

TARTU ÜLIKOOL

Majandusteaduskond

Erika Smirnova

VIHJEKANALI LOOMINE TEENINDUSETTEVÕTTE X NÄITEL

Magistritöö

Juhendaja: kaasprofessor Anne Reino

Tartu 2026

Olen koostanud töö iseseisvalt. Kõigile töö koostamisel kasutatud teiste autorite töödele, põhimõttelistele seisukohtadele, kirjandusallikatest ja mujalt pärinevatele andmetele on viidatud.

Töö koostamisel kasutasin tehisintellekti üksnes abivahendina Exceli funktsiooni Data Analysis kasutamisega seotud tehniliste küsimuste täpsustamiseks. Pärast eelkaitsmist kasutasin tehisintellekti ka joonise 1 parandamiseks – algselt oli joonis U-kujuline, seejärel muutsin selle loetavamaks ja ülevalt alla esitatuks. Kõik analüütilised järeldused, töö sisu ning lõplikud järeldused olen teinud iseseisvalt.

Sisukord

Sissejuhatus.....	4
1. Vihjeandmise teoreetiline käsitlus	6
1.1. Vihjeandmise olemus ja Euroopa Liidu õiguslik raamistik	6
1.2. Organisatsioonisisese vihjeandmissüsteemi toimimine ja selle loomise võimalused	11
1.3. Vihjeandmist soodustavad ja takistavad tegurid	17
2. Vihjekanaliloomise uuring ettevõttes X.....	23
2.1. Uuritav ettevõtte, uurimismetoodika ja valim.....	23
2.2. Empiirilise uuringu tulemuste analüüs.....	28
2.3. Järeldused ja praktilised soovitusel ettevõttele X	35
Kokkuvõte.....	42
Viidatud allikad.....	45
Lisad.....	53
LISA A. Vihjeandmise mõjete kasutus kirjanduses	53
LISA B. Vihjeandmist eeldavad rikkumised	55
LISA C. Küsimustik.....	57
LISA D. Vastajate kokkupuutumine tööalaste rikkumistega.....	63
LISA E. Vastajate hinnang teatamisvajadusele ja -viisile	64
LISA F. Vihjekanalilomaduste korrelatsioonimaatriks	65
LISA G. Uuringu tulemuste ja teoreetiliste seisukohtade võrdlus.....	66
Summary	67

Sissejuhatus

Organisatsioonis võib esineda mitmesuguseid rikkumisi – ebaeetilisi, ebaseaduslikke ja sisekorraeeskirjade rikkumisi. Selliste rikkumiste hulka kuuluvad näiteks diskrimineerimine, pettus, keskkonnareostus ja ohutusjuhiste eiramine. Rikkumised võivad põhjustada nii rahalist, maine- kui ka juriidilist kahju, mistõttu on oluline luua organisatsioonisisene vihjekanal, et rikkumisi varakult avastada ja kahju tekkimise riske maandada.

Kuna organisatsiooni siseandmetele ligipääs on piiratud väljaspool organisatsiooni olevatel isikutel, on töötajad sageli esimesed, kes potentsiaalseid rikkumisi märkavad ning saavad neist organisatsiooni sees või sellest väljaspool teatada. Töötajate võtmerolli organisatsioonisiseste rikkumiste avastamisel kinnitab ka Sertifitseeritud Pettuseuurijate Ühingu (ingl *Association of Certified Fraud Examiners*, edaspidi ACFE) aruanne, mille kohaselt avastati 2024. aastal 43% kõigist maailmas tuvastatud pettuse juhtumitest rikkumisest teatamise kaudu, kusjuures 52% teatajatest olid töötajad (ACFE, 2024). See näitab, et turvaliste rikkumisest teatamise võimaluste loomine on tähtis vahend väärtgevuse ennetamiseks ja avastamiseks.

Organisatsioonisisestest potentsiaalsetest rikkumistest teavitavat isikut nimetavad rahvusvahelised organisatsioonid mitmel moel, näiteks „teavitav isik“ (ingl *reporting person*, United Nations, 2004), „vilepuhuja“ (ingl *whistleblower*, United Nations, 2019), „rikkumisest või väärkäitumisest teavitaja“ (Saaremägi, 2021) ja „vihjeandja“ (Jatsa, 2019). Parema jälgitavuse huvides kasutatakse käesolevas töös termineid „rikkumisest teataja“ ja „vihjeandja“.

Vihjeandmise teema ja selleks otstarbeks spetsiaalse kanali loomine on muutumas üha olulisemaks, kuna kogu Euroopa Liidus (edaspidi ka EL) püütakse rakendada ühtset lähenemisviisi vihjeandjate kaitsmisele. Eestis jõustus esimene vihjeandja kaitse seadus – tööalasest Euroopa Liidu õiguse rikkumisest teavitaja kaitse seadus (edaspidi TÕRTKS) – 1. septembril 2024 ning see kohustas üle 250 töötajaga ettevõtteid looma vihjekanalit. Alates 1. jaanuarist 2025 on sama kohustus kehtinud ka üle 50 töötajaga ettevõtetele. (TÕRTKS, 2024) Vihjeandmise protsesside kohta riiklikul tasandil nõuete kehtestamine tähendab organisatsioonidele täiendavat kohustust luua võimalusi konfidentsiaalseks ja senisest turvalisemaks vihjeandmiseks.

Teaduses on samuti kasvanud huvi vihjeandmise teema vastu. Seda kinnitab Scopuse (n.d.) andmebaas, mille andmetel on alates esimeste vihjeandmist käsitlevate publikatsioonide ilmumisest 1978. aastal kuni tänapäevani avaldatud sel teemal 3329

teadustööd. Neist peaaegu veerand on ilmunud viimase viie aasta jooksul (Scopus, n.d.), mis viitab asjaolule, et sellele teemale pööratakse üha suuremat tähelepanu, ajendatuna nii seadusandlikest muudatustest kui ka kasvavast teadlikkusest teema olulisuse kohta.

Vihjeandmist soodustava keskkonna loomine on eriti oluline teenindussektoris, kuna seda iseloomustab tihe suhtlus klientidega ning teenuse kvaliteedi suur sõltuvus töötajate käitumisest ja töökorraldusest, mis väljendub ebastabiilses töögraafikus ja ajutistes töösuhetes (Goh & Lee, 2018; Lata & Chaudhary, 2020). Töötajate voolavus ja hooajalisus võivad vähendada töötajate teadlikkust sisekorraeskirjadest ja vihjeandmise viisidest, mistõttu on oluline tagada tõhus sisseelamisprogramm ja kättesaadav vihjekanal (Whistlelink, 2024; Zopiat, Constanti & Theocharous, 2014). Samas on teenindussektor lai ja mitmekesine, hõlmates näiteks tervishoidu, haridust ja logistikat (Statistikaamet, n.d.), kuid käesolev töö keskendub majutus- ja toidlustusvaldkonnale.

Eurostati 2023. aasta andmete kohaselt on majutus- ja toidlustusvaldkond Euroopa Liidus üks neid valdkondi, kus surmaga lõppenud tööõnnetuste määr on võrreldes mõne teise valdkonnaga madal, kuid surmaga mitte lõppenud õnnetuste määr on endiselt suhteliselt kõrge (Eurostat, 2025), mis näitab töötingimuste ja -korraldusega seotud suuremaid riske. Valdkonna stressirohkus ja suur füüsiline koormus (Goh & Lee, 2018) võivad kaasa aidata nii tööõnnetuste kui ka muud tüüpi rikkumiste esinemisele, sealhulgas tööõiguse rikkumisele, diskrimineerimisele, töötajate väärkohtlemisele ja klientide õiguste rikkumisele (Whistlelink, 2024; Vesterinen, 2024). Sellistel asjaoludel muutub rikkumiste õigeaegne avastamine sisemiste vihjekanalite kaudu oluliseks vahendiks kahjude ennetamisel või leevendamisel.

Käesolevas magistritöös käsitletud teenindusettevõtte X puudub praegu vihjekanal. Eesti seadustest tulenevate nõuete kohaselt on aga sellise kanali loomine ettevõttele kohustuslik, mis tingib vajaduse sobivate lahenduste väljatöötamiseks. Magistritöö eesmärk on koostada praktilised soovituselised vihjekanalite loomiseks teenindusettevõttes X ning luua selle kanali demoversioon, tuginedes teoreetilisele raamistikule ja empiirilise uuringu tulemustele.

Eesmärgi saavutamiseks on püstitatud järgmised uurimisülesanded:

- selgitada vihjeandmise mõistet ning analüüsida EL-i ja Eesti õiguslikku raamistikku;
- analüüsida vihjekanalite ja -protsessi toimimise põhimõtteid ja loomise võimalusi;
- selgitada välja vihjeandmist soodustavad ja takistavad tegurid;
- töötada välja uurimismetoodika ja kirjeldada uuritava teenindusettevõtte tausta;
- viia uuritavas teenindusettevõttes X läbi küsitlus;

- analüüsida kogutud andmeid, teha nende põhjal järeldusi ja anda ettevõttele X soovitusi vihjekanaliloomiseks;
- luua vihjekanalil demoversioon.

Töö koosneb teoreetilisest ja empiirilisest osast. Teoreetilises osas käsitletakse vihjeandmise mõistet, õiguslikku raamistikku EL-is ja Eestis ning vihjeandmissüsteemi loomise põhimõtteid ja teatamisvalmidust mõjutavaid tegureid. Empiirilises osas kirjeldatakse uuritavat ettevõtet ja kasutatud uurimismeetodeid ning viiakse läbi küsitlus ettevõtte X töötajate ja juhtide seas. Uuringu tulemusi seostatakse teoreetiliste seisukohtadega, mille põhjal tehakse järeldused ettevõtte vajaduste ja sobiva lähenemisviisi kohta vihjeandmissüsteemi loomisel. Lisaks töötatakse välja praktilised soovitusel vihjekanalil ja süsteemi loomiseks ja rakendamiseks ning luuakse vihjekanalil demoversioon.

Käesoleva töö autor tänab juhendaja Anne Reinot asjalike nõuannete ja kasuliku tagasiside eest kogu töö valmimise vältel. Samuti avaldab autor tänu ettevõttele X, küsimustiku täitjatele ning kontaktisikule uuringu korraldamise ja läbiviimise võimaldamise eest. Autor on tänulik ka keeletoimetajale töö keelelise viimistlemise eest ja retsensendile väärtuslike soovitusel eest.

Märksõnad: vihjeandmine, vihjekanal, vihjeandja kaitse, direktiiv, rikkumine.

Teaduseriala koodid: S212 Tööjõu- ja ettevõtlussotsioloogia, S190 Ettevõtete juhtimine.

1. Vihjeandmise teoreetiline käsitus

1.1. Vihjeandmise olemus ja Euroopa Liidu õiguslik raamistik

Kirjanduses käsitletakse vihjeandmise mõistet mitut moodi (vt lisa A), kuid selle tuum on eri autoritel sarnane. Qasem (2025) defineerib vihjeandmist teatamisena sellistest organisatsioonisisestest tegevustest, mis on vastuolus seaduse ja eetikanormidega ning mis kahjustavad erinevaid huvigruppe. Evchenko (2016) määratlus sarnaneb Qasemi (2025) omaga, kuid see puudutab üldisemat konteksti, käsitledes vihjeandmist viisina kaitsta vihjeandjat ennast ja ühiskonda seaduste ja eetikanormide rikkumise eest. Tiitsi (2014) pakutud definitsioon määratleb vihjeandmise tegevusena, mis hõlmab juhi, pädeva asutuse või meedia teavitamist sellest, et organisatsioonis on toimunud või võib toimuda potentsiaalne rikkumine. Hersh (2002) seevastu määratleb vihjeandmist praeguse või endise töötaja poolse teavitamisena sellistest arvatavatest rikkumistest, mis ohustavad, kahjustavad või on ebaseaduslikud või ebaeetilised.

Kuigi eespool mainitud autorid rõhutavad veidi erinevalt, kes kellele ja millest teatab ning millises kontekstis, on kõik ühel meelel järgmises: vihjeandmise korral teatab isik võimalikest rikkumistest, et juhtida neile tähelepanu ja ennetada kahju. Tuginedes üldistele joontele, mis on uuritud allikate põhjal kindlaks tehtud, tähendab vihjeandmine eelkõige organisatsioonisisestest rikkumistest teavitamist eesmärgiga tuvastada, ennetada või leevendada kahjusid, mis tulenevad potentsiaalsetest või tegelikest rikkumistest, mille korral võib tegemist olla nii eetiliste probleemide kui ka seadusvastase tegevusega (Qasem, 2025; Evchenko, 2016; Tiits, 2014; Hersh, 2002). Teod, mille kohta vihje antakse, võivad olla toime pandud organisatsiooni sees kas organisatsiooni enda poolt või organisatsiooni nimel (Terracol, 2022). Vihjeandjad võivad kokku puutuda erinevate riskidega, näiteks turvalisust, tervist ja isegi elu ähvardava ohuga, seetõttu on nende õiguskaitse tagamine oluline (Saaremägi, 2021).

Vihjeandmise tähtsus seisneb selles, et võimalikust rikkumisest teatamisega annab vihjeandja tõuke selle tuvastamiseks ja uurimise algatamiseks, samuti rikkuja karistamiseks ja rikkumise kõrvaldamiseks (Transparency International, 2025; Trofimov, 2021; Cordis & Lambert, 2017; Palojärv, 2021). Organisatsioonides toimuv on väliste osapoolte eest, kes ei ole organisatsiooniga töö või muude partnerlussuhete kaudu seotud ega ole sellega varem kokku puutunud, sageli peidetud (Puh & Tökke, 2024; Transparency International, 2025; Trofimov, 2021). Vihjeandjad võimaldavad paljastada rikkumisi, mis muidu jääksid avastamata, suurendades selle tulemusena organisatsiooni läbipaistvust, vastutust, usaldusväärsust ja ausust, edendades eetilist juhtimist, ennetades võimu kuritarvitamist ning kaitstes keskkonda ja avalikku huvi, tervist, ohutust, finantsstabiilsust ja õigusi nii tervise kui ka rahanduse ja keskkonnakaitse valdkonnas (Adli Roslan et al., 2025; Transparency International, 2025; Transparency International, n.d.; CM/Rec(2014)7; 2014; 2019/1937, 2019; Qasem, 2025; Terracol, 2022).

