TALLINNA TEHNIKAÜLIKOOL
Majandusarvestuse eriala
Ärikorralduse instituut

Maria Mussijenko

RAAMATUPIDAJA TEGEVUS JA VASTUTUS ANDMEKAITSESEADUSE RAKENDAMISEL

Bakalaureusetöö
Õppekava TABB, peaeriala majandusarvestus

Juhendaja: Natalie Aleksandra Gurvitš-Suits, PhD

Tallinn 2020

Deklareerin, et olen koostanud lõputöö iseseisvalt ja
olen viidanud kõikidele selle koostamisel kasutatud
teiste autorite töödele, olulistele seisukohtadele ja andmetele,
ning ei ole esitanud sama tööd varasemalt ainepunktide saamiseks.
Töö pikkuseks on 6 144 sõna sissejuhatusest kuni kokkuvõtte lõpuni.

Maria Mussijenko ……
(allkiri, kuupäev)
Üliõpilase kood: 164086TABB
Üliõpilase e-posti aadress: mariamussijenko@gmail.com

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

……
(allkiri, kuupäev)

Kaitsmiskomisjoni esimees:
Lubatud kaitsmisele

……
(nimi, allkiri, kuupäev)

SISUKORD

LÜHIKOKKUVÕTE

Bakalaureusetöö teema on «Raamatupidaja tegevus ja vastutus andmekaitseseaduse rakendamisel». Antud töö eesmärk on välja selgitada raamatupidajate teadlikkus ja suhtumine andmekaitseseaduse muudatustesse.

Eesmärgi saavutamiseks kasutati kvantitatiivset meetodit, mis põhines elektroonilises keskkonnas loodud küsimustikul. Küsimustikule vastasid raamatupidajad. Saadud tulemusi kirjeldati ning analüüsiti.

Kvantitatiivne analüüs näitas, et suurem osa vastajatest täidab teatud nõudeid töödeldavate isikuandmete kaitseks. Enamik vastajaid on nõus, et nende ettevõtte andmetöötlejad kasutavad isikuandmete kaitse seaduses sätestatud meetodeid. Vaatamata sellele, et vastajad järgivad ettevõttes määratud töötlemiseeskirju, tunnevad nemad puudust regulaarsetest andmekaitsega seotud seminaridest. GDPR nõuab andmete rikkumisest teatamist 72 tunni jooksul, kuid hoolimata asjaolust, et mitte kõik vastajad ei vastanud õigesti, selgus saadud andmete põhjal, et enamik vastanutest saab aru vajadusest kiiresti teavitada Andmekaitse Inspektsiooni andmevargusest. GDPR on toonud veel ühe mõiste, s.o andmekaitsespetsialist. Küsimustiku andmete kohaselt peab enamik vastanutest ettevõttes andmekaitsespetsialisti olemasolu oluliseks, seda vaatamata sellele, et nemad hindasid oma ettevõtte andmekaitset kõrgeks. Uuring näitas, et suurem osa vastanutest on isikuandmete kaitse seaduse muudatustest teadlik ja on rakendanud neid oma töös, kuid siiski on endiselt olemas märkimisväärne protsent töötajaid, kes andmetega töötades ei järgi andmetöötluse põhinõudeid.

Võtmesõnad: raamatupidamine, andmekaitse, GDPR, andmekaitse töötleja, andmekaitse spetsialist.

SISSEJUHATUS

Praegu arenevad tehnoloogiad üha kiiremini ja kiiremini ning inimesed töötlevad suurema hulga andmeid. Iga päevaga kerkib üks rohkem kohti ja võimalusi teabe vahetamiseks, millega seoses tõuseb andmekaitsele suunatud tähelepanu. Seetõttu on Euroopa Parlament ja Nõukogu (EL) välja töötanud andmekaitse määrustiku. Hoolimata sellest, et isikuandmete kaitse üldmääruse (GDPR) vastuvõtmisest on möödunud kolm aastat, on see teema endiselt aktuaalne ning määrustikuga seotud muudatusi ikka juurutatakse samm-sammult erinevates tegevusvaldkondades.

Seoses digitehnoloogiate arenguga tõuseb küberkuritegevuse ja kelmuste tase. Seetõttu tuleb andmekaitset kontrolli all hoida. Tööandjatel tuleb töötajate teadlikkust tõsta ja luua oma ettevõtetes uus andmekaitsespetsialisti ametikoht.

Autor valis oma töö teemaks andmekaitse, et aru saada, kuidas see on seotud raamatupidamisega. Antud töö eesmärk on välja selgitada raamatupidajate suhtumine isikuandmete kaitse seaduse muudatustesse ja teadlikkus nendest. Raamatupidaja igapäevaste kohustuste alla kuulub suure hulga andmete töötlemine. Oma töös tuginevad nad paljudele seadustele, sealhulgas isikuandmete kaitse seadusle. Sellega seoses peavad raamatupidajad selle muudatustest teadlikud olema. Diplomi kirjutamise ajal oli autori ülesanne vastata järgmistele küsimustele:

- Mida kujutab endast andmekaitse?
- Kuidas toimub andmekaitse Eestis?
- Milliseid võimalusi on isikuandmete kaitsmiseks?
- Kuidas on raamatupidaja seotud andmetöötlusega?
- Kuidas raamatupidajad suhtuvad andmekaitseseaduse muudatustesse?
- Kas igas ettevõttes peaks olema andmekaitsespetsialist?

Diplomitöö koosneb kahest osast – teoreetilisest osas „Andmekaitse“ ja praktilisest osast “Isikuandmete kaitse seadusega seotud muutused ning raamatupidamine“.

Teoreetiline osa koosneb kuuest osast, milles autor kirjeldab, mis endast kujutavad isikuandmeid ja nende kaitse; uurib andmekaitse ajalugu kuni määrustiku vastuvõtmiseni; informeerib andmekaitsest Eestis, millised seadused reguleerivad andmekaitset ja kes jälgib nende seaduste täitmist; loetleb isikuandmete kaitse meetodid; räägib andmekaitse olulisusest raamatupidamises. Samuti tõstatatakse teooriaga seotud peatükis andmetöötluse vastutuse teemat ning seda, kes on raamatupidaja andmetöötluses. Teoreetilise osa kirjutamiseks uuris autor Eesti seadusi, Euroopa Liidu määrusi, teaduslikku kirjandust ja andmekaitsealaseid artikleid.

Praktiline osa “Isikuandmete kaitse seadusega seotud muutused ning raamatupidamine“ koosneb kolmest osast: metoodika ja valimi kirjeldus, tulemuste kirjeldus ja tulemuste analüüs. Selgitamaks raamatupidajate suhtumist ja teadlikkust isikuandmete kaitse seaduse muudatustesse viidi küsimustiku põhjal läbi kvantitatiivne analüüs. Tulemused võeti kokku, nende põhjal tehti ja kirjeldati uuringu järeldused.

1. ANDMEKAITSE

1.1. Andmekaitse definitsioon

Isikuandmete kaitse on tänapäeval aktuaalne teema. Kui XX sajandil hoidis enamik ettevõtteid oma andmed paberil, siis uuel sajandil hoitakse suurem osa andmetest arvutifailides kas kohalikes arvutites või sagedamini pilves. Kaasaegsel tehnoloogia- ja teabeajastul vahetavad ja töötlevad inimesed iga päev tohutul hulgal andmeid ja soovivad võimaluse korral säilitada oma õiguse konfidentsiaalsusele.

Kõigepealt tuleb aru saada, mida kujutab endast andmekaitse. Väärib märkimist, et andmekaitset puudutav regulatsioon on suunatud füüsiliste isikute kaitsele andmetöötusel, mitte aga andmete enda kaitsele. Andmed on teave kellegi või millegi kohta (ÕS 1999 2003). Isikuandmed on igasugune teave tuvastatud või tuvastatava füüsilise isiku (andmesubjekti) kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal (ET määrus (EL) 2016/679 art 4 lk 1). Isikuandmete kaitse üldmääruses on määratletud kahte tüüpi isikuandmeid, kuid tegelikkuses võib eristada kolme isikuandmete kategooriat.

- Tavalised isikuandmed on teave inimese, st füüsilise isiku (andmesubjekti) kohta, mille abil saab teda otseselt või kaudselt tuvastada. Oluline on mõista, et konfidentsiaalsus eksisteerib ainult füüsilisel isikul, juriidilisel isikul puuduvad füüsilised andmed. Klassikalisteks isikuandmeteks loetakse näiteks nimi, isikukood, asukohateave, võrgutunnused, samuti füüsilised, füsioloogilised, geneetilised, vaimsed, majanduslikud, kultuurilised ja muud identifitseeritavad omadused ja nende kombinatsioonid.
  (Isikuandmed ja ... 2019)
- Tundlikke isikuandmeid ei tooda üldmääruses eraldi esile, kuid määratletakse andmetena, mis ohustavad inimese eraelu. Nende avalikustamine võib olla seotud isikuandmete

varguse, vara ja maine kahjustamisel tekitava riskiga elule ja tervisele jms. Näiteks loetakse sotsiaalabi saamist konfidentsiaalseks teabeks, nagu ka kriminaalmenetluse ja kogu menetluse vältel tehtud toimingutega seotud andmeid. Neid andmeid töödeldakse vastavalt isikuandmete kaitse üldmääruse artikli 6 lõikele 1. (ET määrus (EL) 2016/679 art 10) Tundlikeks andmeteks võivad olla andmed makseteenuste kohta pankades, krediitkaartide andmed, andmed digitaalallkirjade kohta, isiku rahalise seisu, laenude kohta, kommunikatsiooniandmed, mis lähevad kirjavahetuse saladuse alla jne.
(Isikuandmed ja ... 2019)

- Eriliiki isikuandmed on andmed, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine. Nendeks on ka biomeetrilised andmed, sõrmejäljed, peopesajäljed ja vikerkesta pildid, terviseseisu teave või isiku seksuaalse identiteedi andmed.(ET määrus (EL) 2016/679 art 9 lk 1)

Eesti Vabariigi põhiseaduses on sätestatud, et kõik on seaduse ees võrdsed. Kedagi ei tohi diskrimineerida rahvuse, rassi, nahavärvuse, soo, keele, päritolu, usutunnistuse, poliitiliste või muude veendumuste, samuti varalise ja sotsiaalse seisundi või muude asjaolude tõttu. (PS RT I 15.05.2015, 2; §12) Andmekaitse kaitseb inimest, täpsemalt inimese õigust informatsioonilisele enesemääramisele. Informatsiooniline enesemääramine on inimese põhiõigus ja vabadus valida, kellele ja milliseid andmeid avaldada (Männiko, M. 2011). Isikuandmete töötlemine on automatiseeritud või mitteautomatiseeritud toiming, toimingute kogum isikuandmete või nende kogumitega, näiteks kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja modifitseerimine, lugemine, kasutamine, edastamine, levitamine või muu avalikustamise, kooskõlastamise või integreerimise, piiramise, kustutamise võimalus.(ET määrus (EL) 2016/679 art 4 lk 2) Andmete töötlemisel järgitakse järgmisi põhimõtteid (IKS RT I, 04.01.2019, 11 ; §14):

- Seaduslikkus ja õiglus – isikuandmeid töödeldakse seaduslikult ja õiglaselt;
- Eesmärgi vastavus – isikuandmeid tuleb koguda vastavuses selgelt määratletud ülesandega ja töödelda lubatud viisidel;
- Kvaliteet – isikuandmed peavad olema asjakohased, aktuaalsed ja mitte ülemäärased töötlemise eesmärgi suhtes;
- Usaldusväärsus – andmed peavad olema õiged ja neid tuleb uuendada vajaduse korral. Kui selliseid andmeid peetakse ebatäpseteks, tuleb need kustutada või parandada (kasutaja nõudmisel);

- Säilitamine – isikuandmeid säilitatakse vormis, mis võimaldab andmesubjekte tuvastada mitte kauem, kui see on vajalik isikuandmete töötlemise eesmärgil; Isikuandmeid võib kauem säilitada, kui neid töödeldakse eranditult arhiveerimise eesmärgil ühiskonna, teaduse või ajaloo uurimise huvides või statistilistel eesmärkidel artikli 89 lõike 1 kohaselt, tingimusel, et võetakse vastu vastavad tehnilised ja korralduslikud meetmed andmesubjektide õiguste ja vabaduste kaitseks (ET määrus (EL) 2016/679 art 4 lk 2).
- Turvalisus – isikuandmeid töödeldakse viisil, mis tagab nende turvalisuse, sealhulgas kaitseb neid loata töötlemise ja ebaseadusliku töötlemise eest, samuti juhusliku kadumise, hävimise või kahjustamise eest, kasutades tehnilisi ja korralduslikke meetmeid.

Seega on vastutav töötleja kohustatud lihtsal ja kättesaadaval viisil teatama kasutajatele isikuandmete kogumise eesmärgid. Lisaks peab kasutajatel olema hõlbus juurdepääs nendest juba kogutud teabele. Teave peab olema täpne, kaitstud ja säilima piiratud aja jooksul. Samuti kohustub vastutav töötleja mitte koguma kasutaja kohta ebavajalikku teavet, vaid kogub ainult sellist teavet, mida on vaja näiteks kvaliteetsete teenuste osutamiseks.

