmetega tehtav mistahes toiming: kogumine, korrastamine, säilitamine, muutmine, lugemine, kasutamine, edastamine, ühendamine, kustutamine (Andmekaitse inspeksioon. Isikuandmete töötleja üldjuhend). Isikuandmete töötlemise reeglid on loodud, andmaks inimestele kindlustunnet, et nende kohta käivat teavet kogutakse ja kasutatakse ausalt, õigesti ja turvaliselt. Andmete töötlemise alused: isiku poolt avaldatud andmed, seaduse alusel, avaliku võimu teostamiseks, lepingu alusel, vabatahtlik nõusolek, muud alused (Andmekaitse inspeksioon. Isikuandmete töötleja üldjuhend).

Andmete töötlejad võib jagada kaheks: vastutav töötleja ja volitatud töötleja. Töötlemise ja reeglite täitmise eest vastutab vastutav töötleja. Samuti vastutab vastutav töötleja ka volitatud töötleja eest ehk kui midagi juhtub andmetega, siis vastutav töötleja peab selle eest vastutama. Vastutav töötleja peab olema võimeline tõendama, et ta on täitnud isikuandmete töötlemise põhimõtteid. Vastutav töötleja on isik, kes kogub isikuandmeid ja annab teisele (volitatud töötajale) kasutada kogutud andmeid. Üldmäärus ütleb, et vastutav töötleja annab käsu volitatud töötlejale, kus ta sätestab, mida on lubatud andmetega teha, kui kaua on vaja neid säilitada ja millal on vaja kustutada (Andmekaitse mõju raamatupidajale. Veebipõhine koolitus).

Isikuandmete kaitse reeglid ei kehti, kui

- tegu on juriidilise isiku või asutuse andmetega

- teave ei võimalda inimest mõistlike pingutustega tuvastada
- isikuandmeid ei töödelda automatiseeritult ning neist ei tehta ka andmekogumit
- isikuandmeid kasutatakse isiklikul otstarbel või kodumajapidamise tarvis
- liikmesriik kasutab isikuandmeid oma julgeoleku tagamiseks või Euroopa Liidu ühise välis- ja julgeolekupoliitika raames (Isikuandmete töötleja üldjuhend).

Isikuandmete kaitse õigus ei ole absoluutne õigus. Inimene peab olema ka ise teadlik sellest, kuidas ta tagab oma andmete kaitsmise ja kellel ta lubab oma andmeid töödelda. Praegu on paraku väga raske jälgida kõigi oma isikuandmete jagamist, sest infomaailm on kasvanud nii suureks, et see piir ei ole palja silmaga nähtav.

1.2. Isikuandmete kaitse üldmääruse olemus ja definitsioon

„Igaühel on õigus oma isikuandmete kaitsele“ (Euroopa Liidu toimimise lepingu art 16). Isikuandmete kaitse on õiguslik regulatsioon ja selle rakendamine aitab inimestel säilitada oma eraelu privaatsust. Peamiseks põhjuseks, miks andmeid on vaja kaitsta, on asjaolu, et selliste andmete sisu mõjutab isikute eraelu, mis peab olema puutumatu ja mille avalikustamise üle otsustab igaüks ise. Igal inimesel on õigus puutumatusel ning privaatsusele. „Privaatsus on isiku erasfäär“ (Männiko 2011). Selleks et tagada inimeste privaatsus ja konfidentsiaalsus, on Euroopa Parlament ja nõukogu kulutanud palju aega rangete reeglite koostamiseks. Infotehnoloogia kiire areng, mis lubab isiklikku informatsiooni üle maailma saata ja kasutada, on tekitanud uusi väljakutseid. „Tehnoloogia võimaldab nii era- kui ka avaliku sektori asutustel kasutada isikuandmeid oma tegevuses enneolematul ulatuses. Füüsilised isikud avaldavad isikuandmeid üha avalikumalt ja ülemaailmsealt“ (Isikuandmete kaitse üldmäärus). Iga interneti kasutuskord jätab jälje. Interneti veebilehed, mida kasutatakse iga päev, sisaldavad küpsiseid (ingl *cookies*), mis koguvad ja töötlevad informatsiooni iga kasutaja kohta.

Isikuandmete kaitse üldmääruse peamine ülesanne on tagada inimeste isikliku informatsiooni turvaline säilitamine ja töötlemine. „Isikuandmete igasugune töötlemine peaks olema seaduslik ja õiglane. Üldmääruses määratakse konkreetsete töötlemisjuhtude asjaolud ja tingimused, mille alusel isikuandmete töötlemine on seaduslik. Füüsilisi isikuid puudutavate isikuandmete kogumine, kasutamine, lugemine või muu töötlemine ja nende andmete töötlemise ulatus praegu või tulevikus peaks olema nende jaoks läbipaistev“ (Isikuandmete kaitse üldmäärus).

Isikuandmed peavad olema arusaadavad, kättesaadavad ja lihtsalt sõnastatud selle isiku jaoks, kelle informatsiooni töödeldakse. Iga informatsiooni töötleja või koguja peab teavitama isikut, enne kui hakkab informatsiooni mistahes viisil kasutama. Igasugune isikuandmete kasutamine peab eelkõige olema selge ja seadusliku eesmärgiga.

Üldmääruse eesmärk on aidata kaasa vabadusel, turvalisusel ja õigusel rajaneva ala ning majandusliidu saavutamisele, majanduslikule ja sotsiaalsele arengule, riikide majanduse tugevdamisele ja lähendamisele siseturul ning füüsiliste isikute heaolule (Isikuandmete kaitse üldmäärus). Üldmääruse eesmärk ei ole üksnes andmekaitse, vaid andmete turvaline ringlus Euroopa Liidus. „Täiesti uue õigusena sätestatakse õigus andmete ülekandmisele ühe töötleja juurest teise juurde, mis füüsiliste isikute jaoks võib lihtsustada näiteks teenusepakkuja vahetust (telekommunikatsiooniteenused, kommunaalteenused jm)“ (IKS eelnõu seletuskiri). Sellest võib järeldada, et andmekaitse eesmärk on ka inimeste elu lihtsustamine. Näiteks kui inimene tahab võtta laenu SEB pangast, ent omab kontot Swedbankis ning annab nõusoleku oma andmete töötlemiseks, saavad pangad omavahel edastada vajalikku informatsiooni ilma kliendile lisakohustusi tekitamata. Sarnane on olukord ka näiteks perearsti vahetamisel. Kui varem tuli patsiendil oma terviselugu edastada uuele arstile, siis nüüd ei ole selleks enam vajadust – patsient saab anda nõusoleku oma andmete jagamiseks uue perearstiga ning seeläbi saab uus perearst ligipääsu patsiendi tervisele.

Isikuandmete jälgimine on avalikus arvutivõrgus (internetis) eeskätt profiilianalüüs, et teha inimese kohta otsuseid või analüüsida ja ennustada tema eelistusi, käitumist ja hoiakuid (Andmekaitse inspeksioon. Isikuandmete töötleja üldjuhend). Jälgimine on näiteks püsiklientide ehk tuvastatud klientide ostuajaloo andmete analüüs. Inimese kohta eri allikatest sarnaste andmete kogumine on samuti jälgimine (näiteks krediitdivõimelisuse hindamiseks, ühendades inimese kohta saadaolevad avalikud andmed võlausaldajatelt saadud mitteavalike andmetega). Jälgimine on ka inimese asukoha-andmete jälgimine tema teenuste või seadmete kaudu.

Üldmäärus laieneb kõikidele ettevõtetele, kes osutavad teenust või müüvad kaupu Euroopa Liidu kodanikele (ehk kõik organisatsioonid, kes tegutsevad Euroopa Liidus). Kõik need organisatsioonid töötlevad, kasutavad ja koguvad oma äritegevuses Euroopa Liidu kodanike isikuandmeid. Isikuandmete kaitse üldmäärus omab territoriaalset kehtivust. Euroopa Komisjon on kinnitatud turvaliste riikide nimekirja, millega on lubatud informatsiooni vahetada ja mis

tagavad piisava isikuandmete kaitse taseme (Andmekaitse mõju raamatupidajale. Veebipõhine koolitus). Nendeks riikideks on: Albaania, Andorra, Armeenia, Aserbaidžaan, Valgevene, Bosnia ja Hertsegoviina, Gruusia, Püha Tool, Island, Liechtenstein, endine Jugoslaavia Makedoonia Vabariik, Kosovo (vastavalt ÜRO julgeolekunõukogu resolutsioonile 1244/99), Moldova, Monaco, Montenegro, Norra, Venemaa Föderatsioon, Serbia, St Marino, Šveits, Türgi, Ukraina (Euroopa Liidu Teataja. 2018). Selles loetelus ei ole Ameerika Ühendriike (edaspidi USA); USA jaoks on Euroopa Komisjon loonud EL-USA andmekaitseraamistiku Privacy Shield. Andmeid võib edastada raamistikuga liitunud USA äriühingutele ja kontrollida kõigi liitunud äriühingute nimekirja USA kaubandusministeeriumi veebilehel. „Mittepiisava andmekaitse tasemega kolmandasse riiki isikuandmeid edastades tuleb rakendada üldmääruse artikli 46 kohaseid kaitsemeetmeid. Üldmääruse artikkel 49 reguleerib erandjuhtumeid, mil võib isikuandmeid kolmandasse riiki edastada ilma vastavaid kaitsemeetmeid rakendamata. Kolmandatesse riikidesse edastamise lähemaid reegleid käesolevas üldjuhendis ei käsitleta“ (Andmekaitse inspeksioon. Isikuandmete töötleja üldjuhend).

1.3. Kaasnevad ja olulised muudatused üldmääruses

Pärast 25. maid 2018 pidid kõik ettevõtted teavitama oma kliente uue üldmääruse kasutamisest oma ettevõttes ning selgitama, kuidas ja mis eesmärgil kasutatakse klientide isikuandmeid vastavalt kehtivale üldmäärusele. Kõik ettevõtted pidid küsima klientide nõusoleku andmete töötlemiseks; olenemata sellest, kas klient on ettevõtte või füüsiline isik, on kõikide andmesubjektide nõusolek vajalik andmete kasutamisel. Kõik muudatused, mis on võetud üldmäärusest, kehtivad nii digitaalse informatsiooni töötlemisel kui ka paberikandjal või mingis teises variandis (GDPR for accountants: Your questions answered).

Üks suurematest muudatustest, mida Eesti seadused ei käsitle, on inimeste nõusoleku küsimine enne isikuandmete kasutamist, töötlemist, üleandmist, jagamist, kopeerimist. Inimene on oma isikuandmete omanik. Isikuandmed on iga inimese enda vara. Inimene ise otsustab, mida ta lubab teha oma andmetega ja kellel ta lubab oma andmeid töödelda. Andmesubjekti nõusolek on vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub enda kohta käivate isikuandmete töötlemisega. Nõusolek tuleks anda selge kinnitusena, näiteks kirjaliku kinnituse vormis, sealhulgas elektroonilisel teel, või suulise avaldusena, millega andmesubjekt annab vabatahtlikult,

konkreetselt, teadlikult ja ühemõtteliselt nõusoleku teda puudutavate isikuandmete töötlemiseks“ (Isikuandmete kaise üldmäärus).

Näiteks piltide tegemine suvepäeval või jõulupeol on ettevõtetes tavaline asi ja see puudutab ka inimeste nõusolekut. Kui töötaja teeb pildi enda isiklikuks tarbeks, ei ole sellega probleeme, välja arvatud juhul, kui tööl pildistamine on keelatud sisereeglitega. Kui inimene teeb pildi koos teiste töötajatega ja otsustab seda fotot näiteks Facebookis jagada ilma teiste inimeste nõusolekuta, võivad sellega kaasneda mitmed probleemid, kuna ilma inimeste nõusolekuta piltide avaldamine, jagamine ja postitamine on keelatud.

Inimestel on õigus anda oma nõusolek ja on ka õigus see nõusolek tühistada (tagasi võtta/annuleerida). Andmesubjektil on õigus oma nõusolek igal ajal tühistada. Ei ole oluline, kas inimene keeldub pakkumistest, näiteks kliendipakkumised posti teel saatmiseks, või andmesubjekt on töötaja, kes palus mitte avalikustada oma sünnipäeva.

Inimesel on alati õigus paluda parandada oma isiklikku informatsiooni või paluda ka see informatsioon kustutada. Väljend „õigus olla unustatud“ on kehtiv ja peab olema rakendatav kõikides Eesti ja Euroopa Liidu ettevõtetes. Andmesubjektil peaks olema õigus oma isikuandmete kustutamisele ja nende töötlemise lõpetamisele eelkõige siis, kui isikuandmed ei ole enam vajalikud täpsema eesmärgi jaoks, milleks need koguti või neid muul viisil töödeldi. Andmete kustutamist on kirjeldatud üldmääruse artiklis 17: „Andmesubjektil on õigus nõuda, et vastutav töötleja kustutaks põhjendamatu viivitusega teda puudutavad isikuandmed ja vastutav töötleja on kohustatud kustutama isikuandmed põhjendamatu viivitusega, kui kehtib üks järgmistest asjaoludest:

- a) isikuandmeid ei ole enam vaja sellel eesmärgil, millega seoses need on kogutud või muul viisil töödeldud; 4.5.2016 ET Euroopa Liidu Teataja L 119/43
- b) andmesubjekt võtab töötlemiseks antud nõusoleku tagasi vastavalt artikli 6 lõike 1 punktile a või artikli 9 lõike 2 punktile a ning puudub muu õiguslik alus isikuandmete töötlemiseks
- c) andmesubjekt esitab vastuväite isikuandmete töötlemise suhtes artikli 21 lõike 1 kohaselt ja töötlemiseks pole ülekaalukaid õiguspäraseid põhjuseid, või andmesubjekt esitab vastuväite isikuandmete töötlemise suhtes artikli 21 lõike 2 kohaselt
- d) isikuandmeid on töödeldud ebaseaduslikult
- e) isikuandmed tuleb kustutada selleks, et täita vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õigusega ette nähtud juriidilist kohustust

- f) isikuandmeid koguti seoses artikli 8 lõikes 1 osutatud infoühiskonna teenuste pakkumisega“ (Isikuandmete kaitse üldmäärus artikkel 17).

Õigus andmete kustutamisele ei ole absoluutne õigus, kuna kõik sõltub situatsioonist. On erandeid, kus ei ole võimalik informatsiooni kustutada. Näiteks terviseandmetele, mida andmesubjekt tahab varjata teise arstide eest, on võimalik ligipääs piirata, kuid täiesti kustutada neid ei tohi.

Tänu uuele üldmäärusele tekkisid ettevõtetesse konkreetsed andmete töötlemise eest vastutavad isikud. Isikuandmete vastutav töötleja on see ettevõtte/asutus, kes määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid. Volitatud töötleja on see, kes vastutava töötleja nimel ja ülesandel isikuandmeid töötleb. Vastuvõtja on iga isik või asutus, kellele isikuandmeid avaldatakse (Andmekaitse inspeksioon. Isikuandmete töötleja üldjuhend). Vastutav töötleja peab teavitama andmesubjekti informatsiooni kogumisest ja töötlemisest. Kui vastutav töötleja annab informatsiooni edasi volitatud töötlejale, siis vastutav töötleja peab teavitama töötlemise eesmärgist ja seaduslikust alusest, samuti edastama isikule, kelle informatsioon töödeldakse volitatud töötleja nime ja kontaktandmed.

Uue üldmääruse jõustamisega tekkis tööturule uus ametikoht – isikuandmekaitse spetsialist (DPO – Data protection officer). Vastavalt üldmääruse artikli 37 lõikele 6 võib andmekaitse spetsialist olla andmetöötaja koosseisuline töötaja või täita ülesandeid teenuselepingu alusel. Samuti sätestab artikli 37 lõige 1, et andmekaitse spetsialisti peavad määrama kõik avaliku sektori asutused, välja arvatud õigust mõistvat funktsiooni täitvad kohtud (IKS eelnõu seletuskiri).

„Andmekaitse spetsialist – ei ole kehtestatud diplomiga ega muid formaalseid kvalifikatsiooninõudeid. Soovitav on siiski, et tal oleks asjakohane koolitus täiend- või diplomioppena läbitud“ (Andmekaitse inspeksioon. Isikuandmete töötleja üldjuhend). Peamine on see, et andmekaitse spetsialist peab olema võimeline suhtlema nii andmesubjektide kui inspeksiooniga heas ja korrektses eesti keeles. Põhilised andmekaitse spetsialisti ülesanded (Andmekaitse inspeksioon. Isikuandmete töötleja üldjuhend):

- olla andmesubjektidele kontaktisikuks kõigis küsimustes, mis on seotud nende isikuandmete töötlemise ja nende andmekaitse õiguste kasutamisega
- teavitada ja nõustada oma organisatsiooni (vajadusel ka selle partnerite) juhtkonda ning personali andmekaitse alal

- jälgida andmekaitsestandardite rakendamist, sealhulgas vastutusvaldkondade jaotamist, personali teadlikkust ja koolitamist ning andmekaitse auditeerimist; anda nõu seoses andmekaitsealase mõjuhindamisega ning jälgida selle toimimist; teha koostööd Andmekaitse inspeksiooniga, olles tööandja kontaktisikuks.

Andmekaitse spetsialist peab teadma organisatsiooni väärtuseid ja eesmärgi, sealhulgas ettevõtte visiooni, missiooni ning strateegiat.

Ettevõtte, mille andmetöötlejate põhitegevus on andmesubjektide ulatuslik, korrapärane ja süsteemiline jälgimine, andmete eriliikide ulatuslik töötlemine või süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete ulatuslik töötlemine, peavad määrama andmekaitse spetsialisti. Kui ettevõtte on määranud töötlejad, on vaja sellest teada anda nii avalikkusele kui Andmekaitse inspeksioonile. Määramisest on ettevõttel kohustus teavitada ka oma töötajaid.

