TALLINNA TEHNIKAÜLIKOOL
Majandusteaduskond
Ärikorralduse instituut

Kairi Perk

# ANDMEKAITSE RAAMATUPIDAMISES

Bakalaureusetöö

Juhendaja: dotsent Natalja Gurvitš

Tallinn 2017

# SISUKORD

# ABSTRAKT

Töö pealkiri on: „Andmekaitse raamatupidamises“.

Bakalaureusetöö eesmärk on välja selgitada, missugused teadmised on raamatupidajatel andmekaitsest ning kui palju nad oma igapäevatöös neid kasutavad. Käesolev töö on koostatud Tallinna Tehnikaülikooli Majandusteaduskonna bakalaureuseõppe tudengi poolt, uurimaks teemat, kui palju on seotud raamatupidamine ja andmekaitse. Käesolevas bakalaureusetöös uuris autor raamatupidajate teadlikkust andmekaitsest ning kas need teadmised on piisavad ettevõtte ohutuks hindamisele. Kvantitatiivsete andmete töötluseks kasutati kirjeldavat statistikat. Uuringust selgus, et ligi pooled vastanutest on teadlikud andmekaitsest ning sellega kaasnevatest ohtudest. Sama kehtib ettevõtetes rakendatud meetmete kohta, et tagada andmete turvalisus. Kvalitatiivsed andmed analüüsiti kasutades cross-case analüüsi. Uurimuse tulemustest tuli välja, et mida suurem ettevõte, seda olulisem on andmekaitse firmale ning seda rohkem juhitakse tähelepanu turvalisusele. Sama võib väita ka raamatupidajate kohta. Mikroettevõtte raamatupidaja ei pidanud andmekaitset väga oluliseks, keskettevõtte raamatupidajad olid kuulnud andmekaitsest, kuid arvasid, et nende ettevõte on piisavalt turvatud ning erilist tähelepanu sellele pöörama ei pea, ning suurettevõtte raamatupidaja jaoks on andmekaitse väga oluline ning tema teadmised sellest olid ka kõige paremad. Käesolev töö kinnitab, et sarnaselt mujal maailmas leitule, on ettevõttes olemas ohud seoses andmekaitsega. Inimesed ei ole teadlikud, et andmed, mida nad töötlevad, võivad ohus olla küberrünnakul. Raamatupidajate teadlikkust tuleks tõsta just väiksema suurusega ettevõtetes. Keskmise suurusega ettevõtete raamatupidajate teadmised andmekaitsest olid head ning nad mõistsid andmekaitse peamisi võimalikke ohtusid. Küll aga tihti neid teadmisi praktikas ei ole rakendatud. Enamasti suurettevõtetes töötavad raamatupidajad teadsid andmekaitse turvalisusega kaasnevaid ohtusid ning erinevad meetmed ohtude eemaldamiseks olid ka kasutusele võetud. Kvalitatiivsest uuringust tuli välja, et mida suurem on ettevõte, seda rohkem on andmekaitse peale mõeldud. Kvantitatiivsest uuringust tuli välja, et ettevõtte suurus ei ole määrava tähtsusega andmekaitse seisukohalt. Selgus aga, et need vastajad, kes pidasid ettevõtet, kus töötavad, väga turvaliseks või üldse mitte turvaliseks, hindasid ettevõtet õiglaselt. Need, kes pidasid ettevõtet turvaliseks, hindasid firmat ebaõiglaselt.
Märksõnad: raamatupidaja, andmekaitse, ettevõtte turvalisus, ülikool

# SISSEJUHATUS

Andmekaitse on olnud juba pikka aega väga oluline ning muutub aina olulisemaks infoajastu tõttu, kus informatsioon on kergesti kättesaadav. Andmekaitse puudutab aga kõige rohkem ettevõtte turvalisust. Ettevõtte töötajate jaoks on seega väga oluline teada riske ja võimalikke ohtusid, mis andmekaitsega seonduvad.

Autor uuris antud teemat oma uurimistöös, mis kirjutati 2016.aasta sügissemestril ning kaitsti 2017.aasta jaanuaris. Bakalaureusetööks on autor aga oluliselt teooriat täiendanud ning läinud rohkem sügavuti. Küll aga kasutatakse käesolevas töös varasemalt kirjutatud ning kaitstud uurimistöös kasutatud teooriat ning kvalitatiivse uurimuse tulemusi.

Bakalaureusetöö eesmärk on välja selgitada, missugused teadmised on raamatupidajatel andmekaitsest ning kui palju nad oma igapäevatöös neid kasutavad. Töö püüab anda vastuse küsimusele, kas raamatupidajate teadlikkus andmekaitsest on piisav ettevõtte turvaliseks hindamiseks. Lisaks sellele aitab bakalaureusetöö mõista, kas ettevõtted peaksid oma töötajate teadlikkust andmekaitsest tõstma, sest just raamatupidajate käest liigub läbi väga tähtsat informatsiooni (pangaandmed, paroolid jms). Kui töötajad on isegi teadlikud andmekaitsest, tuleb veenduda, et turvalisusmeetmeid ka rakendatakse ettevõttes. Seetõttu saab bakalaureusetööst ka teada, mida peaksid ettevõtted eriti tähele panema oma turvalisuse paranemisele.

Käesolevas bakalaureusetöös uuris autor raamatupidajate teadlikkust andmekaitsest mikro-, väike-, kesk- ja suurettevõtetes. Antud teema on oluline nii ülikoolidele kui ka tööandjatele, puudutades ettevõtte turvalisuse teemat. Käesoleva uuringu eesmärgiks oli välja selgitada, missugused teadmised on raamatupidajatel andmekaitsest ning kui palju nad neid teadmisi oma igapäevatöös kasutavad.

Kvalitatiivse uurimuse raames viidi bakalaureusetöö autori poolt läbi kolm intervjuud raamatupidajatega mikro-, kesk- ning suurettevõttest. Intervjuude kestvuseks oli keskmiselt 15 minutit. Raamatupidajate teadlikkust andmekaitsest kvantitatiivseks uurimiseks kasutas autor küsimustikku, mis koosnes valikvastustega küsimustest ning likert-skaala põhjal koosnevatest küsimustest. Kõik küsimustiku vastamisel osalejad olid raamatupidajad või sarnasel alal töötavad inimesed. Küsimustik, millele vastati, oli anonüümne ja vastajad pidid olema hetkel töötavad raamatupidajad. Kvantitatiivses uuringus osales 74 raamatupidajat.

Bakalaureusetöö autori poolt välja pakutud hüpotees on, et raamatupidajate teadlikkus andmekaitsest on puudulik ning seda tuleks tõsta, et ettevõtet saaks hinnata turvaliseks. Bakalaureusetöö eesmärgiks on välja selgitada raamatupidajate teadlikkus andmekaitsest. Praegusel infoajastul on palju võimalusi andmetele ligipääsuks. Tudengina tunneb autor, et ülikoolis pööratakse vähe tähelepanu arvuti ning interneti kasutamise turvalisusele (välja arvatud IT-erialad), kuid reaalsuses puutub iga valdkonna töötaja vähemal või suuremal määral sellega kokku. Seepärast on oluline, et vastav koolitus viiakse läbi ettevõttes, kuid see nõuab omakorda aega ja ressurssi.

# 1. ANDMEKAITSE

## 1.1. Andmekaitse definitsioon

Andmekaitset kohtab meie elus üha sagedamini, sest praeguse infoajastu tõttu on oluline inimestel võimalusel privaatseks jääda. Et seda lähemalt uurida, tuleb alustada andmekaitse mõistmisest ning definitsioonist. Andmekaitse õigusharuna ei keskendu andmete kaitsele, vaid püüab kaitsta inimest, keda kaitstavad andmed identifitseerivad. Andmed on informatsioon kellegi või millegi kohta. (Eesti keele sõnaraamat ÕS 1999. Eesti Keele Instituut. Kolmas trükk. Tallinn, Eesti Keele Sihtasutus 2003.) Isikuandmed tähendavad seega informatsiooni kellegi kohta. Andmekaitse kaitseb isikut, täpsemalt isiku õigust informatsioonilisele enesemääratlusele. Informatsiooniline enesemääratlus on isiku põhiõigus ja –vabadus ise valida ja otsustada, kellele ja milliseid andmeid ta enda kohta avaldab. (Männiko, M. (2011) Õigus privaatsusele ja andmekaitse) Isikuandmed on defineeritud kui igasugune tuvastatud teave või tuvastatav füüsiline isik (andmesubjekt). Tuvastatav isik on isik, keda saab tuvastada, kas siis otseselt või kaudselt, näiteks isikukoodi põhjal ja isegi ühe või mitme tema või tema füüsilise, füsioloogilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse (näiteks sünnikuupäev, töökoht, kodune aadress, e-posti aadress, telefoninumber, ja isegi foto) järgi. (What is Personal Data?, 2007) Isikuandmete töötlemine on iga isiku isikuandmetega tehtav toiming või toimingute kogum, sõltumata töötlemise viisist (kas automatiseeritud või manuaalne töötlemine), näiteks kogumine, säilitamine, kohandamine, salvestamine, korrastamine või muutmine, väljavõtete tegemine, päringu teostamine, levitamine, kasutamine, üleandmine või muul moel avaldamine, ühendamine, sulgemine, kustutamine või hävitamine. Isik, kes viib läbi isikuandmete töötlemisega seonduvaid tegevusi, on isikuandmete töötleja. Andmesubjektiks nimetatakse isikut, kelle isikuandmeid töödeldakse. Iga inimene, kelle kohta on olemas tema kohta käivat informatsiooni, mida teab, omab, kasutab jne mõni kolmas isik, on andmesubjekt. (Männiko, M. (2011) Õigus privaatsusele ja andmekaitse)

On oluline mõista, et andmekaitse ei kaitse andmeid, vaid andmete kaudu identifitseeritavat isikut. Need võivad olla mis tahes andmed, mille kaudu on võimalik isikut tuvastada. Kõige rohkem keskendutakse andmete kaitsmisel just neile, mida töödeldakse. Andmete töötlemiseks võib pidada mis tahes viisil andmetega ümberkäimist.

## 1.2. Andmekaitse ajalugu

Isikuandmete kaitse, eraelu austamine ning privaatsus on tähtsad põhiõigused. Euroopa Parlament on alati rõhutanud, et tuleb leida tasakaal turvalisuse suurendamise ning inimõiguste, sealhulgas andmekaitse ja eraelu puutumatuse tagamise vahel. Selleks, et sellist regulatsiooni luua, moodustas Majanduskoostöö ja Arengu Organisatsioon (OECD) ekspertide grupi, et uurida suhet arvuti ja selle privaatsuse vahel. Grupp alustas ametlikke määrusi arvestades füüsiliste isikute isikuandmete käsitlemist nii erasektoris kui ka avalikus sektoris. Sellele tuginedes andis OECD välja seitse põhilist soovitust isikuandmete kaitseks:

1) Andmesubjekte peab teavitama, kui nende andmeid on kogutud;
2) Andmeid peab kasutama ainult eesmärgipäraselt;
3) Andmeid ei tohi avalikustada ilma andmesubjekti nõusolekuta;
4) Kogutud andmed peavad olema hoitud turvaliselt potentsiaalse kuritarvitamise eest;
5) Andmed peavad olema avaldatud andmesubjektidele, kelle andmed on kogutud;
6) Andmesubjektil peab olema lubatud ligipääs andmetele ja ka võimalus ebatäpsusi vajadusel korrigeerida;
7) Andmesubjekt peab olema teadlik meetodist, missugustel põhimõtetel andmekogujad andmeid käitlevad.

(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Matthew Bender)

Euroopa Liit koostas kõigist seitsmest printsiibist direktiivi, millel on kaks peamist eesmärki: Esiteks kaitsta füüsilise isiku põhiõigusi ja vabadusi, samuti osaliselt nende eraelu puutumatust seoses isikuandmete töötlusega. Teiseks tagada seda, et liikmesriigid ei piiraks ega keelaks isikuandmete vaba liikumist liikmesriikide vahel.

Selleks, et täita mõlemad eesmärgid, kehtestas direktiiv mitmesuguseid sätteid, sealhulgas kriteeriumi õiguspäraseks andmetöötluseks, andmesubjekti õiguse tutvuda andmetega, andmesubjekti õiguse esitada vastuväiteid ning tagada andmetöötluse konfidentsiaalsus ja turvalisus. Õiguspärase andmetöötluse kriteeriumi kohaselt täpsustab direktiiv, et isikuandmeid võib töödelda ainult siis, kui andmesubjekt on andnud selleks ühemõttelise nõusoleku või, kui töötlemine on vajalik teatud kindlaksmääratud põhjustel. Direktiiv sätestab ka selle, et andmesubjektil on õigus teada, et tema isikuandmeid töödeldakse ning samuti, miks neid andmeid töödeldakse. Kõik andmed, mis ei vasta käesolevale direktiivile, võib

andmesubjekt parandada, kustutada või blokeerida. Direktiiv sätestab andmesubjektile õiguse esitada vastuväiteid nõuetele mittevastavast andmetöötlusest. Viimaseks, direktiiviga tagatakse andmetöötluse konfidentsiaalsus ja turvalisus lubades, et andmetöötleja ja temaga seotud isikud ei töötleks andmeid ilma kontrollija juhtnöörideta või isiku, kes vastutab määruse eesmärkide ja isikuandmete töötlemise vahendite töötlemise eest. Andmetöötleja ja temaga seotud isikud peavad samuti välja tooma viisid, kuidas peaks vastutav töötleja tagama turvalisuse ja kaitsma juhusliku või ebaseadusliku andmete hävitamise või juhusliku kaotsimineku, muutmise, ebaseadusliku avalikustamise või juurdepääsu eest, eelkõige juhul, kui töötlemine hõlmab andmete edastamist võrgu kaudu. Lisaks kinnitab direktiiv, et võib olla erandeid juurdepääsuõiguse põhimõtetes teatud teadusuuringute või statistilistel eesmärkidel. Nimelt sisaldab direktiiv seitset erandit ja piirangut, mis lubavad liikmesriikidel piirata õigust privaatsusele teatud tingimustel. Täpsemalt võivad liikmesriigid piirata teatud artikleid, kui piirang on vajalik, et kaitsta:

1) Riigi julgeolekut;
2) Riigikaitset;
3) Avalikku julgeolekut;
4) Andmeid, mis on seotud kuriteo või rikkumise eetikaga;
5) Liikmesriikide rahanduslikke või majanduslikke huve;
6) Reguleerivaid funktsioone, mis on seotud avaliku julgeoleku, kuritegude eetika rikkumise või liikmesriikide majanduslike ja rahanduslike huvidega;
7) Andmesubjekti või teise isiku õigusi ja vabadusi.