Isikuandmete töötleja on isik, kes tegeleb isikuandmete töötlemisega. Andmesubjekt on isik, kelle isikuandmeid töödeldakse. Andmesubjekt on iga isik, kelle kohta on edastatud teave, mis on teada, mis kuulub ja mida kasutab kolmas osapool. (Männiko, M. 2011)

Õigusakt kaitseb isikuandmeid sõltumata nende töötlemiseks kasutatavast tehnoloogiast. See kehtib nii automaatse kui ka käsitsi töötlemise kohta, oluline on vaid see, et andmed oleksid korrastatud vastavalt eelnevalt määratletud kriteeriumidele, näiteks tähestiku järjekorras. Samuti ei ole oluline, kus andmeid hoitakse: elektroonilisel kandjal või paberil. Kõigil neil juhtudel kehtivad isikuandmete suhtes üldises andmekaitse määruses sätestatud kaitsenõuded. (Mis on ...)

Oluline on mõista, et Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2016/680 käsitleb füüsilise isiku kaitset seoses isikuandmete töötlemisega. Selleks võib olla igasugune teave, mida saab kasutada isiku tuvastamiseks. Isikuandmete töötlemisega on seotud paljud valdkonnad, nagu näiteks tervishoid, finants-, side- ja kindlustusteenused jne, kõik peavad järgima andmetöötluse reegleid.

1.2. Andmekaitse ajalugu

Andmekaitse ajalugu algab ammu enne GDPR ja muude teabe privaatsust käsitlevate seaduste vastuvõtmist. Isikuandmete kaitse mõte ja põhimõtted on kujunenud terve sajandi jooksul, tuginedes vajadusele kaitsta iga kodaniku eraelu.

1890. aastal avaldati *Harvard Law Review's* artikkel pealkirjaga *The Right to Privacy* („Õigus eraelu puutumatusele"), milles kaks Ameerika juristi, S. D. Warren ja L. D. Brandeis, kirjeldavad õigust olla üksinda jäetud (Warren, Brandeis 1890). 20. sajandi keskpaigale lähemal kajastub õigus eraelu puutumatusele ja muud põhiõigused Inimõiguste Ülddeklaratsioonis (Universal ... 1948) ning 1950. aastal on need kirjas Euroopa Inimõiguste Konventsiooni artiklis 8 (*Inimõiguste ja põhivabaduste ...*).

Ilmtingimata sellise tähelepanu enda õiguste kaitsele on põhjustanud ennekõike II maailmasõja kohutavad tagajärjed. Maailm muretses sõjajärgse perioodi oluliste sotsiaalsete probleemide – era- ja perekonnaelu puutumatuse, kirjavahetuse saladuse – pärast. Paraku ei rõhutatud tollal just isikuandmete kaitse olulisust.

XX sajandi teise poole alguses hakkavad arenema infotehnoloogiad, mis võimaldavad kiiremini töödelda palju rohkem teavet. 60ndatel aastatel sai tehnoloogia laiemale avalikkusele üha kättesaadavamaks. Sellega seoses avaldati 1968. aastal soovitus nr 509, mis kajastab võimalikke ohte eraelu puutumatusele seoses uute tehnoloogiate kasutamisega andmetöötluses.
(REC 509)

1970. aastal võttis Saksa Föderatiivne Vabariik vastu isikuandmete seaduse. Kindlasti väärib märkimist, et see oli kohalik ja seda kohaldati ainult Hesseni osariigis, mitte föderaalsel tasandil. 1974. aastal võeti USAs vastu *Privacy Act* (Eraelu puutumatuse seaduse), milles kajastub esmakordselt õiguse eraelule ja isikuandmete vaheline seos, (Scott 2016) st seadus sätestab, et riigiasutuste poolt isikuandmete kogumine, kasutamine ja levitamine võib otseselt puudutada inimese isikuandmeid. Kumbagi õigusakti ei saa nimetada täisväärtuslikuks seaduseks, mis reguleerib isikuandmete töötlemist, kuid mõlemas kajastus inimese õigus eraelule.

Esimesed isikuandmete kaitset käsitlevad õigusaktid ilmusid Saksamaal 1977. aastal (Raab 2010), järgmisel aastal võtab Prantsusmaa arvutiteaduse ja kodanikuvabaduste seaduse vastu.

Mõlemal riigil olid selleks oma eeldused. Saksamaal muutus isikuandmete kaitse oluliseks eriti seoses ajalooliste sündmustega. XX sajandil seisid sakslased silmitsi mitme poliitilise režiimiga, mis põhinesid elanikkonna jälgimisel. Väärib märkimist, et ka XXI sajandil on Saksamaa endiselt üks isikuandmete ja eraelu puutumatuse kaitse eestvedajaid. Seaduse vastuvõtmise Prantsusmaal põhjustas 70-ndate aastate projekt, s.o ühtne andmeregister iga kodaniku tuvastamiseks sotsiaalkindlustuse numbri alusel. Antud projekt põhjustas skandaali elanikkonna massjälgimise tõttu. 1978. aastal anti välja seadus ja loodi arvutiteaduse ja kodanikuvabaduste komisjon. Registriprojekt viidi ellu, kuid uus komisjon suutis kehtestada teatud piirangud isikuandmete töötlemisel. (Talapina 2012)

Arvestades tehnoloogia arengut, töötati 80ndatel peamised rahvusvahelised võtmedokumendid välja, millega kehtestati isikuandmete kaitse alused ja protseduurid (Hert 2013), vastu võeti esimene rahvusvaheline leping andmete privaatsuse valdkonnas (*Data Privacy*), milleks on isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. See konventsioon on olnud oma valdkonnas suur saavutus. Praeguseks on sellega ühinenud 51 riiki. (*Üksikisikute kaitse konventsioon* ... 1981)

1990ndatel aastatel toimusid olulised muutused tehnoloogiates. Need tõid kaasa põhimõttelised muudatused juhtimispraktikas (riigi raamatupidamissüsteemid, julgeolek ja kuritegevusevastane võitlus). Kuna isikuandmete kogumine, säilitamine ja töötlemine on riikidevahelise interneti põhise äri üks alustalasid, hakkasid äristruktuurid ilmutama aktiivset huvi isikuandmete kaitsepoliitika väljatöötamise vastu. Muutus aktuaalseks ka tegevus rahvusvahelisel tasandil. 1995. aastal avaldati Euroopa Liidu andmekaitsedirektiiv 95/46/EÜ. Selle seaduse peamine eesmärk on kohaneda uute ohtudega ja ühtlustada ELi liikmesriikide isikuandmeid käsitlevad õigusaktid. Selleks täiustati 1981. aasta rahvusvahelises konventsioonis ette nähtud mehhanismid, samuti juurutati ka isikuandmete käitajate uued kohustused ja ELi kodanike uued õigused. (Paziuk, Sokolova 2015)

XX sajandi lõpuks struktureeriti isikuandmete kaitse poliitilise probleemina ja see tagati rahvuslike strateegiate ja seaduste, rahvusvaheliste lepingute, põhimõtete, soovituste ja deklaratsioonide alusel (*Ibid.*).

XXI sajandi alguses hakkasid interneti kasutajad üha enam tunnetama digitaalse arengu mõju. See tekitas aktiivseid arutelusid teabe privaatsuse võimalike ohtude ja nende ohtude ennetamise

võimaluste üle. 2002. aastal võttis EL vastu e-privaatsuse (*ePrivacy*) direktiivi, mis reguleerib sh reklaami tarbeks andmeid kogutavate küpsiste kasutamist. (EN direktiiv 2002/58/EC)

Järgnevatel aastatel seisab maailm silmitsi tõsiste skandaalidega, mis on seotud küberturbe ja andmetöötlusega üldiselt. Võib esile tõsta Julian Assange'i WikiLeaksi (Ayala, Neuman 2012), samuti ka Edward Snowdeni ameeriklaste PRISMi massjälgimisprogrammi päevavalgele toomise.

Seoses nende sündmustega otsustab EL 1995. aasta direktiivi ajakohastada ja täiustada. Antud direktiivi ei kohaldatud otseselt ELi liikmesriikides, mis põhjustas olulisi erinevusi rahvuslike õigusaktide tasandil. Uue seaduse arutelud algasid 2012. aastal, isikuandmete kaitse üldmääruse (ingl. *General Data Protection Regulation, GDPR*) ametlik tekst avaldati 2016. aastal, määrus jõustus 25. mail 2018. Praegu kehtib see Euroopa riikides ja hoiab andmekaitse taset ELis ülal. (ET määrus (EL) 2016/679)

Esmajärjekorras kehtivad GDPRi nõuded järgmistele ettevõtetele, kes:

- töötavad Euroopa juriidiliste või füüsiliste isikutega, olenemata ettevõtte asukohast;
- jälgivad Euroopa elanike käitumist kauba või teenuste pakkumise eesmärgil.

Lisaks võeti samal aastal vastu NIS (ingl. *Network and Information Security*, et. võrgu- ja infoturbe) direktiiv. Selle õigusakti peamine eesmärk on tagada elutähtsate infrastruktuuride ettevõtjatele ja digitaalteenuste pakkujatele kõrgetasemeline infoturve. Silmas peetakse lisaks isikuandmete kaitsele ka kõigi andmete turvalisuse kaitset. (direktiiv (EL) 2016/1148)

Need ja paljud teised seadused on Euroopa Liidu elektroonilise side, küberturbe ja andmete privaatsuse valdkonda puudutava poliitika tulemus. ELi järgmine samm peaks olema e-privaatsuse (ingl. *ePrivacy*) määruse vastuvõtmine, mis peaks asendama 2002. aasta samanimelist direktiivi. Selle reformi põhiküsimused on metaandmed (ingl. *Big Data*, et. suurandmed) ja jällegi küpsised. Määruse eelnõu avaldati juba 2017. aasta alguses. (EK ettepanek 2017/0003 (COD))

1.3. Andmekaitse olemus Eestis

Eesti on ELi liige ja loomulikult mõjutasid teda kõik muudatused, mille põhjustas GDPRi vastuvõtmine, kuid igal riigil on oma seadused ja teenistused, mis täiendavad üldist andmekaitse määrust.

Eesti Vabariigi põhiseaduse § 26 sätestab (PS RT I, 15.05.2015, 2), et igaühel on õigus perekonna- ja eraelu puutumatusele. Riigiasutused, kohalikud omavalitsused ja nende ametiisikud ei tohi kellegi perekonna- ega eraellu sekkuda muidu, kui seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks, st see tähendab, et kõigil on õigus privaatsusele (Tikk, Nõmper 2007) Euroopa Kohus ja Eesti Riigikohus on seisukohal, et isikuandmete kaitse on konfidentsiaalsuse kaitse üks olulisi valdkondi; isikuandmete kogumine, säilitamine, kasutamine ja avalikustamine, olenemata nende vormist, on aga isikuandmete puutumatuse rikkumine.

Eestis reguleerib andmekaitseküsimusi Isikuandmete kaitse seadus[1], milles täpsustatakse ja täiendatakse Euroopa Parlamendi ja Nõukogu (EL) nr 2016/679 määruses sisalduvaid sätteid. (IKS RT I, 04.01.2019, 11 §1 lk1). IKS kehtestab normid määruse juurutamiseks ja selle laenamiseks (*Ibid*. lk 2). Eesmärk on kaitsta füüsiliste isikute põhiõigusi ja -vabadusi isikuandmete töötlemisel, muuhulgas õigust eraelu puutumatusele, sellest järeldub, et suhted teiste inimestega ja inimestevahelised kontaktid on samuti konfidentsiaalsed andmed (Pilving 2005).

Isikuandmete kaitse üldmäärus kehtestab rangeid reegleid nõusolekul saadud andmete töötlemiseks. Kui keegi nõustub oma isikuandmete töötlemisega, saab andmeid töödelda ainult nendel eesmärkidel, milleks nõusolek anti. On ka erandeid. IKSi artiklis 2 on kirjas, et isikuandmeid saab töödelda ilma nõusolekuta, kui selleks on märkimisväärne avalik huvi ja see vastab eetikapõhimõtetele, samuti juhul, kui ilma nende andmete kogumiseta ei ole võimalik saavutada uurimistöö eesmärki. On oluline, et isikuandmete avaldamine ei kahjustaks liigselt andmesubjekti õigusi. (IKS RT I, 04.01.2019, 11 p.2)

Seadus kajastab andmetöötluse üldsätteid ja -põhimõtteid. Seadus määrab kindlaks andmesubjekti õiguse teabe kättesaadavusele ja tema õiguse pöörduda Andmekaitse Inspektsiooni poole. Isikuandmete töötlemise ajal võivad isikuandmeid sattuda erinevate ettevõtete või organisatsioonide kätte. Selle eest vastutab andmetöötleja. IKS artikkel 4 reguleerib vastutava ja volitatud töötleja kohustusi. GDPR tutvustab vajadust määrata andmekaitsespetsialist. IKS artiklid 40-42 selgitavad kõiki andmekaitsespetsialistiga seotud punkte. (IKS RT I, 04.01.2019, 11)

Eestis teostab riiklikku ja haldusjärelevalvet Andmekaitse Inspektsioon (AKI). Oma ülesannete täitmisel on ta sõltumatu ja tegutseb lähtudes IKSist, GDPRist ja teistest nende alusel kinnitatud seadustest ja õigusaktidest. (IKS RT I, 04.01.2019, 11 §51) Andmekaitse Inspektsiooni ettekirjutuse täitmata jätmisel ühekordne maksimaalne trahvimäär on kuni 20 000 000 eurot või kuni 4 protsenti ettevõtja eelmise majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem. (*Ibid.* §60) Kui isikuandmete kadumisega seotud rikkumine kujutab endast ohtu füüsilisele isikule, teatab vastutav töötleja rikkumisest AKIile viivitamata, võimalusel 72 tunni jooksul. (*Ibid*. §44).

