TALLINNA TEHNIKAÜLIKOOL
Majandusteaduskond
Ärikorralduse instituut

Kerli Kask

ETTEVÕTETE PRIVAATSUSPOLIITIKATE VASTAVUS ISIKUANDMETE KAITSE ÜLDMÄÄRUSELE VEEBITEENUSEID OSUTAVATE ETTEVÕTETE NÄITEL

Magistritöö
Õppekava ärirahandus ja majandusarvestus, peaeriala audiitortegevus

Juhendaja: Natalie Aleksandra Gurvitš-Suits, PhD

Tallinn 2021

Deklareerin, et olen koostanud magistritöö 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 10161 sõna sissejuhatusest kuni kokkuvõtte lõpuni.

Kerli Kask, 03.01.2021
(allkiri)
Üliõpilase kood: 183253TARM
Üliõpilase e-posti aadress: kkerlikask@gmail.com

Juhendaja: Natalie Aleksandra Gurvitš-Suits, PhD
Töö vastab kehtivatele nõuetele
……
(allkiri, kuupäev)

Kaitsmiskomisjoni esimees:
Lubatud kaitsmisele
……
(allkiri, kuupäev)

SISUKORD

LÜHIKOKKUVÕTE

Magistritöö eesmärk on välja selgitada, kas veebiteenuseid osutavate ettevõtete privaatsuspoliitikad vastavad 2018. aastal jõustunud isikuandmete kaitse üldmääruses nõutule: kas nad sisaldavad kogu vajalikku teavet andmetöötlustoimingute kohta peegeldades andmesubjekti kõiki õigusi ja võimalusi. Täiendavalt uuritakse, milliseid riske võib füüsilisele isikule kaasa tuua see, kui ettevõte ei ole isikuandmete kogumiseks ja töötlemiseks rakendanud piisavaid meetmeid ning kas privaatsuspoliitika sisu võib seostada ettevõtte läbipaistvusega isikuandmete kogumisel ja töötlemisel.

Teema valik on ajendatud sellest, et privaatsus ning isikuandmed ja nende kaitse on areneva infotehnoloogia ajastul inimeste ja ettevõtete jaoks üha olulisem teema. Sellega seotud seadusandlust on aastakümnete jooksul märkimisväärselt arendatud ja täiendatud.

Magistritöö eesmärgi saavutamiseks luuakse mudel, mis kontrollib läbi andmetöötlustoimingu aspekte peegeldavate märksõnade privaatsuspoliitikate sisu. Märksõnu otsitakse privaatsuspoliitikatest läbi käsuprogrammi AstroGrep. Valim koostatakse 120 veebiteenuseid osutava ettevõtte privaatsuspoliitikatest.

Loodud mudel saavutab manuaalse kontrolli tulemusel keskmiselt 89,6% kindluse. Mudeli tulemused näitavad, et mudel lihtsustab privaatsuspoliitikate lugemist ja nende mõistmist. Koostatud privaatsuspoliitikate analüüsimudel võimaldab füüsilisel isikul anda ettevõttele, kui vastutavale töötlejale, esmane hinnang selle kohta, kui suur on risk tema isikuandmete edastamisel vastavale ettevõttele.

Võtmesõnad: GDPR, privaatsuspoliitika, privaatsus, andmekaitse

SISSEJUHATUS

Innovatsioon ja digitaliseerimine loob uusi ärimudeleid, kus isikuandmete kasutamine ja töötlemine järjest progresseerub, võimaldades ettevõtetel teha põhjalike andmeanalüüside abil aina paremaid ja kasumlikumaid äriotsuseid. Ettevõtted seisavad aga ka silmitsi järjest karmistuvate regulatsioonide ja nõuetega, mis puudutavad isikuandmete töötlemist.

25. mail 2018. aastal rakendus isikuandmete kaitse üldmäärus (edaspidi: GDPR — *The General Data Protection Regulation*), mis sätestab õigusnormid, mis käsitlevad füüsiliste isikute kaitset isikuandmete töötlemisel ja selliste andmete vaba liikumist. GDPR ei loo uut seadustikku, vaid täiendab olemasolevat. GDPR sätestab karmid nõuded sellele, kuidas Euroopa Liidu sees või liidu residentide isikuandmeid töödeldakse. GDPR-i ulatus on suur: see reguleerib füüsilise isiku andmete töötluse igat aspekti ning sisaldab suuri võimalike rahalisi trahve rikkumiste eest. (EL-i määrus 2016/679)

GDPR-i ulatus on lai ja see hõlmab andmekaitse mitmeid aspekte. Selle määruse eesmärk on aidata kaasa vabadusel, turvalisusel ja õigusel rajaneva ala ning majandusliidu saavutamisele, majanduslikule ja sotsiaalsele arengule, riikide majanduse tugevdamisele ja lähendamisele siseturul ning füüsiliste isikute heaolule (EL-i määrus 2016/679 põhjenduspunkt 2).

GDPR-i rakendamine mõjutas väga suurt hulka veebiteenuseid osutavaid ettevõtteid — mitte ainult Euroopas asuvaid ettevõtteid, vaid ka neid väljaspool EL-i asuvaid ettevõtteid, kelle teenused on Euroopa kodanikele kättesaadavad. Sellised teenusepakkujad on kohustatud üle vaatama ja määrusega vastavusse viima kõik oma tegevused, mis puudutavad isikuandmete töötlemist. Tegevus peab muutuma läbipaistvamaks ning info, kuidas isikuandmeid kogutakse ja töödeldakse, peab saama kasutajale kättesaadavamaks. Määrus sisaldab mitmeid otseseid nõudeid veebiteenustega tegelevatele ettevõttetele. Näiteks on sellel ootused veebilehtede tehnilisele poolele: turvalisusele ja sellele, milliseid andmeid ja kuidas kogutakse.

Isikuandmete kaitse määrus nõuab, et ettevõtted võtavad kasutusele asjakohased meetmed, et esitada andmesubjektile teave tema isikuandmete töötlemise kohta ning teavitada teda isikuandmete töötlemisest kokkuvõtlikult, selgelt, arusaadavalt ning lihtsasti kättesaadavas vormis, kasutades selget ja lihtsat keelt (EL-i määrus 2016/679 art 12). Nimetatud kohustust — edastada infot isikutele nende andmete töötlemise kohta — täidavad ettevõtted üldjuhul privaatsuspoliitika / isikuandmete töötlemise korra või muu taolise dokumendina või infona lisatuna ettevõtte veebilehele. Privaatsus ja turvalisus on järjest aktuaalsem ja olulisem teema, eriti areneva e-kaubanduse ajastul. Autor soovib uurida, milline on privaatsuspoliitikate kvaliteet mõni aasta pärast määruse jõustumist.

Magistritöö eesmärk on välja selgitada, kas veebiteenuseid osutavate ettevõtete privaatsuspoliitikad vastavad GDPR-is oodatule: kas nad sisaldavad kogu vajalikku teavet peegeldades andmesubjekti kõiki õigusi ja võimalusi. Autori hinnangul on veebilehtedel osutatav teave väga erinev ning alati ei kata ettevõtete privaatsuspoliitikad kõiki GDPR-is nõutud andmetöötlustoimingute aspekte. Samuti usub autor, et privaatsuspoliitikate sisu võib olla füüsilisele isikule raskesti mõistetav juriidilise teksti või keerulise keelekasutuse tõttu. Autor kasutab uurimuses 120 veebiteenuseid osutava ettevõtte privaatsuspoliitikat ja loob mudeli, mille abil uurib nende sisu ehk püüab välja selgitada, kas privaatsuspoliitikad katavad kõiki andmetöötlustoimingute aspekte. Täiendavalt soovib autor uurida, milliseid riske võib füüsilisele isikule kaasa tuua see, kui ettevõte ei ole isikuandmete kogumiseks ja töötlemiseks rakendanud piisavaid meetmeid ning kas privaatsuspoliitika sisu võib seostada ettevõtte läbipaistvusega isikuandmete kogumisel ja töötlemisel.

Töö koosneb kahest osast. Magistritöö esimeses peatükis loob autor ülevaate privaatsuse mõiste ja isikuandmete kaitse teoreetilisest lähenemisest. Luuakse ülevaade regulatsioonidest ja seadustest, mis isikuandmete kaitset reguleerivad ning millistest seadustest/regulatsioonidest on need välja kujunenud. Esimeses peatükis teeb autor ülevaate GDPR-iga kaasnevatest põhiõigustest isikule ning kohustustest, mis kaasnevad veebiteenuseid osutavale ettevõttele, kui ta isikuandmeid kogub ja töötleb. Tuuakse välja olulisimad seisukohad ehk andmetöötlustoimingute aspektid, millest uurimuses lähtutakse.

Magistritöö teises peatükis koostatakse riskianalüüs, millega hinnatakse, milliseid riske võib füüsilisele isikule kaasa tuua see, kui tema andmete kogumine ja töötlemine ei ole läbipaistev ega

vasta määrusele. Luuakse mudel, millega võiks lihtsustada privaatsuspoliitikate mõistmist ja nende sisu kontrollimist. Mudelis leitakse igale andmetöötlustoimingu aspektile võimalikud vastavad märksõnad ning läbi käsuprogrammi AstroGrep otsitakse neid märksõnu privaatsuspoliitikatest. Mudeli usaldatavust testitakse manuaalselt. Mudeli eesmärk on analüüsida, millisel määral kajastavad vaadeldavad privaatsuspoliitikad määruses nõutud andmetöötlustoimingute aspekte ning kas privaatsuspoliitika sisu on võimalik seostada sellega, milline on risk füüsilisele isikule, kui ta oma andmeid mingile ettevõttele ehk vastutavale töötlejale edastab.

1. ISIKUANDMETE KAITSE JA ANDMEKAITSEMÄÄRUS

25. mail 2018. aastal rakendus isikuandmete kaitse üldmäärus (GDPR — *The General Data Protection Regulation*), mis sätestab õigusnormid, mis käsitlevad füüsiliste isikute kaitset isikuandmete töötlemisel ja selliste andmete vaba liikumist. GDPR, mis on välja kasvanud 13. detsembril 1995. aastal jõustunud andmekaitsedirektiivist, ei loo uut seadustikku vaid täiendab olemasolevat. Selle määrusega kaitstakse füüsiliste isikute põhiõigusi ja -vabadusi, eriti nende õigust isikuandmete kaitsele. (EL-i määrus 2016/679) Privaatsus on läbi aja omanud inimese jaoks erinevat tähendust ning selle väärtus on ajaga saanud füüsilistele isikutele järjest olulisemaks ja hinnalisemaks. Uus andmekaitsemääruse raamistik on justkui eeskuju kõigile poliitikavaldkondadele, kus globaliseerumise ja digitaliseerumise tagajärgede tõttu on väärtuste ja standardite tõhusaks kaitsmiseks vaja uut regulatiivset lähenemisviisi (Albrecht, 2016, 289). Järgmisena on toodud ülevaade, kuidas privaatsuse mõiste on aja jooksul muutunud ning milliste regulatsioonidega on inimese andmeid ja nende turvalisust reguleeritud.

Töös läbivalt kasutatavate mõistete ja definitsioonidega saab tutvuda lisas 1.

1.1. Privaatsus ja andmekaitse

Areneva infotehnoloogia ajastul seatakse inimese privaatsus ja turvalisus järjest kõrgemale, sest aina enam hoitakse andmeid ja infot veebis ning seega on võimalik andmeid kätte saada suures mahus ja korraga. Suurandmed ehk *big data* on meede, kuidas organisatsioonid ühildavad erinevaid digitaalseid andmekogumikke ning kasutavad statistika ja muude andmekaeve võimaluste abil neid andmeid peidetud info tõlgendamiseks ja korreleerimiseks (Rubinstein, 2013). Ärimudelid, mis baseeruvad isikuandmete kasutamisel ja töötlemisel, arenevad meeletu kiirusega üle maailma (Ciriani, 2015, 42). Andmetöötlussüsteemid on loodud selleks, et teenida inimkonda; neid süsteeme kasutades tuleb vaatamata isikute kodakondsusele ja elukohale austada nende põhiõigusi ja -vabadusi, eeskätt õigust eraelu puutumatusele, ning aidata kaasa

majanduslikule ja sotsiaalsele arengule, kaubanduse laiendamisele ja üksikisikute heaolule (EL-i direktiiv 95/46/EÜ põhjenduspunkt 2). Statistika näitab, et üle poole maailmast, ligikaudu 59% kogu inimkonnast, kasutab internetti (Global digital … 2020), genereerides iga päev juurde andmeid, mida teenusepakkujad kasutavad kasutajate profiilide koostamiseks – see on otsene oht kasutaja privaatsusele. Füüsilise isiku privaatsus on järjest olulisem ning seda eelkõige digitaliseerumise tõttu.

1.1.1. Privaatsus

Eesti Vabariigi põhiseaduse § 26 järgi on igaühel 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. (PS-i § 26) Selline õigus privaatsusele on meile tänapäeval iseenesestmõistetav, kuid alati ei ole privaatsust selliselt käsitletud.

Miks on privaatsus meile oluline? Filosoofi James Rachels-i sõnul on privaatsuse idee selles, et privaatsusel on tihe seos meie võimega kontrollida seda, kellel on meile ligipääs ja ligipääs informatsioonile meie kohta, ning tihe seos meie võimega luua ja hoida erinevaid suhteid erinevate inimestega (Rachels, 1975, 326). Seega on privaatsus vajalik, kui soovime säilitada mitmesuguseid sotsiaalseid suhteid teiste inimestega.

Privaatsuse kontseptsioone on väga palju ja ajas on selle mõiste tähendus muutunud. 1890. aastal kõrvutasid juristid Samuel D. Warren ja Louis D. Brandeis väidet „õigus privaatsusele“ väitega „õigus olla üksi jäetud“. Seni seostati „õigust privaatsusele“ pigem materiaalse privaatsusega ehk isiku omandi ja varaga. (Brandeis, Warren, 1890, 195) Mitmed teoreetikud on käsitlenud privaatsust, kui „piiratud juurdepääsu“ ehk justkui inimese soovi end varjata ja teistest eraldada (Solove, 2008). 1970. aastal defineeris Ameerika Ühendriikide Ülemkohus privaatsust selliselt, et eraelu puutumatus on üksikisiku õigustatud nõue, otsustamaks, millises ulatuses soovib ta oma elu teistega jagada. See on kontroll oma aja, asukoha ja asjaolude üle, mida ta teiste inimestega jagab. Informatsioon iseenda kohta on selle isiku omand. See tähendab ka tema õigust oma äranägemise järgi taganeda või osaleda sündmustes. (Breckenridge, 1970) Privaatsust on seostatud ka saladuses hoidmisega või varjamisega, millega piiratakse enda kohta käiva info jagamist. Lisaks on üks privaatsuse kontseptsioone seotud ka intiimsuse ja suhetega. (Solove, 2008)

Privaatsust on tunnustatud fundamentaalse inimõigusena mitmesugustes õiguslikes vahendites, sh inimõiguste ülddeklaratsioonis ja Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis. Euroopa inimõiguste ja põhivabaduste kaitse konventsioon kirjeldab, et igal inimesel on õigus sellele, et austataks tema eraelu, perekonda ja kodu ning ametivõimud ei sekku selle õiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kaasinimeste õiguste ja vabaduste kaitseks (ECHR, art 8). Inimõiguste ülddeklaratsioon ütleb, et kedagi ei tohi meelevaldselt segada tema eraelu, perekonna, kodu ega kirjavahetuse juures ning ei tohi rünnata isiku au ja mainet. Kõigil on õigus seaduse kaitsele sellise sekkumise või rünnaku korral. (UDHR, art 12) Mida aeg edasi, seda suuremal määral on privaatsust tunnustatud inimõigusena. Meie praegune arusaam teabe privaatsusest põhineb mingil määral aga sellel, kuidas isik kontrollib juurdepääsu enda kohta käivale teabele (Botterman *et al.* 2009, 1). GDPR sätestabki õigusnormid, mis käsitlevad füüsiliste isikute kaitset isikuandmete töötlemisel ja isikuandmete vaba liikumist ning selle eesmärk on kaitsta nende isikute põhiõigusi ja –vabadusi, eriti nende õigust isikuandmete kaitsele (EL-i määrus 2016/679 artikkel 1). See tähendab, et isikul on kontroll oma andmete üle, tal on õigus ise otsustada, kellele ta oma andmeid jagab ning millisel määral ta neid kasutada lubab. Tema privaatsus on kaitstud ja tal on vabadus ise otsustada.

1.1.2. Isikuandmete kaitse ja selle reguleerimine

Paul M. Schwartz defineeris 2004. aastal isikuandmeid kui uue millenniumi olulist valuutat, millel on suur rahaline väärtus ning nende väärtus kasvab ajas (Schwartz, 2004, 2056). Mida väärtuslikumad on andmed, seda suurem oht on, et neid andmeid tahetakse enda valdusesse saada ja neid valesti kasutada või kuritarvitada. Inimeste üldise turvalisuse kaitseks on loodud seadused, mis tagavad kodanike õigused ning kaitsevad kodanikke teiste inimeste, organisatsioonide ja valituse kuritarvitamise eest (Law and … 2020). Õigus isiku perekonna- ja eraelu puutumatusele on põhiseaduslik õigus (PS-i § 26) ning seega on isikul ka õigus isikuandmete kaitsele.

