TALLINNA TEHNIKAÜLIKOOL

Tarkvarateaduse instituut

Infotehnoloogia teaduskond

Savva Mirošnikov 178819IABM

ÄRIPROTSESSIDE INVENTUURI JA KASUTATAVATE SÜSTEEMIDE RISKIANALÜÜSI LÄBIVIIMINE GDPR MÄÄRUSE NÕUDE TÄITMISEKS ETTEVÕTTE X NÄITEL

Magistritöö

Juhendaja: Jekaterina Tšukrejeva

MSc

Tallinn 2018

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Savva Mirošnikov

07.05.2018

Annotatsioon

Töö eesmärgiks on läbi viia ettevõtte X äriprotsesside inventuur ning kasutatavate süsteemide riskianalüüs. Selgitatakse välja, millised ettevõttes kasutatavad süsteemid ei vasta hetkel GDPR määruse normidele, et ettevõte X saaks alustada nende süsteemide parandamist ning alates 25. maist 2018 olla vastav GDPR (General Data Protection Regulation, eesti keeles „Isikuandmete kaitse üldmäärus“).

Enda äriprotsesside inventuuri peab läbi viima iga Euroopa Liidu riigis asuv ettevõte, kus töötab rohkem, kui 250 töötajat. Seda nõuab GDPR määruse artikkel nr. 30.

Selleks, et viia läbi äriprotsesside inventuuri, tuli kõigepealt valida kõige sobilikum metoodika. Selle jaoks vaadeldi kõiki teisi võimalikke meetodikaid ning põhjendati tehtud valikut.

Teoreetiline osa on samuti pühendatud sellele, et leida üles kõige sobilikum metoodika kasutatavate süsteemide riskianalüüsi läbiviimiseks. Selle uuringu käigus tuli samuti vaadelda teisi olemasolevaid meetodikaid, valida parim ning põhjendada valikut, tuues välja metoodikate eeliseid ja puudusi.

Kasutatavate süsteemide riskianalüüs peab olema läbi viidud, et saada teada, millised süsteemid ei vasta GDPR määruse normidele ning nõuavad kas tehnilist täiendamist või asendamist teiste süsteemide vastu.

Töö tulemuseks viidi läbi ettevõtte X äriprotsesside inventuur, millega sai GDPR määruse nõue täidetud ning mille käigus koguti infot töödeldavatest isikuandmetest iga äriprotsessi raames, mis annab võimaluse teha edaspidist analüüsi töödeldavate isikuandmete hulga kärpimiseks.

Töö tulemuseks sai samuti läbi viidud ettevõttes X kasutatavate süsteemide riskianalüüs, mis andis ülevaate, et ainult 13 süsteemi 34st vastavad GDPR määruse normidele ning võivad jääda peale 25. maid 2018 töösse. Ülejäänud 21 süsteemi peavad olema kas täiendatud või asendatud.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 67 leheküljel, 8 peatükki, 2 joonist ja 7 tabelit.

Abstract

Carrying Out an Inventory of Business Processes and Conducting a Risk Assessment of Usable Systems in Company X in order to Comply with GDPR Regulation Norms

The goal of this thesis is to conduct an inventory of company X's business processes and the risk analysis of the systems they use. The thesis will give results on which systems do not currently comply with the GDPR (General Data Protection Regulation) norms so company X can start improving these systems in order to be in compliance with the GDPR norms by the 25th of May 2018.

Every company in the European Union that has more than 250 employees needs to conduct an inventory of their business processes. This is required by the GDPR regulation article no. 30.

In order to conduct an inventory of business processes, it is necessary to choose the most appropriate methodology. All possible methodologies were researched for this and the reasons for the end choice were given.

The theoretical part is also devoted to finding the most appropriate methodology to conduct the risk analysis of the systems used. During this study, it was also necessary to research the other methodologies with explaining the pros and cons of each one in order to find the best one and explain the choice.

The risk assessment of the used systems needs to be carried out in order to find out which systems do not comply with the GDPR norms and which ones need technical improvements or replacements by other systems.

The result of the thesis was an inventory of company X's business processes, which filled the necessary requirement for the GDPR and during which data was collected, that

gives information of all the personal data that is processed during every business process, so the amount of data that is processed can be reduced.

The second result of the thesis was a risk assessment of company X's systems, which gave an overview that only 13 of the 34 systems used comply with the GDPR and only these systems can remain in place after the 25th of May 2018. The 21 other systems need to be improved or replaced.

The thesis is written in Estonian and has 67 pages of text, 8 chapters, 2 figures and 7 tables.

Lühendite ja mõistete sõnastik

Ad hoc (ladina keeles)	„väljend, mida kasutatakse tähenduses „kindlaks otstarbeks, selleks korraks või juhtumiks”” [16]
Andmesubjekt	*Data Subject* „füüsiline isik, kes kasutab, on kasutanud või on avaldanud soovi kasutada Vastutava töötleja tooteid või teenuseid ning kelle andmeid isikuandmete töötleja töötleb kooskõlas Isikuandmete töötlemise üldpõhimõtetega” [17]
DPA	*Data Protection Authorities* „Andmekaitseasutused – andmekaitseasutused on sõltumatud riigiasutused, mis jälgivad andmekaitseseaduste täitmist kasutades uurivaid ja korrigeerivaid jõude.” [17]
DPO	*Data Protection Officer* „Andmekaitseametnik – andmekaitseametniku peamine ülesanne on tagada, et isiklik informatsioon, mida tema organisatsiooni protsessides töötajate, klientide, pakkujate või teiste isikute poolt kasutatakse vastaks andmekaitseseadustele.” [18]
EDPB	*European Data Protection Board* (Euroopa andmekaitseamet Ettevõte)
GDPR	*General Data Protection Regulation* (Isikuandmete kaitse üldmäärus)
Isikuandmed	*Personal Data* „igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada” [1]
Isikuandmete töötlemine	*Data Processing* „isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum”[1]
Vastutav töötleja	*Controller* „füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes üksi või koos teistega määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid” [1]
Vastuvõtja	*Recipient* „füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kellele isikuandmed avaldatakse, olenemata sellest,

	kas tegemist on kolmanda isikuga või mitte” [1]
Volitatud töötleja	*Processor* „füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötleja nimel” [1]
WP29	*Article 29 Data Protection Working Party* (Artikli 29 alusel asutatud andmekaitse töörühm) „Töörühm, mis on asutatud direktiivi 95/46/EÜ artikli 29 alusel. Tegemist on Euroopa sõltumatu nõuandeorganiga andmekaitse ja eraelu puutumatuse küsimustes. Töörühma ülesandeid on kirjeldatud direktiivi 95/46/EÜ artiklis 30 ja direktiivi 2002/58/EÜ artiklis 15.” [19]

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

1.1 Taust ja probleem

Vastavalt GDPR määruse artiklile nr. 99, mis jõustus mai 2016, kuid selle kasutuselevõtt algab 25. mail 2018 kui kohustusliku regulatiivse ja juriidilise dokumendina, mida kohaldatakse otseselt Euroopa Liidu liikmesriikides.

Vastavalt GDPR määruse artiklile nr. 30 peavad juriidilised isikud (eriti need, kus töötab rohkem kui 250 inimest) läbi viima äriprotsesside inventuuri, mille käigus iga äriprotsessi kohta peavad olema kogutud sellised kohustuslikud andmed nagu: ettevõtte roll antud äriprotsessis, protsessi omaniku nimi, protsessi eesmärk, juriidiline alus, andmete säilitamisaeg, andmete üleandmise saajad ning nende rollid jne.

Samuti tehakse äriprotsesside inventuuri käigus selgeks, milliseid süsteeme kasutatakse nende äriprotsesside realiseerimikeks. Nende süsteemide vastavus selgub peale riskianalüüsi läbiviimist.

Ettevõte X tegutseb Euroopa Liidu territooriumil ning selles ettevõttes töötab rohkem kui 250 inimest, mistõttu sellel ettevõttel peab kindlasti olema 25. maiks 2018 koostatud kogu vastav dokumentatsioon äriprotsesside inventuuriga (nagu seda nõuab GDPR määruse artikkel nr. 30) ning seega otsustas selle ettevõtte juhtkond tellida ettevõttest Y äriprotesside inventuuri ning kasutatavate süsteemide riskianalüüsi läbiviimise. Lõputöö autor on ettevõtte Y töötaja ning on osa võtnud antud projekti kõikides etappides ärianalüütiku rollis.

1.2 Eesmärk

Töö esimeseks eesmärgiks on viia läbi ettevõtte X äriprotsesside inventuur vastavalt GDPR määruse artiklile nr. 30. Töö teiseks eesmärgiks on viia läbi ettevõttes X kasutatavate süsteemide riskianalüüs ja selle alusel tehakse ettevõtte X juhtkonnale

aruanne, millised kasutatavad süsteemid ei vasta GDPR määruse normidele ning vajavad tehnilist täiendamist või asendamist.

1.3 Metoodika

Viis, kuidas äriprotsesside inventuur peab läbiviidud olema on kirjeldatud GDPR määruses (artikkel nr. 30), läbiviimise metoodikaks otsustas autor valida selline meetod nagu “intervjuu”. Meetodi valimine ning valiku põhjendamine on kirjeldatud antud töös peatükis 3.

Kasutatavate süsteemide riskianalüüsi läbiviimiseks valiti meetodiks "küsimustik", mis oli koostatud audiitorfirma Z abiga ning saadetud ettevõtte võtmeisikutele täitmiseks. Riskianalüüsi tulemused selgitati välja võtmeisikute vastuste põhjal. “Küsimustiku” kui meetodi valimine ning valiku põhjendamine on kirjeldatud antud töös peatükis 4.

1.4 Ülevaade tööst

Esmalt kirjeldatakse magistritöös uue regulatsiooni: üldsätteid, territoriaalset kohaldamisala, kehtivuse algust, põhinõudeid isikuandmete kaitsele ja tihti kasutatavaid definitsioone. Teise peatüki eelviimane punkt tutvustab lugejale seost GDPR määruse ja "Konventsioon üksikisikute kaitseks seoses isikuandmete automaatse töötlemise ja muude isikuandmete kaitse rahvusvaheliste konventsioonidega" ning viimases punktis on välja toodud GDPR määruse õigusaktide rikkumiste puhul määratavate trahvide üldtingimused.

Töö kolmas peatükk on pühendatud ettevõtte X äriprotsesside inventuuri läbiviimise metoodika valimisele. Esmalt tuuakse välja põhinõuded otsitavale metoodikale ning pärast valitakse enim levinud viis metoodika äriprotsesside kaardistamiseks. Samuti räägitakse peatükis kõikide meetodite põhimõtetest ning võrreldakse nende eeliseid ja puudusi. Nendeks meetoditeks valiti: ettevõttes eksisteerivate dokumentide uurimine, intervjuu, vaatlus, küsimustikud ja ankeedid ning tööseminarid. Kolmanda peatüki viimases punktis antakse teada, milline nendest meetoditest välja valiti ning põhjendatakse oma valikut.

Töö neljas peatükk on pühendatud metoodika valimisele ettevõttes X kasutatavate süsteemide riskianalüüsi läbiviimiseks. Antud peatükk on oma struktuurilt sarnane eelmisele peatükile. Alguses kirjeldatakse lühidalt metoodikale sätestatud nõudeid ning hiljem tuuakse välja võimalikud meetodid riskianalüüsi läbiviimiseks. Siis tehakse oma valik ning põhjendatakse kvantitatiivse ja kvalitatiivse meetodi vahel välja valitud kvalitatiivse meetodi valikut, mis omakorda jaguneb veel mitmeks meetodiks: eksperthinnangute meetod, allikate kontrollnimekirjad, reitingute meetod ja analoogi meetod. Autor toob välja kõikide meetodite eelised ja puudused tehes oma valiku eksperthinnangute meetodi kasuks ning samuti põhjendab oma valikut. Lisaks on autor järelduses välja toonud selgituse, et eksperthinnangute meetod jaguneb veel omakorda mitmeks meetodiks: küsimustik, SWOT-analüüs, riskide roos ja spiraal ning Delfi meetod. Järgnevalt kirjeldatakse lühidalt kolme kõige sobilikumat meetodit, milleks on küsimustik, riskide roos ja spiraal ja Delfi meetod, antakse teada, milline nendest meetoditest välja valiti ning põhjendatakse oma valikut.

Viies peatükk on pühendatud äriprotsesside inventuuri käigule ning räägib GDPR määruse nõuetest äriprotsesside inventuuri dokumentatsioonile. Peatüki viimases punktis näitab autor inventuuri käiku ettevõtte X ühe reaalse äriprotsessi näitel.

Kuuendas peatükis demonstreerib autor ettevõtte X kasutatavate süsteemide riskianalüüsi käiku. Siin on välja toodud audiitorfirma Z koostöös loodud küsimustik süsteemide riskihinnangu määramiseks ning riskianalüüs ettevõtte X ühe süsteemi näitel. Peatüki viimases punktis tuuakse välja ettevõtte X süsteemide remediation prioritization heatmap, mis näitab, millised süsteemid vastavad GDPR määruse normidele ning millised kuuluvad ettevõtte X võtmeisikute ja analüütikute ülevaatamisele GDPR määruse normidele vastavuse saavutamiseks.

Töö seitsmendas ehk viimases osas on toodud välja töö järeldused, mis sisaldavad valitud metoodikate hinnanguid ning vajalikke edasisi samme, et ettevõtte X jõuaks vastavusse GDPR määruse normidega.

2 GDPR määrus

2.1 Üldsätted

Kakskümmend aastat tagasi loodi Euroopa Liidus isikuandmete kaitse reguleerimisega seotud direktiiv 95/46/EÜ. Direktiiv on seotud omakorda "Euroopa mudeliga", mis kokkuvõtlikult hõlmab Euroopa Liidu juhtorganite dokumente, andmesubjektide põhiõiguste alusdokumente ja palju muud. Peale selle rakendatakse EL liikmesriikide siseriiklikes õigusaktides. Isikuandmete kaitse dokumentide loomise aluseks on Euroopa Parlamendi ning Euroopa Nõukogu poolt loodud erinevad direktiivid ja määrused. Euroopa Liidu poolt vastu võetud määruste suureks plussiks on see, et neid on võimalik tööle rakendada liikmesriikides ilma siseriikliku õiguse rakendamiseta. [1]

2016-nda aasta 27. aprillil EP ja EN vastu võetud direktiivi 95/46/EÜ kehtetuks tunnistamine tekitas aluse luua (EL) nr 2016/679 määrus - "füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta" (edaspidi – GDPR määrus). [1]

Antud määruse sisuks on mõjutada ELi liikmesriikide õigusloome ja selle täitmise taset, ühtlustada isikuandmete vaba liikumise liikmesriikide vahel kui samas ka põhiõiguste ja -vabaduste kaitset andmetöötluse osas. Oluline on see, et liikmesriigid on kohustatud järgima GDPR määrust ning ühtlustama seda kohaliku õigusega, vajadusel kohaliku õigust muutes või täiustades. [1]

Peale selle juhinduvad liikmesriikide kohtud otseselt GDPR määrusest ning samuti on ühtlustatud ka antud määruse rikkumise karistamine kõigis liikmesriikides. Antud määrust rakendab Euroopa Kohus. [1]

2.2 GDPR määruse kehtivuse algus, põhinõuded isikute andmete kaitsele ning territoriaalne kohaldamisala

GDPR määrus võetakse kasutusele 25. mail 2018 aastal kohustusliku regulatiivse ning juriidilise dokumendina. Selle määruse põhilised nõuded ja sätted on kirja pandud 173 punkti ja 99 artiklina. [1]

Määruse põhilisteks eesmärkideks on kirjeldada põhimõtteid, eeskirju kuidas peaks isikuandmeid Euroopa Liidus töötlema, kuidas peaks olema tagatud nende vaba liikumine nii riigi sees kui ka riikide vahel. [1]

Antud määrus kirjeldab isikuandmeid kui andmeid, mis peaksid olema käsitletud seaduslikult, õiglaselt ja läbipaistvalt. Neid peab koguma kindlate seaduslike eesmärkide jaoks. Kusjuures tegevused nagu arhiveerimine, säilitamine üldistes huvides, kasutamine teaduslikes ja ajaloolistes uuringutes või statistika korjamises ei lähe vastuollu antud punktiga. Peale selle peavad andmed olema töödeldud nõudekohaselt ning piirduma vastavalt seatud eesmärkidega milleks antud andmeid korjatakse. Samuti peavad andmed olema täpsed, ajakohased. Vastavalt eesmärkidele tuleks andmeid parandada või eemaldada. Andmed peavad olema salvestatud kujul ja andmesubjekti peab saama tuvastada nii kaua kuni andme kogumise eesmärgid on rahuldatud. Lisaks, peavad andmed olema töödeldud viisil, et oleks tagatud nõuetekohane säilitamine, kaitse loata või ebaseadusliku töötlemise, juhusliku kadumise, ära kustutamise või muude kahjustuste eest. [1]

Samuti on seatud nõuded ja tingimused andmete õiguspärasuse kaitseks. Eelkõige peab andmesubjekt olema andnud nõusoleku andmete töötlemiseks kindla eesmärgi nimel. Peale selle on töötlemine vajalik lepingu täitmiseks, mille osapooleks on andmesubjekt või andmesubjekti lepingu täitmise tagamiseks. Lisaks võib töötlemine olla vajalik töötleja kohustuste täitmiseks, üldiseid huve teenides, andmesubjekti või kellegi teise eluliste huvide kaitsmiseks. Samuti töötleja või kolmanda isiku õigustatud huvi korral ning seaduslikel eesmärkidel. [1]

Nagu eelnevalt mainitud asendab ning ühtlasi muudab kehtetuks GDPR 1995 aasta direktiivi 95/46/EÜ. Vana dokumendi kohaselt moodustati WP29 (Article 29 Data

Protection Working Party, eesti keeles Artikli 29 alusel asutatud andmekaitse töörühm), mille eesmärgiks oli kaitsta üksikisikuid. [2]

Hetkel on WP29 osalenud aktiivselt uue GDPR määruse väljatöötamisel. [3]

WP29 töö lõpeb koos antud direktiivi lõppemisega ning selle asemel asutatakse EL uus asutus – Euroopa andmekaitseamet (European Data Protection Board, lühidalt EDPB), mis on asutatud vastavalt GDPR määruse eeskirjadele. Euroopa andmekaitseametit juhib Euroopa andmekaitse talituse juht ning antud organisatsioonis töötavad liikmesriikide andmekaitseasutuste kõrgemad esindajad (Data Protection Authorities, lühidalt DPA). [1]

GDPR määruses on sätestatud, et isikuandmete töötlemist teevad "vastutav töötleja" või "volitatud töötleja". Vastutav töötleja on kohustatud mõningal juhul koos töötama andmetöötlejatega, pidama arvestust, töötlemisekäigus hindama andmesubjektide õigustele avalduvat mõju, rakendama andmekaitse mehhanisme. Samuti tuleb andmete kogumise ajal teadvustada andmesubjekti antud tegevustest ning tema õigustest. [1]

Andmete lekke tuvastamisel tuleb teavitada siseriiklikke andmekaitseasutusi (DPA) 72 tunni jooksul. [1]