Seoses 2020. aasta pandeemiaga tekkis andmetöötluse kohta palju küsimusi. Euroopa andmekaitsenõukogu võttis 19.03.2020 vastu avalduse isikuandmete töötlemise kohta COVID-19 puhangu kontekstis. (Jelinek 2020) Jooksevolukorrast lähtuvalt soovitab AKI nii tööandjatel kui ka töötajatel kohaselt hinnata hädaolukorras terviseandmete kogumisel sihipärasuse, minimeerimise ja proportsionaalsuse kontseptsiooni. Seega on tööandjal ilmtingimata õigus küsida, kas töötaja on hiljuti viibinud riskitsoonis, kas ta on olnud kontaktis nakatunud inimestega. See teave ei ole isiklik, nagu on tervise, sümptomite kohta käiv teave, mis tuleb vastastiku mõistmisega jagada. Üldiselt on tööandjal praeguse olukorra kontekstis ilmselt õigus paluda töötajal kinnitust, et ta ei ohusta teisi töötajaid ja töökeskkonda tervikuna, sest tööandja seaduslik kohustus on tagada kõigile töötajatele turvalise keskkonna. (Töötajate isikuandmete ... 2020) Seetõttu on hädavajalik, et töötaja edastab tööandjale vabatahtlikult oma tervisega seotud teavet maksimaalsel võimalikul kujul. „*Märksõnadeks on nagu andmekaitse puhul ikka: nii palju kui vajalik ja nii vähe kui võimalik.“* (Kas töötajat saab ... 2020)

1.4. Andmekaitse meetodid

Vaatamata sellele, et mõiste „informatsiooniline privaatsus" (ingl. *information privacy, data privacy*) lisati Euroopa ekspertide sõnaraamatusse juba 1960–70ndatel aastatel, tehnoloogiate kiire areng, paljude tööprotsesside arvutistamine, andmete integreerimise projektide elluviimine rahvuslikul tasandil toob kaasa palju rikkumisi, mis on seotud teabe töötlemise ja edastamisega. Raamatupidajad puutuvad iga päev silmitsi andmetöötlusega, seetõttu mängib andmekaitse nende tööprotsessis olulist rolli. Alustuseks tasub määratleda raamatupidaja igapäevased tööülesanded, et paremini mõista nende tööks vajalikku kvaliteetset andmekaitse taset.

Raamatupidaja töö hõlmab järgmisi ülesandeid (Millega tegeleb ... 2018):

- ettevõtte arvete tasumine;
- rahavoogude aruandlus;
- arvete tasumise kontroll vastavalt ettevõtte sise-eeskirjadele ja õigusaktidele;
- tehinguid puudutavate riiklike maksude (tulu-, sotsiaalmaks jne) arvutamine;
- töötajate töötasu ja puhkuse arvestamine ning nende eest maksmine;
- arveregistri pidamine;
- aruannete esitamine Maksu- ja Tolliametile;
- juhatuse finantsnõustamine.

Raamatupidaja kohustuste hulka kuulub ka näiteks ettevõtte kõigi tulude ja kulude arvestamine, raamatupidamise majandusaruandluse pidamine ja finantstehingutega seotud aruandluse pidamine vastavalt raamatupidamise seadusele (*Ibid*.)

Ülaltoodu valguses on selge, et seoses tööülesannetega peab raamatupidaja kokku puutuma väga paljude oluliste andmetega nii enda ettevõtte kui ka partnerettevõtte puhul, muuhulgas ettevõtete pangaandmete, salasõnade, rahalise seisundi, palgaandmete, töötajate tervisega jm seoses. Seetõttu on oluline, et raamatupidaja tegutseb pidades isikuandmete kaitse reeglitest kinni. Selgeid andmetöötlusreegleid peab kehtestama iga ettevõte ja nende järgimine on osa andmekaitsest. Allpool on toodud neli põhireeglit (McKenzie L. Kuhn 2018):

- Minimeerimine – ettevõtted peavad koguma, säilitama ainult vajalikku hulka isikuandmeid, et täita oma seaduslikke ärieesmärke ja kustutama andmed kolme aasta möödudes. See aitab vältida suurte andmemahtude säilitamist, mis tekitab häkkeritele

suurt huvi ja vähendab andmete rikkumise korral tarbijatele tekitatavat kahju. Lõuna-Korea näitel, kus ulatuslikud rikkumised 2004-2014. aasta andmetes põhjustasid 80% identifitseerimisnumbri vargused, tõendab minimeerimise vajadust. Riik oli sunnitud välja vahetama kogu oma riikliku identifitseerimissüsteemi, mis maksis miljardeid dollareid. Selle tulemusel võttis Lõuna-Korea vastu seaduse, mis kohustab kodaniku identifitseerimisnumbrit töötlevaid ettevõtteid kustutama selle kahe aasta möödudes.

- Krüpteerimine – ettevõtted peavad andmed krüpteerima selleks, et kaitsta selliseid konfidentsiaalseid isikuandmeid nagu terviseteave, sotsiaalkindlustuse ja pangakonto number. Sellega tagavad ettevõtted, et isegi andmete häkkimise korral on välistatud tarbijate isiku kahjustamise või isikuandmete varguse oht, kuna isikuandmetele ei pääse juurde ilma krüptimisvõtmeta.
- Rikkumisest teatamine – ettevõtted peavad tarbijatele määratud aja jooksul teatama, kui nende isikuandmed on rikutud. Sellistel ettevõtetel nagu Equifax ja Yahoo kulus andmerikkumisest teatamiseks kuid või isegi aastaid. Selle tulemusel kaotavad tarbijad väärtuslikku aega, mida nad saaksid kasutada oma identiteedivarguse eest kaitsmiseks, muutes oma finantsteavet või sulgedes oma pangakontod.
- Andmete töötlemise nõusolek – enne kui ettevõtted saavad isiklikku teavet koguda, säilitada või jagada, peavad ettevõtted andmete kogumisel veenduma, et tarbija on andnud selleks nõusoleku. GDPR kohaselt peab nõusolek olema selges ja lihtsas keeles esitatud taotlusega vabatahtlikult antud, konkreetne, teadlik ja ühemõtteline tarbija nõusolek tema isikuandmete töötlemiseks.

Advokaadibüroo BakerHostetler aruande kohaselt moodustasid andmepüügi/häkkerite/õelvara rünnakud 2015. aastal 31% juhtumitest (Beckett Ference 2017), samas kui PriceWaterhouseCoopersi 2016. aasta aruandest selgub, et küberkuriteod on suuruselt teine registreeritud majanduskuritegu, mõjutades 32% organisatsioonidest ning 56% ohvritest ei tea, et nende andmed varastati. Sellest järeldub, et enamik ohvreid ei ole nendevastasest kuriteost kuigi teadlikud. (Zaharia 2016)

Sellest järeldub, et elektroonilises keskkonnas töötades peavad raamatupidajad olema tähelepanelikud ja ettevaatlikumad. Enne lingil klõpsamist peab veenduma, et see on ohutu. Faili allalaadimisel on parem kasutada mainepõhist tehnoloogiat ühendavat veebilehitsejat, mis analüüsib faili osade olemust ja päritolu. Tehingute ja finantstehingute jaoks on hädavajalik kasutada krüpteeritud andmed ja turvalisi veebilehte. (*Ibid*.) Dokumentide säilitamiseks ja

edastamiseks on parem kasutada pilveteenust, mis pakub saatjale üleslaadimisel krüpteerimist ja saajale allalaadimisel dekrüpteerimist. (Sleeter 2012)

Andmekaitse profülaktika eesmärgil saab iga ettevõte kasutada järgmisi meetmeid (Tejada 2017):

- Andmekaitsetaseme kontroll. Kolmanda osapoole poolt iga-aastane süsteemiaudit on hea tava ettevõtetele, kes töötlevad regulaarselt konfidentsiaalset teavet. Klientidele on sellised regulaarsed kontrollid kindlasti lisaväärtus ja turvalisuse tagamine meede.
- Tehniliselt ohutu keskkonna loomine. Igas organisatsioonis peab olema paigaldatud viirusetõrjetarkvara ja standardne e-posti filtreerimistarkvara. Ettevõte peaks oma kliente teavitama, et e-post ei pruugi olla parim viis konfidentsiaalsete ja finantsandmete jagamiseks. Enne saaja postkasti jõudmist läbib saadetud e-kiri mitut kohta (serverit). Kui sõnum on krüpteerimata, saavad seda häkkerid kinni pidada. Andmete krüpteerimine, varundamine, nende taastamise kava ja äritegevuse järjepidevuse kava võivad kaitsta ettevõtet võrgu katkestuste eest, seetõttu tasub välja töötada turvaline andmevahetussüsteem, mis vähendab häkkimise ohtu (Yeaman 2017; Tejada 2017):
- Juurdepääsu kontroll ja piiramine – töötajate kiipkaartide, külastajate kaartide kasutamine ja kontrollitud juurdepääs kohtadesse, kus hoitakse ettevõtluse jaoks olulist teavet, tagavad kogu ettevõttes usaldusväärse jälgimise ja liikumise kontrolli. Kohase juurdepääsu kontrollimisega saavad ettevõtted kontrollida, kes näeb, saab muuta ja jagada andmeid kogu organisatsiooni raames. On oluline, et neid andmeid perioodiliselt uuendataks.
- Usaldusväärse võrgu kasutamine. Wi-Fi võrku tuleb kaitsta paroolide ja krüpteerimisprotokollidega. Samuti soovitatakse külalisvõrgud sisevõrgust täielikult eraldada.
- Failide regulaarne kopeerimine. Kui arvutid on vastuvõtlikud viiruste või õelvara rünnakutele, aitab regulaarne varundamine taastada kaotatud andmeid. Kliendifailide regulaarne varundamine on hea tava.
- Töötajate teavitamine ja koolitamine. Ettevõtte andmekaitse kõige olulisem element on töötajate koolitamine. Oluline on töötajaid ohutusküsimustes perioodiliselt koolitada ja parimaid tavasid rakendada. Ettevõte peab tagama, et tema töötajad oleksid teadlikud sellistest protokollidest nagu BYOD (et. „too enda seade") ja mobiilsete seadmete kasutamisest, krüpteerimispoliitikatest, salasõnadest jne. Tasub keelata töötajate

juurdepääsu kliendiandmetele nende isiklike arvutitega, kuna võib põhjustada turvalisuse probleemi.

- Klientide julgustamine aktiivselt osalema oma andmeturbe jälgimises. Peab veenduma, et kliendid saavad aru, kuivõrd oluline on regulaarselt jälgida, mida nende äri kohta räägitakse. Avalikud dokumendid sisaldavad sageli vigu ja ettevõtte maine regulaarne jälgimine võimaldab isikuandmete vargust varem tuvastada.

Oluline on aidata töötajatel riske ja nende maandamise viise mõista. Järgides vähemalt osa reegleid, vähendavad ettevõtted nii enda kui ka enda klientide isikuandmete varguse riski.

1.5. Andmekaitse olulisus raamatupidamises

Ei saa raamatupidamise olulisust ega ka selle kaitset alla hinnata. Raamatupidamisarvestus on ettevõtte äri juhtimise oluline ja lahutamatu osa. Raamatupidamisarvestus kajastab teavet äritegevuse kvantitatiivsest ja kvalitatiivsest küljest. Raamatupidamisarvestus on vajalik ettevõtte tegevuse kohta usaldusväärsete andmete õigeaegseks esitamiseks teadlike juhtimisotsuste tegemisel tugevdamaks toodete konkurentsivõimet ja ettevõtte stabiilset positsiooni tootmisturul.

Raamatupidamine täidab kontrolli- ja teabefunktsiooni, tagab omandi turvalisuse, pakub teavet analüüsi jaoks, loob tagasiside tegelike tootmisnäitajate ja tulevikuplaanide vahel. See näitab, et raamatupidajad töötlevad iga päev tohutul hulgal andmeid. Seetõttu on oluline, et raamatupidamine toimuks vastavalt andmekaitse põhimõtetele. Isikuandmete kvalifitseeritud kaitse näitab ettevõtte taset ja suurendab usaldust nii ettevõtte kui ka töötajate vastu. Sellest järeldub, et raamatupidamisarvestuse korraldamise ja teabe esitamise meetodid peavad vastama nii RPSis kehtestatud nõuetele ja finantsaruandluse standarditele nagu Eesti Finantsaruandluse Standard või Euroopa Komisjoni poolt vastu võetud Rahvusvahelised Finantsaruandluse Standardid (IFRS) jne, aga ka ELi isikuandmete kaitse üldmäärus (GDPR) ja Eesti Vabariigi andmekaitseseadus, mida käsitleti lähemalt eelmistes peatükkides.

1.6. Andmekaitse spetsialist ja töötleja

Isikuandmete töötlemise ajal võivad isikuandmeid sattuda erinevatele ettevõtete või organisatsioonide kätte. Isikuandmeid töötlevas tsüklis on kaks peamist osalejat: vastutav andmetöötleja ja volitatud andmetöötleja. (Isikuandmete kaitse … 2020)

Vastutav töötleja on vajadusel kohustatud tõestama IKS seaduses kehtestatud nõuete täitmist, samuti andma volitatud töötlejale andmetöötluse jaoks siduvaid juhiseid ning vastutama selle eest, et volitatud töötleja täidab isikuandmete töötlemisele esitatavaid nõudeid. Kui volitatud töötleja määrab andmekaitseseadusega vastuolus olevad isikuandmete töötlemise eesmärke ja viise, saab temast vastutav töötleja. (IKS RT I 04.01.2019, 11 §29)

Vastutav andmetöötleja määrab volitatud töötleja, kes on kohustatud (*Ibid*. §30):

- Tegutsema ainult vastutava töötleja juhiste kohaselt;
- Säilitama talle tööülesande täitmise ajal teatavaks saanud isikuandmeid;
- Kaitsma andmesubjekti õigusi;
- Kustutama või tagastama vastutavale töötlejale kõik isikuandmed ja nende koopiad.