Nagu ülal mainitud, avab üldmäärus võimaluse inimeste andmeid üle maailma lihtsalt edastada ja kasutada. „Õigus nõuda andmete ülekandmist tähendab, et inimene võib küsida ja saada vastutavalt töötlejalt kõiki teda puudutavaid isikuandmeid, mida ta on andmetöötlejale edastanud. Seda kõike struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul. Samuti on inimesel õigus saada andmed edastada teisele andmetöötlejale kas ise või paluda seda teha andmetöötlejal, kellelt andmed saadi. Andmete ülekandmist saab kohaldada ainult nendele andmetele, mille kogumise aluseks on kas inimese nõusolek või inimese ja andmetöötleja vahel sõlmitud leping“ (Andmekaitse inspeksioon. Isikuandmete töötleja üldjuhend).

Uuteks kohustusteks andmetöötlejatele on isikuandmete töötlemise toimingute registreerimine ja andmekaitsealase mõjuhindamisega koostamine. Registreerimise kohustus on enam kui 250 töötajaga ettevõttel, samuti ettevõttel, mille teostatav töötlemine kujutab tõenäoliselt ohtu andmesubjekti õigustele ja vabadustele, töötlemine ei ole juhtumipõhine või töödeldakse eri liiki isikuandmeid või süütegudega seotud andmeid (IKS eelnõu seletuskiri).

Erilist kaitset vajavad laste isikuandmed, kuna lapsed ei pruugi täielikult mõista andmetöötlusega kaasnevat ohtu, tagajärgi ja kaitsemeetmeid. Seepärast annab alaealise andmete töötlemiseks nõusoleku tema vanem või eestkostja (Andmekaitse inspeksioon. Isikuandmete töötleja üldjuhend). Uueks muudatuseks on alampiiri kehtestamine lapse vanusele, mille puhul on lapse nõusolek isikuandmete töötlemiseks infoühiskonna teenuste pakkumisel seaduslik. Eestis on kavas kehtestada alampiiriks 14 eluaastat. (IKS eelnõu seletuskiri).

Uus üldmäärus paneb paika kõik ettevõtte sisemised reeglid. Samas kohustab see ettevõtteid, millel on vähemalt üks töötaja või vähemalt üks füüsilisest isikust klient, koostama isikuandmete töötlemise ülevaate. Töötlemisülevaates peavad olema vastutava ja volitatud/kasutatava töötleja kontaktandmed, isikuandmete töötlemise eesmärgid, isikuandmete liikide kirjeldus ning kui isikuandmeid edastatakse kolmandasse riiki, siis andmed selle kohta koos riigi nimega ning muu teabega edastamise asjaolude ja kaitsemeetmete kohta ja turvameetmete üldine kirjeldus. Üldmäärus nõuab, et ülevaade peab olema kirjalikus või elektroonilises vormis, suulisest ei piisa. Muid vormistusnõudeid ei ole. Ülevaade võib olla nii ühes kui mitmes dokumendis. Näiteks asutus võib lugeda oma ülevaate osaks enda peetava andmekogu kirjeldust riigi infosüsteemi haldussüsteemis, kui see sisaldab üldmääruse artiklis 30 nõutud teavet (Andmekaitse inspeksioon. Isikuandmete töötleja üldjuhend).

„Isikute või vara kaitseks võib isikuandmeid edastavat või salvestavat jälgimisseadmetikku kasutada üksnes juhul, kui sellega ei kahjustata ülemääraselt andmesubjekti õigustatud huve ning kogutavaid andmeid kasutatakse ainult nende kogumise eesmärgist lähtuvalt. Andmesubjekti nõusolekut asendab sellise andmetöötlemise korral jälgimisseadmetiku kasutamise fakti ning andmete töötleja nime ja kontaktandmete piisavalt selge teatavakstegemine. Nõue ei laiene jälgimisseadmetiku kasutamisele riigiasutuse poolt seaduses sätestatud alustel ja korras“ (IKS § 14 lg 3). Ettevõtte saab kasutada videokaameraga filmitud faile ainult sel juhul, kui ettevõtte on kannatanud kahju ja midagi on juhtunud. Tööndjal ei ole õigust kogu aeg jälgida, kuidas töötajad töötavad, kuid kõik pildistamise, filmimise jt jälgimise reeglid peavad olema kirjas sisereeglitest.

Andmekaitsealase läbipaistvuse võib kokku võtta järgmiselt (Andmekaitse inspeksioon. Isikuandmete töötleja üldjuhend):

- a) inimesele tuleb siis, kui temalt andmeid kogutakse, anda andmetöötleja ja andmetöötlemise kohta teavet
- b) seda tuleb teha ka siis, kui andmed ei ole saadud temalt endalt (v.a. kui teatamine oleks ebaproportsionaalselt keeruline või on andmete saamine või salajas hoidmine seadusega ette nähtud)
- c) inimesel on enda kohta käivate andmete osas: (a) õigus tutvuda oma andmetega, (b) asjakohasel juhul õigus nõuda andmete parandamist, kustutamist, töötlemise piiramist, andmete ülekandmist, samuti õigus esitada vastuväiteid ja keelata otseturundust, (c) kaitse masina tehtud otsuste vastu (v.a. lepingu ja seaduse alusel otsustamisel)
- d) kõigest eelnevast tuleb inimesele teada anda kokkuvõtlikult, selgelt ja arusaadavalt, lihtsasti kättesaadavas vormis, üldjuhul kuu aja jooksul ja tasuta. Eelnevate nõuete täitmiseks

on vastutaval töötlejal hädavajalik koostada ja avaldada oma andmekaitsetingimused (sarnaselt kliendilepingute üld- või tüüptingimustega). Lisaks kindlustab läbipaistvuse ka andmetöötleja kohustus anda suure ohu korral inimesele teada tema andmetega toimunud rikkumisest.

Üldmäärus ei kohaldu ega laiene surnu andmetele. Euroopa liikmesriikidel on õigus surnu kaitseks (ja temaga seotud elavate kaitseks) andmekaitsereegleid kohaldada. “Isiku antud nõusolek kehtib tema eluajal ja 30 aastat pärast tema surma juhul, kui isik ei ole otsustanud teisiti. Kui isik suri alaealisena, siis kehtib tema antud nõusolek 60 aastat pärast tema surma“ (Andmekaitse inspeksioon. Isikuandmete töötleja üldjuhend).

2. ÜLDMÄÄRUSE RAKENDAMINE RAAMATUPIDAMISES

Igas ettevõttes on määratud andmete töötajad; enamasti on need raamatupidajad, kuna nad peavad teadma mitte ainult arvestuslikke protsesse, vaid ka seadusi ja Euroopas kehtivaid nõudeid. Raamatupidajad kasutavad suurt osa klientide ja töötajate isikuandmete informatsioonist. Kõik andmete töötajad peavad olema kursis kõikide üldmääruse nüanssidega.

2.1. Üldmääruse kasutamine raamatupidamises igapäevatoos

Nagu eespool mainitud, mängivad paljudes ettevõtetes raamatupidajad üsna suurt rolli. Nad töötlevad tavaliselt kahte tüüpi isikuandmeid. Kliendiandmed – kliendilt saadud isiklikud andmed, mis on seotud selle ettevõttega. Ettevõtte andmed – ettevõtte enda valduses olevad isikuandmed oma juhtimisest, töötajatest ja töökeskkonnast, sealhulgas ka turunduse andmebaasid. Ettevõtte sisemistes regulatsioonides peab olema lahti kirjutatud isikuandmete kogumise eesmärk, näiteks ettevõtte kogub ja töötleb töötajate laste andmeid selleks, et tagada lapsepuhkusepäevade andmine. Samuti peab kirjas olema, mis dokumente kogutakse ning kui kaua neid säilitatakse.

Infotehnoloogia kiire areng on muutnud ka raamatupidamise sisemisi süsteeme. Näiteks kümme aastat tagasi oli raamatupidamises kasutusel kolmeleheküljeline kontoplaani süsteem, viis aastat tagasi olid kasutusel isikukonto kaardid, kus kõik vajalik info oli paber kandjale prinditud ning pandud kartoteeki. Tänapäeval on enamik infot digitaalselt kättesaadav. Paberarhiivid, mis kulusid palju paberit ja ruumi, ei ole enam vajalikud. Üldmäärus tõi raamatupidajate töösse uusi väljakutseid nõuete ja tegevuste kooskõlastamise näol. Üldmääruse põhimõte on kaitsta kõiki andmeid, sest tänapäeva raamatupidamine on suuresti kolinud arvutisse ja salvestatud elektroonilisel kujul, mistõttu andmekaitse ja range kontroll on väga tähtis. Üldmäärus nõuab ja kohustab raamatupidajaid end arendama, et ajaga kaasas käia. „Aastaid on räägitud sellest, et raamatupidajad peaksid tegelema rohkem nõustamisega ja vähem rutiinse tööga“ (RMP. Kuidas arendada raamatupidajast nõustajaks ja miks see vajalik on?). Selleks et olla tänapäeva tööturul konkurentsivõimeline, peab raamatupidaja hästi teadma isikuandmete kaitse seadusi ja üldmäärusi.

Iga raamatupidaja peab teadma, et töölepinguid on vaja säilitada töölepingu kehtivuse ajal ja kümme aastat pärast töölepingu lõppemist (Töölepingu seadus § 2). Töölepingu pikemaks säilitamiseks seaduslikku alust ei ole. Kõikide teiste dokumentide, näiteks diplomi koopia, keeletaseme tõendi koopia jt tõendite puhul on kohustus need hävitada töötaja töölt lahkumisele järgneval päeval. Kui raamatupidaja otsustab säilitada inimeste isiklikke dokumente, siis peab sisereeglites olema korrektselt lahti kirjutatud, mille jaoks ja mille eesmärgil seda informatsiooni ettevõttes säilitatakse.

Töölepingu koostamine ja selle alusel informatsiooni töötlemine on lahutamatu osa raamatupidaja tööst. Üldmääruse jõustumine kitsendas töötajatelt küsitud isiklikku informatsiooni. Üldmäärus sätestab rangelt selle, et raamatupidajad võivad koguda andmeid minimaalselt ja kindla eesmärgi jaoks, näiteks töölepingu koostamiseks.

Isikuandmed, mis raamatupidaja vajab oma töös:

- eesnimi ja perekonnanimi
- isikukood (siit tuleb sünniaasta, kogumispensioni määr)
- palgainfo
- tulude info (tulumaksuvaba miinimumi arvestamiseks)
- pangakonto number
- laste arv ja vanus/isikukood (lapsehoolduspäevade arvestamiseks)
- tervises seisund (töövõimetuspensioni arvestamiseks)
- e-posti aadress (küsimuste ja palgateatise saatmiseks).

Peaaegu kõik need on tundlikud ja delikaatsed isikuandmed, mille kasutamine nõuab inimese nõusolekut. Enne üldmääruse jõustumist oli võimalik töölepingus küsida andmeid laste, abikaasa, kodukeele ja huvide kohta. Nüüd nõutakse täpset seletust, mille jaoks raamatupidaja või tööandja seda informatsiooni kogub. Tegelikult ei ole kõik nimetatud andmed vajalikud, et inimene tööle võtta ja tööleping sõlmida.

Raamatupidajal on õigus küsida töötajalt tema laste arvu ja omada informatsiooni, kas lapsed on nooremad kui 13 aastat. Kuid töötaja ise otsustab, kas avalikustada see informatsioon ja anda edasitöötlemiseks või mitte. Raamatupidajal on vaja teada, mitu last on töötajal ja kui vanad nad on, selleks et pärast arvutada lapsepuhkuse päevi; teada, kas töötaja saab riigi toetust lapse sünni puhul; kui ettevõttes tehakse lastele kingitusi, siis näiteks jõulude ajal kinkida komme. Kui ettevõttes on hästi loodud töökeskkond ja töötajad jagavad vabalt isiklikku informatsiooni, näiteks

oma perekonna ja laste kohta, siis selle otsuse teevad inimesed ise. Selle informatsiooni töötlemine on lubatud ning raamatupidajad saavad seda täiesti kasutada lubatud piirides.

Kõik, mis puudutab töötaja privaatsust tööl, peab olema ettevõtte sisereeglites lahti kirjutatud. Ettevõttel on õigus salvestada telefonikõnesid ainult sel juhul, kui töötaja on andnud oma nõusoleku. Kõik nõusolekud peavad olema allkirjastatud paberikandjal või digitaalse allkirjaga. Ettevõtetel on õigus kuulata kõiki salvestatud kõnesid ainult sel juhul, kui midagi juhtub. Suured ettevõtted, mis töötavad välismaa pankadega, küsivad oma töötajate nõusolekut telefonikõnede salvestamiseks, sest kui midagi juhtub, näiteks raha ülekandmisel tehti viga, saab ettevõtte kohtus seda informatsiooni täiesti vabalt kasutada.

Tööandjad ise valivad, keda nad tööle võtavad ja kellega tahavad koostööd teha. Kui töövõimetu inimene võetakse tööle koristajaks, siis inimene ise otsustab, kas avalikustada töövõime puue või mitte, kuna see on töötaja enda otsus, kas puue segab töö tegemist. Kui puue ei sega töötamist ja inimene ei soovi seitset päeva lisapuhkust, siis tööandjal ei ole õigust nõuda töövõimetususe tõendit. Samuti kui üliõpilane ei soovi võtta õppepuhkust, siis raamatupidajal ei ole õigust küsida ülikooli tõendit ilma seletuseta, mille jaoks see on vajalik.

Tööandjal on kohustus suunata töötaja tervisekontrolli ja see ei ole töötajale vabatahtlik. Tööandja säilitab tervisekontrolli otsuseid kümme aastat pärast töötajaga töösuhte lõpetamist (Töötajate tervisekontrolli kord p 7 lg 2). Selle informatsiooni avalikustamine on keelatud ning avalikustamise ignoreerimisel kaasneb rahaline karistus.

Pärast üldmääruse jõustumist ilmus lisapunkt töölepingutes sünnipäeva informatsiooni avalikustamisest. Sellest peavad teadlikud olema kõik ettevõtte töötajad, sest kui inimene ei ole andnud oma nõusolekut sünnipäeva avaldamiseks, siis tuleb täpsustada, kas tohib kogu kollektiiviga inimest õnnitleda. Vastasel juhul oleks tegu privaatsusõiguse rikkumisega. See lisapunkt töölepingu sõlmimisel aitab tegutseda kooskõlas üldmäärusega ja vältida ebamugavaid situatsioone.

Isikuandmeid kui eraandmeid ei tohi isiklikule e-postile saata, kuna selline teguviis pole turvaline. Raamatupidaja peab igakuise palgateatise töötajale saatma ise või saadab raamatupidamisprogramm need automaatselt. Need e-posti aadressid, millelt saadetakse ja millele saadetakse, peavad sisaldama kaitstud domeeni. E-posti aadresse, mida raamatupidajad kasutavad tarnijate või klientide saldo kinnitamiseks, müügiarvete saatmiseks ja erinevate tööküsimuste lahendamiseks,

ei tohiks kasutada turunduspostituseks, samuti ei ole lubatud neid klientide e-posti aadresse kellegi teisega jagada või kellelegi anda.

Töötajal on õigus paluda parandada isiklikke andmeid, näiteks kui töötaja abiellub või elukoha aadress või telefoninumber on muutunud. Informatsiooni kustutamist on võimalik nõuda ainult siis, kui ei ole seadusest tulenevat kohustust seda informatsiooni alles hoida. Töötaja ei tohiks paluda tööandjat kustutada palgainformatsiooni kõigis Exceli tabelites või paluda kõigi müügiarvete kustutamist.

Tänapäeval on ettevõtetes levinud BYOD (Bring your own device) poliitika, mis eesti keeles tähendab oma seadme tööle kaasa võtmise poliitikat. Selline lähenemine on ühelt poolt töötajale mugav, kuna ta saab ise valida, kas töötada kontoris või mujal. Teisalt toob see kaasa erinevaid riske ettevõttele, näiteks informatsiooni kaotamine, salastatud info avalikustamine või kustutamine.

Peaaegu kõik veebilehed kasutavad küpsiseid; sellega on vaja olla ettevaatlik. Enamikul veebilehekülgedel kasutatakse küpsiseid, mis käituvad kui informatsiooni jälgijad ja salvestajad. Küpsiste abil määratakse ja salvestatakse teenuste kasutamise valikud, näiteks kui tihti inimene käib veebilehel, mis ajal, samuti on võimalik näha inimese eelistusi ja regionaalseid sätteid.

IP-aadress – internetiprotokoll; „Euroopa andmekaitseasutused on küsimust erinevates arvamustes analüüsinud ning jõudnud järelduseni, et IP-aadress kvalifitseerub üldjuhul isikuandmeteks“ (Andmekaitse inspeksioon. IP-aadress ja privaatsus).

IP-aadressi teades saab näiteks (Andmekaitse inspeksioon. IP-aadress ja privaatsus, lk 4)

- teha kindlaks, kellele võrk kuulub ja kes võrku haldab. IP-aadressi põhjal on WHOIS (andmebaasiteenus, mis annab infot interneti domeeninimede, võrkude ja kasutajate kohta) andmebaasist otsides võimalik leida teavet organisatsiooni kohta (sh nimi, telefoninumber, aadress)
- teha pöördkontrolli (IP-aadressi määramine sellega seostatud domeeninime põhjal), et leida arvuti nimi, mis sisaldab sageli vihjeid füüsilise asupaiga kohta
- jälgida andmeedastuse teekonda (kasutades arvutidiagnostika vahendit, mis kuvab pakettide teekonna IP-võrgu kaudu), et leida loogiline tee arvutini, mis sageli hõlmab vihjeid füüsilise asupaiga kohta

- teha kindlaks arvuti geograafiline asukoht erineva täpsusega. Sõltuvalt kasutatud kontrollivahendist võib see sisaldada riiki, piirkonda, linna, laius- ja pikkuskraadi, telefoni piirkonnakoodi ja asukohaspetsiifilist kaarti;
- erinevate otsinguteenuste abil paljastada failivahetuse tegevused (nn P2P ehk peer-to-peer) või isikute veebitegevused (nt Wikipeedia toimetamine).

Erineva valdkonna ettevõtetal võivad olla eriõigused informatsiooni töötlemiseks. Näiteks ettevõtted, mis osutavad meditsiinilisi teenuseid, saavad kasutada ühist kogumikku, kus on saadaval inimeste haiguste ja analüüside informatsioon.