Volitatud töötleja kohustuste hulka kuulub isikuandmete töötlemise toimugu registri pidamine, mis on täidetud iga vastutava töötleja nimel. Samuti peab töötleja määrama esindaja, kui tal ei ole esindajat Euroopa Liidus. Lisaks tuleb tegeleda piiriüleste andmeedastustega ning andmelekke korral koheselt teatama vastutavat töötlejat. [1]

Samuti on määruses välja toodud, et vastutavad ja volitatud töötlejad on kohustatud määrama andmekaitseinspektori (Data protection Officer, lühidalt DPO). DPO on kohustuslik määrata juhul kui andmetöötlust teostab riigiasutus, kui töödeldakse eriteabe andmeid või kui töötlejate põhitegevus on seotud sellise andmetöötlusega, mis nõuab teatud liiki järelevalvet. [1]

Füüsiliste isikute kaitseks tuleb antud määrust kasutada liidust väljapool olevatel vastutavatel ja volitatud töötlejatel liidus olevate andmesubjektide isikuandmeid töödeldes kahel juhul. Esiteks, kui andmete töötlemine on seotud kaupade või teenuste pakkumisega andmesubjektile olenemata makse olemasolust. [1]

Teiseks, kui isikuandmete töötlemise toimingud toimivad vastutava töötleja või volitatud töötleja poolt Euroopa Liidu sees. [1]

2.3 Seos GDPR määruse ja „Konventsioon üksikisikute kaitseks seoses isikuandmete automaatse töötlemise“ ja muude isikuandmete kaitse rahvusvaheliste konventsioonidega

Nagu paljud teised Euroopa Liidu määrused on samuti GDPR kooskõlastatud paljude õigusaktide ning dokumentidega. Nende hulka kuuluvad Euroopa Liidu põhiõiguste harta, Euroopa Nõukogu 28. jaanuari 1981. aasta isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon ja selle lisaprotokoll, Euroopa inimõiguste ja põhivabaduste kaitse konventsioon, Genfi konventsioonid relvastatud konflikti ajal kohaldatava rahvusvahelise humanitaarõiguse järgimise kohta ning samuti Euroopa Liidu liikmesriikide olemasolevad lepingud vastastikuse õigusabi ja õigussuhete kohta tsiviil-, perekonna- ja kriminaalasjades. [1]

Piiriüleste andmeedastustega tegeledes on GDPR määruses välja toodud punktid, mis seavad reeglid kolmandatele riikidele ja rahvusvahelistele organisatsioonidele. Näiteks on kirjeldatud kolmanda riigi ühinemine 28. jaanuari 1981. aasta Euroopa Nõukogu konventsiooniga üksikisikute kaitse kohta isikuandmete automatiseeritud töötlemisel ja lisaprotokolliga või näiteks on kirjeldatud rahvusvahelise organisatsiooni osalemist nii piirkondlikes kui ka mitmepoolsetes süsteemides, mis on seotud isikuandmete kaitsega. Euroopa Komisjon vaatab, et kohustused oleksid järgitud rahvusvaheliste organisatsioonide ja kolmandate riikide poolt. [1]

2.4 Trahvide määramise üldtingimused

Antud õigusaktide rikkumise ees on GDPR määruses sätestatud mitmestasandilised sanktsioonid. Trahve määravad DPA. Trahvid on rahalised ning ulatuvad kuni 4% organisatsiooni aastakäibeni või 20 miljoni euroni. Teise rikkumise korral määratakse väikse rahatrahv, mis võib olla 2% aastasest käibes või 10 miljonit eurot. Trahv võetakse alati suuremast summast olgu selleks protsent või fikseeritud rahaline summa. Protsendiline trahv määratakse ettevõtetele, antud mõiste on kirjeldatud Euroopa Liidu

toimimise lepingu artiklis 101 ja 102. Peale selle sisaldab tekst asjaolusid miks määrati antud trahv (rikkumise laad, raskusaste ja kestus). [1]

3 Äriprotsesside inventuuri ning riskianalüüsi läbiviimiseks meetodite valimine

3.1 Nõuded metoodikale

Kuna ettevõtte Y (teenusepakkuja ning autori tööandja) omab limiteeritud hulka ärianalüütikuid, kes on valmis teostama antud projekti ja ettevõttel X (klient) on filiaalid kahes eri EL riigis ning kogu projekti teostamiseks (ehk äriprotsesside inventuuri ning kasutatavate süsteemide riskianalüüsi läbiviimiseks) on piiratud hulk aega, siis sellega seoses on äriprotsesside inventuuri läbiviimise metoodikale rida nõudeid.

Milleks on:

1. Kaugtöö võimalus
   Metoodika peab võimaldama viima läbi inventuuri eemalt. Kuna äriprotsesside hulk igas filiaalis on üle neljasaja, siis valitud metoodika ei pea eeldama ettevõtte Y ärianalüütikute pidevat kohalviibimist.
2. Valdkonna igapäevase töö minimaalne katkestamine (kliendi rahulolu)
   Projekti teostamisel peab kliendi (antud juhul äriprotsesside omanikud ning osalejad) töö häirimine olema minimaalne. Kokkupuude äriprotsesside omanikuga tema äriprotsesside inventuuri raames peab olema ühekordne ning samuti ei pea oma igapäevast tööd katkestama ka teised osalejad antud äriprotsessis.
3. Kiirus
   Metoodika peab võimaldama saavutada töö tulemusi maksimaalse kiirusega, kuna projekti teostamiseks aeg on piiratud. Praktikas see tähendab seda, et nii ärianalüütikute töö kui ka äriprotsesside omanike (kui nende osalus on vajalik) töö peab olema ratsionaalne ja optimeeritud.
4. Maksimaalse kvaliteedi saavutamine
   Valitud metoodika peab samuti võimaldama saavutada ettevõtte Y pakutava teenuse maksimaalse kvaliteedi. See tähendab seda, et läbiviidud inventuuris on kaetud kõik

äriprotsessid, kus töödeldakse isiklikke andmeid ning nende äriprotsesside kirjeldus on piisavalt detailne.

3.2 Äriprotsesside kaardistamiseks enamlevinud meetodid ning nende eelised ja puudused

Äriprotsesside kirjelduse kvaliteet sõltub otseselt infost, mis saadakse organisatsiooni uurides ning rakendades erinevaid meetodeid ja võtteid, et saada kvaliteetset, asjakohast ja tõetruud äriteavet. [4]

Teavet saadakse erinevatest allikatest, näiteks suhtlemine juhtidega ja personaliga, dokumentide uurimisega jne. Tundub nagu kõik oleks väga lihtne: uurida dokumente, korraldada intervjuusid juhtide ja töötajatega ning seeläbi saada täielik ülevaade ettevõtte tegevustest, kõikidest organisatsioonisisestest ja -välistest protsessidest ning ettevõtte töötajate/ osakondade/ üksuste vahelistest suhtlemise viisidest. Kuid tegelikult ei ole kõik nii lihtne nagu võib tunduda esmapilgul. Ettevõtte ja selle peamiste protsesside teabe kogumisel esineb piisaval hulgal probleeme, mis võivad negatiivselt mõjutada saadud teabe kvaliteeti ja asjakohasust ning seega ka uuringu lõpptulemust. [4]

Äriprotsesside kirjelduse töö tõhususe parandamiseks peab valima olemasolevate tegevuste kohta õiged meetodid ja teabeallikad. Peamised kogumise viisid ja teabeallikad on järgmised:

1. vaatlus;
2. küsimustikud ja ankeedid;
3. ettevõttes olemas olev dokumentatsioon;
4. intervjuud;
5. tööseminarid. [4]

3.2.1 Vaatluse meetod

Vaatlus on üks meetodeid teabe kogumiseks äriprotsesside kirjeldamiseks. See on rohkem abimeetod, seda kasutatakse peamiste protsesside kohta teabe kogumiseks ja ekspertide küsitluste käigus saadud teabe kontrollimiseks. Vaatlust teostab analüütik

ning saadud teave on peamiselt protsessi teostamise loogika ja kvantitatiivsed andmed protsessi täitmisele kulutatud aja jooksul. [20]

Selle meetodi peamised puudused on järgmised:

1. suured ajakulud;
2. moonutatud teave saamine, st. kui analüütik vaatleb otseselt protsessi, muutub töötajate igapäevane käitumine ja see võib muuta protsessi loogikat ning protsesside ja funktsioonide parameetreid.

Teisest punktist loeme välja järgnevat: töötajad hakkavad vaatleja juuresolekul paremini töötama, mis suurendab nende tootlikkust. Seetõttu peab analüütik selliseid muutusi töötajate käitumises nägema ja arvesse võtma, vastasel juhul on saadud andmed mitteobjektiivsed. [20]

Tänapäeval kasutatakse seda meetodit harva, kuna see põhjustab töötajate ärritust, mistõttu enamik ettevõtteid ka seda ei kasuta. Ainus, mida nad analüütikule lubada saavad on ringkäiku ettevõttes. Ettevõte X ei ole erandiks. Seda teabe kogumise meetodit ei saa mitte mingil juhul käsitleda äriprotsesside inventuuri läbiviimise korral vastavalt GDPR määruse kohandamise artiklile 30. Esiteks tähendaks see väidetavat nõusolekut analüütiku poolt ettevõtte X klientide ja töötajate isikuandmete töötlemiseks ning samuti nõuaks see ettevõtte Y tohutut aja- ja inimressursside hulka, eesmärgiga jälgida ja dokumenteerida kõiki äriprotsesse, mida ettevõttes X, võttes arvesse ka teises riigis asuvat filiaali, on kokku rohkem kui kaheksasada.

Järeldus „vaatluse meetodi“ kohta

Võttes arvesse eelneva info võime järeldada, et „vaatlus meetod“ eeldab kohalolemist, seega esimesele nõudele ta ei vasta.

Teisele nõudele vastab antud meetod poolenisti. Ühelt poolt ta ei nõua äriprotsessi inventuuris osalejate otsest osalemist ning nende igapäevatöö katkestamist, teisalt aga võivad protsessi osalejad võtta seda erinevalt, kedagi võib kolmanda isiku poolne vaatlus häirida ja ärritada.

Kolmandale nõudele “vaatluse meetod“ ei vasta üldse, kuna nõuab väga suurt hulka aega ning teeb projekti realiseerimise ebareaalseks.

Neljandale nõudele vastab see meetod samuti poolenisti, sest ühelt poolt annab ta analüütikule protsessi täisvaate, aga teiselt poolt võib juhtuda see, et protsessi osalejate käitumine võib kolmanda isiku pideva vaatluse tõttu muutuda ning see muudaks kogu protsessi loogikat.

Metoodika hinne: 1/4.

3.2.2 Küsimustikud ja ankeedid

Teiseks potentsiaalseks teabe kogumise meetodiks on ankeetimine. Küsimustike ja ankeetide abil on võimalik kogu ettevõtte info kokku koguda massiliselt ja kiiresti. Kuid teabe kvaliteet jääb antud olukorras madalaks, kuna ankeedid ja küsimustikud annavad edasi ainult pinnapealset infot. Selle meetodi veel üheks puuduseks on samuti asjaolu, et vastajad suhtuvad vastamisse formaalselt. Pärast tulemuste saamist peab analüütik individuaalselt kohtuma küsitletud töötajatega ja täpsustama saadud teavet, et viimistleda küsimustikke ja ankeete. [21]

Peamised küsimused liigitatakse tüüpide kaupa järgmistesse kategooriatesse: avatud, suletud ja “vastuste lehvikuga”. Avatud küsimustele saab vastata suvalises vormis. Suletud küsimustele saab vastusteks anda: "jah", "ei", "ma ei tea". Vastuste lehvikuga küsimustele saab vastata ekspertide poolt välja toodud vastuste variantidega. Avatud küsimusi on soovitatav kasutada probleemi suure ebakindluse korral. Seda tüüpi küsimused võimaldavad meil ulatuslikult käsitleda kõnealust probleemi, et määratleda ekspertide arvamuste spektrid. [21]

Sellega seoses ilmnevad küsitlemise käigus järgmised probleemid:

1. küsimuste sõnastuse keerukus, kuna kvalitatiivse küsimustiku koostamiseks tuleb selgelt mõista organisatsiooni tegevust;
2. suure hulga küsimustike töötlemine, eriti küsimustikud, mis sisaldavad avatud küsimusi.

Seetõttu kasutatakse ankeetimise meetodit peamiselt muude meetodite abil saadud uuringutulemuste kontrollimiseks. [21]

Järeldus „küsimustike ja ankeetide meetodi“ kohta

Antud meetod võimaldab vabalt teha kaugtööd ja seega vastab esimesele nõudele.

„Küsimustike ja ankeetide meetod“ ei vasta teisele nõudele. Küsimustikus toodud küsimustele iseseisev vastamine (eriti avatud küsimustele) võtab äriprotsessi omanikul palju aega ning see viis ei taga, et vastajale meenuvad olulised asjad oma äriprotsessi kaardistades, sest ta võib neid pidada ebaolulisteks.

Samas vastab meetod suurepäraselt kolmandale nõudele, kuna säästab ettevõtte Y ärianalüütikute suurt hulka aega. Antud metoodikat rakendades jääb analüütikute ainsaks ülesandeks valmistada ette küsimustiku, milliste küsimuste vastused kataksid äriprotsesside kõiki nüansse.

Neljandale nõudele kahjuks see meetod ei vasta, kuna eksisteerib võimalus, et mõned vastajad ei võta seda protsessi tõsiselt ning ei kaardista oma äriprotsesse niivõrd detailselt nagu seda peaks tegema, või isegi tõsise suhtumisega, võivad protsessi tähtsamad nüansid jääda mainimata kuna neid peetakse ebaolulisteks.

Metoodika hinne: 2/4.

3.2.3 Ettevõttes eksisteerivate dokumentide uurimine

Üheks ettevõtte äriprotsesside teabeallikaks on dokumendid. Enamikul ettevõtetel on olemas dokumendid, mis reguleerivad nende tegevust: äriprotsesside määrused, allüksuste määrused ja ametijuhendid. Juhul kui reglemendid on vananenud ja ka fragmentaarsed, on siiski soovitatav need kokku koguda. Paljud äriprotsesside elemendid on arusaadavad, kui vaadelda ettevõtte dokumente ja aruandeid. Enne äriprotsesside kirjelduse tööd tuleks kõik need loetletud dokumendid kokku koguda, struktureerida ja tulevikus kasutada kui üht teabeallikatest. [5]

Teabe saamise meetodite rakendamisel ettevõtte dokumentide läbivaatamisel võivad tekkida järgmised raskused:

1. suur hulk dokumente;
2. dokumendid võivad kaotada oma asjakohasuse;
3. puudulik dokumentide pidamine ehk „tüklik dokumentatsioon“. [5]

Töötamisel dokumentidega tuleks järgida järgmist soovitust:

Kindlasti peab uurima ettevõtte dokumente. Peab proovima seda teha enne küsitlusi ja intervjueerimisi, sest vastasel juhul hakkab äriprotsessi omanik küsimustele vastama viidates nendele dokumentidele. Kui analüütikul puudub ülevaade, millest räägitakse dokumendis, tuleks tal see läbi lugeda ja siis tekivad tal lisaküsimused. Kui analüütik ise, vesteldes äriprotsessi omanikuga, viitab nendele dokumentidele, ning samuti loob küsimusi nende põhjal, siis see fakt muudab arvamust tema kohta paremaks äriprotsessi omaniku silmis (antud juhul kliendiettevõtte esindaja), näidates, et ta on kohtumiseks valmistunud rõhutades sellega oma professionaalset lähenemist.

Järeldus „ettevõttes eksisteerivate dokumentide uurimise meetodi“ kohta

Antud meetod vastab hästi esimesele ning teisele kriteeriumitele, kuna võimaldab ärianalüütikutel teha kaugtööd ning peaaegu ei nõua ettevõtte X töötajate abi, kuid ei vasta absoluutselt „kiiruse“ kriteeriumile, kuna nõuab hiidmahulist analüütikute tööd ning järgides seda meetodit ei jõua analüütikute rühm oma töö õigeks ajaks ära teha.

Samuti vastab antud meetod neljandale kriteeriumile, aga vaid osaliselt, kuna dokumentatsioon võib aeguda ning ettevõte X elas üle just liitumise teise ettevõttega, seega enamus äriprotsessidest toimib nüüd uutmoodi.

Metoodika hinne: 2/4.

3.2.4 Intervjuud

Järgmine meetod on teabe saamine äriprotsessi omanikult, milleks on intervjuu läbiviimine. See on üks lihtsamaid ja tõhusamaid meetodeid. Väärtuslikku ja ajakohastatud teavet selle kohta, kuidas ettevõttes äriprotsesse juhitakse, saab ainult läbi individuaalsete vestluste äriprotsessis otseselt seotud valdkondade ekspertidega, st. äriprotsesside omanike ja osalejatega. [8]

Sellel meetodil on mõningaid puudusi, näiteks intervjuu teabe kogumise protsess võtab analüütikult, kes tegeleb kirjeldatuga, suurt ajaressursi hulka. Samuti, rakendades seda meetodit, võivad tekkida järgmised probleemid:

1. äriprotsessi omanik on tööga hõivatud ja tal ei teki vaba aega intervjueerimiseks;

2. teabe subjektiivne olemus ja töötaja (antud juhul äriprotsessi omanik) kitsas silmaring, st. töötaja, kes teeb seda ja teab, mida ta tegema peab ning kes kohe üldse ei saa aru, kuidas siduda oma tegevused teiste töötajate või üksuste tegevustega;
3. sageli on probleemiks see, et töötaja ei ole huvitatud usaldusväärse ja ajakohastatud teabe esitamisest, sest muudatused, mis toimuvad ettevõttes pärast projekti lõppemist, võivad puudutada teda ja tema tegevusi ning see omakorda põhjustab inimeses hirmu ja mitteomaksvõtmist.
4. samuti on probleemiks selline asi nagu näiteks teabe segamine, st. kui inimene räägib mitte ainult seda, kuidas on tegelikult, vaid ka seda, kuidas see peaks olema. [8]

Selleks, et intervjuu kulgeks edukalt ja analüütik saaks vajaliku ja asjakohase teabe, tuleks järgida järgmisi soovitusi:

1. esimene asi, mida teha, on koostada intervjuu kava, st. sõnastama intervjuu eesmärgi ja selgelt mõista, mida tuleb kindlalt teada saada ja vastavalt sellele üles ehitada ka küsimusi. Intervjuu parim tulemus on eesmärgi saavutamine;
2. ühes intervjuus ei tohiks olla rohkem kui üks või kolm teemat. Kui teemasid on rohkem kui kolm, siis tuleks intervjuu jagada mitmeks kohtumiseks. Selle eesmärk on tagada, et teave ei oleks ülemäärane, sest seda tuleb pärast kohtumist töödelda ja struktureerida ning kui jutt on mitmetest teemadest, siis iga teema teave tuleb pealiskaudne;
3. intervjueerimise ajal tuleks rohkem kuulata kui rääkida. Rääkida tuleks intervjuu alguses, et luua inimesega kontakt ja ära määrata vestluse voog. Selles olukorras on peamiseks reegliks: ära muuda teemat enne kui eelmine pole selgeks tehtud. Teema üleminek tuleb ära märkida eelmise teema kokkuvõtmisega, rõhutades veelkord põhipunkte ja andes vastajale võimaluse midagi lisada;
4. saadud vastused tuleks ümber sõnastada ja valjult välja öelda. See on vajalik selleks, et õigesti aru saada, kas mõistsite õigesti vastaja sõnu, ning annab võimaluse vastajal lisada teavet või arendada olulisi punkte.
5. saadud vastused ja avaldused peavad olema kindlasti fikseeritud paberil või salvestatud diktofonile. See on vajalik, et info töötlemisel ei läheks midagi kaduma. [8]

Eraldi kommentaari nõuab soovitud loogilise taseme hoidmise reegel. Sageli intervjueerimise käigus kalduvad kaastöötajad edastama üsnagi abstraktset või küllaltki üksikasjalikku teavet oma tegevuse kohta. Esimesel juhul annab intervjueeritav teavet väga kõrge loogilise tasemega ja seda taset tuleb alandada, küsides küsimust “Millisel kujul viiakse täide antud töö?“. Teisel juhul annab intervjueeritav teavet madala loogilise tasemega ja seda taset tuleb tõsta, küsides küsimust "Milleks või mis eesmärgil seda tööd tehakse?". [8]

Intervjuu peaks olema korraldatud intervjueeritava juhi poolt. See on vajalik, et ei tekiks olukord, kus töötaja keeldub vestluse läbiviimisest, viidates aja- ja juhtimiskorralduse puudumisele. [8]

Intervjuu läbiviimise koht võiks olla eraldatud, vaikne ja rahulik, et välised tegurid ei segaks vestlust. [8]

Järeldus „intervjuu meetodi“ kohta

Antud meetod vastab suurepäraselt esimesele nõudele, kuna Skype ärirakenduse abiga intervjuude läbiviimine võimaldab teha kaugtööd, seega ei teki vajadust olla kohal teiste riikide filiaalides.