Direktiiv avaldati 1995.aastal ning see jõustus samal aastal. Liikmesriigid koostasid hindamisaruande direktiivi rakendamise kohta ning see pälvis üldist edu. Euroopa Komisjon märkis oma esimeses ametlikus aruandes direktiivi rakendamise kohta, et direktiiviga ei õnnestutud luua keskkond, kus on isikuandmete informatsiooni vaba liikumine kogu Euroopa Liidus, säilitades samal ajal kõrge isikuandmete kaitse. (A New Age of Privacy Protection: A Proposal for an International Personal Data Privacy Treaty, 2010, vol 42)

Andmekaitse on oma olemuslikult uus õigusharu. Vajaduse isikuandmete kaitse järele tekitas praegune infotehnoloogia ajastu ja ülikiire areng andmete automatiseeritud kujul töötlemisel, millega seonduvalt muutus isiku identifitseerimine ja isikuandmete töötlemine nii lihtsaks, et tõi endaga kaasa otsese ohu informatsioonilisele enesemääratlusele ning sellega tekkis vajadus õiguskaitse mehhanismide järele. (Männiko, M. (2011) Õigus privaatsusele ja

andmekaitse). Eestis jõustus esimene isikuandmete kaitse seadus 1996.aastal. Praegune isikuandmete kaitse seadus jõustus 2008.aastal, kuid Euroopa Komisjon avaldas 4.novembril 2010.aastal teatise „Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus“. Selles teatati, et kehtiv andmekaitsedirektiiv 95/46/EÜ vajab uuendamist. Nimelt arvatakse, et kaasaegne maailm vajab rahvusvahelise isikuandmete kaitseks lepingut, et kaitsta inimese põhiõigusi eraelu puutumatusele infotehnoloogia ning informatsiooni ajastul. Andmekaitsemääruse eesmärk on anda kodanikele kontroll oma isikuandmete üle, ühtlustada andmekaitse taset kogu Euroopa Liidus ning tugevdada digitaalset ühisturgu. Andmekaitsemäärus kehtib kõikidele organisatsioonidele (olenemata suurusest), mis tegutsevad Euroopa Liidus või käitlevad (koguvad või töötlevad) Euroopa Liidus asuvate isikute andmeid. Määrus on Euroopa Liidu liikmesriikidele otsekohalduv ning sisaldab nõudeid, mille täitmine eeldab eri osapoolte (nt juhtkond, äriprotsesside eest vastutavad isikud) protsessi kaasamist. Euroopa Parlament kiitis 14.aprillil 2016.aastal lõplikult heaks andmekaitse reformi paketi, millega eelnimetatud direktiiv asendatakse otsekohalduva Isikuandmete kaitse üldmäärusega, lisaks sisaldab pakett ka eraldi direktiivi andmete edastamisel politseikoostöö ja õigusalase koostöö valdkonnas. Määrus jõustus 24.mail 2016.aastal ning on avaldatud Euroopa Liidu Teatajas. Määrust hakatakse kohaldama pärast kaheaastast üleminekuaega, alates 25.maist 2018.aastal. (Euroopa Andmekaitse reform. Andmekaitse Inspektsioon. 2016) Hetkel (mai, 2017) peaksid ettevõtted juba aktiivselt tegelema vajalike muudatustega, mis peavad valmis olema tuleva aasta kevadeks. Seega peaks andmekaitse olema väga aktuaalne teema ettevõtetes ning nad peaksid mõistma andmekaitset ning selle tähtsust ettevõttes.

## 1.3. Andmekaitse olemus

Andmekaitse tähendab isiku põhiõiguslikku kaitset – õigust privaatsusele. Seega keskendub andmekaitse kõige rohkem andmesubjektile. Isikuandmete olemasolu iseenesest ei lisa ega võta ära kellegi põhiõigusi, kuid põhiõigust ehk õigust privaatsusele võib riivata isikuandmete töötlemine.

Alljärgnevalt on toodud välja õiguspärase töötlemise põhimõtted, mida isikuandmete töötleja peab järgima vastavalt Isikuandmete kaitse seaduse paragrahvile 6:

- Seaduslikkuse põhimõte – isikuandmeid võib koguda vaid ausal ja seaduslikul teel;

- Eesmärgikohasuse põhimõte – isikuandmeid võib koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkidega kooskõlas;
- Minimaalsuse põhimõte – isikuandmeid võib kasutada vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks;
- Kasutuse piiramise põhimõte – isikuandmeid võib muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal;
- Andmete kvaliteedi põhimõte – isikuandmed peavad olema ajakohased, täielikud ning vajalikud seatud andmetöötluse eesmärgi saavutamiseks;
- Turvalisuse põhimõte – isikuandmete kaitseks tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest;
- Individuaalse osaluse põhimõte – andmesubjekti tuleb teavitada tema kohta kogutavatest andmetest, talle tuleb võimaldada juurdepääs tema kohta käivatele andmetele ja tal on õigus nõuda ebatäpsete või eksitavate andmete parandamist.

(Männiko, M. (2011) Õigus privaatsusele ja andmekaitse)

Kokkuvõtteks võib öelda, et andmekaitse peab olema isiku põhiõigustega tagatud. Andmekaitse ei riiva ega võta kelleltki ära põhiõigusi, see vaid aitab isikul jääda tema soovi korral privaatseks. Et tagada privaatsus, tuleb järgida eelnevalt nimetatud kuut põhimõtet.

# 2. ANDMEKAITSE SEOS RAAMATUPIDAMISEGA

## 2.1. Andmekaitse töösuhetes

Andmekaitse töösuhtes on samuti võrdlemisi uus nähtus ning on tingitud peamiselt sellest, et demokraatia ja ühiskonna areng tervikuna on vähendanud olemuslikku lõhet töötaja ja tööandja vahel ning muutnud range alluvussuhte pigem partnerlussuhteks, kus pooltel peaksid olema võrdsed õigused ja kohustused.

Üldised andmekaitse põhimõtted (vt lähemalt alajaotus 1.3) kuuluvad kohaldamisele ka töösuhete raames toimuvale andmetöötlusele:

- Seadusliku töötlemise põhimõte – Isikuandmete direktiivi artikkel 7(b) sätestab, et isikuandmeid võib töödelda, kui töötlemine on vajalik sellise lepingu täitmiseks, mille osapooleks andmesubjekt on, või lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele. Nimetatud õiguslik alus annab tööandjale õiguse töösuhtes vajalike isikuandmete töötlemiseks. Näiteks ei saa töötaja keelduda tööandjale avaldamast informatsiooni oma laste arvu kohta ning vajadusel tõendama laste olemasolu, kui töötaja soovib kasutada seadusega sätestatud võimalust väikelapse hooldamiseks ettenähtud lisapuhkuse saamiseks.
- Asjakohasuse põhimõte – Tööandja ei tohi töötaja andmeid töödelda (näiteks koguda või säilitada) igaks juhuks. Töösuhtes on isikuandmete töötlemine sageli vajalik näiteks töötulemuste hindamiseks ja/või töötaja edutamiseks. Seega peab tööandja olema töötaja isikuandmeid töödeldes valmis põhjendama, et vajadus töötaja isikuandmete töötlemiseks tuleneb töösuhtest.
- Minimaalsuse põhimõte – Töösuhetes võib koguda andmeid üksnes nii palju, kui andmetöötluse eesmärgist lähtuvalt on vajalik. Näiteks teatud andmete kogumine töötaja laste kohta on põhjendatud. Minimaalsuse põhimõttest lähtudes ei ole põhjendatud näiteks andmete kogumine selle kohta, millises koolis töötaja laps õpib.

(Männiko, M. (2011) Õigus privaatsusele ja andmekaitse)

Isikuandmed, mida tavaliselt töösuhte raames töödeldakse, on järgmised:

- Tööle kandideerimise avaldus, sageli koos elulookirjeldusega, mis sisaldab isikuandmeid;
- Palga ja maksude tasumisega seotud andmed;
- Töövõimetusega seotud andmed;
- Puhkuseandmed (sh seadusega määratud andmed lisapuhkuse kohta, millele õiguse omamist peab töötaja tõendama isikuandmetega (näiteks informatsiooni oma pereliikmete kohta));
- Töötaja peetud arenguvestluste, edutamise, distsiplinaarküsimustega seonduv informatsioon;
- Tööõnnetuste menetlemisega seonduv informatsioon;
- Töötaja poolt töö käigus loodud informatsioon (e-kirjad, telefoniarved, internetiblogid);
- Tööl viibitud aja arvestus (tihti kasutatakse sisenemiseks unikaalseid uksekaarte või –koode, mis fikseerivad tööletuleku ja töölt lahkumise ning võimaldavad tööandjal jälgida töötaja tööaja kasutamist);
- Jälgimisseadmete (turvakaamerate) salvestised.

(Männiko, M. (2011) Õigus privaatsusele ja andmekaitse)

Andmekaitseaktidega on kaitstavad ainult sellised isiku kohta käivad andmed, mille alusel on isik tuvastatud või tuvastatav. Andmed, mille alusel on võimalik isikut identifitseerida, on isikuandmed ehk teiste sõnadega on isikuandmed kõik isiku identifitseerimist võimaldavad andmed. Andmete sisu ning sisust tuleneva riive intensiivsuse järgi jagunevad isikuandmed tavalisteks ja delikaatseteks isikuandmeteks. (Männiko, M. (2011) Õigus privaatsusele ja andmekaitse)

Tavalisi isikuandmeid on lubatud koguda, säilitada ja kasutada tingimusel, kui neid kasutatakse töösuhte eesmärgil. Sellest aga ei piisa, et andmete kogumine on lihtsalt kasulik, tööandja peab täpselt määratlema, milleks tal neid andmeid vaja on (näiteks töötajate palgaarvestuse juurdepääsu kontroll). Tööandjad võivad töösuhte eesmärgil koguda ja talletada isiklikke andmeid nagu sugu, perekonnaseis, haridustase ja keelteoskus. Siiski, kui tööandja vajab põhiinformatsiooni töötasu edutamise kohta edastada kolmandale osapoolele, võib tööandja teha seda ilma töötaja nõusolekuta, kui see on oluline töösuhte arengu jaoks ning tingimusel, kui see on mainitud ka töölepingus. Kui tööandja vajab mitte

tööeesmärkidega seotud põhjustel koguda töötaja kohta teavet, siis tuleb saada luba töötajalt kirjalikult. (Männiko, M. (2011) Õigus privaatsusele ja andmekaitse)

Delikaatsed isikuandmed on:

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 terviseseisundi või puude kohta;
4) Andmed pärilikkuse informatsiooni kohta;
5) Biomeetrilised andmed (eelkõige sõrmejälje-, peopesajälje- ja silmaiirisekujutis ning geeniandmed);
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.

(Delikaatsed isikuandmed, 2014)

Erinevalt tavalistest andmetest ei piisa delikaatsete isikuandmete kogumise puhul ainult põhjusest, et seda tehakse töösuhte eesmärgil. Sel juhul on vajalik töötaja kirjalik nõusolek. Kui töötaja ei anna oma nõusolekut, siis on võimalik siiski tööandja või kolmanda isiku elulistel huvidel olla piisavalt põhjuseid, et koguda ja kasutada delikaatseid andmeid. Tundlikke andmeid võib koguda ja kasutada ka siis, kui töötaja on need ise avalikuks teinud. Tööandjal on kohustuslik teavitada töötajat oma andmete kogumise, säilitamise ja töötlemise kohta.

Delikaatsete andmete puhul tuleks ettevõtetel silmas pidada kümme põhilist punkti:

1) Ettevõtted peavad tegelema delikaatsete andmete turvalise hoiustamisega;
2) Ettevõtted on kohustatud kaitsma end andmete mittekadumise eest ning sõltumatult teatama andmete rikkumisest;
3) Ettevõttes peab olema selge, kus on delikaatne info ning kellel on sellele ligipääs;
4) Ei tohi koguda delikaatset infot, kui seda ei suudeta kaitsta;
5) Probleemidega tuleb tegeleda otsekohe;
6) Ettevõttel peab olema tegutsemisplaan juhuks, kui andmeid on rikutud;

7) Tuleb olla kursis, kui keegi kõrvaline isik pääseb delikaatsetele andmetele ligi;
8) Tuleb tegutseda targalt, kuidas säilitada kasulikke andmeid ja olulisi tõendeid;
9) Tuleb kinni pidada võimalusest, et kliente säilitada;
10) Tuleb pöörata tähelepanu andmete mittekadumise ennetamisele, mitte siis, kui andmed juba on kadunud.

(Ten Practical Things to Know About „Sensitive“ Data Collection and Protection, 2008)

Delikaatsete andmete puhul tuleb silmas pidada seda, et kui isik avaldab ise mõned delikaatsed andmed enda kohta, siis sel juhul on lubatud delikaatseid andmeid ka töödelda kolmandate isikute poolt. See tähendab, et isik on ise andnud loa oma andmete töötlemiseks. Seega tuleb olla väga ettevaatlik igasuguse informatsiooni avaldamisel, eriti avaldamisel Interneti kaudu (näiteks andmete avaldamise lubamine Facebookile või Google´ile).

## 2.2. Isikuandmete töötlemine läbi Interneti

Et paremini mõista andmekaitse tähtsust raamatupidamises, tuleb esmalt uurida, mis on raamatupidaja igapäevased tööülesanded ning missuguste andmetega nad kokku puutuvad. Raamatupidaja põhilised tööülesanded on seotud igapäevase raamatupidamise tööga, mis sisaldavad maksudeklaratsioonide täitmist, statistiliste aruannete koostamist jne. Raamatupidaja tüüpilised igapäevased tööülesanded on:

- Ettevõtte arvete tasumine;
- Rahakäibe liikumise aruandlus;
- Arvete kinnitamise ja tasumise jälgimine ettevõtte sise-eeskirja ning seaduse järgi;
- Tehingutelt riigimaksude arvestamine (tulu-, sotsiaalmaks jt);
- Töötajate palga ja puhkuse arvestus ning nende eest tasumine;
- Arveregistri pidamine;
- Aruannete esitamine maksuametile;
- Juhatuse finantsnõustamine.

Raamatupidaja tööülesannete hulka kuuluvad ka näiteks arvete pidamine kõigi sissetulekute ja väljaminekute üle, ettevõtte finantsdokumentatsioon ning finantstehingu aruannete säilitamine raamatupidamist reguleerivate õigusaktide järgi. (Millega tegeleb igapäevaselt raamatupidaja, 2015)

Seega puutuvad raamatupidajad oma töös kokku paljude tähtsate andmetega, eelkõige ettevõtte pangaandmed, paroolid, finantsseis, töötajate palgaandmed jne. Tuleb silmas pidada, kuidas tähtsaid dokumente töödelda ning samas kinni pidada isikuandmete kaitse reeglitest.
PriceWaterhouseCoopersi 2016.aasta aruanne näitab, et küberkuritegu on teisel kohal kõige rohkem teatatud majanduskuritegevustest, puudutades 32% organisatsioonidest. Sama uuring avaldab teise põhjuse muretsemiseks: see on selline salakaval oht, et 56% juhtudest ütlevad, et nad ei ole ohvrid. Paljud on sattunud ohtu tõenäoliselt eneseteadmata. (Heimdal Security. Andra Zaharia. (19.04.2016) 15 Steps to Maximize your Financial Data Protection.)
Seepärast on oluline teada Internetis andmete töötlemisel põhireegleid ning tähelepanekuid, et mitte sattuda küberkuriteo ohvriks. Alljärgnevalt on toodud kolm väga lihtsat sammu, mida tasub tähele panna:

1) Tuleb kontrollida linki enne, kui sellele „klikkida“ – Et teha kindlaks, et tegemist pole petmisega, siis tuleb tiirutada hiirekursorit kergelt üle lingi, et näha, kas see on suunatud õigustatud asukohta. Hüperlinkimine on tavaline praktika andmepüügirünnakutel ning see on alati parim viis varjatud URL-aadresside topeltkontrollimiseks.
2) Tuleb kontrollida faili enne, kui sellele „klikkida“ – Tähtis samm on kasutada veebibrauserit, mis ühendab reputatsioonipõhist tehnoloogiat. Selline tehnoloogia kasutab pilve punktisüsteemi, et analüüsida iga aplikatsiooni, mida on alla laetud ning näitab, kust see aplikatsioon pärineb. Analüüsi tulemusena veebisaidid, mis levitavad pahatahtlikku tarkvara – ning mis ei ole veel avastatud olemasolevate kaitsemehhanismide seast, on kergemini blokeeritavad.
3) Tuleb kasutada turvalisi veebisaite, et teostada finantstehinguid – kõik finantstehingud ning –operatsioonid peaksid olema kõrge järelevalve all. Selle kindlaks määramise jaoks tuleb vaadata veebiaadressist vasakule ja leida „*lock*“ ikoon. See näitab, et külastatakse krüpteeritud ja/või tõendatud veebisaiti. Teiseks tuleb veenduda, et veebiaadress algab https://. „s“ tuleneb sõnast „*secure socket layer“ (*turvasoklite kiht) ja see näitab, et ollakse ühendatud veebisaidiga, kus on krüpteeritud andmed.