Vastutav ja volitatud töötleja kasutab asjakohaseid tehnilisi ja organisatsioonilisi meetmeid, mis tagavad, et töödeldakse ainult isikuandmeid, mis on vajalikud konkreetsel töötlemise eesmärgil (*Ibid*. §33).

Kuna raamatupidaja töötleb töötajate töötasude ja sotsiaalkindlustuse andmeid, võib öelda, et isikuandmete töötlemine on osa raamatupidaja põhitegevusest.

Palgaarvestuse protsessis töödeldakse töötajate majandusandmeid. Lisaks tegelevad raamatupidajad tervisekindlustuse, maksude ja kindlustusmaksetega, st andmetega, mis on seotud tulu- ja sotsiaalmaksu, tervisekindlustuse, töötuskindlustusmaksetega jms. Töötaja tervisekindlustuse eesmärgil töötlevad raamatupidajad andmeid töötaja tervise kohta, näiteks teavet töötaja lapsehoolduspuhkuse, rasedus- ja sünnituspuhkuse, osalise või täieliku töövõimetuse, põhipuhkuse jms kohta. Seega võib väita, et raamatupidamise spetsialistid on isikuandmete töötlejad.

Andmekaitse üldmääruse (GDPR) kohaselt peavad andmetöötlejad, kelle põhitegevuseks on isikuandmete suuremahuline töötlemine, määrama andmekaitsespetsialistid (ingl. k. DPO ehk Data Protection Officer) ja teavitama sellest Andmekaitse Inspektsiooni ja avalikkust ettevõtja portaali kaudu.

AKS on järelevalveorgani ja andmesubjektide kontaktisik. GDPRi artikkel 37 lõige 1 sätestab, et allpool loetletud isikuandmete töötlejad peavad määrama andmekaitsetöötaja (Isikuandmete töötleja ... .2019):

- valitsusasutus;
- vastutavad töötlejad, kelle põhitegevuseks on andmesubjektide ulatuslik regulaarne ja süsteemne jälgimine;
- vastutavad töötlejad, kelle põhitegevuseks on teatud tüüpi andmete ulatuslik töötlemine või isikuandmete ulatuslik töötlemine seoses süüdimõistvate kohtuotsuste ja kuritegudega. Andmetöötluse ulatuse määramisel lähtub Andmekaitse Inspektsioon ennekõike sellest, kui palju inimesi jälgitakse (näiteks kliendiandmebaasi põhjal). Erikategooria andmete puhul loetakse suuremahuliseks 5000 või enama inimese andmeid.

AKS võib olla organisatsiooni töötaja või teenuslepingu alusel välistöötaja. Andmekaitsespetsialist võib olla üksikisik või organisatsiooni üksus (Isikuandmete kaitse ... 2020). Kui aga andmekaitsespetsialisti ülesandeid täidab ettevõtte üksus või mõni muu juriidiline isik, peab üldsuse ja järelevaataja vaheline kontaktisik olema üks isik konkreetsete kontaktandmetega. (Andmekaitsespetsialist 2019)

Andmekaitsespetsialisti ülesandeks on tagada, et ettevõte järgib uue määruse sätteid. Andmekaitsespetsialist nõustab ettevõtjat määrusest tulenevate kohustuste täitmisel, tagab andmekaitsenormide järgimise, tõstab töötajate teadlikkust ja korraldab nende koolitusi ja andmekaitsega seotud auditi. Lisaks teeb ta koostööd riiklike andmekaitsejärelevalve asutustega (AKI) ja on kontaktisik andmekaitse valdkonnas. (IKS RT I 04.01.2019, 11 p.5)

Andmekaitsespetsialistile, nagu ka raamatupidajale, ei ole kehtestatud diplomi- ega muid kvalifikatsiooninõudeid. Siiski on soovitatav, et selline spetsialist saaks asjakohase väljaõppe. Sellise koolituse võib saada ka raamatupidaja ja asuma täitma andmekaitse spetsialisti

ülesandeid, kuid tuleb aru saada, et see toob endaga kaasa uusi kohustusi ja vastutust. Iga raamatupidaja peab otsustama, kas ta on sellisteks muudatusteks valmis.

2. UURING „ISIKUANDMETE KAITSE SEADUSEGA SEOTUD MUUTUSED NING RAAMATUPIDAMINE”

2.1. Metodoloogia ja valimi kirjeldus

Lõputöö teoreetilises osas on tõstatatud isikuandmete kaitsega seotud teemad. On määratletud isikuandmete kaitse töötlemise mõisted, samuti määratletud, mida kujutab endast töötleja ja andmekaitsja. On kirjeldatud isikuandmete kaitse töötlemise põhimõtted ja meetodid, samuti see, millised seadused ja kes reguleerib andmekaitset Eestis. Selle põhjal valmis bakalaureuse töös püstitatud eesmärgi saavutamiseks vajalik küsimustik. Antud töö eesmärk on välja selgitada raamatupidajate suhtumine isikuandmete kaitse seaduse muudatustesse ja teadlikkus nendest.

Küsimustik koostati Google Forms'i elektroonilises keskkonnas, vastajad olid peamiselt raamatupidajad. Küsimustik oli avatud vastuste saamiseks ajavahemikul 06.04.2019 kuni 08.05.2019 ja seisuga 08.05.2019 vastas sellele 117 inimest. Küsimustik oli anonüümne ja koosnes 26 küsimusest ja sisaldas nii valikvastustega kui ka hinnanguid nõudvaid küsimusi, mis põhinevad viiepunktilisel Likerti skaalal, kus 1 – ei ole täiesti nõus, 2 – ei ole nõus, 3 – nii ja naa, 4 – olen nõus, 5 – olen täiesti nõus. Küsimustik koostati kahes keeles, et hõlmata suuremat arvu vastajaid. Küsimustiku ankeet on esitatud lisas 1. Ankeet töödeldi MS Exceli tarkvara abil ja selle vastused on toodud lisas 2.

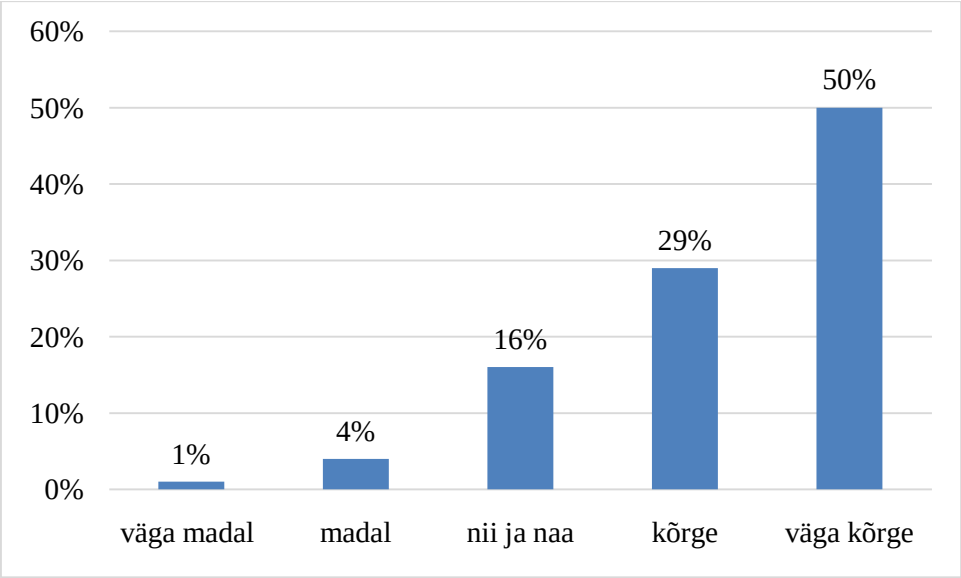
Küsitluses osales kokku 117 inimest, kellel paluti vastata küsimustele oma ametikoha, raamatupidaja töökogemuse ja hariduse ning nende organisatsiooni tegevusvaldkonna kohta. 84,6% (99) vastanutest on majandusharidus. 32,5% (38) vastanutest on 0-3-aastase töökogemusega; 28,2% (33) on 4-6-aastase töökogemusega; 16,2% (19) on 7-9-aastase töökogemusega; 13,7% (16) on üle 12-aastase töökogemusega; 5,1% (6) on 10–12-aastane töökogemus ja 4,3% (5) ei oma üldse töökogemust. 117-st vastanutest 35% (41) töötab raamatupidaja ametikohal; 27,4% (32)töötab raamatupidaja abi ametikohal; 19,7% (23) töötab muul ametikohal ja 17,9% (21) on pearaamatupidajad.

Ettevõtete tegevus on esitatud Eesti majanduse tegevusalade klassifikaatori (EMTAK) alusel. 12,8% (15) vastanutest töötab info ja side tegevusvaldkonnas; 12% (14) töötab ehituse tegevusvaldkonnas; 11.4% (13) töötab majutuse ja toitlustuse tegevusvaldkonnas; 8,5% (10) töötab finants- ja kindlustustegevuse tegevusvaldkonnas ja samapalju töötab tervishoiu ja sotsiaalhoolekande tegevusvaldkonnas; 7,7% (9) töötab veonduse ja laonduse tegevusvaldkonnas, 6,8% (8) kinnisvaraalase tegevuse valdkonnas; 6% (7) vastanutest vastas, et nemad töötavad ettevõttes, mille tegevusvaldkond on muud teenindavad tegevused; 5,1%(6) töötab hulgi- ja jaekaubanduse valdkonnas, 4,3% (5) töötab hariduse tegevusvaldkonnas, 3,4% (4) töötab elektrienergia, gaasi, auru ja konditsioneeritud õhuga varustamise tegevusvaldkonnas; 2,6% (3) töötab põllumajanduse, metsamajanduse ja kalapüügi tegevusvaldkonnas, samapalju vastanutest töötab kodumajapidamiste kui tööandjate tegevuse ning kodumajapidamiste oma tarbeks mõeldud eristamata kaupade tootmise ja teenuste osutamise valdkonnas; 1,7% (2) töötab avaliku halduse ja riigikaitse ning kohustusliku sotsiaalkindlustuse tegevusvaldkonnas;, samapalju vastanutest valisid haldus- ja abitegevuste valdkonna, ning samapalju vastanutest esindab kunsti, meelelahutuse ja vaba aja ning kutse-, teadus- ja tehnikaalase tegevuse valdkondi.

Saadud andmete põhjal võib väita, et vastajate valim on mitmekesine ja autori arvates annab see uuritavast teemast täpsema pildi.

2.2. Uuringu tulemused

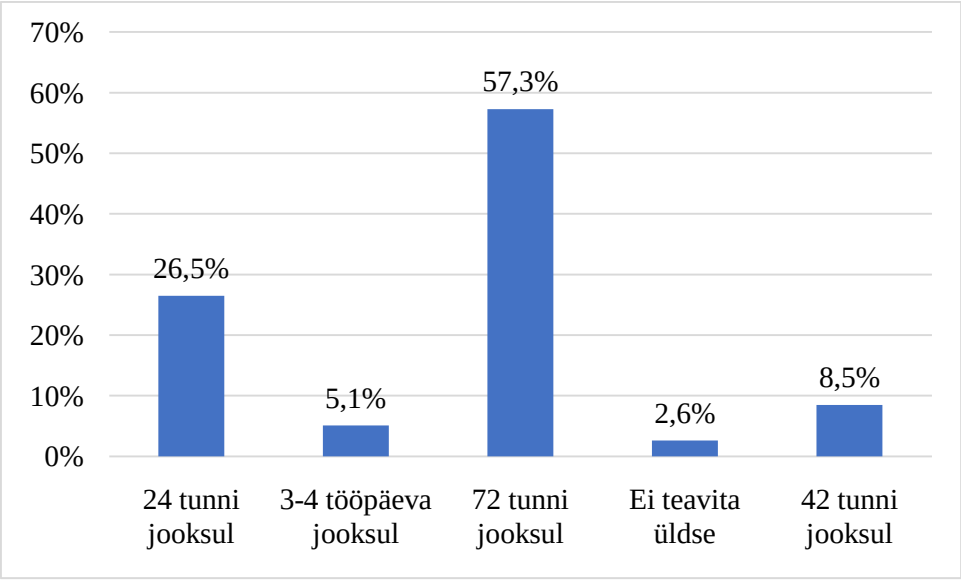
Uuringu andmete kohaselt on 85,5% (100) vastanutest varem andmekaitse-eeskirjadest kuulnud, 14,5% (17) vastanutest ei kujuta GDPRist midagi. 100 vastanust 50% (50 inimest) arvab, et nende ettevõtte kaitsetase on kõrge, mis on võrdne 5-ga (Likerti viiepunktiskaala kohaselt), 16% (16) 100-st vastajast arvab, et nende ettevõtte kaitsetase on keskmine, mis on võrdne 3-ga (Likerti viiepunktiskaala kohaselt) ja 5% (5 inimest) 85,5% vastanust leiab, et nende ettevõttes on kaitsetase keskmisest madalam, mis on võrdne 1 või 2-ga (Likerti viiepunktiskaala kohaselt). Tulemused on kajastatud joonisel 1.



Joonis 1. Vastajate ettevõtte andmekaitse tase (n=100)

Allikas: autori koostatud lisa 2 alusel

57,3% (67) vastanutest ütles, et andmete häkkimisest tuleb Andmekaitse Inspektsioonile teatada 72 tunni jooksul, 35% (41) vastanutest arvab, et rikkumisest tasub teatada varem kui 72 tundi. 5,1% (6) vastanutest usub, et isikuandmete vargusest tasub teada anda 3-4 tööpäeva jooksul ja 2,6% (3) vastanutest leidis, et isikuandmete häkkimisest ei tasu teatada. Tulemused on näidatud joonisel 2.