Samas, mida varem rikkumine avastatakse ja kõrvaldatakse, seda lihtsam on ära hoida rahalist kaotust või seda leevendada ning päästa organisatsioon kohtumenetlusest ja hilisematest sanktsioonidest (Bishop-Monroe et al., 2021; Terracol, 2022; Saaremägi, 2021). Rikkumise hilinenud avastamise või avastamata jätmisega kaasnevate probleemide hulka kuuluvad organisatsiooni vastu tuntava usalduse õõnestamine ning ebavõrdsete võimaluste ja ebaausa konkurentsi tekitamine (Korruptsioonivaba Eesti, n.d.).

Vihjeandmise laiemat ühiskondlikku mõju ilmestavad mitmed tuntud juhtumid, näiteks 2010. aastate keskel aset leidnud LuxLeaksi juhtum. Nimelt, ettevõtte PricewaterhouseCoopers töötajad Antoine Deltour ja Raphaël Halet edastasid ajakirjanikule

konfidentsiaalseid dokumente, mis näitasid, kuidas suurettevõtted on kasutanud Luksemburgi maksusüsteemi maksude optimeerimiseks teiste riikide arvelt. Luksemburgi võimud algatasid vihjeandjate vastu kriminaalmenetluse, kuid hiljem tunnistas riigi kõrgeim kohus Deltouri vihjeandjaks. Süüdistused Haleti vastu jäid aga kehtima, kuna tema lekitatud teave polnud uus, mistõttu ei peetud teda vihjeandjaks. Kuid Haleti kaebus Euroopa Inimõiguste Kohtusse viis 2023. aastal suurkoja otsuseni, mis tunnistas vihjeandja kaitse vajalikkust ka sellistel juhtudel, kui tegemist on süsteemse praktikaga, mis kahjustab avalikku huvi. LuxLeaksi juhtum tekitas laialdast rahvusvahelist arutelu ning sai üheks oluliseks tõukeks Euroopa Liidu vihjeandjate kaitse direktiivi väljatöötamisele. (Banisar, 2023)

23. oktoobril 2019 jõustus vihjeandjate kaitse direktiiv (2019/1937, 2019), mis ühtlustas vihjeandjate kaitset EL-i liikmesriikides miinimumnõuete sätestamise kaudu (Qasem, 2025; 2019/1937, 2019). Euroopa Komisjon määras 22 riigile direktiivi ülevõtmise hilinemise eest trahve, kusjuures Eesti oli üks kahest riigist, mis võttis uue direktiivi üle kaheaastase viivitusega (TÕRTKS, 2024; Whistleblowing International Network, n.d.).

26. jaanuari 2022. aasta istungil ei suutnud Eesti valitsus eri osapoolte arvukate seaduse täiustamiseks esitatud muudatusettepanekute tõttu üksmeelt saavutada, mistõttu tuli uue seaduse vastuvõtmine edasi lükata (Lõvi, 2023; EWR Online, 2025). Samuti on tekitanud arutelu vihjeandjate kaitse sätete liiga lai kohaldamine, kuna piiratud ressursid ei võimalda kõiki rikkumisi jälgida (Lõvi, 2023). Sel põhjusel on tehtud ettepanek võtta seaduse koostamisel aluseks direktiivis sätestatud rikkumised (Voltri & Whyte, 2023; Lõvi, 2023; Kүүts, 2024).

17. detsembriks 2021 pidid liikmesriigid kehtestama õigusaktid, mis nõuavad enam kui 250 töötajaga ettevõtetelt sisemiste vihjekanalite loomist ja asjakohaste meetmete võtmist vihjete menetlemiseks ja vihjeandjate kaitsmiseks. Sama kohustus pidi kaks aastat hiljem laienema ka üle 50 töötajaga ettevõtetele. (2019/1937, 2019) Eesti puhul hakkasid need nõuded üle 250 töötajaga ettevõtete suhtes kehtima 1. septembril 2024 ning üle 50 töötajaga ettevõtete suhtes 1. jaanuaril 2025 (TÕRTKS, 2024). Hoolimata sellest, et Eesti on kohaldatavasse seadusesse üsna tugevalt üle võtnud direktiivi miinimumnõuded, ilma olulisi muudatusi tegemata, on siiski mõned erinevused, mis esitatakse allpool direktiivi nõuete tutvustamise kaudu.

Direktiiv keelab vihjeandjate vastu survemeetmete kasutamise, mis hõlmab näiteks edutamisest keeldumist, trahvimist, maine kahjustamist, rahalise kahju tekitamist, litsentsi või loa kehtetuks tunnistamist ja sunniviisilist suunamist psühhiaatriasse või ravisse (2019/1937, 2019). Eesti seaduses on samuti keelatud survemeetmete kasutamine, kuid need on kokku

võetud ühe üldise terminiga ja ei detailselt loetletud nii, nagu direktiivis (TÕRTKS, 2024). Kaitstud vihjeandjateks võivad olla nii era- kui ka avalikus sektoris töötavad isikud, sealhulgas füüsilisest isikust ettevõtjad, vabatahtlikud ja praktikandid. Vihje võivad anda ka tulevased või endised töötajad. Muus osas hõlmab kaitse vihjeandjaid toetavaid isikuid, nendega seotud ja ohustatud isikuid (kaastöötajad, pereliikmed) ning nendega ametialase tegevuse kaudu seotud juriidilisi isikuid. (2019/1937, 2019) Eesti seadus järgib sama kaitstavate isikute loendit, lisatud on isikud, kes saavad sporditoetust. Samas ei täpsustata konkreetselt, kes vihjeandjatega seotud osapooltest on kaitstud. (TÕRTKS, 2024)

Vihjeandmise usaldusvääruse tagamisel on huvitavaks näiteks Prantsusmaa praktika, mis aitab vältida pahatahtlikke või alusetuid süüdistusi. Prantsusmaa seadustes on sätestatud, et kaitset saab ainult vihjeandja, kes teatab oma ametialase tegevuse käigus teatavaks saanud võimalikust rikkumisest. Juhul, kui võimalik rikkumine ei ole teatavaks saanud ametialase tegevuse käigus, peab vihjeandjal olema sellest isiklik teadmine, et välistada pelgalt kuulujuttudel või oletustel põhinevad vihjed. (LOI n° 2022-401, 2022) See täpsustus on praktikas kasulik, kuna kaitseb vihjeandmise süsteemi kuritarvituste eest ja aitab tagada, et menetluse jõuaksid vaid põhjendatud vihjed.

Direktiiv välistab kaitse otse avalikustamise korral, näiteks ajakirjandusele teatamisel, kui pole täidetud teatud eeldused. Direktiiv lubab avalikustamist ainult juhul, kui esineb mõistlik ootus, et arvatav rikkumine toob kaasa avaliku huvi rikkumise, sealhulgas hädaolukorra või pöördumatu kahju ohu. Teiseks avalikustamise eelduseks on kättemaksu ohu esinemine, sealhulgas tõendite varjamise või hävitamise oht, või oht, et organisatsioon on arvatavas rikkumises kaasosaline. Avalikustamise puhul on kaitse taotlemine võimalik, kui vihjeandja teatab probleemist esmalt ettevõttesiseselt ja seejärel ettevõtteväliselt või teatab probleemist kohe ettevõtteväliselt, millele järgneb vihje ignoreerimine, selle ebaõige töötlemine või ebaõigete meetmete rakendamine pärast direktiivis sätestatud tähtaegade möödumist. (2019/1937, 2019) Ka Eestis on vastu võetud samalaadsed sätted, kuid konkreetseid näiteid, nii nagu on tehtud direktiivis, ei ole esitatud (TÕRTKS, 2024). See võib muuta potentsiaalsete vihjeandjate olukorra ebakindlaks, mõneti arusaamatuks.

Direktiivi kohaselt tuleb vihjeandjaid kaitsta negatiivsete tagajärgede eest, kui nad teatavad võimalikest rikkumistest (vt lisa B), mis hõlmavad näiteks riigihankeid, toote- või transpordiohutust, keskkonnakaitset, rahva- või loomade tervist ja heaolu, tarbijaõiguseid ja küberturvalisust. Ka kõik EL-i õiguse rikkumised kuuluvad selle õigusakti reguleerimisalasse. (2019/1937, 2019) Eesti seaduses on rangelt järgitud direktiivis nimetatud rikkumise valdkondade loetelu, ilma täiendusi tegemata. Kuid oluline on märkida, et Eesti

vihjeandja kaitse seadus ei laiene teatud valdkondadele, näiteks riigisadaladusele, advokaatide kutsetegevuses advokaadisadaladuse säilitamisele ega meditsiinitöötajate töös arstisadaladuse järgimisele. (TÕRTKS, 2024)

Eesti seaduse piiratud loetelu rikkumistest, millest teatamisel kaitse on tagatud (Terracol, 2023; TÕRTKS 2024), võib põhjustada suure hulga muude tõsiste rikkumiste avastamata jäämise, kuna neid seaduses ei käsitleta. See võib omakorda põhjustada kaitseta jäämise hirmu suurenemist. Samal ajal võib potentsiaalsetel vihjeandjatel olla raske kindlaks teha, kas nad on avastanud seaduse alusel teatamisele kuuluva võimaliku rikkumise. See võib olla tingitud ebamäärasest terminoloogiast (nt „avalik huvi“ või „EL-i õigus“), millest kõik ei pruugi ühtviisi aru saada (Erikson, 2021; Paatsi & Haabu, 2024; Terracol, 2019) ja mida võidakse erinevalt tõlgendada.

Siiski ei pea rikkumiste loetelu piirduma ainult õigusaktides sätestatuga, organisatsioonid saavad enda äranägemisel ja vastavalt vajadusele loetelu laiendada (2019/1937, 2019; Terracol, 2022). Näiteks pakub Swedbank Grupp vihjeandjatele võimalust teatada arvatavatest ebaeetilistest rikkumistest, nagu kiusamine või alandav kohtlemine, ning AS Circle K palub teada anda igast arvatavast rikkumisest, isegi kui see jääb „halli alasse“ (Uus, 2016; Jatsa, 2019). Organisatsioonid võivad tunda huvi ka organisatsioonisiseste eetikanormide rikkumise ning seaduserikkumiste vastu, mis ei kuulu direktiivi nimekirja, kuid on karistatavad. Majutus- ja toitlustusvaldkonnas võivad rikkumise liigid hõlmata näiteks külaliste andmete lekkimist, klientide petmist, keskkonna reostamist või vara ilma loata kasutamist (Whistlelink, 2024; Vesterinen, 2024).

Lisaks nõuab direktiiv seda, et organisatsioonisisest vihjekanalit haldaks kas organisatsioonisisene isik või üksus või väline partner, kes vajadusel küsib vihjeandjalt lisateavet ja tagasisidet. Samas peab vihjekanal olema kaitstud volitamata isikute eest, tagamaks vihjeandja ja vihjes esitatud teabe konfidentsiaalsuse. (2019/1937, 2019) Eestis on seadusega ette nähtud ka vihjekanalit ühine haldamine alla 250 töötajaga ettevõtetes (TÕRTKS, 2024).

Vihjeandjalt saadud teavet säilitatakse kuni direktiivis sätestatud kohustuste täitmiseni. Suuline teave peab olema kas taasesitatav või salvestatud, kontrollitud ja vihjeandja poolt allkirjastatud. Pärast vihje esitamist peab vihjeandja saama 7 päeva jooksul kinnituse, et teade on jõudnud vastutava isiku või üksuseni, ning seejärel saama 3 kuu jooksul tagasisidet rakendatud meetmete kohta. (2019/1937, 2019) Eesti seadus sarnaneb nende nõuetega, kuid täpsustab, et andmeid säilitatakse kuni 3 aastat pärast tagasiside andmist, küll aga ei ole täpsustatud, kuidas tuleb säilitada suuliselt kogutud teavet (TÕRTKS, 2024).

Direktiiv võimaldab liikmesriikidel ise määrata karistusi konfidentsiaalsuse rikkumise, survemeetmete rakendamise ja vihjeandmise takistamise eest (2019/1937, 2019). Eesti seaduses on määratud trahvid iga eespool loetletud rikkumise eest, samuti on määratud trahv teadlikult valeinformatsiooni esitamise eest (TÕRTKS 2024). Samas on probleem see, et seadus ega direktiiv ei näe ette, kuidas karistada organisatsioone, mis ei võta vastutust vihjekanalite loomise eest (Terracol, 2023; TÕRTKS 2024). Seetõttu ei ole need organisatsioonid motiveeritud vihjekanalite looma või seda tehakse ainult formaalselt, mis ei vasta aga nõuetele ega vii tulemuseni.

Lisaks ei paku Eesti seadus vihjeandjatele õiguslikku ega rahalist kaitset (Terracol, 2023; TÕRTKS 2024), nagu teeb näiteks Prantsusmaa, pakkudes ajutist rahalist garantiid elamiskulude ja õigusabikulude katmiseks, kui vihjeandja teade on oluliselt halvendanud tema rahalist olukorda (LOI n° 2022-401, 2022). Kuna Eestis ei ole sellist tuge seadusega ette nähtud, võivad vihjeandjad karta teatamisega kaasnevaid lisakulusid ja ebapiisavat seaduslikku kaitset ning see vähendab nende teatamisvalmidust.