Julgelt võib väita, et “intervjuu meetod“ vastab ka teisele nõudele, kuna nõuab ainult valdkonna ühe esindaja osalemist (tavaliselt on selleks äriprotsesside omanik) ja seega kõik teised protsessis osalejad ei pea oma igapäevast tööd katkestama.

Antud meetod vastab ka „kliendi rahulolu“ kriteeriumile, selle poolest, et ettevõtte X töötajate kulutatud aeg ettevõtte Y analüütikute abile on minimaalne, kuna keskmine intervjuu võtab aega mitte rohkem kui 1-2 tundi (olenevalt äriprotsesside arvust).

Kolmandale nõudele vastab antud meetod poolenisti, võttes arvesse äriprotsesside inventuuri läbiviimise kiirust on ta palju kiirem kui meetod „ettevõttes eksisteerivate dokumentide uurimine“, aga võib jääda alla kiiruse poolest teisele meetodile.

Kvaliteedi nõudele vastab “intervjuu meetod“ suurepäraselt, kuna intervjuu käigus püüab ärianalüütik äriprotsessi kaardistada kui kolmas isik, seega protsessi üldpilt tuleb väga selgelt välja. Analüütiku küsimused on esitatud väga detailselt ning ta on võimeline pöörama tähelepanu ka nendele äriprotsessi nüanssidele, mida protsessi

omanik võib pidada ebaolulisteks ning jätaks need mainimata juhul, kui kaardistaks seda protsessi ise.

Metoodika hinne: 3,5/4.

3.2.5 Tööseminarid

Äriprotsesside teabe saamise käesoleva magistritöö viimaseks potentsiaalseks meetodiks on tööseminarid (ajurünnakud). Mõnede hinnangute kohaselt on antud meetod kõige efektiivsem. Tööseminaride käigus kogunevad kokku kõik äriprotsesside peamised osalejad ning koostööna töötatakse välja protsesside skeeme. Seetõttu on saadud teabe kvaliteet, tõhusus ja asjakohasus kõrgel tasemel. [6]

Sellise seminari tulemuseks on:

- lühikese aja jooksul saadakse kokkuvõtte kõigi osalejate teadmistest, kogemustest ja ülesannete optimaalsetest lahendustest, mis sobivad kõikidele osalejatele;
- tööseminari osalejate arvamuste sõltumatus. [6]

Selleks, et tööseminar oleks viljakas ja tõhus, tuleks järgida järgmisi näpunäiteid:

1. mõni päev enne ajurünnakut peaksid osalejad saama probleemi sõnastuse ja mõtlema (ükshaaval) selle probleemi lahendamise viisidele ning valima välja nende arvates kõige optimaalsema ja sobivama. See tähendab, et tulles kohale peaksid osalejad valmis olema – see annab võimaluse kaaluda kõiki võimalikke võimalusi, uurida neid ja jõuda ühisele arvamusele või otsusele;
2. seminari vältel ei tohiks lubada teise osaleja kohta teha kõiksugu kriitilisi märkusi.
3. samuti ei tohiks ka arutelu ajal olla jagunemist ülemusteks ja alluvateks, on ainult juhtiv isik ja osalejad;
4. kui meeskond pole arutelus 30-40 minuti jooksul leidnud ühtegi sobivat ideed, tuleks arutelu katkestada ning tähelepanu kõrvale juhtida, selleks et naasta arutellu uue jõu ja mõtetega. [6]

Nagu ülaltoodud kirjeldusest on näha, tuleks ajurünnakuid korraldada siis, kui on vaja lahendada globaalseid probleeme, näiteks: tootearendusstrateegia, bränding, uute toodetega turule sisenemine jne. Antud meetod ei sobi siis, kui on vajadus saada

kindlaid teadmisi ja arusaamu, kuidas konkreetne see või teine äriprotsess toimib – nii nagu on käsitletud käesolevas töös. [6]

Järeldus „tööseminaride meetodi“ kohta

Tööseminare on keeruline läbi viia Skype ärirakenduse abiga, seega võib väita, et see meetod eeldab kohalolemist, mis ei vasta esimesele nõudele.

Teisele nõudele antud meetod ka ei vasta, kuna nõuab äriprotsessi kõikide osalejate pikaajalist osalemist ning tööseminariks eelnevat ettevalmistust.

Kolmandale nõudmisele vastab see meetod samamoodi nagu „intervjuude meetod“, sest tööseminaride läbiviimise kiiruse suhtes on ta palju kiirem, kui „ettevõttes eksisteerivate dokumentide uurimismeetod“, aga aeglasem kui „ankeetide ja küsimustike meetod“.

Saab julgelt väita, et tööseminaride meetod vastab suurepäraselt kvaliteedi nõudele, kuna seminaride käigus vaadeldakse äriprotsessi otsast lõpuni, analüütikul on alati võimalus küsida täpsustavaid küsimusi protsessi mingi osa kohta ja ta võib saada väga täpse vastuse, kuna tema küsimust kuulavad ja analüüsivad kõik protsessi osalejad.

Metoodika hinne: 1,5/4.

3.3 “Intervjuu” kui äriprotsesside inventuuri läbiviimise meetodi valik

Punkti 3.2 alusel, milleks oli viie äriprotsesside teabe kogumisviiside kirjeldused, otsustas autor valida nendest neljas, nimelt “intervjuu“. See meetod tõusis kahtlematult liidriks teiste esitatud meetodite hulgast, saades kokku rekordilise 3,5 punkti.

Selle meetodi eelisteks, antud X ettevõtte äriprotsesside inventuuri tegemisel, omades üle neljasaja äriprotsessi kahes eri riigi filiaalides, on:

1. suhteliselt kiire teabe kokku kogumine arvestades ettevõtte dokumentatsiooni ja vaatluste läbiviimisega;
2. otsene kontakt eksperdiga, mis võimaldab sel viisil küsida otseseid ja täpsustavaid küsimusi, et kiiresti vajalik teabe kätte saada. See parandab ettevõttele X pakutava teenuse kvaliteeti, seega on ka eeliseks “küsimustike ja ankeetide meetodi“ ees;
3. Skype ärirakenduse abiga intervjuude läbiviimise võimalus;

4. äriprotsesside omanike tööaja suhteliselt tagasihoidlik kasutamine võrreldes seda “küsimustike ja ankeetide meetodiga”, kus suure hulga küsimustike töötlemine, eriti avatud küsimused, tekitaks suurema seisaku, sest vastaja ei mõista, mida temalt täpsemalt nõutakse.

Intervjuu meetodi puudusteks on:

1. intervjueeritava mõjutamise võimalus ekspertidele vastamisel;
2. aja puuduse tõttu puudub võimalus vastuseid sügavamalt kaalutleda;
3. suured ajakulud kogu äriprotsesside omanike grupi küsitluste jaoks.

Sellegipoolest oli autorile ilmne, et antud konkreetse juhtumi kohta võrreldes teistega on kõige kasulikum ja eelistatavam kasutada äriprotsesside teabe kogumiseks “intervjuu meetodit“.

Tuleb ära märkida, et ülaltoodud loendist oli teiseks sobivaimaks meetodiks “küsimustike ja ankeetide meetod“. Seda meetodit kasutatakse laialdaselt äriprotsesside inventuuride läbiviimisel vastavalt GDPR määruse artiklile 30 teistes sarnastes ettevõtetes, kuid see ei mõjutanud autori otsust eelistada "intervjuu meetodit" ülaltoodud „küsimustike ja ankeetide meetodi“ asemel.

4 Metoodika valimine kasutatavate süsteemide riskianalüüsi läbiviimiseks

Sõltuvalt asjaoludest millegi riskianalüüsi läbiviimiseks kasutatakse kahte meetodit: kvalitatiivset või kvantitatiivset. Mõningatel juhtudel on nende kombinatsioon samuti võimalik. Kvalitatiivse või kvantitatiivse hindamismeetodit kasutatakse esmalt tavaliselt hinnatava objekti ohu taseme üldise teave saamiseks. [9]

Kvalitatiivse hindamisega kasutatakse riskiastme hindamiseks kvalifikatsiooni skaalat, näiteks: madal, keskmine ja kõrge ning samuti nende tagajärgede tekete tõenäosusi. Kvalitatiivse analüüsi meetodi peamiseks eeliseks on selle kerge vastuvõtmine ja arusaamine kõikide töötajate poolt, kes on kaasatud asjakohase riskianalüüsi tegemisse. Kvalitatiivse hindamise puudus peitub skaala enda olenevalt subjektiivsest valikust. [9]

Kvalitatiivset analüüsi meetodit kasutatakse:

- kui esmast etappi riskide ja nende taseme määratlemisel enne üksikasjalikumat kontrolli;
- seal, kus sellise analüüsi tegemine on otsuse vastuvõtmisel asjakohane;
- seal, kus on arvandmed või kvantitatiivseks hindamiseks ebapiisavad andmed. [9]

Just see teave ongi vajalik ettevõtte X jaoks kasutatavate süsteemide riskianalüüsi läbiviimiseks, mistõttu autor tegigi ilmse otsuse valida ühe kvalitatiivse analüüsi meetodi.

4.1 Nõuded kvalitatiivse analüüsi metoodikale

1. Kiirus.
   Metoodika peab võimaldama saada töötulemused maksimaalse kiirusega.
2. Võimalus kohe alustada, isegi siis kui, mis tahes algandmed puuduvad.

Metoodikat peab saama rakendada ka uuritava objekti riskitaseme ebamäärasuse tingimusel.

3. Maksimaalse kvaliteedi saavutamine.
   Valitud metoodika peab samuti võimaldama saavutada ettevõtte Y pakutava teenuse maksimaalse kvaliteedi. See tähendab seda, et läbiviidavas riskianalüüsis peavad olema välja selgitatud kasutavate süsteemide kõik olemasolevad nõrgad kohad.

4.2 Riskianalüüsi läbiviimiseks enamlevinud kvalitatiivsed meetodid ning nende eelised ja puudused

Kvalitatiivse analüüsi jaoks on olemas mitu enamlevinud meetodite rühma. Need hõlmavad järgmisi meetodeid.

4.2.1 Eksperthinnangute meetod

Eksperthinnangute meetod – see on kombinatsioon matemaatilistest ja loogilistest menetlustest, mille tulemuseks on eksperdi järeldus teatud küsimustes. [7]

Eelised:

1. võime rakendada meetodit ka siis, kui uuritava objekti riskitase ei ole määratletav;
2. meetodi õpetamise ja hindamise lihtsus;
3. puudub vajadus suure ajakulu järele, samuti puudub ka organiseerimise ja läbiviimise kulu;
4. võimalus saada kvantitatiivseid hinnanguid juhtudel, kui mis tahes statistilised andmed puuduvad;
5. tulemuste saavutamise kiirus.

Puudused:

1. vastuste puudulikkus;
2. küsitluse osalejate subjektiivne tegur;
3. küsitletavate poolt valesti tõlgendatud küsimused. [11]

Järeldus “eksperthinnangute meetodi” kohta

Antud meetod vastab esimesele kriteeriumile, st. ta on kõige vähem aega nõudev. Samuti ei ole eksperthinnangute meetod vastuolus ka teise kriteeriumiga, võimaldab alustada riskianalüüsiga ebamäärastes tingimustes ning samuti võimaldab saavutada analüüsi soovitud kvaliteedi, vastates seega kolmandale nõudele.

4.2.2 Allikate kontrollnimekirjad

See meetod on kõige efektiivsem, kui vastav kontrollnimekiri on juba olemas ja ülesanne on kontrollida riskijuhtimise kvaliteeti äriprotsessi teatud etappides, st. võrrelda riskijuhtimise tegelikku rakendamist koostatud põhikirjaga, mille eesmärk on reguleerida seda juhtimist. Meetodit rakendatakse ainult riskide tuvastamise etapis, muude meetodite täiendusena. [12]

Eelised:

1. võimalus kasutada ka mittespetsialistidel;
2. võimalus analüüsida eelmisi vigu, mis omakorda annab võimaluse neid vigu mitte korrata;
3. võimaldab veenduda, et kontroll üldiste probleemide ja vigade üle ei läheks kaduma. [12]

Puudused:

1. meetod tugineb varasemate vaatluste tulemustele, seetõttu ei ole võimalik välja selgitada varem lahendamata probleemid;
2. mitte kõik tegurid võivad olla nimekirja lisatud õigeaegselt ja sellest lähtuvalt ei ole tulevikus arvesse võetud;
3. tõlgendamise keerukus. [12]

Järeldus allikate kontrollnimekirjade meetodi kohta

See meetod ei vasta esimesele ja teisele kriteeriumile, kuna see tähendab spetsiaalsete kontrolldokumentide täiendavat uurimist, mida antud juhul ei eksisteeri.

4.2.3 Reitingu hindamise meetod

Reitingu hindamise meetod on juba olemasolevate hinnangute kujundamine. Selle meetodi kõige lihtsamaks vormiks on järjestamine (palliline hindamise süsteem). Kõige sagedamini kasutatakse viiepunktisüsteemi, harvemini aga kümne või enama. Tulemuste põhjal luuakse "riski hindamise" tabel, mida täidab ekspert, kes määrab iga riski kohta vastava punkti. Samuti on vaja arvestada eksperdi pädevusega hinnangu koostamisel. Ka seda meetodit saab kasutada ainult muude meetodite täiendusena. [12]

Eelised:

1. kasutamise lihtsus;
2. suhteliselt kõrge täpsus. [12]

Puudused:

1. nimekirja koostamise keerukus ja selle õige tõlgendamine;
2. hinnangu subjektiivsus. [12]

Järeldus hinnangute meetodi kohta

Nii nagu eelmine meetod, ei vasta ka see meetod esimesele ja teisele kriteeriumile, see tähendab seda, et see eeldaks juba olemasolevat hinnangut eelnevate ekspertide poolt, mida aga antud juhul meil ei ole.

4.2.4 Analoogi meetod

Analoogi meetodiks nimetatakse sarnaste rakenduste andmete analüüsi, mida ettevõte on kasutanud varem. Sellisel juhul võivad vajalike andmete allikateks olla ettevõtte arhiivid, teabebaasid, samuti välishindamised, eksperthinnangud ja uurimistulemused. [14]

Eelised:

1. kasutamise lihtsus. [14]

Puudused:

2. selle meetodi peamiseks probleemiks on olemasoleva analoogi valimine hindamiseks, kuna potentsiaalse rakenduse hindamiseks pole selgeid kriteeriume. [14]

Järeldus „analoogi meetodi“ kohta

Kuna ettevõttel X pole arhiive, mis sisaldavad varem kasutatud infosüsteemide riskianalüüsi andmeid, siis selle kohaldamine antud konkreetsel juhul muutub võimatuks. Isegi kui sellised andmed oleksid olemas, oleks nende täiendav uurimine vastuolus kiiruse nõudega. Kuna on ebatõenäoline, et eelnevalt kasutatud süsteemid oleksid praeguste süsteemide täielikud analoogid, oleks analüüsi nõutav kvaliteeditase vähemal määral rahuldav.

4.2.5 Järeldus

Seekordne autori valik on eksperthinnangute meetod, kuna antud meetod vastab kõige paremini metoodikale välja toodud nõuetele – eriti kahele esimesele. Autor teeb sellise järelduse tuginedes asjaolule, et eksperthinnangute meetod ei hõlma endas infosüsteemide täiendavate dokumentide uurimist ning samuti võimaldab teha analüüsiga algust ebamäärastel tingimustel. Selleks aga, et saavutada riskianalüüsi nõutavat kvaliteeditaset, tuleb autoril teha veel üks valik.

Kuid tuleb ära mainida, et eksperthinnangute meetod jaguneb omakorda veel neljaks meetodiks, milleks on:

1. SWOT-analüüs;
2. riskide roosi ja spiraal;
3. Delfi meetod;
4. küsimustik. [11]

"SWOT-analüüsi meetod on ettevõtte strateegiline planeerimine, see seisneb sise- ja väliskeskkonna tegurite väljaselgitamises, jagades need nelja kategooriasse: tugevused, nõrkused, võimalused ja ohud." [13]

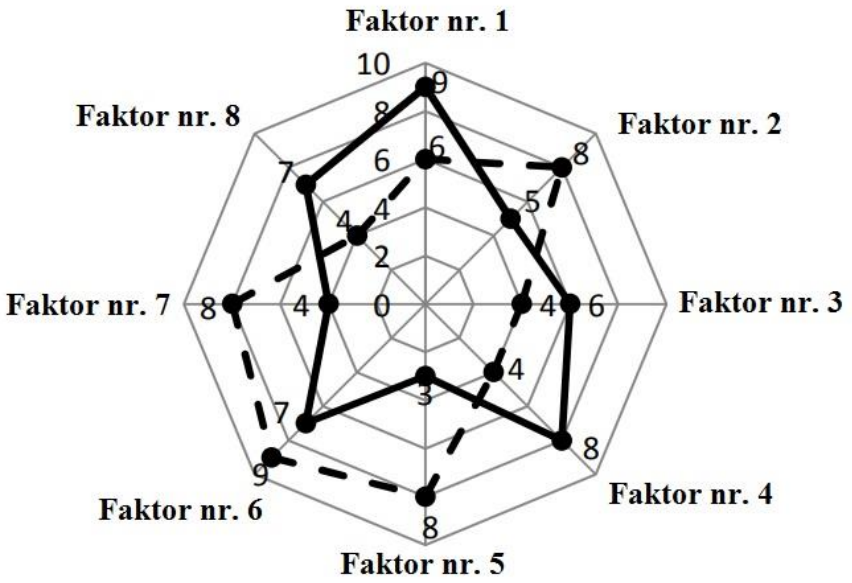
Eeltoodust lähtuvalt võime järeldada, et tarkvara riskianalüüs ei ole SWOT-analüüsi kasutusala.