2.2. Üldmääruse rikkumise tagajärjed

Isikuandmete kaitse üldmäärus kohustab kõiki andmete töötlejaid kaitsma inimeste andmeid ja töötleva neid vastavalt seadusele. Mistahes andmete kaotamine ja avalikustamine toob kaasa karistuse. „Isikuandmetega seotud rikkumise korral teatab vastutav töötleja isikuandmetega seotud rikkumisest 72 tunni jooksul pärast sellest teada saamist, välja arvatud juhul, kui rikkumine ei kujuta endast tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele. Kui järelevalveasutust teavitatakse hiljem kui 72 tunni jooksul, esitatakse teates selle kohta põhjendus“ (Isikuandmete kaitse üldmäärust 2016/679 artikkel 33). Vastutav töötleja dokumenteerib kõik isikuandmetega seotud rikkumised: asjaolud, mõju ja parandusmeetmed (Andmekaitse inspeksioon. Töö). Üldmääruse rikkuja peab esitama avalduse Andmekaitse inspeksioonile oma tegevustest. „Andmekaitse inspeksioon jätab andmetöötleja pädevusse otsustada, kas teatis edastatakse krüpteeritult või mitte. Krüpteerimise korral tuleb kasutada DigiDoc3 krüptot“ (Andmekaitse inspeksioon. Rikkumisteate edastamine 2018). Samuti on vaja esimesel võimalusel teavitada inimest, kelle informatsioon kadus või avalikustati. „Vastutav töötleja peaks ilma põhjendamatu viivitusega teavitama andmesubjekti isikuandmetega seotud rikkumisest, kui rikkumise tulemusena tekib tõenäoliselt suur oht füüsilise isiku õigustele ja vabadustele, et võimaldada andmesubjektil võtta kasutusele vajalikke ettevaatusabinõusid“ (Isikuandmete kaitse üldmäärus 2016/679 artikkel 86).

Üldmääruse rikkumise tagajärjeks on range karistus – trahv, mille suurus on kuni 20 000 000 eurot või ettevõtja puhul kuni 4% tema eelmise majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem (Isikuandmete kaitse üldmäärus 2016/679 artikkel 83).

Eestis ei ole palju ettevõtteid, mis oleksid võimelised nii suurt trahvi maksma. Andmekaitse inspeksioon määrab trahvisummaks väärteokaristusena kuni 32 000 ning sunnirahana kuni 9600 eurot (Andmekaitse inspeksioon. Kas isikuandmete kaitse üldmäärus toob tõesti kaasa hiigeltrahvid? 2017). Kuid kehtiva IKS kohaselt saab isikuandmete töötlemise nõuete rikkumisest karistada füüsilist isikut rahatrahviga kuni 1200 eurot ning juriidilist isikut kuni 32 000 eurot. AKI peab tagama, et trahvi määramine oleks tõhus, proportsionaalne ja heidutav. Üldmäärus sätestab konkreetsed aspektid, mida järelevalveasutus peab kaaluma karistuse üle otsustamisel (IKS eelnõu seletuskiri).

Isikuandmetega seotud rikkumisest saab teavitada ka isik ise, kelle andmed töödeldakse. Kui inimene tunneb, et tema isikuandmeid on valesti salvestatud või ilma tema nõusolekuta kasutatud, on inimesel õigus ise pöörduda Andmekaitse inspeksiooni, kus uuritakse, kas tegemist oli üldmääruse rikkumisega.

2.3.Olulised turvameetmed raamatupidajate ja kogu ettevõtte jaoks

Isikuandmete kaitse seaduse 26. paragrahv sätestab, et „füüsiline isik, kes isikuandmete töötleja alluvuses töötleb isikuandmeid, on kohustatud neid töötleva käesolevas seaduses lubatud eesmärkidel ja tingimustel ning vastutava töötleja antud juhiste ja korralduste kohaselt“. „Isikuandmete töötleja on kohustatud tagama oma alluvuses isikuandmeid töötlevate isikute väljaõppe isikuandmete kaitse alal“ (IKS 26 lg 3). Seega esimene turvameetod on töötajate koolitamine. Pole oluline, kas tegemist on uue või staažika töötajaga, kõik töötajad vajavad õigeaegset koolitust ja neid peab teavitama uuetest reeglitest, majandusmuutustest jt tööd puutuvatest asjadest.

Isikuandmete töötleja on kohustatud kasutusele võtma organisatsioonilised, füüsilised ja infotehnilised turvameetmed isikuandmete kaitseks (IKS 25 lg 1):

- andmete tervikluse osas – juhusliku või tahtliku volitamata muutmise eest
- andmete käideldavuse osas – juhusliku hävimise ja tahtliku hävitamise eest ning õigustatud isikule andmete kättesaadavuse takistamise eest
- andmete konfidentsiaalsuse osas – volitamata töötlemise eest.

Isikuandmete töötleja on isikuandmete töötlemisel kohustatud (IKS 25 lg 2)

- vältima kõrvaliste isikute ligipääsu isikuandmete töötlemiseks kasutatavatele seadmetele

- ära hoidma andmete omavolilise lugemise, kopeerimise ja muutmise andmetöötlussüsteemis, samuti andmekandjate omavolilise teisaldamise
- ära hoidma isikuandmete omavolilise salvestamise, muutmise ja kustutamise ning tagama, et tagantjärele oleks võimalik kindlaks teha, millal, kelle poolt ja milliseid isikuandmeid salvestati, muudeti või kustutati või millal, kelle poolt ja millistele isikuandmetele andmetöötlussüsteemis juurdepääs saadi
- tagama, et igal andmetöötlussüsteemi kasutajal oleks juurdepääs ainult temale töötlemiseks lubatud isikuandmetele ja temale lubatud andmetöötluseks
- tagama andmete olemasolu isikuandmete edastamise kohta: millal, kellele ja millised isikuandmed edastati, samuti selliste andmete muutusteta säilimise
- tagama, et isikuandmete edastamisel andmesidevahenditega ja andmekandjate transportimisel ei saaks isikuandmeid omavoliliselt lugeda, kopeerida, muuta või kustutada;
- kujundama ettevõtte, asutuse või ühenduse töökorralduse niisuguseks, et see võimaldaks täita andmekaitse nõudeid.

Isikuandmete töötleja on kohustatud pidama arvestust isikuandmete töötlemisel kasutatavate tema kontrolli all olevate seadmete ja tarkvara üle, dokumenteerides järgmised andmed (IKS 25 lg 3):

- seadme nimetus, tüüp ja asukoht ning seadme valmistaja nimi
- tarkvara nimetus, versioon, valmistaja nimi ja kontaktandmed.

Teine turvameede on, et töötajad peavad kasutama tugevaid paroole. Kõik olulised andmed peavad olema kaitstud lisaparooliga. Ettevõttes peab olema struktureeritud süsteem tagamaks andmete kaitse ning vältimaks võimalikke lekkeid, mis peaks käima käsikäes töötajatele tehtava teavitustööga võimalikest ohtudest. Levinud andmekaitsemeetmeks on töötajate kohustus kasutada tugevaid paroole, sh peavad paroolid olema piisavalt pikad, sisaldama suuri tähti, juhuslikke numbrimärke, erisümboleid jne. Lisaks kasutatakse kohustust paroole teatud aja tagant vahetada, vältimaks seda, et ettevõttest lahkunud töötajad omaks ligipääsu turvatud infole. Levinud meetmeks on ka töötajate identifitseerimine kiipkaardi, ID-kaardi või muu vahendi abil.

Kolmas turvameede on mitte kasutada töö tegemisel isiklikku arvutit või teisi isiklikke seadmeid. Eespool mainitud BYOD poliitika rakendamine aitab ettevõttel hoida kokku seadmete soetamise kulusid, ent samal ajal on ohuks informatsiooni kaotamine või mittetahtlik avaldamine. Sellest tulenevalt on nõue kasutada tööl olevaid või töökoha poolt antud seadmeid ning vältida isiklike seadmete kasutamist töökohustuste täitmiseks. Kõikidel kontoriarvutitel peab olema viirusetõrje

tarkvara ning arvutid peavad olema turvaliselt konfigureeritud ja pahavaravabad. Kui siiski soovitakse kasutada oma seadet töökohustuste täitmiseks, on oluline turvaetiketi säilitamine, näiteks pärast informatsiooni eksportimist oma seadmesse ja selle töötlemist tuleks informatsiooni jäljed oma seadmest kustutada.

Neljandaks turvameetmeks on ettevõtte sisereeglid. Ettevõttes peab olema struktureeritud süsteem tagamaks andmete kaitse ning vältimaks võimalikke lekkeid, mis peaks käima käsikäes töötajatele tehtava teavitustööga võimalikest ohtudest.

Viies turvameede on enne lepingu sõlmimist uue kliendi või tarnijaga kontrollida isikut tõendavat dokumenti, vaadata, kas esitaja ikka on see, kellenä ta end esitleb.

Mõnes raamatupidamistarkvaras on võimalik seadistada ka isikuandmete kaitse moodul, mille abil töötajad saavad mõnede seadustega tutvuda või kinnitada, et nad on seda seadust lugenud ja teavitatud. Igas raamatupidamise tarkvaras peab olema seadistatud kasutajate ajalugu ja programmi sisenemisel peab olema iga kasutajal oma kasutajatunnus. Seega kuuendaks turvameetmeks peetakse raamatupidamise programmi kaitstud ligipääsu ja võimalust jälgida töötajate tegevusi.

Uue töötajatega töölepingu sõlmimisel tasub täpsustada, milline on ettevõttes kontrollivate ja järelevalvesüsteemide kasutamine. Tööandja on kohustatud austama töötaja privaatsust ja kontrollima töökohustuste täitmist viisil, mis ei riku töötaja põhiõigusi. Läbi tuleks rääkida kõik võimalikud jälgimise meetmed ja küsida selleks töötaja nõusolekut. Seitsmes turvameede on sisereeglites täpselt lahti kirjutada jälgimise reeglid ja tutvustada neid töötajatele.

Nagu eespool tutvustati, on raamatupidaja vastutava töötleja rollis, ent volitatud töötleja rolli võtab ettevõtte, kes osutab raamatupidamistarkvara haldamise teenust. Ettevõtte, kes hoolib oma andmebaasist, klientide ja töötajate privaatsusest, peab sõlmima tarkvarateenuse osutajaga lepingu andmete kasutamiseks ja töötamiseks. Ja see ongi kaheksas turvameede. Iga mõistlik andmetöötleja hindab nii või teisiti oma tänaseid ja tulevaseid ohte, kui selleks on vajadus (Andmekaitse inspeksioon. Isikuandmete töötleja üldjuhend).

Paljud ettevõtted nagu Eesti AGA AS ja Telia Eesti AS on oma veebileheküljel teinud kättesaadavaks andmekaitsega seotud dokumendid ja lihtsalt selgitanud, kuidas nad kasutavad oma

kliendi andmeid. Need dokumendid tehakse ümber ja täiendatakse, kui seadused või üldmäärused muutuvad. Selline lähenemine aitab tavalistel inimestel ja klientidel olla kursis enda andmete töötlemisega. Üheksas turvameede on kõikide oma klientidega – pole oluline, kas uuega või vanaga – kokku leppida andmete kogumine ja töötlemine.

Ettevõtted peavad põhjalikult kaardistama võimalikud andmekaitseriskid, seda nõuab üldmäärus. Kümnes turvameede on kogu aeg arendada ettevõtte turvameetmeid, otsida nõrku ja halvasti kaitstud kohti, et teha kindlaks, kas ettevõtte on kaitstud.

„Samas on selge, et kui inimene ise oma eraelu kaitsest ei hooli, siis ka teenuseosutaja ei saa teda vägisi kaitsta“ (Andmekaitse inspeksioon. Isikuandmete töötleja üldjuhend). Kuid iga ettevõtte, kes tegutseb Euroopa Liidus, peab panustama, et vastata kõikidele üldmääruse nõuetele.

3. EESTI ETTEVÕTETE RAAMATUPIDAJATE TEADMISTE HINNANG JA ANALÜÜS

3.1. Uuringu meetoodika ja valimi kriteeriumid

Lõputöös püstitatud uurimisprobleemi lahendamiseks kasutati kombineeritud uurimismeetodit ehk nii kvalitatiivset kui ka kvantitatiivset uurimust. Kvantitatiivse uurimismeetodina kasutati küsitlust keskkonnas Google Forms, mille abil koguti raamatupidajatelt statistilisi vastuseid. Uurimusest võttis osa 60 inimest, kes olid erineva suurusega ettevõtetes otseselt või kaudselt seotud raamatupidamisega. Vastajate vanus jäi vahemikku 22-60 eluaastat. Küsimustiku koostamisel lähtuti sellest, et vastuste abil oleks võimalik anda võimalikult täpne hinnang raamatupidajate teadmisele üldmääruse kohta ning tuvastada võimalikud kitsaskohad määruse kohaldamisel igapäevatöös. Küsimused olid valikvastustega, hinnanguskaalaga või arutlevad küsimused, kus oli vaja avaldada oma arvamust ning põhjendada kirjapandut. Küsimuste ülesehitus oli selline, et vastaja sai kontrollida oma teadmisi antud valdkonnas ja analüüsida, kui palju ta antud teemast teab. Küsimustik on kättesaadav: <https://goo.gl/CcPJWS>, (vt lisa 7).

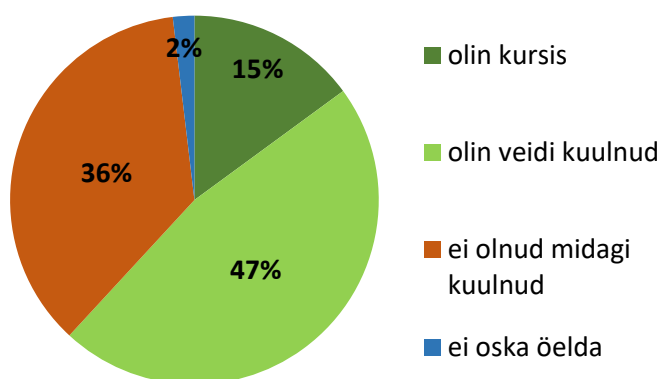
Kvalitatiivse meetodina kasutati intervjuude läbiviimist raamatupidajatega. Intervjuu küsimused koos raamatupidajate vastustega on välja toodud lisas 1-6. Uuringust võtsid osa kuus raamatupidajat erineva suurusega ettevõtetest ning intervjuud viidi läbi vahemikus 05.11.2018–15.11.2018. Intervjueeritavate valimisel lähtuti sellest, et leida raamatupidajaid eri suurusega ettevõtetest – väikestest, keskmistest ja suurtest – ning võrrelda nende oskusi ja teadmisi. Intervjuu keskmine pikkus oli 15–20 minutit. Enne intervjuuga alustamist küsiti töötajatelt nende nõusolekut intervjuu vastuste lindistamise, lõputöös kasutamise ning nende isiku avaldamise kohta. Mõned intervjueeritud soovisid jääda anonüümseks, mistõttu osad vastajad on välja toodud nimega, teised muu numbriga (näiteks Vastaja 1).

Intervjuu analüüsi tegemiseks kasutas autor Schütze meetodit, mis koosneb erinevatest etappidest (Diskursusanalüüs jt intervjuu analüüsi meetodid 2016). I etapp on detailne transkribeerimine. Kõik raamatupidajate vastused on välja toodud lisades. II etapis eristatakse narratiivsed (kes,

millal, kus ja miks midagi tegi) ja mittenarratiivsed lõigud (kirjeldavad ja argumenteerivad väited). III etapis analüüsitakse narratiivseid osasid, nende järgnevust ehk trajektoori. IV etapp on mittenarratiivsete osade analüüs ehk teadmusanalüüs. V etapp: individuaalsete trajektooride võrdlemine ja nende rühmade leidmine. VI etapis võrreldakse äärmuslikke juhtumeid, asetatakse individuaalsed trajektoorid oma konteksti ja tuvastatakse sarnasusi. See protsess võimaldab välja selgitada kollektiivseid trajektoore.

3.2. Interneti uuringu tulemused

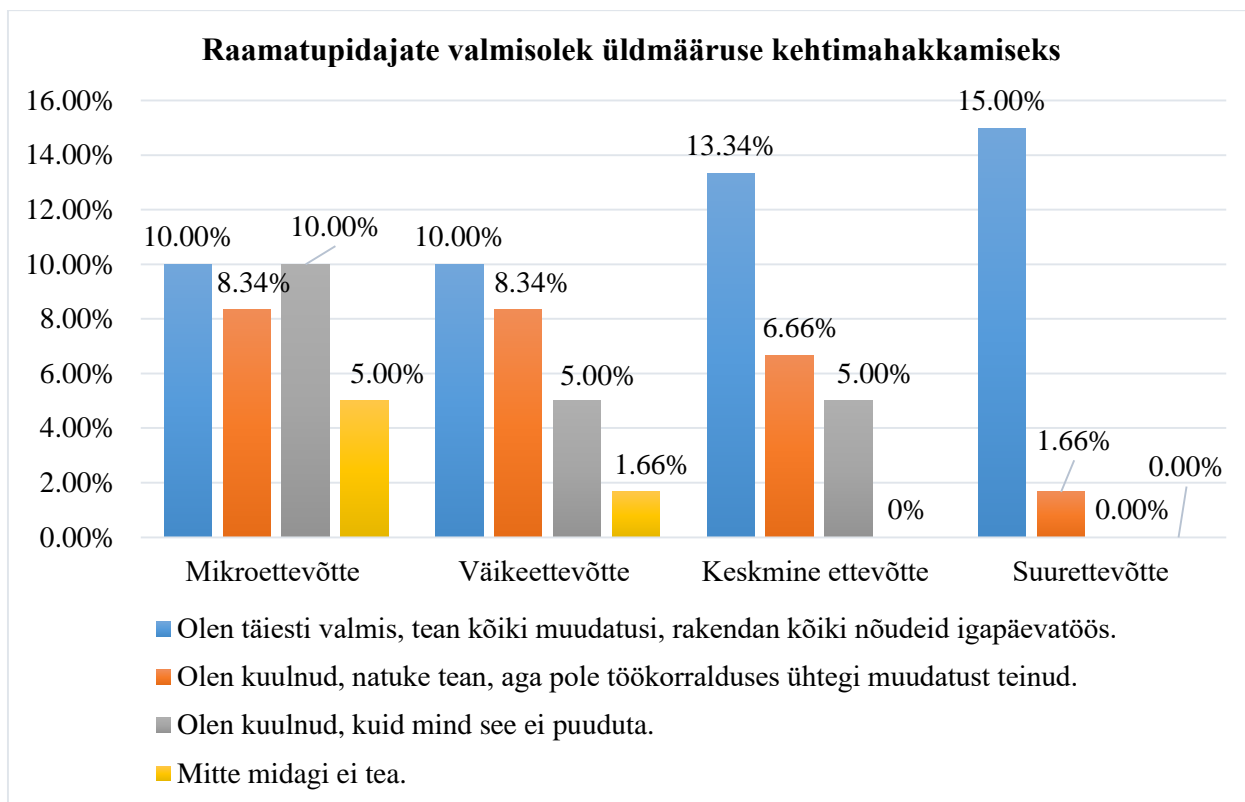
Kuigi üldmäärus jõustus 2018. aasta mais, alustas Andmekaitse inspeksioon 2016. aastal prognooseerima täiendavaid kulusid seoses andmekaitseõiguse rakendamisega ja läbi viima küsitlusuuringuid.