Esimene samm, mis astuti Euroopas isikuandmete kaitsmiseks, tehti 1973. aastal, kui Euroopa Nõukogu Ministrite Komitee võttis vastu resolutsiooni 73 (22), mis kirjeldas elektroonilistes kanalites hoitavate isikuandmete töötlemist erasektoris. 1974. aastal laienes see avaliku sektorini resolutsiooniga 74 (29). Nendest resolutsioonidest kasvas 1981. aastal välja Euroopa Nõukogu

konventsioon nr 108, mille eesmärk oli tagada üksikisikute privaatsus ja kaitse isikuandmete automaattöötlusel, mille tulemusel tagatakse Euroopa Nõukogu liikmesriikide suurem ühtsus. Konventsioon kirjeldas ka delikaatsete isikuandmete mõistet, keelates ilma õigusliku aluseta töödelda isikute selliseid andmeid, mis viitavad näiteks poliitilisele ja usulisele kalduvusele, rassilisele päritolule vms. (Fuster, 2014) Praeguseks on konventsiooni ratifitseerinud 52 riiki, sealhulgas Eesti (Chart of … 2020). 1980. aastal avaldas Majanduskoostöö ja Arengu Organisatsioon (OECD — Organisation for Economic Co-operation and Development) privaatsuseeskirjad (*The OECD Privacy Guidelines*), mis on suuniste kogum, reguleerimaks piiriüleste andmete liikumist ja privaatsust. See oli esimene rahvusvaheline kokkulepe, mis defineeris eraelu puutumatuse kaitse peamised põhimõtted. Eeskirju täiendatakse pidevalt ning need on kasutusel ka tänapäeval. OECD eeskirjad on mõjutanud paljude riikide õigusaktide väljatöötamist. (Thirty Years After … 2011)

Mainitud reeglid ei olnud Euroopa Liidu tasandil ühtlustatud ning mõned liikmesriigid kohaldasid enda rangeid piiranguid, samas kui teistel reeglid puudusid. Euroopa siseturu areng oli pärsitud ja sellest ajendatuna loodi andmekaitse direktiiv (DPD — *Data Protection Directive*), mis ühtlustas siseturgu ning arendas piiriülest kaubandust. (Botterman *et al*. 2009) Andmekaitse direktiiv jõustus 24. oktoobril 1995. aastal (EL-i direktiiv 95/46/EÜ). Selle eesmärk oli kaitsta liikmesriikides isikuandmete töötlemisel füüsiliste isikute põhiõigusi ja -vabadusi, eelkõige nende õigust eraelu puutumatusele, ning tagada isikuandmete vaba liikumine liikmesriikide vahel (EL-i direktiiv 95/46/EÜ art 1). DPD laienes ka nendele andmetele, mis edastatakse liikmesriikidest välja kolmandatesse riikidesse — kolmandad riigid pidid andmeid vastu võttes tagama piisava turvalisuse taseme (EL-i direktiiv 95/46/EÜ art 25).

12. juulil 2002. aastal rakendus eraelu puutumatust ja elektroonilist sidet käsitlev Euroopa Parlamendi ja Nõukogu direktiiv 2002/58/EÜ (ePD — *Directive on privacy and electronic communications*), milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (EL-i direktiiv 2002/58/EÜ). Direktiiv tunnistas kehtetuks seni kehtiva direktiivi, mis käsitles isikuandmete töötlemist ja eraelu puutumatuse kaitset telekommunikatsioonisektoris (EL-i direktiiv 2002/58/EÜ art 19). Direktiiv loodi seoses elektrooniliste sideteenuste turu ja tehnoloogia arenguga, et tagada üldkasutatavate elektrooniliste sideteenuste kasutajatele isikuandmete ja eraelu puutumatuse kaitse võrdne tase olenemata kasutatavast tehnoloogiast (EL-i direktiiv 2002/58/EÜ põhjenduspunkt 4).

Nende aastate jooksul, kui DPD ja ePD on olnud kehtivad, on maailm muutunud, eriti selles, millisel moel ja kuidas isikuandmeid kogutakse ning töödeldakse (Botterman *et al.* 2009). Kasvab sotsiaalne integratsioon, areneb majandus- ja ühiskondliku elu eri valdkondade koostöö riikide vahel ning ka teadus- ja tehnikaalane koostöö (EL-i direktiiv 95/46/EÜ põhjenduspunktid 4–6). Lisaks neile muutustele on ka inimesed muutunud tunduvalt teadlikumaks sellest, kuidas nende isikuandmetega on võimalik pahatahtlikult ümber käia ja millised võivad olla tagajärjed (Botterman *et al.* 2009). Direktiiv on õigusakt, milles sätestatakse eesmärk, mille kõik EL-i liikmesriigid peavad saavutama. See jätab igale riigile õiguse otsustada, milliseid õigusakte kehtestada, et kõnealuseid eesmärke saavutada. (Määrused … 2020) Tekkis vajadus ajakohastada seni kehtivat direktiivi, elimineerides ebaühtlused riiklike seaduste vahel ning tõstes isikute andmete turvalisuse taset. Euroopa Komisjon tegi ettepaneku asendada kehtiv andmekaitse direktiiv isikuandmete kaitse üldmäärusega. (Blackmer, 2016) Määrus on siduv õigusakt, mida tuleb kohaldada tervikuna kogu EL-is (Määrused … 2020). Euroopa Ülemkogu ja Parlament kiitsid ettepaneku heaks (Blackmer, 2016). Euroopa Parlamendi ja Nõukogu määrus võeti vastu 27. aprillil 2016. aastal ning hakkas kehtima pärast kaheaastast üleminekuperioodi 25. mail 2018. aastal (EL-i määrus 2016/679).

GDPR ehk isikuandmete kaitse üldmäärus on regulatsioonina ühtne ja otsekohalduv kogu Euroopa Liidule (EL-i määrus 2016/679 art 3), asendades seni kehtinud DPD sätted. Määrust tuleb rakendada ettevõtetel, indiviididel, kohtutel ja võimuorganitel (Blackmer, 2016). GDPR on välja kasvanud 24. oktoobril 1995. aastal jõustunud andmekaitse direktiivist ehk ajast, kus internet ei olnud veel nii laialdaselt kasutusel kui praegu. Tänapäeval aga annavad tarbijad oma isikuandmeid päevast päeva ettevõtete käsitlusse, näiteks krediitkaardiga maksmisel, meditsiiniteenuste saamisel, sotsiaalmeedias, e-kaubanduse teenuseid kasutades jne — seega on oluline, et ka seadusi täiendatakse tänapäeva vajaduste järgi. Andmekaitsereform ei häiri piiriüleseid andmevooge ega teenuste kaubandust; selle asemel aitab see lahendada regulatiivseid erinevusi Euroopa ja USA digiteenuste pakkujate vahel, soodustades ausat konkurentsi Euroopa turul (Ciriani, 2015, 42–43). GDPR on otsekohalduv kõigile toimingutele, mis hõlmavad isikuandmete täielikult või osaliselt automatiseeritud töötlemist ja isikuandmete automatiseerimata töötlemist (EL-i määrus 2016/679 art 2) Euroopa Liidus või Euroopa Liidu kodanikega mujal maailmas (EL-i määrus 2016/679 art 3). See tähendab, et ka riigid väljaspool Euroopa Liitu peavad olema GDPR-iga kursis ning kogudes ja töödeldes Euroopa Liidu kodanike andmeid, peavad nad neid reegleid järgima ning oma toimingud määrusega vastavusse viima. Sanktsioonid määruse rikkumisel on suured: trahv

ulatub kuni 4%-ni ettevõtte aastasest kogukäibest, maksimaalselt 20 miljoni euroni (EL-i määrus 2016/679 art 83).

GDPR-i põhimõtted isikuandmete töötlemisel on, et tagatakse (EL-i määrus 2016/679 art 5):

1) seaduslik, õiglane ja andmesubjektile läbipaistev töötlemine;
2) täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel isikuandmete kogumine;
3) asjakohased, ajakohastatud ja olulised isikuandmed ehk andmed on piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt;
4) isikuandmete säilitamine kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik selle eesmärgi täitmiseks;
5) isikuandmete töötlemine viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ja juhusliku kaotamise, hävitamise või kahjustumise eest.

Enne GDPR-i rakendumist olid kehtivad andmekaitse direktiiv ning eraelu puutumatust ja elektroonilist sidet käsitlev Euroopa Parlamendi ja Nõukogu direktiiv, mis annab eelduse, et ettevõtted ei pidanud tegema suuri muudatusi GDPR-i rakendumisega, vaid oma protsessid üle vaatama ning vajadusel oma toimingud määrusega vastavusse viima. Turvalisus ja kaitse isikuandmete töötlemisel oli juba enne GDPR-i oluline.

1.2. Isikuandmete töötlemine veebiteenuseid osutavates ettevõtetes

Isikuandmed on mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on. 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. (EL-i määrus 2016/679 art 4) Seega, kui andmesubjekt ei ole tuvastatav ehk andmed on anonüümsed või ühegi tunnuse abil ei ole võimalik konkreetset isikut identifitseerida, siis ei ole GDPR-i mõistes tegemist isikuandmetega.

GDPR nõuab, et andmesubjekte teavitatakse, kuidas nende andmeid kogutakse ja töödeldakse (EL-i määrus 2016/679 art 12). E-kaubandusega tegelevad ja muud veebi kaudu teenuseid

osutavad ettevõtted koguvad isikuandmeid tihti juba hetkel, kui kasutaja jõuab nende veebisaidile. Tänapäeval on tavaline, et mõnda veebisaiti külastades või e-poest ostu sooritades leiab saidilt privaatsuspoliitika või küpsiste kasutamise teavituse. GDPR-i rakendumine muutis eelnimetatud teavitused kohustuslikuks. Näiteks on määruse kohaselt IP-aadress samuti personaalne informatsioon (EL-i määrus 2016/679 põhjenduspunkt 30) ning seega on pärast määruse rakendumist kohustuslik kasutajaid teavitada, kui veebisait kasutab küpsiseid. Et küpsiste kasutamine võimaldab parandada veebisaidi kasutajakogemust ning seeläbi suurendada veebisaidi kasutamise tulemuslikkust ja kasumlikkust, siis kasutab küpsiseid väga suur hulk veebisaite ning kasutaja võib teavitusi nende kasutamise kohta leida väga paljudelt külastatavatelt veebilehtedelt.

GDPR rakendus 2018. aasta maikuus (EL-i määrus 2016/679), kuid uuringud näitavad, et paljud ettevõtted ei ole endiselt nende nõuetega vastavuses (Fearn, 2018). 2019. aasta mais tehti uuring Euroopas väikese suurusega ettevõtete seas, kus uuriti ettevõtetelt nende GDPR-ile vastavuse kohta. Vastused viitasid laialdasele teadmatusele andmekaitse kohta ja sellele, et privaatsussätteid jäetakse järgimata. (*Ibid*.) GDPR näiteks nõuab, et ettevõtted kirjeldaksid andmetöötlustegevusi selges ja arusaadavas keeles (EL-i määrus 2016/679 art 12). Vaid 44% vastanud ettevõtetest kinnitasid, et nende ettevõtetes seda nõuet järgitakse (Fearn, 2018). Isikuandmete kaitse määrus nõuab ka, et ettevõtted tuvastaksid isikuandmete kasutamiseks seadusliku aluse (EL-i määrus 2016/679 art 6). Ligikaudu pooled vastanutest polnud täiesti kindlad, kas nad seda nõuet järgivad (Fearn, 2018). Selgub, et GDPR-i rakendamine on siiani probleemne, kuigi see rakendus juba 2018. aasta mais. Paljud suurettevõtted otsustasid enne määruse rakendumist panna selle juurutamise üheks oma võtmetegevuseks juhtkonna tasandil (Albrecht, 2016, 288). Privaatsus, turvalisus ning andmekaitse sai Euroopas justkui arenevaks kaubamärgiks, isegi kui määrus ei olnud veel rakendunudki (*Ibid*.). Paraku aga näitavad uuringud, et paljud väikese suurusega ettevõtted ei ole siiani GDPR-iga vastavuses.

1.2.1. Privaatsus- ja andmekaitsesätted

Isikuandmete kaitse määrus nõuab, et vastutav töötleja peab rakendama nii töötlemisvahendite kindlaksmääramisel kui ka isikuandmete töötlemise ajal asjakohaseid tehnilisi ja korralduslikke meetmeid, näiteks pseudonümiseerimine. Need on vajalikud andmekaitse põhimõtete (nagu võimalikult väheste andmete kogumine) tõhusaks rakendamiseks ja vajalike kaitsemeetmete lõimimiseks isikuandmete töötlemisse, et täita määruse nõudeid ja kaitsta andmesubjektide õigusi. (EL-i määrus 2016/679 art 25) GDPR nõuab ka, et vastutav töötleja võtab asjakohased meetmed,

et esitada andmesubjektile teave tema isikuandmete töötlemise kohta ja et teavitada teda isikuandmete töötlemisest järgneval viisil (EL-i määrus 2016/679 art 12):

- kokkuvõtlikult;
- selgelt;
- arusaadavalt;
- lihtsasti kättesaadavas vormis;
- kasutades selget ja lihtsalt keelt (eelkõige lapsele suunatud teabe puhul).

See teave esitatakse kirjalikult või muude vahendite abil, sealhulgas asjakohasel juhul elektrooniliselt. Kui andmesubjekt seda taotleb, võib teabe esitada suuliselt, tingimusel et andmesubjekti isikusamasust tõendatakse muude vahendite abil. (EL-i määrus 2016/679 art 12)

Selline info privaatsus- ja andmekaitsesätete kohta edastatakse tavaliselt kasutajatele veebilehe privaatsuspoliitikana. Privaatsuspoliitika ehk ettevõtte andmetöötlustoimingute põhimõtted võivad olla leitavad ettevõtte kodulehel ka järgmiste nimedega: privaatsustingimused, isikuandmete töötlemise põhimõtted, andmekaitse põhimõtted vms. Privaatsuspoliitikad sisaldavad infot selle kohta, milliseid andmeid teenusepakkuja kasutaja kohta kogub ning kuidas ja millisel eesmärgil ta nende andmeid töötleb. GDPR-i järgi on andmetöötlejal õigus isikuandmeid töödelda üksnes andmesubjekti nõusoleku saamisel või õiguslikul alusel (EL-i määrus 2016/679 art 6). Näiteks kui kasutaja algatab e-poes ostu, siis on e-poel õigus töödelda kasutaja nime, aadressi ja makseinfot lepingulise kohustuse järgi, et tehing lõpuni viia. Privaatsuspoliitikad peegeldavad tavaliselt ka isikute õigusi ja võimalusi nende andmete töötlemisel, näiteks, et andmesubjektil on õigus saada infot andmete kohta, mida vastutav töötleja hoiab ning et andmesubjektil on õigus igal ajal nõuda oma andmete kustutamist jms (EL-i määrus 2016/679 art 15, 16).

Uuringud on näidanud, et inimesed pühendavad privaatsuspoliitika lugemisele vähe aega või ei loe neid üldse ja nõustuvad tingimustega ilma privaatsussätteid lugemata (Steinfeld, 2016), samuti on leitud, et privaatsuspoliitikaid on raske lugeda ja mõista (Ali *et al.* 2008). USA-s tehtud uuring tõi välja, et paljud ei mõista, et privaatsustingimustega nõustumine on leping kahe poole vahel (Anderson, Vogels 2019). Näiteks kui isik teeb endale mõnele veebilehele kasutajakonto, jagades oma isiklikke andmeid, siis üldjuhul on tal vaja pärast ankeedi täitmist lugeda läbi privaatsuspoliitika või muu sarnase nimega dokument ning sellega enne oma andmete edastamist

nõustuda. Nõustumine nende tingimustega ja jätkamine oma andmete edastamisega on leping kahe poole vahel, mis kinnitab, et isik on lugenud läbi ettevõtte andmete kogumise ja töötlemise põhimõtted ja nendega nõustunud. 2018. aasta juunis, kui GDPR oli juba rakendunud, korraldati 543 katse inimesega, mis kinnitas, et 74% osalistest liikus ankeedi täitmisel edasi isikuandmete töötlemise põhimõtetega nõustudes, kuid seda dokumenti isegi ei avatud (Hirsch, Obar 2018).

Privaatsuspoliitikad erinevad sisu, pikkuse, sõnakasutuse ja keerukuse poolest. Lisaks võivad privaatsuspoliitikad erineda ka valdkondade kaupa ehk sõltuda sellest, mis teenust ettevõte pakub. Näiteks terviseasutused töötlevad isikute terviseandmeid, tavalised e-kaubandusettevõtted selliseid andmeid ei kogu. GDPR reguleerib erineva tegevusulatusega valdkondi, mis töötlevad väga erinevaid isikuandmeid. Näiteks võivad suurettevõtted omada mitut erinevat veebisaiti ja mobiilirakendust, nad võivad omada füüsilisi asutusi (näiteks kauplusi) või töödelda inimeste terviseandmeid jms.

Magistritöö autor töötas läbi Euroopa Parlamendi ja Nõukogu määruse 2016/679 ning tõstab esile tähtsamad aspektid GDPR-ist, mis on uurimuses olulised. Selle eesmärk on võtta ülevaatlikult kokku olulisimad andmetöötlustoimingute aspektid, mida peaks teenusepakkuja infona andmesubjektile edastama. Selles uurimuses käsitletakse e-kaubanduse ja muid veebiteenuseid osutavate ettevõtete käsitletavaid isikuandmeid.

Autor ei erista töö uurimisosas isikuandmete eriliikide töötlemist ja nendest tulenevaid erisusi. GDPR käsitleb isikuandmete eriliikide töötlemist, mis tähendab, et keelatud on töödelda isikuandmeid, millest ilmneb (EL-i määrus 2016/679 art 9):

- rassiline või etniline päritolu;
- poliitilised vaated;
- usulised või filosoofilised veendumused või ametiühingusse kuulumine;
- geneetilised andmed;
- füüsilise isiku kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed;
- terviseandmed või andmed füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta.