Samuti väärib märkimist, et "SWOT-analüüs kuulub strateegilise analüüsi nn. juhendmaterjalide mudelite rühma, mis näitavad ainult ühiseid eesmärke ja konkreetseid meetmeid nende saavutamiseks tuleks arendada eraldi." [13]

See avaldus kinnitab asjaolu, et infosüsteemide ohu analüüsimisel antud meetod ei suuda pakkuda objektiivset kvalitatiivset hinnangut infosüsteemi ohutaseme kohta.

Erinevalt SWOT-analüüsi meetodile saab riskide roosi ja spiraali meetodit kasutada selleks, et võrrelda tarkvarariskide ekspertiisi tulemusi erinevate aspektidega ning selle peamine eelis on infosüsteemide võrdlevate hinnangute kohta saadud andmete visualiseerimise erivorm. [15]

Selle meetodi abil infosüsteemide riskide analüüsimiseks peavad eksperdid täitma analüütikute poolt koostatud ettevalmistatud küsimustikud, milles tehakse iga teguri jaoks riskihinnangud, tavaliselt kümnepunktilisel skaalal. Tavaliselt näitab kõrgem skoor objekti kõrgemat riski. Uuringu käigus saadud täiendavad tulemused on esitatud roosi või tähe kujul (vaata joonis 1). Sellisel juhul näitab riskide roos suuremalt kahe võrreldava objekti riskisuhte visuaalset esitust. Seejärel luuakse riskide spiraali, mis kajastaks riskitegurite järjekorda (järjestamine). [15]



Joonis 1 Riskide roosi näide, mis näitab kahe objekti riskide suhet. [23]

Nii nagu "riskide roosi ja spiraali meetodit", võib ka Delfi meetodit kasutada infosüsteemide ohtude analüüsimiseks, kuid see eeldab teatud järjestikuste meetmete järgimist, nagu näiteks:

1. uuringute läbiviimine (küsimustikud);
2. intervjuude läbiviimine;
3. ajurünnak. [22]

Siis jaguneb meetod kolmeks etapiks:

1. Esialgne etapp.
   Esialgse etapi käigus kogutakse kokku ekspertide rühm. [22]
2. Peamine etapp.
   See tähendab küsimuste kujundamist ja laiali saatmist ekspertidele, neile vastuste saamist ning uue täiustatud küsimustiku analüüsi ja laiali saatmist. [22]
3. Analüütiline etapp.
   Viimase analüütilise etapi käigus analüüsitakse kogutud ja kooskõlastatud järeldusi, soovituste koostamine. [22]

Delfi meetodi eelised:

- lihtne kasutada;
- arvesse võetakse kõigi uuringus osalenud inimeste arvamus;
- aitab kaasa iseseisva mõtlemise arendamisele. [22]

Delfi meetodi puudused:

- inimgrupi arvamus ei pruugi alati olla tõene;
- küsitluse korraldajad omavad rohkem volitusi kui ekspertide rühm – see tähendab, et mõne eksperdi arvamus võib jääda märkamatuks;
- võib juhtuda, et väikese hulgalise ekspertide grupi (eriti üks ekspert) loominguline lahendus võib jääda märkamatuks ja analüütikute poolt arvestamata, vaatamata selle võimalikule suurele tõhususele;
    - enamus arvamuse püüdlus;
    - suured ajakulud (iga etapp võib kesta 1 kuni 30 päeva). [22]

Autor arvas, et selle konkreetse juhtumi kasutatavate süsteemide riskitaseme selge pildi annab lihtne ühetasemeline ekspertide küsitlus (võtmeisikud). Kusjuures, iga süsteemi kohta vastusi annab ainult üks võtmeisik.

Küsimustik ise hakkab endas kujutama küsimuste loetelu koos esitatud vastuste variantidega, kus iga vastuse variant saab teatud arvu punkte. Pärast ettevõtte X mistahes kasutuses oleva infosüsteemi uuringu lõppu, arvutatakse kokku punktide kogusumma, mis kvalitatiivselt kinnitab selle riski taseme.

Autor ei pidanud vajalikuks riskianalüüsi läbiviimisel kasutada sellist sügavat meetodit nagu Delfi meetod, sest seda ei nõua ka see konkreetne olukord. Lisaks suurendaks see põhjendamatult ja märkimisväärselt ajakulusid, tekitades nõnda vastuolu metoodika esimese nõudega.

Samuti puudus ka vajadus "riskide roosi ja spiraali" meetodi visualiseerimiseks, sest autoril oli vaja iga infosüsteemi kohta ainult punktide kogusummat, mille kasvu

põhimõtte alusel oleks infosüsteemide prioriteediks seatud ka üks neist ja millises järjekorras need tuleb täita või asendada vastavalt GDPR määruse normidele.

5 Äriprotsesside inventuur

5.1 GDPR määruse nõued äriprotsesside inventuuri dokumentatsioonile

Oluline on välja tuua GDPR määruse artikkel nr. 30, mis kirjeldab järgmist – "vastutav töötleja ja asjakohasel juhul vastutava töötleja esindaja peavad registreerima nende vastutusel tehtavad isikuandmete töötlemise toimingud." [1]

Antud dokument peab sisaldama vastutava töötleja ning asjakohasel juhul kaasvastutava töötleja, vastutava töötleja esindaja ja andmekaitseametniku nimi ja kontaktandmed, töötlemise eesmärgid, andmesubjektide kategooriate ja isikuandmete liikide kirjeldus. Peale selle veel vastuvõtjate kategooriad, kelle isikuandmeid on avalikustatud või avalikustatakse kaasa arvatud rahvusvahelised organisatsioonid ja kolmandates riikides olevad vastuvõtjad. Juhul kui edastatakse infot kolmandatele riikidele või rahvusvahelisele organisatsioonile, siis andmed riigi või organisatsiooni nimega. Lisaks tuleb lisada ka kaitsemeetmete kohta koostatud dokumendid kui on tegemist artikli 49 lõike 1 teises lõigus kirjeldatud saatmisega. [1]

Samuti peaks võimaluse korral lisama tähtajad millal erinevaid andmeid kustutatakse ning tehniliste ja korralduslike turvameetmete üldine kirjeldus. [1]

Dokumendis on kirjeldatud ka see, et registreerimine peaks olema elektrooniline ning taotluse korral peab olema võimalik teha vastutava või volitatud töötleja poolt register kättesaadavaks. [1]

Oluline on ka rääkida artikli viimasest punktist, mis viitab, et eelnevalt mainitud kohustused ei kehti vähem kui 250 töötajaga ettevõttele või organisatsioonile, välja arvatud juhul, kui "tema teostatav töötlemine kujutab endast tõenäoliselt ohtu andmesubjekti õigustele ja vabadusele, töötlemine ei ole juhtumipõhine või töödeldakse kui, artikli 9 lõikes 1 osutatud isikuandmete eriliigiga või artiklis 10 osutatud süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud andmeid." [1]

Teiste sõnadega see tähendab seda, et põhimõtteliselt kõik juriidilised isikud peaksid ette valmistama enda äriprotsesside inventuuri, kuna vajadusel tõestamine, et mingi ettevõte, kus töötab vähem kui 250 inimest, ent nende teostatav töötlemine ei ole ikkagi juhtumipõhine või kujutab endast tõenäoliselt ohtu andmesubjekti õigustele ja vabadusele – on juristide oskuste ja kompetentsuse asi.

Kuna ettevõttes X töötab rohkem kui 250 inimest, siis üleval toodud teksti põhjal tuleb ettevõttel X GDPR määruse vastavuseks kindlasti ära teha äriprotsesside inventuur.

5.2 Äriprotsesside inventuuri läbiviimise käik intervjuu meetodi rakendades

Inventuuri läbiviimise alustamiseks ettevõttes X peab iga valdkonnajuht ette valmistama kõikide tema valdkonnas toimuvate äriprotsesside loetelu ning iga äriprotsessi kõrvale määrama ühe äriprotsessiomaniku ehk inimese, kes omandab kõige rohkem infot antud äriprotsessi kohta.

Intervjuu esimene etapp

Selleks, et rahuldada GDPR määruse artikli nr. 30 nõude ehk info kogumine määratud punktide järgi ning nende alusel vastava registri valmistamine, küsib analüütik intervjuu esimese etapi käigus äriprotsessi omanikult äriprotsessi kohta järgmisi andmeid:

- äriprotsessi kirjeldus ehk lühikirjeldus, millest protsess algab ning millega lõpeb;
- äriprotsessi voog ehk kuidas protsess sujub (intervjuu oluline osa, kus tehakse selgeks, mis etappidest antud protsess koosneb, kuidas need etapid välja näevad, milliseid infosüsteeme kasutatakse, kas toimub andmete edastamine ja kui jah, siis kellele ning mis on andmete säilitamisaeg). Sellel intervjuu etapil selguvad tihti protsessi kõige nõrgemad kohad, mis võivad olla vastuolus GDPR määruse nõuetega ning millele hiljem juhitakse tähelepanu;
- roll, ehk antud äriprotsessis ettevõtte X roll GDPR määruse aspektist (kas vastutav töötleja või volitatud töötleja);

- andmete päritolu ehk mis on andmete allikaks antud protsessis (klient/töötaja, siseallikas või kolmas osapool);
- äriprotsessi eesmärk;
- äriprotsessi juriidiline alus (kas andmesubjekti nõusolek lepingu täitmiseks, õigusnormi täitmiseks või õigustatud huvide kasutamiseks;
- andmeedastuse asukoht – juhul kui äriprotsessi voogu kirjeldamisel selgub, et antud äriprotsessi jooksul toimub andmete edastamine, siis tuleb ära märkida, kas edastamine on sisene (see tähendab kui andmed on liikunud ettevõtte X erinevate äriüksuste vahel), EU/EEA tsoonis, kolmandatesse riikidesse või rahvusvahelistesse organisatsioonidesse.

Sellega lõpeb intervjuu esimene etapp, mille käigus analüütik konspekteerib saadud vastused ning edasi algab intervjuu teine ehk viimane etapp.

Intervjuu teine etapp

Selle etapi eesmärgiks on andmesubjektide tüüpide ning kasutatavate süsteemide määratlemine. Andmesubjektiks on iga isik, kelle isiklikke andmeid töötleb ettevõte X antud äriprotsessi raames.

Andmesubjektide nimekiri on autori väljaarendatud ning siin on nende peamised tüübid:

- Klient – Iseenda (kui tegemist on eraisiku andmetega);
- Klient – Esindaja (kui tegemist on juriidilise- või erakliendi esindaja andmetega);
- Klient – Kontaktisik (kui tegemist on juriidilise isiku kontaktisiku andmetega);
- Töötaja – Iseenda (kui tegemist on ise töötaja andmetega);
- Töötaja – Kontaktisik (kui tegemist on töötaja kontaktisiku andmetega);
- Tarnija/Töövõtja/Partner – Iseenda (kui partneriks on eraisik ning tegemist on tema andmetega);

- Tarnija/Töövõtja/Partner – Kontaktisik (kui partneriks on juriidiline isik ning tegemist on tema kontaktisiku andmetega);

- Tarnija/Töövõtja/Partner – Esindaja (kui partneriks on juriidiline- või eraisik ning tegemist on tema esindaja andmetega).

Kui kõik andmesubjektid, kelle isiklikke andmeid töötleb ettevõte X antud äriprotsessis, saavad määratletud, koostatakse süsteemide loetelu. Süsteemideks on vaid kõik spetsiaalsed sisesed ja välised infosüsteemid, milliseid kasutatakse äriprotsessi käigus selle realiseerimiseks. Tavaliselt kujuneb kasutatavate süsteemide loetelu juba esimesel etapil, siis kui protsessi omanik kirjeldab äriprotsessi voogu.

Kui andmesubjektid ning kasutatavad süsteemid saavad määratletud, siis pidi autor veel ära täitma, mis tüüpi andmete töötlemist on rakendatud iga süsteemi puhul konkreetse iga andmesubjekti tüübi juures, kas lugemist, loomist, uuendamist, monitoorimist ja/või ülekandmist. Autori välja töötatud süsteemi järgi üleval mainitud töötlemistüüpe kasutatakse järgmistel juhtudel:

- lugemine – kui töötaja ainult vaatab andmeid või ekspordib avalduses olevat infot failile;

- loomine - kui töötaja loob uued andmed, mida varem ei eksisteerinud (käsitsi, fail), loob faili töökohale/failiserverile või loob e-kirja, kus andmeid kasutatakse kirja koostamisel;

- uuendamine (sealhulgas lugemine) – kui töötaja uuendab olemasolevaid andmeid avalduses/failis;

- monitoorimine (sealhulgas lugemine) – kui töötaja jälgib midagi või otsib muudatusi;

- edastamine – kui töötaja või süsteem edastab andmed teisele juriidilisele isikule e-posti teel; erinevate süsteemide vahel (automaatselt või nupu vajutusega) või postitusega.

Intervjuu teise etapi kaardistatud andmed on demonstreeritud allolevas tabelis.

Tabel 1 Töötlemistoimingute mall märgitud näidisäriprotsessi süsteemidega, andmesubjektidega ning nende töötlemistüüpidega.

Riik	Protsessi ID	Valdkond	Protsessi nimi	Andmesubjekt	Süsteem		Töötlemise kirjeldus	Töötlemise tüüp				
					Süsteemi tüüp	Süsteemi nimi		Lugemine	Loomine	Uuendamine	Monitoorimine	Edastamine
X Y	ÄP.0001	Raamatupidamine	Näidisäriprotsess	Klient – Kontaktisik	rakendus	Süsteem 1	Andmed vaadatud, loodud, uuendatud	x	x	x		
X Y	ÄP.0001	Raamatupidamine	Näidisäriprotsess	Klient – Kontaktisik	rakendus	Süsteem 2	Andmed on vaadatud	x				
X Y	ÄP.0001	Raamatupidamine	Näidisäriprotsess	Klient – Kontaktisik	väline rakendus	Süsteem 3	Andmed on kätte saadud	x				
X Y	ÄP.0001	Raamatupidamine	Näidisäriprotsess	Klient – Esindaja	rakendus	Süsteem 1	Andmed on vaadatud, loodud ja uuendatud	x	x	x		

Riik	Protsessi ID	Valdkond	Protsessi nimi	Andmesubjekt	Süsteem		Töötlemise kirjeldus	Töötlemise tüüp				
					Süsteemi tüüp	Süsteemi nimi		Lugemine	Loomine	Uuendamine	Monitoorimine	Edastamine
X Y	ÄP.0001	Raamatupidamine	Näidisäriprotsess	Klient – Esindaja	rakendus	Süsteem 2	Andmed on vaadatud					
X Y	ÄP.0001	Raamatupidamine	Näidisäriprotsess	Klient – Esindaja	väline rakendus	Süsteem 3	Andmed on kätte saadud	x				
X Y	ÄP.0001	Raamatupidamine	Näidisäriprotsess	Klient – Iseenda	rakendus	Süsteem 1	Andmed on vaadatud, loodud ja uuendatud	x	x	x		
X Y	ÄP.0001	Raamatupidamine	Näidisäriprotsess	Klient – Iseenda	rakendus	Süsteem 2	Andmed on vaadatud, loodud ja uuendatud	x	x	x		
X Y	ÄP.0001	Raamatupidamine	Näidisäriprotsess	Klient – Iseenda	Väline rakendus	Süsteem 3	Andmed on vaadatud, loodud ja uuendatud	x	x	x		

Tabelis 1 on näha, et näidisäriprotsessi raames kasutatakse kolme süsteemi (1, 2 ja 3) ning figureerivad kolm andmesubjekti (Klient – Kontaktisik, Klient – Esindaja ja Klient

– Iseenda). Protsessi kaardistamisel peab kindlasti iga andmesubjekti vaatlema iga süsteemi raames – tänu sellele selgub, mis tüüpi andmetöötlemine toimub iga subjekti puhul (kas lugemine, loomine, uuendamine, monitoorimine ja/või edastamine). Näidisel on demonstreeritud, et andmesubjekti „Klient – Iseenda“ puhul süsteemi 2 ja 3 raames töödeldakse lugemise, loomise ja uuendamise tüübi järgi. Andmesubjekti "Klient – Kontaktisik" ning "Klient – Esindaja" puhul on samade süsteemide raames selleks tüübiks, aga vaid lugemine.

Kõik need andmed (andmesubjektide tüüpe ja kasutatavaid süsteeme ning nende liike) saadakse läbi vestluste äriprotsessi omanikuga. Analüütik esitab protsessi omanikule üksikasjalikke küsimusi, millele vastates saab mõlemale selgeks, millised punktid peavad kindlasti kirja pandud saama.

Pärast äriprotsessi kaardistamist on veel viimaseks nüansiks selle protsessi lõpetamiseks andmeatribuutide välja toomine. Andmeatribuutideks on isiku konkreetsed isiklikud andmed (nt. ees- ja perekonnanimi, isikukood, elukoha aadress, e-post, kodakondsus jne.).

Kuna äriprotsessi omanikul on kõige rohkem infot enda äriprotsessi kohta ning ta teab täpselt, milliseid subjekti andmeid töödeldakse ühe või teise süsteemi puhul antud äriprotsessi raames, on seega andmeatribuutide välja toomine tema iseseisvaks ülesandeks. Selleks aga saadab analüütik peale intervjuud äriprotsessi omanikule töötlemistoimingute malli kaardistatud äriprotsessiga, kus on juba välja toodud andmesubjektid vastavate kasutatavate süsteemide ning andmete töötlemistüüpidega (Tabel 1). Samal mallil on välja toodud ka andmeatribuutide loetelu, mis koosneb suurest hulgast erinevatest võimalikest atribuutidest (atribuutide täis nimekiri on välja toodud Lisas 2). Omakorda täidab protsessi omanik ära ka kõik andmeatribuudid, mis on töödeldud antud äriprotsessi raames konkreetsete andmesubjektide ning konkreetsete süsteemide puhul.

Andmeatribuutide äratäitmiseks antakse protsessi omanikule tavaliselt nädal aega. Pärast seda saadab ta töötlemistoimingute malli autorile tagasi koos märgitud andmeatribuutidega. Analüütik omakorda sisestab saadud andmeatribuudid ühte protsessi inventuuri faili, kus on kaardistatud ettevõtte X kõik teised äriprotsessid vastavalt GDPR määruse artiklile nr. 30. Sellega äriprotsessi inventuur lõpeb.

5.3 Äriprotsesside inventuuri läbiviimine (ühe äriprotsessi näitel)

Antud punktis on välja toodud näide ettevõtte X ühe reaalse äriprotsessi otsast lõpuni kaardistamisest. Selleks, et säilitada ettevõtte X tegevusala saladus, sai valituks selline universaalne äriprotsess nagu "Töötasu ülevaatamine". Antud protsessi kaardistamine oli autori tehtud.

Protsess oli kaardistatud intervjueerides kahte personaliosakonna esindajat.

Intervjuu esimene etapp

Nagu oli eelmises punktis mainitud, intervjuu esimese etapi käigus toimub äriprotsessi järgnevate osade kaardistamine: protsessi kirjeldus, protsessi voog, ettevõtte X roll, andmete päritolu, protsessi eesmärk, juriidiline alus protsessi teostamiseks ning andmeedastuse asukoht.

Tabel 2 Äriprotsessi „Töötasu ülevaatamine“ inventuuri mall.