Joonis 1. Ettevõtjate teadlikkus andmekaitse reformist (vastused küsimusele „Kui palju te teadsite enne käesoleva ankeedi täitmist kevadel jõustuvast andmekaitse reformist?“)

Allikas: Turu-uuringute AS

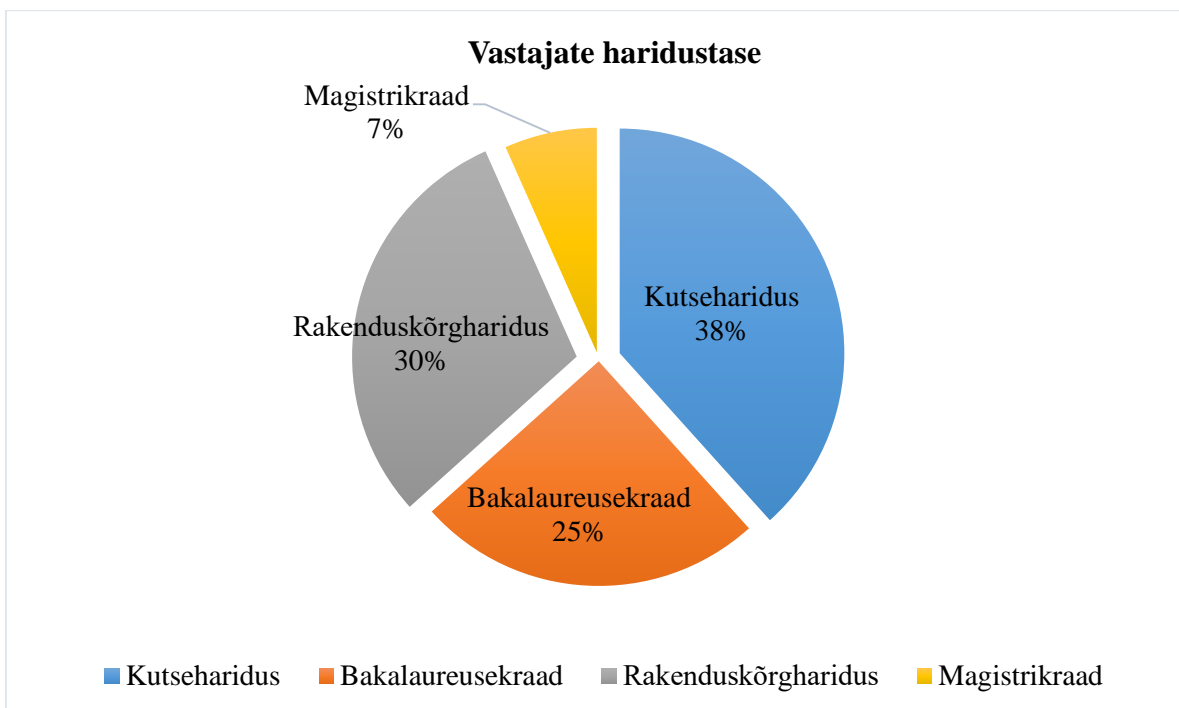
Jooniselt 1 on näha, et iga seitsmes oli üldmääruse jõustumisega kursis, pooled olid üldmääruse kohta veidi kuulnud ning kolmandik ei olnud midagi kuulnud. Sellest võib järeldada, et teavitustöö ei olnud piisav või ei jõudnud piisavalt hästi ettevõtjateni. 2017. aastal oli majandusüksuste arv Eestis 158 000. Kuna ettevõtete arv kasvab, on oluline, et erinevad ettevõtteid puudutavad seadusemuudatused jõuaksid õigel ajal firma juhtkonnani, et nad oleksid ette valmistatud muudatuste läbiviimiseks.



Joonis 2. Raamatupidajate valmisolek üldmääruse kehtimahakkamiseks

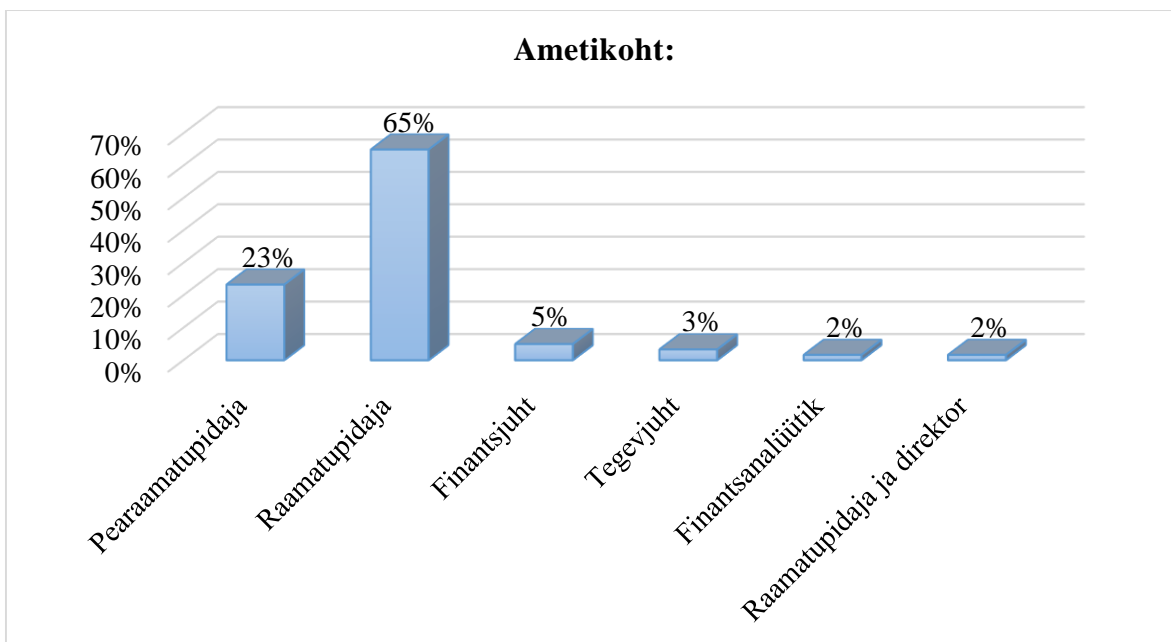
Allikas: küsitlusuuring, autori arvutused

Jooniselt 2 on näha, et 10% (6 inimest) mikroettevõtete raamatupidajatest rakendab üldmääruse nõudeid oma igapäevatoos. Väikeettevõtetes rakendab üldmääruse nõudeid pidevalt 10% raamatupidajatest, keskmise suurusega ettevõtetes 13,34% raamatupidajatest ja suurtes ettevõtetes 15% raamatupidajatest. Ettevõtte suuruse kasvades kasvab ka määruse rakendamise protsent. Mikro- ja väikeettevõtete raamatupidajatest 8,34% ei olnud teinud töökorralduses vastavaid muudatusi. Keskmise suurusega ettevõtete raamatupidajatest 6,66% ei olnud läbi viinud üldmäärusele vastavaid muudatusi. Madalaim on osakaal suurettevõtete raamatupidajate seas, kus antud näitaja on 1,66%. Mikroettevõtete raamatupidajatest 10% arvas, et üldmääruse nõuded nende tööd ei puuduta, väikeettevõtete raamatupidajate seas oli see näitaja kaks korda väiksem, ainult 5%. Antud osakaal on võrdne keskmise suurusega ettevõtetes, kus 5% raamatupidajatest arvas, et üldmääruse nõuded nende tööd ei puuduta. Üldmäärusest ei olnud midagi kuulnud 5% mikroettevõtete ja 1,66% väikeettevõtete raamatupidajatest.



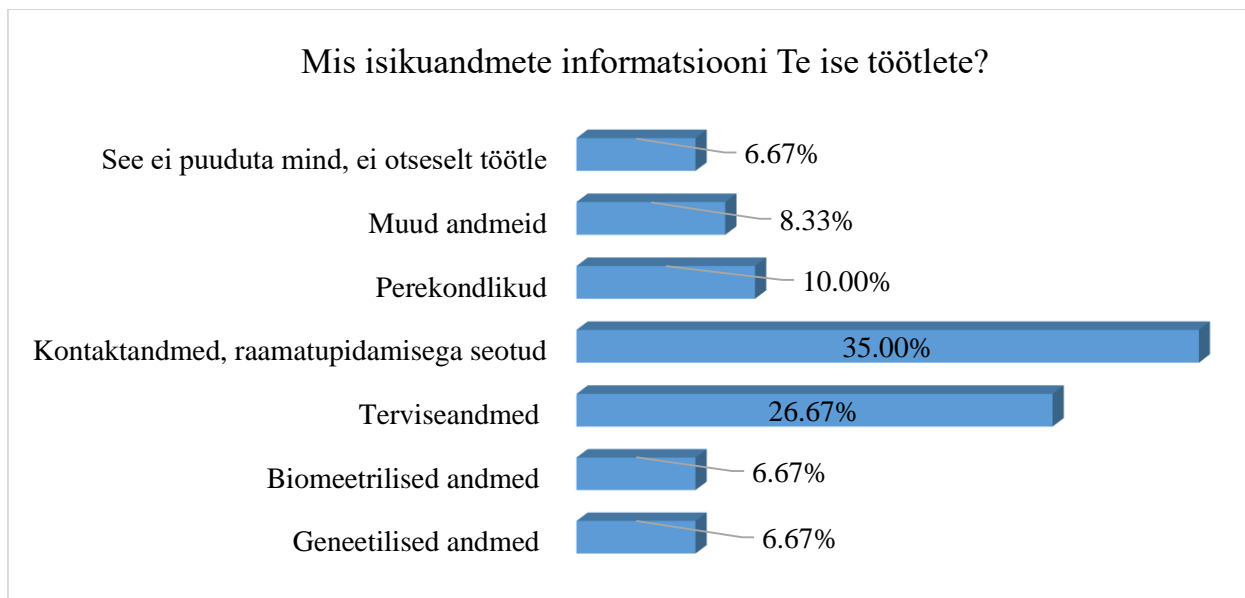
Joonis 3. Vastajate haridustase
Allikas: Küsitlusuuring, autori arvutused

Jooniselt 3 on näha, et 30% vastajatest on rakenduskõrgharidus, 38% vastajatest omavad kutseharidus, 25% vastajatest on bakalaureusekraadiga, 7% magistrikraadiga.



Joonis 4. Vastajate ametikoht
Allikas: küsitlusuuring, autori arvutused

Jooniselt 4 on näha, et vastajatest 65% on ametikohalt raamatupidajad, 23% pearaamatupidajad, 5% finantsjuhid, 3% tegevjuhid, 2% finantsanalüütikud, 2% raamatupidaja ja direktor ühes vormis.



Joonis 5. Raamatupidajate töödeldava informatsiooni liigid

Allikas: küsitlusuuring, autori arvutused

Kõige rohkem töödeldakse kontaktandmeid ja raamatupidamisega seotud andmeid (35%). Terviseandmeid töötles 26,67% vastajatest. Biomeetrilisi ja geneetilisi andmeid töötles 6,67% vastajatest. Perekondlike andmeid töötles 10% vastajatest ja 8,33% vastajatest töötlesid muid andmeid. Vastajatest 6,67% ei töödelnud üldse mingeid andmeid.

Küsimuses, kus paluti nimetada ja selgitada üldmäärusega kaasnevaid muudatusi (kokku viis tükki), ei osanud ükski vastaja nimetada kõiki viite muudatust ega neid selgitada. Õigeks vastuseks oli vaja nimetada: õigus olla unustatud, õigus oma nõusolek tagasi võtta, igalt inimeselt on vaja küsida nõusolekut enne informatsiooni töötlemist, inimestel on õigus paluda parandada informatsiooni enda kohta, samuti inimene ise valib kellele ta lubab oma isiklikud andmeid töödelda ja kellele mitte, andmete jurdepääsu omavad ainult vastutav ja volitatud töötajad, tööturul ilmub uus ametikoht - andmekaitse spetsialist. Kõige rohkem nimetati „õigus olla unustatud“ muudatust (esines 40 korral), ent levinumaks vastuseks oli „ei tea“.

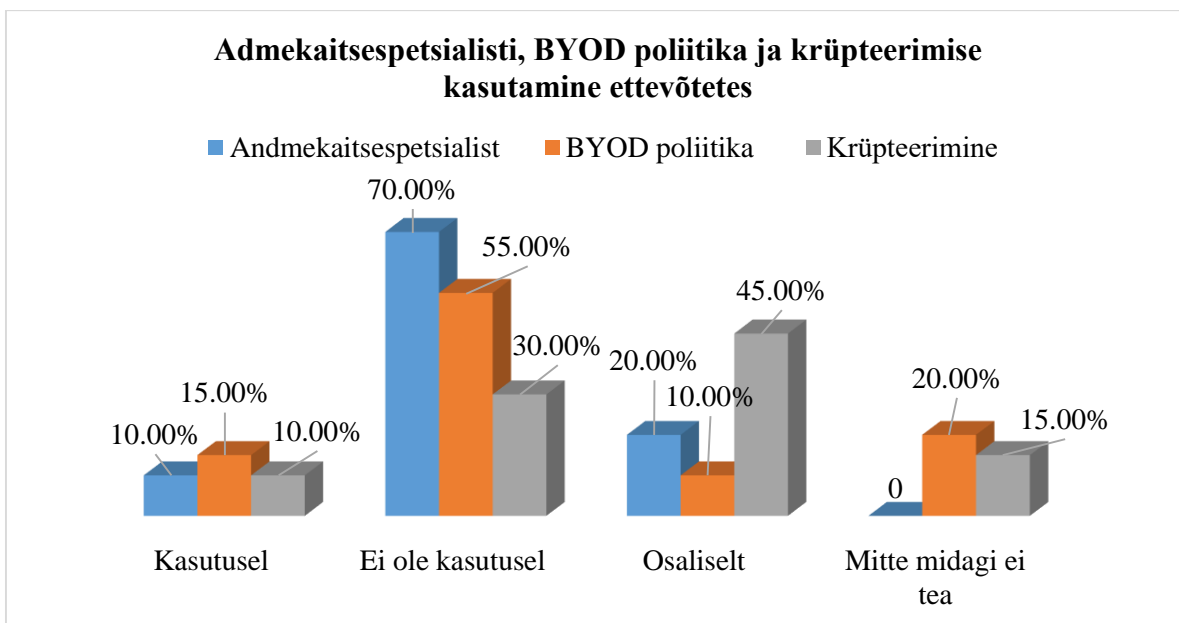
Tabel 1. Kust raamatupidajad said teada üldmääruse muudatustest?

	Mikro	Väike	Keskmine	Suur	Kokku osakaal
Ise käin koolitusele	1	1	4	0	10.00%
Töö pakub erinevaid koolitusi	1	4	4	8	28.34%
Ise uurisin ja lugessin internetis	11	9	5	2	45.00%
Töökaaslased jutustasid	3	1	2	0	10.00%
Mitte midagi ei tea	4	0	0	0	6.66%
Kokku ettevõtete osakaal	33%	25%	25%	17%	100%

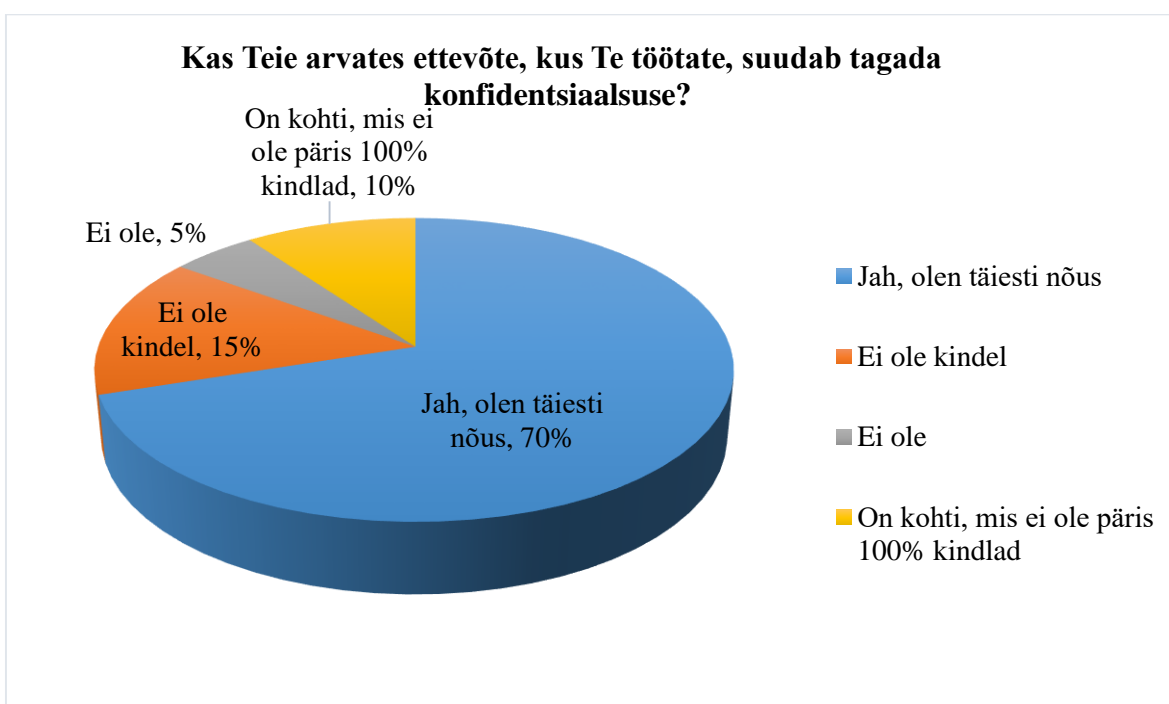
Umbes pool vastajatest (45%) viis end üldmääruse muudatustega interneti abil ise kurssi. Töökoht pakkus koolitusi 28.34 protsendile vastajatest, 10% vastajatest käis end ise koolitamas, 10% teadis üldmäärusest tänu nende töökaaslastele, 6.6% ei teadnud muudatustest midagi. Vastusest selgus, et mikro- ja väikeettevõtetes on kõige suurem osakaal ise uurimisel ja internetist lugemisel. Suurtes ettevõtetes on suurim koolituste osakaal. Mikroettevõtetes on töökaaslastelt kuulnud info ja teadmatus osakaal suurim.