1.2. Organisatsioonisisese vihjeandmissüsteemi toimimine ja selle loomise võimalused

Vihjeandmine võib toimuda kolmel viisil: sisemiselt, kas juhtkonna või spetsiaalselt vihjete uurimiseks loodud osakonna kaudu, kellel on õigus vastavaid probleeme lahendada; väliselt, esitades asjakohase teabe pädevale asutusele; või avaldades teavet laiemale publikule, näiteks sotsiaalse meedia, meedia ja ametiühingute kaudu (Palojärvi, 2021; Furlow, 2011; Transparency International, n.d.; Tiits, 2014; Hakim Z., Safira & Mahmudah, 2019; Hersh, 2002; Fischer & Gollwitzer, 2025; Terracol, 2022). Avalikustamine on pigem äärmuslik tegevus, kuna organisatsioonile kaasnevad tagajärjed võivad olla pöördumatud, näiteks mainekahju. Sisemiste kanalite loomine potentsiaalsetest rikkumistest teatamiseks aitab vähendada rikkumisega seotud teabe avalikustamise riski (Evchenko, 2016). Käesolev peatükk keskendub sisemisele vihjeandmisele, mis on organisatsiooni jaoks esmaseks ja eelistatud viisiks võimalike rikkumiste tuvastamiseks.

Kuigi juhid on sageli esimesed, kellele töötajad probleemidest või arvatavatest rikkumistest teada annavad (Saaremägi, 2021; Putri, 2018), ei pruugi töötajad alati juhtkonda usaldada. Lisaks esineb olukordi, kus juhid ise võivad olla rikkumise toimepanijad. Seetõttu on sisemise vihjeandmissüsteemi olemasolu organisatsioonis ülioluline.

Vihjeandmissüsteem koosneb vihjeandjast, vihjest, rikkumise toimepanijast ja vihjesaajast. Vihjeandja on isik, kes on avastanud rikkumise toimepanija poolt tehtud arvatava väärtegevuse ja annab selle kohta vihje vastutavale isikule organisatsiooni sees või väljaspool. (Bishop-Monroe et al., 2021) Vihjesaaja on organisatsioonis määratud vastutav

isik või osakond, kes võtab vihje vastu, hindab selle sisu ning otsustab edasiste sammude üle: kas tegeleda probleemiga organisatsioonisiseselt või on seaduserikkumise tõttu vaja välist sekkumist (Bishop-Monroe et al., 2021; Terracol, 2022).

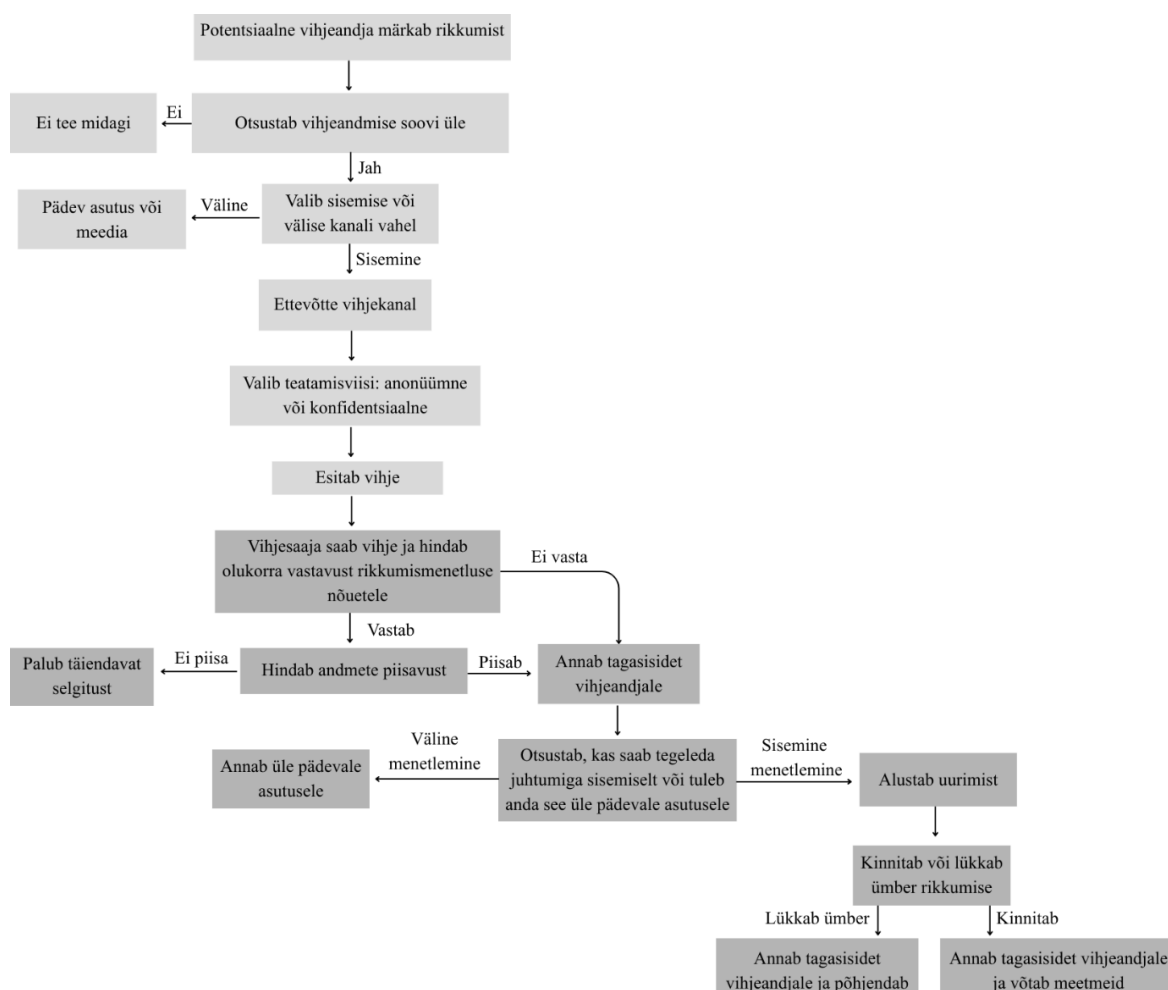
Vihjesaaja peab olema inimene, kelle puhul ei esine huvide konflikti, kes on sõltumatu vihjeandjatest ja arvatavate rikkumistega seotud pooltest ning kes omab tööülesannete täitmiseks vajalikke teadmisi, ressursse ja volitusi (Terracol, 2024). Tema teisteks ülesanneteks on vihjete menetlemine, tagasiside andmine vihjeandjale ja vihjeandmise protsessi täiustamine (Bishop-Monroe et al., 2021; Terracol, 2022). Vihjeandjale antav tagasiside peaks hõlmama perioodi vihje kättesaamisest kuni tulemuste saavutamiseni ja uurimise lõpuleviimiseni (Terracol, 2022). Regulaarne suhtlus vihjeandjaga on oluline, kuna see näitab, et vihjega tõesti tegeletakse (Palojärvi, 2021; Terracol, 2022; Jatsa, 2019), mis omakorda vähendab kahtlusi sisemiste protsesside suhtes (Saaremägi, 2021; Bishop-Monroe et al., 2021).

Samuti saab eristada anonüümset ja konfidentsiaalset vihjeandmist. Anonüümsuse korral organisatsioon ei tea vihjeandja identiteedi, aga konfidentsiaalsuse korral on identiteet vihjesaajale teada, kuid seda ei tohi väljaspool vihje menetlust avaldada (Terracol, 2022). Anonüümsuse korral võib olla takistatud põhjaliku uurimise läbiviimine, kuna vihjeandjat ei ole võimalik tuvastada (Hakim Z., Safira & Mahmuda, 2019; Furlow, 2011; Jatsa, 2019), et küsida temalt üksikasjalikumaid teavet, mis võiks uurimise tõhusust parandada (Putri, 2018). Selle probleemi vältimiseks saab kasutada vihjekanalit, mis võimaldab esitada teavet anonüümselt ning vihjesaajal ja -andjal suhelda täiendava teabe saamiseks ilma identiteeti teadmata (Terracol, 2022). Kuna aga vihjeandja ei pruugi pärast teabe esitamist enam edasises uurimises osaleda, tuleb juba vihje kogumise etapis esitada võimalikult täpsed küsimused (Jatsa, 2019).

Pärast uurimise lõpetamist tuleb rikkumine kõrvaldada või selle jätkumine ära hoida, vastutavaid isikuid karistada, vajadusel maksta hüvitist või edastada juhtumi kohta teavet pädevatele asutustele (Terracol, 2022). Kui vihje uurimise käigus selgub, et rikkumist ei ole toimunud, tuleb samuti vihjeandjat teavitada ja otsust põhjendada (Jatsa, 2019). Vihjesaajale võidakse määrata ka lisaülesandeid, kuid oluline on see, et need ülesanded ei kattuks teiste töötajate juhtimisega (Terracol, 2022). See on vajalik vihjesaaja sõltumatuse tagamiseks ja huvide konflikti ennetamiseks. Lisaülesannete määramine võib sobida väiksematele organisatsioonidele, kus rikkumiste hulk võib olla oluliselt väiksem.

Eelnevast tulenevalt algab vihjeandmise protsess (vt joonis 1) olukorras, kus potentsiaalne vihjeandja tuvastab potentsiaalse rikkumise ning otsustab, kas anda selle kohta

vihje või mitte. Eitava otsuse korral protsess katkeb, samas jaatav otsus suunab vihjeandjat valima sisemise ja välise vihjekanal vahel. Välise kanali valimisel edastab vihjeandja vihje pädevale asutusele või teatud juhtudel meediale. Sisemise kanali korral jääb vihje organisatsiooni sisse ning vihjeandja valib anonüümse ja konfidentsiaalse teatamisviisi vahel. Seejärel esitatakse vihje vastutavale isikule, kes jätkab protsessi.



Joonis 1. Vihjeandja ja -saaja otsustuspuid

Märkus: Vihjeandja tegevused on esitatud helehallil taustal ja vihjesaaja tegevused tumehallil taustal.

Allikas: Autor koostanud järgmiste allikate põhjal: Bishop-Monroe et al., 2021; Putri, 2018; Palojärvi, 2021; Furlow, 2011; Transparency International, n.d.; Tiits, 2014; Hakim Z., Safira & Mahmudah, 2019; Herish, 2002; Fischer & Gollwitzer, 2025; Terracol, 2022; Jatsa, 2019.

Pärast vihje kättesaamist hindab vihjesaaja esmalt, kas tegemist on rikkumisega, mis kuulub vihjekanal kaudu menetlemisele. Kui arvatav rikkumine ei vasta menetluse kriteeriumitele, teavitatakse vihjeandjat menetluse lõpetamisest koos põhjendusega. Kui aga

arvatav rikkumine kuulub menetlemisele, hinnatakse esitatud teabe piisavust. Ebapiisava teabe korral küsitakse vihjeandjalt täiendavaid selgitusi. Kui teave on aga piisav, teavitatakse vihjeandjat vihje saamisest ja alustatakse uurimist kas organisatsioonisiselt või edastatakse juhtum pädevale asutusele sõltuvalt rikkumise iseloomust ja raskusastmest. Uurimise tulemusena võib arvatav rikkumine leida kinnitust või saada ümber lükatud. Mõlemal juhul antakse vihjeandjale tagasisidet ning vajadusel rakendatakse ka asjakohaseid meetmeid.

Üle maailma kõige sagedamini kasutatavad vihjekanalid on veebivorm (40%), e-post (37%) ja telefoniliin (30%). Väiksemates organisatsioonides on soovitatav alustada kulutõhusate lahendustega, näiteks veebivormi või e-postiga. (ACFE, 2024) Täiendavalt võib kaaluda kirjalike vihjete kogumist posti teel (Palojärvi, 2021; Terracol, 2022), nagu teeb näiteks AS Eesti Energia, märgistades oma postkasti „Anna teada“ viitega (Jatsa, 2019). Mitme vihjekanaliga pakkumine on eeliseks, sest nii saab iga töötaja valida endale mugavaima ja turvalisema viisi (Aren, 2025). Lisaks on oluline arvestada töötajate töötingimusi: kui tööülesanded ei ole seotud arvutiga, ei pruugi veebivorm olla parim lahendus (Jatsa, 2019).

Kui siiski otsustatakse veebivormi kasuks, mis võimaldab nii anonüümset kui ka konfidentsiaalset vihjeandmist, peaks see sisaldama küsimusi arvatava rikkumise aja ja koha kohta ning laskma juhtumit võimalikult detailselt kirjeldada, küsides muu hulgas selle kohta, kuidas arvatavast rikkumisest teada saadi ja kas ka tõendeid omatakse. Konfidentsiaalse teatamise motiveerimiseks peaks vormis olema märgitud, kellele ja mis eesmärgil neid andmeid vaja on. Samuti tuleks kinnitada, et kogu teave jääb konfidentsiaalseks ja ainult vihje menetlemise eest vastutaval isikul on juurdepääs nendele andmetele. (Jatsa, 2019)

Kontsernis võivad ettevõtted luua ühise vihjekanalid, kuid rahvusvahelise kontserni puhul tuleb arvestada iga riigi õigusaktidega. Näiteks võib kasutada kahekanalilist vihjeandmissüsteemi, kus vihjeid menetletakse kohalikul tasandil, et tagada lähedus vihjeandjale ja protsessi tõhusus. Isegi kui emaettevõtte osaleb tütarettevõtte sisemise kanali kaudu saadud vihje uurimises, jääb tütarettevõttele kohustus vihjeandjaga suhelda, talle tagasisidet anda ja asjakohaseid meetmeid võtta. (Kusmierz, 2024; Ciupala, 2024)

Kuna omaenda vihjekanalid loomine võib olla keeruline ja kulukas, võivad organisatsioonid kaaluda teenusepakkujate loodud kanalite kasutamist (Palojärvi, 2021; Terracol, 2022). Näiteks Euroopa Komisjon soovib kasutada GlobaLeaksi tarkvara, mis on tasuta ja avatud lähtekoodiga, võimaldades ettevõtetel vähendada tarkvara nullist arendamise kulusid (European Commission, n.d.) ning muutes selle parimaks lahenduseks neile, kellel puuduvad piisavad ressursid vihjekanalid loomiseks. GlobaLeaks pakub nii anonüümset kui ka konfidentsiaalsust ning on hõlpsasti kohandatav ettevõtte vajadustele isegi mittetehniliste

kasutajate korral (European Commission, n.d.). Vihjeandmisel loob süsteem unikaalse koodi, mis võimaldab vihjet jälgida isegi anonüümse teatamisviisi korral (GlobaLeaks, n.d.). Programm on tõlgitud enam kui 70 keelde, sealhulgas eesti ja vene keelde (European Commission, n.d.), mis on paljude Eesti ettevõtete jaoks väga asjakohane ja mugav.