Protsessi kirjeldus	Protsess algab vaadates läbi arenguvestluste tulemused ning lõpeb otsusega selle kohta, millist boonust tuleks määrata.
Protsessi voog	Personaliosakond valmistab äriüksuse juhile ette nimekirja töötajatest ja nende palkadest. Äriüksuse juht vaatab nimekirja üle ning võttes aluseks arenguvestluse näitajad, määrab järgmised tulemused: 1) ühekordne makse; 2) motivatsioonitasu (tulemustasu). Arenguvestluste tulemusi hoitakse süsteemis 2. Äriüksuse juht tagastab ajakohase palkade nimekirja tagasi personaliosakonnale, kes edastavad info emailiga süsteemile 34. (Süsteem 34 on personalihalduse portaal lõppkasutajate ehk töötajate jaoks. Töötaja saab näha oma andmeid, tööaega, küsida puhkust, panna kirja kontorist väljas olemise aega, saab küsida luba reisimiseks. Juhtide jaoks on seal informatsioon tiimi kohta – palgad, puhkused jne).
Protsessi omanik	Nimi on peidetud
Ettevõtte roll	☐ Volitatud töötleja ☑ Vastutav töötleja
Andmete päritolu	☐ Klient / Töötaja ☑ Sisene allikas ☐ Kolmas osapool

Protsessi eesmärk	Töötasude iga-aastane ülevaatamine
Juriidiline alus protsessi teostamiseks	☐ Andmesubjekti nõusolek ☑ Lepingu täitmiseks ☐ Õigusnormi täitmiseks ☐ Õigustatud huvide kasutamiseks
Andmeedastamine	☐ Sisene ☑ EU/EEA ☐ Kolmas riik ☐ Rahvusvaheline organisatsioon
Andmeedastamise asukoht	Ettevõtte nimi ja selle asukoht on peidetud
Vastuvõtja kategooria	☑ Volitatud töötleja ☐ Vastutav töötleja

Tabelis 2 on ette näidatud äriprotsessi "Töötasu ülevaatamine" kaardistamise tulemused ning valikute põhjendused:

- esimeses ja teises punktis said vastavalt kirjeldatud äriprotsessi lühikirjeldus ja protsessi voog;
- kolmandas punktis on näidatud protsessi omaniku nimi ehk inimene, kes omab kõige rohkem infot antud äriprotsessi kohta;
- neljandas punktis määrati ettevõtte X roll antud äriprotsessis. Selleks sai vastutav töötleja kuna ettevõte X antud juhul ei töötle, vaid määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid;
- viiendas punktis sai valituks variant „sisene allikas“, kuna teises punktis kättesaadud info alusel saab üksuse juht andmeid töötajate kohta personaliosakonna käest;
- protsessi eesmärk on defineeritud kui „iga-aastane töötasude ülevaatamine“ ja seega sai ka kuues punkt täidetud;
- seitsmendas punktis näidatud juriidiliseks aluseks antud äriprotsessi puhul on tõenäoliselt „lepingu täitmiseks“, kuna ettevõtte X töölepingutes on sisse viidud vastav punkt, mis lubab töötajate palgad iga-aastaselt ülevaadata;

- kaheksandas punktis olev andmeedastamine (näide selle kohta, kas selles protsessis olevad andmed edastatakse riikidesse, mis asuvad EMP piirkonnas, kolmandates riikides väljaspool EMP-d või rahvusvahelistes organisatsioonides. Rahvusvaheliste organisatsioonide all peetakse silmas avalik-õiguslik organisatsioone või sellele alluvaid organeid või muid organeid, mis on loodud kahe või enama riigi vahel sõlmitud kokkuleppe alusel.) antud protsessis toimub, mis tuleneb protsessi voogust: üksuse juht tagastab ajakohase palkade nimekirja tagasi personaliosakonnale, kes edastavad info e-mailiga süsteemile 34 (mis on väliseks süsteemiks ning kujutab endast eraldi ettevõtet);

- üheksandas punktis on andmeedastuse asukoht (geograafiline asukoht, kuhu isikuandmed edastatakse) peidetud eesmärgiga hoida saladuses ettevõte, millisele kuulub süsteem 43;

- kümnendas punktis näidatud vastuvõtjaks on just see ettevõte X ehk süsteem 43 ja selle roll antud protsessis on volitatud töötleja, kuna see töötleb isikuandmeid vastutava töötleja nimel.

Intervjuu teine etapp

Nagu ütleb punkt 5.2 on intervjuu teiseks etapiks andmesubjektide, kasutatavate süsteemide ning nende raames atribuutide töötlemistüüpide määratlemine. Allolevas tabelis on need parameetrid ette näidatud äriprotsessi “Töötasu ülevaatamine” puhul.

Tabel 3 Äriprotsessi „Töötasu ülevaatamine“ töötlemistoimingud.

Andmesubjekt	Süsteemi tüüp	Süsteemi nimi	Töötlemise kirjeldus	Töötlemise tüüp				
				Lugemine	Loomine	Uuendamine	Monitoorimine	Edastamine
Töötaja – Iseenda	e-mail	E-mail	Personaliosakond edastab uuendatud palkade nimekirja info edasi peidetud ettevõttele.					x
Töötaja – Iseenda	failiserver	Süsteem 2	Süsteemist 2 võetakse infot läbiviidud arenguvestluste kohta	x				
Töötaja – Iseenda	Väline süsteem	Süsteem 34	Töötasudest informatsiooni sisestamine; töötaja sisestab töötunnid, mis on kinnitatud juhi poolt		x	x		

Nagu on näha tabelist 3, äriprotsessi „Töötasu ülevaatamine“ raames töödeldakse ainult töötajate andmeid, seega andmesubjektiks sai valitud üks tüüp – „Töötaja – Iseenda“. Kasutatavate süsteemide loetelu koosneb vaid kolmest süsteemist, milleks on:

- E-mail (töötlemistüübiks on „edastamine“, kuna selle süsteemi kaudu edastatakse töötajate andmeid üsteemi 43 esindamisettevõttele);

- süsteem 2, mis kujutab endast failiserverit ning hoiab infot läbiviidud arenguvestluste kohta (töötlemistüübiks on „lugemine“, kuna sellest süsteemist võetakse töötajate andmeid uurimiseks);

- ettevõttele-partnerile kuuluv süsteem 34; kuna siia esmalt sisestakse andmeid töötajate palkade kohta ja seejärel uuendatakse, siis andmete töötlemistüüpideks on määratletud „loomine“ ja „uuendamine“.

Seega intervjuu äriprotsessi omanikega lõppes ning kohe peale vestlust saatis autor nendele töötlemistoimingute malli antud protsessi andmeatribuutide täitmiseks, kuna just protsessi omanikud (antud juhul kaks personaliosakonna esindajat) omavad kõige rohkem infot, milliseid isiklikke andmeid töödeldakse ning mis süsteemide raames. Töötlemistoimingute mall edastati Excel failina, kuhu oli pandud „Töötasu ülevaatamise“ protsessis kasutatavad süsteemid, andmesubjektid, kelle andmeid protsessi käigus töödeldakse ning andmeatribuutide loetelu, millest personaliosakonna esindajad pidid valima need, mis saavad töödeldud iga süsteemi puhul.

Nädala hiljem sai autor tagasi töötlemistoimingute malli märgitud andmeatribuutidega:

Tabel 4 Äriprotsessi „Töötasu ülevaatamine“ andmeatribuudid.

Andmesubjekt	Süsteemi nimi	Andmeatribuudid												
		Nimi	Perekonnanimi	Isikukood	Elukoha aadress	Telefoni number	ID number süsteemis 1	E-posti aadress	Sugu	Sünnikuupäev	Kodakondsus	Ametinimetus	Kuupalk	Perekonnaseis
Töötaja – Iseenda	E-mail	x	x	x	x	x	x	x	x	x	x	x	x	x
Töötaja – Iseenda	Süstee m 2	x	x					x				x	x	
Töötaja – Iseenda	Süstee m 34	x	x	x	x	x	x	x	x	x	x	x	x	x

Tabelis 4 on ette näidatud kõik andmesubjekti „Töötaja – Iseenda“ andmeatribuudid, mis töödeldakse äriprotsessi „Töötase ülevaatamine“ puhul süsteemi 2 ning süsteemi 34 raames. Praktikas see tähendab järgmist: süsteemi 2 raames töödeldakse andmesubjekti „Töötaja – Iseenda“ ainult ees- ja perekonnanime, e-posti aadressi, ametikohta ning töötasu arvu. Kusjuures tabelist 3 me teame, et töötlemise tüüp süsteemi 2 puhul on ainult „lugemine“.

Autor sisestas saadud andmeatribuudid ühte „protsesside inventuuri“ faili, kus on kaardistatud ettevõtte X kõik teised äriprotsessid. Seega äriprotsessi „Töötasu ülevaatamine“ inventuur edukalt lõppes.

6 Kasutavate süsteemide riskianalüüsi läbiviimine

Ettevõttes X on kokku kasutusel 34 süsteemi, millest 20 nimetavad võtmeisikud ärikriitilisteks.

Võtmeisikud peavad ärikriitiliseks sellist süsteemi, mille mittetöötamise puhul ei saa ettevõte X jätkata oma igapäevast tööd.

6.1 Küsimustiku koostamine

Riskianalüüsi läbiviimiseks otsustas autor kasutada „küsimustiku“ meetodit. Seega oli algselt vaja luua vastav küsimustik.

Oli vaja teha otsus, milliseid parameetreid küsimustik mõõtma hakkab ning mille alusel hiljem riskianalüüsi läbi viia.

Nendeks parameetriteks said:

1. Süsteemi vastavus;
   Parameeter osutus valituks, sest GDPR määrus kirjeldab norme, millele ettevõttes kasutatavad süsteemid peavad vastama. Vastavuse parameeter võeti GDPR määruses esinevaid tehnilisi näitajaid tõlgendades.
2. Süsteemi keerukus.
   Keerukuse parameeter saadi analüüsides süsteemiga seotud ning arendustegevust mõjutavaid näitajaid. Motivatsioon keerukuse mõistmiseks lähtub vajadusest mõista muudatuste keerukust ning mõju, mis nendel muudatustel on tegevustele ja kuludele.

   Küsimuste koostamiseks pöördus autor audiitorfirma Z poole. Üheskoos audiitorfirma kahe töötajaga valmisid peale üldiste küsimuste veel 7 küsimust mõõtmaks süsteemi vastavust ning 6 küsimust mõõtmaks süsteemi keerukust. Küsimused koostati valikvastustega. Iga vastus annab 1-4 punkti, millest lõpuks

kujuneb üldine skoor. Mida riskantsem on vastuse iseloom, seda rohkem punkte ta annab.

6.1.1 Süsteemide vastavus

Süsteemi vastavuse mõõtmiseks peab läbi käima seitse GDPR määruses kirjeldatud näitajat.

1. Nõusoleku haldamine
   Antud kriteerimumi all mõeldakse nõusolekute kogumise ja haldamise tehnilistele nõuetele vastavuse mõõtmist, et võtta arvesse nõusolekute kogumist, kasutamist, avalikustamist ja tühistamist. [1]
   Selle kriteeriumi jaoks mõeldi välja järgnev küsimus: „Kuidas süsteemi/rakenduse puhul hallatakse nõusolekuid?“ (Vt. lisa 1)

Vastusevariandid:

- A – Madal (1 punkt): Süsteemil/rakendusel on olemas võimekus, et hallata nõusolekuid (või väljastada nõusolekutaotlusi) ja toetab nõusolekute tühistamist, mida saab teha automaatiseeritult/digitaalselt.

- B – Keskmine (2 punkti): Süsteemil/rakendusel on olemas võimekus, et hallata nõusolekuid ja toetada nõusolekute tühistamist, kuid läbi manuaalsete/alternatiivsete lahenduste.

- C – Kõrge (3 punkti): Süsteemil/rakendusel on limiteeritud võimekus nõusolekute haldamiseks ning see ei toeta kerget nõusolekute tühistamist. Need ei pruugi olla kergesti kättesaadavad.

- D – Väga kõrge (4 punkti): Süsteemil/rakendusel puudub võimekus või funktsionaalsus nõusolekute haldamiseks või nõusolekute tühistamiseks.

2. Andmete teisaldatavus
   Andmete teisaldatavus mõõdab vastavust nõuetele, mis täpsustavad tehnilist võimekust platvormilt (ja seotud seadmetest) isikuandmete saamiseks struktureeritud, üldkasutataval ja masinloetavas formaadis. Nende nõuete hulka kuulub ka tehniline võimekus neid andmeid teistele töötlejatele edastada. [1]

Andmete teisaldatavuse mõõtmiseks mõeldi välja järgnev küsimus: „Kas andmesubjekti soovil on võimalik andmeid liigutada ning kui jah, siis mis formaadis?“ (Vt. lisa 1)

Vastusevariandid:

- A – Madal (1 punkt): Süsteem/rakendus lubab andmesubjektidel oma andmeid liigutada struktureeritud, üldkasutatavas ja masinloetavas formaadis ja toetab isikuandmete liigutamist otse teistele töötlejatele (nt üle API).
- B – Keskmine (2 punkti): Süsteem/rakendus võimaldab osade isikuandmete teisaldamist teisele töötlejale, kui mittestruktureeritul kujul ning andmesubjektid võivad taotleda oma andmete kopeerimist.
- C – Kõrge (3 punkti): Süsteem/rakendus ei luba isikuandmete liigutamist, kuid andmesubjektid võivad taotleda oma andmete kopeerimist.
- D - Väga kõrge (4 punkti): Süsteem/rakendus ei luba isikuandmete liigutamist ja süsteem ei luba andmesubjektidel taotleda oma andmete kopeerimist.

3. Säilitamine ja kustutamine
   Kriteerium „säilitamine ja kustutamine“ mõõdab vastavust nõuetele, mis täpsustavad andmete säilitamise tingimusi ning tehnilist võimekust andmete (automaatseks) kustutamiseks peale säilitamistähtaja lõppemist ja isikuandmete hankimist süsteemist ning juhtumipõhist kustutamist. [1]
   Kriteeriumi „säilitamine ja kustutamine“ mõõtmiseks mõeldi välja järgnev küsimus: „Kuidas süsteemis andmeid kustutatakse, kas see on dokumenteeritud ning kas see on korratav protsess?“ (Vt. lisa 1)

Vastusevariandid:

- A – Madal (1 punkt): Süsteem/rakendus suudab andmed kustutada kohe, kui töötlemine on lõpetatud ja/või ei salvesta isiklikku informatsiooni.
- B – Keskmine (2 punkti): Süsteem/rakendus suudab andmeid kustutada ükskõik millistele kindlaks määratud säilitusnõuetele vastavalt, kuid see protsess ei ole automatiseeritud ning peab toimuma manuaalselt.

- C – Kõrge (3 punkti): Süsteem/rakendus säilitab andmeid määramata ajaks, kuigi andmeid kustutatakse „ad hoc“ alusel.

- D – Väga kõrge (4 punkti): Süsteem/rakendus ei ole võimeline andmeid kustutama.

4. Andmete ligipääs ja parandamine
   Kriteerium „andmete ligipääs ja parandamine“ mõõdab vastavust nõuetele, millega määratakse funktsionaalsed nõuded, kuidas isikutel on võimalik oma infole ligi pääseda. Sellega on lähedalt seotud isikute õigus valesid andmeid parandada ning põhjendatult taotleda loata omandatud, ebavajalike või valede andmete kustutamist. Seda aga välja arvatud teatud erandjuhtudel. [1]
   Kriteeriumi „andmete ligipääs ja parandamine“ mõõtmiseks mõeldi välja järgnev küsimus: „Kas andmesubjektidel on võimalik oma andmetele ligi pääseda ning neid kustutada?“ (Vt. lisa 1)

Vastusevariandid:

- A – Madal (1 punkt): Andmesubjektid pääsevad oma andmetele ligi ning saavad andmeid uuendada, kui tegemist on valeinfoga.

- B – Keskmine (2 punkti): Andmesubjektidel on ligipääs vaid osale oma infost ning nad saavad taotleda andmete uuendamist, kui info on ebakorrektne, kuid neil pole võimalik andmeid ise muuta.

- C – Kõrge (3 punkti): Andmesubjektidel pole otsest ligipääsu oma andmetele, kuid neil on võimalik taotleda oma andmetele ligipääsu ning ka nende muutmist kui nende kohta käiv info on ebakorrektne. Seejuures on aga ebaselge, kuidas Ettevõte X selliseid taotluseid õigeaegselt täidaks.

- D – Väga kõrge (4 punkti): Andmesubjektidel ei ole ligipääsu oma andmetele ning neil ei ole mingit võimalust taotleda ligipääsu või parandusi oma andmetele.

5. Andmete kasutamine ja eraldamine
   Kriteerium „andmete kasutamine ja eraldamine“ mõõdab vastavust pseudonüümsusega, et võimaldada andmete kasutamine ja kasulikkus. Määrus nimetab pseudonüümsust kui võimalust kaitsta indiviidide õigusi samaaegselt andmete kasutamisega. Andmete kogumiku pseudonüümseks muutmiseks peab

“lisainformatsiooni” hoidma “eraldi ja tehnilise ning organisatsioonilise kontrolli all, et tagada tuvastatud või tuvastamata inimese kätte sattumist”. [1]

Kriteeriumi „andmete kasutamine ja eraldamine“ mõõtmiseks mõeldi välja järgnev küsimus: „Mil määral on kasutatud pseudonüümsust või muid tehnikaid et vähendada andmete töötlemisega seotud riske, säilitades samaaegselt andmete kasutatavus?“ (Vt. lisa 1)

Vastusevariandid:

- A – Madal (1 punkt): Andmetega kasutatakse alati pseudonüümsust või andmed on varjatud viisil, kus otseselt tuvastatavad andmed on hoitud turvaliselt eraldatuna töödeldavatest andmetest, et tagada andmete lekkimist. Nendele pääsevad ligi/neid kasutavad ainult professionaalid Euroopa Majanduspiirkonna (EMP) riikidest.

- B – Keskmine (2 punkti): Andmetega kasutatakse pseudonüümsust või neid varjatakse ning varjatud andmetele pääsevad ligi või neid kasutavad professionaalid Euroopa Majanduspiirkonna (EMP) riikides ja ka väljaspool EMP keskkondi (tootmine ja arendamine).

- C – Kõrge (3 punkti): Andmetega kasutatakse pseudonüümsust või varjamist ainult arenduskeskkonnas ja sellele pääsevad ligi/seda kasutavad professionaalid Euroopa Majanduspiirkonna (EMP) riikides ja väljaspool EMP-i.

- D – Väga kõrge (4 punkti): Ei kasutata mingeid tehnikaid, mis vähendaksid andmete töötlemisega seotud riske või mingid tehnikad siiski eksisteerivad, kuid neid ei testita ja need ei pruugi vastata regulatsioonidele.

6. Andmete kvaliteet

   „Andmete kvaliteedi“ kriteeriumi all mõeldakse vastavuse mõõtmist nõuetele mõõtes andmete minimaliseerimist ja täpsust. GDPR määrus nõuab, et andmed oleksid (a) adekvaatsed, ajakohased ja piirduvad sellega, mis on nende eesmärk, mille jaoks neid töödeldakse (“andmete minimaliseerimine”); (b) isikuandmete puhul on tagatud õigsus ning ajakohasus ja on võetud iga mõistlik samm, et tagada andmete täpsus ning võetakse arvesse eesmärke, mille jaoks neid andmeid töödeldakse, kustutatakse või viivitamatult parandatakse (“täpsus”). [1]

„Andmete kvaliteedi“ kriteeriumi mõõtmiseks mõeldi välja järgnev küsimus: „Milliseid meetmeid süsteemis/rakenduses kasutatakse, et tagada andmete piisav kvaliteet?“ (Vt. lisa 1)

Vastusevariandid:

- A – Madal (1 punkt): Süsteemil/rakendusel on olemas protsessid ja funktsionaalsus, mis tagavad andmete täpsuse ja vajadusel ajakohasuse, usaldusväärsuse ja terviklikkuse. Süsteemis on olemas automaatsed protsessid, mis tagavad andmete olulisuse ja määravad, et andmed on kohased eesmärkidele, mille jaoks neid töödeldakse.