Delikaatsete andmete loetlemise küsimusest selgus, et vastajad on teemaga kursis. Kõige sagedamini esinev vastus delikaatsete andmete kohta oli: nimi, isikukood, allkiri, vanus, sugu, religioon, poliitilised eelistused, seksuaalsed eelistused, perekonnaseis, lapsed, aadress ja elukoht, telefoninumber. Üks vastus oli täiesti üldmäärusest kopeeritud ja see ei läinud arvesse.

Jooniselt 6 on näha, et BYOD poliitikat kasutatakse Eesti ettevõtetes vähe – 15% vastajate ettevõtte kasutab seda igapäevatoos, 10% kasutab osaliselt. BYOD poliitika ei ole kasutusel 55% ettevõtetes. 20% vastajatest ei ole antud teemaga kursis. Krüpteerimist kasutab täies ulatuses 10% vastajatest ja osaliselt 45% vastajatest. Krüpteerimist ei kasuta 30% vastajatest 15% vastajatest krüpteerimistest mitte midagi ei tea. Andmekaitse spetsialist on olemas 10% ettevõttes ning 70% ettevõttes ei ole olemas andmekaitse spetsialisti. 20% vastajatest vastasid, et nende ettevõttes andmekaitse spetsialisti kasutatakse osaliselt, see tähendab, et ettevõtte ostavad eraldi vajalikud teenused.



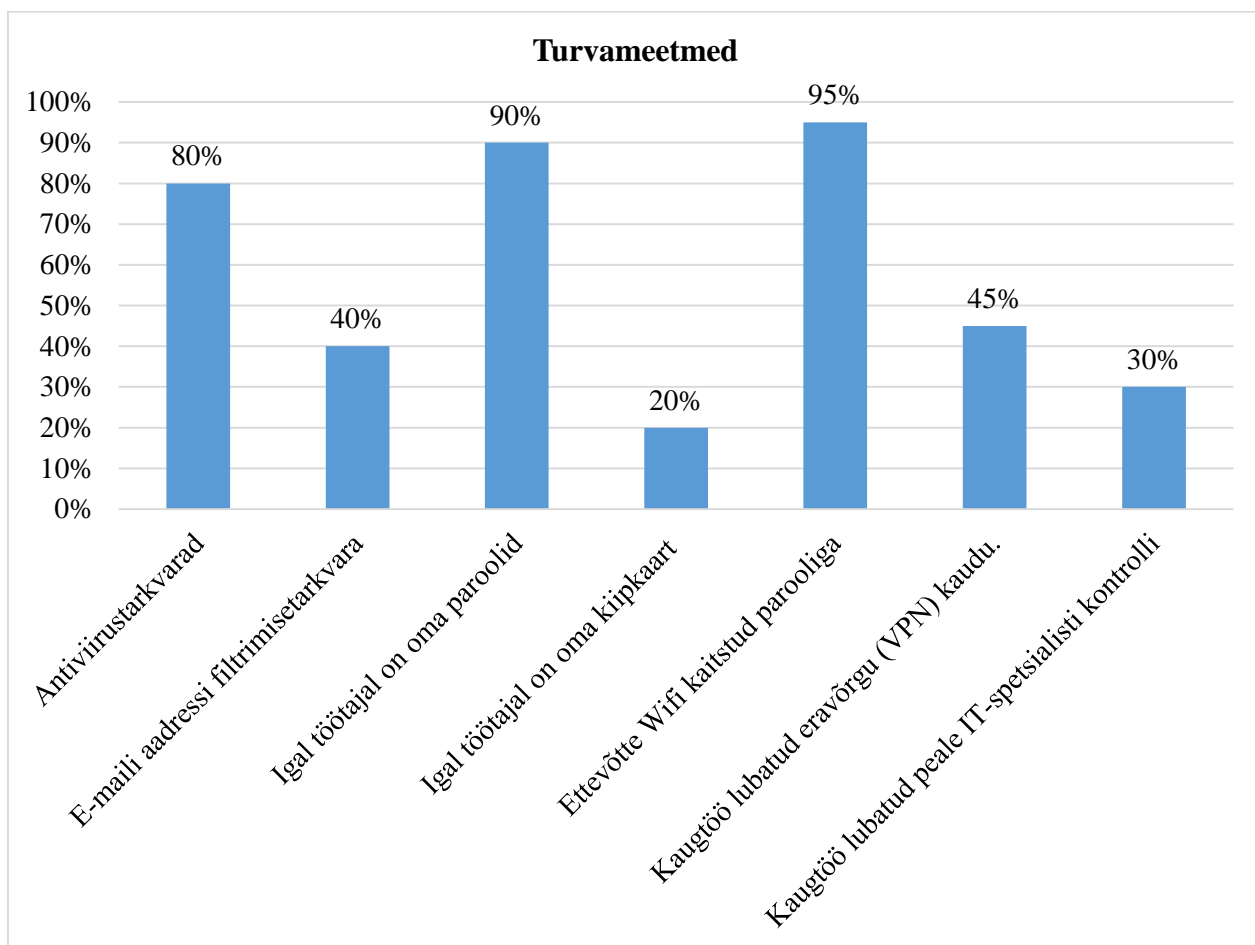
Joonis 6. Admekaitespetsialisti, BYOD poliitika ja krüpteerimise kasutamine ettevõtetes
Allikas: küsitlusuuring, autori arvutused



Joonis 7. Kas Teie arvates ettevõtte, kus Te töötate, suudab tagada konfidentsiaalsuse?
Allikas: küsitlusuuring, autori arvutused

Jooniselt 7 on näha, et 71% vastajatelt on täiesti nõus sellega, et nende ettevõtte suudab tagada konfidentsiaalsuse. 21% vastajatest ei ole kindlad, 4% ei ole päris kindlad ja 4% ei ole üldse nõus sellega, et ettevõtte suudab tagada konfidentsiaalsuse. Väite juures „Peale üldmääruse jõustamist

tuleb isikuandmeid töödelda“ oli vaja nimetada põhiväärtusi ja sellele küsimustele vastasid õigesti pooled.



Joonis 8. Tehnilised turvameetmed

Allikas: küsitlusuuring, autori arvutused

Joonisel 8 on välja toodud tehnilised turvameetmed, mida rakendatakse tagamaks andmeturvet. Kõige levinumad andmekaitsemeetodid on ettevõtte Wifi parooliga kaitsmine, mida tehti 95% ettevõttes, personaalsete paroolide ja kasutajatunnuste omamine, mida esines 90% ettevõttes, ning anti-viirustarkvara omamine, mis esines 80% ettevõttes. 40% ettevõttes on seadistatud e-posti filtreerimistarkvara, 20% omab töökohta kiipkaarti, 45% vastajatele on võimaldatud kaugtöö tegemine virtuaalse eravõrgu (VPN) kaudu ning 30% on võimalik teha kaugtööd oma arvutis sel juhul, kui arvuti on eelnevalt kontrollitud töökohta määratud IT-spetsialisti poolt.

3.3. Intervjuu uuringu tulemused

Ettevõtete valimisel lähtuti sellest, et need oleksid võimalikult erineva tegevusala ja suurusega, võrdlemaks erinevate valdkondade raamatupidajate taset ning saamaks võimalikult erinevaid näiteid nende igapäevatööst. Esimene vastaja töötab meditsiiniteenuste ettevõttes, teine vastaja õigusabi büroos, kolmas erimasinate tootmisettevõttes, neljas mere-lastiveo organiseerimisettevõttes, viies suurtööstuses ning kuues suuremahulises logistika- ja laondusettevõttes.

Raamatupidajate teadmiste taseme võrdlemiseks ja hindamiseks koostas autor tabeli (vt lisa 8) ja selle põhjal ka väikse kokkuvõtava tabeli, kus on selgelt näha teadmiste erinevused. Kokku oli intervjuus üldmäärust puudutavaid küsimusi 20, iga õige vastus andis ühe punkti, osaline vastus andis pool punkti, vale vastus või mittevastamine andis null punkti.

Tabel 3. Raamatupidajate teadmise tase

Vastajad:	Punktid:
Vastaja 1 väikeettevõtte	9.5
Vastaja 2 väikeettevõtte	15.5
Vastaja 3 keskmine ettevõtte	15.5
Vastaja 4 keskmine ettevõtte	19
Vastaja 5 suurettevõtte	15
Vastaja 6 suurettevõtte	17

Allikas: Autori arvutused

Vastaja 1 on uurinud ja lugenud üldmääruse muudatuste kohta iseseisvalt. Vastaja ei osanud õigesti vastata küsimustele „Kui kaua on vaja säilitada töölepingut pärast inimese töölt lahkumist?“. Vastaja 1 ei ole muutunud oma töös midagi peale üldmääruse jõustumist, samas ei rakenda ta üldmääruse nõudeid. Vastaja 1 töötleb ettevõtte töötajate andmeid ning ka patsiendiandmeid. Ettevõttes on lubatud teha tööd oma isiklikus arvutis ja IT-spetsialist ei ole seda arvitit kontrollinud, mistõttu ettevõtte andmeturbetase on madal. Vastaja ei osanud täpsemalt seletada, kuidas üldmääruse nõuded on kahe aasta jooksul muutunud, ega osanud õigesti nimetada üldmääruse rikkumise trahvisummat. Delikaatsete isikuandmete küsimuste puhul tõi vastaja välja ainult kaks tüüpi kaheksast: terviseandmed ning andmed seksuaalelu kohta. Kuid ettevõttes on kasutusel krüpteerimine ja vastaja 1 seletas, et nad kasutavad seda, varjamaks inimeste nimesid ja

isikukood (isiklikud andmed), kui edastavad vereanalüüse SYNLAB Eesti OÜ-le. See oli väga hea näide oma igapäevatööst, mis samas kinnitas, et raamatupidajad puutuvad oma töös kokku erinevate isiklike andmetega, tahtmata olla vastutavad või volitatud töötajad. Vastaja 1 ei järginud kõiki üldmääruse nõudeid oma igapäevatöös ning tema teadmiste tase üldmäärusest ei ole piisav.

Vastaja 2 on osalenud tööandja poolt korraldatud koolitusel. Vastaja 2 on kindel, et üldmääruse jõustumine ei ole toonud mingisuguseid muutusi tema töösse, kuigi ta allkirjastab iga uue kliendiga avalduse andmete mitteavaldamisest. Seega vastaja 2 tegeleb üldmääruse nõuetega oma igapäevatöös. Delikaatsete andmete küsimuse juures nimetas vastaja 2 üksteist tüüpi, täpsemalt: nimi, sugu, isiklik ja töökontakti informatsioon, ametikoht, sünnipäev, sünnikoht, rahvus, passi andmeid, ID-kaardi ja viisa andmeid. Seega see oli kõige parem vastus võrreldes teistega. Ta vastas õigesti ka töölepingu säilitamise küsimusele ning andis lisainformatsiooni antud küsimuse kohta. Samuti teadis ta õiget trahvisumma suurust. Vastaja kasutab teadmisi üldmäärusest igapäevatöös ning ta teadmiste tase vastab nõuetele.

Vastaja 3 oli ise hankinud informatsiooni internetist ja küsinud kolleegidelt üldmääruse muudatuste kohta. Vastaja 3 oli märganud, et üldmäärus annab inimestele suurema kontrolli oma andmete üle ja tugevdab õigust eraelu puutumatusel internetis. Ta tõi välja kõik üldmääruse muudatused. Antud töötaja tegeleb töötajate autode registreerimisnumbritega, selleks et anda töötajatele parkimisvõimalus. Delikaatsete andmete küsimusele ning töölepingu säilitamise küsimusele vastas ta õigesti, kuid küsimusele, mis puudutab üldmääruse rikkumise tagajärgi, vastas „trahvisummad varieeruvad kuni 20 miljoni euroni või 4 protsendini ettevõtte käibest“, mis on liiga üldine vastus. Vastaja 3 kasutab teadmisi üldmäärusest igapäevatöös ning ta teadmiste tase vastab nõuetele.

Vastaja 4 vastused on saadud kahelt raamatupidajalt – kuna mõlemad töötavad koos ja teevad ühte ja sama tööd, siis nad leidsid, et nad peaksid ka küsimustele vastama koos. Vastaja 4 käis tööandja poolt korraldatud koolitusel ning viis end lisaks kurssi tööandja poolt saadetud kasuliku infoga üldmääruse muudatuste kohta. Võrreldes teiste vastajatega olid nende vastused kõige korrektsemad. Vastaja 4 tõi välja kõik üldmääruse muudatused, nemad tõi ainsana välja oma näite üldmääruse muudatustest töökorralduses kahe viimase aasta jooksul. Delikaatsete andmete ning töölepingu säilitamise küsimustele vastati õigesti. Vastaja 4 kasutab teadmisi üldmäärusest igapäevatöös ning ta teadmiste tase vastab nõuetele.

Vastaja 5 sai teada üldmääruse kohta infot meediast ja tööandjalt, temale jagati eraldi infot määruse kohta ning viidi läbi koolitus. Vastajal 5 olid head teadmised üldmääruse muutuste ja delikaatsete isikuandmete kohta, ent trahvi küsimusele ta vastata ei osanud. Vastaja 5 tõi hea näite, miks üldmääruse muudatused on inimestele kasulikud: „Mulle küll meeldib, et saan telefoni teel müüjatele öelda, et nad mu andmed kustutaks ja enam ei helistaks.“ Ettevõttes, kus vastaja 5 töötab, „tehti programmid ümber, näiteks Outlook ja Skype, automaatselt kustutatakse vestluseid mingi aja tagant, varem säilisid vestlused pikemalt ja pidi ise kustutama“. Ettevõttes, kus vastaja 5 töötab, kasutatakse isikliku meilivahetuse krüpteerimist, seega nad tagavad oma meilide korraliku kaitse. Vastaja 5 kasutab teadmisi üldmäärusest igapäevatoos ning ta teadmiste tase vastab nõuetele.

Vastaja 6 sai teada üldmääruse muudatustes tänu koolitusele ning on lugenud artikleid andmekaitse inspeksiooni veebileheküljel. Vastaja 6 koosnes samuti kahest töötajast, need olid raamatupidaja ja krediidiuht. Vastaja 6 oli kindel, et kõik raamatupidajad on võimelised rakendama kõiki üldmääruse nõudeid oma igapäevatoos. Samas vastaja andis head ja õiged vastused peaaegu kõikidele küsimustele. Küsimustele, kus oli vaja nimetada täpne trahvisumma, vastati liiga üldiselt, mitte nimetades täpset trahvisummat, seega sai ta pool punkti selle küsimuste eest. Ettevõttes on väga kõrge sisekultuur ja olemas sisereeglid, kus pandud kirja kõik üldmäärusega seotud protseduurid. Kuid ettevõttes on kasutusel tavalised turvameetmed ja ei kasutata andmete krüpteerimist, seega ettevõtte ei kaitse piisavalt oma andmeid. Vastaja 6 teab üldmääruse muudatustest ja on võimeline rakendama nõudeid oma igapäevatoos.

Läbiviidud uurimuse tulemuste põhjal on võimalik teha järeldus, et suure ja keskmise suurusega ettevõtete raamatupidajatel on kõrgem teadmiste tase. Kõige paremad teadmised üldkaitsemääruse nõuetest olid vastajal 4, kes sai peaaegu maksimaalse punktide arvu (19 punkti). Vastustest ilmselg, et raamatupidajad, kes käisid koolitustel, olid paremini kursis üldmäärusega ning sellega kaasnevate muudatustega, võrreldes nendega, kes lugesid selle kohta ise või kuulsid infot kolleegidelt. Kõigis ettevõtetes on raamatupidamise tarkvara ja arvutid kaitstud parooliga. Laua tagant lahkudes kasutavad turvalisuse tagamiseks paroole 4 vastajat, isikut tõendavat kaarti 1 vastaja, 1 vastaja lukustab kabineti ukse. Kõigis ettevõtetes on töötajatel oma e-posti aadressid töökoha domeeniga.

3.4. Arutelu, järeldused ja ettepanekud

Lõputöös on uuritud isikuandmete kaitse üldmääruse muutuste mõju ja antud hinnang Eesti ettevõtete raamatupidajate teadmiste taseme kohta ning selle kohta, kuidas kasutatakse teadmisi igapäevatoös. Esimesest ja teisest peatükist järeldub, et raamatupidajad on ettevõtetes enamasti peamised andmete töötledjad. Nad puutuvad iga päev kokku suure hulga teiste inimeste ja ettevõtete isiklike andmetega. See tähendab, et raamatupidajad peavad oma töös täitma kõiki üldmääruse nõudeid, mis on välja toodud esimeses ja teises peatükis, ning samas peavad teadma kõiki turvameetmeid ja rakendama neid igapäevatoös.