Järgnevad andmed andmetöötlustoimingute aspektide väljatoomiseks on võetud Euroopa Liidu määrusest 2016/679. Põhjalikum info ja regulatiivne lähenemine toodud aspektidest on leitavad

seadusest ning viited, millistest määruse punktidest on aspekti kirjeldused kokku pandud, on leitavad tabelis 1 ning lisas 2. Eristatud on üheksat aspekti (EL-i määrus 2016/679):

1. Andmete kogumine ja töötlemine. Andmeid tuleb koguda ainult kindlaksmääratud ja õiguspärastel eesmärkidel ning neid töödeldakse hiljem üksnes nende eesmärkidega kooskõlas oleval viisil. Andmed on asjakohased ja olulised ehk kogutakse võimalikult vähe andmeid, andmeid ajakohastatakse vajadusel ning ebaõiged andmed kustutatakse. Andmete töötlemine on seaduslik juhul, kui andmesubjekt on andnud nõusoleku oma isikuandmeid töödelda, töötlemine on vajalik vastutava töötleja juriidilise kohustuse täitmiseks, isiku eluliste huvide kaitsmiseks või andmesubjektiga sõlmitud lepingu täitmiseks / lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele. Andmete kogumisel ja töötlemisel on oluline edastada andmesubjektile vastutava töötleja kontaktandmed.
2. Nõusoleku andmine. Andmesubjekti nõusolekut oma isikuandmete töötlemiseks peab olema võimalik tõendada, see peab olema antud selge kinnitusena. Nõusolekut peab olema võimalik igal ajal tagasi võtta.
3. Kolmandate osapooltega andmete jagamine. Kui vastutav töötleja kavatseb edastada andmeid kolmandatele osapooltele, siis tuleb andmesubjekti sellest teavitada. Samuti peab andmesubjektile teatavaks tegema, mis eesmärgil andmeid edastatakse.
4. Andmete säilitamine. Isikuandmeid säilitatakse selliselt, et andmesubjekte on võimalik tuvastada ainult seni, kuni see on vajalik eesmärgi täitmiseks. Andmete säilitamiseks kasutatakse tehnilisi ja korralduslikke meetmeid, mis toetavad andmesubjektide õiguste ja vabaduste kaitset. Vastutav töötleja peab teavitama andmesubjekti isikuandmete säilitamise ajavahemikust.
5. Lapse turvalisus. Kui teenust pakutakse otse lapsele, siis on lapse isikuandmete töötlemine seaduslik ainult juhul, kui nõusoleku andnud laps on vähemalt 16-aastane. Muul juhul on lapse isikuandmete töötlemine seaduslik ainult selles ulatuses, mis ulatuses on nõusoleku andnud tema vanem.
6. Teavitamine. Vastutav töötleja peab teavitama andmesubjekti isikuandmete parandamisest, töötlemisest või nende mittetöötlemisest vähemalt ühe kuu jooksul pärast andmesubjekti vastavat taotlust. Lisaks peab töötleja teavitama andmesubjekti isikuandmete töötlemise toimingu tegemisest ja selle eesmärkidest.
7. Andmete haldamine andmesubjekti poolt. Andmesubjektil on õigus taotleda enda kohta käivate andmete kustutamist, parandamist või andmete töötlemise piiramist. Tal on igal ajal õigus nõuda teavet enda kohta käivate andmete kohta masinloetaval kujul ning edastada neid

teisele vastutavale töötlejale. Andmetöötleja peab seadma vaikimisi privaatsussätted või võimaldama andmesubjektil neid sätteid vastavalt soovile reguleerida.

8. Profiilianalüüs ja küpsised. Andmesubjektil on õigus, et tema kohta ei võetaks üksnes automatiseeritud töötlusel põhinevaid otsuseid. Kasutajal on õigus saada infot, kui tema isikut seostatakse IP-aadresside või küpsistega. Kasutajal on igal ajal õigus keelduda otseturunduse eesmärgil tehtud isikuandmete töötlusest.
9. Andmete turvalisus. Vastutav töötleja peab rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid andmete turvalisuse tagamiseks. Andmetöötleja on kohustatud teavitama andmesubjekti isikuandmetega seotud rikkumisest.

Tabel 1. EL-i määruse 2016/679 aspektide loetelu ja nende koostamise aluseks olevad määruse artiklite ja põhjenduspunktide viited

Aspektid ja nende kirjeldus	Viide
1. Andmete kogumine ja töötlemine	Artiklid 5 (1), 6, 9, 10, 11, 13, 14 (1), põhjenduspunktid 39, 44–47, 58
2. Nõusoleku andmine	Artiklid 7, 12 (2), 14 (2), põhjenduspunktid 32, 40–43
3. Kolmandate osapooltega andmete jagamine	Artiklid 13 (1), 14 (1), põhjenduspunkt 48
4. Andmete säilitamine	Artiklid 5 (1), 13 (2), 14 (2), põhjenduspunkt 39
5. Laste turvalisus	Artikkel 8, põhjenduspunkt 38
6. Teavitamine	Artiklid 12 (1,3,4), 13 (1), 19, põhjenduspunktid 60, 61
7. Andmete haldamine andmesubjekti poolt	Artiklid 12 (2), 15, 16, 17, 18, 20, 21 (1), 25, põhjenduspunktid 59, 63, 65, 66, 68, 70, 78
8. Profiilianalüüs ja küpsised	Artiklid 21, 22, põhjenduspunktid 28–30, 71, 72
9. Andmete turvalisus	Artiklid 32, 34

Allikas: Autori koostatud EL-i määruse 2016/679 alusel

Eeltoodud üheksa andmetöötlustoimingu aspekti saavad olema aluseks töö teisele osale, kus nende aspektide põhjal koostatakse mudel privaatsuspoliitikate sisu kontrollimiseks.

1.2.2. Küpsised ja profiilianalüüs

Aspekt 8 puudutab profiilianalüüsi ja küpsiseid. Küpsiste kasutamist on GDPR-is üsna vähe mainitud, kuid tegelikult on küpsiste kasutamine enim levinud viis isikuandmete kogumiseks.

Valdav osa külastatavaid veebisaite kasutavad lehe kasutajakogemuse parandamiseks küpsiseid. Küpsised on informatsioon, mida edastatakse internetiserveri ja kasutaja veebibrauseri vahel (Cunningham, 2002). Need on failid väikeste andmetega, mida kasutatakse kasutaja arvuti tuvastamiseks. Internetiserver tuvastab minimaalselt kasutaja IP-aadressi ja selle, milline veebibrauser on kasutusel. Küpsistesse salvestatud andmed aitavad parandada kasutaja veebibrauseri kogemust. (*Ibid.)* Näiteks kui kasutaja külastab jalatsipoe veebilehte, siis küpsiseid kasutades saab e-pood ennast kasutajale rohkem nähtavaks teha ja ennast meelde tuletada. Kasutaja võib näiteks pärast külastust leida nimetatud veebipoe *pop-up*-reklaame internetis navigeerides.

Veebisaidid kasutavad erinevaid küpsiseid ja enamjaolt on kasutajal võimalik ise seadistada, milliseid küpsiseid ta lubab veebisaidil kasutaja kohta koguda. Edasi on mõned näited, millist tüüpi küpsiseid kogutakse (Different types … 2020):

1. Sessiooniküpsised — aitavad veebisaidil kasutajat ja nende informatsiooni tuvastada, kui nad läbi veebisaidi navigeerivad. Need küpsised säilitavad infot ainult ajal, kui kasutaja on veebisaidil. Kui veebibrauser suletakse, siis küpsised kustutatakse. Kasutatakse enim e-kaubandusega seotud veebilehtedel.
2. Püsivad küpsised — jäävad toimima ka pärast veebibrauseri sulgemist. Näiteks võivad nad jätta meelde sisselogimisandmed, et veebikasutaja ei peaks neid iga kord saidi kasutamisel uuesti sisestama.
3. Kolmandate osapoolte küpsised — need küpsised installeerivad veebisaidile kolmandad osapooled eesmärgiga koguda veebikasutajalt teatud teavet. Näiteks et uurida kasutaja käitumist või harjumusi. Selliseid küpsiseid kasutavad tavaliselt reklaamijad, kes soovivad tagada toodete ja teenuste turundamise õigele sihtrühmale.
4. *Flash*-küpsised — need küpsised on veebibrauserist sõltumatud. Need on loodud püsivalt kasutaja arvutisse salvestamiseks. Seda tüüpi küpsised jäävad kasutaja seadmesse ka siis, kui kõik küpsised on nende veebibrauserist kustutatud. Neid kasutatakse näiteks veebisaidil mingisuguste kasutaja püsivate eelistuste säilitamiseks (näiteks helitugevus video vaatamisel).
5. *Zombie*-küpsised — need on *flash*-küpsiste tüüp, mis luuakse automaatselt pärast kasutaja kustutamist, neid on raske avastada ja hallata. *Zombie*-küpsiseid saab kasutada inimeste jälgimiseks ja ka identifitseerimiseks.

GDPR-i rakendumine mõjutas märkimisväärselt neid ettevõtteid, kes tuginevad oma tegevuses kliendianalüütikale ja isikustatud turundusele. Eelkõige koguvad veebipõhised ettevõtted andmeid

selle kohta, kuidas jõuavad kasutajad veebisaidile ja kuidas nad seal navigeerivad. Veebianalüüsi tulemusel on võimalik meelitada kasutajaid oma saiti külastama ja kogutud andmete abil on võimalik saidi sisu parandada. (Goldberg *et al.* 2019, 2) Küpsised on üks võimalus kliendianalüütikaks. Ka läbi profiilianalüüsi on võimalik kliendianalüütikat teha. Profiilianalüüs on igasugune isikuandmete automatiseeritud töötlemine, millega on võimalik viia läbi füüsilise isikuga seotud teatavate isiklike aspektide hindamist, kasutades isikuandmeid (EL-i määrus 2016/679 art 4). Seda kasutatakse eelkõige selliste aspektide analüüsimiseks või prognoosimiseks, mis on seotud füüsilise isiku töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste, huvide, usaldusväärsuse, käitumise, asukoha või liikumisega (*Ibid*.). Andmesubjekti tuleb teavitada küpsiste kasutamisest ja profiilianalüüsi kasutamisest (EL-i määrus 2016/679 art 13, 14).

Esimeses peatükis kirjeldatud andmetöötlustoimingute aspektid on olulised teise peatüki ehk uurimisosa juures. Nimetatud üheksa aspekti saavad aluseks teises peatükis riskihindamiseks ning uurimismudeli koostamiseks ja analüüsiks.

2. PRIVAATSUSPOLIITIKATE VASTAVUS ISIKUANDMETE KAITSE ÜLDMÄÄRUSELE

Peatükis arutletakse, milliseid riske võib tuua füüsilisele isikule kaasa see, kui tema isikuandmete töötlemise tulemusel tekib talle materiaalne või mittemateriaalne kahju. Arutletakse, millisel määral võib füüsilisele isikule peegeldada ettevõtte privaatsuspoliitika sisu riski, et tema isikuandmete edastamisel sellele vastutavale töötlejale kaasneb mingi tagajärg. Luuakse mudel, millega oleks võimalik lihtsustada privaatsuspoliitikate sisu lugemist ja isikuandmete kaitse määrusele vastavuse kontrollimist ning koostatakse valim ettevõtetest, kelle privaatsuspoliitikate peal mudelit testitakse.

2.1. Isikuandmete edastamisega kaasnevad võimalikud riskid füüsilisele isikule

Riskil on mitmeid definitsioone, näiteks:

1. risk on sündmuse tõenäosuse ja selle tagajärgede kombinatsioon (ISO/Guide … 2009);
2. risk on võimalus, et tulevikus võib juhtuda midagi halba või olukord, mis võib olla ohtlik või millel võib olla halb tulemus (Oxford … 2020).

Kui füüsiline isik jagab informatsiooni ja andmeid enda kohta, kaasneb risk, et sellega tekib isikule mingisugune kahju. Jagamine on sündmus, kahjujuhtum on tagajärg. Kahju võib olla materiaalne või immateriaalne ehk risk, et isiku konfidentsiaalsus ei ole tagatud. Isikuandmete kaitse üldmääruse üks eesmärke on aidata kaasa füüsiliste isikute heaolule ja seega vähendada riski, et nende isikuandmete kogumisel ja töötlemisel juriidiliste isikute poolt ei oleks tagajärgi (EL-i määrus 2016/679 põhjenduspunkt 2).

GDPR otseselt ei defineeri riski, mis isikuandmete kogumise ja töötlemisega kaasneb, kuid viitab kahjudele, mis võivad füüsilisele isikule tekkida isikuandmete töötlemisel. 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 (EL-i määrus 2016/679 põhjenduspunkt 75):

- töötlemine võib põhjustada:
    - diskrimineerimist;
    - identiteedivargust või -pettust;
    - rahalist kahju;
    - maine kahjustamist;
    - ametisaladusega kaitstud isikuandmete konfidentsiaalsuse kadu;
    - pseudonümiseerimise loata tühistamist;
    - 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;
    - ametiühingusse kuulumist;
    - geneetilisi andmeid;
    - terviseandmeid;
    - seksuaalelule viitavaid andmeid;
    - süüteoasjades süüdimõistvate kohtuotsusteid ja süütegusid ning nendega seotud turvameetmeid;
- hinnatakse profiilide loomiseks isiklikke aspekte, eelkõige aspekte, mis on seotud:
    - töötulemuste;
    - majandusliku olukorra;
    - tervise;
    - isiklike eelistuste või huvide;
    - asukoha või liikumisega;
- töödeldakse kaitsetute füüsiliste isikute, eriti laste isikuandmeid;
- töötlemine hõlmab suurt hulka isikuandmeid ning mõjutab paljusid andmesubjekte.

Järgmiseks analüüsitakse, milliseid tagajärgi võib kaasa tuua füüsilisele isikule see, kui ettevõtted ei rakenda piisavaid meetmeid tema andmete kogumisel ja töötlemisel (vt tabel 2). Tegu on autori objektiivse hinnanguga.

Tabel 2. Võimalikud immateriaalsed ja materiaalsed kahjud füüsilisele isikule tema isikuandmete valesti töötlemisel

Immateriaalne kahju	Materiaalne kahju
1. mainekahju 2. häbi või stress, mis tulenevad andmete eksponeerimisest 3. hirm enda või pere heaolu üle 4. eraelu avalikustamine 5. laimamine või diskrimineerimine 6. sõnavabaduse kaotus 7. kontrolli kaotamine oma andmete üle 8. suhete rikkumine isiku lähedastega	1. rahaline kahju, kui keegi kuritarvitab isikuandmeid või kui kaob sissetulek 2. vabaduse kaotus

Allikas: autori koostatud

Esimeses peatükis analüüsis autor GDPR-i andmetöötlustoimingute aspekte, mis on olulised, kui veebiteenuseid osutavad ettevõtted koguvad ja töötlevad isikuandmeid. Autor tõi välja üheksa aspekti ehk teabe, mida peaks vastutav töötleja esitama andmesubjektile tema isikuandmete töötlemise kohta. Autor usub, et ettevõtte veebilehel kuvatavad privaatsustingimused peegeldavad ettevõtte usaldusväärsust ning privaatsuspoliitika nõuetele vastav sisu näitab, et ettevõte on oma andmetöötlustoimingud läbi mõelnud ja kaardistanud. See näitab, et ettevõtte tegevus on läbipaistev ja andmetöötlustoimingud on füüsilistele isikutele turvalised.

Kui vastutav töötleja on avaldanud iga aspekti kohta kokkuvõtliku, selge ja arusaadava info, siis võib öelda, et vastutava töötleja tegevus on füüsilise isiku jaoks läbipaistev ning seega on väike risk, et andmesubjekti jaoks kaasneb mingisugune tagajärg, kui ta oma isikuandmeid töötlemiseks edastab. Kui vastutav töötleja on avaldanud iga aspekti kohta mingisuguse info, mida ei saa võibolla lugeda selgeks, kokkuvõtlikuks või arusaadavaks, siis võib järeldada, et vastutav töötleja võibolla ei ole oma andmetöötlustoiminguid täielikult läbi mõelnud ja määrusega vastavusse viinud. Andmesubjekt võib arvestada, et on olemas keskmine risk, et tema andmete edastamisel

vastutavale töötlejale kaasneb oht, et andmete kogumine ja töötlemine ei ole turvaline või nõuetekohane. Kui puudub igasugune info andmetöötlustoimingute kohta, siis võib järeldada, et füüsilise isiku jaoks on olemas suur risk, kui ta oma andmeid vastutavale töötlejale edastab.

Järgmiseks hinnatakse kvalitatiivse riskihindamise käigus, milline privaatsuspoliitika sisu võiks peegeldada erineva tasemega riski füüsilisele isikule, kui ta oma isikuandmeid vastutavale töötlejale edastab. Kui andmetöötlustoimingud on kirjeldatud vastutava töötleja privaatsuseeskirjades kokkuvõtlikult, selgelt ja arusaadavalt, siis on väike risk, et isikule kaasneb mingi tagajärg, kui ta oma andmed ettevõttele töötlemiseks edastab. Kui aga privaatsuspoliitikas on andmetöötlustoimingud kajastatud puudulikult või on sisu ebaselge, siis võib järeldada, et tegemist on andmesubjektile suurema riskiga, kui ta otsustab oma andmeid vastutavale töötlejale edastada. Eristatakse kolme riskiastet: väike, keskmine ja suur risk.

Aspekt 1. Andmete kogumine ja töötlemine:

- Väike risk — privaatsuspoliitikas on välja toodud andmete kogumise põhimõtted ja töötlemise eesmärgid. Esitatud on kogu vajalik teave andmetöötleja kohta ja muu info, mida kasutaja peaks teadma selle kohta, kuidas kogutud andmeid töödeldakse.
- Keskmine risk — privaatsuspoliitikas on välja toodud andmete kogumise üldpõhimõtted, kuid töötlemise eesmärk ei ole täielikult mõistetav.
- Suur risk — privaatsuspoliitikast ei ole võimalik välja lugeda, milliseid andmeid kogutakse ja millisel eesmärgil neid töödeldakse. Olemas on andmetöötleja kontaktandmed.

Aspekt 2. Nõusoleku andmine:

- Väike risk — kasutajal on võimalik anda nõusolek selge kinnitusena ja antud nõusoleku ulatus on selge. Nõusolekut on võimalik igal ajal tagasi võtta.
- Keskmine risk — kui isikuandmeid kasutatakse mitmel eesmärgil, küsitakse kasutajalt vaid ühekordne kinnitus isikuandmete töötlemiseks.
- Suur risk — kasutajalt ei küsita nõusolekut isikuandmete töötlemiseks ja andmeid töödeldakse ilma nõusolekuta. Nõusolekuks loetakse eelmärgistatud lahtreid.

Aspekt 3. Kolmandate osapooltega andmete jagamine:

- Väike risk — privaatsuspoliitikas on kinnitatud, et andmeid ei jagata kolmandate osapooltega. Juhul kui kolmandate osapooltega andmeid jagatakse, siis toimub see vaid kasutaja nõusolekul ja kindlaksmääratud eesmärkidel.
- Keskmine risk — olemas on info kolmandatele osapooltele andmete jagamise kohta, kuid pole infot, millisel eesmärgil edastatud andmeid kasutatakse.
- Suur risk — puudub info kolmandate osapooltega andmete jagamise kohta. Andmed edastatakse kolmandatele osapooltele ilma kasutaja nõusolekuta.