- B – Keskmine (2 punkti): Süsteemil/rakendusel on olemas manuaalsed protsessid, mis tagavad andmete täpsuse, terviklikkuse ja vajalikkuse ning piiratuse, olemas kohased eesmärkidele, mille jaoks neid töödeldakse.

- C – Kõrge (3 punkti): Süsteemil/rakendusel ei ole defineeritud protsesse või funktsionaalsust, mis tagaksid andmete vastavuse kvaliteedinõuetele, kui kvaliteeti kontrollitakse juhuslikult või vastavalt vajadusele.

- D – Väga kõrge (4 punkti): Andmete kvaliteedistandardeid ei ole rakendatud või arvesse võetud; ei eksisteeri mingeid mehhanisme või protsesse (defineeritud või vajadusepõhiseid).

7. Andmekaitse

   „Andmekaitse“ kriteeriumi all mõeldakse vastavuse mõõtmist administratiivsetele, tehnilistele või turvalisuse kontrollidele, mis peaksid olema süsteemi/rakendusse integreeritud, et takistada autoriseerimata või juhuslikku isikuandmete kadu, andmelaostust või avaldamist. [1]

   „Andmekaitse“ kriteeriumi mõõtmiseks mõeldi välja järgnev küsimus: „Kuidas on andmekaitse ja turvalisuse kontrolli meetodid süsteemis/rakenduses kaitstud?“ (Vt. lisa 1)

Vastusevariandid:

- A – Madal (1 punkt): Andmekaitse/turvakontrollid on süsteemi/rakendusse sisse ehitatud, et kaitsta isikuandmeid ja andmete terviklikkust; eksisteerivad auditeerimiste logimise protseduurid ning andmete krüpteerimine on võimalik.

- B – Keskmine (2 punkti): On olemas mõned andmekaitse/turvalisuse kontrolli meetmed, et kaitsta isikuandmeid ning andmete terviklikkust; olemas on auditeerimiste logimise protseduurid, kuid ei ole kindel, kui tihti logisid jälgitakse või kas krüpteerimine on võimalik.

- C – Kõrge (3 punkti): On väga vähe või pole üldse andmete kaitset/turvalisuse kontrolle, nt krüpteerimist ja turvalist suhtlemist ning logide ülevaatus tehakse juhuslikult.

- D – Väga kõrge (4 punkti): Puudub korralik andmekaitse/turvalisuse kontroll, nagu näiteks krüpteerimine ja turvaline kommunikatsioon, logisid ei jälgita.

6.1.2 Vastavuse riskimaatriks

Süsteemi vastavuse riskitaseme määratlemiseks lõi autor järgmise gradatsiooni:

- 1,0-1,74 punkti ehk madal risk – süsteemil/rakendusel on vähe või pole üldse mingeid funktsionaalsusi või kontrollkohti ning see vastab GDPR määruse tehnilistele nõuetele funktsionaalsuse ja turvakontrollide kohta.

- 1,75-2,49 punkti ehk keskmine risk – süsteemil/rakendusel puudub mõningane funktsionaalsus/turvalisus ning on loodud alternatiivseid tööviise, et manuaalsed protsessid vastaksid tehnilistele nõuetele.

- 2,5-3,24 punkti ehk kõrge risk – süsteemil/rakendusel puudub suur osa funktsionaalsusest ja turvalisusest, mis tagaksid vastavuse GDPR määruse tehnilistele nõuetele.

- 3,25-4,0 punkti ehk väga kõrge risk – süsteemil/rakendusel puudub peaaegu kogu funktsionaalsus ja turvalisus, et vastata GDPR määruse tehnilistele nõuetele.

6.1.3 Süsteemide keerukus

Süsteemi keerukuse taseme mõõtmiseks said kirja pandud kuus kriteeriumi.

1. Süsteemi välised sõltuvused

   Antud kriteeriumi abil toimub teostatavuse ja teistest süsteemidest/rakendustest sõltuvuse suuruse mõõtmine. Kui süsteem on tihedalt seotud paljude teiste süsteemidega, siis on väga raske seda süsteemi asendada, integreerida või muuta.

   „Süsteemi väliste sõltuvuste“ kriteeriumi mõõtmiseks mõeldi välja selline: „Kas süsteem/rakendus on seotud või sõltuv teistest süsteemidest ja/või rakendustest?“ (Vt. lisa 1)

Vastusevariandid:

- A – Madal (1 punkt): Süsteem/rakendus on suletud ja ei ole seotud ühegi teise süsteemiga.
- B – Keskmine (2 punkti): Süsteem/rakendus on seotud teiste süsteemidega, aga seda seotust saab eemaldada.
- C – Kõrge (3 punkti): Süsteem/rakendus on seotud paljude teiste süsteemidega ja mittesidumine on raskendatud ning uuendused mõjutaksid teisi süsteeme.
- D – Väga kõrge (4 punkti): Süsteem/rakendus on seotud teiste süsteemiga ning on ebatõenäoline, et lahti sidumine on võimalik.

2. Süsteemi sisemised sõltuvused

   Antud kriteerium mõõdab lahutatavust ja sisemiste süsteemide/alamsüsteemide omavahelist sõltuvuse suurust.

   Selle kriteeriumi mõõtmiseks mõeldi välja järgnev küsimus: „Kas süsteem/rakendus sõltub sisemistest komponentidest/alamsüsteemidest?“ (Vt. lisa 1)

Vastusevariandid:

- A – Madal (1 punkt): Süsteem/rakendus on tehtud lõdvalt ühendatud komponentidest, mida on võimalik kergelt lahti ühendada/asendada.
- B – Keskmine (2 punkti): Süsteem/rakendus on tehtud sõltuvuses olevatest komponentidest, mida on võimalik lahti ühendada/asendada.

- C – Kõrge (3 punkti): Süsteem/rakendus on tehtud tihedalt seotud komponentidest, mida on võimalik raskustega lahti ühendada/asendada.

- D – Väga kõrge (4 punkti): Süsteemi/rakenduse arhitektuur on väga tihedalt omavahel seotud ehk see pole loodud mõttega neid osasid lahti ühendada.

3. Lepingu piiravus

   Antud kriteeriumi all mõeldakse lepingu paindlikkuse mõõtmist muudatuste, lepingu lõpetamise ja pikendamise osas. GDPR määrus seab andmete töötlejatele kindlad nõuded. Organisatsioonidel võib olla vaja olla uuesti läbi rääkida lepingud kolmandate osapooltega, et nõuetele vastata. Kui lepingut ei saa muuta nõuetele vastavaks/disaininõudeid arvestavaks, siis luuakse ettevõttele X väga suur vastutus. [1]

   Selle kriteeriumi mõõtmiseks mõeldi välja järgnev küsimus: „Kui paindlik on süsteemi/rakenduse lepingu struktuur?“ (Vt. lisa 1)

Vastusevariandid:

- A – Madal (1 punkt): Süsteemi/rakendusega seotud leping lõpeb või on muutuste jaoks paindlik.

- B – Keskmine (2 punkti): Süsteemi/rakendusega seotud lepinguid on võimalik muuta, kuid lepingumuudatusega on seotud trahvid, ärilised riskid või lisakulud.

- C – Kõrge (3 punkti): Süsteemi/rakendusega seotud leping(ud) on väga piiravad ning seda on väga raske lõpetada ja/või parandada, aga neid saab uurida.

- D – Väga kõrge (4 punkti): Süsteemi/rakendusega seotud leping(ud) ei ole paindlikud. Äril ei ole võimalik muutuda või sellest lepingust vabandada GDPR määruse jõustumise ajaks.

4. Dokumentatsiooni kättesaadavus

   Selle kriteeriumi all mõeldakse ettevõtte X võimekuse mõõtmist, et kiiresti sisse viia muudatusi või välja tuua uuendusi vastavalt hästi dokumenteeritud süsteemi informatsioonile, protseduuridele ja teadmistele.

   Selle kriteeriumi mõõtmiseks mõeldi välja järgnev küsimus: „Kas süsteemil on asjakohane dokumentatsioon selle kohta, kuidas süsteem/rakendus töötab (sh

arhitektuuridiagrammid, spetsifikatsioonid, riskianalüüs ja muud dokumendid)?“ (Vt. lisa 1)

Vastusevariandid:

- A – Madal (1 punkt): Süsteemil/rakendusel on hästi struktureeritud ja piisav dokumentatsioon. Lisaks on ka süsteem, et hallata süsteemiga seotud teavet selle seostamisel süsteemi arenduse, üleval hoidmise ja operatsiooniga.

- B – Keskmine (2 punkti): Süsteemil/rakendusel on mõningane dokumentatsioon olemas või selline dokumentatsioon on arenduses, mis seostub süsteemi arenduse, üleval hoidmise ja operatsioonidega.

- C – Kõrge (3 punkti): Süsteemil/rakendusel on väga limiteeritud dokumentatsioon, mis seostub süsteemi arenduse ja üleval hoidmisega ja/või selline dokumentatsioon on aegunud.

- D – Väga kõrge (4 punkti): Süsteemil/rakendusel puudub dokumentatsioon, mis seostuks süsteemi arenduse, üleval hoidmise ja operatsioonidega ning piiratud ülekantavate teadmistega süsteemist.

5. Ressursside kättesaadavus

   Kriteerium „ressursside kättesaadavus“ mõõdab ettevõtte X võimekust, et kasutada piisavat ressursilist tuge süsteemi arenduse ja operatsioonide jaoks. Süsteemi rahuldavaks muutmiseks, uuendamiseks, integreerimiseks või asendamiseks on vaja rahuldavat tugimeeskonda.

   Selle kriteeriumi mõõtmiseks mõeldi välja järgnev küsimus: „Kas rakendusel on olemas piisavad ressursid selle rakenduse toetamiseks (arendus, operatsioonid, üleval hoidmine)?“ (Vt. lisa 1)

Vastusevariandid:

- A – Madal (1 punkti): Süsteemil/rakendusel on täielik meeskond, millel on spetsiaalsed ressursid ja/või ressursside kogum, mis toetab süsteemi igapäevaselt.

- B – Keskmine (2 punkti): Süsteemil/rakendusel on meeskond või vajadusel valmis olev kontakt, kes saavad vajadusel teha süsteemiuuendusi, kuid ei ole kedagi, kes oleks spetsiaalselt pühendunud või on see pidevas muutumises.

- C – Kõrge (3 punkti): Süsteemil/rakendusel on piiratud tugi ja vajalike ressursside saamiseks on vaja aega.

- D – Väga kõrge (4 punkti): Süsteemil/rakendusel ei ole määratud omanikku või ressursside kogumit, mis oleks abiks süsteemi toetamisele.

6. Uuenduste sagedus
   Kriteerium „uuenduste sageduse“ all mõeldakse süsteemi paindlikkuse ja stabiilsuse mõõtmist uuenduste välja laskmise ajal. Süsteemile, millele tehakse regulaarseid ja sagedasi uuendusi, on lihtsam teha muudatusi.
   Selle kriteeriumi mõõtmiseks mõeldi välja järgnev küsimus: „Kui tihti tehakse süsteemi/rakenduse uuendusi?“ (Vt. lisa 1)

Vastusevariandid:

- A – Madal (1 punkt): Süsteemi/rakenduse uuendusi tehakse tihti ning õigeaegselt.

- B – Keskmine (2 punkti): Süsteemi/rakenduse uuendusi tehakse järjepidevalt, kuid vajalikke muudatusi on terve nimekiri.

- C – Kõrge (3 punkti): Süsteemi/rakenduse uuendusi ei tehta tihti ning vajalikke muudatusi on terve nimekiri.

- D – Väga kõrge (4 punkti): Süsteemi/rakenduse muudatusi tehakse vastavalt vajadusele ja ette planeerimata ning vajalikke muudatusi on terve nimekiri.

6.1.4 Keerukuse riskimaatriks

Süsteemi keerukuse riskitaseme määratlemiseks arendas autor järgmise gradatsiooni välja.

- 1,0-1,74 punkti ehk madal risk – süsteemil/rakendusel on dünaamiline arhitektuur, mis on väga paindlik ning mis laseb teha vajalikke muudatusi.

- 1,75-2,49 punkti ehk keskmine risk – süsteemil/rakendusel on vähe arhitektuurilisi sõltuvusi ning piirav paindlikkus, kuid neid on võimalik adresseerida ning nad on leevendatavad, kui ilmneb vajadus muudatusteks.

- 2,5-3,24 punkti ehk kõrge Risk – süsteemil/rakendusel on mitmeid arhitektuurilisi või paindlikkuse piiranguid, mis loovad mitmeid takistusi juhtudel, mil muudatused on vajalikud.

- 3,25-4,0 punkti ehk väga kõrge risk – süsteemil/rakendusel on keeruline arhitektuur, mis ei ole piisavalt paindlik, et lubada ettevõttel X teha muudatusi GDPRi nõuetele vastamiseks.

6.1.5 Küsimustiku laiali saatmine

Koostatud küsimustik on toodud välja Lisas 1 ning saadeti kõikidele võtmeisikutele. Võtmeisikuid oli kokku 11 inimest.

Küsitluse läbiviimiseks valmistas autor ette Exceli faili kõikide väljamõeldud küsimustega ning lisas lahtrid vastusevariantide jaoks.

Küsimustikus paluti võtmeisikutel hinnata igat kasutatavat süsteemi, mida nad tegid vastates valikvastustega küsimustele. Iga süsteemi kohta vastas ainult üks võtmeisik.

Küsitlusest võtsid osa kõik 11 inimest. Omavahel lepiti kokku, kes millist süsteemi hindab. Neile isikutele oli saadetud küsimustikuga Exceli fail ning antud nädal aega selle täitmiseks.

Pärast kõikide täidetud ankeetide kättesaamist, sisestas autor käsitsi kõik tulemused ühte Excel faili, millest kujunes tabel kõikide süsteemide riskihinnangutega.

Järgmine punkt kirjeldab detailselt riskihinnangu määratlemist võtmeisikutelt saadud tulemuste alusel ühe süsteemi näitel.

6.2 Kasutavate süsteemide riskihinnangu läbiviimine (ühe süsteemi näitel)

Ettevõttes X kasutatakse igapäevaselt 34 infosüsteemi. Nende seas on nii sisesed kui ka välised rakendused. Süsteemid on jagatud kahte suurte gruppi – ärikriitilisteks ja mitteärikriitilisteks. Nimekiri süsteemide jagamisest oli ette antud ettevõtte X võtmeisikute poolt.

Riskihinnangu käigu demonstreerimiseks valis autor sisese mitteärikriitilise HR süsteemi. Järgnevalt on näidatud küsimustele vastamise protsess valitud süsteemi kohta.

Süsteemi nr: 34

Süsteemi tüüp: Sisemine

Ärikriitiline või mitte: Mitte

Süsteemi kirjeldus: keskkond personaliosakonnale ja ettevõtte töötajatele. Töötaja saab näha enda informatsiooni, töötunde, esitada puhkuseavaldust, panna kirja aega kontorist väljas olemiseks, küsida luba reisimiseks. Juhtkonna jaoks sisaldab see tiimiinformatsiooni (palgad, puhkused jne). Samuti võimaldab palgaarvutusi ja –makseid.

Allolevas tabelis on toodud võtmeisiku vastused süsteemi 34 vastavuse parameetri kohta.

Tabel 5 Süsteemi 34 vastavuse skoor.

Nõusoleku haldamine	Andmete teisaldatavus	Säilitamine ja kustutamine	Andmete ligipääs ja parandamine	Andmete kasutamine ja eraldamine	Andmete kvaliteet	Andmekaitse		
K30	K31	K32	K33	K34	K35	K36	Vastavuse skoor	Vastavuse risk
D	B	B	B	C	D	A	2,57	Kõrge

Nagu Tabelist 6 on näha, hindas võtmeisik nõusoleku haldamise kriteeriumi „D“ ehk kõige kõrgema (mitterahuldava) hindega. See tähendab, et süsteemil 34 puudub võimekus või funktsionaalsus nõusolekute haldamiseks või nõusolekute tühistamiseks. See andis kohe süsteemile 4 punkti. Sellised kriteeriumid nagu „andmete teisaldatavus“, „säilitamine ja kustutamine“ ning „andmete ligipääs ja parandamine“ hindas võtmeisik hindega „B“, mis andis süsteemile 34 veel 2*3=6 punkti. „Andmete kasutamine ja eraldamine“ kriteeriumi eest sai süsteem „C“ ehk 3 punkti, moodustades eelmiste hinnetega summa 13. Kõige halvema hinde ehk „D“ sai Süsteem 34 samuti ka „andmete kvaliteedi“ kriteeriumi eest, mis lisas üldskoorile veel 4 punkti. „Andmekaitse“ kriteerium oli väga hästi hinnatud hindele „A“, mis kokku andis süsteemile 18 punkti. Võttes üldsumma ning peale kriteeriumite summa lahutamist saadi kätte 18/7~2,57 punkti, mis moodustabki antud süsteemi vastavuse skoori. Tegemist on kõrge hinnanguga.

Allolevas tabelis on ette antud võtmeisiku vastused Süsteemi 34 keerukuse parameetri kohta.

Tabel 6 Süsteemi 34 keerukuse skoor.

Välised sõltuvused	**Sisemised sõltuvused**	**Lepingu piiravus**	**Dokumentatsiooni kättesaadavus**	**Ressursside kättesaadavus**	**Uuenduste sagedus**		
K18	**K25**	**K26**	**K27**	**K28**	**K29**	**Keerukuse skoor**	**Keerukuse risk**
D	D	D	A	A	A	2,50	Kõrge

Tabelist 6 on näha, et võtmeisik on hinnanud hindega „D“ ehk kõige kõrgema (mitterahuldava) hindega järgmised kriteeriumid: „välised sõltuvused“, „sisemised sõltuvused“ ning „lepingu piiravus“. See andis kohe süsteemile 3*4=12 punkti. Ülejäänud kolm kriteeriumi „dokumentatsiooni kättesaadavus“, „resursside kättesaadavus“ ning „uuenduste sagedus“ võtmeisik hindas hindele „A“, mis andis süsteemile 34 vaid 3*1=3 punkti. Kokku kogus süsteem küsitluse käigus 15 punkti, mis tähendab seda, et selle aritmeetiline keskmine võrdub 15/6=2,5 punkti, mis moodustabki

antud süsteemi keerukuse skoori ning mis on samuti kõrge nagu oli skoor ka vastavusega.

Kuna süsteemi 34 kohta läbi viidud küsitlusest selgus, et selle vastavuse ja keerukuse riskitasemed on kõrged, siis saab järeldada, et see süsteem peab olema prioriteetne ning selle jaoks peab tegema plaani vähendamaks riske nõuetega mittevastavuste jaoks. Nendel süsteemidel võivad puududa mõned funktsionaalsused ja turvakontrollid, mis seavad mõningaid väljakutseid, kuid neid tuleb hallata õigete plaanidega. Sellega on süsteemi nr 34 riskihinnang lõppenud.