Vihjeandmissüsteemi loomisel tuleb kõigepealt välja töötada selge protsess, mida vaadatakse üle ja täiustatakse vähemalt kord aastas (Jatsa, 2019; Terracol, 2024). Selle abil tagatakse süsteemi tõhusus ja kehtivale seadusele vastavus (Terracol, 2024). Muudatused võivad põhineda töötajate küsitlustel või kogemustel, näiteks kui süsteemi tulemuslikkuses on ilmnenud lünki. Protsessi väljatöötamise kõrval tuleks koostada ka juhised, mis selgitaksid vihjeandmise vajalikkust ja kasulikkust organisatsiooni väärtuste järgimisel. Juhised peaksid määratlema muu hulgas selle, kes vastutab vihjete vastuvõtmise ja menetlemise eest, samuti selle, milleks andmeid kogutakse, kuidas neid töödeldakse ja millistel tingimustel need kustutatakse ning kuidas tagatakse andmekaitse. (Jatsa, 2019) Samuti tuleb juhistes täpsustada, kellel on õigus võimalikest rikkumistest teatada ja kaitset saada ning millistest võimalikest rikkumistest ja kuidas tuleks teatada (Jatsa, 2019; Terracol, 2022).

Kuna vihjeandja võib tunda hirmu, et teda ei usuta või tema vastu võidakse kasutada kättemaksumeetmeid, peaks võimaliku rikkumise uurimine olema prioriteet ja tuleks selgitada vihjeandmise eesmärki. Näiteks AS Circle K peab arvatavast rikkumisest teatamata jätmist tõsisemaks rikkumiseks kui valeandmete esitamist. (Jatsa, 2019) Siiski tuleks vaeinfo tahtliku esitamise riski vähendamiseks selgelt sõnastada, et vihjeandmise eesmärk ei tohi olla hirmutamine ega isikliku kasu saamine ning seda ei sallita (Palojärvi, 2021; Jatsa, 2019). Samuti tuleks juhistes selgitada, et vihjekanal ei ole mõeldud isiklike kaebuste esitamiseks, mis erinevad rikkumistest oma eesmärgi poolest: vihjeandmine toimub avalikes huvides, kaebuste esitamine aga erahuvides (Jatsa, 2019).

Oluline on ka regulaarselt informeerida töötajaid vihjekanalile olemasolust, see võiks toimuda vähemalt üks kord aastas näiteks koolitustel (Terracol, 2022; Jatsa, 2019; Palojärvi, 2021). Koolitustel saab rääkida nii vihjeandmise viisidest, teatamist vajavatest rikkumistest kui ka kaitse saamise võimalustest (Palojärvi, 2021). Üldiselt peab ka teave vihjeandmise võimaluse kohta olema avalikult kättesaadav ja nähtav, seda saab teha nii elektrooniliste kui ka füüsiliste kanalite kaudu (Terracol, 2024; Terracol, 2022). Kui organisatsioonil on siseveeb, saab seal hästi nähtaval kohal kuvada teabebänneri (Jatsa, 2019), mida klõpsates saab teavet vihjeandmise protsessi ja tingimuste kohta. Kasutada saab füüsilisi meeldetuletusi, levitades organisatsioonis infovoldikuid või riputades seintele plakateid koos vihjekanalile viiva QR-koodiga (Smirnova, 2024; Terracol, 2022; Jatsa, 2019).

Organisatsiooni eetikakoodeks peaks ette nägema võimaluse arvatavatest rikkumistest organisatsioonisiseselt teatada ja juhendama töötajaid seda kasutama, viidates sellise käitumise vastavusele organisatsiooni eetikanormide ja -standarditega (Bishop-Monroe et al., 2021). Koodeks peaks rõhutama ka vihjeandjate vastu suunatud kättemaksu ja muude ähvarduste keelatud (Bishop-Monroe et al., 2021; Terracol, 2022). Töötajatele koodeksi regulaarne meeldetuletamine võib tugevdada organisatsiooni eetiliste normide järgimist.

Paljud ettevõtted on juba loonud vihjeandmissüsteemid, millest leiab kasulikke lahendusi. Üks hea näide on hotellikett Hilton, mis haldab kõikidel kontinentidel 25 kaubamärki (Hilton, n.d.b). Hiltoni vihjekanalit tuuakse käesolevas töös välja näitena, kuna see on välja töötatud majutus- ja toitlustus valdkonna ettevõtete jaoks ning ühendab endas praktilisust ja kasutajasõbralikust.

Hilton pakub vihjeandmiseks veebivormi ja telefoniliini, mille kohta saavad töötajad teavet nii käitumisjuhendis, vihjeandmise veebilehel kui ka tööruumides olevatel trükitud materjalidel. Ühtlasi sisaldab kontserni käitumisjuhend näitlikke olukordi ja küsimusi, mis aitavad potentsiaalsetel vihjeandjatel otsustada, kas kõnealusel juhul on tegemist rikkumisega, millest tuleks märku anda. Näiteks palutakse neil kaaluda, kas tegevus on eetiline ja seaduslik ning kas ajalehes kõlapinda saades oleks see hea või halb uudis. (Hilton, n.d.a)

Enne veebivormi täitmist peab vihjeandja tutvuma teabe töötlemise tingimustega (Hilton, n.d.c) ning märkima enda ja arvatava rikkumise asukoha (Hilton, n.d.d). Mõningate riikide valimisel kuvatakse märkeruut, mis näitab, et neis piirkonnas saab vastavalt kohalikele seadustele teatada ainult teatud liiki rikkumistest (Hilton, n.d.d). Seejärel suunatakse vihjeandja lehele, kus on esitatud rikkumiste kategooriad, alates huvide konfliktidest ja dokumentide võltsimisest kuni diskrimineerimise ja uimastitega seotud rikkumisteni. Iga kategooria juures on ka selgitus, mis aitab mõista, mis selle kategooria alla kuulub. (Hilton, n.d.e) Pärast rikkumise kategooria valimist saab hakata veebivormi täitma (vt tabel 1).

Hiltoni veebivorm algab vihjeandjalt vihjeandmise tingimustega nõusoleku küsimisega. Seejärel saab vihjeandja valida, kas teatada arvatavast rikkumisest konfidentsiaalselt või anonüümselt. Konfidentsiaalse teatamise korral peab ta esitama oma nime ja kontaktandmed. Nii anonüümse kui ka konfidentsiaalse teatamise puhul peab vihjeandja märkima oma suhte ettevõttega. Seejärel peab vihjeandja esitama rikkuja isiku ja ametikoha, sealhulgas üksuse, kus rikkuja töötab. Ühtlasi saab vihjeandja täpsustada, kas arvatavast rikkumisest on teavitatud ka juhtkonda või personaliosakonda ja millal seda tehti. Veebivorm võimaldab vihjeandjal ka faile üles laadida, kui tal neid rikkumise kohta on.

Lõpus peab vihjeandja arvatavat rikkumist üksikasjalikult kirjeldama ja seejärel looma parooli, et saada jälgimisvõti. (Navex, n.d.)

Tabel 1

Hilteni veebivormi täitmise etapid

Etapi nimetus	Tegevus 1	Tegevus 2	Tegevus 3	Tegevus 4
Teatamisviis	Tingimustega nõustumine	Konfidentsiaalsus: nimi, kontaktandmed / Anonüümsus	Seos ettevõttega	
Arvatava rikkumise üksikasjad	Rikkuja andmed: nimi, ametinimetus, töökoht	Teave juhi/personaliosakonna teavitamise kohta	Faili üleslaadimine	Olukorra kirjeldus
Teatamisvõti	Parooli loomine			

Allikas: Autor koostanud Navex, n.d. põhjal.

Vihje jälgimise võimaluse kaudu saab ka anonüümse teatamise korral hoida vihjeandjaga ühendust, et paluda temalt täiendavaid selgitusi ja andes tagasisidet menetluse käigu kohta. Peale selle sisaldab Hilteni veebivorm suunavaid abivahendeid, näiteks rikkumiste kategooriate loetelu ning täiendavaid selgitusi, mis muudavad protsessi vihjeandja jaoks lihtsamaks. Veebivorm on loodud kasutusmugavust silmas pidades: vihjeandjat juhendatakse kogu protsessi vältel ning töövoog on intuitiivne. Käitumisjuhendis esitatud suunavate küsimuste ja olukordade kirjelduste olemasolu on heaks abivahendiks rikkumiste tuvastamisel ja mõtestamisel.

Tõhus sisemine vihjeandmissüsteem hõlmab nii selget protsessi, mitmekülgseid teatamisviise, anonüümsuse ja konfidentsiaalsuse tagamist kui ka vihjesaaja sõltumatust ning regulaarset tagasisidestamist. Siiski ei piisa vaid süsteemi loomisest – oluline on arvestada ka teguritega, mis soodustavad või takistavad töötajate valmisolekut vihjet anda.

1.3. Vihjeandmist soodustavad ja takistavad tegurid

Töötajate valmisolekut potentsiaalsetest rikkumistest teatada võivad mõjutada väga erinevad tegurid, mis ulatuvad riiklikust ja kultuurilisest tasandist organisatsioonilise ja individuaalse tasandini. Näiteks riikliku tasandi tegurite puhul saab riik soodustada vihjeandmist, võttes vastu õigusakte, mis tagavad vihjeandjate kaitse (Cordis & Lambert, 2017). Selliste õigusaktide loomine on oluline, sest vihjeandja võib seista silmitsi kättemaksu või rikkumise varjamise püüetega, mis avaldavad negatiivset mõju vihjeandmise kavatsusele (Trofimov, 2021; Evchenko, 2016; Hersh, 2002).

Õiguslik kaitse suurendab turvatunnet ja motiveerib arvatavast rikkumisest teatama (Mechtenberg, Muehlheusser & Roider, 2020; Cordis & Lambert, 2017; Palojärv, 2021). Vihjeandja vaatenurgast võivad riskide hulka kuuluda töökoha kaotamine, nii-öelda musta nimekirja sattumine, tööülesannete muutmine, sotsiaalsesse isolatsiooni jäämine või õiguslik hirmutamine, mis omakorda võivad halvendada nii vihjeandja füüsilist ja vaimset tervist kui ka tema majanduslikku ja sotsiaalset olukorda (Hakim Z., Safira & Mahmudah, 2019; Ramazanov, 2016; Dungan, Waytz & Young, 2015; Hersh, 2002; Furlow, 2011; Qasem, 2025; Transparency International, 2025; Terracol, 2022).

Riikide- ja kultuuridevahelised erinevused mõjutavad viisi, kuidas vihjeandmisse suhtutakse. Näiteks USA-s suhtutakse vihjeandmisse positiivsemalt kui Aasia riikides, mida võib seostada ameeriklaste individualistliku ja aasialaste kollektivistliku kultuuriga. (Dungan, Waytz & Young, 2015) Kollektivism on iseloomulik kultuuridele, kus kogukonna vajadused seatakse indiviidi vajadustest kõrgemale ja kus rõhutatakse sotsiaalseid norme. Individualism seevastu eeldab vähem sidusaid grappe ja indiviidi suuremat tähtsust. (Komisarof & Akaliyski, 2025) See tähendab, et mida ühtsem on kogukond, nagu Aasia riikides, seda väiksem on tõenäosus, et selle liikmed teatavad potentsiaalsetest rikkumistest, kuna nad on üksteisele väga lojaalsed. USA-le iseloomulik individualism seevastu vähendab negatiivset suhtumist potentsiaalsete rikkumiste paljastamisse. (Dungan, Waytz & Young, 2015)

Organisatsiooni tasandi tegurite puhul tuleb rõhutada, kuivõrd oluline on see, et juhtkond kujundaks eetilisele orienteeritud keskkonna, mis soodustaks eetilist käitumist järgmiste tegevuste abil: töötajate teavitamine vajadusest anda teada potentsiaalsetest rikkumistest, töötajatele turvalise vihjekanaliloomine ja vihjeandjate kaitsmine (Palojärv, 2021; Ibrahim et al., 2025; Dungan, Waytz & Young, 2015; Daroglou et al., 2025; Bishop-Monroe et al., 2021). Kui aga organisatsioonis on valdav autoritaarne kultuur, võib inimene otsustada vihjet mitte anda, kuna kardab, et vihjeandmine mõjutab teda negatiivselt. Sel põhjusel peavad juhid looma töötajatele turvalise keskkonna, sealhulgas tagama nende psühholoogilise turvalisuse, ja juurutama töötajate seas vastutustundlikku kultuuri, andes seeläbi mõista, et vihjeandmine on organisatsioonis teretulnud (Ibrahim et al., 2025).

Vähene valmisolek vihjet anda võib olla tingitud stiimulite puudumisest, näiteks ei ole organisatsioonis vihjekanalit või ei pakuta koolitusi, mis aitaksid töötajatel teada saada vihjekanaliloomisest ja seda usaldada (Dungan, Waytz & Young, 2015; Puh & Tökke, 2024; Palojärv, 2021). Vihjeandmiseks loodud vihjekanal on ebatõhus, kui vihjeid ignoreeritakse, sest neid ei usuta või neisse ei suhtuta tõsiselt (Saaremägi, 2021; Palojärv, 2021). Vihjete ignoreerimine ja tegevusetus võib viidata organisatsiooni ükskõiksusele ja

vihjeandja heatahtlikkuse eiramisele, mis võib kaasa tuua selle, et vihjetest teatatakse väljaspool organisatsiooni ja organisatsioonisisene vihjeandmine väheneb (Saaremägi, 2021; Palojärv, 2021).

Vihjeandmise protsessi usaldamiseks tuleb pakkuda asjakohaseid koolitusi nii uutele töötajatele kui ka regulaarse meeldetuletusena vanematele töötajatele (Terracol, 2022). See aitab vihjeandmist tõhustada, kuna teadlikkuse tõstmine viib põhjalikumate ja asjakohasemate vihjeteni (Saaremägi, 2021; Palojärv, 2021). Muu hulgas tuleks koolitustel rõhutada, et vihjeandmine on eetiline ja väärtuslik tegevus, mis parandab organisatsiooni läbipaistvust (Qasem, 2025).