Aspekt 4. Andmete säilitamine:

- Väike risk — isikuandmete säilitamise ajavahemik on selgelt välja toodud ja andmete säilitamiseks kasutatakse turvalisi meetmeid.
- Keskmine risk — määratud on isikuandmete säilitamise ajavahemiku kriteeriumid. Andmed kustutatakse mõistliku aja möödudes pärast nende kasutamise lõppu.
- Suur risk — puudub info, kuidas ja kui kaua isikuandmeid säilitatakse. Isikuandmeid hoitakse kauem, kui see on eesmärgi täitmiseks vajalik.

Aspekt 5. Laste turvalisus:

- Väike risk — laste andmeid ei koguta ega töödelda. Juhul kui teenusepakkuja töötleb laste andmeid, siis on privaatsuspoliitikas kirjas, milliseid andmeid kogutakse ja millistel eesmärkidel. Andmeid kogutakse ja töödeldakse vaid lapsevanema nõusolekul.
- Keskmine risk — laste andmeid kogutakse ja töödeldakse lapsevanema nõusolekul, kuid pole välja toodud, millisel eesmärgil andmeid töödeldakse.
- Suur risk — laste andmeid kogutakse ja töödeldakse vanema nõusolekuta ning andmete töötlemise eesmärk on teadmata.

Aspekt 6. Teavitamine:

- Väike risk — isikuandmete parandamisest, töötlemisest või mittetöötlemisest teavitatakse kasutajat kohe. Privaatsuspoliitika tingimuste muutumisest teavitatakse kasutajat kohe.
- Keskmine risk — privaatsuspoliitika tingimuste muutumisest ja isikuandmete parandamisest, töötlemisest või mittetöötlemisest teavitatakse kasutajat mõistliku aja möödudes pärast muudatuste tegemist.

- Suur risk — privaatsuspoliitika ei sisalda teavet selle kohta, kas kasutajat teavitatakse, kui muutuvad privaatsuspoliitika tingimused. Kasutajat ei teavitata, kui isikuandmete töötlemise eesmärgid muutuvad või isikuandmeid enam ei töödelda.

Aspekt 7. Andmete haldamine andmesubjekti poolt:

- Väike risk — kasutajal on võimalik igal ajal oma andmeid ise kustutada, muuta või nende töötlemist piirata. Teave on igal ajal kättesaadav.
- Keskmine risk — muudatused kasutaja andmetega tehakse mõistliku aja möödudes pärast kasutaja tehtud sellekohast avaldust.
- Suur risk — informatsioon selle kohta, kuidas on kasutajal võimalik oma andmeid hallata, puudub. Puudub info, et kasutajal on õigus oma andmeid kustutada, muuta või saada infot, milliseid andmeid töödeldakse.

Aspekt 8. Profiilianalüüs ja küpsised:

- Väike risk — kasutajale kuvatakse nähtavalt küpsiste teavitused ja on kirjeldatud, milliseid küpsiseid kasutatakse. Kui kasutatakse profiilianalüüsi, siis on kirjas, millistel eesmärkidel.
- Keskmine risk — kasutajale kuvatakse nähtavalt küpsiste teavitused.
- Suur risk — puudub info küpsiste kasutamise kohta, kuid veebileht kasutab neid.

Aspekt 9. Andmete turvalisus:

- Väike risk — privaatsuspoliitika toob välja, et isikuandmete kogumisel ja töötlemisel rakendab andmetöötleja asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada andmete turvalisus. Isikuandmetega seotud rikkumistest teavitatakse andmesubjekte kohe.
- Keskmine risk — privaatsuspoliitikas on välja toodud, et andmete turvalisus on tagatud ja andmesubjekte teavitatakse isikuandmetega seotud rikkumistest.
- Suur risk — privaatsuspoliitikas ei ole välja toodud, et andmete kogumisel ja töötlemisel rakendatakse meetmeid nende andmete turvalisuse tagamiseks.

Iga aspekti kolme riskiastet arvesse võttes uuritakse uurimismudeli abil magistritöö teise osa kolmandas alapeatükis, millise riskiastmega on valimisse sattunud ettevõtete privaatsuspoliitikad füüsilise isiku jaoks, kes oma andmed vastavatele ettevõtetele edastab.

2.2. Valimi ja uurimismudeli koostamine

Valim koostatakse ettevõtetest, kes tegelevad e-kaubanduse ja muude veebiteenuste osutamisega. Valimi koostamisel võeti aluseks Alexa.com veebilehelt leitud tabel enimkülastatud veebilehtede kohta Eestis (Top Sites … 2020). Tabelis on esitatud 500 enimkülastatud veebilehte (*Ibid.*). Autor otsib esimeselt 250-lt nimekirjas esitatud veebilehelt privaatsuspoliitika ja kasutab edasisel töötlusel neid andmeid tekstidokumentidena.

Kriteeriumiteks on:

1. veebileht kogub ja töötleb isikuandmeid;
2. saadaval on eestikeelne privaatsuspoliitika / isikuandmete töötlemise põhimõtted / privaatsuseeskirjad või muu taoline dokument, mis kajastab veebilehe põhimõtteid isikuandmete kogumisel ja töötlemisel.

Eesti elanikkonnas on suur hulk vene keelt kõnelevaid ja seega ka venekeelseid veebisaite külastavaid inimesi ning seetõttu on Alexa tabelis palju saite, mis on venekeelse sisuga. Samuti on edetabelis palju ingliskeelseid saite, mida Eesti elanikkond kasutab ja vaid vähestel on saadaval eestikeelne privaatsuspoliitika.

Alexa.com veebilehelt algandmete kogumisel leidis autor, et uurimuseks ei sobi 182 veebilehte, millest:

1. 150 veebilehte olid võõrkeelse sisuga ja seetõttu ei olnud saadaval eestikeelne privaatsuspoliitika.
2. Kaheksal juhul oli tegemist korduva sisuga privaatsuspoliitikaga. Näiteks Youtube.com kuulub Google.com-i gruppi ja neil on ühised privaatsuseeskirjad, mida on juba uurimuses kajastatud.
3. 19 juhul oli lehe sisu ebasobiv, veebileht ei avanenud või ei töötle see veebileht isikuandmeid.
4. Kolmel juhul privaatsuspoliitikale viitav link ei avanenud ehk privaatsuspoliitika ei olnud kättesaadav.
5. Kahel juhul ei olnud privaatsuspoliitika veebisaidilt leitav, kuigi oli selge, et veebileht tegeleb isikuandmete töötlemisega.

Autor leidis, et 68 uurimuseks kogutud privaatsuspoliitikat on liiga väike valim uurimuse tegemiseks. Alexa.com edetabeli esimesest 250 veebilehest oli võimalik kasutada vaid 27,2% veebilehtedest. Et see protsent on küllaltki väike ja uurimuses võiks olla rohkem e-kaubandusega seotud ettevõtteid, siis otsustas autor koguda lisaks andmeid Eesti E-kaubanduse Liidu kodulehelt. Seal on nimekiri 325 ettevõttest, kes kuuluvad E-kaubanduse Liitu (Liidu liikmed … 2020). Eesti E-kaubanduse Liit on e-kauplejate ja e-kaubandusega seotud ettevõtete esindusorganisatsioon, kuhu kuulub 325 ettevõtet. Liidu liikmeks on oodatud kõik aktiivsed ja edumeelsed ettevõtted ning eraisikud, kes soovivad panustada e-kaubanduse arengusse Eestis. (*Ibid.*) Autor soovis koguvalimi koostada 120 privaatsuspoliitikast, seega kasutades süstemaatilist juhuvalimit, otsis autor Eesti E-kaubanduse Liidu lehelt juurde 52 privaatsuspoliitikat (vt lisa 3).

Autor koostas privaatsuspoliitikate analüüsimudeli, et teha selgeks, kas vaadeldavad privaatsuspoliitikad sisaldavad informatsiooni, mida isikuandmete kaitse üldmäärus nõuab. Kasutatakse varem koostatud GDPR-i andmetöötlustoimingute aspektide loetelu ja koostatud privaatsuspoliitikate sisu peegeldavat riskihindamist. Nende põhjal koostatakse analüüs selle kohta, millised märksõnad võiksid viidata määruse igale üheksale aspektile, arvestades nende riskiastet. Autor otsib iga aspekti võimalikud peegeldavad märksõnad (vt tabel 3). Märksõnadest on eraldatud sõnatüved ja sõnatüvesid kasutatakse otsingus. Mõne märksõna puhul kasutatakse mitut tüve, sest sõna käänamisel võib tüvi muutuda (näiteks *hoid/ma* või *hoia/me* või *hoitakse*).

Märksõnu kasutava otsingu eesmärk on välja selgitada, kas sellise mudeliga on võimalik kontrollida privaatsuspoliitikate sisu ja milline on vaadeldavate ettevõtete privaatsuspoliitikate riskiaste füüsilise isiku jaoks, kes oma andmed neile ettevõtetele edastab. See mudel võiks lihtsustada privaatsuspoliitikate lugemist ja nende mõistmist.

Küpsiste kasutamise teavitusi ei ole võimalik selle mudeliga kontrollida. Autor koostab vaadeldavate veebilehtede küpsiste kasutamise kohta eraldi ülevaate.

Tabel 3. Märksõnad andmetöötlustoimingute aspektide kontrollimiseks

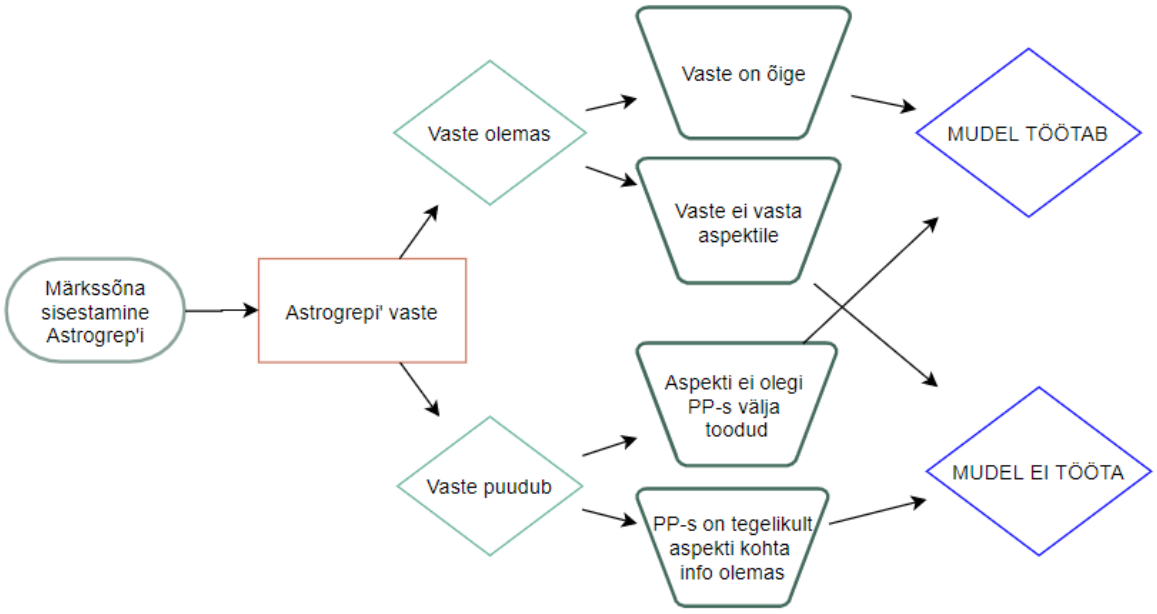
Andmetöötlustoimingute aspekt	Väike risk	Keskmine risk	Suur risk
Andmete kogumine ja töötlemine	*kogu/mine, töötle/mine* või *töödeldakse, eesmär/gid, kontakt*	*kogu/mine, töötle/mine* või *töödeldakse, kontakt*	*kontakt või* -
Nõusoleku andmine	*nõusolek, kinnit/ama*	*nõusolek, kinnit/ama*	-
Kolmandate osapooltega andmete jagamine	*kolmanda/d, osapool/ed*	*kolmanda/d, osapool/ed*	-
Andmete säilitamine	*säilita/mine, hoid/ma* või *hoia/me* või *hoitakse,*	*säilita/mine, hoid/ma* või *hoia/me* või *hoitakse,*	-
Laste turvalisus	*laps/ed* või *laste*	*laps/ed* või *laste*	-
Teavitamine	*teavita/ma*	*teavita/ma*	-
Andmete haldamine andmesubjekti poolt	*kustuta/ma, muut/ma* või *muudatus/ed, paranda/ma,*	*kustuta/ma, muut/ma* või *muudatus/ed, paranda/ma,*	-
Profiilianalüüs ja küpsised	*profiilianalüüs või automatiseeri/tud (otsused)*	*profiilianalüüs või automatiseeri/tud (otsused)*	-
Andmete turvalisus	*turva/line, rikku/mine, tehnili/ne*	*turva/line, rikku/mine,*	-

Allikas: autori koostatud

Autor kasutab mudeli tulemuste saamiseks programmi AstroGrep. AstroGrep on Microsoft Windowsi käsuprogramm, mis otsib failidest sõnu. (AstroGrep … 2019) Analüüsimiseks lasti kõik märksõnad läbi programmi ja programm otsis märksõnu kõigist 120 privaatsuspoliitikast. Et aru saada, kas mudel töötab ja leida ligikaudne veaprotsent, mis mudeli kasutamisel tekib, kasutas autor manuaalset kontrolli.

Mudeli kontrollimiseks kasutatakse manuaalset kontrolli. Süstematiseeritud juhuvalimiga valitakse välja 10% kontrollitud privaatsuspoliitikaid ning kontrollitakse manuaalselt, kas mudel

töötab (vt joonis 1). Kui AstroGrep leiab privaatsuspoliitikast (PP) vaste sisestatud märksõna kohta ja PP sisaldab märksõnale vastavat aspekti, siis mudel töötab. Kui mudel leiab vaste, kuid PP-s käib vaste mingi muu aspekti kohta või on märksõna täiesti teises kontekstis, siis mudel ei tööta. Kui AstroGrep ei leia vastet märksõnale ja PP ei sisalda ka märksõnale vastavat aspekti, siis mudel töötab. Kui AstroGrep ei leia vastet märksõnale, kuid PP tegelikult sisaldab märksõnale vastavat aspekti (näiteks on sõnastus erinev), siis mudel ei tööta.



Joonis 1. Mudeli manuaalse kontrolli protsess
Allikas: autori koostatud

Manuaalne kontroll viidi läbi kõigi märksõnade (kokku 19 tk) puhul ja selle tulemusel selgus, milline on erinevate märksõnade täpsus ehk usaldatavus loodud mudeli puhul (vt. tabel 4).

Tabel 4. Mudeli ligikaudne täpsus märksõna kohta

Mudeli täpsus märksõna puhul	Märksõna (tüvisõna)
91–100%	*töötle* või *töödelda, nõusolek, säilita , kustuta, turva, eesmär, kinnit, profiilianalüüs* või *automatiseeri ja tehni*
81–90%	*teavi, kogu* ja *rikku*
71– 80%	*paranda, kolmanda ja osapool*
61–70%	*hoid* või *hoia* või *hoitakse* ja *muut* või *muudatus*
51–60%	*kontakt*

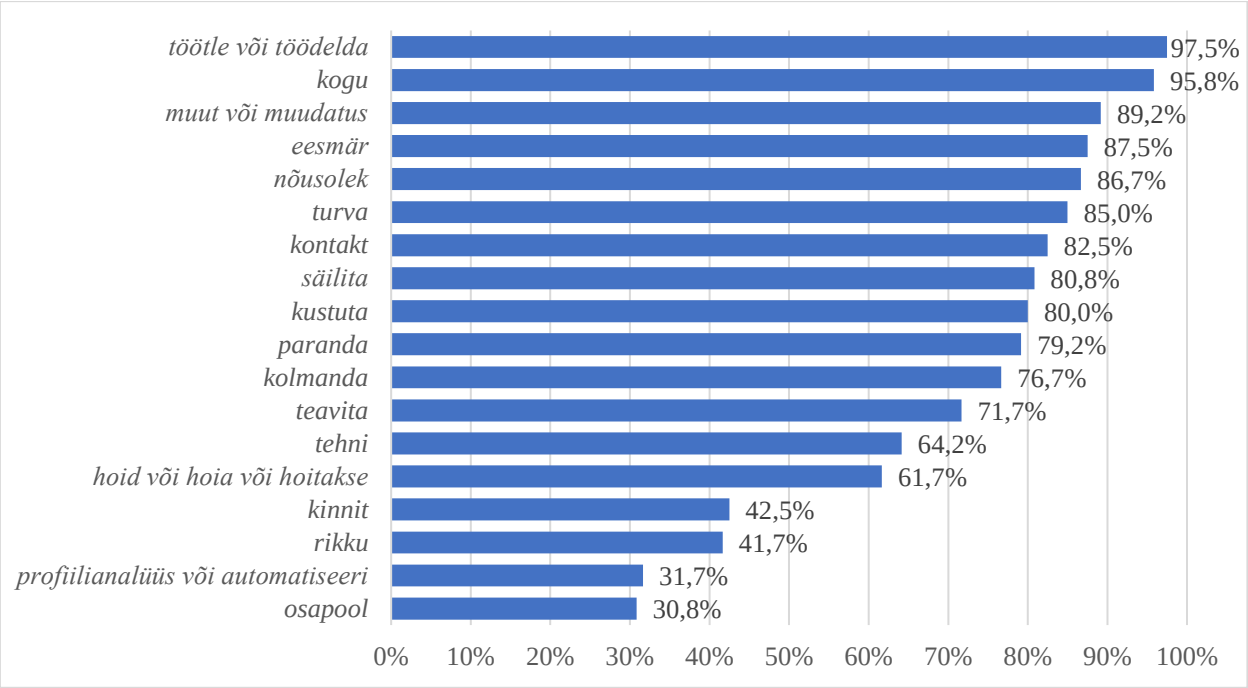
Allikas: autori koostatud

Manuaalne kontroll näitas, et suuremad ebatäpsused tulid ette järgmiste märksõnade puhul:

1. *Kontakt* — mudeli täpsus antud märksõna puhul oli umbes 58%. Andmesubjektilt isikuandmete kogumisel peab vastutav töötleja isikuandmete saamise ajal andmesubjektile teatavaks tegema vastutava töötleja kontaktandmed (EL-i määrus 2016/679 art 13). Manuaalne kontroll näitas, et mõnel juhul oli sõna *kontakt* olemas, kuid vaste oli mingis muus kontekstis. Samas viitas dokument vastutava töötleja andmetele ja kontaktidele, kellega saab andmesubjekt küsimuste korral ühendust võtta. Teisel juhul ei andnud programm sõnale *kontakt* vastet, kuid privaatsuspoliitika sisaldas vastutava töötleja kontaktandmeid. Kuna see märksõna ei andnud oodatud tulemust, eemaldatakse see mudelist.
2. *Hoid/ma* või *hoia/me* või *hoitakse* — mudeli täpsus antud märksõna puhul oli umbes 67%. Autor kasutas märksõna, kontrollimaks 4. aspekti, mis viitas andmete säilitamisele. Märksõna *säilitama* andis manuaalsel kontrollil 100% täpsuse, kuid *hoid/ma, hoia/me* või *hoitakse* olid vasted mitmel juhul mingis muus kontekstis (näiteks *hoiame andmeid turvaliselt või hoiame kursis*). Et märksõna *säilitama* andis mudeli puhul märkimisväärselt suurema usaldatavuse, ei ole mõistlik mudelisse jätta märksõna *hoidma*.
3. *Muut/ma* või *muudatus* — mudeli täpsus antud märksõna puhul oli ligi 67%. Autor kasutas märksõna kontrollimaks 7. aspekti, mis viitas andmete haldamisele andmesubjekti poolt. Märksõnad *muutma* või *muudatus* ei sobi antud mudelisse, sest sõna kasutatakse tihti teises kontekstis (näiteks *muudame privaatsuspoliitika tingimusi*). Kuna märksõnad *kustutama* ja *parandama* andsid mudeli puhul märkimisväärselt suurema usaldatavuse, siis ei ole mõistlik mudelisse jätta märksõna *hoidma*.