Tänu interneti- ja intervjuu-uuringutele on võimalik teha järeldus, et suured ettevõtted panustavad rohkem sellesse, et tagada oma töötaja õigeaegne koolitus. Suurte ja keskmise suurusega ettevõtete raamatupidajad on rohkem teadlikud üldmääruse muudatustest ja nendel on rohkem võimalusi rakendada üldmääruse nõudeid oma igapäevatoös. Raamatupidajad vanusegruppis 51-60 teavad üldmäärusest rohkem kui nooremad. Peaaegu kõikides ettevõtetes on kasutusel tavalised turvameetmed: viirusetõrjetarkvarad, erinevad paroolid ja kaitstud parooliga Wifi. Vastustest on võimalik järeldada, et Eesti firmades ei ole BYOD poliitika väga levinud. See on positiivne tulemus, sest kui ettevõtted lubavad kasutada oma isiklike arvuteid, peavad nad ka tagama ranged kaitsemeetmed. Kui võrrelda vastuseid küsitlusele, mis viidi läbi 2016. aastal („Kui palju te teadsite enne käesoleva ankeedi täitmist kevadel jõustuvast andmekaitse reformist?“), kus ainult üks seitsmendik oli üldmäärusest kuulnud, siis tänapäeval kõik teavad üldmäärusest, kuid mitte kõik pole sellesse süvenenud.

Intervjuu vastustest on võimalik teha järeldus, et kõik vastanud raamatupidajad olid kursis üldmääruse jõustamisega, kui mitte kõik polnud võimelised rakendama kõiki nõudeid oma igapäevatoös.

Kõik raamatuidajad, keda intervjueriti, olid võimelised vastama küsimustele üldmääruse kohta ja peaaegu kõik oskasid nimetada peamiseid muudatusi. Mitte keegi ei osanud vastata kõikidele 20 küsimusele üldmäärusest, kuid vastaja 4 vastas 19 küsimusele, see on positiivne tulemus. Teistel vastajatel olid nõrgemad tulemused. Kõik vastajad oskasid vastata peaaegu pooltele küsimustele ja tuua näiteid isiklikust tööst. Seega intervjuude põhjal on võimalik järeldada, et Eesti ettevõtete raamatupidajad on kursis üldmääruse muudatustega, enamik rakendab üldmääruse nõudeid oma

igapäevatöös ja raamatupidajatel on keskmine teadmiste tase. Need intervjuu-uuringu tulemused olid positiivsed.

Peamine asi ettevõtete ja raamatupidajate jaoks on piiratud ligipääs ettevõtte, kliendi ja töötajate andmebaasile. Turvameetmed valib iga ettevõtte ise, mõned kasutavad siiani arhiiviruume, mis pannakse lukku, mõned kasutavad ainult interneti andmebaase. Igal töötajal, kes omab ligipääsu andmetele, oleks vaja oma identsefitseerimisvahendit. Kui inimene logib sisse raamatupidamise tarkvarasse või vaatab midagi arhiivist, peab see isik olema tuvastatud, seega ettevõtte peab tagama suure kontrolli oma andmete üle.

Väga oluline on tagada töötajate koolitamine ja arendada ettevõtte sisereegleid. Kõikides ettevõtetes peab olema arenenud sisekultuur ja sisereeglid, kus on kirjas kõik isikuandmetega seotud nõuded. Kui ettevõtte lubab oma töötajal teha tööd oma arvutis, siis enne seda peab IT-spetsialist kontrollima arvutit ning seadistama programme, mis ennetavad informatsiooni kadumist ja tahtmatut avaldamist. Samas on väga oluline, et arvuti tehakse täiesti puhtaks ja kasutatakse ainult töö jaoks. Veel on vaja kõik andmed kopeerida ja salvestada teave kõvakettale või pilve, et kui arvutiga midagi juhtub, oleks andmed salvestatud teisel kujul. Ettevõtted peavad ka kogu aeg arendama oma turvameetmeid ja kaardistama rikked. Iga päevaga turvameetmed vananevad ja nende asemele tulevad uued.

KOKKUVÕTE

Lõputöö eesmärk oli välja selgitada Euroopa Parlamendi ja nõukogu isikuandmete kaitse üldmääruse muutuste mõju ja anda hinnang, millisel määral Eesti ettevõtete raamatupidajad on kursis kõikide isikuandmete kaitse nõuetega. Esimeses ja teises peatükis on antud täpne ülevaade kõikidest üldmääruse muudatustest ja üldmääruse kasutamisest raamatupidaja igapäevatoos. Peamiseks uurimisprobleemiks olid raamatupidajate teadmised üldmääruse jõustumisest ja võimekus kasutada üldmääruse nõudeid igapäevatoos.

Lõputöö uurimisprobleemide lahendamiseks oli kasutusel kvantitatiivne ja kvalitatiivne uurimismeetod. Esimeses etapis tegi autor internetiküsitluse ja teises etapis intervjuu-uuringu. Internetiküsitlusest võttis osa 60 raamatupidajat erineva suurusega ettevõtetest ja intervjuu-uuringust võttis osa kuus raamatupidajat. Intervjuu-uuring tõestas, et Eesti ettevõtete raamatupidajad on kursis üldmääruse muudatustega, kuid mitte kõik raamatupidajad pole võimelised neid rakendama oma igapäevatoos. Suur- ja keskettevõtete raamatupidajad oskavad paremini oma teadmisi rakendada ja nende teadmiste tase on kõrgem kui mikro- ja väikeettevõtete raamatupidajatel. Suurtes ettevõtetes pakutakse koolitusi, mistõttu töötajad on ilmselt rohkem kursis muudatustega, kui seda on keskmise suurusega ja väikeettevõtete töötajad, kes on pidanud end ise asjaga kurssi viima. Samas peaaegu kõik raamatupidajad teavad, mis on delikaatsed isikuandmed ning millal on õige küsida inimese nõusolekut andmete töötlemiseks. Kuid küsimusele, missugused karistused kaasnevad üldmääruse rikkumisega ja milliseid muudatused tõi kaasa üldmääruse jõustamine, polnud võimelised kõik vastama. Internetiküsitluse põhjal sai teha järelduse, et raamatupidajate teadmiste taset on vaja tõsta ja raamatupidajad peavad ise rohkem panustama sellesse, et arendada ennast. Samuti tõestas interneti-uuring, et ettevõtetes kasutatakse vähe turvameetmeid, nagu krüpteerimist, enamikul ettevõtetel ei ole võimalik jälgida töötajate aktiivsust raamatupidamisprogrammides ning ka andmekaitse spetsialisti ametikoht ei ole Eestis levinud.

Lõputöös püstitatud eesmärk said täidetud, uuringu käigus selgus, et raamatupidajate teadlikkust andmekaitsest ja üldmäärusest tuleb tõsta. Eesti ettevõtete raamatupidajate teadmiste tase üldmäärusest ja selle kasutamisest on ebapiisav. Ettevõtted (sõltumatu suuruselt) peavad tagama andmete hea kaitse läbi sisereeglite ja oma töötajate koolitamise. Raamatupidajad peavad ka ise koolitustel käima või püüdma ennast ise arendada. Näiteks maksu- ja tolliamet pakub tihti tasuta koolitusi raamatupidajatele. Ettevõtted peavad ka kaardistama riskid seoses informatsiooni tahtmatu avaldamise, kustutamise ja kaotamisega ning rakendama ja kogu aeg uuendama turvameetmeid. Isiklikud andmed iga inimeste kohta on konfidentsiaalne informatsioon ja mitte keegi ei soovi selle informatsiooni avaldamist. Seega peavad ettevõtted rohkem panustama sellesse, et oleks võimalik kõiki isikuandmetega seotud nõudeid rakendada.

Töö autoril on raamatupidajate teadmiste taseme parandamiseks ja ettevõtte turvalisuse tõstmiseks kaks soovitus. Raamatupidajatel ja ettevõtetel on vaja tõsta teadmiste taset koolituste kaudu ning ka üldmäärust ise uurides. Eraldi tähelepanu tuleks pöörata sellele, kuidas ettevõtetes isikuandmeid kogutakse, salvestatakse ja töödeldakse. Et vältida soovimatuid olukordi, on vaja ettevõtte sissereeglites lahti kirjutada kõik punktid, mida ettevõtte on võtnud kasutusele andmete kaitseks; kuidas klientide andmeid töödeldakse ning mille eesmärgi jaoks. Kõik need tavalised asjad saavad lihtsustada ettevõtte ning ka raamatupidajate tööd. Ettevõtted peavad kogu aeg arendama oma turvaameetmeid ja kaardistama riske, mis seotud interneti kasvu ja häkkimisega.

SUMMARY

REQUIREMENTS OF GENERAL DATA PROTECTION REGULATION FOR ACCOUNTANTS

Anna Bogdanskaja

The goal of the diploma thesis was to find out the impact of the changes adopted by the European Parliament in General data protection regulation and to assess how well the accountants of Estonian companies are aware of all the requirements for the protection of personal data.

The first and second chapters give a detailed overview of all changes in the general regulations and use of General data protection regulation in accountant's daily work. The main problem of the study was not awareness of new requirements for the general requirements and the inability to use in their daily work. 2 Types of researches were used during the work: quantitative and qualitative. At the first stage, the author conducted an online survey, and at the second - an interview. Sixty accountants from various companies took part in the online survey and six accountants took part in the interview. A research conducted during the survey showed that accountants from Estonian companies are familiar with the amendments to the general rule, but not all accountants can apply them in their daily work. Accountants of large and medium-sized companies have more opportunities for applying their knowledge, and their level of knowledge is higher than of small business accountants. The training is conducted in large companies, so employees are probably more informed about changes than employees of small and medium businesses, who had to introduce themselves in the course of business and learn on their own. At the same time, almost all accountants know what confidential personal information is and when it is appropriate to ask for consent to data processing. However, the question of what penalties are connected with the violation of the general regulations and what changes in the execution of the general regulations cannot be carried out. Based on an online survey, it was concluded that the level of knowledge of accountants should be improved and that accountants themselves should invest more in the development of themselves. In addition, an online survey showed that companies use few security

measures, such as encryption, but most companies cannot track employee activity in accounting programs, and the position of a data protection officer for data protection is not common in Estonia.

The goal set in the final thesis was achieved, the survey showed that it is necessary to increase the awareness of accountants about data protection and general regulation. The knowledge of Estonian accountants in general regulations and its use is insufficient. Companies (regardless of size) should ensure good data protection through internal rules and training of their employees. Accountants must also attend trainings themselves or try to develop independently. The tax and customs agency often also offers free courses to accountants. Companies must also determine the risks associated with unintended disclosure, deletion and loss of information, as well as constantly implement and update security measures. Personal information about each person is confidential and no one wants to disclose this information. Therefore, companies need to invest more in order to be able to fulfil all the requirements for personal data.

The author has two recommendations for improving the level of knowledge of accountants and security in the enterprise. Accountants and enterprises should increase their level of knowledge through training, as well as by studying the most general regulations. Particular attention should be paid to how all personal data is collected, stored and processed in companies. To avoid undesirable situations, it is necessary to write down all the points in the company's rules that were used by the company, how the customer data is processed and for what purpose. All these common things can simplify the work of the company, as well as the work of accountants. It is also necessary to pay attention to developing technologies and monitor the risks associated with the loss of information. Firms should use stacked passwords and systems to identify workers, which is used to track activity.

VIIDETUD ALLIKATE LOETELU

- Addena Koolitus ja Konsultatsioonid. (2017). Andmekaitse mõju raamatupidajale. Veebipõhine koolitus. Kättesaadav: <https://seminarid.addenda.ee/courses/enrolled/327153> 16 oktoober 2018.
- American Accounting Association. (2011). A Survey of Consumer Information Privacy from the Accounting Information Systems Perspective. Kättesaadav: <http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=4&sid=85a8a6cf-1fa1-4302-a52e-2e35b181fc64%40sessionmgr4008> 22. oktoober 2018.
- Andmekaitse inspeksioon. (2016). IP-aadress ja privaatsus. Kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ip_ja_privaatsus.pdf 28. oktoober 2018.
- Andmekaitse inspeksioon. (2018). Rikkumisteate edastamine. Kättesaadav: <http://www.aki.ee/et/poordu-inspektsiooni-poole/rikkumisteate-edastamine> 22.oktoober 2018.
- Andmekaitse inspeksioon. (2018). Mis on isikuandmed? Kättesaadav: <http://www.aki.ee/et/mis-isikuandmed> 30. september 2018.
- Andmekaitse Inspeksioon. (2018). Isikuandmete töötaja üldjuhend. Kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/2018.05.31_andmetootleja_uldjuhend.pdf 25. oktoober 2018.
- Andmekaitse Inspeksioon. (2017). Isikuandmete kaitse uue õigusliku raamistiku kontseptsioon. Kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/andmekaitse_kontsepsioon_11.04.2017.pdf 16. oktoober 2018.
- Andmekaitse Inspeksioon. (2018). Isikuandmete kaitse seaduse eelnõu. Kättesaadav: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/iks_sk_21.03.18.pdf 22. oktoober 2018.
- Diskursusanalüüs jt intervjuu analüüsi meetodid. (2016). Kättesaadav: http://www.tlu.ee/~sirvir/Intervjuu_vaatlus_ja_sisuanals/diskursusanals_jt_intervjuu_ansi_meetodid.html 04. november 2018.
- Elektroonilise side seadus. RT I, 22.05.2018, 3. Kättesaadav: <https://www.riigiteataja.ee/akt/122052018003> 16. oktoober 2018.

- Emory International Law Review. (2018). E ETERNAL SUNSHINE: THE RIGHT TO BE FORGOTTEN IN THE EUROPEAN UNION AFTER THE 2016 GENERAL DATA PROTECTION REGULATION. Kättesaadav: <http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=7&sid=02615981-a1bf-4c1a-85c3-210c92f28963%40sessionmgr120> 11. oktoober 2018.
- Euroopa Liidu Teataja. (2018). Teave ja teatised. Kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=OJ:C:2018:397:FULL&from=ET> 04. november 2018.
- Euroopa Liidu Teataja. (2016). Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679. Kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016R0679&from=et> 20. september 2018.
- Euroopa Liidu Toimimise Lepingu Konsolideeritud Versioon. (2012). Kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:12012E/TXT&from=Et> 22. september 2018.
- European Data Protection Supervisor. (2009). Euroopa Andmekaitseinspektor ja isikuandmete ühenduse institutsioonides ja asututes. Kättesaadav: file:///C:/Users/annab/Downloads/Eur_andmekaitseinspektor.pdf 23. oktoober 2018.
- European Commission. (2014). Progress on EU data protection reform now irreversible following European Parliament vote. Kättesaadav: http://europa.eu/rapid/press-release_MEMO-14-186_et.htm 16. oktoober 2018.
- ICEW Business Law/IT Faculty. (2018). GDPR For Accountants: Your questions answered. Kättesaadav: <https://www.icaew.com/-/media/corporate/files/technical/information-technology/cyber-resource-centre/faqs-what-does-gdpr-mean-for-accountants.ashx> 09. oktoober 2018.
- Isikuandmete kaitse seadus. RT I, 06.01.2016, 10. Kättesaadav: <https://www.riigiteataja.ee/akt/130122010011?leiaKehitiv> 16. oktoober 2018.
- Kukk, U. Isikuandmete kaitse ja E-Riik. Kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmete%20kaitse%20ja%20E-Riik%20-%20%20U.Kukk%20k%C3%B5ne.pdf 30. september 2018.
- Küberturvalisuse seaduse eelnõu seletuskiri. (2017). Kättesaadav: https://www.koda.ee/sites/default/files/content-type/content/2017-10/seletuskiri_k%C3%BCberturvalisuse%20seadus.pdf 18. oktoober 2018.
- Küberturvalisuse seadus. RT I, 22.05.2018, 1. Kättesaadav: <https://www.riigiteataja.ee/akt/122052018001> 16. oktoober 2018.
- Männiko, M. (2011). Õigus privaatsusele ja andmekaitse. Tallinn: Tallinna Raamatutrükikoda.
- Marx, G. A. (2007). Privacy. Blackwell Encyclopedia of Sociology. Blackwell Publishing.

- OECD. (2013). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Kättesaadav: <http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm#part1> 30. september 2018.
- The History of the General Data Protection Regulation. (2018). Timeline. Kättesaadav: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en 16. oktoober 2018.
- Viljar, P. (2017). Andmekaitse inspeksioon. Kas isikuandmete kaitse üldmäärus toob tõesti kaasa hiigeltrahvid? Kättesaadav: <http://www.aki.ee/et/uudised/uudiste-arhiiv/kas-isikuandmete-kaitse-uldmaarus-toob-toesti-kaasa-hiigeltrahvid> 14. oktoober 2018.

LISAD

Lisa 1. Intervjuu küsimuste transkriptsioon: vastaja 1 (väikeettevõtte)

- 1. Kas Te olete valmis andma oma nõusoleku, et see intervjuu salvestatakse ja pärast kasutatakse lõputöö koostamiseks?**

Jah, olen täiesti nõus.

- 2. Kas soovite jääda anonüümseks vastajaks või on lubatud ettevõtte nimi avalikustada?**

Anonüümseks.

- 3. Teie ettevõtte suurus (kui palju töötajaid, väikeettevõtte 10-49, keskmine 50-249, suurettevõtte 250)?**

Väikeettevõtte, meil töötab 25 inimest.

- 4. Teie haridustase?**

Kõrgtase, õppisin TTÜ-s.

- 5. Teie ametikoht?**

Raamatupidaja, kuid mina olen üksinda siin töötanud.

- 6. Kust Te saite teada isikuandmete kaitse üldmääruse muudatustest?**

Meedia, ajakirjandus, töö juures räägiti, kõik kolleegid teistest tööst ka rääkisid sellest, paljud ettevõtted pakkusid erinevaid koolitusi.

- 7. Mis mõju tõid kaasa üldmääruse muutused?**

Minu töös veel mitte midagi erilist.

- 8. Kas üldmääruse muutused saaksid lihtustada ettevõtte tööd?**

Ei saa.