(Heimdal Security. Andra Zaharia. (19.04.2016) 15 Steps to Maximize your Financial Data Protection)
Kui andmete ning failide vastuvõtmise turvalisus on tagatud, tuleb tähelepanu pöörata ka vastuvõetud dokumentide säilitamisele ning edastamisele. Kui hoida dokumente

„pilvesüsteemis“, siis sellel on kaks tähtsat kontseptsiooni, mida silmas pidada andmete säilitamisel, haldamisel ning edastamisel. Esimeseks, kuidas edastada faile turvaliselt arvutite vahel, ja teiseks, kuidas ja kus säilitada, hallata ning arhiveerida andmeid nii, et see oleks turvatud ning samas ka paindlik äritegevusele. Kui otsida internetist „pilve“ hoiustamise kohta, leiab sealt mitu „tasuta“ toodet/teenust, nagu Box.net, DropBox, Google Drive, Microsoft Skydrive ja Apple iCloud. Kõik sellised „tasuta“ teenused, mis tähendab seda, et teenust saab kasutada piiratud võimalustel tasuta ning pärast mida saab uuendada ja maksta teenuse eest juhul, kui on vajadus suurema koguse andmete edastamise või säilitamise järele. Enamikel juhtudel võib selliseid teenuseid kasutada tavaliseks kasutamiseks nagu piltide jagamine, personaalsete failide säilitamine ning sarnased mitte-ärilistel eesmärkidel kasutatavad andmed. Kui aga on vajadus kasutada teenust ärilistel eesmärkidel, siis tuleks otsida mõni rohkem turvatud ning täisfunktsionaalne lahendus. Parem lahendus dokumentide edastamiseks on kasutada pilvepõhist teenust, mis pakub krüpteerimist saatja üleslaadimisel ning dekrüpteerimist saaja allalaadimisel. (Are You Protecting Client Data When Sending Files Over the Internet?, 2012)

Ettevõtted saavad palju ise ära teha, et leevendada andmete riski sattumist ning hallata oma turvalisust. Selleks peaksid ettevõtted oma infoturvet analüüsima, rakendama ja harima.

Alljärgnevalt on toodud välja viis sammu, mida ettevõtted saavad teha, et tugevdada oma kaitsevõimet häkkerite eest:

1) Regulaarne turvalisus ning andmete hindamine – Ettevõtted ei saa kindlaks teha, kus nende võrgu turvaaugud asuvad ilma turvameetmete põhjaliku hindamiseta ning firma andmekasutuse harjumuste hindamiseta. Üksikust ülevaatusest aga paraku ei piisa. Firmad peaksid regulaarselt hindama nende turvalisuse strateegiaid ning teostama perioodilisi ülevaatusi, et aru saada, kuidas andmeid on kasutatud ning säilitatud kogu organisatsioonis. Kuigi see võib olla võimatu parandada kõike ühe korraga, kirjeldatud IT-strateegia aitab kaitsta ettevõtte võrku ning ette valmistada organisatsiooni mis tahes probleemidega, mis võivad kaasneda eelseisvate muudatustega.
2) Tehniline turvalisus – enamik äritegevusi toimub läbi andmete ülekande ja ettevõtte usaldusväärsus põhineb tema võimel kaitsta seda teavet. Igal organisatsioonil peab olema installitud oma võrku tasemel tulemüür. Anti-pahavara, antiviirus ning standardne e-maili filtreerimistarkvara on samuti oluline osa võrgu sissetungi kaitsmiseks. Andmete krüpteerimine, andmete varukoopiate tegemine, katastroofi

taastamiskava ja ettevõtte jätkuvuse lahendus saavad kaitsta firmat võrgurikkumiste eest.

3) Füüsiline kaitse – Töötajate kiipkaardid, külastajate kaelakaardid ja kontrollitud ligipääs kohtadele, kus hoitakse ärikriitilist informatsiooni võimaldavad kindlalt jälgida ja kontrollida liikumist kogu ettevõttes.
4) Administratiivne kaitse – Töötajate ligipääs tundlikele andmetele tõstab võrgu ohtu seadmise riski, on see tahtlik või mitte. Töötajad võivad juhuslikult tundlikud failid e-mailida kellelegi väljaspool organisatsiooni, seades ohtu firma turvalisuse ja maine. Sobiva juurdepääsukontrolli olemasolul saavad firmad kontrollida, kes näeb, kes saab muuta ning jagada andmeid kogu organisatsioonis. Sellised kontrollid peaksid olema regulaarselt uuendatud, et kajastada kõik rollide muutused organisatsioonis.
5) Töötajate koolitus ja väljaõpe – Kõige tähtsam element firma andmete turvalisuses on töötajate väljaõpe. Töötajate teadlikkus meetoditest, mida häkkerid kasutavad, et omandada teavet, on murranguline. Kui kõik protokollid ning poliisid on olemas ja töötaja klikib valele veebisaidile või avab vale faili, sest häkkerid olid meelitanud või sotsiaalse tehnikaga püüdnud andmeid, siis lõpptulemuseks on eesmärk kaitsta andmeid endiselt läbi kukkunud. On oluline sageli koolitada töötajaid turvalisuse teemadel ning rakendada parimat praktikat. Firma peaks töötama selle nimel, et tagada oma töötajate teadlikkus protokollidest nagu BYOD (Bring Your Own Device) ja mobiiliseadmete kasutamis-, krüpteerimis- ja salasõnapoliisidest jne. Esimene samm küberkriminaalide vastu on aidata töötajatel mõista riske ning kuidas neid leevendada.

Ettevõtted kasutavad palju tehnikaid, et säilitada, laadida ja levitada andmeid nii endale kui ka klientidele. Firmadele on oluline kaitsta oma klientide andmeid sama palju kui firma mainet, ja need kasulikud ja kergesti teostatavad meetodid võivad mõjutada palju – tulemuseks võib olla andmete turvalisus või katastroof. (How Accounting Firms Can Protect Their Data, And Their Clients) Maailma arenemisega areneb ka igasugune pahavara ning muutub aina targemaks ja nutikamaks. Seepärast on oluline regulaarselt hinnata ettevõttes hetkeolukorda, kas on võimalik leida mingisuguseid turvaauke või mitte. Uus andmekaitsemäärus aitab ka meelde tuletada ning taastähtsustada andmekaitse olulisust, et ettevõtted olulisemad võimalikud ohud ning riskid üle vaatavad ning selle ennetustööga tegeleksid.

## 2.3. Andmekaitsemäärus raamatupidajatele

Tänases infoühiskonnas saab aina suuremaks probleemiks see, et üksikisikul puudub kontroll Internetis tema kohta leiduvate andmete osas. Seepärast koostati 2016.aasta kevadel Euroopa Parlamendi ja Nõukogu määrus nr 2016/679, mis on otsekohalduv kõikidele liikmesriikidele. Selle peamisteks eesmärkideks oli kehtestada ühtne õigusnormide kogum, mis kehtiks kogu Euroopa Liidus. Samuti keskendub määrus üksikisiku turvalisusele: üksikisikutele antakse suurem kontroll ja rohkem teavet nende andmete töötlemise kohta. (Elis Prangli. Andmekaitse reform – kes omab minu andmeid. Majandus24. 2016)

24.mail 2016.aastal avaldatud andmekaitsemääruses esitatud nõuded lähtuvad sellest, et andmeid käideldakse põhjendatult ja kindlatel reeglite järgi (andmesubjekti kirjalik nõusolek, seadusest tulenevad põhjused või subjektiga sõlmitud leping). Rangemad nõuded puudutavad organisatsioone, mis tegelevad andmesubjektide süstemaatilise ning regulaarse jälgimisega (siia alla võivad liigituda ka näiteks kasutajate profileerimisega tegelevad ettevõtted). Delikaatsete isikuandmete (näiteks rassi, usuliste, seksuaalsete eelistuste) käitlemine on lubatud vaid erijuhtudel ning andmesubjekti nõusolekul. Olulisematest muudatustest saab välja tuua järgmised punktid:

1) Andmesubjektil on õigus saada informatsiooni enda kohta kogutud andmetest ja keelduda teenuse pakkumiseks mittevajalike andmete üleandmisest. Andmesubjekt peab mõistma, milleks tema andmeid on tarvis ning mida nendega tehakse.
2) Andmesubjektil on õigus nõuda oma andmete kustutamist, kui neid ei ole tarvis koguda teenuse osutamise eesmärgil.
3) Juhul, kui andmeid töödeldakse andmesubjekti kirjaliku nõusoleku alusel, tuleb arvestada, et subjektil on õigus nõusolek igal ajal tühistada.
4) Turvaintsidentidest, mis põhjustavad isikuandmetega seotud rikkumise, tuleb teavitada keskset andmekaitseorganit esimesel võimalusel ning teatud juhtudel ka mõjutatud andmesubjekte. Isikuandmetega seotud rikkumine on defineeritud kui tahtmatu või õigusvastane andmete hävitamine, kadu, muutmine, loata avaldamine või neile juurdepääsu võimaldamine. Turvaintsidentidest teavitamata jätmine või teavitamisega põhjendamatult viivitamine võib kaasa tuua trahvi.

5) Andmekäitleja peab andmesubjekti teavitama, kui tema andmeid otsustatakse edastada kolmandale osapoolele. Samas on andmesubjektil õigus paluda oma andmed edastada kolmandale osapoolele, näiteks mõnele teisele teenusepakkujale.
6) Isikuandmete käitlemisega seotud protsesside puhul, millega võib kaasneda suurem oht andmesubjekti õigustele, tuleb teha mõjuanalüüs. Mõjuanalüüsid aitavad tuvastada võimalikke riske ja kasutusele võtta asjakohaseid turvameetmeid. Mõjuanalüüside olemasolu ja täielikkust võib kontrollida järelevalveasutus.
7) Kui andmekäitleja puhul on tegemist avaliku sektori üksusega, ettevõttega, kus töötab vähemalt 250 inimest, või ettevõttega, kus andmekäitlemine eeldab regulaarset ja süstemaatilist andmesubjektide monitoorimist, tuleb organisatsioonis luua andmekaitseametniku roll.

(Andmekaitsemäärus – Mis see on ja mida tähele panna, 2016)

Väikesed ja keskmise suurusega ettevõtted peavad andmeid säilitama ainult juhul, kui andmetöötlus:

- On korrapärane;
- Kujutab ohtu inimeste õigustele ja vabadustele;
- Puudutab delikaatseid isikuandmeid või karistusregistri teavet.

Eeskirjade täitmist jälgib kohalik andmekaitseasutus, mille tööd koordineeritakse Euroopa Liidu tasandil. Mitterikkumisega kaasneb trahv. Vastavalt rikkumise suurusele, ulatusele ning tõsidusele võib rikkujat ees oodata hoiatus, noomitus, andmetöötluse peatamine või trahv (kuni 20 miljonit eurot või 4% ettevõtte aastakäibest). (Isikuandmete kaitse üldmäärus. Andmekaitse Inspektsioon. 20.03.2017). Suuremad trahvid aitavad motiveerida ettevõtteid vastavaid muudatusi ellu viima, kuid tegelikult tuleb mõista, et muudatused on olulised nii ettevõtte turvalisuse kui isikute, kelle andmeid töödeldakse, seisukohalt.

### 2.3.1. Vaikimisi ja lõimitud andmekaitse

Andmekaitse põhimõtete rakendamine ei ole ainult õigusaktide järgimine. Andmetöötlejad peavad olema ka kursis igapäevaste tehnoloogia arengusuundadega, lisanduvate uute toodete ja teenustega. Mis puudutab andmetöötlustoiminguid, siis need on muutunud automaatseks. Inimene sekkub üldjuhul ainult siis, kui teenus ei toimi ja on vaja tuvastada viga. Andmekaitse üldmääruse põhimõte ning eesmärk on see, et andmetöötlustoimingute eest ei saa vastutust panna kellelegi teisele. Isikuandmete töötleja ise peab omama täielikku ülevaadet toimingute eesmärgistamisel, privaatsusmõjude hindamisel ning pädevate turvameetmete rakendamisel. Andmetöötlus peab inimeste jaoks olema läbipaistev, õiglane ning põhjendatud. Seetõttu on andmekaitse üldmäärusesse (artikkel 25) lisatud lõimitud ja vaikimisi andmekaitse põhimõte. Põhimõtete vaatenurk on see, et inimeste eraelu ei saa tagada ainult õigusnormistikule vastavuse abil, vaid eraelu puutumatus peab tulenema vaikimisi organisatsiooni töökorraldusest. Nii organisatsiooni tegevuspõhimõtted ja äritavad kui ka IT taristu kavandamine, arendamine ja haldamine on kohad, millele organisatsiooni andmekaitseline alusmüür toetub. Lõimitud andmekaitse printsiipe võib rakendada igat tüüpi isikuandmete puhul. Rangemat tähelepanu nõuavad aga tundlikumad isikuandmed, nagu näiteks inimese tervise- , finants- või sideandmed. Järgnevalt on toodud 7 põhimõtet, mis kirjeldavad lõimitud andmekaitse rakendamise eesmärke, milleks on üldiselt eraelu puutumatuse kindlustamine ning organisatsioonide jätkusuutliku konkurentsieelise saavutamine:

1) Ennetav, mitte tagantjärele reageeriv; ärahoidev, mitte parandav – Lõimitud andmekaitset iseloomustavad pigem ennetavad kui tagajärgedega tegelevad meetmed. See näeb ette ja hoiab ära eraelu riivamise juba enne nende toimumist. Lõimitud andmekaitse ei oota niikaua, kuni ohud eraelule tegelikkuseks saavad. See ei paku ka ravimit juba toimunud rikkumistele – selle eesmärgiks on nende toimumist ära hoida. Kui rikkumine on juba toimunud, siis on hilja vastavaid muudatusi ellu viia. Lühidalt, lõimitud andmekaitse tuleb enne ja mitte pärast tegusid.
2) Andmekaitse kui püsiseisund – Lõimitud andmekaitse püüdleb eraelu puutumatuse maksimaalse taseme saavutamise poole, kindlustades isikuandmete automaatse kaitse kõikides IT-süsteemides ja äritegevustes. Üksikisik ei pea oma privaatsuse säilitamiseks ise mitte midagi tegema – see olgu süsteemi vaikimisi sisse ehitatud.

3) Andmekaitse kui süsteemi ülesehituse osa – Lõimitud andmekaitse on sisse ehitatud IT-süsteemide disaini ja arhitektuuri ning äritegevusse. Selle tulemusena saab andmekaitsest tuumfunktsionaalsuse põhiosa. Andmekaitse on süsteemi lõimitud, ilma sealjuures funktsionaalsust kahandamata.
4) Täielik otstarbekohasus – Lõimitud andmekaitse soovib kõik seaduslikud huvid koondada nn pluss-summa mängu, kus võidavad mõlemad pooled, mitte aga iganenud null-summa lähenemise abil, kus tehakse ebavajalikke kompromisse. Lõimitud andmekaitse väldib võlts-vastandusi, nagu privaatsus vs julgeolek, näidates, et korraga on võimalik saavutada mõlemaid.
5) Algusest lõpuni turvaline – Lõimitud andmekaitse, mis on süsteemi sisse ehitatud enne esimeste andmete kogumist, laieneb turvaliselt kogu kõnealuste andmete täielikule elueale. See põhimõte kindlustab kõigi andmete turvalise säilitamise ning seejärel töötlemise lõppedes nende turvalise hävitamise sobival viisil. Seega kindlustab lõimitud andmekaitse rakendamine informatsiooni turvalise käsitsemise kogu selle eluea ulatuses nn hällist kuni hauani.
6) Nähtav ja läbipaistev – Lõimitud andmekaitse tagab kõigile osapooltele, olgu tegemist mis tahes äritegevuse või tehnoloogiaga, sõltumatu kontrolli. Süsteemi osad ja tegevus jääb ühtmoodi nähtavaks ja läbipaistvaks nii selle kasutajatele kui ka levitajatele.
7) Tuleb austada kasutaja eraelu – eelkõige nõuab lõimitud andmekaitse selle koostajailt ja kasutajailt üksikisiku huvide seadmist esmatähtsaks, pakkudes selliseid meetmeid nagu andmekaitse vaikimisi seadeid, asjakohaseid hoiatusi ning julgustavaid kasutajasõbralikke valikuid.