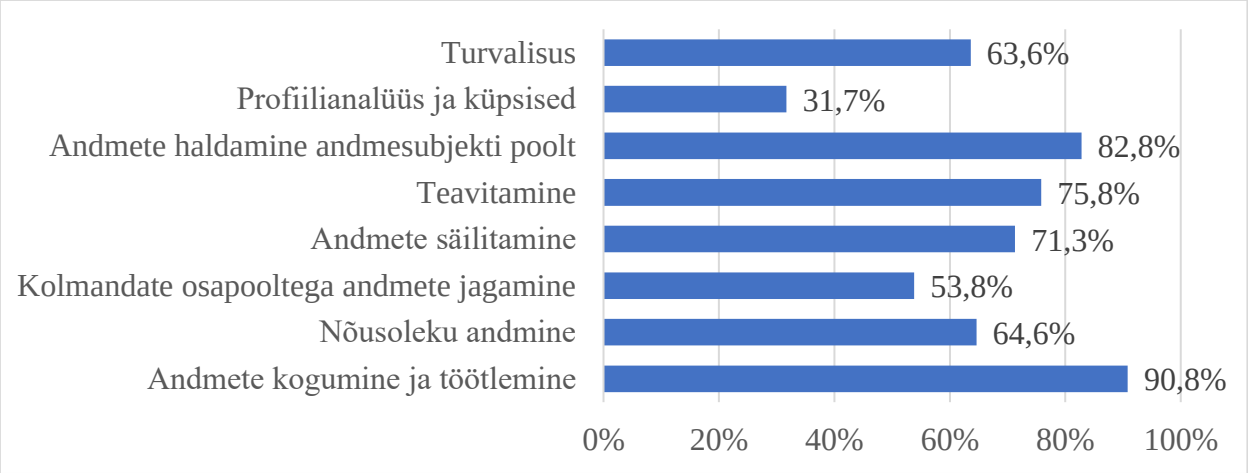
Samuti selgus, et mudel ei tööta selle aspekti puhul, mis puudutab laste turvalisust. Paljud infoühiskonna teenuseid osutavad ettevõtted ei paku teenuseid otse lapsele ning seega ei pea sellised ettevõtted seda punkti ka privaatsuspoliitikasse lisama. Mudel andis otsinguga vaste vaid ligikaudu veerandile privaatsuspoliitikale koguvalimist, mis manuaalsel kontrollil näitas, et vaste oli õige. Mudel töötaks mõne kindla grupi privaatsuspoliitikate puhul, kus on teada, et laste andmeid töödeldakse. Laste isikuandmed väärivad erilist kaitset, kuna lapsed ei pruugi olla piisavalt teadlikud asjaomastest ohtudest, tagajärgedest ja kaitsemeetmetest ning oma õigustest seoses isikuandmete töötlemisega (EL-i määrus 2016/679 põhjenduspunkt 38), seega laste andmete töötlemisel on oluline rakendada erilist tähelepanu nende andmete turvalisusele.

Vaadeldes kogu tulemust vastetele, mis AstroGrep andis (vt lisa 4), siis 69,4% juhtudel andis märksõna programmis vaste ehk kokku leidis AstroGrep vaste 1582-l juhul 2280-st. Kui mudelist on eemaldatud 5. aspekt, mis puudutas laste turvalisust, siis on keskmine vaste protsent 71,4%, mis märksõnade lõikes varieerusid vahemikus 30,8–97,5% (vt joonis 2). Kõige väiksema protsendi vasteid andis märksõna *osapool* (30,8%) ja kõige suurema vaste märksõna *töötle* või *töödelda* (97,5%). Edasises mudeli tulemuste analüüsis eemaldatakse 5. aspekti tulemused, sest mudel ei toiminud selle aspekti puhul nii, nagu oodatud.



Joonis 2. Märksõnade (tüvisõna) vastete osakaal koguvalimist
Allikas: autori koostatud analüüsi tulemuste põhjal (vt lisa 4)

Aspektide kaupa andis mudel järgmised tulemused (vt joonis 3). Enim vasteid andis mudel esimesele andmetöötlustoimingu aspektile, mis puudutas andmete kogumist ja töötlemist (90,8%). Kõige vähem vasteid andis programm 8. aspektile, mis puudutas profiilianalüüsi ja küpsiseid.

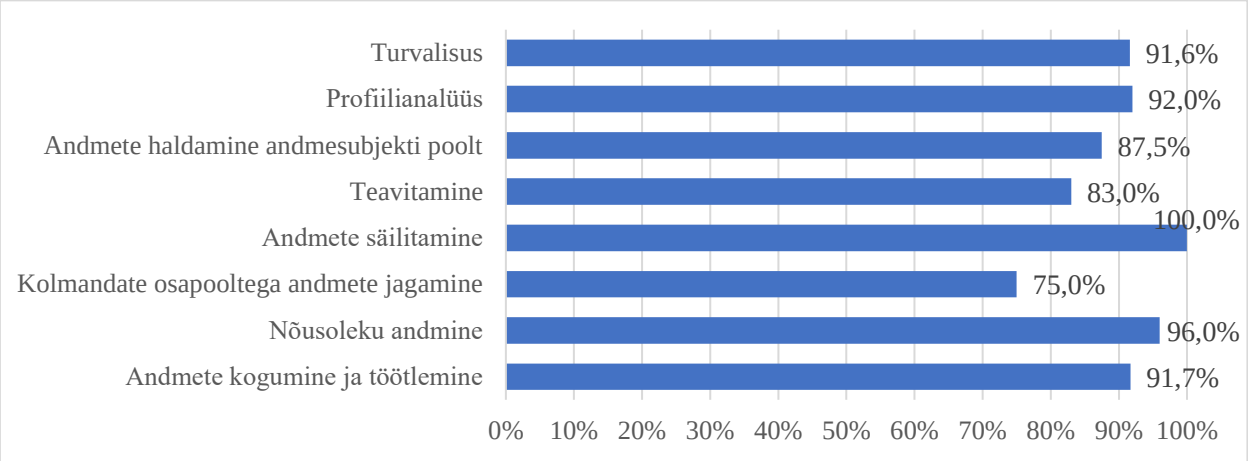


Joonis 3. Märksõnade vastete osakaal koguvalimist aspektide kaupa
Allikas: autori koostatud analüüsi tulemuste põhjal (vt lisa 4)

Järgmiseks tuuakse aspekti kaupa välja, kuidas töötas mudel erinevate andmetöötlus toimingute aspektide kontrollimiseks ja selgitatakse iga aspekti puhul välja mudeli usaldatavus (vt joonis 4).

Need märksõnad, mis manuaalse kontrolli tulemusel saavutasid usaldatavuse alla 70%, eemaldatakse mudelist, et saavutada mudeli efektiivsem toimimine. Tulemused on järgmised:

1. Andmete kogumine ja töötlemine. Esimese aspekti kontrollimiseks kasutati mudelis nelja märksõna, millest, nagu eespool kirjeldatud, üks märksõna ei toiminud — märksõna *kontakt* ei andnud mudelis oodatud tulemust. Ülejäänud kolme märksõna (*koguma, eesmärk,* ning *töötlema*) puhul oli mudeli keskmine täpsus manuaalsel kontrollil 91,7% aspekti kohta. Edasisel analüüsil jäetakse mudelisse esimese aspekti juurde vaid kolm märksõna, sest selliselt on mudel efektiivsem.
2. Nõusoleku andmine. Teise aspekti kontrollimiseks kasutati mudelis kahte märksõna: *nõusolek* ja *kinnitama*. Manuaalne kontroll andis selle aspekti kohta mudelis ligikaudu 96% täpsuse ehk esialgne mudel toimis teise aspekti puhul kõige paremini.
3. Kolmandate osapooltega andmete jagamine. Kolmanda aspekti kontrollimiseks kasutati mudelis kahte märksõna: *kolmandad* ja *osapooled*. Manuaalne kontroll andis selle aspekti kohta mudelis ligikaudu 75% täpsuse. Manuaalselt kontrollil selgus, et mõnel juhul, kus programm ei leidnud märksõnale vastet, oli privaatsustingimustes GDPR-i artiklite 13 ja 14 nõutud info tegelikult olemas, kuid kasutatud oli teisi sõnu (näiteks *teistele isikutele andmete edastamine*).
4. Andmete säilitamine. Neljanda aspekti kontrollimiseks kasutati mudelis kahte märksõna: *säilitama* ja *hoidma*. Nagu eespool kirjeldatud, siis sõna *hoidma* ei andnud manuaalsel kontrollil mudelis oodatud täpsust. Märksõna *säilitama* andis 100% täpsuse ja seetõttu jäetakse edasiseks analüüsiks mudelisse 4. aspekti juurde vaid üks märksõna.
5. Laste turvalisus. Eeltoodud põhjustel jäi see aspekt mudelist välja.
6. Teavitamine. Kuuenda aspekti kontrollimiseks kasutati mudelis ühte märksõna: *teavitama*. Manuaalne kontroll andis sellele aspektile mudelis 83% täpsuse.
7. Andmete haldamine andmesubjekti poolt. Seitsmenda aspekti kontrollimiseks kasutati mudelis kolme märksõna: *kustutama, muutma* või *parandama*. Nagu eespool kirjeldatud, siis manuaalsel kontrollil oli märksõna *muutma* täpsus vaid 58% ja seega jäetakse mudeli efektiivsemaks toimimiseks mudelisse kaks märksõna *kustutama* ja *parandama*. Sellisel juhul on mudeli täpsus 7. aspekti puhul keskmiselt 87,5%.
8. Profiilianalüüs. Kaheksanda aspekti kontrollimiseks kasutati mudelis kahte märksõna: *profiilianalüüs* või *automatiseeritud (otsused).* Mudeli täpsus manuaalsel kontrollil selle aspekti puhul oli umbes 92%.
9. Turvalisus. Üheksanda aspekti kontrollimiseks kasutati mudelis kolme märksõna: *turvaline, rikkuma* ja *tehniline*. Mudeli keskmine täpsus selle aspekti puhul oli ligikaudu 91,6%.



Joonis 4. Mudeli usaldatavus aspekti kohta
Allikas: autori koostatud

Manuaalse kontrolli tulemusel välistati mudeli optimeerimiseks ja maksimaalse efektiivsuse saavutamiseks kokku neli märksõna 19-st, sh üks aspekt, mis puudutas laste turvalisust. Sellisel juhul jäi mudelisse kaheksa aspekti (vt joonis 4) ja kogu mudeli usaldatavuseks saab ligikaudu 89,6%.

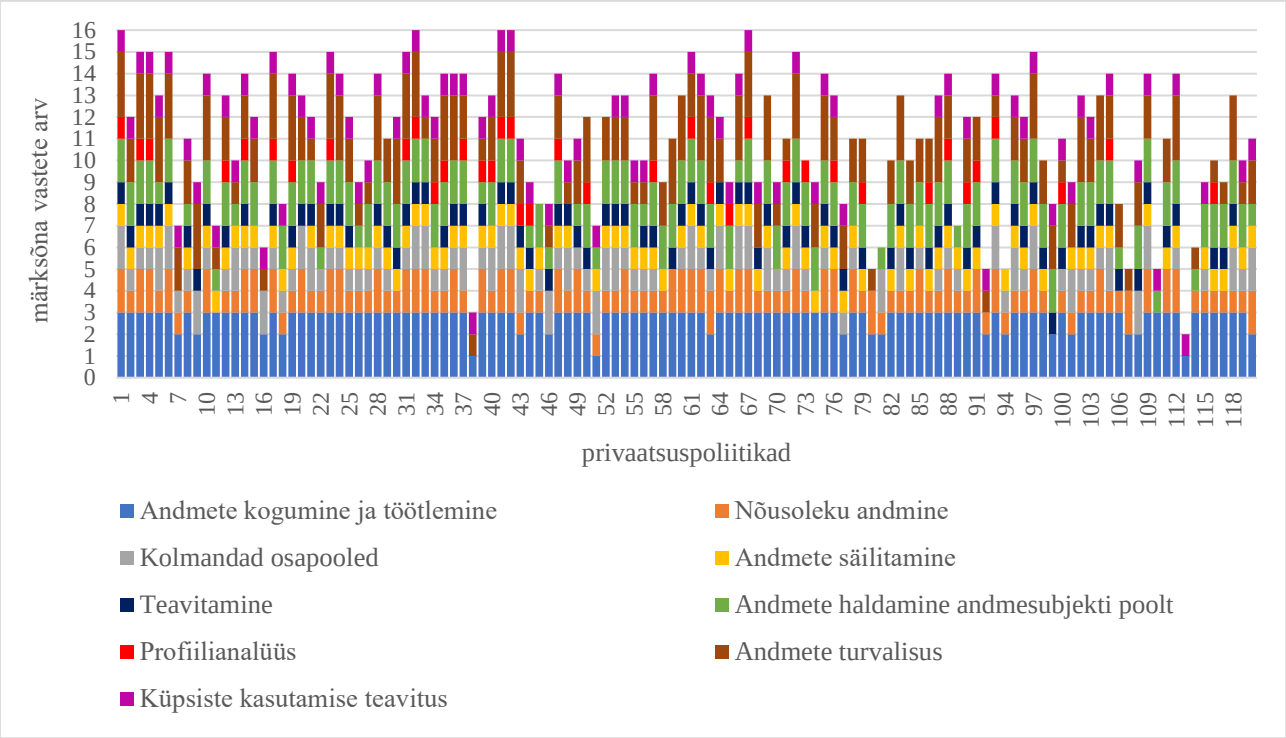
2.3. Analüüsimudeli tulemused

Järgmiseks vaadeldakse mudeli abil tehtud ettevõtete privaatsustingimuste analüüsi tulemusi. Analüüsitakse, milline on privaatsuspoliitikate sisu, kasutades varem optimeeritud mudelit ja programmi AstroGrep tulemusi ning hinnatakse, milline on nende tase:

1. Kas privaatsuspoliitikad sisaldavad määruses nõutud informatsiooni andmetöötlustoimingute kohta?
2. Kas selle mudeli abil on võimalik hinnata, milline on privaatsussätete riskiaste füüsilise isiku jaoks, kui ta kasutab e-kaubanduse ja muude veebiteenuseid osutavate ettevõtete teenuseid?

Joonis 5 peegeldab kõigi 120 privaatsuspoliitika tulemusi programmis AstroGrep. Joonisel on näidatud, mitu vastet iga privaatsuspoliitika sai — need on eristatud andmetöötlustoimingute aspektide kaupa. Näiteks vasakult esimene privaatsuspoliitika sai programmis vaste kõigile märksõnadele. Lisaks on jooniselt võimalik vaadata, et näiteks kui aspekti „andmete kogumine ja töötlemine“ kontrolliti kolme märksõna abil, siis jooniselt on näha, et see aspekt on saanud esimese

privaatsuspoliitika puhul kolm vastet. Lisaks on jooniselt võimalik näha, kui paljud veebilehed, millelt privaatsuspoliitikaid koguti, sisaldavad küpsiste kasutamise teavitusi.



Joonis 5. Privaatsuspoliitikate kontrolli tulemused programmis AstroGrep andmetöötlus-toimingute aspektide kaupa
Allikas: autori koostatud analüüsi tulemuste põhjal (vt lisa 4)

Analüüsil leiti 120 privaatsuspoliitikast viis, millele andis mudel maksimaalse tulemuse ehk programm AstroGrep leidis nende viie privaatsuspoliitika puhul igale otsitavale märksõnale vaste. Neid viit privaatsuspoliitikat loeti ka manuaalselt ja nende sisu oli vastav määruses nõutule: toodud info oli kokkuvõtlik, selge, arusaadav ning kasutatud oli selget ja lihtsat keelt.

Ühe privaatsuspoliitika puhul leidis programm vaste ainult ühele märksõnale. Valimisse ei sattunud ühtegi privaatsuspoliitikat, millele ei oleks programm leidnud mitte ühtegi vastet. Mediaan oli 11 vastet mudelile ehk üle poole privaatsuspoliitikatest sisaldas vähemalt 11 märksõna ning mood oli 13 vastet mudelile ehk 23 privaatsuspoliitikat sisaldasid 13 märksõna.

Kõige rohkem tulemusi andmetöötlustoimingute aspektide lõikes andis esimene aspekt ehk andmete kogumine ja töötlemine. Vähim vasteid andis programm kaheksandale aspektile, mis puudutas profiilianalüüsi ja küpsiste kasutamist.