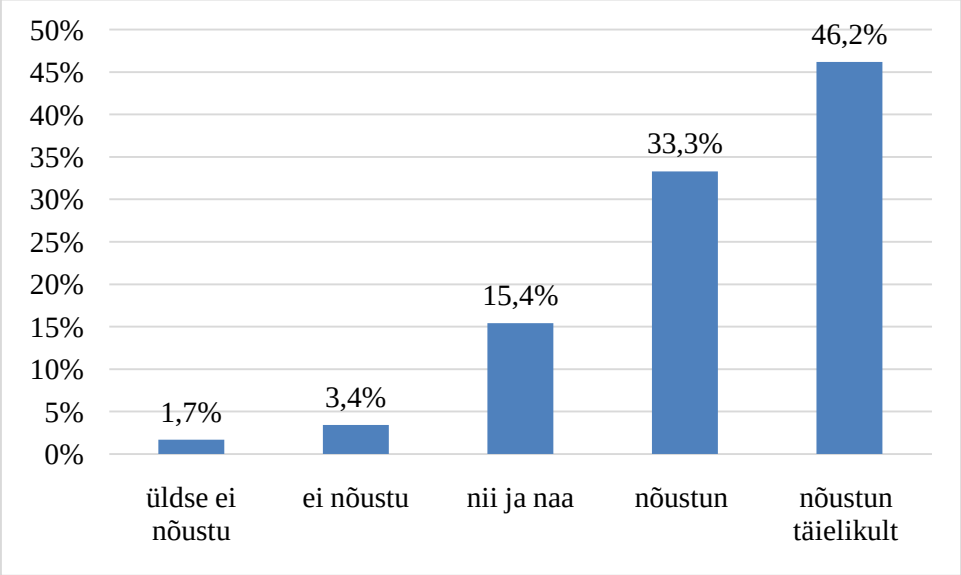


Joonis 2. Küsitletute vastused küsimusele, millal tuleb andmete rikkumisest teatada inspektsioonile (n=117)

Allikas: autori koostatud lisa 2 alusel

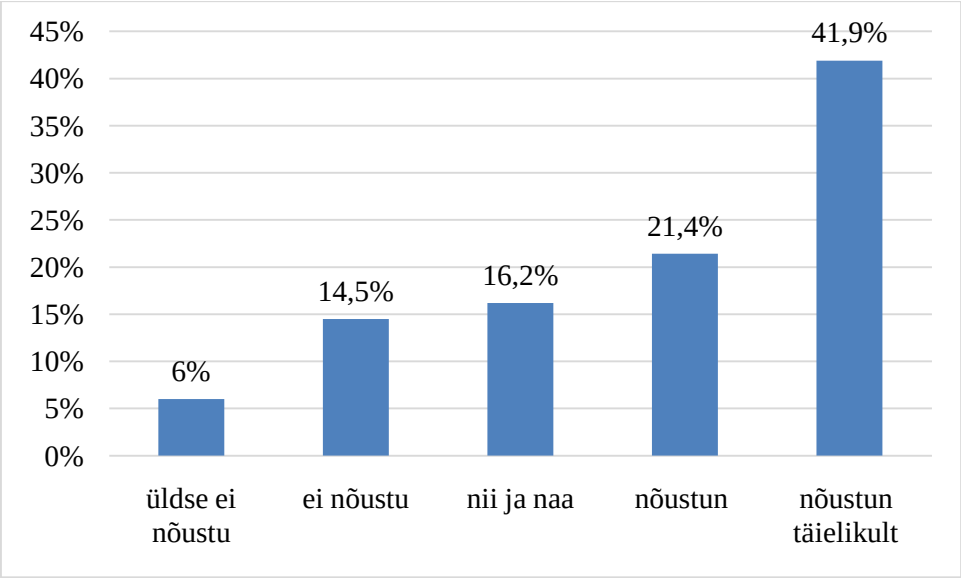
35% (41) vastanutest vastas, et nende ettevõttes puudub andmekaitsespetsialist, nendest 51,2% (21) vastanutest teab täpselt, mis aja jooksul on vaja teavitada AKI isikuandmete kadumisest, vaid 4,8% (2) leiab, et andmete kadumisest võib üldse mitte teatada. (vt. Lisa 2)

Enamik vastanutest vastas, et raamatupidaja tegeleb mahulise andmetöötlusega: 81,2% (95) vastanutest on selles kindel ja on andud 5 punkti; 14,5% (17) on andnud 4 punkti; 4,3% (5) on andnud 3 punkti; punktid vastavad Likerti viiepalliskaalale. Andmed on võetud lisas 2. 79,5% (93) vastanutest arvab, et isikuandmete kaitse on osa raamatupidaja tööst; 15,4% (18) vastanutest kahtleb, et raamatupidaja peaks isikuandmeid kaitsma ja 5,1% (6) vastanutest usub, et andmekaitse ei ole raamatupidaja kohustus. Tulemused on kajastatud joonisel 3.



Joonis 3. Küsitletute vastused küsimusele, andmekaitse on raamatupidaja töö osa (n=117)
Allikas: autori koostatud lisa 2 alusel

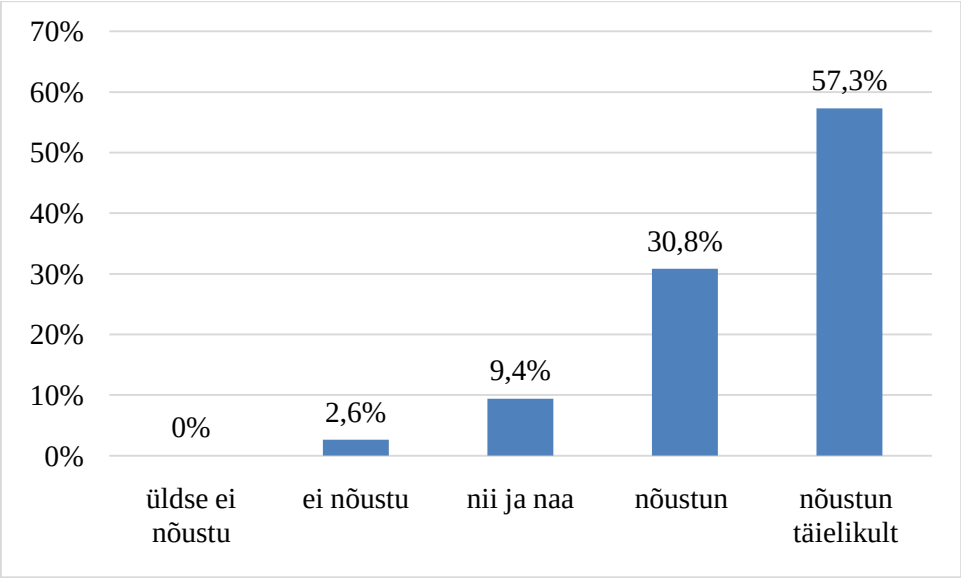
Üle poole vastanutest, nimelt 63,3% (74) usub, et ettevõte vajab andmekaitsespetsialisti, 16,2% (19) kahtleb selle vajalikkuses ja üle 1/5 (24) vastanutest usub, et andmekaitsespetsialist on ettevõttes esmavajalik. (vt. Joonis 4)



Joonis 4. Küsitletute vastused küsimusele, andmekaitsespetsialisti olemasolu ettevõttes on esmavajadus (n=117)
Allikas: autori koostatud lisa 2 alusel

Andmekaitse tagamiseks peab ettevõte rakendama teatud meetmeid. Kuid läbiviidud uuring näitas, et mitte kõik ettevõtted ei järgi oma töös elementaarseid reegleid, mis aitavad isikuandmete kaitsmisele kaasa. Sellele vaatamata vastas enamus – 78,7% (92) vastanutest, et nende ettevõttes kehtivad mitmed nõuded, mis suurendavad andmete turvalisust (näiteks arvutist eemaleminemisel tuleb süsteemist välja logida jne). 6% (7) vastanutest vastas, et nende ettevõte ei kohaldanud nõudeid, mis vähendavad andmete kadumise riski. 15,4% (18) kahtleb, et nende ettevõttes kehtivad isikuandmetega töötamise nõuded. Nendest 83,3% (15) vastas, et nende ettevõtted ei korralda regulaarset isikuandmete kaitse alast koolitust. Kui võtta arvesse kõiki vastajaid, nõustus üle poole vastanutest 53,9% (63), et nende ettevõtetes korraldatakse regulaarselt isikuandmete kaitse teemalist koolitust. Tulemused on esitatud lisas 2 olevas tabelis.

Uuringust selgub, et enamik vastajaid mõistab selgelt, et GDPR nõuete kohaselt tuleb isikuandmete rikkumisest teatada AKI: 103 (88,1%) vastanutest vastas jaatavalt, 11 (9,4%) kahtles ja vaid 3 (2,6%) arvas, et rikkumisest pole vaja teatada. (vt. Joonis 5)



Joonis 5. Küsitletute vastused küsimusele, kas on vaja rikkumistes Andmekaitse Inspektsiooni teavitada. (n=117)
Allikas: autori koostatud lisa 2 alusel

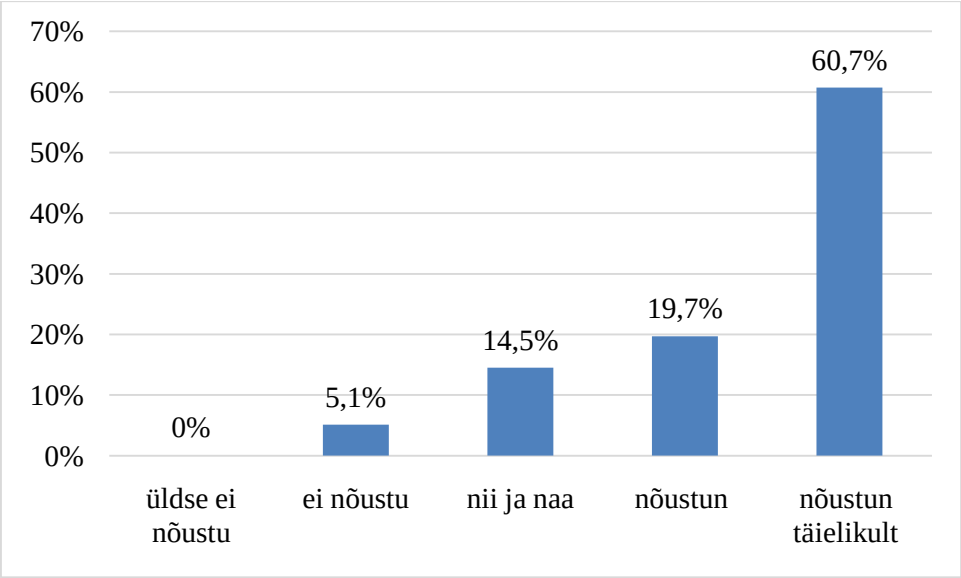
Eesti Vabariigi andmekaitseseadus sisaldab mitmeid reegleid andmete ohutuks töötlemiseks. Andmekaitseseaduse sätete rakendamise uurimiseks palus autor uuringus vastajatel hinnata oma ettevõtte andmekaitsemeetmeid. Tabel 1 kajastab vastajate nõusolekut oma ettevõttes mõne andmekaitsemeetodi kasutamisega. Keskendudes iga meetodi keskmisele hindele, võime öelda järgmist: vastajad arvavad, et nende ettevõtted järgivad andmetöötlusel andmekaitsemeetodeid. Kuid samal ajal näitab uuring, et 16,2% vastanutest kahtleb, et nad hoiduvad andmetöötlussüsteemi kasutamisest rakendades selleks volitamata isikute poolseid andmete edastamise vahendeid. 11,1% vastanutest ei oska kindlalt öelda, kas nende juurdepääsu tase automatiseeritud andmetöötlussüsteemis nähtavale teabele on piisav. Peaaegu 1/10 vastanutest ei ole kindlad selles, et on võimalik aru saada, kes, millal ja mis andmed sisestas andmetöötlussüsteemi. 12,8% vastanutel on rakse öelda, kas nemad saavad andmeid taastada pärast nende kadumist. On võimalik, et see segadus on seotud sellega, et nendel vastanutel ei ole veel kunagi tekkinud andmekadumisega probleeme. 8,5% vastanutel ei oska kindlalt öelda, kas nemad tagavad andmetöötlussüsteemi normaalse toimimise ja mis on kõige tähtsam, kas oskavad õigeaegselt süsteemiveast aru saada ja sellest teatada. Tuleb nentida, et küsitluse käigus selgitati välja, et mõnes ettevõttes ei kasutata tabelis 1 toodud ohutusmeetmeid.