(Vaikimisi ja lõimitud andmekaitse. Andmekaitse Inspektsioon. 13.03.2017)

Teise mõistena toob üldmääruse artikkel 25(2) sisse vaikimisi andmekaitse. See tähendab, et vaikimisi tuleks töödelda ainult neid isikuandmeid, mis on vajalikud töötlemise konkreetse eesmärgi saavutamiseks. See kehtib kogutud isikuandmete hulga, nende töötlemise ulatuse, nende säilitamise aja ja nende kättesaadavuse suhtes. Seega isikuandmeid ei tohi töödelda valimatult ja vaikimisi, ilma asjaomase inimese sekkumiseta. Sisuliselt tähendab see nii nimetatud opt-in põhimõtte rakendamist ehk toodete ja teenuste algseaded peavad võimaldama inimesele maksimaalset kaitset.

(Vaikimisi ja lõimitud andmekaitse. Andmekaitse Inspektsioon. 13.03.2017)

Näitena võib tuua mitmeid olulisi aspekte, mida inimesed tihti ise tähele ei pane, kuid siiski on olulised:

- uue nutiseadme soetamisel ja sisse lülitamisel ei tohiks olla WiFi, sinihammas või asukohateenus vaikimisi aktiveeritud. Kasutaja lülitab need ise sisse, kui selleks vajadus tekib;
- nutirakendused ei tohi küsida valimatult juurdepääsu kasutaja seadme funktsioonidele ja sisule. Lisamugavusi tagavate õiguste piiramine ei ole takistuseks rakenduse põhifunktsioonide kasutamisel;
- veebilehitseja turvaseaded ei tohiks vaikimisi võimaldada inimese veebikasutuse ulatuslikku jälgimist. Olgu selleks siis kas küpsiste seaded, keelekasutuse- või kasutusprofilli meeldejätmise seaded;
- jaepoodide lojaalsusprogrammiga ühinemiseks ei tuleks vaikimisi küsida klientide elukoha aadressandmeid. Piisab linna, maakonna täpsusest. Vastavad andmed on asjakohased juhul, kui klient on nõus saama näiteks toodete pakkumisi. Sama kehtib ka e-posti või telefoninumbri kohta;
- e-pood ei peaks küsima mitteregistreerunud klientidelt, kes teevad e-poes impulssostu ja tellivad toote pakiautomaati, aadressandmeid. Need on vajalikud juhul, kui kasutatakse näiteks kullerteenust;
- suhtlusrakendustes või sotsiaalmeedia teenustes peab olema vaikimisi andmete jagamine piiratud. Kasutaja ise otsustab, kellele ja millised andmeid ta kättesaadavaks teeb.

(Vaikimisi ja lõimitud andmekaitse. Andmekaitse Inspektsioon. 13.03.2017)

Uue andmekaitsemääruse üks eesmärkidest on tuua andmekaitse inimestele lähemale, et nad ise oleksid kursis, kuhu ning milleks nende andmeid töödeldakse. Eelnevad punktid näitavad väga hästi seda, et andmekaitsemäärus on väga kasutajasõbralik ning „tavaline“ inimene võib samuti hakkama saada oma andmete turvamisel. Ettevõtted ei saa enam vaikimisi salvestada klientide andmeid, mida nad küsivad tulevikus ärakasutamise eesmärgil. Sellele peab olema mõjuv põhjus.

### 2.3.2. Osapoolte kaasatus

Soovitatav on isikuandmete kaitse muuta kasutajatele võimalikult automaatseks, näiteks süsteemidesse ja protsessidesse sisse ehitada, sest see lihtsustab määruse nõuetega vastavuse tagamise protsessi. Olulise rolli võivad saada (pea)raamatupidajad ja finantsjuhid, kes nii mõneski ettevõttes on formaalselt või sisuliselt määratud vastutama ka suuremate regulatsioonidega vastavuse tagamise eest. Olenevalt sellest, millist kompetentsi ettevõttel majasiseselt leidub, võib vajalik olla kaasata ettevõttevälist (näiteks juriidilist või IT-alast) abi. Osapoolte vähene kaasatus on esmane ohumärk: selle tulemuseks võib olla nõuete juurutamise tegevuskava, mis eesmärke ja andmete käitlemisega seotud riske piisavalt ei arvesta. (Maarja Heinsoo, Märten Padu. Andmekaitsemäärus – Mis see on ja mida tähele panna. 2016)

Määruses esitatud isikuandmete definitsioon on lai: isikuandmed on kõik füüsilise isikuga seostatavad andmed. Seega puudutab määrus ka täiesti „tavalisi“ ettevõtteid, mis spetsiaalselt oma klientide või muude isikute profileerimise või monitoorimisega ei tegele. Isikute kohta käivaid andmeid leidub ju mujalgi, näiteks raamatupidamisinfos. Nii võib näiteks ehitusettevõtte arvete ja pangatehingute alusel teha kindlaks, kellele, mida, kuhu ja mis summa eest rajati ning kes selle eest maksis. Konkreetselt jaemüügis kujutavad omaette riskikohta kliendikaardid, mille abil võib olla võimalik siduda konkreetne isik tema ostuajalooga, mida ettevõtted saavad ära kasutada äri edenemise eesmärgil. (Maarja Heinsoo, Märten Padu. Andmekaitsemäärus – Mis see on ja mida tähele panna. 2016)

Infosüsteemid on tänapäeva äride lahutamatu osa. Aina suurenev süsteemide integreeritus (näiteks kliendihaldustarkvara ja finantstarkvara ühendamine) tähendab, et kitsa valdkonna töötajal on aina keerulisem omada ülevaadet andmekogumitest ja andmete liikumisest. Erinevate protsesside eest vastutavate isikute koostöös on parem kaardistada, kus isikuandmed tekivad, kuhu ja kelleni need jõuavad, ning mõista, kas nende käitlemine on määruse tingimuste valguses õigustatud. (Maarja Heinsoo, Märten Padu. Andmekaitsemäärus – Mis see on ja mida tähele panna. 2016)

Andmekaitse üldmääruse üks eesmärke on andmetöötleja vastutustundlikkus. See tähendab, et andmetöötlejad peavad olema võimelised aru saama kogu andmetöötlusahelast, tagades inimeste suhtes seadusliku, õiglase ning läbipaistva andmetöötlusprotsessi. Selle nõude täitmist aitab see, kui andmetöötleja dokumenteerib ja säilitab kõik andmed tema

vastutusalasse kuuluvate isikuandmete töötlemise toimingute kohta. Andmetöötlustoimingute registreerimine aitab andmetöötlejatel paremini mõista isikuandmete kaitse olemust, kaardistada oma tegevusi ning paremini planeerida isikuandmete kaitsega seonduvat. See aitab kaasa inimeste põhiõiguste ning -vabaduste parema kaitse tagamisele. Samuti tähendab see ka infosüsteemides logide pidamist andmete kogumise, muutmise, lugemise, avalikustamise, edastamine, ühendamise ja kustutamise kohta. Seetõttu sätestab andmekaitse üldmääruse artikkel 30 andmetöötleja kohustuse registreerida kõik isikuandmete töötlemise toimingud. Üldmääruse artikli 30(1) kohaselt peab register sisaldama järgmisi kandeid:

- vastutava töötleja ning asjakohasel juhul kaasvastutava töötleja, vastutava töötleja esindaja ja andmekaitseametniku nimi ja kontaktandmed;
- töötlemise eesmärgid;
- andmesubjektide kategooriate ja isikuandmete liikide kirjeldus;
- vastuvõtjate kategooriad, kellele isikuandmeid on avalikustatud või avalikustatakse, sealhulgas kolmandates riikides olevad vastuvõtjad ja rahvusvahelised organisatsioonid;
- kui isikuandmeid edastatakse kolmandale riigile või rahvusvahelisele organisatsioonile, siis andmed selle kohta koos asjaomase kolmanda riigi või rahvusvahelise organisatsiooni nimega, ning juhul, kui tegemist on artikli 49 lõike 1 teises lõigus osutatud edastamisega, siis sobivate kaitsemeetmete kohta koostatud dokumendid;
- võimaluse korral eri andmeliikide kustutamiseks ette nähtud tähtajad;
- võimaluse korral artikli 32 lõikes 1 osutatud tehniliste ja korralduslike turvameetmete üldine kirjeldus.

(Töötlustoimingute registreerimine. Andmekaitse Inspektsioon. 27.02.2017)

Isikuandmete töötlemise käigus võib paraku esineda turvanõuete rikkumisi, mis võivad põhjustada edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurepääsu. Sellist turvanõuete rikkumist käsitleb andmekaitse üldmäärus isikuandmetega seotud rikkumisena.

Andmekaitsemäärus nõuab ka turvanõuete rikkumistest teavitamist. Seni pidid isikuandmetega seotud rikkumistest teavitama Andmekaitse Inspektsiooni kõik üldkasutatava elektroonilise sideteenuse osutajad. Teatud juhtudel tuli teavitada ka teenust kasutavaid üksikisikuid. Vastav kohustus tulenes Euroopa Komisjoni määrusest (EL) 611/2013. 25. mail

2018 kehtima hakkava andmekaitse üldmääruse artikli 33 kohaselt laieneb rikkumisteadete edastamise kohustus kõikidele isikuandmete töötlejatele. (Rikkumisteated. Andmekaitse Inspektsioon. 13.02.2017)

Kui isikuandmete vastutav töötleja on tuvastanud isikuandmetega seotud rikkumise, mis tõenäoliselt kujutab endast ohtu füüsiliste isikute õigustele ja vabadustele, peab sellest teavitama pädevat järelevalveasutust. Eestis on selleks Andmekaitse Inspektsioon. Vastavalt üldmääruse artiklile 33(1) peab teavitamine toimuma põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul pärast rikkumise teada saamist. Seda siis ka juhul, kui kõik rikkumise põhjused ei ole veel teada või pole lõplikult selge näiteks rikkumist puudutavate isikute arv. Ühelt poolt annab üldmäärus andmetöötlejale kaalutlusõiguse hinnata, millal on tegu ohuga füüsiliste isikute õigustele ja vabadustele. Teisalt selgitavad määruse põhjenduspunktid 75, 76 ja 85, et erineva tõenäosuse ja tõsidusega ohud füüsiliste isikute õigustele ja vabadustele võivad tuleneda isikuandmete töötlemisest, mille tulemusel võib tekkida füüsiline, materiaalne või mittemateriaalne kahju, eelkõige juhtudel, kui:

- töötlemine võib põhjustada diskrimineerimist, identiteedivargust või -pettust, rahalist kahju, maine kahjustamist, ametisaladusega kaitstud isikuandmete konfidentsiaalsuse kadu, pseudonümiseerimise loata tühistamist või mõnda muud tõsist majanduslikku või sotsiaalset kahju;
- andmesubjektid võivad jääda ilma oma õigustest ja vabadustest või kontrollist oma isikuandmete üle;
- töödeldakse isikuandmeid, mis paljastavad rassilist ja etnilist päritolu, poliitilisi vaateid, religioosseid või filosoofilisi veendumusi ning ametiühingusse kuulumist, samuti geneetilisi andmeid, andmeid tervise, seksuaalelu ning süüteoasjades süüdimõistvate kohtuotsuste ja süütegude ning nendega seotud turvameetmete kohta;
- hinnatakse isiklikke aspekte (nt isiku vaated, seisukohad, isikuomadused, sotsiaalne staatus), eelkõige töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste või huvide, usaldusväärsuse või käitumise, asukoha või liikumisega seotud aspektide analüüsimisel või prognoosimisel, et luua või kasutada isiklikke profiile;
- töödeldakse kaitsetute füüsiliste isikute, eriti laste isikuandmeid;
- töötlemine hõlmab suurt hulka isikuandmeid ning mõjutab paljusid andmesubjekte.

Andmesubjekti õigustele ja vabadustele tekkiva ohu tõenäosus ja tõsidus tuleks teha kindlaks lähtudes andmetöötluse laadist, ulatusest, kontekstist ja eesmärkidest. Ohtu tuleks hinnata

objektiivse hindamise põhjal, millega tehakse kindlaks, kas andmetöötlustoimingutega kaasneb oht või suur oht. (Rikkumisteated. Andmekaitse Inspektsioon. 13.02.2017)
Uus andmekaitsemäärus kaasab mitmeid isikuid ning nõuab ettevõttes palju tähelepanu. Kui avaliku sektori ettevõttes töötab üle 250 inimese või ettevõttes monitooritakse andmesubjekte regulaarselt ja süstemaatiliselt, siis tuleb ettevõttes luua lausa andmekaitseametniku ametikoht. Paljudele ettevõtetele on see suur ettevõtmine, kuid eesmärgikohaselt tasub see kindlasti ennast ära.

### 2.3.3. Turbehügieen on oluline

Andmetöötlejaile suunatud saktsioonide (vähemalt teoreetiline) kasv võib suurendada kuritahtlikke ründeid seni vähem huvi pakkunud valdkondade ettevõtete andmete vastu. Infoturbehügieeni hoidmine ei ole ammugi enam kindla tegevusharu (näiteks pangandus, tervishoid) probleem. Turbehügieeni tagamisel tasub muu hulgas läbi mõelda alljärgnevad küsimused:

1) Kas ligipääs andmetele on lubatud vaid selleks ettenähtud isikutele tööülesannetega piiratud ülatuses? Kas kasutusel on individuaalsed kasutajakontod? Näiteks finantstarkvarade (kui ka muude arvutisüsteemide) puhul peaks kasutajaõiguste jagamisel järgima vähimate õiguste põhimõtet, mille kohaselt antakse töötajale süsteemidesse võimalikult vähe ligipääsuõigusi. Andmete turvalisuse seisukohast võetuna on loomulik, et kõikidel tarkvara kasutajatel ei ole näiteks pearaamatupidaja õigusi. Täiendavalt ei ole mõistlik kasutada ka ühiskontosid.
2) Kas töötajatelt nõutakse tugevate paroolide kasutamist? Parooliga turvamata kasutajakonto on andmete lekitaja jaoks nagu lukustamata välisuks. Selliseid kasutajakontosid on lihtne ära kasutada, et pääseda ligi näiteks ettevõtte klientide isikuandmetele.
3) Kas ettevõtte töötajad on kursis infoturbeohtudega? Tundmatu mälupulga ühendamine arvutiga, väidetavalt tuttavalt saabunud e-kirjas sisalduva manuse avamine või mõnel veebilehel kahtlasel uudis- või reklaamlausel klikkamine võib ohtu seada terve kontori võrgu ja andmete turvalisuse.
4) Kas isikuandmeid säilitatakse muudest andmetest eraldi? Kas tundlikke andmeid hoitakse/edastatakse krüpteeritult? Juhul kui häkitakse sisse ühte andmebaasi, siis

informatsiooni segregeerituna hoidmise korral ei saa häkker enda valdusse kogu andmestikku. Andmete krüpteerituna hoidmine aitab tagada, et need ei satuks kuritahtlike andmelekitajate kätte lihtsasti loetaval kujul.

5) Kas andmetest tehakse regulaarseid varukoopiaid? Kas andmete varukoopiast taastamist testitakse? Seoses sellega, et andmesubjektil on õigus igal ajal teada saada, milliseid andmeid tema kohta on kogutud, tuleks veenduda, et säärase info jagamine ei takerduks, kui põhilised andmekandjad peaksid ootamatult töötamast lakkama.