Üheks täiendavaks organisatsioonipoolseks stiimuliks võib olla premeerimine. Näiteks USA-s makstakse vihjeandjatele kuni 30% valitsusasutuse poolt sissenõutud summast. Valitsuse pakutavate rahaliste stiimulite tõttu võivad organisatsioonid pidada tulusamaks pakkuda sarnaseid rahalisi hüvesid organisatsioonisisese teatamise eest, et kolmandad pooled jääksid kaasamata. (Bishop-Monroe et al., 2021) Tasustatud vihjed võivad hõlmata väga tõsiste rikkumiste paljastamist, mis nõuavad viivitamatut tegutsemist ning põhjustavad organisatsioonile ja ühiskonnale olulist kahju, näiteks korruptsioon.

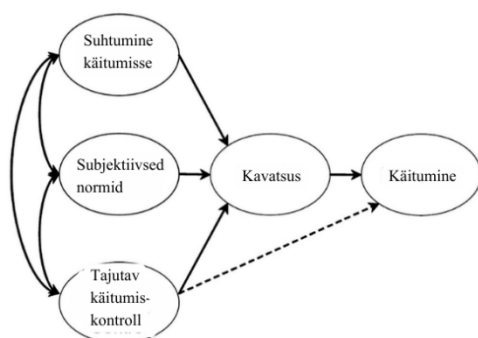
Trofimov (2021) ja Putri (2018) seevastu väidavad, et arvatavast rikkumisest teatanud vihjeandjad ei vaja avalikkuse huvides preemiaga motiveerimist, kuna otsustades vihjet anda, arvestatakse ka võimalike riskide ja muude teguritega. Premeerimise vähest rolli Ida-Euroopas ning Lääne- ja Kesk-Aasias kinnitab ka ACFE (2024) aruanne, mille kohaselt on preemiad vihjeandmise motiveerimiseks kõige vähem efektiivne viis, ainult 8% juhtumitest.

Samas ei ole rahaline premeerimine ainus viis vihjeandjate tänamiseks ja vihjeandmise motiveerimiseks. Näiteks võidakse väga tõsiseid rikkumisi avastanud vihjeandjatele anda ka tänukirju või kanda nad auraamatusse (Ramazanov, 2016), millega kaasnev uhkustunne ja tunnustus võib samuti suurendada vihjeandmise motivatsiooni. Seejuures tuleb aga arvestada, et anonüümse vihjeandmise korral jääb vihjeandja identiteet teadmata ning tunnustamine on võimatu. Konfidentsiaalse vihjeandmise puhul on tunnustamine võimalik kas konfidentsiaalses vormis või vihjeandja nõusolekul avalikult.

Vihjeandmise motivatsiooni tuleb suurendada mitte ainult üksikisikute mõjutamise, vaid ka lojaalse grupi loomise kaudu, mis suhtub rikkumistesse negatiivselt (Dungan, Waitz & Young, 2015). Grupi suhtumise muutmine vihjeandmisse positiivsemaks, vastutustunde suurendamine ja selliste eksiarvamuste kummutamine, mille kohaselt kaastöötajad suhtuvad vihjeandmisse negatiivselt, võib parandada vihjekanal toimimise tõhusust, mis aitab

omakorda kaasa üldisele eesmärgile korrigeerida ebaeetilist ja sotsiaalselt hälbivat käitumist (Dungan, Waytz & Young, 2015; Djawadi, Plaß & Loer, 2025; Daroglou et al., 2025).

Indiviidi tasandiga seotud tegurite puhul on oluline kõigepealt mõista, mis mõjutab inimeste käitumist vihjeandmisel. Planeeritud käitumise teooria on üks lähenemisviise, mis aitab mõista inimese käitumist, ennustades seda lähtuvalt inimese kavatsusest tegevus sooritada (Nur'aini & Pujiningsih, 2021; Ajzen, 2020) ehk arvatavast rikkumisest teatada või sellest teatamata jätta. Teooria kohaselt sõltub käitumine kavatsusest, mida omakorda kujundavad kolm peamist tegurit (vt joonis 2): suhtumine käitumisse, subjektiivsed normid ja tajutav käitumiskontroll. Need tegurid kujundavad inimese kavatsuse arvatavast rikkumisest teatada, mis omakorda koos tajutava käitumiskontrolliga määrab tegeliku käitumise. (Ajzen, 1991; Ajzen, 2020)



Joonis 2. Planeeritud käitumise teoorias aluseks võetavate tegurite mõju käitumisele
Allikas: Ajzen, 1991, autori tõlge.

Suhtumine teatud viisil käitumisse viitab sellele, kui positiivselt või negatiivselt inimene hindab kavandatavat tegu. Hinnang kujuneb selle põhjal, millised tagajärjed inimene usub sel teol olevat ja kas need tagajärjed on tema arvates soovitatavad (Ajzen, 2020; Puh & Tökke, 2024). Teisisõnu, vihjeandmise kontekstis hindab vihjeandja arvatavast rikkumisest teatamise tegu ja selle tagajärge. Näiteks võib vihjeandja uskuda, et arvatavast rikkumisest organisatsioonisisese vihjekanali kaudu teatamine aitab vältida organisatsioonile tekitatavat mainekahju ja kaitsta kaastöötajaid, ning see muudab teo tema jaoks positiivseks.

Subjektiivsed normid aga peegeldavad inimese tajutavat sotsiaalset survet, kusjuures ta hindab, kas tema ümbruskond kiidab teatud käitumise ehk vihjeandmise heaks või mõistab selle hukka (Ajzen, 2020). Kui organisatsiooni töötajad peavad vihjeandmist üldiselt kaebamiseks, on kavatsus rikkumisest teatada nõrgem. Ja vastupidi, kui organisatsioon toetab vihjeandmist, siis teatamise tõenäosus kasvab.

Tajutav käitumiskontroll näitab, kui lihtsaks või keeruliseks inimene teatud käitumise sooritamist (Ajzen, 2020) ehk vihjeandmist peab. See sõltub ressursside ja takistuste olemasolust ning enda võimetest (Ajzen, 2020). Näiteks kui vihjeandja kardab vihjeandmisega kaasneda võivat kättemaksu, siis tajutav käitumiskontroll on madal ja kavatsus rikkumisest teatada nõrgeneb. Samas võib tugev tajutav käitumiskontroll leevendada negatiivse suhtumise või normide mõju kavatsusele (Ajzen, 2020). Näiteks võib töötaja karta kolleegide negatiivset suhtumist, ent kui tal on tugev veendumus, et organisatsioonis on turvaline ja konfidentsiaalne vihjekanal, siis tajutav käitumiskontroll võib suurendada tema kavatsust potentsiaalsest rikkumisest teatada.

Vihjeandmise valmidust võivad mõjutada ka muud individuaalsed tegurid, näiteks vanus, isiksuseomadused ja ametikoht. Nooremad töötajad teatavad arvatavatest rikkumistest suurema tõenäosusega (Palojärvi, 2021), seevastu vanemate töötajate puhul võib teatamise tõenäosus organisatsioonilise lojaalsuse või kättemaksuhirmu tõttu olla väiksem (Puh & Tõkke, 2024). Vanuse mõju võib tuleneda ajaloolisest kontekstist, näiteks Eestis võib vanematel inimestel olla vihjeandmise suhtes negatiivne suhtumine Nõukogude Liidu aegse autoritaarse valitsemisviisi tõttu (Puh & Tõkke, 2024; Palojärvi, 2021; Jatsa, 2019). Kuna Nõukogude Liitu iseloomustas range sotsiaalne kontroll ja vihjeandjate ülesanne oli teisitimõtlemine maha suruda, tekkis umbusaldus igasuguse vihjeandmise suhtes (Puh & Tõkke, 2024; Korruptsioonivaba Eesti, n.d.; Jatsa, 2019). Sel põhjusel võivad vanemad põlvkonnad tajuda vihjeandmist ohuna oma turvalisusele ja karta võimalikku tagakiusamist (Puh & Tõkke, 2024). Vihjeandmise negatiivse kuvandi parandamiseks tuleb panustada töötajate harimisse koolituste kaudu (Puh & Tõkke, 2024; Palojärvi, 2021).

Isiksuseomadustest lähtudes annab ekstravert vihjet suurema tõenäosusega (Dungan, Waytz & Young, 2015), mis võib peegeldada tema väiksemat hirmu teiste inimeste reaktsioonide ja tähelepanu ees. Muu hulgas võib vihjeandjat mõjutada tema roll organisatsioonis: mida kõrgem on töötaja ametikoht, seda tõenäolisemalt on tal juurdepääs konfidentsiaalsele teabele, suurem võim ja volitused probleemide lahendamiseks ning rohkem ressursse ja ekspertteadmisi, mis suurendab teatamise tõenäosust (Hakim Z., Safira & Mahmudah, 2019; Puh & Tõkke, 2024; Dungan, Waytz & Young, 2015). See toimib ka vastupidises suunas: kui rikkujal on võim, saab ta veenda rohkem inimesi enda poolele asuma ja nõrgestada vihjeandja positsiooni (Hakim Z., Safira & Mahmudah, 2019). Lisaks, mida kauem on vihjeandja organisatsioonis töötanud, seda tõenäolisemalt ta rikkumisest teatab (Dungan, Waytz & Young, 2015).

Tabel 2

Vihjeandmist mõjutavad tegurid

Teguri tasand	Tegur	Mõju vihjeandjale	Valmidus teatada
Riiklik ja kultuuriline	Õigusliku kaitse olemasolu	Tunneb kaitset.	Kõrgem
	Individualistlik kultuur	Keskendub rohkem isiklikele väärtustele ja õiglusele.	Kõrgem
	Kaitse puudumine Kollektivistlik kultuur	Kardab negatiivseid tagajärgi. Kardab teatamisega kahjustada kaastöötajaid või organisatsiooni.	Madalam Madalam
Organisatsiooni	Turvalise vihjekanali kättesaadavus	Tunneb end vihjet andes turvalisemalt.	Kõrgem
	Töötajate koolitamine	Teab, kuidas teatada.	Kõrgem
	Juhtkonna tugi	Usaldab protsessi rohkem.	Kõrgem
	Rahaline premeerimine	Saab täiendava motivatsiooni.	Kõrgem
	Tänu kiri/auraamat	Tunneb uhkust.	Kõrgem
	Vihje kanali puudumine	Puudub turvaline võimalus rikkumisest teatada.	Madalam
Individuaalne	Autoritaarne kultuur	Kardab negatiivset reaktsiooni.	Madalam
	Vihjete ignoreerimine	Arvab, et vihjeandmine on mõttetu.	Madalam
	Vastutustunne ja soov kahju ära hoida	On motiveeritud kaitsma kaastöötajaid ja organisatsiooni.	Kõrgem
	Noorem vihjeandja	Suhtub vihjeandmisse positiivsemalt.	Kõrgem
	Ekstravertsus	Ei karda oma seisukohta avaldada.	Kõrgem
	Pikk tööstaaž organisatsioonis	Tunneb organisatsiooni paremini ja omab rohkem teavet.	Kõrgem
	Kõrge ametikoht	Tunneb end vastutustundlikumana.	Kõrgem
	Negatiivsed tagajärjed	Väldib ohtu.	Madalam
	Vanem vihjeandja	Ajaloolise mineviku tõttu võib tajuda vihjeandmist negatiivsemalt.	Madalam
	Introvertsus	Väldib endale tähelepanu tõmbamist.	Madalam
	Madal ametikoht	Võib karta tagajärgi.	Madalam
	Lühike tööstaaž	On vähem seotud olemasolevate normidega.	Madalam

Allikas: Autor koostanud järgmiste allikate põhjal: Cordis & Lambert, 2017; Dungan, Waytz & Young, 2015; Ramazanov, 2016; Palojärvi, 2021; Saaremägi, 2021; Ajzen, 2020; Djawadi, Plaß & Loer, 2025; Daroglou et al., 2025; Puh & Tökke, 2024; Komisarof & Akaliyski, 2025; Bishop-Monroe et al., 2021; Ibrahim et al., 2025.

Tabel 2 koondab vihjeandmist mõjutavad tegurid kolmel tasandil: riiklikul, organisatsioonilisel ja individuaalsel tasandil. Iga tegur kas suurendab vihjeandmise valmidust või hoopis vähendab seda. Samas võib tegurite koosmõju olenevalt kontekstist olla erinev.

Vihjeandmise valmidust suurendavad eelkõige õigusliku kaitse olemasolu, turvalise vihjekanaliga kättesaadavus, juhtkonna toetus ja töötajate teadlikkus vihjeandmissüsteemist. Teatamisvalmidust võivad aga vähendada hirm negatiivsete tagajärgede ees, autoritaarne organisatsioonikultuur ja vihjete ignoreerimine. Teatamisvalmidus sõltub ka sellistest individuaalsetest teguritest nagu vanus, isiksuseomadused, ametikoht ja tööstaaž: noorem iga, ekstravertsus, kõrgem ametikoht ja pikaajaline tööstaaž suurendavad teatamisvalmidust, seevastu hirm negatiivsete tagajärgede ees, vanem iga, introvertsus, madalam ametikoht ja lühike tööstaaž vähendavad seda.

2. Vihjekanaliloomise uuring ettevõttes X

2.1. Uuritav ettevõtte, uurimismetoodika ja valim

Käesoleva töö empiirilises osas viidi läbi uuring teenindusettevõtte X näitel, mille nimi on ettevõtte enda soovil esitatud anonüümsel kujul. Ettevõtte X on tegutsenud majutus- ja toitlustusvaldkonnas üle 15 aasta, pakkudes lisaks majutusele ja toitlustusele ka spaa- ja heaoluteenuseid ning konverentside korraldamise võimalust. Ettevõtte kuulub hotelliketti ja annab tööd enam kui 50 inimesele (suhtlus kontaktisikuga, 2026). Seega pidi ta vihjeandja kaitse seaduse kohaselt olema 2025. aasta alguseks loonud endale sisemise vihjekanaliga, mis võimaldaks potentsiaalsetest rikkumistest konfidentsiaalselt teatada (TÕRTKS, 2024). Uuringu läbiviimise ajal, 2026. aasta märtsis eraldi vihjekanalit uuritavas ettevõttes veel ei olnud (suhtlus kontaktisikuga, 2026).