Tabel 1. Andmetöötleja reeglid andmete turvaliseks

Teie ettevõttes andmetöötlejad andmete peavad turvaliseks töötlemiseks lähtuma järmistest reeglitest	Vastajate hinnangud Likerti skaala põhjal 1-5					Hinnangute kaalutud keskmine
	üldse ei nõustu (1)	ei nõustu (2)	nii ja naa (3)	nõustun (4)	nõustun täielikult (5)	
Keelata volitamata isikutel kasutada andmetöötlussüsteemi andmesidevahendite abil	0 (0%)	1 (0,9%)	19 (16,2%)	40 (34,2%)	57 (48,7%)	4,31
Tagada automatiseeritud andmetöötlussüsteemi kasutamise luba omavale kasutajale juurdepääs üksnes sellistele isikuandmetele, mida tema juurdepääsuluba hõlmab	0 (0%)	2 (1,7%)	13 (11,1%)	32 (27,4%)	70 (59,8%)	4,45
Tagada võimalus tõendada ja kindlaks teha, milliseid isikuandmeid on automatiseeritud andmetöötlussüsteemi sisestatud ning millal ja kes need on sisestanud	0 (0%)	4 (3,4%)	12 (10,3%)	35 (29,9%)	66 (56,4%)	4,39
Tagada võimalus paigaldatud andmetöötlussüsteemi katkestuse korral taastada	1 (0,9%)	5 (4,3%)	15 (12,8%)	28 (23,9%)	68 (58,1%)	4,34
Tagada andmetöötlussüsteemi toimimine ja selles ilmnevatest toimimisvigadest teavitamine	0 (0%)	4 (3,4%)	10 (8,5%)	21 (17,9%)	82 (70,1%)	4,54

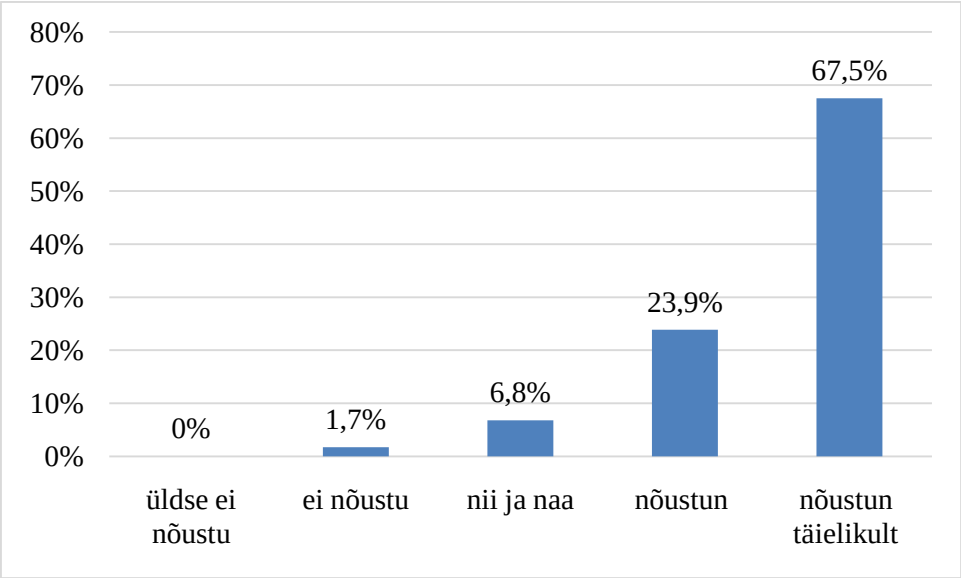
Allikas: autori koostatud lisa 2 alusel

Uuringu käigus oli oluline mõista, kas vastajad on teadlikud, millised on AKSi eesmärgid vastavuses GDPR nõuetega. 80,4% (94) vastanutest on kindlad, et andmekaitsespetsialist peaks andmesubjektide kontaktisikuna tegutsema kõigis isikuandmete töötlemise ja andmekaitseõiguse kasutamisega seotud küsimustes. 5,1% (6) vastanutest ei ole sellega nõus, 14,5% (17) vastanutest ei ole sel teemal selget arvamust. Tulemused on näidatud joonisel 7.



Joonis 7. AKS - kontaktisik kõigis küsimustes, mis on seotud isikuandmete töötlemisega(n=117)
Allikas: autori koostatud lisa 2 alusel

Küsimustiku vastuste põhjal nõustus 91,4% (107) vastanutest, et AKSi ülesanne on jälgida andmekaitsestandardite rakendamist, sealhulgas kohustuste jaotus, töötajate teadlikkus ja koolitus ning andmekaitseauditid. 6,8% (8) vastanutest ei suuda sellele küsimusele täpselt vastata ja vaid 2 vastanut 117-st ei nõustu ülalnimetatud ülesandega (vt. Joonis 8).



Joonis 8. AKS ülesanne: teavitada ja nõustada andmekaitse küsimustes (n=117)
Allikas: autori koostatud lisa 2 alusel

90,6% (106) vastanutest arvab, et andmekaitsespetsialist peab teavitama ja nõustama organisatsiooni juhtkonda ja töötajaid (vajadusel ka selle partnereid) andmekaitse küsimustes. 2,6% (3) vastanutest arvab, et see ei ole AKS-i kohustus. Tulemused on esitatud lisas 2 olevas tabelis.

2.3. Uuringu tulemuste analüüs

Kvantitatiivne analüüs näitas, et kuigi isikuandmete kaitse üldmäärus võeti vastu kolm aastat tagasi, oli autor üllatunud sellest, et ka praegu on vastajaid, kes ei ole määrusest varem kuulnud. Enamik vastanutest kuulis määrustest ja 76% nendest arvas, et nende ettevõtete andmekaitse tase on keskmisest kõrgem. Hoolimata asjaolust, et vaid umbes pool vastanutest teab, mis aja jooksul on vaja GDPRi kohaselt isikuandmete häkkimisest teatada, 35% arvab, et teatada on vajalik 72 tunnist varem. See näitab, et vastajad mõistavad informeerimise ja selle kiiruse olulisust. Mida kiiremini teatada isikuandmetega seotud rikkumisest, seda vähem kahju on nende kadumisest.

Raamatupidaja tööst rääkides näitas uuring järgmist: enamik vastajaid on nõus, et raamatupidaja töö on seotud isikuandmete mahuka töötlemisega ja sellega, et töötamise ajal peab raamatupidaja kaitsma tema töödeldavaid isikuandmeid. Enamik vastanutest nõustus, et raamatupidaja kui andmetöötleja üks ülesanne on teatada kõigist isikuandmete rikkumistest otse Andmekaitse Inspektsioonile.

Igal ettevõttel on oma meetmed andmete kaitsmiseks nende töötlemise ajal. Kvantitatiivse analüüsi põhjal selgus, et enamik ettevõtete meetmeid on suunatud andmekaitsele. Nad loovad töötajatele isiklikud kontod, mis võimaldavad juurdepääsu vajalikule teabele. Ettevõtted kehtestavad töötajatele teatud nõuded, näiteks lahkuda süsteemist töökohalt lahkudes jne. Saadud andmete põhjal arvab autor siiski, et mitte kõik ettevõtted ei teavita oma töötajaid andmekaitsest piisavalt. Vaatamata asjaolule, et 53,9% vastanutest kinnitas, et nende ettevõttes korraldatakse regulaarselt isikuandmete kaitse alaseid koolitusi, 46,1% vastajatest on need, kes ei andnud jaatavat vastust. Autori arvates on see kõrge näitaja, mida tuleb vähendada töötajatele isikuandmete kaitse teemaliste koolituste läbiviimise teel. Tõepoolest, kasvab igal aastal küberkuritegude arv ja andmetöötlejad peaksid olema teadlikud uutest võimalustest kaitsta ennast, töötajaid, kliente ja kogu ettevõtet.

Uuringu käigus saadud andmed näitavad, et enamasti vastutavad andmetöötlejatena töötavad vastajad järgides uuendatud andmekaitseseaduses sätestatud ohutusmeetmeid. Töötlejad püüavad hoiduda kolmandate osapoolte vahendite kasutamisest andmetöötlussüsteemi sisenemisel, töötada ainult oma taseme andmetega, tagada süsteemi töö ja teatada aegsasti rikkumistest selle töös. Iga ohutuks töötlemiseks kasutatud meetme keskmine tulemus oli kõrgem kui 4, mis tähendab, et vastajad nõustuvad, et neid meetmeid kohaldatakse nende ettevõttes.

Andmekaitse üldmäärusega on kehtestatud andmekaitsespetsialisti (AKS) ametikoha loomise vajadus. Uue ametikoha kehtestamine on vajalik 63,3% vastanute arvamusel. Kvantitatiivse analüüsi käigus saadud vastuste põhjal saab suurem osa vastanutest aru, mis on AKSi töö, millised on tema peamised ülesanded..

KOKKUVÕTE

Antud bakalaureusetöö eesmärk on välja selgitada raamatupidajate suhtumine ja teadlikkus isikuandmete kaitse seaduse muudatustest, mis on põhjustatud isikuandmete kaitse üldmääruse (GDPR) vastuvõtmisest 25. mail 2018. Eesmärgi saavutamiseks kasutati küsimustikul põhinevat kvantitatiivset uurimismeetodit. Vastajad olid raamatupidamistöötajad. Eesmärgi täitmiseks esitati küsimused, millele leiti vastused töö käigus.

Bakalaureusetöö esimene peatükk on pühendatud isikuandmete kaitsele. Andmekaitse kaitseb isikut, täpsemalt inimese õigust informatiivsele enesemääramisele. Informatsiooniline enesemääramine on inimese põhiõigus ja vabadus valida, kellele ja milliseid andmeid avaldada.

Isikuandmete töötlemine on isikuandmetega seotud toimingute kogum, see võib olla automatiseeritud või mitteautomatiseeritud toiming. Õigusakt kaitseb isikuandmeid sõltumata nende töötlemiseks kasutatavast tehnoloogiast. Seda kohaldatakse nii automaatsele töötlemisele kui ka käsitsi töötlemisele. Samuti ei ole oluline, kus andmeid hoitakse: elektroonilisel kandjal või paberil. Kõigil nendel juhtudel kehtivad isikuandmete suhtes üldises andmekaitse määruses sätestatud kaitsenõuded.

Oluline on mõista, et andmetöötlus peab põhinema GDPRi põhiprintsiipidel: minimeerimine, krüpteerimine, andmete töötlemise nõusolek, rikkumisest teatamine. Eestis reguleerib andmekaitset Eesti Vabariigi andmekaitseseadus, mida ajakohastati pärast andmekaitse üldmääruse (GDPR) vastuvõtmist 2019. aastal. Lisaks jälgib Andmekaitse Inspektsioon isikuandmete töötlemise nõuete täitmist.

See töö puudutab ka andmetöötlust ja raamatupidamist. Raamatupidajad töötavad iga päev suure hulga tervist, finantse jms puudutavate isikuandmetega. Raamatupidaja on andmetöötleja ja seetõttu on ta petiste sihtmärk. Seetõttu peab raamatupidaja olema tähelepanelik ja isikuandmetega töötades rakendama teatud turvameetmeid.

Teine peatükk on suunatud saadud andmete analüüsile. Uuring näitas, et enamik vastajaid on GDPRist kuulnud ja peavad oma ettevõtte andmekaitse taset kõrgeks. Uuringu tulemustele tuginedes järeldas autor, et vastajad mõistavad isikuandmetega seotud rikkumisest õigeaegse teatamise olulisust. Kodumaiste ettevõtete kogemus kinnitab, et viivitamise korral kaotavad tarbijad väärtuslikku aega, mida nad saaksid kasutada näiteks identiteedivarguste eest kaitsmiseks oma finantsteabe muutmise või näiteks oma pangakontode sulgemise teel.

Need uuringud on näidanud, et enamikul juhtudel rakendatakse andmekaitseseaduses määratletud turvameetmeid. Vastajad, s.o. andmetöötlejad proovivad süsteemi sisenemiseks kasutada turvalisi vahendeid, teatada rikkumistest õigeaegselt ja töödelda ainult lubatud andmeid. Kuna igaks turvaliseks töötlemiseks kasutatud meetme keskmine tulemus oli kõrgem kui 4, järeldas autor, et vastajad kinnitavad, et nende ettevõttes on olemas meetmed andmete kaitsmiseks. Vaatamata turvameetmete järgimisele leidis autor andmete analüüsi käigus, et töötajad ei saa andmekaitsealaseid teadmisi värskendatud. Autori arvates peaks selle probleemi lahendamiseks ettevõtte juhtkond pöörama suuremat tähelepanu andmekaitse teemaliste koolitusprogrammide korraldamisele.

Uurides ettevõttes andmekaitsja olemasolu vajadust, leidis autor, et 63,3% vastanutest arvab, et on vaja luua uus andmekaitsespetsialisti ametikoht.

Lõputöö eesmärk on täidetud ja püstitatud küsimustele vastused on saanud avatud töö kirjutamisel. Autor arvab, et enamik raamatupidamisvaldkonna töötajaid on muudatustest teadlikud ja on valmis neid aktsepteerima, kuid raamatupidajate andmekaitset puudutavate teadmiste alalhoidmiseks on vaja läbi viia andmekaitseteemalisi koolitusi.

SUMMARY

DATA PROTECTION ACT: IMPLICATION FOR ACCOUNTANTS - CASE OF ESTONIA

Maria Mussijenko

In 2018, the General Data Protection Regulation (GDPR) was issued, which amended the laws of the EU countries. In Estonia, a new data protection law was adopted in 2019. The purpose of Bachelor Thesis is to find out the attitude and awareness of accountants to changes in the law on the protection of personal data.

In the course of the analysis, a quantitative research method was used based on a survey that was conducted among accounting employees. To complete the work, the following research questions were raised:

- What is data protection?
- How does data protection work in Estonia?
- What options are there to protect personal data?
- How is an accountant related to data processing?
- How do accountants relate to changes in data protection law?
- Should every company have a data protection specialist?

Thy Bachelor Thesis consists of two chapters. The first chapter is devoted to the protection of personal data. Data protection gives a person the right to informational self-determination. Information self-determination is a fundamental human right and freedom to decide what data to disclose.

The processing of personal data is a set of operations with personal data; it can be an automated or non-automated operation. The legal act protects personal data regardless of the technology

used to process it. It applies to both automatic and manual processing. It also does not matter where the data is stored: on electronic media or on paper. In all these cases, the protection requirements set forth in the GDPR apply to personal data.