(Andmekaitsemäärus – Mis see on ja mida tähele panna, 2016)

Praeguseks ei ole veel välja kujunenud kindlaid praktikaid, kuidas saavutada seda, et isikuandmete kaitse oleks vastavuses üldmäärusega. See, milliseid nüansse arvesse võtta, sõltub paljuski ettevõtte eripärast. Vettpidava lähenemise kujundamine on kindlasti töömahukas, küll aga võiksid määrusesse sisse kirjutatud olla kõrgemad trahvid motiveerida regulatsioonile tähelepanu pöörama ja vajaduse korral eri valdkondade spetsialiste kaasama. (Andmekaitsemäärus – Mis see on ja mida tähele panna, 2016)

Seoses andmekaitsemääruse jõustumisega on erinevad organisatsioonid koostanud ka mitmeid koolitusi, et ettevõtetele määruse jõustumisel vajaminevaid muudatusi paremini selgitada ning lihtsamaks teha. Erinevaid koolitusi on toimunud juba 2016.aasta sügisest, näiteks septembris toimunud Rahvakooli õppepäev, (Rahvakool. ÕPPEPÄEV: Uus isikuandmete kaitse määrus ja andmekaitsereform. 2016), FECC (Finnish-Estonian Chamber of Commerce) hommikuseminar „Euroopa Liidu andmekaitse määrus – mõju ettevõtte protsessidele ning süsteemidele“, (FECC. hommikuseminar „Euroopa Liidu andmekaitse määrus – mõju ettevõtte protsessidele ning süsteemidele“. 2017) Äripäeva veebiseminar „Pilvelahendused ja uus andmekaitsemäärus“, (Äripäev. Pilvelahendused ja uus andmekaitsemäärus. 2017) Excellence koolitus- ja arenduskeskuse koolitus „Isikuandmete töötlemine organisatsioonis: Euroopa Liidu andmekaitsereformi määruse muudatused“. (Excellence koolitus- ja arenduskeskus. Isikuandmete töötlemine organisatsioonis: Euroopa Liidu andmekaitsereformi määruse muudatused. 2017) Kindlasti toimub sarnaseid koolitusi veelgi ning see teema on aktuaalne veel pikka aega.

24.mail 2016.aastal avaldatud andmekaitse määruses keskendutakse sellele, et andmete käitlemine oleks põhjendatud ning et seda tehakse kindlatel alustel ning eesmärkidel. Suurem osa määruses esitatud põhimõtetest ning nõuetest on kehtivas Eesti seaduses juba olemas. Suuremad uuendused on senisest kõrgemad trahvid, andmete kolmanda osapoolega jagamise

põhimõtted, mõjuanalüüside tegemise kohustus ja (teatud juhtudel) andmekaitseametniku rolli loomise kohustus. Ettevõtte seisukohalt võivad olulise rolli saada (pea)raamatupidajad ja finantsjuhid, vaadates üle ettevõtte hetkeolukorra ning tehes vajadusel vastavaid muudatusi. Keerukust lisab asjaolu, et määrus puudutab ka täiesti „tavalisi“ ettevõtteid, mis spetsiaalselt oma klientide või muude isikute profileerimise või monitoorimisega ei tegele. Isikute kohta käivaid andmeid leidub mujalgi, näiteks puiduettevõtte raamatupidamisinfos. Selleks tuleb tagada piisavalt turvaline süsteem andmete kogumiseks, säilitamiseks ja edastamiseks.

# 3. UURING ANDMEKAITSEST EESTI ETTEVÕTETE RAAMATUPIDAJATEGA

## 3.1. Uuringu metoodika, andmete kogumine ja valim

Bakalaureusetöö eesmärk oli välja selgitada, missugused on raamatupidajate teadmised andmekaitsest ning kui palju neid teadmisi ettevõtetes rakendatakse. Uurimisülesannete täitmiseks kasutas autor nii kvalitatiivset kui ka kvantitatiivset metoodikat. Nii kvalitatiivse kui ka kvantitatiivse analüüsi küsimused on koostatud eelnevalt välja toodud teooria põhjal. Kvalitatiivsel analüüsil viidi läbi kolm intervjuud, mis toimusid novembris 2016. Intervjueeritavate kriteeriumiks oli, et intervjueeritavad peavad olema raamatupidajad, kes hetkel töötavad mõnes ettevõttes. Intervjuus osales neli raamatupidajat, kellest kõik olid naised. Üks nendest töötab mikroettevõttes, kahega tehti ühine intervjuu keskettevõttest ning ühega suurettevõttest. Esimene intervjueeritavatest oli raamatupidaja mikroettevõttest nimega Tarknet OÜ, teised kaks raamatupidajat keskettevõttest nimega AS R-Kiosk Estonia ning kolmas suurettevõttest nimega ABB AS. Intervjuude kestvuseks oli keskmiselt 15 minutit. Enne intervjueerimist küsiti luba intervjuu salvestamiseks diktofoniga. Kõigilt intervjueeritavatelt saadi ka nõusolek. Mikroettevõtte raamatupidajaga viidi intervjuu läbi telefoni teel, teised intervjuud ettevõtte enda ruumides. Intervjuu käigus esitati peamiselt avatud küsimusi ning samuti ka täpsustavaid alaküsimusi. Vastused olid ammendavad ning nende põhjal oli võimalik järeldusi teha. Intervjuuga sooviti uurida, kas ja kui palju on raamatupidajad teadlikud andmekaitsest ning kui palju nad neid teadmisi oma igapäevatöös kasutavad.

Pärast intervjuude läbiviimist koostati transkriptsioon, et selle põhjal saadud andmeid edasi uurida. Intervjuude küsimused ning vastuste transkriptsioonid on esitatud täies mahus käesoleva töö lisades 1-4. Transkriptsiooni põhjal koostati tabel, et leida, milliseid sarnasusi või erinevusi on intervjueeritavad kasutanud küsimustele vastamisel ning kas vastustes on läbiv sarnane teema. Intervjueeritavad olid väga erineva suuruse ning valdkonnaga ettevõtetest. Firmade üldandmed on esitatud tabelis 1.

**Tabel 1. Vaatlusalusel olevate organisatsioonide üldandmed**

| Organisatsioon | Töötajate arv | Tegevusala |
|---|---|---|
| TarkNet OÜ | -9 | Raamatupidamisteenus |
| AS R-Kiosk Estonia | ~250 | Esmatarbekaupade jaemüük |
| ABB AS | ~1300 | Energeetika ja automaatika |

Allikas: autori koostatud, aluseks ettevõtete koduleheküljed

Kvantitatiivsel analüüsil palus autor raamatupidajatel või sarnases valdkonnas töötavatel isikutel vastata anonüümsele küsimustikule, mis oli koostatud võttes arvesse teooriast lähtudes üldisi ohte andmekaitses ning ka uuendusi seoses andmekaitsemäärusega, mis hakkab 2018.aasta maist kehtima. Uuringu läbiviimiseks koostati küsimustik elektrooniliselt keskkonnas Google Form (küsimustiku link: https://goo.gl/forms/PWj33zpmCSKCQUFI2) ning edastati raamatupidajatele Facebooki suletud grupis nimega „Raamatupidamine, majandusarvestus ja maksundus“, samuti jagati küsimustikku Eesti Raamatupidamis- ja maksuinfoportaalis www.rmp.ee. Ankeetküsitlus on toodud välja käesoleva töö lisades 5. Küsimustik koosnes kolmest osast: kuuest valikvastustega küsimusest, viiest likert skaalal põhinevast küsimusest ning kolmest küsimusest, mis olid vastaja enda kohta. Esimese osa eesmärk oli hinnata ettevõtete turvalisust, kus vastajad töötavad, teises osas uuriti vastajate teadlikkust andmekaitsest ja selle olulisusest. Kolmanda osa eesmärk oli profileerida vastajat, et hiljem analüüsida tulemusi vastavalt vajadusele (ettevõtte suuruse, vastajate vanuse, ametinimetuste järgi).

Uuring toimus vahemikus 04.05.2017 – 10.05.2017. Küsimustikule vastas 74 raamatupidajat või sarnases valdkonnas töötavat inimest. Ankeetküsitlusele vastajad olid väga erineva suurusega ettevõtetest ning samuti olid vastajad erinevate ametinimetustega, seega nende kogemus ka andmekaitsest oli erinev. Vastajate ning ettevõtete üldandmed on toodud välja tabelis 2.

**Tabel 2. Andmed ettevõtte suuruse, vastajate vanuse ning ametinimetuse kohta**

| **Töötajate arv** | **Vastajate arv** |
|---|---|
| 1-9 | 27 |
| 10-49 | 17 |
| 50-249 | 10 |
| 250- | 9 |
| **Ametinimetus** | |
| Raamatupidaja | 34 |
| Audiitor | 2 |
| Assistent | 9 |
| Juht | 12 |
| Vanemraamatupidaja | 8 |
| **Vanus** | |
| 18-28 | 25 |
| 29-39 | 15 |
| 40-50 | 21 |
| 50- | 7 |

Allikas: Autori koostatud, aluseks võetud küsimustiku vastuseid.

36% vastajatest (27 vastajat) töötas mikroettevõttes, 22% vastajatest (17 vastajat) töötas väikeettevõttes, 14% vastajatest (10 vastajat) töötasid keskettevõttes ning 12% vastajatest (9 vastajat) töötasid suurettevõttes. 46% vastajatest (34 vastajat) olid raamatupidajad, 3% vastajatest (2 vastajat) olid audiitorid, 12% vastajatest (9 vastajat) olid finantsvaldkonna assistendid, 16% vastajatest (12 vastajat) olid finantsvaldkonna juhid ning 11% vastajatest (8 vastajat) olid vanemraamatupidajad. 34% vastajatest (25 vastajat) olid vanuses 18-28, 20% vastajatest (15 vastajat) olid vanuses 29-39, 28% vastajatest (21 vastajat) olid vanuses 40-50 ning 9% vastajatest (7 vastajat) olid üle 50 aasta vanused.

Analüüsil kasutati kõigi vastajate vastuseid. Andmed olid esitatud MS Excel tabelis. Esmalt tuli korrastada andmed, seejärel kodeerida vastused, et läbi viia analüüs ning vastustest leida järeldus. Kvantitatiivsel andmeanalüüsil kasutati kirjeldavat statistikat. Analüüsi üks eesmärk oli leida, kui hästi vastajad hindavad oma ettevõtte turvalisust andmekaitse seisukohalt ning kui turvaline ettevõte tegelikult oli. Teiseks eesmärgiks oli leida, kui hästi vastajad hindavad oma teadmisi andmekaitsest ning kui head need teadmised tegelikult olid.

## 3.2. Uuringu tulemused

Intervjueeritavatelt küsiti kokku kuus põhiküsimust. Kaks küsimust käisid ettevõtte andmekaitse kohta ja ülejäänud neli andmekaitsest üleüldiselt. Vastustel hinnati intervjueeritavate teadlikkust andmekaitsest ning teadlikkust üleüldiselt ettevõttes. Intervjueeritavad olid nõus vastama kõikidele küsimustele ja vastuste mõtlemiseks palju aega ei kulunud.

Esimene vastaja mikroettevõttest on kuulnud andmekaitsest küll, kuid ei pea seda väga oluliseks, kuna tegemist on nii väikse ettevõttega ning pakutakse teenust teistele ettevõtetele, siis ollakse pigem paindlikud oma klientidele ja tegutsetakse vastavalt nende soovidele. Intervjueeritav arvab ka, et üksi töötades kodukontoris on andmed piisavalt turvaliselt, et keegi ei peaks neile ligi pääsema. Käesoleva töö autori arvates peaks ettevõttes rohkem rõhku pöörama andmekaitse turvalisusele, just nimelt dokumentide edastamisel läbi internetivõrgu. Kuna ei kasutata VPNi ega sisevõrku, siis häkkeritel oleks tunduvalt lihtsam edastatavatele andmetele ligi pääseda.

Teise intervjuu vastajad keskettevõttest on andmekaitsest kuulnud ainult koolist ning mõnelt konverentsilt, tööalaselt seda teavet väga puudutatud ei ole. Selles ettevõttes tegeleb andmekaitsega rohkem IT-osakond ning on ka partnerettevõte väljastpoolt, kes tegeleb nende turvalisusega. Intervjueeritavad arvavad, et ettevõte on hästi kaitstud ning ei peaks mingisuguseid muudatusi selles valdkonnas ette võtma (siiani pole nende väitel ühtegi negatiivset kogemust olnud). Autori arvates on ettevõte mõõdukalt kaitstud andmeturvalisuse poole pealt ning raamatupidajate teadmised on ka piisavad hoidmaks ettevõtet väljaspool andmekaitseriske. Ühe ettepanekuna siiski tooks välja, et arvuti juurest lahkumisel peaks infosüsteemist välja logima.

Kolmas vastaja suurettevõttest leiab, et tema firmas on andmekaitse väga olulisel kohal ning töötajad on ka teadlikud võimalikest ohtudest. Nimelt korraldatakse mitmeid koolitusi, et töökeskkonda turvalisemaks muuta. Autori arvates olid raamatupidaja teadmised ka piisavad ohtude vältimiseks. Samuti on ettevõte teinud palju selleks, et muuta töökeskkond turvaliseks. Kvalitatiivse uuringu cross-case tabelit on võimalik näha tabelis 3.

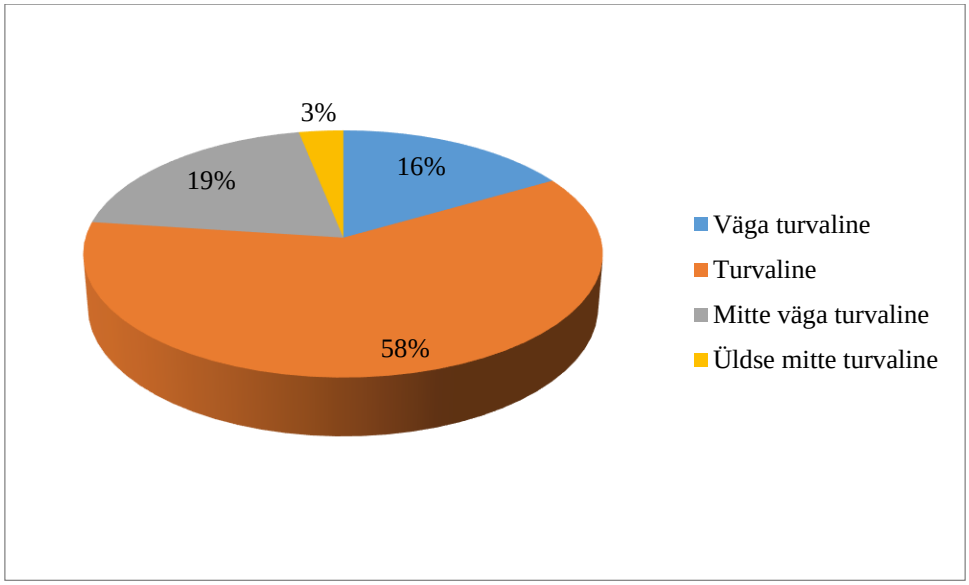
**Tabel 3**

| Küsimus | Mikroettevõte | Keskettevõte | Suurettevõte |
|---|---|---|---|
| Kui palju kuulnud andmekaitsest. | Kuulnud, pole väga oluline. | Kuulnud, on oluline, kuid IT-valdkond tegeleb sellega | Kuulnud, väga oluline. |
| Tähtsate dokumentide saatmine. | e-maili kaudu, ei ole väga turvaline. | e-maili kaudu, ei ole turvaline. | e-maili kaudu, ei ole kõige turvalisem. |
| Arvamus isikute pahatahtlikult süsteemidesse sattumise kohta. Paroolide vahetamine ja valimine. | Võiks olla karistatav. Ei meeldi paroolide vahetamine. | Karistatav. IT paroolide reeglid ette andnud. | Kindlasti karistatav. Kasutatakse tugevaid paroole. |
| Eriti hoolikalt kaitstud andmed. Delikaatsed isikuandmed. | Panga sisselogimise paroolid, salasõnad. | Panga- ja palgaandmed, isikuandmed, hinnainfo. Delikaatne nime avaldamine. | Isikuandmed, ettevõtte andmed. Delikaatsed andmed, mis võivad inimest diskrimineerida |
| Isikukoodi kasutamine dokumentides. | Ei peaks varjama | Ei ole delikaatne | Ei ole salajane |
| Kaks kõige tähtsamat põhimõtet isikuandmete töötlemisel. | Andja peab teadlik olema ning nõustuma andmete edastamisest ning töötlemisest. Tähtis turvalisus ning andmete asukoht. | Andmeid ei tohi jätta ripakile, et kellelgi ei tekiks ahvatlust neid kuritarvitada. | Isikuandmeid kaitstakse õiguspäraste eesmärkide saavutamiseks. Et kõik oleks seaduspärane ning andmeid kogutud õiglaselt. |

Allikas: koostatud autori poolt.