1. aspekt ehk andmete kogumine ja töötlemine andis programmis 93,6% juhul vaste ning oli ainus aspekt, mis oli kõigis privaatsuspoliitikates mingil määral kajastatud. See tulemus peegeldab seda, et valdav osa vastutavaid töötlejaid kirjeldab oma andmete kogumise ja töötlemise protsesse — nad kajastavad, millistest allikatest ja milliseid isikuandmeid kogutakse ning kuidas nad neid andmeid edasi töötlevad. Valdav osa (88%) privaatsuspoliitikaid kirjeldab ka seda, millistel eesmärkidel andmeid kasutatakse. Mudel andis esimese aspekti tulemustele ligikaudu 91,7% kindluse.

2. aspekt ehk nõusoleku andmine andis programmis 64,6% juhul vaste — 86,7% juhul andis programm vaste märksõnale *nõusolek* ning 42,5% juhul märksõnale *kinnitama*. Aspektile ei leidnud vastet 10 privaatsuspoliitikat. Tulemus peegeldab seda, et valdav osa privaatsuspoliitikaid kirjeldab, kuidas andmesubjekt annab oma nõusoleku isikuandmete töötlemiseks — nõusolek peab olema antud selge kinnitusena. Võib eeldada, et privaatsuspoliitikad selgitavad, millistel tingimustel on võimalik nõusolek tagasi võtta. Mudel andis sellele aspektile 96% kindluse.

3. aspekt ehk kolmandate osapooltega jagamine andis programmis 64,5% juhul vaste. 92 privaatsuspoliitikat 120-st leidsid vaste märksõnale *kolmandad* ja 37 privaatsuspoliitikat leidsid vaste sõnale *osapooled*. Aspektile ei leidnud ühtegi vastet 27 privaatsuspoliitikat. Võib järeldada, et enamik privaatsuspoliitikaid kajastab, kas ja millistel tingimustel ning eesmärkidel nad jagavad andmeid kolmandatele osapooltele, kuid on ettevõtteid, kellel see info puudub. Mudel andis sellele aspektile 75% kindluse.

4. aspekt ehk andmete säilitamine andis programmis 81% juhul vaste. Mudel andis sellele aspektile 100% kindluse. Võib järeldada, et 81% vastutavaid töötlejaid selgitab andmesubjektile, kuidas nende andmeid säilitatakse: milline on isikuandmete säilitamise ajavahemik ja kas nende andmete säilitamiseks kasutatakse turvalisi meetmeid.

6. aspekt ehk teavitamine andis programmis 72% juhul vaste. Mudel andis sellele aspektile 83% kindluse. Võib järeldada, et peaaegu kolmandik privaatsuspoliitikaid ei sisalda infot selle kohta, kas ja kuidas andmesubjekti teavitatakse isikuandmete parandamisest, töötlemisest või mittetöötlemisest.

7. aspekt ehk isikuandmete haldamine andmesubjekti poolt andis programmis 79,6% juhul vaste, millest märksõna *kustutama* ja märksõna *parandama* andsid vaste vastavalt 96-l ja 95-l juhul

120-st. Võib järeldada, et suur osa vaadeldavaid privaatsuspoliitikaid sisaldab infot selle kohta, et kasutajal on võimalik igal ajal oma andmeid ise kustutada, muuta või nende töötlemist piirata. 15 valimisse sattunud privaatsuspoliitikat ei sisaldanud infot selle kohta, et andmesubjektil on õigus oma andmeid parandada või kustutada. Mudel andis 7. aspektile 87,5% kindluse.

8. aspekti ehk profiilianalüüsi ja küpsiste kasutamise puhul oli mudelis vaid märksõna *profiilianalüüs* ja see andis programmis vaste 32% privaatsuspoliitikate puhul. Mudeli kindlus selle aspekti puhul oli ligikaudu 92%. Üksnes ligikaudu neljandik valimisse sattunud andmetöötlejaid tõstis esile, et nad kasutavad isikuandmete töötlemisel profiilianalüüsi ja manuaalne kontroll näitas, et neil juhtudel olid ka enamjaolt toodud eesmärgid, milleks profiilianalüüsi kasutatakse. Küpsiste kasutamise teavitusi kontrolliti eraldi. 89-l veebilehel 120-st oli lehte külastades küpsiste kasutamise teavitus, neist enamik võimaldas isikul ka ise määrata, milliseid küpsiseid kasutaja soovib, et veebileht tema kohta koguks. 11 veebilehel oli kirjas info küpsiste kasutamise kohta kas kuskil valikmenüüs või privaatsuspoliitikas, kuid teavitus ei olnud leitav kohe veebilehele sisenedes. Tegelikult hakkab veebileht küpsiseid kasutama hetkel, kui saidile sisenetakse, kuid see info ei olnud piisavalt nähtav. 20 veebilehel puudus info küpsiste kasutamise kohta — nad ei pruugigi küpsiseid kasutada.

9. aspekt ehk andmete turvalisus andis programmis vaste 63,7% juhul. Enim vasteid sai märksõna *turvaline* — 102 vastet 120-st. Märksõnad *rikkumine* ja *tehniline* andsid vastavalt 50 ja 77 vastet 120-st. Andmete turvalisuse aspektile ei leidnud programm ühtegi vastet 12 privaatsuspoliitikal. Võib järeldada, et suur osa privaatsuspoliitikaid kajastab, et vastutav töötleja on rakendanud isikuandmete kogumisel ja töötlemisel asjakohaseid tehnilisi ja korralduslikke meetmeid eesmärgiga tagada andmete turvalisus. Üheksanda aspekti kindlus oli ligikaudu 91,6%.

Üldiselt on autori hinnangul privaatsuspoliitikate tase hea, kuid olulised on tähelepanekud selle kohta, et valimi koostamisel ei leitud mõnelt veebilehelt üldse informatsiooni andmetöötlustoimingute kohta, kuigi oli selge, et veebileht kogub ja töötleb isikute andmeid (näiteks oli olemas küpsiste kasutamise teavitus). Selliste ettevõtete privaatsuspoliitikad ei jõudnud seega ka valimisse. Privaatsuspoliitikat oli mõnel juhul väga raske ettevõtte kodulehelt leida ja valimi koostamisel ei avanenud kolmel juhul link, mis viitas andmetöötlustoimingute dokumendile. Lisaks on oluline märkida, et suur osa valimisse sattunud veebilehti leiti Eesti E-kaubanduse Liidu kodulehelt, mis tähendab, et tegu on ettevõtetega, kes peaksid olema aktiivsed ja edumeelsed ning soovivad panustada e-kaubanduse arengusse Eestis. Autori hinnangul ei

peegeldanud mõned vaadeldavad privaatsuspoliitikad GDPR-is nõutud andmetöötlustoimingute aspekte, kuid sellised ettevõtted, kes kuuluvad E-kaubanduse Liitu, võiksid olla oma e-kaubandusega seotud tegevustes eeskujulikumad.

Mudel saavutas keskmiselt 89,6% kindluse ja autori hinnangul on see piisav kindlus, et anda selle mudeli abil privaatsuspoliitikatele üldist hinnangut. Mudel võimaldab lihtsustada kasutajatel ettevõtte andmetöötlustoimingutega tutvumist ja nende mõistmist.

Manuaalsel kontrollil loeti läbi mõnikümmend privaatsuspoliitikat ning need erinesid tunduvalt oma sisu, pikkuse ja keelekasutuse poolest. Mahukaim privaatsuspoliitika sisaldas ligikaudu 9000 sõna, seevastu oli kõige lühema privaatsuspoliitika maht alla 100 sõna. Keelekasutuses olid mõned ettevõtted kasutanud küllaltki palju juriidilist teksti, osa seevastu lihtsat ja kohati ka vigast teksti. Autori hinnangul on mõned privaatsuseeskirjad tavakasutajale ebamõistlikult pikad ehk ajakulu nende lugemisele ei ole õigustatud. Lisaks võib juriidiline ja keeruline tekst olla lugejale raskesti mõistetav. Autori arvamust toetab sarnane uuring, kus loeti läbi 150 privaatsuspoliitikat ning hinnati nende pikkust ja loetavust, kasutades programmi, mis mõõdab teksti keerukust lause pikkuse ja sõnakasutuse järgi (Litman-Navarro, 2019). Tulemused näitasid, et valdava osa tekstide lugemiseks kulus väga palju aega ja keerukuse tasemelt nõudsid üle poolte vaadeldavatest tekstidest lugemiseks kõrgharidust (*Ibid.*).

Järgmiseks analüüsitakse, millisel määral on võimalik privaatsuspoliitika sisu järgi defineerida, milline on risk isikule, kui ta edastab oma andmeid privaatsuspoliitika koostanud ettevõttele töötlemiseks.

Mudeli koostamisel sai selgeks, et riskihindamise seisukohalt on mudeli abil väga keeruline eristada suurt, keskmist ja väikest riski. Kindlasti saab võtta seisukoha, et juhul kui füüsiline isik edastab ettevõttele oma andmed töötlemiseks, siis need privaatsuspoliitikad, mis ei sisaldanud mingi aspekti kohta üldse infot, on selle isiku jaoks suure riskiga ettevõtted. Võib eeldada, et ettevõtte ei ole andmete töötlejana oma andmetöötlustoiminguid ootuspäraselt kaardistanud ning tema tegevus pole isikuandmete töötlemisel läbipaistev, seaduslik ja õiglane. Andmeid nimetatud vastutavale töötlejale edastades võib olla füüsilisele isikule risk, et tema andmeid ei hoita turvaliselt ja töötlemisel ei rakendata määruses esitatud nõudeid ning sellega kaasneb isikule mingisugune kahju. Samamoodi saab võtta ka seisukoha, et need privaatsuspoliitikad, mis said mudeli järgi programmis vaste kõigile märksõnadele, kuuluvad ettevõtetele, kes on oma

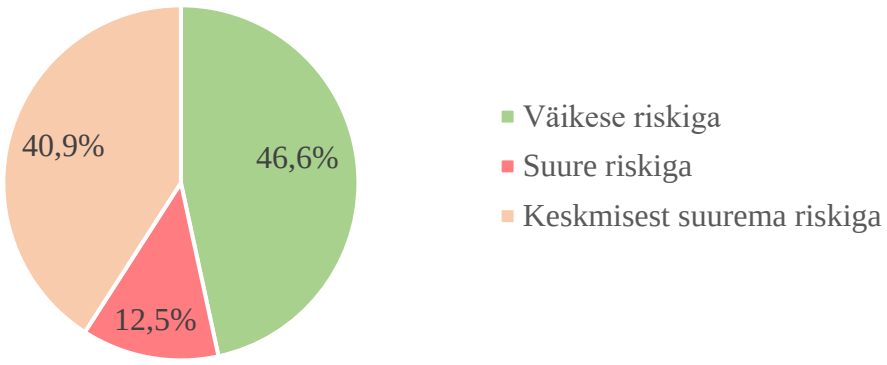
andmetöötlustoimingud piisavalt hästi kaardistanud, et füüsiline isik võiks tunda vaid väikest riski oma andmete edastamisel sellele ettevõttele.

Et selle mudeli järgi oleks võimalik eristada väikest, keskmist ja suurt riski, tuleks võtta kasutusele tunduvalt rohkem märksõnu ja see tähendaks, et mudeli kindlus väheneks. Mudeli kindlus väheneks seetõttu, et mida rohkem märksõnu, seda rohkem kattuksid need märksõnad teiste andmetöötlustoimingute aspektidega ehk märksõnad ei oleks oodatud kontekstis. Seda fakti toetab ka mudeli testimisel tehtud manuaalne kontroll, sest sellel põhjusel eemaldati elemente ka esialgsest mudelist (märksõnad *hoidma* ja *muutma*). Need mudelis kasutatavad märksõnad ei olnud oodatud kontekstis ja seega oleks nende märksõnade mudelisse jätmine vähendanud märkimisväärselt mudeli kindlust.

Eeltoodut arvesse võttes analüüsitakse, kui mitmeid valimisse sattunud privaatsuspoliitikaid võib pidada füüsilise isiku jaoks riskiastmelt suureks, ning mitmeid võib pidada väikese riskiga privaatsuspoliitikaks. Analüüsitakse, millised andmetöötlustoimingute aspektid on kõige vähem kajastatud. Väikese riskiga privaatsuspoliitikateks peetakse neid, mille iga aspekt sai programmis vähemalt ühe vaste.

Väikse riskiga privaatsuspoliitikaks võib pidada eeltoodud kriteeriume arvesse võttes 23 privaatsuspoliitikat 120-st ehk 19,2% koguvalimist. Nendel privaatsuspoliitikatel olid kaetud kõik andmetöötlusaspektid. Lisaks oli veel 33 privaatsuspoliitikat, millel olid kaetud kõik aspektid peale kaheksanda aspekti ehk profiilianalüüsi. Profiilianalüüsi tegemisest tuleb andmesubjekti teavitada üksnes juhul, kui vastutav töötleja viib läbi profiilianalüüsi (EL-i määrus 2016/679 art 13) ja seetõttu võib arvata, et need ettevõtted profiilianalüüsi läbi ei vii. Seega saab liigitada ka need täiendavad 33 privaatsuspoliitikat väikese riskiga privaatsuspoliitikate hulka ehk kokku on väikese riskiga 46,6% privaatsuspoliitikatest (vt joonis 6). Selliseid privaatsuspoliitikaid, millel olid kaetud pooled või vähem kui pooled andmetöötlustoimingute aspektid, oli kokku 15 ehk 12,5% koguvalimist. Need saab liigitada suure riskiga privaatsuspoliitikate hulka. Võib järeldada, et need on ettevõtted, kes ei ole oma andmetöötlustoiminguid kaardistanud ja nõuetega vastavusse viinud, sest olulised andmetöötlustoimingute aspektid on nende privaatsuspoliitikatest puudu. Ülejäänud 49 privaatsuspoliitikas olid kaetud 5–7 andmetöötlustoimingu aspekti 8-st. Ka need privaatsuspoliitikad ei kata kogu informatsiooni, mida vastutav töötleja peab andmesubjektile tema andmeid kogudes ja töödeldes edastama. Mudeli järgi ei ole võimalik neid privaatsuspoliitikaid lahterdada suure või väikese riskiga privaatsuspoliitikate hulka. Need

privaatsuspoliitikad on füüsilise isiku jaoks kindlasti keskmisest suurema riskiga. Eeltoodud tulemusi vaadeldes tuleb arvesse võtta ka seda, et kogu mudeli kindlus oli ligikaudu 89,6%.



Joonis 6. Privaatsuspoliitikate riskitase
Allikas: autori koostatud

Selliste ettevõtete privaatsuspoliitikad, mis ei töötle eriliiki isikuandmeid, peaksid sisaldama kõiki olulisi andmetöötlustoimingu aspekte, mis autor on uurimuses välja toonud. E-kaubanduse ja muid veebiteenuseid osutavad ettevõtted, kes koguvad ja töötlevad isikuandmeid, peavad informeerima andmesubjekti kogu andmetöötlusprotsessi kuuluvast. Punktid, mida ettevõtted ei ole oma privaatsuspoliitikas välja toonud, on ettevõttel tõenäoliselt kaardistamata ja seega puuduvad ettevõttel ka vastavad protsessid. Näiteks kui isik, kes on oma andmed vastutavale töötlejale edastanud, soovib oma andmeid muuta või kustutada, peab tal olema võimalik leida vastavast dokumendist info, kuidas sellist sooviavaldust ettevõttele edastada ning ettevõttel peaks olema läbi mõeldud protsessid, kuidas selles olukorras tegutseda.

Loodud mudel ning manuaalne privaatsuspoliitikate lugemine näitasid, et valimisse sattunud privaatsuspoliitikates oli andmetöötlustoimingutest kõige paremini kajastatud andmete kogumise ja töötlemisega seotud aspekt. Olid välja toodud andmete kogumise põhimõtted ja töötlemise eesmärgid. Kontaktandmed ja info vastutava töötleja kohta oli kergesti leitav. Info selle kohta, mida loetakse isiku nõusolekuks andmete töötlemiseks oli olemas ligikaudu 90% privaatsuspoliitikatest. Samuti oli üldiselt hästi kajastatud seitsmes aspekt ehk andmete haldamine andmesubjekti poolt — privaatsuspoliitikatest oli võimalik välja lugeda, et andmesubjektil on võimalik leida infot, kuidas oma andmeid kustutada, muuta või nende töötlemist piirata. See info oli suuremal või vähemal määral olemas ligikaudu 87,5% privaatsuspoliitikatest. Suur osa ehk

ligikaudu 90% dokumente kinnitasid, et andmetöötleja rakendab isikuandmete kogumisel ja töötlemisel asjakohaseid tehnilisi ja korralduslikke meetmeid, tagamaks andmete turvalisus.

Kõige vähem olid privaatsuspoliitikates kajastatud andmete säilitamise, kolmandate osapooltega jagamise, teavitamise ja profiilianalüüsi aspektid. Andmesubjektile tuleb selgitada isikuandmete säilitamise ajavahemik või selle kriteeriumid. Ligikaudu 81% privaatsuspoliitikatest sisaldas seda infot. Privaatsuspoliitika peaks sisaldama infot, kas andmeid jagatakse kolmandate osapooltega ning kui jah, siis peab andmesubjektile tegema teatavaks, mida peetakse isiku nõusolekuks ja millistel eesmärkidel andmeid edastatakse. Info kolmandate osapooltega jagamisest oli olemas vaid 77% privaatsuspoliitikatest.

Kokkuvõttes saab väita, et koostatud andmetöötlusaspektide ülevaade võimaldab lihtsustada GDPR-i põhimõtete ja eesmärkide mõistmist. Koostatud privaatsuspoliitikate sisu analüüsimudel töötab 89,6% kindlusega ja võimaldab kontrollida privaatsuspoliitikate sisu vastavust isikuandmete kaitse üldmäärusele. See mudel lihtsustab privaatsuspoliitikate lugemist ja nende mõistmist. Koostatud analüüsimudeli abil ei ole võimalik eristada, kas ettevõtte privaatsuspoliitika peegeldab füüsilise isiku jaoks väikest, keskmist või suurt riski oma andmete edastamisel andmetöötlejale, kuid võimaldab mingil määral eristada suurt ja väikest riski ning anda füüsilisel isikul esmane hinnang ettevõttele kui isikuandmete töötlejale.