It is important to realize that data processing should be based on the basic principles of GDPR, which include minimization, coding, consent to processing, notification of violation. In Estonia, data protection is regulated by the Data Protection Act of the Republic of Estonia, which was updated after the adoption of the GDPR in 2019. In addition, compliance with the requirements for the processing of personal data is monitored by the Data Protection Inspectorate.

This work also touched on data processing and accounting. Bookkeeper works daily with large amounts of personal data regarding health, finance, etc. An accountant is a person who processes data, and therefore, is the target of fraudsters. In this regard, the accountant must be careful and apply certain security measures when working with personal data.

The second chapter was aimed at analyzing the data obtained. The study showed that most respondents have heard about GDPR and consider the level of data protection at their enterprise as high. Based on the results of the study, the author concluded that respondents understand the importance of timely reporting of a violation related to personal data. The experience of domestic companies confirms that as a result of delay, consumers lose valuable time that they could use to protect themselves from identity theft by changing financial information or closing bank accounts.

These studies have shown that the security measures specified in the data protection law are in most cases implemented. Respondents whose purpose is to use only safe tools to enter the system, report violations and process only authorized data. Since the average score for each measure used for safe processing was higher than 4, the author concluded that the respondents confirm that their company has measures to protect data. However, despite the observance of security measures, the author found that employees do not receive a qualitative improvement in knowledge regarding data protection, and to solve this problem, company management should pay more attention to the organization of training programs on data protection.

Analyzing the need for data protection in the company, the author found that 63.3% of the respondents believe that the introduction of a new position as a data protection specialist is necessary.

In the course of the work, the goal of the study was achieved and answers to the questions raised were found. The author believes that most of the employees in the accounting sector are aware of the changes and are ready to accept them, however, it is necessary to conduct training seminars on the topic of data protection in order to maintain the knowledge of accountants in the field of data protection.

KASUTATUD ALLIKATE LOETELU

Andmekaitsespetsialist. AKI. Kättesaadav: https://www.aki.ee/et/eraelu-kaitse/andmekaitsespetsialist, 18. aprill 2020.

Ayala, M., Neuman, W. (2012) Ecuador Grants Asylum to Assange, Defying Britain. *The New York Times*. Kättesaadav: https://www.nytimes.com/2012/08/17/world/americas/ecuador-to-let-assange-stay-in-its-embassy.html?searchResultPosition=18, 3. aprill 2020.

Eesti keele sõnaraamat ÕS 1999. (2003) Eesti keele Instituut. Kolmas Trükk. Tallinn, EestikKeele Sihtasutus

Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus

Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv),

Euroopa Komisjoni 10. jaanuari 2017. aasta ettepanek 2017/0003 (COD): Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus),

Euroopa Parlamendi ja nõukogu 27. aprill 2016. aasta määrus 2016/679, mis käsitleb füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks direktiivi 95/46/EÜ (isikuandmete kaitse üldmäärus)

Eesti Vabariigi Põhiseadus RT I, 15.05.2015, 2.

Ference, S. B. (2017) The armor of awareness. *In Journal of Accountancy*. Kättesaadav: https://www.journalofaccountancy.com/issues/2017/mar/defense-from-cyberattacks-at-cpa-firms.html, 25. aprill 2020.

Hea Tava. (2018). *Millega tegeleb igapäevaselt raamatupidaja*. Kättesaadav: https://www.heatava.ee/millega-tegeleb-igapaevaselt-raamatupidaja/, 17. aprill 2020.

Hert, P., (2013). *Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?* Kättesaadav: https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/isjlpsoc9&id=273&men_tab=srchresults, 29. märts 2020.

Human rights and modern scientific and technological developments (REC 509). Parliamentary Assembly. Kättesaadav: http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-en.asp?FileID=14546&lang=en, 29. märts 2020.

Isikuandmete kaitse seadus[1] RT I, 04.01.2019, 11.

Inimõiguste ja põhivabaduste kaitse konventsioon muudetud ja täiendatud protokollidega nr 11 ja nr 14. Council of Europe. Kättesaadav: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680063778, 25. märts 2020.

Isikuandmed ja töötlemine. AKI. Kättesaadav: https://www.aki.ee/et/eraelu-kaitse/isikuandmed-ja-tootlemine, 25. märts 2020.

Isikuandmete kaitse üldmääruse kohane andmekaitse. Teie Euroopa. Kättesaadav: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_et.htm, 2. mai 2020.

Isikuandmete töötleja üldjuhend. AKI. Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf, 2. mai 2020.

Jelinek, A. (2020). *Statement on the processing of personal data in the context of the COVID-19 outbreak.*

Kas töötajat saab kohustada rääkima kõike oma tervislikust seisundist? AKI. Kättesaadav: https://www.aki.ee/et/uudised/kas-tootajat-saab-kohustada-raakima-koike-oma-tervislikust-seisundist

McKenzie, L. K. (2018). *147 Million Social Security Numbers for Sale: Developing Data Protection Legislation After Mass Cybersecurity Breaches.* Kättesaadav: https://ilr.law.uiowa.edu/print/volume-103-issue-6/147-million-social-security-numbers-for-sale-developing-data-protection-legislation-after-mass-cybersecurity-breaches/, 17. aprill 2020.

Mis on isikuandmed? Euroopa Komisjon. Kättesaadav: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_et#nited-andmetest-mida-ei-loeta-isikuandmeteks, 25. märts 2020.

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

Paziuk, A., Sokolova. M. (2015). *Isikuandmete kaitse: sissejuhatus probleemile.* Kättesaadav: https://www.researchgate.net/publication/287912317_Zasita_personalnyh_dannyh_vvedenie_v_problematiku, 3. aprill 2020.

Pilving, I. (2005). *Õigus isikuandmete kaitsele*. Juridica, 533.

Raab, C., (2010). *Information Privacy: Networks of Regulation at the Subglobal Level.* Global Policy, 1: 291-302. Kättesaadav: https://onlinelibrary.wiley.com/doi/full/10.1111/j.1758-5899.2010.00030.x, 29. märts 2020.

Scott, K. L., (2016). *Overview of the privacy act of 1974*. Kättesaadav: https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition, 29. märts 2020.

Sleeter, D. (2012). *Are You Protecting Client Data When Sending Files Over the Internet?* Kättesaadav: https://www.cpapracticeadvisor.com/directory/portals/article/10708072/are-you-protecting-client-data-when-sending-files-over-the-internet, 25. aprill 2020.

Zaharia, A. (2016). *15 Steps to Maximize your Financial Data Protection.* Kättesaadav: https://heimdalsecurity.com/blog/online-financial-security-guide/, 25. aprill 2020.

Talapina, E. V. Isikuandmete õiguslik kaitse prantsusmaal. Kättesaadav: https://cyberleninka.ru/article/n/pravovaya-zaschita-personalnyh-dannyh-vo-frantsii, 3. aprill 2020.

Tejada, N. (2017). *7 tips for keeping your clients' data secure.* Kättesaadav: file:///C:/Users/Lenovo/Desktop/LT/lõputöö/Новая%20папка/7%20tips%20for%20keeping%20your%20clients'%20data%20secure.pdf, 6 märts 2020.

Tikk, E., Nõmper, A. (2007) *Informatsioon ja õigus.* Tallinn: Juura, 47.

Töötajate isikuandmete töötlemisest koroonaviiruse kontekstis. AKI. Kättesaadav: https://www.aki.ee/et/uudised/tootajate-isikuandmete-tootlemisest-koroonaviiruse-kontekstis, 28. märts 2020

Universal Declaration of Human Rights. (1948) *In United Nations*. Kättesaadav: https://www.un.org/en/universal-declaration-human-rights/index.html, 25. märts 2020.

Üksikisikute kaitse konventsioon isikuandmete automaatse töötlemise osas. Council of Europe. Kättesaadav: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078c46, 3. aprill 2020.

Yeaman, W. (2017). *Five Data Security Tips for Accounting Firm*. Kättesaadav: https://mainstreetpractitioner.org/feature/5-data-security-tips-for-accounting-firms/, 25. aprill 2020.

LISAD

Lisa 1. Uuringu küsimustik

Lugupeetud vastaja,

Uuringu on koostanud Tallinna Tehnikaülikooli III kursuse tudeng bakalaureusetöö raames.
Uuringu eesmärk on selgitada välja raamatupidajate suhtumine isikuandmete kaitse seaduse muudatustesse.
Uuringu läbiviimiseks on koostatud küsimustik, mille täitmine võtab aega orienteerivalt 10 minutit. Teie nime ei küsita (küsimustik on anonüümne) ja tulemusi kasutatakse üldistatud kujul.

Уважаемый респондент,

Исследование составлено студентом III курса Таллиннского Технического университета в рамках дипломной работы. Целью данного исследования является выявление отношения бухгалтеров к изменениям закона о защите личных данных. Для проведения исследования был составлен опросник, который займет примерно 10 минут. Ваше имя не спрашивается (опросник анонимный) и результаты используют в объединенном виде.

1. Kas Teil on majandusalane haridus? / Есть ли у Вас экономическое образование?
   a) Jah / Да;
   b) Ei / Нет.

2. Teie töökogemus (aastad) / Ваш опыт работы (года):
   a) Puudub / Отсутствует;
   b) 0-3 a./г.;
   c) 4-6 a./г.;
   d) 7-9 a./г.;

e) 10-12 a./г.;
f) Üle 12 a. / Свыше 12 г.

3. Teie ametikoht / Ваша должность.

a) Pearaamatupidaja / Главный бухгалтер;
b) Raamatupidaja / Бухгалтер;
c) Raamatupidaja assistent / Асистент бухгалтера;
d) Muu... / Другое.

4. Valige Teie ettevõtte tegevusvaldkond / Назовите сферу деятельности вешего предприятия.

a) Avalik haldus ja riigikaitse; kohustuslik sotsiaalkindlustus
b) Ehitus
c) Elektrienergia, gaasi, auru ja konditsioneeritud õhuga varustamine
d) Haldus- ja abitegevused
e) Haridus
f) Hulgi- ja jaekaubandus
g) Info ja side
h) Kinnisvaraalane tegevus
i) Kodumajapidamiste kui tööandjate tegevus; kodumajapidamiste oma tarbeks mõeldud eristamata kaupade tootmine ja teenuste osutamine
j) Kunst, meelelahutus ja vaba aeg
k) Kutse-, teadus- ja tehnikaalane tegevus
l) Majutus ja toitlustus
m) Muud teenindavad tegevused
n) Põllumajandus, metsamajandus ja kalapüük 3
o) Tervishoid ja sotsiaalhoolekanne
p) Töötlev tööstus
q) Veondus ja laondus
r) Finants- ja kindlustustegevus

5. Kas Teie vastutate statistiliste aruannete ja deklaratsioonide esitamise eest? / Вы отвечаете за подачу статистических отчетов, деклараций?

a) Jah / Да;
b) Ei / Нет.

6. Kas olete kuulnud GDPR-ist? / Слышали ли Вы об "Общем регламенте защиты данных"

a) Jah / Да;
b) Ei / Нет.

7. Millal tuleb andmete rikkumisest teatada inspektsioonile? / В течении какого времени следует сообщить инспекции о взломе данных?

a) 24 tunni jooksul / В течении 24 часов;
b) 3 - 4 tööpäeva jooksul / В течении 3 - 4 рабочих дня;
c) 72 tunni jooksul / В течении 72 часов;
d) Ei teavita üldse / Вообще не сообщать;
e) 42 tunni jooksul / В течении 42 часов.

8. Kas Teie ettevõttes on andmekaitsespetsialist? На вашем предприятии есть специалист по защите данных?

a) Jah / Да;
b) Ei / Нет.

Palun hinnake viiepalliskaalal (1 - üldse ei nõustu; 2 - ei nõustu; 3 - nii ja naa; 4 – nõustun; 5 - nõustun täielikult) järgmisi väiteid / Пожалуйста, оцените по пятибалльной шкале следующие утверждения (1 - вообще не согласен; 2 - не согласен; 3 - так и так; 4 – согласен; 5 - полностью согласен)

9. Raamatupidaja tegeleb mahuka andmetöötlusega / Бухгалтер занимается объемной обработкой данных.

10. Andmekaitse on raamatupidaja töö osa / Защита данных - часть работы бухгалтера.

11. Andmekaitsespetsialisti olemasolu ettevõttes on esmavajadus / Наличие специалиста по защите данных - это первая необходимость

12. Hinnake oma ettevõtte andmekaitse tase 5-palli skaalal (1 – väga madal; 2 – madal; 3 nii ja naa; 4 – kõrge; 5 – väga kõrge) / Оцените по 5 бальной шкале уровень защиты данных на вашем предприятии (1 – очень низкий; 2 – низкий; 3 – так и так; 4 – высокий; 5 очень высокий)

Hinnake viiepalliskaalal (1 - üldse ei nõustu; 2 - ei nõustu; 3 - nii ja naa; 4 – nõustun; 5 - nõustun täielikult) järgmisiväiteid: / Оцените по пятибалльной шкале следующие утверждения (1 - вообще не согласен; 2 - не согласен; 3 - так и так; 4 – согласен; 5 - полностью согласен): Teie ettevõte on võtnud isikuandmete kaitsmiseks järgmised meetmed... / На вашем предприятии приняты следующие меры способствующие защите личных данных ...

13. Regulaarsed koolitused andmekaitse teemadel / Регулярное обучение по теме защиты личных данных.

14. Kehtestatud erinevad nõuded (nt arvuti tagant lahkudes tuleb infosüsteemist välja logida jms) / Действуют различные требования (пр. уходя от своего компьютера, необходимо выйти из системы и тд).