Kvantitatiivsest uurimusest selgus, et 16% vastajatest (12 vastajat) pidasid ettevõtet, kus nad töötavad, väga turvaliseks. 64% nendest vastajatest tegelikult oli ettevõttes rakendatud erinevaid meetmeid, et tagada turvalisus andmekaitse seisukohalt. 58% vastajatest (42 vastajat) pidas ettevõtet turvaliseks. Nendest 55%-l olid ettevõttes täidetud vajalikud kriteeriumid, et tagada turvalisus. 19% vastajatest (14 vastajat) ei pidanud ettevõtet, kus töötavad, väga turvaliseks. Nendest kõik hindasid ka ettevõtet õiglaselt. 3% vastajatest (2 vastajat) ei pidanud ettevõtet, kus töötavad, üldse turvaliseks. Mõlematel vastajatel oli õigus ning ettevõtetes polnud rakendatud peaaegu mitte ühtegi kriteeriumi, et kaitsta seda andmeriskide eest. Vastajates arvamused ettevõtte turvalisusest on toodud välja joonisel 1.

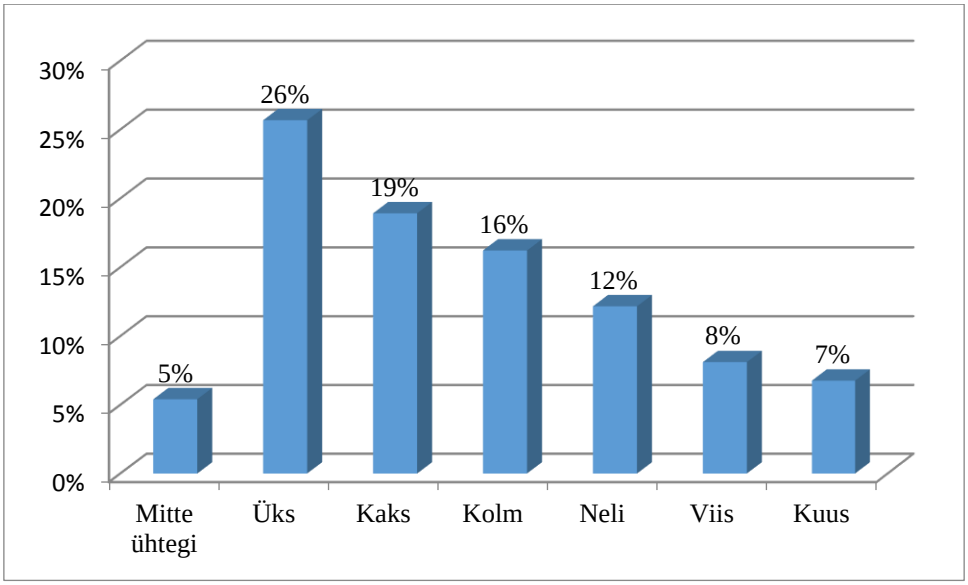
**Joonis 1. Vastajate arvamus ettevõtte turvalisusest.**




Allikas: Autori poolt koostatud. Aluseks võetud küsimustiku vastused.

Joonisel 2 on välja toodud ettevõtete, kus vastajad töötavad, rakendatud kriteeriumite arv. Mida rohkem kriteeriume on täidetud, seda turvalisem on ettevõte andmekaitse seisukohalt.

**Joonis 2. Ettevõttes täidetud kriteeriumite arv andmekaitse rakendamise kohta.**




Allikas: Autori koostatud, aluseks võetud küsimustiku vastused.

Ettevõtet võib pidada turvaliseks, kui on täidetud vähemalt kolm kriteeriumi (nendest põhilisemad ja vajalikumad). Väga lihtsad ning loogilised kriteeriumid andmekaitse seisukohalt on näiteks töötajate isiklike kasutajakontode olemasolu, arvuti tagant lahkudes tuleks infosüsteemist välja logida (ka lõunale minnes, wc-kasutamisel või kohvi võtmisel) ning aeg-ajalt koolituste pidamine. Tähelepanuväärne on aga fakt, et 50% vastanutest on täidetud vähem kui kolm kriteeriumit.

Et uurida vastajate teadmisi andmekaitse olulisusest, küsiti ankeedis Likert-skaala põhjal vastajate arvamust delikaatsete isikuandmetega töötlemise olulisuse kohta. Et tagada ettevõttes andmekaitse turvalisus, peaksid kõik väited olema hinnatud väga oluliseks. Tulemused on kajastatud tabelis 4.

**Tabel 4. Delikaatsete isikuandmete töötlemine**

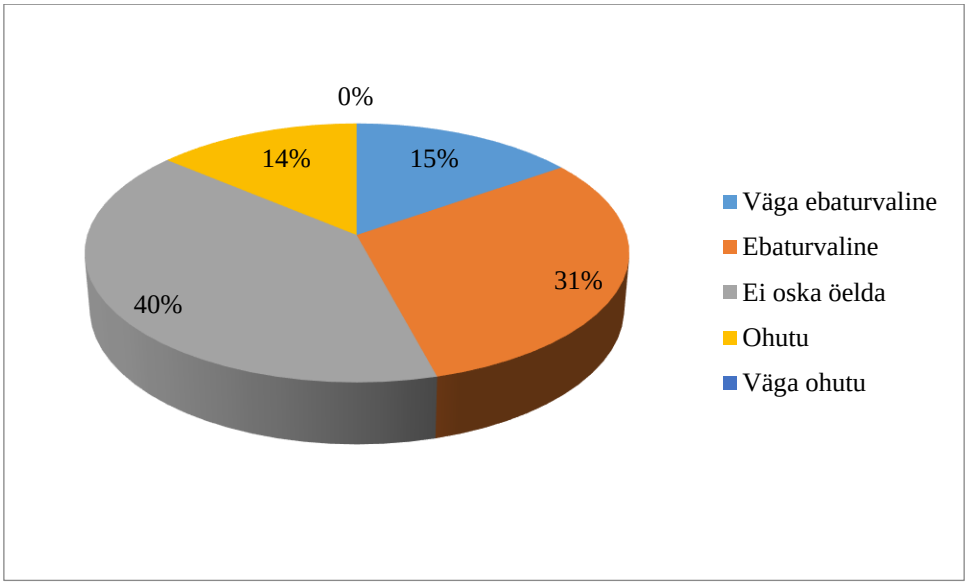
| Delikaatsete isikuandmetega töötlemine | Vastajate hinnangud Likerti skaala põhjal 1-5. | | | | | Hinnangute kaalutud keskmine |
|---|---|---|---|---|---|---|
| | Ei ole üldse oluline (1) | Pigem ei ole oluline (2) | Ei oska öelda (3) | Pigem oluline (4) | Väga oluline (5) | |
| Ettevõttes peab olema selge, kus on delikaatne info ning kellel on sellele juurdepääs | 1<br>1,35% | 0<br>0% | 3<br>4,05% | 11<br>14,86% | **57**<br>**77%** | **4,71** |
| Ettevõtted peavad tegelema delikaatsete andmete turvalise hoiustamisega | 1<br>1,35% | 0<br>0% | 3<br>4,05% | 11<br>14,86% | **57**<br>**77%** | **4,71** |
| Töötajatelt nõutakse tugevate paroolide kasutamist. (keerulised numbri- ja tähekombinatsioonid) | 1<br>1,35% | 2<br>2,7% | 9<br>12,16% | 25<br>33,78% | **35**<br>**47,3%** | 4,26 |
| Tundlikke andmeid hoitakse krüpteeritult. | 3<br>4,05% | 2<br>2,7% | 10<br>13,51% | 27<br>36,49% | **30**<br>**40,54%** | 4,1 |

Allikas: Autori koostatud, aluseks võetud küsimustiku vastused.

Tulemustest selgub, et vastajate jaoks on oluline, et ettevõttes peab olema selge, kus on delikaatne info ning kellel on sellele ligipääs. Sama oluline on vastajate jaoks see, et ettevõtted peavad tegelema delikaatsete andmete turvalise hoiustamisega.

Lisaks meetmete uurimisele, mida ettevõtetes rakendatakse, et kaitsta andmeid ohtude eest, hinnati ka küsimustikule vastajate teadmisi andmekaitsest. Selleks küsis autor, kui ohutuks peavad vastajad dokumentide edastamist läbi Interneti, täpsemalt läbi ühiskaustade nagu Google Drive, Dropbox jms. 40% vastajatest ei osanud selle kohta seisukohta võtta, mis tähendab, et tõenäoliselt sellist viisi ettevõtetes väga ei kasutata (mõnel juhul lisati ka see kommentaaridesse). Hea on tõdeda, et 41% vastanutest peab sellist viisi ebaturvaliseks. Tulemused on kajastatud joonisel 3.

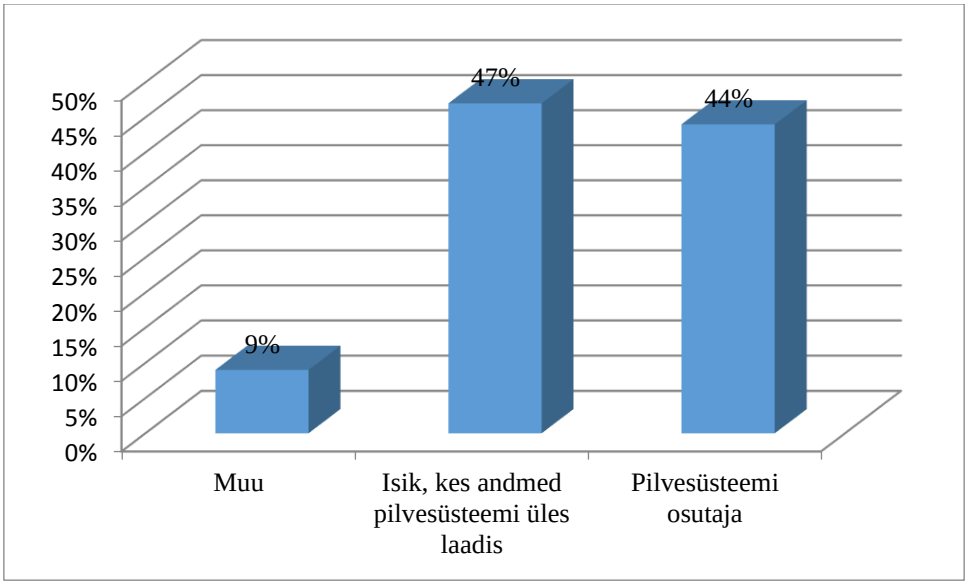
**Joonis 3. Andmete edastamise turvalisus läbi ühiskaustade**




Allikas: Autori koostatud, aluseks võetud küsimustiku vastused

Ankeetküsitluse üks küsimusi oli pilvesüsteemis hoitavate andmete väärkasutamise vastutuse kohta. Küsimus oli selles, kes peaks vastutama selle eest, kui pilvesüsteemis hoitavaid andmeid on väärkasutatud. Tulemusi illustreerib joonis 4.

**Joonis 4**




Allikas: Autori koostatud. Aluseks võetud küsimustiku vastused.

Üllatav oli autori jaoks see, et 31 vastajat vastas, et pilvesüsteemi osutaja ning kõigest 33 inimest vastas, et vastutab isik, kes andmed pilvesüsteemi üles laadis. Ülejäänud vastajatel ei olnud seisukohta selle küsimuse suhtes. See näitab suurt ohtu andmete jagamisel Internetis. Inimesed ei kipu ega taha vastutust võtta andmete töötlemisel ning jagamisel Internetti.

## 3.3 Uuringu analüüs

Kvalitatiivsest analüüsist selgus, et väga palju sõltub ettevõtte suurusest. Mida suurem on ettevõte, seda olulisem on ka andmekaitse ning teadmised sellest. Samuti juhitakse suuremates ettevõtetes rohkem tähelepanu andmete töötlemise turvalisusele. Sama võib öelda ka raamatupidajate kohta. Mikroettevõttes töötava raamatupidaja arvates ei mängi andmekaitse väga suurt rolli tema tööelus, kuna tegemist on väga väikses mahus andmetega. Samuti on määravaks see, et ettevõttes töötab vähe inimesi ning seega ei puutu andmetega kokku suur hulk inimesi. Kuna mitmed andmekaitset puudutavad meetmed on üpris kulukad, siis mikro- ning väikeettevõtetele oleks nende meetmete rakendamine väga kulukas. Samas kui mõelda turvalisusele, siis kindlasti on odavam ning vähem riskantsem turvameetmete kasutuselevõtt, kui hiljem negatiivseid tagajärgi likvideerida. Kvalitatiivsest uuringust selgus, et keskmise suurusega ettevõttes ollakse teadlikud andmekaitsest, kuid väga rangeid reegleid ei ole kehtestatud, pigem tegelevad teised üksused programmide turvalisemaks muutmisega. Intervjuust selgus, et suurettevõttes töötava raamatupidaja teadmised andmekaitsest on head ning ta peab ka seda teemat väga oluliseks. Kvantitatiivsest uuringust selgus, et ettevõtte suurus ei oma üldse olulist rolli. Teadmised andmekaitsest olid ühesugused nii mikro-, väike-, kesk- kui ka suurettevõtetes. Küll aga üldiselt selgus, et ettevõtted, kus vastajad töötavad, ei ole väga turvalised andmekaitse seisukohalt. Ligi 50% vastanute ettevõtteid võib pidada turvaliseks andmekaitse seisukohalt. Seda on ilmselgelt vähe arvestades uue andmekaitsemääruse jõustumist 2018.aasta mais. Selle tõttu peaks andmekaitse olema hetkel aktuaalne teema. Samas peavad raamatupidajad delikaatsete isikuandmete töötlemisega seonduvat väga oluliseks. Kõiki küsimustikus esitatud väiteid delikaatsete isikuandmete töötlemise kohta hindasid vastajad väga oluliseks. Kõigi väidete kaalutud keskmine oli üle 4,1, mis tähendab, et vastajatel on olemas vastavad teadmised delikaatsete isikuandmetega töötlemisest. Seda tõestab ka fakt, et 41% vastanutest peab dokumentide edastamist läbi ühiskaustade ohtlikuks, sest need dokumendid võivad samuti sisaldada tundlikke andmeid. Autorit paneb imestama ainult vastajate teadmised andmete väärkasutamise vastutamise kohta. Nimelt kõigest peaaegu pooled vastanutest arvavad, et andmete üleslaadimisel pilvesüsteemi vastutab isik ise, mitte pilveteenuse osutaja. See näitab seda, et inimesed usaldavad oma andmete turvalisust üleslaadimisel pilvesüsteemi ning Internetti. Üldiselt võib öelda, et pooled uuringus osalejatest teavad andmekaitsega kaasnevaid riske ning ohtusid.