KOKKUVÕTE

Isikuandmed ja nende kaitse on infotehnoloogia ajastu võimaluste arenedes saanud järjest olulisemaks teemaks, millele pööravad tähelepanu ettevõtted ja eraisikud. Isikuandmete kaitse alast seadusandlust on aastakümnete jooksul oluliselt edasi arendatud ja ühtlustatud Euroopa Liidu tasemel.

25. mail 2018. aastal jõustus isikuandmete kaitse üldmäärus, mis reguleerib füüsilise isiku andmete töötluse igat aspekti ning annab füüsilisele isikule võimaluse saada parem ülevaade sellest, kuidas tema andmeid kogutakse ja töödeldakse. Määrus nõuab, et andmesubjekti teavitatakse tema andmetega tehtavatest andmetöötlustoimingute kokkuvõtlikult, selgelt, arusaadavalt, lihtsasti kättesaadavas vormis ning kasutades selget ja lihtsalt keelt. Vastutavad töötlejad teavitavad andmesubjekte nendest toimingutest läbi privaatsuspoliitika või muu taolise dokumendi.

Ettevõtete kodulehtedelt võib leida väga erineva sisu, pikkuse, keerukuse ja keelekasutusega privaatsuspoliitikaid. Magistritöö eesmärk oli välja selgitada, kas veebiteenuseid osutavate ettevõtete privaatsuspoliitikad vastavad isikuandmete kaitse üldmääruses oodatule ehk sisaldavad vajalike andmetöötlustoimingute aspekte, mis peegeldaksid andmesubjekti kõiki õigusi ja võimalusi. Täiendavalt sooviti välja selgitada, milliseid riske võib füüsilisele isikule tuua see, kui ettevõte ei ole isikuandmete kogumiseks ja töötlemiseks rakendanud piisavaid meetmeid ning kas privaatsuspoliitika sisu võib seostada ettevõtte läbipaistvusega isikuandmete kogumisel ja töötlemisel.

Magistritöös eristati isikuandmete kaitse määrusest üheksat andmetöötlustoimingu aspekti:

1. andmete kogumine ja töötlemine;
2. nõusoleku andmine;
3. kolmandate osapooltega andmete jagamine;
4. andmete säilitamine;

5. laste turvalisus;
6. teavitamine;
7. andmete haldamine andmesubjekti poolt;
8. profiilianalüüs ja küpsised;
9. andmete turvalisus.

Ettevõtete privaatsuspoliitikate kontrollimiseks loodi mudel, mis kontrollis läbi andmetöötlustoimingu aspekte peegeldavate märksõnade nende sisu. Märksõnu otsiti privaatsuspoliitikatest läbi käsuprogrammi AstroGrep, kuhu sisestati valitud märksõnad, misjärel otsis programm neid sõnu valimisse sattunud privaatsuspoliitikatest. Mudeli kindlust kontrolliti manuaalselt. Mudeli kindlus varieerus manuaalse kontrolli tulemusel andmetöötlustoimingute aspektide kaupa vahemikus 75–100%. Keskmiseks mudeli kindluseks sai ligikaudu 89,6%.

Mudeli testimise tulemusena oli võimalik järeldada, et mudel võimaldab kontrollida privaatsuspoliitikate sisu vastavust GDPR-ile ning lihtsustab mahukate ja keerukate privaatsuspoliitikate lugemist ning nende mõistmist. Mudel andis arvestatavad tulemused kõigi märksõnade puhul ja programm leidis vähemalt ühe vaste kõigist valimisse sattunud privaatsuspoliitikatest. Vaadeldavates privaatsuspoliitikates oli enim kajastatud aspekt, mis kirjeldas andmete kogumise ja töötlemise põhimõtteid. Enamasti oli kirjeldatud, mida peab vastutav töötleja andmesubjekti nõusolekuks isikuandmete kogumisel ja töötlemisel ning kuidas on andmesubjektil võimalik oma andmeid hallata: nendega tutvuda, neid muuta või kustutada. Kõige kesisemalt oli privaatsuspoliitikates välja toodud aspekt, mis puudutas andmete edastamist kolmandatele isikutele. Ligikaudu 46,6% valimisse sattunud privaatsuspoliitikatest sisaldas kõiki olulisi andmetöötlustoimingute aspekte. 12,5% dokumentidest olid oluliste puudustega.

Isikuandmete edastamisega vastutavale töötlejale kaasneb füüsilisele isikule risk, et tema andmete kogumisel või töötlemisel tekitatakse talle mingi materiaalne või immateriaalne kahju. Uuriti, kas mudeliga on võimalik määrata seda, kas privaatsuspoliitika sisu peegeldab füüsilisele isikule väikest, keskmist või suurt riski, kui ta otsustab oma andmeid vastavale ettevõttele töötlemiseks edastada.

Selgus, et koostatud mudeli abil ei ole võimalik eristada, kas ettevõtte privaatsuspoliitika peegeldab füüsilisele isikule väikest, keskmist või suurt riski, kui ta edastab oma isikuandmed ettevõttele edasiseks töötlemiseks. Küll aga on mudeli abil võimalik eristada väikest ja suurt riski

— kui privaatsuspoliitika sisaldab kõiki GDPR-is nõutud andmetöötlustoimingute aspekte, siis see näitab, et ettevõte on oma andmetöötlustoimingud kaardistanud ning võib järeldada, et ettevõtte tegevus isikuandmete töötlemisel on läbipaistev, seaduslik ja õiglane. Kui ettevõtte privaatsuspoliitika on puudulik ehk ei sisalda kõiki andmetöötlustoimingute aspekte, võib järeldada, et füüsilisele isikule kaasneb suurem risk, kui ta otsustab oma isikuandmed ettevõttele töötlemiseks edastada. Et mudeliga oleks võimalik määrata selgelt kolme erinevat riskiastet, siis peaks mudelisse lisama palju märksõnu, kuid tõenäoliselt väheneks sellega mudeli kindlus.

Magistritööd võiks edasi arendada järgmiselt:

- Täiendada loodud analüüsimudelit rohkemate märksõnade võrra ja testida, kas mudel töötab.
- Testida mudelit teises keeles, näiteks inglise keeles.

Lisaks võiks samal teemal — privaatsuspoliitikate sisu vastavus isikuandmete kaitse üldmäärusele — uurida edasi järgmist:

- privaatsuspoliitikate vastavus ettevõtete tegelikele andmetöötlustoimingutele või tööprotsessidele ühe või mitme konkreetse ettevõtte näitel.

Kokkuvõtteks võib järeldada, et ettevõtted on GDPR-i nõudeid privaatsuspoliitikates üldiselt kajastanud ja privaatsuspoliitikaid on füüsilistel isikutel kerge leida. Privaatsuspoliitikate tase on väga erinev ja ette tuleb puudulikke dokumente, mis näitab, et mõned ettevõtted ei ole oma andmetöötlustoiminguid piisavalt kaardistanud või määrusega vastavusse viinud. Loodud mudel võimaldaks füüsilisel isikul anda ettevõttele kui isikuandmete töötlejale esmane hinnang selle kohta, kui suur on risk tema isikuandmete edastamisel vastavale ettevõttele.

SUMMARY

COMPLIANCE OF COMPANIES' PRIVACY POLICIES WITH THE GENERAL DATA PROTECTION REGULATION ON THE EXAMPLES OF COMPANIES PROVIDING WEB SERVICES

Kerli Kask

With the development of the possibilities in the information technology era, personal data and the protection of personal data have become an increasingly important topic, to which individuals and companies advert to. Legislation on the protection of personal data has been significantly developed and harmonized in the European Union over decades.

The General Data Protection Regulation entered into force on the 25th of May in 2018. It regulates every aspect in processing personal data and gives the natural person the opportunity to get a better overview of how their data is collected and processed. The Regulation requires that the data subject must be informed of the processing operations that are carried out with their data, in a concise, clear, comprehensible, easily accessible form and in plain and simple language. The data controllers inform data subjects about these actions through a privacy policy or through another similar document.

The privacy policies that can be found on companies' websites vary from different content, length, complexity and the use of language. The aim of the master's thesis was to find out whether the privacy policies of companies, providing web services meet the expectations of the General Data Protection Regulation and whether they include the necessary aspects of the data processing operations that would reflect all rights and possibilities of the data subject. It was further sought out to clarify, what kind of risks a company may pose to a person, if the company has not taken adequate measures when collecting and processing personal data. Furthermore, whether the content of the privacy policy can be related to the company's transparency in collecting and processing personal data.

In the master's thesis, nine aspects of data processing operations from the Personal Data Protection Regulation were brought out:

1. data collection and processing;
2. giving consent;
3. data sharing with third parties;
4. data retention;
5. child safety;
6. providing information;
7. managing data by the data subject;
8. profiling and cookies;
9. data security.

In order to examine the content of the companies' privacy policies, a model was created that checked the content through keywords that reflected the aspects of the data processing operations. The keywords were searched from privacy policies through the Astrogrep command program, where the selected keywords were entered, and the program searched them from the selected privacy policies. The reliability of the model was controlled manually. As a result of manual control, the reliability of the model varied between 75% and 100% for each aspects of data processing operations. The average model accuracy was approximately 89.6%.

As a result of testing the model, it was possible to conclude that the model allows to check the compliance of the content of privacy policy with the GDPR and simplifies the reading and understanding of long and complex privacy policies. The model yielded significant results for all keywords, and the program found at least one match for all the sampled privacy policies. The most important aspect of the observed privacy policies was the description of data collection and processing principles. In most cases, the description included what the controller considers to be the data subject's consent, when collecting and processing personal data and how the data subject can manage their data: access, modify or delete it. The least mentioned aspect of the privacy policies was the transmission of data to third parties. Approximately 46.6% of the sampled privacy policies contained all significant aspects of the data processing operations. 12.5% of the documents had significant deficiencies.

The transmission of personal data to the controller entails a risk for the natural person that the collection or processing of their data will cause them material or immaterial damage. It was examined whether the model could determine if the content of the privacy policy reflects a small, medium or a large risk to an individual, if they decide to transfer their data to the company for processing.

It revealed that the model does not distinguish whether the company's privacy policy reflects a small, medium or a large risk to an individual, when they transfer their personal data to the company for further processing. However, the model can distinguish a small and a large risk - if the privacy policy includes all aspects of the data processing activities required by the GDPR, it shows that the company has mapped its data processing activities and it can be deduced, that the company's data processing is transparent, lawful and fair. If a company's privacy policy is incomplete and does not cover all aspects of data processing operations, it can be infer that the individual is at a larger risk, if they decide to transfer their personal data to the company for processing. In order for the model to clearly identify three different degrees of risk, there should be significantly more keywords added into the model, but this would likely reduce the reliability of the model.

This master's thesis could be further developed as follows:
• The analysis model could be supplemented and tested with more keywords.
• The model could be tested in another language – English for example.

The compliance of the privacy policies with the General Data Protection Regulation could be further explored on the topic:
• Compliances of the privacy policies with the companies' actual data processing operations or work processes on the example of one or more specific companies.

In conclusion, it can be deduced that companies have generally reflected the requirements of the GDPR in their privacy policies and that they are easy to find for individuals. The level of the privacy policies varies widely and there are a lot of incomplete documents indicating that some companies have not sufficiently mapped their data processing activities or brought them into line with the Regulation. The created model would allow a natural person to give a company, as a processor of personal data, an initial assessment of the risk that they take, when transferring their personal data to the company.

KASUTATUD ALLIKAD

AstroGrep programm. (2019). Kättesaadav: http://astrogrep.sourceforge.net/, 25.oktoober 2020.

Albrecht J. P. (2016). How the GDPR Will Change the World. *European Data Protection Law Review*, 2(3), 288-289.

Ali, M. A., Proctor, R. W., Vu, K. L., (2008). Examining the Usability of Web Privacy Policies. *International Journal of Human-Computer Interaction,* 24(3). 307-328.

Anderson, M., Vogels, E. A. (2019). *Americans and Digital Knowledge.* Kättesaadav: https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/, 19. oktoober 2020.

Blackmer, W. S. (2016). *GDPR: Getting Ready for the New EU General Data Protection Regulation.* Kättesaadav: https://web.archive.org/web/20180514111300/https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/, 29. september 2020.

Botterman M., Graux H., Robinson N., Valeri L. (2009). Review of the European Data Protection Directive. *Information Commissioner's Office.* (1-6).

Brandeis L. D., Warren S. D. (1890). The Right to Privacy. *Harvard Law Review*, 4 (5). (193-195).

Breckenridge, A. C. (1970). The Right to Privacy. *U of Nebraska Press.* USA. (1-2).

Chart of signatures and ratifications of Treaty 108. (2020). Council of Europe. Kättesaadav: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=CYmuraq0, 10. september 2020.

Ciriani, S. (2015). The Economic Impact of the European Reform of Data Protection. *Communications & Strategies*. 97. 42-43.

Council of Europe. Euroopa Inimõiguste Konventsioon. Kättesaadav: https://www.echr.coe.int/Documents/Convention_ENG.pdf, 02.september 2020.

Cunningham, J. P., (2002). Are Cookies Hazardous to Your Privacy? *Information Managenent Journal,* 52.

Different types of Internet cookies. Rocket Lawyer. Kättesaadav: https://www.rocketlawyer.com/gb/en/quick-guides/different-types-of-internet-cookies, 03. november 2020.

Eesti Vabariigi põhiseadus. RT 1992, 26, 349.

Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ.

Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679.

Fearn, N. (2018). *Small businesses worryingly unprepared for GDPR, warns Federation of Small Businesses.* Kättesaadav: https://www.computing.co.uk/ctg/news/3027321/small-businesses-worryingly-unprepared-for-gdpr-warns-federation-of-small-businesses, 15. september 2020.

Fuster, G. G., (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Brüssel: Springer. 84-92.

Global digital population as of October 2020. (2020). Statista. Kättesaadav: https://www.statista.com/statistics/617136/digital-population-worldwide/, 20. detsember 2020.

Goldberg, S., Johnson, G., Shriver, S. (2019). *Regulating Privacy Online: The Early Impact of the GDPR on European Web Traffic ja e-commerce Outcomes*. Kättesaadav: https://pdfs.semanticscholar.org/974a/2878b134ac6238b8d18d77d371109a1f6e79.pdf?_ga=2.144348149.1791350371.1605376450-1665413320.1604899827, 29. september 2020.

Hirsch, J. A., Obar, J. A., (2018). The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *Information, Communication & Society* 14.

Inimõiguste ülddeklaratsioon. Välisministeerium. Kättesaadav: https://vm.ee/et/uro-inimoiguste-ulddeklaratsioon, 08. september 2020.

Law and the Rule of Law. (2020). Judicial Learning Center. Kättesaadav: https://judiciallearningcenter.org/law-and-the-rule-of-law/, 08. september 2020.

Liidu liikmed. (2020). Eesti E-kaubanduse Liit. Kättesaadav: https://e-kaubanduseliit.ee/liidu-liikmed, 20. oktoober 2020.

Litman-Navarro, K. (2019). We Read 150 Privacy Policies. They Were an Incomprehensible Disaster. *New York Times.* Kättesaadav: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html, 14. september 2020.

Määrused, direktiivid ja muud õigusaktid. Euroopa Liidu ametlik veebisait. Kättesaadav: https://europa.eu/european-union/law/legal-acts_et, 8. september 2020.

Oxford Learner's Dictionaries. Kättesaadav: https://www.oxfordlearnersdictionaries.com/definition/english/risk_1?q=risk, 27. oktoober 2020.

Rachels, J. (1975). Why Privacy is Important. *Philosophy and Public Affairs, 4 (4)*, 326-327.

ISO/Guide 73:2009, Risk management — Vocabulary. (2009). ISO Guide 73:2009. Kättesaadav: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en, 28. september 2020.

Rubinstein, I. S. (2013). Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law, 3 (2)*, 74-75.

Schwartz, P. M. (2005). Property, Privacy, and Personal Data. *Harvard Law Review, 117 (7)*, 2056.

Solove, J. D. (2008). Conceptualizing Privacy. *California Law Review, 90*, 1102-1107, 1121.

Steinfeld N. (2016) „I Agree to the Terms and Conditions": (How) Do Users Read Privacy Policies Online? *Hebrew University of Jerusalem and Ariel University*

Thirty Years After The OECD Privacy Guidelines (2011). Organisation for Economic Co-operation and Development Kättesaadav: http://www.oecd.org/sti/ieconomy/49710223.pdf, 10-11. 08. september 2020.

Top Sites in Estonia. (2020). Alexa – An Amazon Company. Kättesaadav: https://www.alexa.com/topsites/countries;0/EE, 18. oktoober 2020.