Ettevõttel X on kehtivad sisekorraeeskirjad, mis on üles pandud puhkeruumide infotahvlitele ning reguleerivad töötajate käitumist ja probleemidest teatamise korda. Iga uus töötaja tutvub eeskirjadega tööle asumisel ning kinnitab nende omaksvõtu allkirjaga. Probleemi ilmnemisel peab töötaja esmalt pöörduma oma vahetu juhi poole, kuid probleemi lahendamise ebaõnnestumisel, võib töötaja pöörduda ettevõtte direktori poole. (Smirnova, 2024) Varem oli hotelliketil eraldi personaliosakond, kuid enam mitte, mistõttu töölevõtmise, konfliktide lahendamise ning muude tööga seotud küsimustega tegelevad ettevõtte tasandil osakondade juhid ja direktor (suhtlus kontaktisikuga, 2026).

Uuring tehti 2026. aasta märtsis ja aprillis kombineeritud lähenemisviisi rakendades (vt tabel 3), millel on nii kvantitatiivseid kui ka kvalitatiivseid tunnuseid. Andmete kogumise meetodina kasutati veebipõhist küsitlust, mis viidi läbi ettevõtte töötajate ja juhtide seas.

Sarnast lähenemist on varem kasutanud näiteks Palojärvi (2021), Fischer (2025) ja Daroglou et al. (2025), kes uurisid töötajate suhtumist vihjeandmisesse ja erinevate tegurite mõju teatamisvalmidusele.

Tabel 3

Empiirilise osa tegevuste ajakava

Tegevus	Ajaperiood	Tegevuse kirjeldus
Küsimustiku ettevalmistamine	12.02.2026–06.03.2026	Küsimustiku koostamine teoreetilise osa ja kirjanduse põhjal, kooskõlastamine juhendajaga ja paranduste sisseviimine (12.02–06.03); tõlkimine eesti ja vene keelde (06.03–07.03); testimine kahe inimese peal (09.03) ning tehniliste vigade parandamine Google Forms (09.03)
Andmete kogumine	09.03.2026–18.03.2026	Küsimustiku saatmine kontaktisikule ja levitamine (09.03); meeldetuletuse saatmine (13.03)
GlobaLeaksi funktsionaalsuse uurimine ja testimine	13.03.2026–14.03.2026	GlobaLeaksi demoversiooni seadistamine ja katsetamine
Andmete analüüsimine	19.03.2026–22.03.2026	Vastuste laadimine Excelisse, andmete korrastamine, avatud vastuste temaatiline rühmitamine ning analüüsi läbiviimine (19.03–20.03); tulemuste analüüsimine ja järelduste tegemine (21.03–22.03)
Vihjekanali demoversiooni loomine	22.03.2026–23.03.2026	Demoversiooni loomine ettevõtte X jaoks GlobaLeaksis
Lõplike järelduste tegemine	03.04.2026–07.04.2026	Soovituste väljapakkumine teoreetilise käsitluse ja empiirilise uuringu alusel

Allikas: Autori koostatud.

Küsitluse eesmärk oli tuvastada teenindusettevõtte X töötajate kogemused, hoiakud ja eelistused vihjeandmise suhtes ning kogutud teave aitas koostada töötajate silmis mugavama ja turvalisema vihjekanali loomise soovitusi. Küsimustik (vt lisa C) sisaldas 18 küsimust, millest 13 olid suletud ehk valikvastuste või hinnanguskaaladega ja viis olid avatud. Likerti skaalat on kasutanud uuringutes ka näiteks Hakim, Safira ja Mahmudah (2019) ning Palojärvi (2021). Hinnanguskaalade abil uuriti tegurite olulisust, sisemise vihjekanali olemasolu vajalikkust ja kasutamise tõenäosust ning vihjekanalite vormide sobivust. Suletud küsimused võimaldasid koguda kvantitatiivseid andmeid töötajate hoiakute, eelistuste ja vihjekanali kasutamise valmisoleku kohta. Avatud küsimused andsid võimaluse saada lisaselgitusi kogemuste, arvamuste ning ettepanekute kohta.

Küsimustiku algusesse lisati sissejuhatus, mis selgitas uuringu eesmärgi, osalemise vabatahtlikkust ja anonüümsust ning kinnitas, et andmeid kasutatakse ainult selle magistritöö tarbeks. Kuna ettevõtte X on kakskeelne, koostati küsimustik eesti ja vene keeles. See muutis osalemise kõigile töötajatele kättesaadavamaks ja suurendas vastuste täpsust.

Küsimustiku koostamisel tugineti käesoleva töö teoreetilisele osale ja varasematele vihjeandmise teemal tehtud uuringutele (vt tabel 4), kusjuures ka suletud või skaalaküsimuste vastusevariandid olid koostatud teoreetilises osas käsitletud teemade abil. Küsimustik oli jagatud mitmeks temaatiliseks osaks.

Tabel 4

Küsimuste koostamisel aluseks võetud varasemate teadustööde aines

Selle uuringu küsimuse teema	Küsimuste sõnastamisel aluseks võetud teemad ja allikad
Küsimus 3: Võimaliku rikkumise märkamine	Kokkupuude tööalase rikkumisega (Jatsa, 2019)
Küsimus 5: Teavitamiskogemus	Vihjeandmise kogemus (Palojärvi, 2021)
Küsimus 6: Võimalikust rikkumisest teavitamise viis ja selle tulemus	Vihjeandmise viis (Palojärvi, 2021)
Küsimus 8: Esmane tegevus võimaliku rikkumise avastamisel	Töötajate teavitamiskäitumine rikkumise avastamisel (Jatsa, 2019)
Küsimus 9: Võimaliku rikkumise kohta vihje andmise vajadus ja viis	Teavitamisotsus ja vihjeandmise viis (Fischer ja Gollwitzer, 2025)
Küsimus 11: Riskide olulisus teatamisotsuse tegemisel	Vihjeandmist takistavad tegurid (Jatsa, 2019)
Küsimus 12: Vihjekanalite omaduste olulisus	Vihjeandmist soodustavad tegurid (Palojärvi, 2021)
Küsimus 13: Vihjekanalite olemasolu olulisus teenindusettevõtte X jaoks	Vihjekanalite olemasolu olulisus organisatsioonis (Palojärvi, 2021)
Küsimus 14: Loodud vihjekanalite kasutamise tõenäosus	Vihjeandmise soodustamise võimalus vihjekanalite olemasoluga (Palojärvi, 2021)
Küsimus 15: Teatamisviiside sobivus	Teatamisviiside eelistused (Palojärvi, 2021)
Küsimus 17: Vihjekanalite korralduse sobivus	Vihjekanalite korralduse eelistused (Palojärvi, 2021)

Märkus: Esitatud on ainult need küsimused, mis põhinesid käesoleva töö teoreetilises osas käsitletud teadustöodes läbiviidud küsitlustel.

Allikas: Autor koostanud järgmiste allikate põhjal: Fischer & Gollwitzer, 2025; Jatsa, 2019; Palojärvi 2021.

Esimese kahe küsimusega koguti demograafilisi andmeid vastajate tööstaaži ja ettevõttes täidetava rolli kohta. Neid tunnuseid valiti teadlikult vaid kaks, et säilitada vastajate anonüümsus, kuna liiga paljude demograafiliste küsimuste lisamine oleks suhteliselt väikeses

ettevõttes suurendanud äratundmise riski. Samas on need kaks tunnust uurimise jaoks olulised, sest võimaldavad võrrelda vastuseid kogemuse taseme ja ametipositsiooni lõikes. Need tunnused valiti demograafilisteks näitajateks, kuna kirjandusest tuli välja, et inimesed, kes on ettevõttes töötanud kauem ja kellel on kõrgem ametikoht, on suurema tõenäosusega valmis vihjet andma (Puh & Tökke, 2024; Dungan, Waytz & Young, 2015).

Küsimused 3–8 võimaldasid välja selgitada vastajate varasema kogemuse rikkumistega, nende tegeliku käitumise sellistes olukordades ning hüpoteetilise tegutsemise võimaliku rikkumise avastamisel. Küsimusega 9 uuriti, kuidas vastajad tajuvad erinevaid rikkumisega seotud olukordi ning kas ja milliste kanalite kaudu neist tuleks teavitada. Järelküsimus 10 andis võimaluse oma vastuseid täpsustada. Küsimused 11 ja 12 keskendusid vihjeandmisega seotud riskide olulisusele ning vihjekanalil puhul soovitud omadustele. Küsimused 13–15 aitasid välja selgitada, milline on töötajate suhtumine vihjekanalil vajalikkusesse, milline on nende valmisolek kanalit kasutada ning milliseid kanalite vorme nad eelistavad. Viimaste küsimuste 17 ja 18 abil uuriti, millist vihjekanalil korraldust peavad vastajad kõige sobivamaks, ning paluti vastajatel valikut põhjendada.

Enne küsimustiku levitamist testiti seda kahe inimese peal: üks oli autori töökaaslane finantssektorist ja teine oli ettevõtte X kontaktisik. Testimise käigus avaldus Google Formsil skaalaküsimuste puhul tehniline probleem, mis seisnes seades „Piirang ühe vastusega veeru kohta“ ja takistas mitme variandi märkimist ühes veerus. Probleem kõrvaldati kohe pärast tuvastamist, nii et ühes veerus sai edaspidi märkida mitu vastust. Küsimustiku loogika ja arusaadavusega probleeme ei esinenud.

Küsimustik saadeti ettevõtte X kõigile 75 töötajale ja juhtidele ettevõttesisese kontaktisiku vahendusel Google Formsil lingina. Link edastati 9. märtsil 2026 ja esialgu laekus 32 vastust. Osavõtu suurendamiseks saadeti 13. märtsil töötajatele uuringu kohta meeldetuletus, mille tulemusena lisandus uusi vastajaid. Uuringus osales kokku 44 töötajat, mis moodustas 58,7% töötajate ja juhtide koguarvust. Analüüsis kasutatakse vastajate koguarvu tähistamiseks tähist *N*. Valim hõlmas töötajaid ja juhte eri osakondadest ja ametikohtadelt (vt tabel 5), kusjuures ainult viis vastajat märkisid, et töötavad juhtival ametikohal, ja üks otsustas oma rolli mitte täpsustada.

Vastajate tööstaaz varieerus laialt. Suurima rühma moodustasid kuni 4-aastase tööstaaziga vastajad, neile järgnesid üle 15-aastase tööstaaziga vastajad. Väikseima osa moodustasid vastajad, kelle tööstaaz jäi vahemiku 5–14 aastat, oli ka neid, kes ei täpsustanud tööstaazi. Seega võib öelda, et uuringusse oli kaasatud nii suhteliselt uusi kui ka pikaajalise töökogemusega töötajaid ja juhte.

Valim on üldjoontes esinduslik, kuid esineb mõningaid erinevusi rühmade lõikes. Juhid on valimis mõnevõrra ülesindatud, kuna nende osakaal valimis (11,4%) ületab nende tegeliku osakaalu ettevõttes (9,3%). Töötajad seevastu on kergelt alaesindatud, kuna nende osakaal valimis (86,4%) jääb alla nende tegelikule osakaalule ettevõttes (90,7%). Tööstaaži lõikes ilmneb, et kuni 4-aastase tööstaažiga vastajad on valimis ülesindatud (osakaal valimis 43,2% ja tegelik osakaal 36%), samas 5–14-aastase (osakaal valimis 20,5% ja tegelik osakaal 25,3%) ja üle 15-aastase tööstaažiga vastajad (osakaal valimis 31,8% ja tegelik osakaal 38,7%) on pigem alaesindatud. Vaatamata mõningatele erinevustele võib valimit pidada piisavalt suureks ja üldjoontes esinduslikuks, et uuringu tulemusi laiendada ettevõtte kogu töötajaskonnale.

Tabel 5

Küsimustiku valimi jaotus ja rühmade esindatus

Rühm	Töötajaskonna koguarv (N = 75)	Töötajaskonna osakaal (%)	Valimi koguarv (N = 44)	Valimi osakaal (%)	Valimisse kaasatuse määr (%)
Roll					
Töötaja	68	90,7	38	86,4	55,9
Juht	7	9,3	5	11,4	71,4
Määramata	–	–	1	2,3	–
Tööstaaž					
Kuni 4 aastat	27	36	19	43,2	70,4
5–14 aastat	19	25,3	9	20,5	47,4
Üle 15 aasta	29	38,7	14	31,8	48,3
Määramata	–	–	2	4,5	–

Allikas: Autor koostanud küsitluse vastuste ja kontaktisikuga toimunud suhtluse (2026.b) põhjal.

Vastused laaditi Microsoft Excelisse, kusjuures sõnalised skaalad teisendati numbrilisteks. Näiteks vihjekanalil vajalikkuse kohta esitatud küsimuse vastused, mis hõlmasid vahemikku „üldse mitte vajalik“ kuni „väga vajalik“, muudeti numbriteks nii, et „üldse mitte vajalikust“ sai „1“ ja „väga vajalikust“ sai „5“. Samuti jagati vastused vastajate rollide ja töötamise kestuse järgi, mis võimaldas võrrelda erinevate rühmade arvamusi ja tuvastada võimalikke erinevusi nende vastustes.