6.3 Ettevõttes X kasutatavate süsteemide riskianalüüsi tulemused

6.3.1 Küsitluse tulemuste töötlemine

Pärast seda, kui küsitlus sai läbi viidud ning kõik tulemused võtmeisikutelt tagasi saadud, sisestas autor käsitsi kõik saadud tulemused ühte Excel faili, mille käigus kujunes tabel kõikide süsteemide riskihinnangutega.

Tabel 7 Ettevõtte X kasutatavate süsteemide riskihinnangud keerukuse ja vastavuse parameetri järgi.

Süsteem	Keerukuse skoor	Keerukuse risk	Vastavuse skoor	Keerukuse risk	Üldskoor	Süsteemi riskihinnang
Süsteem 1	3,00	Kõrge	3,43	Väga kõrge	6,43	Kõrge
Süsteem 2	1,67	Madal	1,00	Madal	2,67	Madal
Süsteem 3	3,00	Kõrge	3,00	Kõrge	6,00	Kõrge
Süsteem 4	3,25	Väga kõrge	2,67	Kõrge	5,92	Kõrge
Süsteem 5	3,00	Kõrge	2,80	Kõrge	5,80	Kõrge
Süsteem 6	2,33	Keskmine	3,29	Väga kõrge	5,62	Kõrge
Süsteem 7	2,60	Kõrge	3,00	Kõrge	5,60	Kõrge
Süsteem 8	2,60	Kõrge	2,86	Kõrge	5,46	Kõrge
Süsteem 9	2,60	Kõrge	2,60	Kõrge	5,20	Kõrge
Süsteem 10	2,50	Kõrge	2,57	Kõrge	5,07	Kõrge
Süsteem 11	1,83	Keskmine	3,17	Kõrge	5,00	Kõrge
Süsteem 12	3,00	Kõrge	2,00	Keskmine	5,00	Kõrge
Süsteem 13	2,00	Keskmine	2,86	Kõrge	4,86	Keskmine
Süsteem 14	2,25	Keskmine	2,60	Kõrge	4,85	Keskmine
Süsteem 15	2,20	Keskmine	2,57	Kõrge	4,77	Keskmine
Süsteem 16	2,50	Kõrge	2,20	Keskmine	4,70	Keskmine
Süsteem 17	1,83	Keskmine	2,71	Kõrge	4,54	Keskmine
Süsteem 18	2,00	Keskmine	2,50	Kõrge	4,50	Keskmine
Süsteem 19	1,80	Keskmine	2,67	Kõrge	4,47	Keskmine
Süsteem 20	2,17	Keskmine	2,29	Keskmine	4,46	Keskmine
Süsteem 21	2,00	Keskmine	2,25	Keskmine	4,25	Keskmine
Süsteem 22	1,83	Keskmine	2,40	Keskmine	4,23	Keskmine
Süsteem 23	1,83	Keskmine	2,40	Keskmine	4,23	Keskmine
Süsteem 24	1,83	Keskmine	2,40	Keskmine	4,23	Keskmine
Süsteem 25	2,20	Keskmine	2,00	Keskmine	4,20	Keskmine

Süsteem	Keerukuse skoor	Keerukuse risk	Vastavuse skoor	Keerukuse risk	Üldskoor	Süsteemi riskihinnang
Süsteem 26	2,33	Keskmine	1,60	Madal	3,93	Keskmine
Süsteem 27	2,00	Keskmine	1,75	Keskmine	3,75	Keskmine
Süsteem 28	1,83	Keskmine	1,83	Keskmine	3,66	Keskmine
Süsteem 29	1,17	Madal	2,00	Keskmine	3,17	Madal
Süsteem 30	1,00	Madal	2,00	Keskmine	3,00	Madal
Süsteem 31	1,50	Madal	1,50	Madal	3,00	Madal
Süsteem 32	1,00	Madal	2,00	Keskmine	3,00	Madal
Süsteem 33	2,60	Kõrge	3,50	Väga kõrge	6,10	Kõrge
Süsteem 34	2,57	Kõrge	2,50	Kõrge	5,07	Kõrge

Tabelis 7 on näidatud keerukuse ja vastavuse parameetrite tulemused kõikide (34) ettevõttes X kasutatavate süsteemide kohta. Iga arv (kas keerukuse skoori või vastavuse skoori reast) kujutab endast aritmeetilist keskmist tulemust vastava parameetri kõikide kriteeriumite eest (7 kriteeriumi vastavuse puhul ja 6 kriteeriumi keerukuse puhul – vt. punktid 6.1.1 ja 6.1.2).

Samuti on tabelis 7 eraldi välja toodud keerukuse ning vastavuse riskihinnangud, mille taseme määratluse printsiip on kirjeldatud punktis 6.1.4.

Rida üldskooriga tekkis süsteemi keerukuse ning vastavuse näitajaid liites. Vastavate riskihinnangute tasemed on kirjeldatud siin:

- madal riskihinnang – siia kuuluvad süsteemid, milliste vastavuse ja keerukuse näitajate summa võrdub 1 kuni 3,48;
- keskmine riskihinnang – siia kuuluvad süsteemid, milliste vastavuse ja keerukuse näitajate summa võrdub 3,49 kuni 4,98;
- kõrge riskihinnang – siia kuuluvad süsteemid, milliste vastavuse ja keerukuse näitajate summa võrdub 4,99 kuni 6,48;

- väga kõrge riskihinnang – siia kuuluvad süsteemid, milliste vastavuse ja keerukuse näitajate summa võrdub 6,49 kuni 8.

6.3.2 Süsteemide parandamise prioritiseerimise kaart

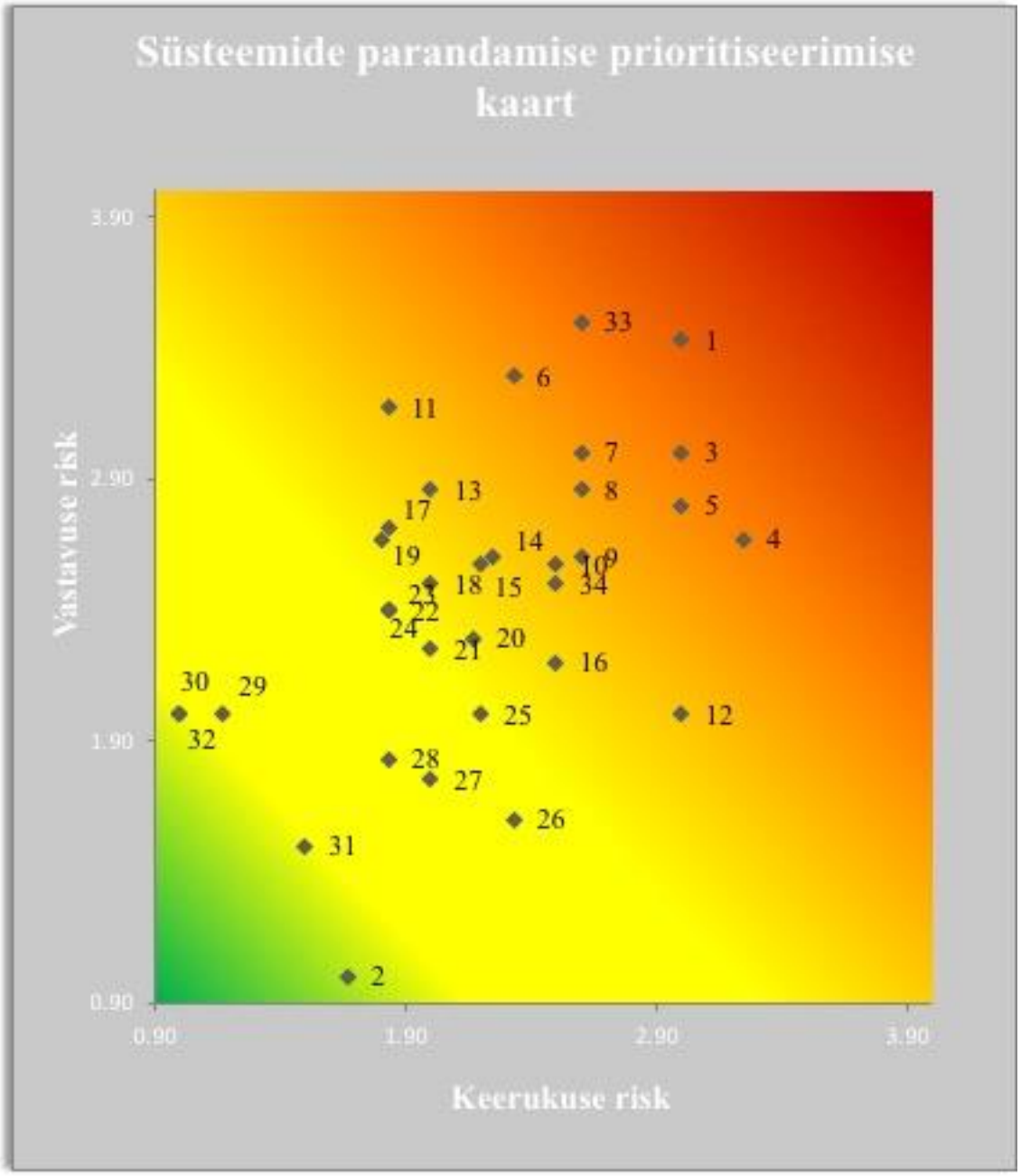
Paranduste prioritiseerimisest ülevaate saamiseks võeti riskidel põhinev lähenemine ning kombineeriti vastavuse ja keerukuse skoorid. Järgnevas tekstis on kujutatud vastavuse ja keerukuse riskiskoorid x/y telgedel, et näidata üldist riski ettevõttele X. Näiteks, kui süsteem ei ole eriti järeleandlik ning süsteemi arhitektuur ei ole üldse paindlik, see kõrgendab üldist riskitaset. Seda seetõttu, et süsteemile tehtavad muudatused saavad olema rasked, mis viib omakorda mittevastavuseni ning mis võib potentsiaalset ettevõttele X mõjuda halvasti.

Ettevõtte X IT osakonna juhatajaga kooskõlastamisel jõudis autor arvamusele, et süsteemi vastavuse ja keerukuse hinnangute summad tähendavad järgmist:

1. Madal Vastavuse risk + Madal Keerukuse risk = Süsteemid/rakendused, mille vastavuse ja keerukuse skoorid langevad allapoole rohelist koordinaati (vt. joonis 2), et oma mingit potentsiaalsed mõju või kahju ettevõttele X. Neid süsteeme ei peaks jälgima ettevõtte X vastavuse ja privaatsuse hindamise eeskirjades.
2. Keskmine Vastavuse risk + Keskmine Keerukuse risk = Süsteem/rakendus, mille vastavuse ja keerukuse skoorid langevad allapoole kollast koordinaati, vajab ainult plaani, et võimaldada ja kindlustada nõuetele vastavus. Nendel süsteemidel on mõningased funktsionaalsused või turvaaugud, kuid neid saab kergesti parandada.
3. Kõrge Vastavuse risk + Kõrge Keerukuse risk = Süsteemid/rakendused, mille vastavuse ja keerukuse skoorid langevad allapoole oranži koordinaati, peavad olema prioritiseeritud ning nõuavad plaani riskide vähendamiseks, et hallata mittevastavuse riski. Nendel süsteemidel puuduvad mõned funktsionaalsused ja turvakontrollid, kus võib muudatuste tegemisel esineda väljakutseid, kuid neid peab haldama piisava planeeringuga.
4. Väga Kõrge Vastavuse risk + Väga Kõrge Keerukuse risk = Süsteemid/rakendused, mille vastavuse ja keerukuse skoorid langevad allapoole punast joont, nõuavad kohest tähelepanu ja läbivaatust. Nendel süsteemidel puudub funktsionaalsus ja turvakontroll, et nõuetele vastata ning nende mittepaindlikus nõuetele vastavata

muudatuste tegemist osas on väga halb. Seega on neil suur potentsiaal mõjutada ja kahjustada ettevõtet X.

Peale küsitluse läbiviimist sai autor võtmeisikutelt kõik tulemused tagasi ning need kandis käsitsi ühte Exceli faili, mille järel töötles need ning koostas nende põhjal üldgraafiku nelja tsooniga.



Joonis 2 Ettevõttes X kasutatavate süsteemide parandamise prioritiseerimise kaart.

Riskide parandamise prioritiseerimise kaardilt on näha, et ainult süsteemid 2, 30, 31 ja 32 asuvad oma üldskoori näitajate järgi rohelises tsoonis ning see tähendab, et need ei oma mingit potentsiaalset mõju või kahju ettevõttele X ning et neid peaks jälgima vastavalt ettevõtte X vastavuse jälgimise ja privaatsuse hindamise eeskirjadega.

Vaatamata sellele, et vastavalt Tabelile 7 omavad süsteemid 13-28 kollast värvi ehk keskmist riskihinnangut, on neil riskide parandamise prioritiseerimise kaardil kardinaalselt erinevad positsioonid. Süsteemid 21-30 asuvad kollases tsoonis. Need süsteemid omavad mõningast funktsionaalsust ja turvaauke, kuid neid on kerge adresseerida. Nende parandamiseks ka nõuetele vastavaks muutmiseks on vaja ainult plaani. Ettevõtte X IT osakonna juhatajaga oli tehtud otsus mitte alustada hetkel kollases tsoonis asuvate süsteemidega, olenemata sellest, et nende süsteemide seas on ka ärikriitilisi süsteeme. Selline otsus tehti selleks, et võita aega kehvemate riskianalüüsi tulemustega süsteemide parandamiseks.

Süsteemid 13-20 kuuluvad juba nende süsteemide hulka, mis nõuavad suuremat tähelepanu. Need süsteemid peavad olema prioritiseeritud ning nõuavad plaani, et tegeleda mittevastavuse riskidega. Nagu on näha kaardilt ning Tabelist 7, siis neil süsteemidel on erineva tasemega keerukus, mida tuleb parandamise plaanide koostamisel arvesse võtta.

Süsteemid 1, 3-12, 33 ja 34 omavad samuti ühte värvi (punast) ehk kõrget riskihinnangut. Nende asukohad loodud kaardil on samuti erinevad. Süsteemid 5-12 ning 33 on saanud kõrge skoori vastavuse aukude osas, mida peaks koheselt adresseerima. Tänu nende süsteemide lisatud keerukusele peab ettevõte X analüüsima, kas neid süsteeme on võimalik asendada, kasutuselt kõrvaldada või vabastada kasutuses ettevõtte äri kergendamise jaoks. Mis tahes erand ja riski aktsepteerimine peab olema dokumenteeritud ning kontrollid rakendatud. Süsteemi 1, 3, 4 ja 33 on ärikriitilised ning neid peab parandama nii pea kui võimalik. Nende süsteemidega esineb olulisi väljakutseid, sest nende süsteemide GDPR määruse nõuetele vastavaks muutmine ei pruugi olla võimalik.

7 Järeldus

7.1 Kasutatud meetodite hinnang

7.1.1 Äriprotsesside inventuuri läbiviimismetoodika hinnang

Töö esimese eesmärgi saavutamiseks ehk ettevõtte X äriprotsesside inventuuri läbiviimiseks oli valitud meetod „intervjuu“.

Algul tundus see olevat parim valik. Valiti sellistest meetoditest: tööseminarid, ettevõttes eksisteerivate dokumentide uurimine, vaatluse ning küsimustike ja ankeetimise meetod.

Ettevõttes eksisteerivate dokumentide uurimismeetodist ning vaatluse meetodist tuli kohe loobuda, kuna need nõuavad teiste meetoditega võrreldes palju rohkem aega. Tööseminaride meetod on sama kiire kui intervjuu, aga nõuab paljude inimeste osalust, millega oleks takistatud valdkondade igapäevast tööd.

Vaatamata sellele, et küsimustike ja ankeetide meetod sai hinde 2/4, siis see oli siiski põhiliseks konkurendiks intervjuu meetodiga. Küsimustike meetodit rakendatakse laialt äriprotsesside inventuuri läbiviimiseks GDPR analüüsi raames, kuna see säästab analüütikute aega. Selle põhiliseks miinuseks oli kogu analüüsi kvaliteedi langus, kuna protsessi tähtsamad nüansid võivad jääda mainimata, sest vastaja võib pidada neid ebaolulisteks.

Nüüd, peale inventuuri läbiviimist ehk kõikide äriprotsesside kaardistamist võib autor järeldada, et targemaks lahenduseks antud juhul oleks olnud nende kahe meetodi (küsimustike ja intervjuu) kombineerimine.

Kuna enamikel äriprotsesside omanikel on haldamisel rohkem kui üks äriprotsess (mõnedel juhtudel kuni 10 protsessi), oleks õigemaks taktikaks viia läbi intervjuu, kus vaadeldakse ja kaardistatakse ühte protsessi koos intervjueerijaga ning hiljem protsesside omanik kaardistab kõik oma ülejäänud protsessid ise. Samal ajal täidaks ta protsessi inventuuri ja protsesside töötlemise vormi. Sellisel juhul protsessi omanik juba teab, millised protsessi nüansid peavad olema kindlasti kirja pandud ning kogu inventuuri kvaliteet ei lange.

7.1.2 Kasutatavate süsteemide riskianalüüsi läbiviimismetoodika hinnang

Kasutatavate süsteemide riskianalüüsi läbiviimiseks oli valitud kvalitatiivsete meetodite hulgast eksperthinnangute meetodi alammeetod – küsimustik. Valida tuli sellistest eksperthinnangute meetoditest nagu riskide roos ja spiraal ning Delfi meetod. SWOT-analüüs jäi kohe kõrvale, sest tarkvara riskianalüüs ei ole SWOT-analüüsi kasutusala.

Riskide roosi ja spiraali meetod ning Delfi meetod kõik põhinevad kõigepealt küsimustikul, kuid on selle keerulisemaks variandiks. Autor arvas, et selle konkreetse juhtumi kasutatavate süsteemide riskitaseme selgema pildi annab lihtne ühetasemeline võtmeisikute küsitlus ning nagu näitas riskianalüüs – autor ei eksinud.

Tavaline, korrektselt koostatud küsimustik, mis suudab mõõta süsteemi riskihinnangut kahe parameetri järgi, tõestas ennast hästi riskianalüüsi läbiviimismeetodina. Ei ole midagi, mida autor tahaks järgmine kord juurde lisada ega ära võtta – see on meetod on absoluutselt valmis ja usaldusväärne viis kvaliteetse riskianalüüsi läbiviimiseks.

7.2 Ettevõtte X edasised sammud GDPR määrusele vastavuseni jõudmiseks

GDPR määruse nõuetega vastavuses olek nõuab tehnoloogia, inimeste ja protsesside abi. GDPR määrus teeb organisatsioonid täielikult vastutavaks nõuetele vastavuse täitmise eest. See nõuab organisatsioonidelt dokumentide vastavust nõuetele, riskantsetele andmetöötlusprotsessidele andmekaitse testide tegemist ning läbi omaenda protsesside ja disaini andmekaitse implementeerimist.

Äriprotsesside inventuuri tulemuste edasine töötlemine

Omades kõigi äriprotsesside inventuuri ning täpselt teades, millistes protsessides milliste andmesubjektide ja milliseid andmeatribuute töödeldakse ning mismoodi see töötlemine toimub (lugemine, loomine, uuendamine, vaatlemine või edastamine), saab hakata tegelema isikuandmete hulga optimiseerimisega vastavalt GDPR määruse normidele.