- 9. Kas raamatupidajad saavad täita kõik isikuandmetega seotud nõuded?**

Suuremas osas saavad.

- 10. Kuidas isikuandmete kaitse nõuded on kahe aasta jooksul muutnud?**

Arvestades seadust, siis kindlasti. Seaduse kehtivuse ajal – ei oska öelda.

- 11. Millised andmed on Teie arvates delikaatsed isikuandmed?**

Terviseandmed, andmed seksuaalelu kohta.

Lisa 1. järg

12. Mis isikuandmed on vajalikud raamatupidajatele, et teha igapäevatööd?

Töötajate isikukoodid, töövõimetuse aste, lapseandmed, palgaandmed, kasutan töötajate isiklikud meilid igapäevatoos. Samuti ettevõtte küljelt pangaandmed, tarnijate andmed. Kuna töötan meditsiini osutavas ettevõttes, siis kliendiandmeid, nendele tehtud operatsioonid ja proteduurid töötlen arvete koostamisel.

13. Millal on vaja küsida inimeste nõusolekut nende andmete töötlemiseks?

Töölepingu sõlmimisel.

14. Kas Te olete küsinud oma töötajate nõusolekut andmete kasutamiseks?

Ei, ei ole küsinud, mina ei ole sõlminud töötajate lepingud ka, sellega tegutseb tegevjuht.

15. Kas Te olete teavitanud oma kliente sellest, kuidas Te olete nende andmeid töödeldud ja mis eesmärgi jaoks?

Ei ole teavitanud.

16. Kas Te teate, kui kaua on vaja säilitada töölepingut pärast inimese töölt lahkumist?

Täpselt ei tea, varem oli vajalik 7–5 aastat säilitada.

17. Kas Teie tööarvuti ja raamatupidamise programm on kaitstud parooliga?

Jah.

18. Kas Teie majandusarvestuse programmis on nähtav, kes ja milliseid andmeid vaatas ja kasutas?

Ei ole nähtav, eelmisel töökohal oli kõik tegevused jälgitus, praegu mitte.

19. Kui Te lähete kohvi jooma, Te panete oma arvuti lukku?

Jah, jah, jah.

20. Kas keegi klientidest või töötajatest on palunud Teid kustutada informatsiooni nende kohta? Mis Te teate väljendist „õigus olla unustatud“?

Ei ole, kuid need olukorrad täiesti võivad juhtuda.

Näiteks kui inimene ei tahaks, et keegi teistest arstidest vaatab, et talle on teinud mingi operatsioon. Rohkem ei tea mitte midagi.

21. Kuidas Teie arvate, kas tööandjal on õigus küsida töötajatelt nende laste arvu ja laste vanust?

On õigus. Aga ei küsinud veel kellegil, keegi ei ole ju võtnud lapsepäevi endale.

22. Kas Teie ettevõttes kasutatakse andmete krüpteerimist?

Jah, läbi SynLan ettevõtte. Krüpteeritatakse patsiendi nimed vereanalüüsi üleandmisel.

Lisa 1. järg

23. Kas Teie ettevõttes on e-mailid turvalised, domeeniga?

Jah, igal töötajal on tehtud töö e-maili aadress.

24. Kas Teie ettevõttes on rakendatud poliitikat, et töötajad saavad teha tööd oma isiklikus arvutis?

Jah, mul ise oma arvuti võtnud tööle kaasa ja mina saan kodus tööd ka teha.

25. Mis toob kaasa isikuandmete nõuete rikkumised raamatupidamises?

Jah, suured trahvid, täpselt ei oska öelda kui suured, umbes 30 000 eurot.

26. Kas tahate ise midagi täiendada või oma mõtteid jagada üldmäärusest?

Ei, mina ei tea väga palju uuest üldmäärusest, et midagi veel lisada.

Lisa 2. Intervjuu küsimuste transkriptsioon: vastaja 2 (väikeettevõtte)

1. Kas Te olete valmis andma oma nõusoleku, et see intervjuu salvestatakse ja pärast kasutatakse lõputöö koostamiseks?

Jah.

2. Kas soovite jääda anonüümseks vastajaks või on lubatud ettevõtte nimi avalikustada?

Olen Zoja Vlassova ja töötan õigusabibüroos.

3. Teie ettevõtte suurus (kui palju töötajaid, väikeettevõtte 10-49, keskmine 50-249, suurettevõtte 250)?

Väikeettevõtte, 28 inimest.

4. Teie haridustase?

Olen lõpetanud Tallinna Majanduskooli, siis mul on kutseharidus.

5. Teie ametikoht?

Raamatupidaja.

6. Kust Te saite teada isikuandmete kaitse üldmääruse muudatustest?

Meil oli üldkoosolek, kus meie firma juristid andsid meile väikese koolituse.

7. Mis mõju töid kaasas üldmääruse muutused?

Eriti ei ole tehtud mingeid muudatusi töös.

Lisa 2. järg

8. Kas üldmääruse muutused saaksid lihtustada ettevõtte tööd?

Minu jaoks midagi ei ole muutunud. Raamatupidajate jaoks on loodud RTJ (raamatupidamise juhend) isiklike konfidentsiaalsete klientide andmete mitteavaldamisest. Samuti allkirjastame lepingu iga kliendiga, kus on sätestatud mitteavaldamise tingimused.

9. Kas raamatupidajad saavad täita kõik isikuandmetega seotud nõudeid?

Jah, ütlen niimoodi, et kõik raamatupidajad peavad täitma kõiki nõudeid.

10. Kuidas isikuandmete kaitse nõuded on kahe aasta jooksul muutnud?

Mina ei saa täpselt öelda, töötan raamatupidajana ainult kaks aastat. Minu märkuste kohaselt on kõiki isikuandmetega seotud nõudeid ainult ajaga karmistatud.

11. Millised andmed on Teie arvates delikaatsed isikuandmed?

Minu arvates kõik andmed, sealhulgas nimi, sugu, isiklik ja töökontakti informatsioon, ametikoht, sünnipäev, sünnikoht, rahvus, passiandmeid, ID-kaardi ja viisa andmeid.

12. Mis isikuandmed on vajalikud raamatupidajatele, et teha igapäevatööd?

Pole ühtegi. Me ei pea klientidega ise tegutsema. Meil on olemas osakond, kus töödeldakse klientide info, kõigipealt tuvastatakse kliendi ja ainult pärast seda protseduurilt, kõik kliendi info satud meile raamatupidamisosakonda. Kui on vaja esitada dokumendid riigiasutusele, siis ei saa seda andmeid ilma kliendi teadmisteta ja loata saata. Esiteks teavitame klienti sellest olukorrast ja ootame tema nõusolekut. Me oleme töödeldud esmased dokumendid, näiteks arved, pangaväljavõtted, lepingud jne. Tõenäoliselt siia kuuluvad kliendi nimi, e-maili aadress, telefoninumber, et me saaksime igal ajal helistada ja kirjutada kliendile. Aga tihti juhtub, mitte iga päev, erinevate lepingute koostamisel on vaja küsida kliendilt elukoha teavet, pangandmeid.

13. Millal on vaja küsida inimeste nõusolekut nende andmete töötlemiseks?

Sel hetkel, kui alustad kliendiga lepingu allkirjastama.

14. Kas Te olete küsinud oma töötajate nõusolekut andmete kasutamiseks?

Ei ole küsinud, me ei jaga kusagile oma klientide andmeid.

15. Kas Te olete teavitanud oma kliente sellest, kuidas Te olete nende andmeid töödeldud ja mis eesmärgi jaoks?

Peaaegu kõik kliendid küsivad ja on huvitatud, mille jaoks me kogume nende kohta informatsiooni. Seepärast muidugi oleme teavitanud.

Lisa 2. järg

16. Kas Te teate, kui kaua on vaja säilitada töölepingut pärast inimese töölt lahkumist?

Tööandja peab säilitama töölepingu töö ajal ja kümme aastat pärast töölepingu lõpetamist.

17. Kas Teie tööarvuti ja raamatupidamise programm on kaitstud parooliga?

Muidugi. Kõikjal on paroolid.

18. Kas Teie majandusarvestuse programmis on nähtav, kes ja milliseid andmeid vaatas ja kasutas?

Ei ole, meie raamatupidamise programmis on võimalik leida ainult seda jälgi, kes sisestas informatsiooni, kes tegi mingeid muudatusi, vaatas või kustutas, ei ole nähtav. Aga meie raamatupidamise programmi ligipääs on ainult raamatupidajatel, siis me oleme kindel, et informatsiooniga midagi ei juhtu.

19. Kui Te lähete kohvi jooma, Te panete oma arvuti lukku?

Tingimata! Me ei saa oma arvutit lihtsalt avatuks jätta

20. Kas keegi klientidest või töötajatest on palunud Teid kustutada informatsiooni nende kohta? Mis Te teate väljendist „õigus olla unustatud“?

Ei ole veel oma töös seda puutunud.

Pole piisavalt. Kui ma mõistan õigesti, siis kui klient või isik palub kustutada kõik tema andmed. Kuna ma pole seda õigust lugenud ja uurinud, mul tekib vastuolu andmete säilitamise seadustega.

21. Kuidas Teie arvate, kas tööandjal on õigus küsida töötajatelt nende laste arvu ja laste vanust?

Kui vaadata raamatupidamise küljest, siis muidugi saab küsida, kui töötaja näiteks lapsevanem ja tahab võtta endale lapsepäevi, siis raamatupidajale on vaja teada laste vanus. Ainult tänu sellele on võimalik arvutada ja teada saada, kui palju talle on lubatud lapsepäevi võtta.

22. Kas Teie ettevõttes kasutatakse andmete krüpteerimist?

Ei, ei kasuta.

23. Kas Teie ettevõttes on e-mailid turvalised, domeeniga?

Jah, ja meile igakuiselt vahetavad paroolid.

Lisa 2. järg

24. Kas Teie ettevõttes on rakendatud poliitikat, et töötajad saavad teha tööd oma isiklikus arvutis?

Jah, kuid töötajad saavad töötada kodust ainult sellel juhul, kui laps jäi haigeks ja ei ole võimalik tööle tulla. Aga mõnedel teisel juhul ei ole lubatud.

25. Mis toob kaasas isikuandmete nõuete rikkumised raamatupidamises?

Võin eksida, aga tean, et trahvid - umbes 32 000 tuhat eurot ja ettevõtja jaoks nagu trahv üle 300 000–400 000 tuhat eurot.

26. Kas tahate ise midagi täiendada või oma mõtteid jagada üldmäärusest

Kõik tegevused, mida te kasutate kliendi või tema jaoks, kõigepealt on parem klienti sellest teavitada ja alles seejärel midagi ette võtta.

Lisa 3. Intervjuu küsimuste transkriptsioon: vastaja 3 (keskettevõte)

1. Kas Te olete valmis andma oma nõusoleku, et see intervjuu salvestatakse ja pärast kasutatakse lõputöö koostamiseks?

Jah.

2. Kas soovite jääda anonüümseks vastajaks või on lubatud ettevõtte nimi avalikustada?

Anonüümseks.

3. Teie ettevõtte suurus (kui palju töötajaid, väikeettevõtte 10-49, keskmine 50-249, suurettevõtte 250)?

98 töötajat.

4. Teie haridustase?

Rakenduslik kõrgharidus.

5. Teie ametikoht?

Raamatupidaja.

6. Kust Te saite teada isikuandmete kaitse üldmääruse muudatustest?

Internetist ja kolleegide käest.

7. Mis mõju töid kaasas üldmääruse muutused?

See annab inimestele suurema kontrolli oma andmete üle ja tugevdab õigust eraelu puutumatussele internetis.

Lisa 3. järg

8. Kas üldmääruse muutused saaksid lihtustada ettevõtte tööd?

Pigem mitte.

9. Kas raamatupidajad saavad täita kõik isikuandmetega seotud nõuded?

Jah, kuid see on väga keeruline.

10. Kuidas isikuandmete kaitse nõuded on kahe aasta jooksul muutnud?

Andmete töötlemiseks ja salvestamiseks peab alati olla seaduslik eesmärk või nõusolek.

Inimesed saavad nõuda infot kõike andmete kohta, mis on asutusel olemas.

11. Millised andmed on Teie arvates delikaatsed isikuandmed?

Kodune aadress, telefon, töötasu, pereseis.

12. Mis isikuandmed on vajalikud raamatupidajatele, et teha igapäevatööd?

Palgad, töötajate kontaktandmed: nimi, isikukood, e-maili aadressid.

13. Millal on vaja küsida inimeste nõusolekut nende andmete töötlemiseks?

Näiteks, kui töö jaoks on vaja teada töötaja sõiduauto registreerimisnumeri, tehnilise passi koopia, kui see pole vaja lepingust töökohustuste täitmiseks.

14. Kas Te olete küsinud oma töötajate nõusolekut andmete kasutamiseks?

Mina pole küsinud, personaliosakond tegeleb sellega.

15. Kas Te olete teavitanud oma kliente sellest, kuidas Te olete nende andmeid töödeldud ja mis eesmärgi jaoks?

Mina pole küsinud.

16. Kas Te teate kui kaua on vaja säilitada töölepingut pärast inimese töölt lahkumist?

10 aastat.

17. Kas Teie töö arvuti ja raamatupidamise programm on kaitstud parooliga?

Jah.

18. Kas Teie majandusarvestuse programmis on nähtav, kes ja milliseid andmeid vaatas ja kasutas?

Jah.

19. Kui Te lähete kohvi jooma, Te panete oma arvuti lukku?

Ma panen üks oma kabineti kinni.

20. Kas keegi klientidest või töötajatest on palunud Teid kustutada informatsiooni nende kohta? Mis Te teate väljendist „õigus olla unustatud“?

Ei, ei ole.

Lisa 3. järg

Inimene saab nõuda kustutada andmed, mis ei ole enam vaja sellel eesmärgil, millega seoses need on kogutud või kui tema isikuandmed on töödeldud ebaseaduslikult.

21. Kuidas Teie arvate, kas tööandjal on õigus küsida töötajatelt nende laste arvu ja laste vanust?

Kui see on vaja töö jaoks (nt töötaja võtab lapsepuhkust). Küsida saab, kuid on vaja selgitada, mille jaoks need andmed on vaja ja andmete avaldamine on vabatahtlik.

22. Kas Teie ettevõttes kasutatakse andmete krüpteerimist?

Jah.

23. Kas Teie ettevõttes on e-mailid turvalised, domeeniga?

Jah.

24. Kas Teie ettevõttes on rakendatud poliitikat, et töötajad saavad teha tööd oma isiklikus arvutis?

Jah, kuid mitte kõik.

25. Mis toob kaasa isikuandmete nõuete rikkumised raamatupidamises?

Trahvid, kuni 20 miljonit eurot või 4% ettevõtte käibest.

26. Kas tahate ise midagi täiendada või oma mõtteid jagada üldmäärusest?

Ei tänan, edu lõputöö koostamise.

Lisa 4. Intervjuu küsimuste transkriptsioon: vastaja 4 (keskettevõte)

1. Kas Te olete valmis andma oma nõusoleku, et see intervjuu salvestatakse ja pärast kasutatakse lõputöö koostamiseks?

Jah.

2. Kas soovite jääda anonüümseks vastajaks või on lubatud ettevõtte nimi avalikustada?

Anonüümseks.

3. Teie ettevõtte suurus (kui palju töötajaid, väikeettevõtte 10-49, keskmine 50-249, suurettevõtte 250)?

Meil 223 töötajat ja see on keskmine ettevõtte.

4. Teie haridustase?

Magister ja bakalaureus.

Lisa 4. järg

5. Teie ametikoht?

Me oleme raamatupidajad, pearaamatupidaja kohta meie ettevõttes ei ole.

6. Kust Te saite teada isikuandmete kaitse üldmääruse muudatustest?

Tuli meilile koolituse info, alustasid mingisuguseid koolitused pihta, töö koht maksis kinni ja kohapeal meile tegiti koolitus. Veel olid ka veebipõhised seminarid, mis me kuulsime kõrvaklapidega.

7. Mis mõju tõid kaasas üldmääruse muutused?

Me peame töötajate käest nõusolekut küsima, vastavalt seadusele saame töötajate andmeid kasutada ja kui andmeid ei ole enam vajalikud, siis me peame kustutama inimeste andmeid. Me pidime oma kõik protsessid ülevaadata ja kooskõlastada direktiiviga, kaardistama kõik protseduurid ja kirja panema.

8. Kas üldmääruse muutused saaksid lihtustada ettevõtte tööd?

Ei, nad ei lihtsustanud, nad raskemaks teinud, me peame lisapabereid tegema. Aga teisest küljest me teame, et meil on dokumentatsioon on korras ja ei teki mõned küsimused sellest, et miks te kasutate seda või teist informatsiooni. Kohe saame põhjendada ja argumenteerida, miks ja kus kirja pannud, et see informatsioon on vajalik.

9. Kas raamatupidajat saavad täita kõik isikuandmetega seotud nõuded?

Jah, minu arvates küll saavad, neil ei ole mingeid takistused.

10. Kuidas isikuandmete kaitse nõuded on kahe aasta jooksul muutnud?

Me kogume hoopis vähem andmeid, me varem neid kui keegi tööle tuli küsisime tema haridustase tõendav diplomi, nüüd me küsime ainult need vajalikke, mis on seadusest tuleneb. Näiteks lapsepuhkusel mina peab teadma lapse nime ja isikukoodi, et ilma selleta ei ole üldse võimalik lapsepuhkust vormistada. Põhiliselt kõik info, mis meie raamatupidamisele on vaja seaduslikult, aga muud infot ei ole vaja koguda raamatupidamises.

11. Millised andmed on Teie arvates delikaatsed isikuandmed?

Usulised, rassilised, sugu, need andmeid põhiliselt, mille järgi on võimalik tuvastada isiku, kindlaks teha, et need andmeid on puudutavad just seda konkreetse inimese. Näpujälg.

12. Mis isikuandmed on vajalikud raamatupidajatele, et teha igapäevatööd?

Töötasu väljamaksmiseks, pangakonto, haiguspäevade arvestus, haigekassa info, laste isikukoodid.