15. Igal töötajal on oma isiklik kasutajakonto, mille kaudu ta pääseb ligi vajalikele andmetele / У каждого работника личная учетная запись, которая дает доступ к нужной информации.

16. Regulaarne turvalisuse hindamine (tehakse kindlaks, et ettevõttes ei oleks turvaauke) / Регулярная оценка безопасности (определять, что на предприятии нет пробелов в безопасности).

Lisa 1 järg

Hinnake viiepalliskaalal (1 - üldse ei nõustu; 2 - ei nõustu; 3 - nii ja naa; 4 – nõustun; 5 - nõustun täielikult) järgmisiväiteid: / Оцените по пятибалльной шкале следующие утверждения (1 - вообще не согласен; 2 - не согласен; 3 - так и так; 4 – согласен; 5 - полностью согласен): Andmetöötlejate uued kohustised on GDPR-i alusel ... / Обязанности обработчиков данных в рамках GDPR ...

17. Andmekaitse Inspektsiooni teavitamine rikkumistest / Обязаность информировать Инспекцию по защите данных в случае нарушения.

18. Vastutamine andmekaitsja tegevuse eest / Обязанность нести ответственность за действия защитника данных.

Hinnake viiepalliskaalal (1 - üldse ei nõustu; 2 - ei nõustu; 3 - nii ja naa; 4 – nõustun; 5 - nõustun täielikult) järgmisiväiteid: / Оцените по пятибалльной шкале следующие утверждения (1 - вообще не согласен; 2 - не согласен; 3 - так и так; 4 – согласен; 5 - полностью согласен):
Teie ettevõttes andmetöötlejad andmete peavad turvaliseks töötlemiseks lähtuma järmistest reeglitest ... / На вашем предприятии для безопасной обработки данных обработчики данных должны придерживаться следующих правил ...

19. Keelata volitamata isikutel kasutada andmetöötlussüsteemi andmesidevahendite abil / Воздерживаться от использования системы обработки данных с помощью средств передачи данных по данным не уполномоченными лицами.

20. Tagada automatiseeritud andmetöötlussüsteemi kasutamise luba omavale kasutajale juurdepääs üksnes sellistele isikuandmetele, mida tema juurdepääsuluba hõlmab / Обеспечить доступ пользователю, имеющему разрешение на использование автоматизированной системы обработки данных исключительно к таким личным данным, которые охватывает его разрешение на доступ.

21. Tagada võimalus tõendada ja kindlaks teha, milliseid isikuandmeid on automatiseeritud andmetöötlussüsteemi sisestatud ning millal ja kes need on sisestanud / Обеспечить возможность подтверждать и устанавливать, какие личные данные введены в автоматизированную систему обработки данных и когда и кто их ввёл.

22. Tagada võimalus paigaldatud andmetöötlussüsteemi katkestuse korral taastada / Обеспечить возможность восстановления системы обработки данных в случае поломки.

23. Tagada andmetöötlussüsteemi toimimine ja selles ilmnevatest toimimisvigadest teavitamine / Обеспечить функционирование системы обработки данных и уведомление о появляющихся ошибках её функционирования.

Hinnake viiepalliskaalal (1 - üldse ei nõustu; 2 - ei nõustu; 3 - nii ja naa; 4 – nõustun; 5 - nõustun täielikult) järgmisiväiteid: / Оцените по пятибалльной шкале следующие утверждения (1 - вообще не согласен; 2 - не согласен; 3 - так и так; 4 – согласен; 5 - полностью согласен): Andmekaitsespetsialisti ülesanded on ... / Задачи специалаиста по защите данных ...

24. Olla andmesubjektidele kontaktisikuks kõigis küsimustes, mis on seotud nende isikuandmete töötlemise ja nende andmekaitseliste õiguste kasutamisega / Выступать в качестве контактного лица для субъектов данных по всем вопросам, касающимся обработки их личных данных и осуществления их прав на защиту данных.

25. Teavitada ja nõustada oma organisatsiooni (vajadusel ka selle partnerite) juhtkonda ning personali andmekaitse küsimustes / Информировать и консультировать руководство и персонал организации (при необходимости и ее партнеров) по вопросам защиты данных.

26. Jälgida andmekaitsenormide rakendamist, sealhulgas vastutusvaldkondade jaotamist, personali teadlikkust ja koolitamist, ning andmekaitselist auditeerimist / Контролировать внедрение стандартов защиты данных, включая распределение обязанностей, осведомленность и обучение персонала, а также аудиты защиты данных.

Allikas: autori koostatud

Lisa 2. Küsitluse tulemused

1. Kas Teil on majandusalane haridus?

a) Jah	99 vastust
b) Ei	18 vastust

2. Teie töökogemus (aastad)

g) Puudub / Отсутствует	5 vastust
h) 0-3 a./г.	38 vastust
i) 4-6 a./г.	33 vastust
j) 7-9 a./г.	19 vastust
k) 10-12 a./г.	6 vastust
l) Üle 12 a. / Свыше 12 г.	16 vastust

3. Teie ametikoht

a) Pearaamatupidaja	21 vastust
b) Raamatupidaja	41 vastust
c) Raamatupidaja assistent	32 vastust
d) Muu ...	23 vastust

4. Valige Teie ettevõtte tegevusvaldkond:

a) Avalik haldus ja riigikaitse; kohustuslik sotsiaalkindlustus	2 vastust
b) Ehitus	14 vastust
c) Elektrienergia, gaasi, auru ja konditsioneeritud õhuga varustamine	4 vastust
d) Haridus	5 vastust
e) Hulgi- ja jaekaubandus	6 vastust
f) Info ja side	15 vastust
g) Kinnisvaraalane tegevus	8 vastus
h) Kodumajapidamiste kui tööandjate tegevus; kodumajapidamiste oma tarbeks mõeldud eristamata kaupade tootmine ja teenuste osutamine	3 vastust

i) Kutse-, teadus- ja tehnikaalane tegevus	2 vastust
j) Majutus ja toitlustus	13 vastust
k) Muud teenindavad tegevused	7 vastust
l) Põllumajandus, metsamajandus ja kalapüük	3 vastust
m) Tervishoid ja sotsiaalhoolekanne	10 vastust
n) Töötlev tööstus	2 vastust
o) Veondus ja laondus	9 vastust
p) Finants- ja kindlustustegevus	10 vastust

5. Kas Teie vastutate statistiliste aruannete ja deklaratsioonide esitamise eest?

a) Jah	80 vastust
b) Ei	37 vastust

6. Kas olete kuulnud GDPR-ist?

a) Jah	100 vastust
b) Ei	17 vastust

7. Millal tuleb andmete rikkumisest teatada inspektsioonile?

a) 24 tunni jooksul	31 vastust
b) 3 - 4 tööpäeva jooksul	6 vastust
c) 72 tunni jooksul	67 vastust
d) Ei teavita üldse	3 vastust
e) 42 tunni jooksul	10 vastust

8. Kas Teie ettevõttes on andmekaitsespetsialist?

a) Jah	76 vastust
b) Ei	41 vastust

9. Raamatupidaja tegeleb mahuka andmetöötlusega

a) 1 - üldse ei nõustu	0 vastust
b) 2 - ei nõustu	0 vastust
c) 3 - nii ja naa	5 vastust

d) 4 – nõustun	17 vastust
e) 5 - nõustun täielikult	95 vastust

10. Andmekaitse on raamatupidaja töö osa

a) 1 - üldse ei nõustu	2 vastust
b) 2 - ei nõustu	4 vastust
c) 3 - nii ja naa	18 vastust
d) 4 – nõustun	39 vastust
e) 5 - nõustun täielikult	54 vastust

11. Andmekaitsespetsialisti olemasolu ettevõttes on esmavajadus

a) 1 - üldse ei nõustu	7 vastust
b) 2 - ei nõustu	17 vastust
c) 3 - nii ja naa	19 vastust
d) 4 – nõustun	25 vastust
e) 5 - nõustun täielikult	49 vastust

12. Hinnake oma ettevõtte andmekaitse tase 5-palli skaalal

a) 1 – väga madal	1 vastust
b) 2 - madal	5 vastust
c) 3 - nii ja naa	18 vastust
d) 4 – kõrge	36 vastust
e) 5 – väga kõrge	57 vastust

13. Regulaarsed koolitused andmekaitse teemadel

a) 1 - üldse ei nõustu	16 vastust
b) 2 - ei nõustu	15 vastust
c) 3 - nii ja naa	23 vastust
d) 4 – nõustun	14 vastust
e) 5 - nõustun täielikult	49 vastust

14. Kehtestatud erinevad nõuded (nt arvuti tagant lahkudes tuleb infosüsteemist välja logida jms)

a) 1 - üldse ei nõustu	2 vastust
b) 2 - ei nõustu	5 vastust
c) 3 - nii ja naa	18 vastust
d) 4 – nõustun	23 vastust
e) 5 - nõustun täielikult	69 vastust

15. Igal töötajal on oma isiklik kasutajakonto, mille kaudu ta pääseb ligi vajalikele andmetele

a) 1 - üldse ei nõustu	2 vastust
b) 2 - ei nõustu	5 vastust
c) 3 - nii ja naa	12 vastust
d) 4 – nõustun	18 vastust
e) 5 - nõustun täielikult	80 vastust

16. Regulaarne turvalisuse hindamine(tehakse kindlaks, et ettevõttes ei oleks turvaauke)

a) 1 - üldse ei nõustu	4 vastust
b) 2 - ei nõustu	11 vastust
c) 3 - nii ja naa	22 vastust
d) 4 – nõustun	23 vastust
e) 5 - nõustun täielikult	57 vastust

17. Andmekaitse Inspektsiooni teavitamine rikkumistest

a) 1 - üldse ei nõustu	0 vastust
b) 2 - ei nõustu	3 vastust
c) 3 - nii ja naa	11 vastust
d) 4 – nõustun	36 vastust
e) 5 - nõustun täielikult	67 vastust

18. Vastutamine andmekaitsja tegevuse eest

a) 1 - üldse ei nõustu	6 vastust
b) 2 - ei nõustu	2 vastust

c) 3 - nii ja naa	16 vastust
d) 4 – nõustun	27 vastust
e) 5 - nõustun täielikult	66 vastust

19. Keelata volitamata isikutel kasutada andmetöötlussüsteemi andmesidevahendite abil

a) 1 - üldse ei nõustu	0 vastust
b) 2 - ei nõustu	1 vastust
c) 3 - nii ja naa	19 vastust
d) 4 – nõustun	40 vastust
e) 5 - nõustun täielikult	57 vastust

20. Tagada automatiseeritud andmetöötlussüsteemi kasutamise luba omavale kasutajale juurdepääs üksnes sellistele isikuandmetele, mida tema juurdepääsuluba hõlmab

a) 1 - üldse ei nõustu	0 vastust
b) 2 - ei nõustu	2 vastust
c) 3 - nii ja naa	13 vastust
d) 4 – nõustun	32 vastust
e) 5 - nõustun täielikult	70 vastust

21. Tagada võimalus tõendada ja kindlaks teha, milliseid isikuandmeid on automatiseeritud andmetöötlussüsteemi sisestatud ning millal ja kes need on sisestanud

a) 1 - üldse ei nõustu	0 vastust
b) 2 - ei nõustu	4 vastust
c) 3 - nii ja naa	12 vastust
d) 4 – nõustun	35 vastust
e) 5 - nõustun täielikult	66 vastust

22. Tagada võimalus paigaldatud andmetöötlussüsteemi katkestuse korral taastada

a) 1 - üldse ei nõustu	1 vastust
b) 2 - ei nõustu	5 vastust
c) 3 - nii ja naa	15 vastust

d) 4 – nõustun	28 vastust
e) 5 - nõustun täielikult	68 vastust

23. Tagada andmetöötlussüsteemi toimimine ja selles ilmnevatest toimimisvigadest teavitamine

a) 1 - üldse ei nõustu	0 vastust
b) 2 - ei nõustu	4 vastust
c) 3 - nii ja naa	10 vastust
d) 4 – nõustun	21 vastust
e) 5 - nõustun täielikult	82 vastust

24. Olla andmesubjektidele kontaktisikuks kõigis küsimustes, mis on seotud nende isikuandmete töötlemise ja nende andmekaitseliste õiguste kasutamisega

a) 1 - üldse ei nõustu	0 vastust
b) 2 - ei nõustu	6 vastust
c) 3 - nii ja naa	17 vastust
d) 4 – nõustun	23 vastust
e) 5 - nõustun täielikult	71 vastust

25. Teavitada ja nõustada oma organisatsiooni (vajadusel ka selle partnerite) juhtkonda ning personali andmekaitse küsimustes

a) 1 - üldse ei nõustu	2 vastust
b) 2 - ei nõustu	1 vastust
c) 3 - nii ja naa	8 vastust
d) 4 – nõustun	30 vastust
e) 5 - nõustun täielikult	76 vastust

26. Jälgida andmekaitsenormide rakendamist, sealhulgas vastutusvaldkondade jaotamist, personali teadlikkust ja koolitamist, ning andmekaitselist auditeerimist

a) 1 - üldse ei nõustu	0 vastust
b) 2 - ei nõustu	2 vastust

c) 3 - nii ja naa	8 vastust
d) 4 – nõustun	28 vastust
e) 5 - nõustun täielikult	79 vastust

Allikas: autori koostatud

LIHTLITSENTS

Maria Mussijenko

1. annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose « Raamatupidaja tegevus ja vastutus andmekaitseseaduse rakendamisel », mille juhendaja on Natalie Aleksandra Gurvitš-Suits, PhD,

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

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

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

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