Kvantitatiivsest uuringust tuli veel välja, et need, kes ei pidanud ettevõtet, kus nad töötavad, turvaliseks, ei olnud kasutatud ka vastavaid meetmeid ettevõtte andmekaitse turvalisuse jaoks. Vastajad, kes pidasid ettevõtet turvaliseks, nendest pooled tegelikult ei olnud turvalised andmekaitse seisukohalt. Samuti need, kes pidasid ettevõtet, kus nad töötavad, väga turvaliseks, 64% neist oli rakendatud vastavaid meetmeid, et ettevõte oleks väga turvaline andmekaitse koha pealt. Seega need vastajad, kes pakkusid äärmuslikult ehk kas nende ettevõte pole üldse turvaline või just on väga turvaline, siis nemad teadsid täpselt, mis puudused või plussid ettevõttes on rakendatud, et andmekaitse oleks firmas tagatud. Kuna andmekaitse on praegu väga aktuaalne teema uue andmekaitse määruse tõttu, siis peaksid ettevõtete töötajad samuti sellega kursis olema. Kuna määrus avaldati 2016.aasta maikuus ning jõustub 2018.aasta maikuus, siis praegusel hetkel peaksid toimuma juba muudatused ettevõtetes. Seepärast saab pidada tulemusi negatiivseteks ehk töötajate teadlikkus andmekaitsest on puudulik.

Intervjuude alusel võib väita, et raamatupidajatel on olemas teadmised andmekaitsest, kuid enamus nendest ei pea neid teadmisi väga oluliseks oma töös rakendama. Samuti ei piisa ainult teadmised, vaid neid peab ka praktikas rakendama.

## 3.4. Arutelu, järeldused ja ettepanekud

Teooriat arvestades peaksid raamatupidajad tähele panema paljugi isikuandmete kaitsega seonduvast. Uus andmekaitsemäärus puudutab pea kõiki töötajaid, kes andmetega vähemal või suuremal määral kokku puutuvad. Oluline on tähele panna, kas ettevõttes oleks täidetud kindlad kriteeriumid. Olulisemad kriteeriumid ettevõtte turvaliseks pidamisel andmekaitse koha pealt: kas andmetele ligipääs on lubatud vaid selleks ettenähtud isikutele, kelle tööülesanded seda nõuavad? Kas ettevõttes kasutatakse individuaalseid kasutajakontosid? Kas töötajatelt nõutakse tugevate paroolide kasutamist? Kas ettevõtte töötajad on kursis infoturbega, nende riskidega ning kaasnevate ohtudega? Kas isikuandmeid säilitatakse muudest andmetest eraldi? Kas delikaatseid andmeid hoitakse/edastatakse krüpteeritult? Kas andmetest tehakse regulaarselt varukoopiaid? Kas andmete varukoopiate taastamist testitakse regulaarselt?

Intervjuudest selgus, et kahes suuremas ettevõttes on enamasti need kriteeriumid täidetud. Raamatupidajad on teadlikud võimalikest ohtudest, mis võivad tekkida andmete käitlemise,

kogumise ning edastamise tagajärjel. Mikroettevõte on aga liialt väike, et selle põhjal järeldusi teha, sest raamatupidaja ei puutu sellega väga palju kokku. Kvantitatiivsest uuringust selgus, et 43% ettevõtetes, keda küsitleti, on rakendatud enamus kriteeriumid, et pidada firmat turvaliseks andmekaitse seisukohalt. Sellest võib järeldada, et ettevõtted peaksid rohkem tähelepanu pöörama andmekaitsele. Inimestel võivad isegi teadmised olla erinevatest ohtudest, kuid meetmeid, mis kaitseks ettevõtet andmeriskide eest, nii hästi rakendama ei kiputa. Käesoleva uurimuse tulemusi ei saa pidada ainuõigeteks, kuid tulemusi analüüsides võib väita, et üldiselt raamatupidajate teadlikkus andmekaitsest on puudulik. Samuti peaks ettevõttes rakendama erinevaid meetmeid, et riske ära hoida. Kõige lihtsamatest meetmetest on näiteks tugevate paroolide kasutamine, igal töötajal isiklik kasutajakonto ning alati enne arvuti tagant lahkumist tuleb infosüsteemist välja logida (ka wc-kasutamise või kohvi võtmise ajaks). Lisaks pole väga kulukad ning suured ettevõtmised aeg-ajalt andmekaitse-teemaliste koolituste pidamine. Loomulikult nõuab see erinevaid ressursse (nii aega, teadmisi kui ka raha), kuid hiljem andmete väärkasutamise katastroofi likvideerida on palju kulukam. Raamatupidajate teadlikkust andmekaitsest saab tõsta õpingute käigus, kus selleks võiks olla vastavateemaline õppeaine. Kuna teema ei puuduta ainult raamatupidajaid, siis peaks see aine olema mõeldud suuremale kuulajaskonnale. Eelkõige peaksid ettevõtted tagama ohutuse nii nende töötajate isikuandmetele kui ka klientide ning ettevõtte enda andmetele, mida töödeldakse.

# KOKKUVÕTE

Käesoleva bakalaureusetöö eesmärgiks oli välja selgitada raamatupidajate teadlikkust andmekaitsest. Uuringus selgitati välja, kas raamatupidajate teadlikkust andmekaitsest tuleks tõsta. Kuna iga ettevõte on erinev oma olemuselt, ülesehituselt ning eesmärkide poolest, siis võib arvata, et ka raamatupidajate teadmised andmekaitsest on erinevad. Nagu ka intervjuudest selgus, siis väga suurt rolli mängib juba ettevõtte suurus. Mida suurem ettevõte, seda olulisem on töötajate teadlikkus andmekaitsest, samas mikroettevõtte raamatupidaja ei pidanud seda üldse väga oluliseks, kuivõrd arvas, et andmekaitse teda väga ei puuduta, sest ettevõttes on vähe töötajaid ning tegutsetakse peamiselt oma klientide ehk siis teiste ettevõtete soovide järgi. Kvantitatiivsest uuringust selgus, et ligi pooled vastanutest on teadlikud andmekaitsest ning sellega kaasnevatest ohtudest. Sama kehtib ettevõtetes rakendatud meetmete kohta, et tagada andmete turvalisus. Kõigest vastanud ettevõtetest 43%-l rakendavad vähemalt kolme kriteeriumi, mis tagaks turvalisuse ettevõttes andmekaitse seisukohalt.

Kvalitatiivse uurimuse raames viidi autori poolt läbi kolm intervjuud erineva suurusega ettevõtete raamatupidajatega. Intervjuude kestvuseks oli keskmiselt 15 minutit. Intervjuudest selgus, et raamatupidajate teadmised andmekaitsest on piisavad hoidmaks ära andmekaitseriske ettevõttes. Teadmised olid head keskettevõttes, väga head suurettevõttes, kuid mikroettevõttes võiks neid teadmisi tõsta. Kvantitatiivse uurimuse raames koostas autor küsimustiku andmekaitse kohta, millele vastas 74 raamatupidajat. Vastustest selgus, et ligi poolte vastanute teadmised andmekaitsest on head ning ligi pooltes ettevõtetes on rakendatud meetmeid andmekaitse kohta, et tagada andmete turvalisus.

Bakalaureusetöö autori poolt välja pakutud hüpotees oli, et raamatupidajate teadlikkus andmekaitsest on puudulik ning seda tuleks tõsta. Hüpotees pidas paika. Analüüsi käigus selgus, et teadlikkust andmekaitsest tuleks tõsta. Tähelepanuväärne on see, et inimesed, kes peavad ettevõtet ning oma teadmisi turvaliseks, tegelikult ei ole turvalises keskkonnas andmekaitse seisukohalt. Seega inimesed ei oska isegi arvata, et midagi ettevõttes valesti on ning ei pea ka vajalike meetmete rakendamist oluliseks. Seepärast on oluline, et informatsioon erinevate andmekaitsega seotud riskide ning ohtude kohta tuleks ka väljaspoolt ettevõtet, näiteks koolist.

# SUMMARY

The aim of the thesis was to find out the accountants awareness of data protection. This study determined whether the data protection should increase the awareness of acountants or not. As every company is different by its nature, in terms of structure and objectives, it can be assumed that the accountants have different understanding about data protection. According to the interviews, it plays a very large role in the company´s size. The larger the company, the more important is the awareness of employee´s data. For micro-company accountant it was not so important at all. They thought that the data protection does not affect them very much, because the company has a few employees and operates mainly like their customers or other businesses wish. Quantitative study showed that almost half of the respondents are aware of the data protection and the dangers involved. The same applies to businesses to implement measures to ensure data security. Just 43% of the respondents implement at least three of the criteria that would ensure the security of the company data protection.

Qualitative research was conducted three interviews on different sized businesses accountants. The interviews lasted an average of 15 minutes. The interviews revealed that accountants´ knowledge of data protection are sufficient to prevent the data protection risks of the company. The knowledge were good in medium-sized companies, very good in big companies, but in micro-companies should increase the knowledge of data protection. In the quantitative analysis the author put together the questionnaire about data protection, which was answered by 74 accountants. The responses showed that almost half of the respondents have good knowledge about data protection, and nearly half of the companies have implemented measures on data protection to ensure data security.

In Bachelor thesis the author proposed hypothesis that the accountants´ awareness of data protection is inadequate and should be increased. The hypothesis was true. The analysis revealed that awareness of data protection should be raised. It is remarkable that people who have knowledge of their business and secure, in fact, is not a safe environment protection point of view. Therefore, people can not even believe that something is wrong with the company and does not have the necessary measures on essential. It is therefore important that information about the various data protection risks and hazards should be from outside the company, such as schools.

# VIIDATUD ALLIKAD


Eesti keele sõnaraamat ÕS 1999. Eesti Keele Instituut. Kolmas trükk. Tallinn, Eesti Keele Sihtasutus 2003

Männiko, M. (2011) Õigus privaatsusele ja andmekaitse

What is Personal Data?, 2007 [WWW] https://www.dataprotection.ie/docs/What-is-Personal-Data/210.htm

A New Age of Privacy Protection: A Proposal for an International Personal Data Privacy Treaty, 2010, vol 42 [WWW] http://connection.ebscohost.com/c/articles/67061599/new-age-privacy-protection-proposal-international-personal-data-privacy-treaty

Euroopa Andmekaitse reform. Andmekaitse Inspektsioon. 2016 [WWW] http://www.aki.ee/et/eraelu-kaitse/euroopa-andmekaitse-reform

Hea Tava. Millega tegeleb igapäevaselt raamatupidaja. 2015 [WWW] http://www.heatava.ee/uudis/millega-tegeleb-igapaevaselt-raamatupidaja/

CPA Practice Advisor. Are You Protecting Client Data When Sending Files Over the Internet?. 2012 [WWW] http://www.cpapracticeadvisor.com/article/10708072/are-you-protecting-client-data-when-sending-files-over-the-internet

CPA Pracitce Advisor. How Accounting Firms Can Protect Their Data, And Their Clients. 2016. [WWW] http://www.cpapracticeadvisor.com/article/12233937/how-accounting-firms-can-protect-their-data-and-their-clients

Andmekaitse Inspektsioon. Delikaatsed isikuandmed. 2014 [WWW] http://www.aki.ee/et/delikaatsed-isikuandmed

Ten Practical Things to Know About „Sensitive“ Data Collection and Protection. 2008 [WWW] http://web.a.ebscohost.com/ehost/detail/detail?vid=3&sid=e60c0ce5-dc21-4291-b20b-cc3ac0951890%40sessionmgr4006&hid=4206&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=32623546&db=bth

Heimdal Security. Andra Zaharia. (19.04.2016) 15 Steps to Maximize your Financial Data Protection. [WWW] https://heimdalsecurity.com/blog/online-financial-security-guide/

Maarja Heinsoo, Märten Padu. Andmekaitsemäärus – Mis see on ja mida tähele panna. 2016 [WWW] https://www.pwc.com/ee/et/press/artiklid/assets/articles/andmekaitsemaeaerus--mis-see-on-ja-mida-taehele-panna-.html

Rikkumisteated. Andmekaitse Inspektsioon. 13.02.2017 [WWW] http://www.aki.ee/et/andmekaitse-reform/rikkumisteated

Töötlustoimingute registreerimine. Andmekaitse Inspektsioon. 27.02.2017 [WWW] http://www.aki.ee/et/andmekaitse-reform/tootlustoimingute-registreerimine

Vaikimisi ja lõimitud andmekaitse. Andmekaitse Inspektsioon. 13.03.2017 [WWW] http://www.aki.ee/et/andmekaitse-reform/vaikimisi-ja-loimitud-andmekaitse

Isikuandmete kaitse üldmäärus. Andmekaitse Inspektsioon. 20.03.2017 [WWW] http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/dataprotectioninfographicet-lr.pdf

Elis Prangli. Andmekaitse reform – kes omab minu andmeid. Majandus24. 2016. [WWW] http://majandus24.postimees.ee/3724113/andmekaitse-reform-kes-omab-minu-andmeid

Rahvakool. ÕPPEPÄEV: Uus isikuandmete kaitse määrus ja andmekaitsereform. 2016 [WWW] http://www.rahvakool.ee/21-09-2016-oppepaev-uus-isikuandmete-kaitse-maarus-ja-andmekaitsereform/

FECC. hommikuseminar „Euroopa Liidu andmekaitse määrus – mõju ettevõtte protsessidele ning süsteemidele“. 2017 [WWW] http://www.fecc.ee/et/kalender/158-9-03-hommikuseminar

Äripäev. Pilvelahendused ja uus andmekaitsemäärus. 2017 [WWW] http://www.ituudised.ee/uritused/2016/12/06/pilvelahendused-ja-uus-andmekaitsemaarus

Excellence koolitus- ja arenduskeskus. Isikuandmete töötlemine organisatsioonis: Euroopa Liidu andmekaitsereformi määruse muudatused. 2017 [WWW] http://www.excellence.ee/koolitused/andmekaitsereform

# LISAD

## Lisa 1. Intervjuu küsimused

1. Kui palju olete kuulnud andmekaitsest? Mida on ettevõte teinud omalt poolt, et töötajaid teavitada ohtudest? Kas on korraldatud koolitusi ja informatsioon on personalile kättesaadav?
2. Kuidas saadate tähtsaid faile nagu palgalehed? Mida arvate selle turvalisusest?
3. Mida arvate aga pangaandmete edastamisest e-maili kaudu? Kui turvaline see on Teie arvates? Kas Teie arvates tähtsate dokumentide edastamine läbi ühiskaustade nagu DropBox või Google Drive kaudu on ohutu?
4. Mis arvate, kas see on karistatav, kui arvuti tagant lahkudes ei logita infosüsteemist välja ja keegi teine infosüsteemis andmeid vaatab? Miks on oluline, et töötajad teaksid, kuidas ja missuguseid paroole tuleb süsteemidesse sisselogimiseks kasutada (parooli pikkus, keerukus, vahetamine jne)?
5. Missuguseid andmeid peab raamatupidaja eriti hoolikalt kaitsma? Missugused on delikaatsed isikuandmed? Mida peab silmas pidama isikukoodi kasutamisel dokumentides?
6. Mis on Teie arvates kaks kõige tähtsamat põhimõtet, mida tuleb silmas pidada isikuandmete töötlemisel?

## Lisa 2. Intervjuu transkriptsioon 1 (suurettevõte)

1. Kui palju olete kuulnud andmekaitsest? Mida on ettevõte teinud omalt poolt, et töötajaid teavitada ohtudest? Kas on korraldatud koolitusi ja informatsioon on personalile kättesaadav?

Olen kuulnud andmekaitsest päris palju. Meie ettevõttes on andmekaitse väga oluline teema. Juba tööle asumisel korraldati vastavasisulisi koolitusi. Jah, on korraldatud koolitusi ja alati on võimalik koolituse esitlusi järele vaadata. Need on kättesaadavad meie intranetis.

2. Kuidas saadate tähtsaid faile nagu palgalehed? Mida arvate selle turvalisusest?

Palgalehe soovist annab iga töötaja ise teada e-posti teel ja seejärel hakatakse talle seda iga kuu saatma. Arvan, et selles ei ole midagi halba.