Andmeid analüüsiti funktsiooni Data Analysis abil, kasutades kirjeldavat statistikat, korrelatsioonianalüüsi ja regressioonanalüüsi. Kirjeldav statistika võimaldas saada ülevaate vastuste üldisest jaotumisest, arvutades keskmisi väärtusi, mediaane ja standardhälbeid. Samuti tuvastati korrelatsioonianalüüsi abil seoseid erinevate vihjekanalil omaduste vahel, mis

aitas selgitada, millised tegurid on omavahel tugevalt seotud. Korrelatsiooni tugev seos on defineeritud, kui väärtus on vahemikus 0,7–1 (Ratner, 2009). Likerti skaalade vastuste analüüsimisel võeti kasutusele mediaan, mitte keskmine väärtus, kuna Sullivan ja Artino (2013) järgi on skaala järjestustunnus ja erinevus vastusevariantide vahel ei ole alati võrdne. Kasutatavate analüüside lähenemine on kooskõlas Palojärvega (2021), kes kasutas oma uuringus töötajate hoiakute analüüsimiseks kirjeldavat statistikat ja korrelatsioonianalüüsi.

Lisaks viidi läbi regressioonanalüüsi, mis võimaldas kindlaks teha, millised omadused on statistiliselt olulised vihjeandmise valmiduse ennustamisel. Täiendavalt viidi läbi paaristatud t-test (ingl *t-Test: paired two sample for means*) Data Analysis tööriista abil, et võrrelda erinevate vihjekanali vormide keskmisi hinnanguid ning hinnata, kas nende vahel esineb statistiliselt olulisi erinevusi. Avatud küsimuste vastused rühmitati aga jagatud konteksti ja tähenduse järgi, mis võimaldas tuvastada peamised korduvad teemad ja ideed. Analüüsi hõlbustamiseks oli iga sarnaste vastuste kategooria värvikoodiga tähistatud, mis aitas andmeid paremini visualiseerida ja näha järelduste tegemiseks vajalikku üldpilti.

Teema teoreetilise käsitlemise, küsitluse tulemuste ja analüüsi põhjal töötati välja vihjekanali demoversioon, mille eesmärk oli näidata vihjekanali praktilist rakendusvõimalust, mida uuritav ettevõtte saaks kasutada. Kulude kokkuhoidmiseks pakuti ettevõttele X välja võimalus kasutada Euroopa Komisjoni soovitatavat tasuta GlobaLeaksi (European Commission, n.d.). Demoversiooni loomisel ühendati käesoleva töö teoreetiline käsitus ja empiirilise osa tulemused ning selle põhjal anti uuritavale teenindusettevõttele soovitusi vihjekanali loomiseks ja selle kasutusele võtmiseks.

2.2. Empiirilise uuringu tulemuste analüüs

Läbiviidud uuringu tulemuste põhjal selgus, et pooled vastajatest on töökohal pealt näinud olukordi, mida nad on pidanud rikkumiseks või väärkäitumiseks. Samas tõid mitmed vastajad avatud vastustes välja, et neil oli raske kindlaks teha, kas konkreetset olukorda pidada rikkumiseks või mitte. See osutab vihjekanali loomisega seoses olulisele vajadusele: töötajatele tuleb selgitada, millistest olukordades on vaja teatada.

Avatud vastuste põhjal (vt lisa D) tulid esile mitmed sageli esinevad probleemid, mida peetakse rikkumiseks. Enim mainiti ebaeetilist käitumist ja sobimatut kolleegidevahelist suhtlemist, mis seisnes ebaviisakuses, solvangutes, karjumises, solvavate naljade tegemises, klatšimises ja naeruvääristamises. Samuti esines psühholoogilise surve ja kiusamise juhtumeid, sealhulgas ebasoodsa töökeskkonna loomine, tahtlik eksitamine tööle asumisel ning eelarvamustest tingitud pingeline õhkkond. Tööõiguse ja sisekorra rikkumistega seoses toodi esile ebavõrdset kohtlemist, probleeme tööaja, puhkuse ja palgaga, dokumentatsiooni

rikkumist ning tööle ilmumist joobes olekus. Need tulemused kinnitavad, et ettevõttes X esineb ebaetilisi olukordi ja sisekorraeskirjade rikkumist, mis mõjutab töökeskkonda ja töötajate heaolu.

Tabel 6 annab põhjaliku ülevaate vastajate kogemusest rikkumistega ning nende tegelikust käitumisest. Võimalike rikkumistega oli kokku puutunud 22 vastajat, kellest ainult 10 vastajat oli rikkumisest ka teatanud. Juhtide seas oli kokkupuutumise osakaal kõrgem, kuid mitte keegi neist ei olnud arvatavast rikkumisest teatanud. Juhid eelistasid olukorda ise reguleerida, suheldes nende töötajatega, kes käitusid ebaetiliselt.

Tabel 6

Vastajate kogemus potentsiaalsete tööalaste rikkumiste ja vihjeandmisega

Rühm	Ko gua rv	Rikkumi se märkajad (N/%)	Teatas rikkumi sest (N/%)	Peamine mitteteatamise põhjus	Esimene hüpoteetiline tegevus arvatava rikkumise avastamisel
Koguvali m	44	22/50%	10/45%	Negatiivsete tagajärgede kartus (6); usk, et midagi ei muutu (6)	Juhi teavitamine (25)
Juht	5	3/60%	0/0%	Ise reguleeris olukorda (1); usk, et midagi ei muutu (1)	Arutelu kolleegide või lähedastega (3)
Töötaja	39	17/44%	8/47%	Negatiivsete tagajärgede kartus (6)	Juhi teavitamine (24)
Kuni 4 aastat tööstaaži	19	9/47%	4/44%	Negatiivsete tagajärgede kartus (3)	Juhi teavitamine (12)
5–14 aastat tööstaaži	9	5/56%	2/40%	Usk, et midagi ei muutu (2)	Juhi teavitamine (6)
Üle 15 aasta tööstaaži	14	6/43%	4/67%	Ise reguleeris olukorda (1); negatiivsete tagajärgede kartus (1); usk, et midagi ei muutu (1); ebakindlus, et tegemist on rikkumisega (1)	Juhi teavitamine (5)

Märkus: Teatamismäär on arvutatud rikkumisega kokkupuutunud hulgast põhjal.

Mitteteatamise põhjuseid sai valida mitu ning mõni vastaja ei täpsustanud oma valikut.

Sulgudes on märgitud vastajate arv. Kuna kolm vastajat jätsid rolli või tööstaaži märkimata, ei kajastu nad rühmade võrdluses.

Allikas: Autor koostanud küsitluse vastuste põhjal.

Kõikidest avatud vastustest selgus, et töötajad teatasid rikkumistest oma vahetutele juhtidele. Üks töötaja püüdis esialgu lahendada sisekorra rikkumisega seotud probleemi iseseisvalt, kuid lõpuks peale ebaõnnestumist pidi ta pöörduma oma juhi poole. Mõni teatatud probleem leidis lahenduse, kuna juht pidas maha vestluse, mis viis lahenduseni. Mõnel teisel juhul aga lahendust ei leitud, kuid saadi olukorra kohta selgitusi. Paraku ei võimaldanud need probleemi täielikult lahendada.

Peamised mitteteatamise põhjused olid negatiivsete tagajärgede kartus ja usk, et midagi ei muutu. Lühema tööstaaziga töötajate hulgas domineeris hirm negatiivsete tagajärgede ees, pikema tööstaaziga töötajad mainisid ka ebakindlust, kas tegemist on üldse rikkumisega. Saadud tulemuste põhjal olid hirm kättemaksu ees ja usalduse puudumine olulised takistused, miks vihjeandmisest loobuti.

Kui vastajad kujutaksid ette, et nad on arvatava rikkumise tunnistajaks, siis enamik teataks sellest esmalt oma vahetule juhile – see on kooskõlas ettevõttes X kehtivate sisekorraeeskirjadega. Samas märkis seitse vastajat, et eelistaks kasutada spetsiaalset vihjekanalit, kui see ettevõttes olemas oleks. Samuti eelistaks enamik juhtidest arutada olukorda kõigepealt kaastöötajate, sõprade või pereliikmetega.

Lisas E on esitatud tabel, mis sisaldab vastajate hinnanguid teatamisvajadusele ja eelistatud teatamisviisile. Enamiku arvatavate rikkumiste korral eelistaks enamik töötajaid ja juhte ettevõttesisest vihjeandmist, samas korruptsiooni puhul esines tugevam kalduvus eelistada ettevõttevälist vihjeandmist. Juhtide seas tuli esile tugev kalduvus eelistada ettevõttesisest vihjeandmist peaaegu kõigi olukordade puhul. Avatud vastustest selgus, et otsus võimalikust rikkumisest teatada sõltub suuresti selle raskusastmest: vähem tõsiste juhtumite korral kaalutakse sageli teatamisest loobumist, samas raskete rikkumiste, näiteks ebaseaduslike tegude või finantsmahhinatsioonide puhul peetakse teatamist vajalikuks. Mõned vastajad rõhutasid, et esmalt tuleks pöörduda juhtkonna poole, kuid kui olukord ei lahene või on eriti raske ja ohtlik, tuleks pöörduda pädevate organisatsiooniväliste asutuste poole.

Vihjeandmist takistavate tegurite olulisuse hinnangute analüüsimisel (vt tabel 7) selgus, et neid tegureid peetakse suhteliselt oluliseks. Samas on standardhälbed suhteliselt mõõdukad, millest tulenevalt on vastajate arvamused üsna ühtlased ning suuri erimeelsusi ei esine.

Tabel 7

Vihjeandmist pärssivate tegurite olulisus

Negatiivsed aspektid	Keskmine	Standardhälve	Mediaan	Tõlgendus
Kohtumenetlusega ähvardamine	4,5	0,84	5	Väga oluline
Vallandamine/koondamine	4,3	1,01	5	Väga oluline
„Musta nimekirja“ kandmine	4,2	0,99	5	Väga oluline
Sotsiaalne isolatsioon	4,1	0,92	4	Pigem oluline
Teavituse ignoreerimine	4,1	0,95	4	Pigem oluline
Tööülesannete muutmine	4	0,93	4	Pigem oluline
Kaastöötajate või juhtide negatiivne reageering	3,8	1,05	4	Pigem oluline

Märkus: Kasutatud on viiepallist skaalat, kus 1 on „üldse mitte oluline“, 2 on „pigem ebaoluline“, 3 on „nii ja naa“, 4 on „pigem oluline“ ning 5 on „väga oluline“. Tõlgendus tehtud mediaani alusel.

Allikas: Autor koostanud küsitluse vastuste ja Exceli funktsiooni Data Analysis kirjeldava statistika põhjal.

Kõige kõrgemalt hinnati kohtumenetlusega ähvardamist, mis näitab, et võimalikud õiguslikud tagajärjed on vastajate jaoks üks olulisemaid vihjeandmist takistavaid tegureid. Samuti hinnati kõrgelt vallandamise või koondamise ohtu ning „musta nimekirja“ sattumise riski, mis on otseselt seotud tööalaste negatiivsete tagajärgedega. Ülejäänud tegureid hinnati mõnevõrra madalamalt, kuid ka nende keskmised hinnangud viitavad pigem nende olulisele rollile vihjeandmise valmidusega seoses.

Vihjekanalite omaduste hindamise tulemustest (vt tabel 8) selgus, et kõige kõrgemalt hinnati konfidentsiaalsust ja kaitset negatiivsete tagajärgede eest – mõlema keskmised väärtused on võrdselt kõrged. Vastajate jaoks on kõige olulisem tagada turvaline ja riskivaba vihjeandmise keskkond. Samuti hinnati kõrgelt protsessi selgust ja vihjesaaja sõltumatust, mistõttu peetakse vihjekanalite kasutamisel oluliseks selle arusaadavust ja usaldusväärsust. Ülejäänud tegurid said küll veidi madalama hinnangu, kuid olid vastajate vaates siiski olulised. Standardhälbed on aga mõõdukad, viidates enam-vähem ühetaolisele arvamusele vihjekanalite omaduste olulisuse puhul.

Tabel 8

Vihjekanalil omaduste olulisus

Vihjekanalil omadused	Keskmine	Standardhälve	Mediaan	Tõlgendus
Konfidentsiaalsus	4,7	0,64	5	Väga oluline
Kaitse negatiivsete tagajärgede eest	4,7	0,60	5	Väga oluline
Selge protsess	4,5	0,73	5	Väga oluline
Vihjesaaja sõltumatus	4,4	0,75	5	Väga oluline
Anonüümsus	4,3	0,94	5	Väga oluline
Tagasisidestamine	4,3	0,84	4	Pigem oluline
Juhi vahenduseta teatamine	4,1	0,96	4	Pigem oluline
Selged tagasisidestamise tähtajad	3,9	0,82	4	Pigem oluline

Märkus: Kasutatud on viiepallist skaalat, kus 1 on „üldse mitte oluline“, 2 on „pigem ebaoluline“, 3 on „nii ja naa“, 4 on „pigem oluline“ ning 5 on „väga oluline“. Tõlgendus tehtud mediaani alusel.

Allikas: Autor koostanud küsitluse vastuste ja Exceli funktsiooni Data Analysis kirjeldava statistika põhjal.

Korrelatsioonimaatriks (vt lisa F) kinnitab tugevat seost anonüümsuse ja konfidentsiaalsuse vahel ning tagasisidestamise ja selgete tähtaegade vahel. Need tugevad korrelatsioonid on ootuspärased, kuna nimetatud tegurid on oma olemuselt väga sarnased: anonüümsus ja konfidentsiaalsus puudutavad vihjeandja identiteedi kaitset ning turvatunnet, tagasisidestamine ja selged tähtajad on aga tihedalt seotud protsessi läbipaistvuse ja selgusega. Töötajate jaoks on vihjeandmise otsuse tegemisel olulised selgus ja turvatunne.

Enamik vastajaid suhtub vihjekanalil loomise ideesse positiivselt: vihjekanalil vajalikkuse keskmine hinnang on 3,9, mis näitab, et seda peetakse pigem vajalikuks. Kasutamise tõenäosus sai keskmiseks hindeks 2,6 ja mediaanhindeks 3, mis näitab, et vastajad kalduvad pigem vihjekanalil kasutamise suunas.

Eelistatud teatamisviiside analüüs (vt tabel 9) tõi esile, et kõige sobivamaks peetakse konfidentsiaalset veebivormi. Samas on standardhälbed mõne teguri puhul üsna suured, mis näitab, et vastajate arvamused nende tegurite suhtes on mõnevõrra erinevad.