GDPR määruse suureks plussiks on see, et ettevõtete jaoks on see ajend enda klientide ning töötajate isikuandmete töötlemise ümber vaatamisele. Ettevõtted on harjunud koguma suurt hulka enda klientide ja töötajate isikuandmeid ilma piisava põhjuseta

selleks, et neid kunagi mingis protsessis kasulikuks peetakse. Ettevõte X ei olnud antud juhul erandiks.

Praktikas paljusid isikuandmeid ettevõte enda igapäevaste äriprotsesside läbiviimiseks ei nõua. Samuti tekitab see lisaohtu isikuandmete ebakorrektseks töötlemiseks ning lekkeks.

Omades äriprotsesside inventuuri, peab ettevõtte X DPO analüüsima kõik äriprotsessid ning viima läbi uuringu, mille käigus vastatakse kolmele küsimusele iga äriprotsessi puhul:

1. Kas me vajame antud andmesubjekti isikuandmeid antud äriprotsessi realiseerimiseks?
2. Mis on antud andmesubjekti minimaalne vajalik andmeatribuutide komplekt antud äriprotsessi realiseerimiseks?
3. Millist tüüpi andmeatribuutide töötlemist peame rakendama antud äriprotsessi realiseerimiseks?

Selline lähenemine kärbib oluliselt töödeldud andmeatribuutide hulka kõikides äriprotsessides, mis lähendab ettevõtte X GDPR määrusele vastavusele.

Kasutatavate süsteemide riskianalüüsi tulemuste edasine töötlemine

Kasutatavate süsteemide riskianalüüsi tulemusi edastatakse ettevõtte X IT osakonna ärianalüütikutele, kelle põhiülesandeks on iga süsteemi kohta, mis jäid punasesse ning oranži tsooni, viia läbi uuring prioritiseerimise järjekorras. Selle jaoks tulevad neile kasuks küsimustiku tulemused, mis näitavad kriteeriumite kaupa, millised on süsteemi nõrgad ja tugevad küljed.

Uuringu eesmärgiks on määrata:

1. millistest kasutatavatest süsteemidest peab loobuma ning kas:
    - arendada uued süsteemid vastavalt GDPR määruse normidele (selle jaoks peavad ärianalüütikud koostama arendajate jaoks ärinõuded kasutades loodud küsimustikku riskianalüüsi läbiviimiseks);
    - või asendada olemasolevad süsteemid teiste sobilikumate süsteemidega (selle jaoks peavad ärianalüütikud viima läbi turul pakutavate süsteemide riskianalüüsi ning valima sobilikumad).

2. millised kasutatavad süsteemid võivad jääda ning vastata GDPR määruse normidele tingimusel, et neile saab tehtud parandustegevusi (selle jaoks peavad ärianalüütikud küsimustiku tulemuste alusel arendajate jaoks ette valmistama ärinõuded, mis täpselt kirjeldaksid, mis nendes süsteemides peab ära muutma).
   Pärast seda on kas ettevõtte X või tellitud tarkvarafirma arendajate ülesandeks teha ärianalüütikute koostatud nõuete järgi vajalikud toimingud süsteemide arendamise või asendamise suunas, mis äriprotsessides isikuandmete töötlemise optimiseerimise tulemusel viiksid ettevõtte X GDPR määrusele täiuslikult vastavaks

8 Kokkuvõte

Töö eesmärgiks oli läbi viia ettevõtte X äriprotsesside inventuur, et täita GDPR määruse 30. artiklis kirjeldatud nõue. Teine eesmärk oli viia läbi ettevõttes X kasutatavate süsteemide riskianalüüs, et selgitada välja, mis süsteemid hetkel ei vasta GDPR määruse normidele ja alustada süsteemide parandamist eesmärgiga 25. maiks 2018 saavutada nende normidele vastavus.

Enne äriprotsesside inventuuri läbiviimise alustamist tegi autor uuringu, mille eesmärgiks oli kõige sobilikuma metoodika leidmine. Uuringu käigus sai vaadeldud viit erinevat populaarset metoodikat: tööseminarid, küsimustikud ja ankeedid, ettevõttes olemasoleva dokumentatsiooni uurimine, vaatlus ja intervjuu. Autor tõi välja kõikide metoodikate eelised ja puudused ning hindas iga metoodikat eraldi. Kõige rohkem punkte sai „intervjuu“ meetod, millega oligi põhjendatud selle meetodi valik.

Enne kui asuti koostama kasutatavate süsteemide riskianalüüsi, viis autor läbi uuringu enamlevinud kvalitatiivsete meetodite kohta. Autor sai teada nende „hierarhiast“ ning seega esimeses „ringis“ vaatles ta selliseid kvalitatiivseid hindamismeetodeid nagu „eksperthinnangute meetod“, „allikate kontrollnimekirjade meetod“, „reitingu hindamise meetod“ ning „analoogi meetod“. Pärast meetodite eeliste ja puuduste väljatoomist sai selgeks, et ettevõtte X puhul sobib kõige rohkem just „eksperthinnangute meetod“, mis omakorda jaguneb veel selliseks neljaks alammeetodiks nagu „SWOT-analüüs“, „riskide roos ja spiraal“, „Delfi meetod“ ning „küsimustiku meetod“. „SWOT-analüüsi meetod“ jäi kõrvale, kuna tarkvara riskianalüüs ei ole selle kasutusala. Ülejäänud meetoditest sobis kõige rohkem „küsimustiku“ meetod, kuna antud juhul piisas lihtsast ühetasemelisest küsitlusest.

Omades valitud ja põhjendatud metoodikat äriprotsesside inventuuri läbiviimiseks asus autor protsesse kaardistama. Autor kirjeldas töös, kuidas toimub kaardistamise protsess, rakendades „intervjuu meetodit“. Samuti demonstreeris autor kaardistamise käiku äriprotsessi „töötasu ülevaatamine“ näitel. Järgmiseks etapiks oleks kõikide protsesside kohta saadud inventuuri analüüs eesmärgiga minimaliseerida andmesubjektide isikuandmete hulka iga äriprotsessi raames.

Töö eelviimane peatükk räägib küsimustiku loomisest riskianalüüsi läbiviimiseks. Küsimustik loodi koostöös audiitorfirmaga ning on ülesehitatud sellise printsiibi järgi, et mõõdab süsteemi vastavuse ja keerukuse parameetrit. Peale küsimustiku koostamist saatis autor selle laiali ettevõtte X kõikidele 11 võtmeisikule, kelle vastuste alusel määratati süsteemidele hiljem riskihinnangud. Samuti demonstreeris autor riskihinnangu määramise protsessi mitteärikriitilise süsteemi nr. 34 näitel, mis sai kõrge riskihinnangu.

Järgnevalt koostas autor võtmeisikutelt saadud küsitluse tulemuste põhjal ettevõttes X kasutatavate süsteemide riskide parandamise prioritiseerimise kaardi, mis selgelt näitas, et 21 süsteemi kogu hulgast ehk 34st ei vasta hetkel GDPR määruse normidele ning vajavad kas täiendamist või asendamist.

Töö järgmiseks etapiks oleks viia läbi uurimus, mille eesmärk oleks koostada ärinõuete loetelu süsteemide täiendamise kohta, et süsteemid vastaksid GDPR määruse normidele.

Kasutatud kirjandus

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

[2] T. Feehan, „The WP29 will become the EDPB – but what does that mean?," Interactive Advertising Bureau, 2016. [Võrgumaterjal]. Saadaval: https://www.iabeurope.eu/policy/data-protection/the-wp29-will-become-the-edpb-but-what-does-that-mean/. [Kasutatud 22 Veebruar 2018].

[3] „Article 29 Working Party," European Commission, 2016. [Võrgumaterjal]. Saadaval: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083. [Kasutatud 22 Veebruar 2018].

[4] С. М. Ковалев и В. М. Ковалев, «Методы сбора информации при описании бизнес-процессов,» *Консультант директора,* № 12, 2004.

[5] „Data Collection Methods for Evaluation: Document Review," Centers for Disease Control and Prevention, 2009. [Võrgumaterjal]. Saadaval: https://www.cdc.gov/healthyyouth/evaluation/pdf/brief18.pdf. [Kasutatud 20 Märts 2018].

[6] E. Ampt, „Workshop synthesis: Longitudinal methods: overcoming challenges and exploiting benefits," *Transport survey methods: best practice for decision making,* lk. 393-408, 2013.

[7] Г. И. Купалова, Теория экономического анализа, 2008.

[8] L. Cohen, L. Manion ja K. Morrison, Research Methods in Education, 5th Ed., kd.

Chapter 15, London: RoutledgeFalmer, 2000, lk. 267-292.

[9] *ISO/IEC 27005:2011,* International Organization for Standartization, 2011.

[10] „Идентификация и оценка рисков. 4. Метод контрольных списков,“ Лаборотория "Статистическое знание", 2014. [Võrgumaterjal]. Saadaval: http://best-stat.ru/risk-menedzhment/identifikatsiya-i-otsenka-riskov-4-metod-kontrolnykh-spiskov.html/. [Kasutatud 2 Aprill 2018].

[11] В. Н. Волкова, Моделирование систем и процессов: учебник для академического бакалавриата, Санкт-Петербург: Санкт-Петербургский политехнический университет Петра Великого, 2015.

[12] Е. Е. Куликова, Управление рисками: инновационный аспект, Бератор-Паблишинг, 2008, lk. 204.

[13] В. М. Воронина ja Д. В. Кокарев, „SWOT-анализ как современный инструмент исследования в целях антикризисного управления предприятием,“ *Слияния и Поглощения,* kd. 3, nr 49, lk. 23-26, 2007.

[14] E. Zorita ja H. von Storch, „The Analog Method as a Simple Statistical Downscaling Technique: Comparison with More Complicated Methods,“ *JCLI,* kd. 12, nr 8, 1999.

[15] М. Грачева, Риск-менеджмент инвестиционного проекта: учебник, Москва: ЮНИТИ-ДАНА, 2009, lk. 544.

[16] „Ad hoc,“ Dictionary.com, [Võrgumaterjal]. Saadaval: http://www.dictionary.com/browse/ad-hoc. [Kasutatud 20 Aprill 2018].

[17] „Privaatsustingimused,“ VEHO Eesti AS, [Võrgumaterjal]. Saadaval: https://www.veho.ee/et/privaatsustingimused. [Kasutatud 15 Aprill 2018].

[18] „Data Protection Officer (DPO) Print,“ European Data Protection Supervisor, 2018. [Võrgumaterjal]. Saadaval: https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en. [Kasutatud 29 Aprill

2018].

[19] A. Inspektsioon, „Suunised andmete ülekandmise õiguse kohta (16/ET WP 242 rev. 01),“ Tallinn, 2017.

[20] L. Manion, L. Cohen ja K. Morrison, Research Methods in Education, 5th Edition, kd. Chapter 17, London: RoutledgeFalmer, 2000, lk. 306-316.

[21] „DATA COLLECTION METHODS,“ Food and Agriculture Organization of the United Nations, [Võrgumaterjal]. Saadaval: http://www.fao.org/docrep/003/x2465e/x2465e09.htm#b7-6.3.2%20Questionnaires .[Kasutatud 1 Mai 2018].

[22] M. N., „Delphi Method - Presentation,“ University of Mysore, 2011. [Võrgumaterjal]. Saadaval: https://www.slideshare.net/Muruli_88/delphi-method. [Kasutatud 1 Mai 2018].

[23] „Инструменты риск-анализа,“ Студопедия, 2015. [Võrgumaterjal]. Available: https://studopedia.ru/16_87686_sushchnost-risk-analiza-investitsionnogo-proekta.html. [Kasutatud 2 Aprill 2018].

Lisa 1 – Küsimustik

Küsimustik kasutavate süsteemide riskianalüüsi läbiviimiseks.

Küsimuse kood	Küsimus	Grupp
K01	Algusaeg	Metaandmed
K02	Lõpetusaeg	Metaandmed
K03	E-post	Metaandmed
K04	Nimi	Metaandmed
K05	Süsteemi/rakenduse nimi	Üldine
K06	Süsteemi/rakenduse kood	Üldine
K07	Sisu antud	Üldine
K08	Riik	Üldine
K09	Süsteemi/rakenduse Omaniku nimi	Üldine
K10	Süsteemi/rakenduse Omaniku e-post	Üldine
K11	Palun kirjeldage süsteemi/rakendust	Üldine
K12	Kus asub server? (nt andmekeskuse füüsiline asukoht)	Üldine
K13	Kasutajate koguarv	Üldine
K14	Palun valige selles süsteemis/rakenduses isikuandmeid sisaldavate väljade arv	Üldine

Küsimuse kood	Küsimus	Grupp
K15	Palun valige selles süsteemis/rakenduses tundlikke (sensitiivseid) andmeid sisaldavate väljade arv	Üldine
K16	Kui paljude inimeste infot hoitakse rakenduses? (kliendid või töötajad)	Üldine
K17	Kas süsteem sisaldab struktureerimata isikuandmeid? (dokumente, pilte, vabasid tekstivälju jne)	Üldine
K18	Kas süsteem/rakendus on seotud või sõltuv mõnest teisest süsteemist ja/või rakendusest?	Keerukus
K19	Nimekiri süsteemidest/rakendustest, kust isikuandmed pärinevad (sise või välis).	Üldine
K20	Kogu arv süsteemidest/rakendustest, kust isikuandmed pärinevad (sise või välis).	Üldine
K21	Nimekiri süsteemidest/rakendustest, kuhu isikuandmeid saadetakse (sise või välis).	Üldine
K22	Kogu arv süsteemidest/rakendustest, kuhu isikuandmeid saadetakse (sise või välis).	Üldine
K23	Kas isikuandmeid edastatakse või kas neile on ligipääs partneritel?	Üldine
K24	Kas andmete töötlemine toimub kolmandate isikute poolt? (varukoopiad, andmete püüdmised, väline salvestamine jne)	Üldine
K25	Kas süsteem/rakendus sõltub sisemistest komponentidest/allsüsteemidest?	Keerukus
K26	Kui paindlik on süsteemi/rakenduse lepingu struktuur?	Keerukus
K27	Kas süsteemil on asjakohane dokumentatsioon selle kohta, kuidas süsteem/rakendus töötab (sh arhitektuuridiagrammid, spetsifikatsioonid, riskianalüüs ja muud dokumendid)?	Keerukus
K28	Kas süsteemil/rakendusel on selle süsteemi/rakenduse toetamiseks (arendus, toimingud ja hooldus) piisavad ressursid?	Keerukus

Küsimuse kood	Küsimus	Grupp
K29	Kui tihti toimuvad süsteemi/rakenduse versiooniuuendused?	Keerukus
K30	Kuidas hallatakse süsteemis/rakenduses nõusolekut?	Vastavus
K31	Kas andmeid on andmesubjekti soovi korral võimalik transportida ja kui on, siis mis formaadis?	Vastavus
K32	Kuidas toimub süsteemis andmete kustutamine ja kas see on dokumenteeritud või korratav protsess?	Vastavus
K33	Kas andmesubjektidel on võimalik oma andmetele ligi pääseda ning andmeid parandada?	Vastavus
K34	Mil määral on andmete edastusega seotud riskide maandamiseks kasutatud pseudonüüme või muid meetodeid, säilitades samaaegselt andmete kasutegurit?	Vastavus
K35	Millised meetmed eksisteerivad, et tagada süsteemi/rakenduse andmete kvaliteet?	Vastavus
K36	Kuidas kaitstakse süsteemis/rakenduses andmekaitse ja turvalisuse vahendeid?	Vastavus

Lisa 2 – Andmeatribuutide loetelu

Ettevõtte X töötajate ja klientide kohta käivate töödeldavate andmeatribuutide loetelu.

Atribuut	Alamatribuut
Nimi	Nimi
Nimi	Perekonnanimi
Nimi	Keskmine nimi
Nimi	Lühike nimi
Nimi	Muu
Isikukood	Isikukood
Isikukood	Muu
Elukoha aadress (alaline asukoht)	Riik
Elukoha aadress (alaline asukoht)	Linn
Elukoha aadress (alaline asukoht)	Tänav
Elukoha aadress (alaline asukoht)	Postiindeks
Elukoha aadress (alaline asukoht)	Muu
Postiaadress	
Telefoninumber	Töö
Telefoninumber	Isiklik
Telefoninumber	Muu

Atribuut	Alamatribuut
E-posti aadress	Töö
E-posti aadress	Isiklik
E-posti aadress	Muu
Sugu	
Sünnikuupäev	Year
Sünnikuupäev	Päev ja kuu
Sünnikuupäev	Muu
Sünniriik	Riik
Sünniriik	Linn
Sünniriik	Muu
Kodakondsus	
Passiandmed	Passi number
Passiandmed	Rahvus
Passiandmed	Väljastamise Riik
Passiandmed	Väljastamise asutus
Passiandmed	Väljastamise kuupäev
Passiandmed	Aegumiskuupäev
Passiandmed	Muu
Pilt (välja arvatud pass)	
Tööandja / Eelmine tööandja	Ettevõtte Nimi
Tööandja / Eelmine tööandja	Ettevõtte kood

Atribuut	Alamatribuut
Tööandja / Eelmine tööandja	Ettevõtte aadress
Tööandja / Eelmine tööandja	Soovitaja nimi
Tööandja / Eelmine tööandja	Töötamise periood
Tööandja / Eelmine tööandja	Tegevusala
Tööandja / Eelmine tööandja	Muu
Ametikoht / eelmine ametikoht	Amet
Ametikoht / eelmine ametikoht	Ametis oleku aeg
Ametikoht / eelmine ametikoht	Ametinimetus
Ametikoht / eelmine ametikoht	Muu
Töökogemus	Jah/Ei
Töökogemus	Aastate arv
Töökogemus	Muu
Kuupalk	Summa
Perekonnaseis	
Haridus	Kooli nimi
Haridus	Tulemus
Haridus	Õppevaldkond
Haridus	Ajaperiood
Haridus	Muu
Teave sotsiaalkindlustusmaksete ja kindlustuse kohta	Kogus
Teave sotsiaalkindlustusmaksete ja kindlustuse kohta	Kindlustusperiood

Atribuut	Alamatribuut
Teave sotsiaalkindlustusmaksete ja kindlustuse kohta	Muu
Info makstava pensioni/toetuse/hüvitise kohta	Tüüp
Info makstava pensioni/toetuse/hüvitise kohta	Kuu summa
Info makstava pensioni/toetuse/hüvitise kohta	Aasta summa
Info makstava pensioni/toetuse/hüvitise kohta	Muu
Kutsetunnistused	Sertifikaadi pealkiri
Kutsetunnistused	Sertifikaadi väljaandja
Kutsetunnistused	Kestus
Kutsetunnistused	Sertifikaadi number
Kutsetunnistused	Muu
Muud isikuandmete atribuudid	
Terviseandmed või teave	Seisundi nimi
Terviseandmed või teave	Tervisega seotud mõõdikud
Terviseandmed või teave	Viimane tervisekontrolli kuupäev
Terviseandmed või teave	Muu
Teave puuete kohta	Jah/Ei
Teave puuete kohta	Tüüp
Teave puuete kohta	Muu
Karistusandmed	Jah/Ei
Karistusandmed	Tüüp
Karistusandmed	Muu