3. Mida arvate aga pangaandmete edastamisest e-maili kaudu? Kui turvaline see on Teie arvates? Kas Teie arvates tähtsate dokumentide edastamine läbi ühiskaustade nagu DropBox või Google Drive kaudu on ohutu?

On oluline eelnevalt veenduda, kellele sa neid edastad. Arvan, et see ei ole kõige turvalisem variant. Läbi ühiskaustade dokumentide saatmine ei ole kindlasti ohutu.

4. Mis arvate, kas see on karistatav, kui arvuti tagant lahkudes ei logita infosüsteemist välja ja keegi teine infosüsteemis andmeid vaatab? Miks on oluline, et töötajad teaksid, kuidas ja missuguseid paroole tuleb süsteemidesse sisselogimiseks kasutada (parooli pikkus, keerukus, vahetamine jne)?

Jah, see on karistatav. Iga töötaja vastutab temale usaldatud vara ja andmete eest. Paroolid on olulised, et töötajad mõistaksid, millised riskid kaasnevad nö nõrkade paroolidega, mida on lihtne ära arvata.

5. Missuguseid andmeid peab raamatupidaja eriti hoolikalt kaitsma? Missugused on delikaatsed isikuandmed? Mida peab silmas pidama isikukoodi kasutamisel dokumentides?

Eriti hoolikalt peab kaitsma isikuandmeid ja ettevõtte andmeid, mis ei ole mõeldud avalikustamiseks. Delikaatsed on isikuandmed, mille avalikustamine võib inimest kuidagi ohustada või diskrimineerida. Näiteks terviseseisund. Isikukood ei ole salajane teave, seega võib seda dokumentides kasutada. Kuid alati peab kaaluma, kas seda peab kasutama või piisab inimese nimest ja ametikohast.

## Lisa 2. Intervjuu transkriptsioon 1 (suurettevõte). Järg

6. Mis on Teie arvates kaks kõige tähtsamat põhimõtet, mida tuleb silmas pidada isikuandmete töötlemisel?

Esiteks, et isikuandmeid kogutakse õiguspäraste eesmärkide saavutamiseks. Teiseks, et kõik oleks seaduspärane, see tähendab, et isikuandmed on saadud seaduslikul teel.

## Lisa 3. Intervjuu transkriptsioon (mikroettevõte)

1. Kui palju olete kuulnud andmekaitsest? Mida on ettevõte teinud omalt poolt, et töötajaid teavitada ohtudest? Kas on korraldatud koolitusi ja informatsioon on personalile kättesaadav?

Olen kuulnud andmekaitsest küll, aga mikroettevõttes pole vaja väga palju sellele tähelepanu pöörata, sest töötan üksi ning olen ikkagi väga paindlik teistele ettevõtetele. Töötan kodukontoris, elan ka üksi. Hoian uksed kõik lukus, teistel ei tohiks olla ligipääsu mingitele andmetele.

2. Kuidas saadate tähtsaid faile nagu palgalehed? Mida arvate selle turvalisusest?

Kuna teen raamatupidamist erinevatele ettevõtetele, siis olen väga paindlik, teen nii, kuidas iga ettevõte soovib. Enamus soovivad seda saada e-maili kaudu. Ettevõtetele olen pakkunud ka süsteemide kaudu edastamist, kuid pigem tahetakse kõige lihtsamat viisi.

3. Mida arvate aga pangaandmete edastamisest e-maili kaudu? Kui turvaline see on Teie arvates? Kas Teie arvates tähtsate dokumentide edastamine läbi ühiskaustade nagu DropBox või Google Drive kaudu on ohutu?

Teen seda ka e-maili kaudu, just nimelt selle tõttu, et ettevõtted nii soovivad. Vist ei ole väga turvaline, võib-olla peaks pakkuma välja variandi allkirja võtmisest, kas võib andmeid edastada e-maili kaudu, siis pole vastutus ainult raamatupidajal. Ühiskaustade kasutamine ilmselt ei ole ohutu, aga ei kasuta selliseid kohti ka. Olen küll pakkunud ettevõtetele, kuid neil pole lihtsalt aega selle jaoks, nemad tahavad ikka kõige lihtsamat viisi.

4. Mis arvate, kas see on karistatav, kui arvuti tagant lahkudes ei logita infosüsteemist välja ja keegi teine infosüsteemis andmeid vaatab? Miks on oluline, et töötajad teaksid, kuidas ja missuguseid paroole tuleb süsteemidesse sisselogimiseks kasutada (parooli pikkus, keerukus, vahetamine jne)?

Oleneb andmete tundlikkusest. Kui inimene teeb seda teadlikult ning tegemist on väga tundlike andmetega, siis kindlasti on see karistatav. Pean kohe ära ütlema, et ei meeldi üldse paroolide vahetamine. Mõned programmid ise paluvad vahetada. Häkkerite jaoks on see kindlasti oluline, et kasutatakse keerulisemaid paroole, et nemad programmidele ligi ei pääseks.

## Lisa 3. Intervjuu transkriptsioon (mikroettevõte). Järg

5. Missuguseid andmeid peab raamatupidaja eriti hoolikalt kaitsma? Missugused on delikaatsed isikuandmed? Mida peab silmas pidama isikukoodi kasutamisel dokumentides?

No kindlasti panga sisselogimise paroolid, salasõnad. Need peavad olema eriti salastatud. Isikukood on igalpool väga vajalik, kas või maksuametisse sisse logides tuleb sisestada isikukood. See on juba nii levinud teave, et seda ei peaks varjama. Väga lihtne on isikukoodi kätte saada.

6. Mis on Teie arvates kaks kõige tähtsamat põhimõtet, mida tuleb silmas pidada isikuandmete töötlemisel?

Andja peab teadlik olema, et oma isikuandmed kuskile annab ja nõus olema, et neid töödeldakse. Tähtis on ka, et neid hoitakse turvalises kohas.

## Lisa 4. Intervjuu transkriptsioon (Keskettevõte)

1. Kui palju olete kuulnud andmekaitsest? Mida on ettevõte teinud omalt poolt, et töötajaid teavitada ohtudest? Kas on korraldatud koolitusi ja informatsioon on personalile kättesaadav?

Pearaamatupidaja: Põhiliselt olen kuulnud koolist igasuguste seadusandluse õppeainete raames. Aga niimoodi tööalaselt seda nii väga mitte, võib-olla mõnel konverentsil sellest räägitakse, aga pigem väga suurt rõhku sellele küll ei panda. Finantskontroller: Mina olen kuulnud sisekontrolli aastakonverentsil sellel teemal korra räägiti. Meil on enamus andmekaitse poole pealt on IT-valdkond, et kui me võtame niimoodi, et üleüldse andmekaitses meil on iseenesest programmid tõmmatud erinevate partnerite poolt. Siis meil on VPN loodud, Telial on sisevõrk, mis meil on loodud, siis kui me võtame raamatupidajad üleüldiselt, siis meil on igaühel antud õigused nendesse programmidesse siseneda, meil on igaühel personaalsed õigused, et üldse mingeid erinevaid asju näha, meil on kõigil lepingutes sees see, et konfidentsiaalsus, meil on arvete poole pealt see, et ei lekiks näiteks hinnad kuskile välisturule, siis väga paljud arved on sellised, et kui tuleb meile kaup, siis ei tule üldse arvega, tulevad saatelehed, kus on ainult kogused peal ja arved saadetakse ainult raamatupidajatele kas siis e-maili teel.

2. Kuidas saadate tähtsaid faile nagu palgalehed? Mida arvate selle turvalisusest?

Pearaamatupidaja: Palgalehed lähevad ikka e-maili kaudu. Turvaline pole väga, sest alati võib keegi sinna vahele sattuda.

3. Mida arvate aga pangaandmete edastamisest e-maili kaudu? Kui turvaline see on Teie arvates? Kas Teie arvates tähtsate dokumentide edastamine läbi ühiskaustade nagu DropBox või Google Drive kaudu on ohutu?

Pearaamatupidaja: Selles mõttes ei ole turvaline, kui sa ei tea vastaspoolt, et sa ei saa seda ohtu minimaliseerida, et seda saab konfidentsiaalsuslepingutega ka, aga selles suhtes, et selles ei saa kindel olla, et keegi sealt vahepealt mingit infot ei saa, et küberrünnakutega jne. Aga muud, ma ei teagi, omavahelised kirjad on ikka ainult sisevõrgus, et naljalt need ei tohiks kuskile lekkida. Finantskontroller: Mõned üksikud väga tähtsad dokumendid, need tegelikult tuuakse meile siia personaalselt kätte. Pearaamatupidaja: Ainult serveri-siseselt, et ainult kõvakettal, seal on samamoodi, et seal on siis kõigile kasutatavad üldkettad ja on siis

## Lisa 4. Intervjuu transkriptsioon (Keskettevõte). Järg

võrgukettad, mis on ainult osadele kasutajatele ja ka võrgukettad, mis on ainult osakonna sees mõnele inimesele ligipääsetavad.

4. Mis arvate, kas see on karistatav, kui arvuti tagant lahkudes ei logita infosüsteemist välja ja keegi teine infosüsteemis andmeid vaatab? Miks on oluline, et töötajad teaksid, kuidas ja missuguseid paroole tuleb süsteemidesse sisselogimiseks kasutada (parooli pikkus, keerukus, vahetamine jne)?

Finantskontroller: Ma arvan ikka, et see on karistatav, ma ei oska seda riski siin meie ettevõttes hinnata, aga sellel samal sisekontrolli aastakonverentsil sai see ka märkimisväärset tähelepanu, näiteks väga palju oli seal riigiasutusi, kus on see kohustuslik. Meil pole see kohustuslikuks pandud ja siiani pole vist ühtegi pahatahtlikku asja juhtunud. Võib-olla sekretär ja nemad seal logivad välja, aga jah…kui ma lõunale lähen, siis ma panen iseendal ka, aga kui lihtsalt natuke liigun, siis ma ei logi välja. Parooli nõuded on meil tegelikult IT selle ette andnud, et tähekombinatsioon, numbrikombinatsioon. Meil ei saa seda ka väga tihti korrata seda ühte ja sama parooli, meil on see tsükkel päris pikk seal.

5. Missuguseid andmeid peab raamatupidaja eriti hoolikalt kaitsma? Missugused on delikaatsed isikuandmed? Mida peab silmas pidama isikukoodi kasutamisel dokumentides?

Finantskontroller: kõiki, aga loomulikult on pangad ja mingid andmed, palgad… Pearaamatupidaja: meil on küll eraldi osakond, personaliosakond, kes tegeleb palkadega, et nemad teevad seda arvestust ka ja isikuandmed on kindlasti väga olulised, hinnainfod ja kõik sellised ja ega tulemused ka, no põhimõtteliselt jah kogu värk. Finantskontroller: Nojah, me oleme saanud sellise sertifikaadi ka, muidu ei saagi pangamakseid vastu võtta, siis peavad olema sertifikaadid, mis näitavad seda, et kui inimene paneb oma maksekaardi kaarditerminali, siis tema isikuandmed ei lähe sealt kuskile laia maailma edasi, et need sertifikaadid on tagatud. Ja neid tuleb mingi perioodi tagant ka siis uuendada. Pangamaksetel on samamoodi, et neli silma on need, kes teevad ülekande ja kuus silma vaatab üldse dokumentidele peale. Pearaamatupidaja: Ma ei tea, töötaja nimesid vist tegelikult ei tohi ka avaldada. Kui näiteks keegi küsib, et kas teil töötab selline inimene, välja arvatud kohtutäiturid, kes saavad selleks korralduse, aga muidu mingid suvalised inimesed seda ei saa. Tänapäeval vist enam ei ole isikukood oluline, sünnikuupäevgi, mis tuleb isikukoodist välja.

## Lisa 4. Intervjuu transkriptsioon (Keskettevõte). Järg

6. Mis on Teie arvates kaks kõige tähtsamat põhimõtet, mida tuleb silmas pidada isikuandmete töötlemisel?

Pearaamatupidaja: Ongi, et sa teed oma asju hoolikalt ja ei jäta ripakile midagi, ei tekita seda riski, et kellelgi oleks ahvatlus teha midagi pahatahtlikku. Finantskontroller: Nojah, ma arvan ka, et see turvalisus, et meil on ka tegelikult ju isikuandmete poole pealt personaliosakonnal seif, mis on alati kinni ja personaliosakonnas uks on ka üldjuhul õhtuti kinni. Et seal on üldse väga piiratud, kes saavad sinna.

## Lisa 5. Kvantitatiivse uurimuse küsimustik

1. Kui turvaliseks peate ettevõtet, kus töötate, andmekaitse seisukohalt?

- Väga turvaliseks
- Turvaliseks
- Mitte eriti turvaliseks
- Üldse mitte turvaliseks
- Ei oska öelda

2. Mida on teinud ettevõte, kus töötate, et töötajad andmekaitsest ja sellega seotud ohtudest teadlikud oleksid?

- Regulaarsed koolitused andmekaitse teemadel
- Kehtestatud erinevad nõuded (nt arvuti tagant lahkudes tuleb infosüsteemist välja logida jms)
- Regulaarne turvalisuse hindamine (määratakse kindlaks, et ettevõttes ei oleks turvaauke)
- Igal töötajal on oma isiklik kasutajakonto, millega pääseb ligi talle vajalikele andmetele
- Ärikriitilised andmed on dubleeritud (back-up)
- Ettevõtte ruumidesse, kus hoitakse delikaatset infot, on piiratud ligipääs (pääsevad ainult teatud isikud)
- Muu

3. Millised on Teie arvates delikaatsed isikuandmed?

- Poliitilisi vaateid, usulisi ja maailmavaatelisi veendumusi kirjeldavad andmed
- Etnilist päritolu ja rassilist kuuluvust kirjeldavad andmed
- Isikukood
- Andmed terviseseisundi või puude kohta
- Palgainfo
- Andmed pärilikkuse informatsiooni kohta
- Aadress
- Andmed seksuaalelu kohta

## Lisa 5. Kvantitatiivse uurimuse küsimustik. Järg

- Muu

4. Kui olulised on Teie arvates järgmised väited delikaatsete isikuandmetega töötlemisel:

Ettevõttes peab olema selge, kus on delikaatne info ning kellel on sellele juurdepääs

Ei ole üldse oluline Väga oluline

1 2 3 4 5

Ettevõtted peavad tegelema delikaatsete andmete turvalisuse hoiustamisega

Ei ole üldse oluline Väga oluline

1 2 3 4 5

Töötajatelt nõutakse tugevate paroolide kasutamist. (keerulised numbri- ja tähekombinatsioonid)

Ei ole üldse oluline Väga oluline

1 2 3 4 5

Tundlikke andmeid hoitakse krüpteeritult.

Ei ole üldse oluline Väga oluline

1 2 3 4 5

5. Kuidas saadate tähtsaid faile nagu pangaandmed?

- E-maili teel
- Läbi ühiskaustade (Google Drive, DropBox jms)
- Postiga
- Isiklikult käest kätte
- Muu

6. Kas selline viis on teie arvates turvaline? (Kommentaari jätmiseks kasutage lahtrit Other)

- Jah
- Ei
- Ei oska öelda
- Muu

7. Kui ohutu on Teie arvates tähtsate dokumentide edastamine läbi ühiskaustade nagu Google Drive, DropBox jms?

Ei ole üldse oluline Väga oluline

1 2 3 4 5

## Lisa 5. Kvantitatiivse uurimuse küsimustik. Järg

8. Kes vastutab selle eest, kui andmeid hoitakse pilvesüsteemis ning neid on rikutud või väärkasutatud?

- Isik, kes andmed pilvesüsteemi üles laadis
- Pilvesüsteemi osutaja
- Andmekaitse Inspektsioon
- Muu

Andmed vastaja kohta:

Vanus:

- -18
- 18-28
- 29-39
- 40-50
- 50-...

Ametinimetus:

Ettevõtte suurus, kus töötate:

- -9 töötajat
- 10-49 töötajat
- 50-249 töötajat
- 250-... töötajat