Lisa 4. järg

13. Millal on vaja küsida inimeste nõusolekut nende andmete töötlemiseks?

Kui alustad inimeste informatsiooni töödelda, alati sellest küsitatakse töölepingus.

14. Kas Te olete küsinud oma töötajate nõusolekut andmete kasutamiseks?

Ei, sellest küsivad personali konsultandid, kes teavitavad sellest, kes järgmisena saab inimeste informatsiooni kasutada ja mille jaoks.

15. Kas Te olete teavitanud oma kliente sellest, kuidas Te olete nende andmeid töödeldud ja mis eesmärgi jaoks?

Kõikidel klientidel on oma lepingud, kus on kirjutatud sellest.

16. Kas Te teate, kui kaua on vaja säilitada töölepingut pärast inimese töölt lahkumist?

Kõik dokumendid on vaja säilitada 7 aastat, aga töölepingu 10 aastat.

17. Kas Teie töö arvuti ja raamatupidamise programm on kaitstud parooliga?

Jah, ja need paroolid on vaja tihti muuta.

18. Kas Teie majandusarvestuse programmis on nähtav, kes ja milliseid andmeid vaatas ja kasutas?

Jah, „Skaalas“ on kõik nähtav.

19. Kui Te lähete kohvi jooma, Te panete oma arvuti lukku?

Meie ettevõttes, töölepingus on kirjas, et kui töötaja läheb kusagile on vaja teha „Win“+“L“ ja arvuti kohe küsib parooli.

20. Kas keegi klientidest või töötajatest on palunud Teid kustutada informatsiooni nende kohta? Mis Te teate väljendist „õigus olla unustatud“?

Ei.

See ongi vist see, et kui näiteks laps saab 15 aastat vana, siis peaks kustutama, kui meil ei ole enam neid andmeid vaja, siis peaks neid andmeid kustutama. Või kui tööle kandideerija ei osutanud valituks, siis mingi aasta pärast (sõltub ettevõttest ja nende reeglist, kui kaua neid säilitavad seda) seda peaks ka hävitama.

21. Kuidas Teie arvate, kas tööandjal on õigus küsida töötajatelt nende laste arvu ja laste vanust?

Jah, ilma selleta ei ole võimalik lapsepuhkuse päevi anda.

22. Kas Teie ettevõttes kasutatakse andmete krüpteerimist?

Jah, me oma faile ka krüpteerime salasõnaga ja need andmeid, mis oleme saatnud maksutolli ametile ka krüpteerime.

Lisa 4. järg

23. Kas Teie ettevõttes on e-mailid turvalised, domeeniga?

Jah, muidugi.

24. Kas Teie ettevõttes on rakendatud poliitikat, et töötajad saavad teha tööd oma isiklikus arvutis?

Ei, ei ole, meil on ainult tööarvutid.

25. Mis toob kaasa isikuandmete nõuete rikkumised raamatupidamises?

Trahv 32 tuhat.

26. Kas tahate ise midagi täiendada või oma mõtteid jagada üldmäärusest?

Ei ei soovi, aitäh.

Lisa 5. Intervjuu küsimuste transkriptsioon: vastaja 5 (suurettevõte)

1. Kas Te olete valmis andma oma nõusoleku, et see intervjuu salvestatakse ja pärast kasutatakse lõputöö koostamiseks?

Jah

2. Kas soovite jääda anonüümseks vastajaks või on lubatud ettevõtte nimi avalikustada?

Anonüümseks

3. Teie ettevõtte suurus (kui palju töötajaid, väikeettevõtte 10-49, keskmine 50-249, suurettevõtte 250)?

Suurettevõtte, umbes 2500 töötajat.

4. Teie haridustase?

Keskharidus. Kohe ülikooli lõpetamas, bakalaureust omandamas.

5. Teie ametikoht?

Raamatupidaja

6. Kust Te saite teada isikuandmete kaitse üldmääruse muudatustest?

Meediast; tööandja poolt – meile jagati eraldi infot selle kohta ning oli koolitus.

7. Mis mõju tõid kaasas üldmääruse muutused?

Osade arvete jagamine läks keerulisemaks. Mõni arve oli teenusepakkuja poolt koostatud ning infoks olid juures töötajate nimed ja isikukoodid, nüüd isikukoode enam juurde ei pandud ja samanimelisi isikuid on meil mitmeid. See segas õigetele kulukohtadele jagamist.

Lisa 5. järg

Samuti tehti meil programmid ümber, näiteks Outlook ja Skype, automaatselt kustutatakse vestluseid mingi aja tagant, varem säilisid vestlused pikemalt ja pidi ise kustutama.

Praegu peab ka jälgima, kellele millist infot esitada. Isiklikke meilivahetusi krüpteerime jne.

8. Kas üldmääruse muutused saaksid lihtustada ettevõtte tööd?

Ei oska vastata.

9. Kas raamatupidajad saavad täita kõik isikuandmetega seotud nõuded?

Ma arvan, et saavad. Kasutavad andmeid vaid oma tööülesannete täitmiseks.

10. Kuidas isikuandmete kaitse nõuded on kahe aasta jooksul muutnud?

Selle aasta maikuus muutusid, rohkem ei tea.

11. Millised andmed on Teie arvates delikaatsed isikuandmed?

Usk, päritolu, tervis, ametiühingusse kuulumine, õiguserikkumine.

12. Mis isikuandmed on vajalikud raamatupidajatele, et teha igapäevatööd?

Mina konkreetset tegelen ainult arvete jagamise ning kuluaruannete kontrollimisega, mis puudutab töötajaid. Palka arvestab teine raamatupidaja, seega tema eest ei oska rääkida. Ilmselt tema vajab rohkem andmeid. Ta teab haiguslehtede, puudumiste ja muu sellise kohta. Mina näen ainult töötajate nimesid, nendele antud kasutajanimedid ning osakonda, kus nad töötavad.

Oma ettevõtte töötajate nimesid sisaldavaid dokumente. Konkreetset kui on arvel oleva kulu jagamine mingi grupi inimeste vahel, siis nime järgi vaatan, kus nad töötavad ja selle järgi panen kulukoha. Samuti kontrollin kuluaruandeid, seega näen, milliseid kulutusi on töötajad teinud lähetustel või millistes trennides käivad. Töötajate isiklikke andmeid ei näe.

13. Millal on vaja küsida inimeste nõusolekut nende andmete töötlemiseks?

Kliendi käest tuleb alati küsida.

14. Kas Te olete küsinud oma töötajate nõusolekut andmete kasutamiseks?

Ei ole küsinud, aga nagu varem mainisin, siis ei kasuta ma oma töös palju isikuandmeid, ainult nime.

15. Kas Te olete teavitanud oma kliente sellest, kuidas Te olete nende andmeid töödeldud ja mis eesmärgi jaoks?

Mina isiklikult ei ole, sest ei töötle klientide andmeid, aga tean, et mu ettevõttes seda tehakse. Need, kes andmeid töötlevad, kindlasti küsivad.

Lisa 5. järg

16. Kas Te teate, kui kaua on vaja säilitada töölepingut pärast inimese töölt lahkumist?
10 aastat.

17. Kas Teie tööarvuti ja raamatupidamise programm on kaitstud parooliga?
Jah.

18. Kas Teie majandusarvestuse programmis on nähtav, kes ja milliseid andmeid vaatas ja kasutas?

Jah, aga mitte kõigile.

19. Kui Te lähete kohvi jooma, Te panete oma arvuti lukku?

Kui võtan kaardi (töötõendi) välja, siis läheb arvuti kinni.

20. Kas keegi klientidest või töötajatest on palunud Teid kustutada informatsiooni nende kohta? Mis Te teate väljendist „õigus olla unustatud“?

Ei ole.

Igal inimesel on võimalus teenusepakkujale öelda, et ta tema andmed ära kustutaks.

21. Kuidas Teie arvate, kas tööandjal on õigus küsida töötajatelt nende laste arvu ja laste vanust?

Pigem mitte.

22. Kas Teie ettevõttes kasutatakse andmete krüpteerimist?

Jah.

23. Kas Teie ettevõttes on e-mailid turvalised, domeeniga?

Jah.

24. Kas Teie ettevõttes on rakendatud poliitikat, et töötajad saavad teha tööd oma isiklikus arvutis?

Ei, ainult töötaja arvutis, aga arvuti saab vajadusel koju kaasa võtta.

25. Mis toob kaasa isikuandmete nõuete rikkumised raamatupidamises?

Ei tea, aga arvan, et päris suured trahvid.

26. Kas tahate ise midagi täiendada või oma mõtteid jagada üldmäärusest?

Arvan, et kliendi seisukohalt on see päris mõistlik. Mulle küll meeldib, et saan telefoni teel müüjatele öelda, et nad mu andmed kustutaks ja enam ei helistaks.

Lisa 6. Intervjuu küsimuste transkriptsioon: vastaja 6 (suurettevõte)

- 1. Kas Te olete valmis andma oma nõusoleku, et see intervjuu salvestatakse ja pärast kasutatakse lõputöö koostamiseks?**
Ainult lõputöö koostamiseks.
- 2. Kas soovite jääda anonüümseks vastajaks või on lubatud ettevõtte nimi avalikustada?**
Soovime jääda anonüümseks vastajaks.
- 3. Teie ettevõtte suurus (kui palju töötajaid, väikeettevõtte 10-49, keskmine 50-249, suurettevõtte 250)?**
Suurettevõtte, 254 töötajat.
- 4. Teie haridustase?**
Ei soovi avaldada.
- 5. Teie ametikoht?**
Raamatupidaja ja krediidijuht.
- 6. Kust Te saite teada isikuandmete kaitse üldmääruse muudatustest?**
Andmekaitse inspeksioonist, määrusest ja koolituselt.
- 7. Mis mõju tõi ettevõttele kaasa mitmeid uusi kohustusi ning vajaduse üle vaadata protseduurid, et tagada nende vastavus üldmäärusele.**
- 8. Kas direktiivi muutused saaksid lihtustada ettevõtte tööd?**
Ei saanud.
- 9. Kas raamatupidajad saavad täita kõik isikuandmetega seotud nõuded?**
Muidugi saadav.
- 10. Kuidas isikuandmete kaitse nõuded on kahe aasta jooksul muutnud?**
Uus üldmäärus on andnud töötajale suurema õiguse ise otsustada, millisel otstarbel tema andmeid kasutatakse.
- 11. Millised andmed on Teie arvates delikaatsed isikuandmed?**
Terviseandmed, poliitilised ja usulised vaated, etniline päritolu, sõrnejäljed jne.
- 12. Mis isikuandmed on vajalikud raamatupidajatele, et teha igapäevatööd?**
Telefon, e-posti aadress, kui see on seotud isikuga.
- 13. Millal on vaja küsida inimeste nõusolekut nende andmete töötlemiseks?**
Enne töölepingu sõlmimist.

Lisa 6. järg

- 14. Kas Te olete küsinud oma töötajate nõusolekut andmete kasutamiseks?**
Jah, oleme küsinud kogu aeg, kui tuleb uus töötaja.
- 15. Kas Te olete teavitanud oma kliente sellest, kuidas Te olete nende andmeid töödeldnud ja mis eesmärgi jaoks?**
Jah, kõikides lepingus on see kirjas.
- 16. Kas Te teate, kui kaua on vaja säilitada töölepingut pärast inimese töölt lahkumist?**
Jah, 10 aastat.
- 17. Kas Teie tööarvuti ja raamatupidamise programm on kaitstud parooliga?**
Jah, on kaitstud parooliga.
- 18. Kas Teie majandusarvestuse programmis on nähtav, kes ja milliseid andmeid vaatas ja kasutas?**
Jah, kõik on nähtav ja jälgitav, kui on vajalik.
- 19. Kui Te lähete kohvi jooma, Te panete oma arvuti lukku?**
Jah, paneme kõik lukku vastavalt ettevõttes kehtestatud korrale.
- 20. Kas keegi klientidest või töötajatest on palunud Teid kustutada informatsiooni nende kohta? Mis Te teate väljendist „õigus olla unustatud“?**
On küll, küsinud ja me oleme kustutanud, kuid kõik lubatu piirides.
Õigus lasta oma andmeid kustutada ja üle kanda.
- 21. Kuidas Teie arvate, kas tööandjal on õigus küsida töötajatelt nende laste arvu ja laste vanust?**
On õigus, kuid tööandja peab selleks küsima töötaja nõusolekut.
- 22. Kas Teie ettevõttes kasutatakse andmete krüpteerimist?**
Ei kasuta.
- 23. Kas Teie ettevõttes on e-mailid turvalised, domeeniga?**
Jah, ainult need e-posti aadressid on kasutusel.
- 24. Kas Teie ettevõttes on rakendatud poliitikat, et töötajad saavad teha tööd oma isiklikus arvutis?**
Ei ole kasutusel.
- 25. Mis toob kaasas isikuandmete nõuete rikkumised raamatupidamises?**
Jah, teame, et suured trahvid kuni 20 miljonit eurot või 4% ettevõtte käibest.

Lisa 6. järg

26. Kas tahate ise midagi täiendada või oma mõtteid jagada üldmäärusest?

Ei soovi.

Lisa 7. Google Forms küsimustik

Informatsioon vastajate kohta

Teie vanus: (ainult arv)

- Oma vastus...

Teie haridustase:

- Põhiharidus
- Keskkharidus
- Kutseharidus
- Bakalaureusekraad
- Rakenduskõrgharidus
- Kutsekõrgharidus
- Magistrikraad
- Kõrgem kui magistrikraad
- Oma vastus...

Ettevõtte suurus, kus töötate:

- Mikroettevõtte – töötajaid 0-9
- Väikeettevõtte – töötajaid 10-49
- Keskmise ettevõtte – töötajaid 50-249
- Suurettevõtte – töötajaid üle 250

Teie ametikoht:

- Perraamatupidaja
- Raamatupidaja
- Finantsjuht
- Audiitor
- Vandeaudiitor
- Tegevjuht
- Personalikonsultant
- Personalijuht
- Oma vastus...

Lisa 7. järg

Küsimused isikuandmete üldmääruse kohta

Teie arvamus, ettevõtte kus Te töötate on „konfidentsiaalselt ette valmistanud“?

- Jah, olen täiesti nõus.
- Ei ole kindel.
- Ei ole.
- Oma vastus...

Kui hästi Te olete valmis isikuandmete kaitse üldmääruseks?

- Olen täiesti valmis, tean kõik muudatused, rakendan kõiki nõuded igapäevatöös.
- Olen kuulnud, natuke tean, aga midagi töös ei ole muutnud üldmääruse muutusega.
- Olen kuulnud, kui mind seda ei puutu.
- Mitte midagi ei tea.
- Oma vastus ...

Peale üldmääruse jõustamist tuleb isikuandmeid töötelda: (Nimetage 3 põhiväärtust)

- Oma vastus...

Mis on delikaatsed andmed? (Nimetage 5-6 delikaatsete andmete näited)

- Oma vastus...

Mis isikuandmete informatsiooni Te ise töötlete?

- Geneetilised andmed
- Biomeetrilised andmed
- Terviseandmed
- Oma vastus...

Palun nimetage 3-5 isikuandmete kaitse üldmääruse muudatust.

- Oma vastus...

Milliseid tehnilisi meetmeid Te olete kasutatud või Teie ettevõttes on võtnud kasutusele, et tagada isikuandmete kaitstud säilitamist ja kinnist juurdepääsu?

Vastuse variandid (jah; ei; osaliselt; ei kasuta)

- Antiviirustarkvarad.
- Igal töötajal on oma paroolid ja kasutajanimed.

Lisa 7. järg

- Igal töötajal on oma kiipkaart millega iga isik saab ennast identifitseerida enne tööle alustamist.
- Ettevõtte Wifi kaitstud parooliga ja teised võrgu võimalused ei ole lihtsalt kätte saadavad võõrastele inimestele.
- Kaugtöö lubatud ainult virtuaalse eravõrgu (VPN) kaudu.
- Kaugtöö lubatud oma arvutis peale seda IT-spetsialisti kontrolli.

Kas Teie ettevõttes on rakendatud BYOD (Bring your own device) poliitika?

- Jah, rakendatud, peaaegu kõik töötajad kasutavad.
- Jah, kuid mitte eriti palju, kes kasutavad.
- Ei, ei ole kasutusel.
- Ei tea sellest mitte midagi.
- Oma vastus...

Kas Teie ettevõttes kasutatakse andmete krüpteerimist?

- Jah, kõik tundlikud asjad krüpteeritakse.
- Jah, kuid mitte kõik, selektiivselt krüpteeritakse.
- Ei, ei ole kasutusel.
- Ei tea sellest mitte midagi.
- Oma vastus...

Kas on Teie ettevõttes palgatud andmekaitse spetsialist?

- Jah, on olemas.
- Ei, ei ole.
- Oma vastus...

Kust Te saite teada isikuandmete kaitse üldmääruse muudatusest?

- Ise käin koolitusele.
- Töö pakub erinevaid koolitusi.
- Ise uurisin ja lugesin internetis.
- Töökaaslased jutustasid sellest.
- Mitte midagi ei tea.
- Oma vastus...

Lisa 8. Raamatupidajate teadmiste tase tabel

	Vastaja 1	Vastaja 2	Vastaja 3	Vastaja 4	Vastaja 5	Vastaja 6
1	0.5	1	0.5	1	1	1
2	0	0	1	1	1	1
3	0	0.5	0	1	0	1
4	0.5	1	1	1	1	1
5	0	0.5	1	1	0	1
6	0.5	1	1	1	1	0.5
7	1	1	1	1	1	1
8	1	1	0.5	1	1	1
9	0.5	0.5	0.5	1	0.5	1
10	0	1	1	1	0.5	1
11	0	1	1	1	1	1
12	1	1	1	1	1	1
13	0.5	0.5	1	1	1	1
14	0.5	1	1	1	1	1
15	1	1	1	1	0	1
16	1	0	1	1	1	0
17	1	1	1	1	1	1
18	0.5	0.5	0.5	1	1	1
19	0	1	0.5	1	0	0.5
20	0	1	0	0	1	0
Kokku	9.5	15.5	15.5	19	15	17