LISAD

Lisa 1. Definitsioonid ja läbivad mõisted

Andmesubjekt – on isik, kelle isikuandmeid töödeldakse. (EL-i määrus 2016/679 artikkel 4)

Isikuandmete töötlemine – on iga isikuandmetega tehtav toiming, sealhulgas isikuandmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, ristkasutamine, ühendamine, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest. (EL-i määrus 2016/679 artikkel 4)

Isikuandmete töötleja – on füüsiline või juriidiline isik, välismaa äriühingu filiaal või riigi- või kohaliku omavalitsuse asutus, kes töötleb või kelle ülesandel töödeldakse isikuandmeid. (EL-i määrus 2016/679 artikkel 4)

Vastutav töötleja – annab volitatud töötlejale kohustuslikke juhiseid isikuandmete töötlemiseks ja vastutab selle eest, et volitatud töötleja täidab isikuandmete töötlemise nõudeid. (EL-i määrus 2016/679 artikkel 4)

Pseudonümiseerimine – isikuandmete töötlemine sellisel viisil, et isikuandmeid ei saa enam täiendavat teavet kasutamata seostada konkreetse andmesubjektiga, tingimusel et sellist täiendavat teavet hoitakse eraldi ja andmete tuvastatud või tuvastatava füüsilise isikuga seostamise vältimise tagamiseks võetakse tehnilisi ja korralduslikke meetmeid. (EL-i määrus 2016/679 artikkel 4)

Profiilianalüüs – igasugune isikuandmete automatiseeritud töötlemine, mis hõlmab isikuandmete kasutamist füüsilise isikuga seotud teatavate isiklike aspektide hindamiseks. (EL-i määrus 2016/679 artikkel 4)

Lisa 2. Andmetöötlustoimingute aspektid ja nende kirjeldused

Aspektid ja nende kirjeldus	Viide
1. Andmete kogumine ja töötlemine Andmeid tuleb koguda ainult kindlaksmääratud ja õiguspärastel eesmärkidel ning neid töödeldakse hiljem vaid nende eesmärkidega kooskõlas oleval viisil. Andmed on asjakohased ja olulised ehk kogutakse võimalikult vähe andmeid, andmeid ajakohastatakse vajadusel ning ebaõiged andmed kustutatakse. Andmete töötlemine on seaduslik juhul, kui andmesubjekt on andnud nõusoleku oma isikuandmeid töödelda, töötlemine on vajalik vastutava töötleja juriidilise kohustuse täitmiseks, isiku eluliste huvide kaitsmiseks või andmesubjektiga sõlmitud lepingu täitmiseks / lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele. Andmete kogumisel ja töötlemisel on oluline edastada andmesubjektile vastutava töötleja kontaktandmed.	Artiklid 5 (1), 6, 9, 10, 11, 13, 14 (1), põhjendus-punktid 39, 44-47, 58
2. Nõusoleku andmine Andmesubjekti nõusolekut oma isikuandmete töötlemiseks peab olema võimalik tõendada, see peab olema antud selge kinnitusena. Nõusolekut peab olema võimalik igal ajal tagasi võtta.	Artiklid 7, 12 (2), 14 (2), põhjendus-punktid 32, 40-43
3. Kolmandate osapooltega andmete jagamine Kui teenusepakkuja kavatseb edastada andmeid kolmandatele osapooltele, siis tuleb andmesubjekti sellest teavitada. Samuti peab andmesubjektile teatavaks tegema, mis eesmärgil andmeid edastatakse.	Artiklid 13 (1), 14 (1), põhjendus-punkt 48
4. Andmete säilitamine Isikuandmeid säilitatakse selliselt, et andmesubjekte on võimalik tuvastada ainult seni, kuni see on vajalik eesmärgi täitmiseks. Andmete säilitamiseks kasutatakse tehnilisi ja korralduslike meetmeid, mis toetavad andmesubjektide õiguste ja vabaduste kaitset. Andmete töötleja peab teavitama andmesubjekti isikuandmete säilitamise ajavahemikust.	Artiklid 5 (1), 13 (2), 14 (2), põhjendus-punkt 39

Lisa 2 järg

5. Laste turvalisus Kui teenust pakutakse otse lapsele, siis on lapse isikuandmete töötlemine seaduslik ainult juhul, kui nõusoleku andnud laps on vähemalt 16-aastane. Muul juhul on lapse isikuandmete töötlemine seaduslik ainult selles ulatuses, mis ulatuses on nõusoleku andnud tema vanem.	Artikkel 8, põhjendus-punkt 38
6. Teavitamine Andmete töötleja peab teavitama andmesubjekti isikuandmete parandamisest, töötlemisest või nende mittetöötlemisest vähemalt ühe kuu jooksul peale andmesubjekti vastavat taotlust. Lisaks peab töötleja teavitama andmesubjekti isikuandmete töötlemise toimingu tegemisest ja selle eesmärkidest.	Artiklid 12 (1,3,4), 13 (1), 19, põhjendus-punktid 60, 61
7. Andmete haldamine andmesubjekti poolt Andmesubjektil on õigus taotleda enda kohta käivate andmete kustutamist, parandamist või andmete töötlemise piiramist. Tal on igal ajal õigus nõuda teavet enda kohta käivate andmete kohta masinloetaval kujul ning edastada neid teisele vastutavale töötlejale. Andmetöötleja peab seadma vaikimisi privaatsussätted või võimaldama andmesubjektil neid sätteid vastavalt soovile reguleerida.	Artiklid 12 (2), 15, 16, 17, 18, 20, 21 (1), 25, põhjendus-punkt 59, 63, 65, 66, 68, 70, 78
8. Profiilianalüüs ja küpsised Andmesubjektil on õigus, et tema kohta ei võetaks üksnes automatiseeritud töötlusel põhinevaid otsuseid. Kasutajal on õigus saada infot, kui tema isikut seostatakse IP-aadresside või küpsistega. Kasutajal on igal ajal õigus keelduda otseturunduse eesmärgil tehtud isikuandmete töötlusest.	Artiklid 21, 22, põhjendus-punktid 28-30, 71, 72
9. Andmete turvalisus Andmete töötleja peab rakendama asjakohaseid tehnilisi ja korralduslike meetmeid andmete turvalisuse tagamiseks. Andmetöötleja on kohustatud teavitama andmesubjekti isikuandmetega seotud rikkumisest.	Artiklid 32, 34

Lisa 3. Valim

1	Google.com	41	Cvkeskus.ee	81	Epood24.ee
2	Delfi.ee	42	Elisa.ee	82	Epp.ee
3	Postimees.ee	43	Euronics.ee	83	Homeemotion.ee
4	Swedbank.ee	44	Geopeitus.ee	84	Noortehnik.ee
5	Wikipedia.org	45	Kutsehariduskeskus.ee	85	Okaidi.ee
6	Facebook.com	46	Uueduudised.ee	86	Heveren.ee
7	Ekool.eu	47	Barbora.ee	87	Collect.net
8	Seb.ee	48	Tele2.ee	88	Paysera.ee
9	Harjuelu.ee	49	Hansapost.ee	89	Grenardi.ee
10	Auto24.ee	50	Teatmik.ee	90	Sparkle.ee
11	Neti.ee	51	Piletilevi.ee	91	S1.ee
12	Err.ee	52	Tartu.ee	92	Eestietno.ee
13	Microsoftonline.com	53	Betsafe.ee	93	Moobliait.ee
14	Ohtuleht.ee	54	Ikea.ee	94	Hth.ee
15	Ut.ee	55	Maanteeamet.ee	95	Fastbaltics.eu
16	Zone.ee	56	Ria.ee	96	Tellimine.ee
17	Kv.ee	57	Omniva.ee	97	Sirvi.eu
18	Eki.ee	58	Astri.ee	98	Dunker.ee
19	Lhv.ee	59	Innove.ee	99	Espresso.ee
20	Yahoo.com	60	K-rauta.ee	100	Aquaphor.com
21	Tallinn.ee	61	Kalkulaator.ee	101	Aeromotors.ee
22	Tootukassa.ee	62	1a.ee	102	Emor.ee
23	Elu24.ee	63	Cooppank.ee	103	Isolta.ee
24	Inforegister.ee	64	Tpilet.ee	104	Recommy.com
25	Mail.ee	65	Onninen.ee	105	Pakendikeskus.ee
26	Rik.ee	66	Harid.ee	106	Hammerjack.eu
27	Mnt.ee	67	Membershop.ee	107	Interbauen.ee
28	Osta.ee	68	Dpd.ee	108	Prindistuudio.ee
29	Opiq.ee	69	Usesoft.ee	109	Azeta.ee
30	Energia.ee	70	Rehvid.com	110	Andbeauty.ee
31	City24.ee	71	Esto.ee	111	Termomeeter.ee
32	Olybet.ee	72	Svea.ee	112	Bigbox.ee
33	Kaup24.ee	73	Taust.ee	113	Pesumati.ee
34	Taltech.ee	74	Cramo.ee	114	Flex.ee
35	E-krediidiinfo.ee	75	K-rauta.ee	115	Lambero.ee
36	Kuldnebors.ee	76	Chilli.ee	116	Klotsipood.ee
37	Aripaev.ee	77	Kupud.ee	117	Maksekeskus.ee
38	Digilugu.ee	78	Bottegaverde.ee	118	Eestijuveel.ee
39	Apollokino.ee	79	Mediron.ee	119	Omaking.ee
40	Kaubamaja.ee	80	Lensexpress.ee	120	Suitsuandur.ee

Lisa 4. Analüüsimudeli tulemused, algandmed

	Aspekt	Andmete kogumine ja töötlemine				Nõusoleku andmine		3. osapooltega jagamine		Andmete säilitamine		Laste turvalisus	Teavitamine	Andmete haldamine andmesubjekti poolt			Profiilianalüüs	Andmete turvalisus		
	Märksõna	kogu	töötle või	eesmär	kontakt	nõusolek	kinnit	kolmanda	osapool	säilita	hoid/ma või	laps või laste	teavita	kustuta	muut või	paranda	profiilianalüüs	turva	rikku	tehni
1	Google.com	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2	Delfi.ee	x	x	x	x	x		x		x	x		x	x	x	x		x		x
3	Postimees.ee	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x
4	Swedbank.ee	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x
5	Wikipedia.org	x	x	x	x	x		x	x	x		x	x		x	x		x	x	x
6	Facebook.com	x	x	x	x	x	x	x	x	x	x		x	x	x	x		x	x	x
7	Ekool.eu	x	x		x	x		x			x				x			x	x	
8	Seb.ee	x	x	x	x	x		x		x	x	x	x		x	x		x	x	
9	Harjuelu.ee	x	x		x			x	x		x		x		x			x	x	x
10	Auto24.ee	x	x	x	x	x	x	x		x	x		x	x	x	x		x	x	x
11	Neti.ee	x	x	x						x	x			x	x			x		
12	Err.ee	x	x	x	x	x		x		x	x	x	x	x	x	x	x	x		x
13	Microsoftonline.com	x	x	x	x	x		x	x	x		x			x	x		x		
14	Ohtuleht.ee	x	x	x	x	x	x	x		x	x		x	x	x	x	x	x		x
15	Ut.ee	x	x	x	x	x	x	x		x				x	x	x		x		x
16	Zone.ee		x	x	x			x	x						x			x		
17	Kv.ee	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x
18	Eki.ee	x	x		x	x		x		x		x		x		x				
19	Lhv.ee	x	x	x	x	x		x		x	x	x	x	x	x	x	x	x	x	x
20	Yahoo.com	x	x	x		x	x	x	x				x	x	x	x		x	x	
21	Tallinn.ee	x	x	x	x	x		x	x	x	x		x	x	x	x		x		
22	Tootukassa.ee	x	x	x	x	x		x				x				x		x	x	
23	Elu24.ee	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x
24	Inforegister.ee	x	x	x	x	x	x	x		x	x		x	x	x	x		x	x	x
25	Mail.ee	x	x	x	x	x		x		x	x		x	x	x	x		x		x
26	Rik.ee	x	x	x	x	x		x		x				x				x		
27	Mnt.ee	x	x	x	x	x		x		x	x	x		x	x	x		x		
28	Osta.ee	x	x	x	x	x	x	x		x	x	x	x	x	x	x		x	x	x
29	Opiq.ee	x	x	x	x		x	x		x	x	x	x	x	x	x		x	x	
30	Energia.ee	x	x	x	x	x				x	x		x	x	x	x		x	x	x
31	City24.ee	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x
32	Olybet.ee	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x
33	Kaup24.ee	x	x	x	x	x	x	x	x	x			x	x	x	x		x		
34	Taltech.ee	x	x	x		x		x		x				x	x	x	x	x		x
35	E-krediidiinfo.ee	x	x	x	x	x		x		x	x		x	x	x	x	x	x	x	x
36	Kuldnebors.ee	x	x	x	x	x	x	x		x	x	x	x	x	x	x		x	x	x
37	Aripaev.ee	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x		x
38	Digilugu.ee	x									x				x			x		
39	Apollokino.ee	x	x	x	x	x	x	x		x	x		x	x	x		x	x		
40	Kaubamaja.ee	x	x	x	x	x		x	x	x	x			x	x	x	x	x		x
41	Cvkeskus.ee	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
42	Elisa.ee	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
43	Euronics.ee	x	x		x	x		x	x	x	x		x		x		x	x		x

Lisa 4 järg

44	Geopeitus.ee	x	x	x		x				x	x		x	x	x		x			
45	Kutsehariduskeskus.ee		x	x	x	x		x		x				x		x				
46	Uueduudised.ee	x	x		x			x	x				x	x				x		
47	Barbora.ee	x	x	x	x	x	x	x		x	x		x	x	x	x	x	x		x
48	Tele2.ee	x	x	x	x	x		x	x	x			x		x			x		
49	Hansapost.ee	x	x	x		x	x	x				x	x	x	x			x		x
50	Teatmik.ee	x	x	x	x	x		x					x	x	x	x	x	x	x	x
51	Piletilevi.ee		x			x		x	x	x				x	x					
52	Tartu.ee	x	x	x	x	x		x	x	x	x		x	x	x	x			x	x
53	Betsafe.ee	x	x	x	x	x		x	x	x	x		x	x	x	x		x	x	
54	Ikea.ee	x	x	x	x	x	x	x		x	x		x	x	x	x		x		x
55	Maanteeamet.ee	x	x	x	x	x		x		x	x	x		x	x	x		x		
56	Ria.ee	x	x	x	x	x		x		x			x		x	x		x		
57	Omniva.ee	x	x	x	x	x		x		x	x		x	x	x	x	x	x	x	x
58	Astri.ee	x	x	x	x	x				x				x	x	x		x	x	
59	Innove.ee	x	x	x	x	x	x						x	x	x	x		x	x	x
60	K-rauta.ee	x	x	x	x	x	x	x		x	x	x	x	x	x	x		x	x	x
61	Kalkulaator.ee	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x		x
62	1a.ee	x	x	x	x	x	x	x		x	x	x	x	x	x	x		x	x	x
63	Cooppank.ee	x		x	x	x	x	x			x		x	x	x	x	x	x	x	x
64	Tpilet.ee	x	x	x		x	x	x	x	x	x	x	x		x			x	x	
65	Onninen.ee	x	x	x	x	x				x	x	x		x		x	x			
66	Harid.ee	x	x	x	x	x	x	x	x	x	x	x	x	x	x			x	x	x
67	Membershop.ee	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
68	Dpd.ee	x	x	x	x	x				x			x		x			x		x
69	Usesoft.ee	x	x	x	x	x		x	x	x	x	x	x	x	x	x		x	x	x
70	Rehvid.com	x	x	x	x	x		x						x		x			x	
71	Esto.ee	x	x	x	x	x		x		x	x		x	x	x	x	x			x
72	Svea.ee	x	x	x	x	x	x	x	x	x	x		x	x	x	x		x	x	x
73	Taust.ee	x	x	x		x		x		x		x	x	x	x	x	x			
74	Cramo.ee	x	x	x						x				x	x	x		x		x
75	K-rauta.ee	x	x	x	x	x	x	x		x	x	x	x	x	x	x		x	x	x
76	Chilli.ee	x	x	x	x	x	x			x	x		x	x	x	x	x	x		x
77	Kupud.ee	x	x		x			x		x			x		x			x		x
78	Bottegaverde.ee	x	x	x		x	x	x		x	x			x	x	x		x		x
79	Mediron.ee	x	x	x	x	x				x	x		x	x	x	x	x	x		x
80	Lensexpress.ee	x	x		x	x	x								x			x		
81	Epood24.ee	x		x		x		x	x					x	x					
82	Epp.ee	x	x	x	x	x				x	x		x	x	x	x		x		x
83	Homeemotion.ee	x	x	x	x	x		x	x	x			x	x	x	x		x	x	x
84	Noortehnik.ee	x	x	x	x	x				x	x		x	x	x	x		x		x
85	Okaidi.ee	x	x	x		x	x	x		x	x			x	x	x		x		x
86	Heveren.ee	x	x	x	x	x				x	x		x	x	x	x	x	x		x
87	Collect.net	x	x	x	x	x		x		x	x	x	x	x	x	x		x	x	x
88	Paysera.ee	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x		x
89	Grenardi.ee	x	x	x		x		x		x					x	x				
90	Sparkle.ee	x	x	x	x	x				x	x		x	x	x	x	x	x		x
91	S1.ee	x	x	x	x	x	x			x	x		x	x	x	x	x	x		x
92	Eestietno.ee	x	x		x		x											x		
93	Moobliait.ee	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x			x
94	Hth.ee		x	x	x		x	x		x	x				x					
95	Fastbaltics.eu	x	x	x	x	x		x	x	x			x	x	x	x		x		x
96	Tellimine.ee	x	x	x		x		x		x			x	x	x	x		x	x	
97	Sirvi.eu	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x
98	Dunker.ee	x	x	x	x	x				x	x		x	x	x	x		x		x
99	Espresso.ee	x	x		x						x		x	x	x	x		x		x

Lisa 4 järg

100	Aquaphor.com	x	x	x	x	x		x			x		x	x	x	x	x	x	
101	Aeromotors.ee	x	x		x	x		x	x	x								x	x	
102	Emor.ee	x	x	x	x	x		x		x	x	x	x	x	x	x		x	x	x
103	Isolta.ee	x	x	x	x		x	x		x		x	x	x	x	x		x		x
104	Recommy.com	x	x	x	x	x	x	x		x	x	x	x	x	x	x		x	x	x
105	Pakendikeskus.ee	x	x	x	x	x		x	x	x	x		x	x	x	x	x	x		x
106	Hammerjack.eu	x	x	x	x	x							x		x	x		x		x
107	Interbauen.ee	x	x		x	x	x											x		
108	Prindistuudio.ee		x	x	x			x	x				x	x	x	x		x		x
109	Azeta.ee	x	x	x	x	x	x	x	x	x		x	x	x	x	x			x	x
110	Andbeauty.ee	x	x	x											x	x				
111	Termomeeter.ee	x	x	x	x	x	x			x		x	x	x		x		x		x
112	Bigbox.ee	x	x	x	x	x	x	x		x	x		x	x	x	x		x	x	x
113	Pesumati.ee		x																	
114	Flex.ee	x	x	x	x		x									x		x		
115	Lambero.ee	x	x	x	x	x		x		x	x	x		x	x	x				
116	Klotsipood.ee	x	x	x	x	x				x			x	x	x	x	x	x		
117	Maksekeskus.ee	x	x	x	x	x				x			x	x	x	x				x
118	Eestijuveel.ee	x	x	x	x	x		x	x	x			x	x	x	x		x	x	x
119	Omaking.ee	x	x	x		x		x		x				x	x	x		x		
120	Suitsuandur.ee	x	x			x	x	x	x	x				x	x			x		x

Lisa 5. Lihtlitsents

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina Kerli Kask

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
Ettevõtete privaatsuspoliitikate vastavus isikuandmete kaitse üldmäärusele veebiteenuseid osutavate ettevõtete näitel, mille juhendaja on Natalie Aleksandra Gurvitš-Suits,

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

1.2 üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli 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.

03.01.2021

[1] *Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil.*