Kuigi veebivorm on enamiku jaoks kõige eelistatum teatamisviis, tundusid mõne vastaja jaoks teised kanalid sobivamad. Spetsiaalne sõnumikast oli eelistuselt teisel kohal. Isiklik kohtumine vastutava isikuga ning e-posti ja telefoni kasutamine said madalamaid hinnanguid, millest võib järeldada, et need viisid on vähem sobilikud ega paku vastajatele piisavat turvatunnet.

Läbiviidud t-testi tulemuste põhjal (olulisuse nivoo 0,05) saab järeldada, et kõik eelistatud teatamisviiside paarid erinevad statistiliselt olulisel määral, välja arvatud kaks viisi – isiklik kohtumine ja e-post. Need ei ole statistiliselt erinevad, ka nende keskmine hinnang on üsna sarnane. See tähendab, et nende kahe kanali kohta antud hinnangute erinevus ei ole piisavalt suur ja need saab paigutada eelistuste järjestuses ühele tasemele. Kõikide ülejäänud vihjekanalite osas on vastajatel selged eelistused, eriti paistab see silma veebivormi ja sõnumikasti puhul, mis said kõrgeimad hinnangud.

Tabel 9

Vastajate arvamus vihjekanalide vajadusest ja kasutamise tõenäosusest ning vihjekanalide vormi sobivusest

Eelistatud teatamisviisid	Keskmine	Standardhälve	Mediaan	Tõlgendus
Konfidentsiaalne veebivorm	4,3	1,15	5	Väga sobiv
Spetsiaalne sõnumikast	3,6	1,28	4	Pigem sobib
Isiklik kohtumine vastutava isikuga	3	1,24	3	Nii ja naa
E-post	2,9	1,33	3	Nii ja naa
Telefon	2,6	1,28	3	Nii ja naa

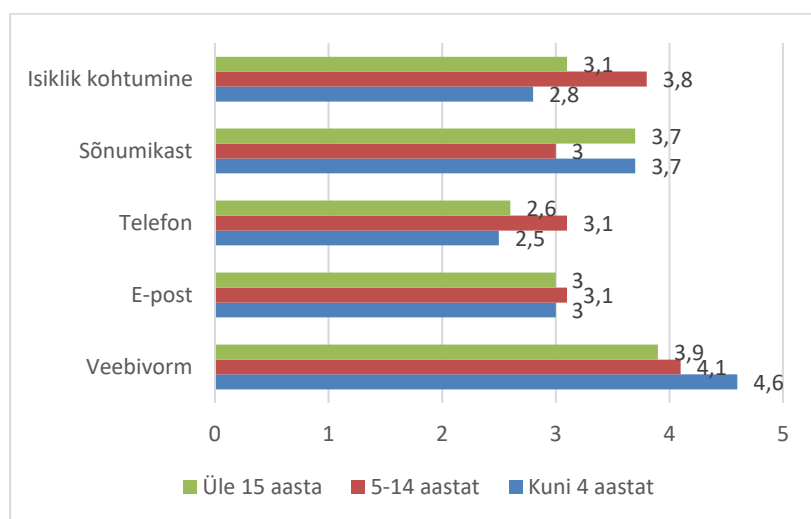
Märkus: Kasutatud on viiepallist skaalat, kus 1 on „üldse ei sobi“, 2 on „pigem sobimatu“, 3 on „nii ja naa“, 4 on „pigem sobib“ ning 5 on „väga sobiv“. Tõlgendus tehtud mediaani alusel.

Allikas: Autor koostanud küsitluse vastuste ning Exceli funktsiooni Data Analysis kirjeldava statistika ja kahe valimi paaristatud t-testi põhjal.

Joonisel 3 on näha mõningad erinevused vastajate eelistustes olenevalt nende tööstaažist. Kõik vastajate rühmad pidasid üksmeelselt veebivormi parimaks vihjeandmise viisiks, kusjuures kuni 4-aastase tööstaažiga vastajad andsid sellele vihjekanalile vormile kõrgeima hinnangu. Enamiku teiste vihjekanalite puhul olid arvamused aga segasemad. Näiteks hindasid keskmise tööstaažiga (5–14 aastat) töötajad võrreldes teiste rühmadega kõrgemalt isiklikku kohtumist vastutava isikuga, samas uuemad töötajad suhtusid isiklikesse kohtumistesse tagasihoidlikumalt, andes neile neutraalsest allapoole jääva hinnangu.

Spetsiaalset sõnumikasti hindasid kõrgelt nii uued kui ka pikaajalise tööstaažiga töötajad, seevastu keskmise tööstaažiga vastajad jäid selle teatamisviisi suhtes neutraalseks. T-test (olulisuse nivoo 0,05) ei näidanud, et erineva tööstaažiga rühmade vahel esineks statistiliselt olulisi erinevusi. Üldiselt peavad kõik tööstaaži rühmad e-posti neutraalseks

vihjeandmise vormiks, samas telefon osutus kõige vähem atraktiivseks viisiks nii kogenud töötajate, kellel on üle 15-aastane tööstaaž, kui ka uute töötajate hulgas.



Joonis 3. Tööstaaži rühmade keskmised hinnangud teatamisviiside sobivusele

Märkus: Kasutatud on viiepallist skaalat, kus 1 on „üldse ei sobi“, 3 on „nii ja naa“ ja 5 on „väga sobiv“. Joonisel kajastatud arvud tähistavad iga rühma keskmist hinnangut.

Allikas: Autor koostanud küsitluse vastuste põhjal ja Exceli abil.

Peaaegu mitte keegi vastajatest ei esitanud lisamõtteid ega alternatiivseid ideid vihjekanalite kujundamiseks. Üks vastaja mainis, et võiks luua ka anonüümse vihjekanalit, kuid ainsaks konkreetseks ettepanekuks oli avatud vastus, milles sooviti sellise vestluserakenduse loomist, mille kaudu saaks anonüümselt suhelda vastutava isikuga. Vastaja hinnangul oleks selline kiire ja mugav vestluskanal tõhus vahend arvatavatest rikkumistest teatamiseks ettevõtte sees.

Arvamused vihjekanalite korralduse kohta jagunesid peaaegu pooleks: 19 vastajat eelistas ainult ettevõttesisest kanalit ja 19 mõlema variandi kasutamist. Mõned vähesed toetasid ainult kontserni tasandil toimivat kanalit. Sisemise vihjekanalit pooldajad rõhutasid kiirust, lokaalsust ja ettevõtte maine säilitamist. Näiteks üks vastajatest mainis: „*Päring ettevõtte sees toimiva kanali kaudu aitab probleemi kiiremini, lokaalsemalt ja ettevõtte mainet vähem kahjustades lahendada.*“ Teine vastaja lisas: „*Kui töötaja kardab probleemi grupi tasandile eskaleerida, siis võib ta end mugavamalt tunda, kui saab [probleemist] ettevõttesiselt teavitada.*“ Probleemi ettevõttesisest lahendamist põhjendati sellega, et probleemid peaksid jääma ettevõtte X sisse. See rõhutab olukorra üle kontrolli omamise olulisust.

Kontserni tasandil toimiva kanali pooldajad hindasid kõrgelt sellega kaasnevat suuremat sõltumatust, distantsti ja läbipaistvust, mis vähendab hirmu, et vihjet võiksid menetleda tuttavad inimesed, kes suudavad vihjeandja identiteedi lihtsasti vihjega kokku panna. Näiteks üks vastaja ütles: „*Mõned töötajad võivad tunda end anonüümsena, kui nad teatavad rikkumisest grupiülese kanali kaudu, kuna sellega tegelevad kaugemalt võõrad töötajad, kes on sõltumatud.*“ Samuti rõhutati, et kontserni tasand aitab probleemide varjamise ohtu vähendada ja sel tasandil on rohkem võimalusi sellist kanalit paremini seadistada.

Mõlema variandi pooldajad märkisid, et erinevates olukordades sobivad erinevad lähenemised ja et sel viisil on kõigile tagatud mugavus. Näiteks üks vastajatest mainis: „*Mõlema kanali kasutamine annab töötajatele võimaluse valida kõige mugavam ja turvalisem viis rikkumistest teatamiseks ning suurendab protsessi läbipaistvust.*“

Üldiselt kinnitavad küsitluse tulemused seda, et ettevõttes X on vajadus turvalise ja mugava vihjekanaliga järele olemas. Töötajad on valmis sellist kanalit kasutama, eriti kui see tagab nende konfidentsiaalsuse ja kaitse negatiivsete tagajärgede eest ning hõlmab selget protsessi. Praegune praktika pöörduda võimalikust rikkumisest teatamiseks vahetu juhi poole ei kata kõiki olukordi piisavalt turvaliselt, mistõttu vihjekanaliga loomine on oluline nii seadusliku kohustuse täitmiseks kui ka parema töökeskkonna kujundamiseks ja rikkumiste varajaseks avastamiseks.

2.3. Järeldused ja praktilised soovitused ettevõtte X

Uuringu tulemused näitavad, et teenindusettevõttes X põhineb rikkumistest teatamine peamiselt vahetul suhtlusel juhtidega. See tuleneb olemasolevast töökorraldusest ja juhi kättesaadavusest. Juhtide poole pöördumist peamise probleemide lahendamise viisina on kinnitanud ka Saaremägi (2021) ja Putri (2018). Kuigi see on kiire ja lihtne lähenemisviis, ei taga see töötajatele piisavat turvatunnet ega sõltumatust. Seetõttu ei ole praegune vihjeandmise praktika piisavalt motiveeriv ega seaduse nõuetega kooskõlas, mistõttu on vaja luua eraldi vihjekanal. Allpool hinnatakse uuringu tulemuste haakumist varasemate teoreetiliste seisukohtadega (vt ka lisa G) ning sellest tulenevalt antakse ettevõtte X soovitusi.

Seadus võimaldab organisatsioonidel vihjeandmissüsteemi kaudu käsitletavate rikkumiste loetelu vastavalt vajadusele laiendada (Terracol, 2023; Terracol, 2022). Käesoleva töö raames läbi viidud uuring kinnitab sellist vajadust, kuna töötajad tõid lisaks seaduses sätestatule esile ka ebaeetilise käitumise ja sisekorraeskirjade rikkumise. Seetõttu peaks vihjeandmissüsteem katma ka töökorralduslikke ja eetilisi probleeme. Vihjete kogumine

võimalikult paljude teemade kohta aitab kaasa rikkumiste varajasele ja õigeaegsele avastamisele, juhul kui töötajad on teadlikud teatamise vajadusest ja ettevõttes eksisteerib vihjeandmissüsteem.

Varajane rikkumiste avastamine aitab vähendada organisatsioonile kaasnevaid negatiivseid tagajärgi, mis võivad väljenduda näiteks organisatsiooni suhtes tuntava usalduse kahjustumises (Bishop-Monroe et al., 2021; Terracol, 2022; Korruptsioonivaba Eesti, n.d.; Saaremägi, 2021). Sama arusaam ilmnes ka ettevõtte X töötajate seas, kes peavad probleemide kiiret organisatsioonisisest lahendamist oluliseks mainekahju vältimist soodustavaks asjaoluks.

Samas peab vihjesaaja olema sõltumatu nii rikkujatest kui ka vihjeandjatest, et vältida huvide konflikti (Terracol, 2024) ja suurendada usaldust. Kuigi vihjekanalite tegurite olulisuse küsimusele vastates märkisid paljud teenindusettevõtte X töötajad esmaseks valikuks juhi teavitamise, pidasid nad tähtsaks ka sõltumatust, mis kinnitab vajadust eraldiseisva vihjekanalite järele. Samuti on tähtis tagasisidestamine, mille regulaarsus ja õigeaegsus aitab luua usaldust vihjeandmise süsteemi vastu (Terracol, 2022; Jatsa, 2019). Kui inimene ei tea, mis tema vihjega ette võetakse ja kas seda üldse menetletakse, võib ta edaspidi olla vähem valmis vihjet andma. Kuigi teenindusettevõtte X töötajad peavad tagasisidestamist oluliseks, ei ole täpsed tähtajad nende jaoks kriitilised. Sellest saab järeldada, et teenindusettevõtte X puhul on töötajatele olulisem saada üldist infot selle kohta, et vihjega tegeletakse ja milline on menetluse käik, kui range ajakava, mida kohustab seadus.

Samuti selgus uuringust, et töötajad sageli rikkumistest ei teavita, mis viitab vajadusele usaldusväärse ja sõltumatu vihjekanalite järele. Peamised mitteteatamise põhjused olid negatiivsete tagajärgede kartus ja usk, et midagi ei muutu. Samuti peeti üsna oluliseks teguriks hirmu, et suhted kaastöötajatega võivad halveneda. Need hirmud on kinnitust leidnud ka varasemas teaduskirjanduses. Takistavad hirmud väljenduvad selles, et eksisteerib kättemaksu või vihjeandja mitteuskumise risk (Jatsa; 2019, Saaremägi, 2021; Palojärvi, 2021). Lisaks võib esineda eksiarvamus, et kaastöötajad suhtuvad vihjeandmisega negatiivselt – selle mõju leevendamiseks tuleb kujundada töötajaskonnas positiivset suhtumist, mis võib kaasa aidata üldise tööõhkkonna paranemisele (Djawadi, Plaß & Loer, 2025; Dungan, Waytz & Young, 2015; Daroglou et al., 2025).

Erinevalt Hakim Z., Safira ja Mahmudah' (2019), Dungan, Waytzi ja Youngi (2015) ning Puhi ja Tökke (2024) uuringutest, ei leitud käesolevas uuringus seost ametikoha või tööstaži ja vihjeandmise tõenäosuse vahel. Pigem ilmnes, et juhid püüavad probleeme ise lahendada, mis tuleneb praegusest töökorraldusest, tekkivate probleemide sisust ja

organisatsiooni suurusest. Üks põhjus on see, et ilmselt on juhtide avastatavad probleemid sellised, millele nad ise oskavad lahenduse leida. Teine põhjus on see, et ettevõtte X pole personaliosakonda, vaid on ainult direktor, kelle poole pöördatakse arvatavasti üksnes väga tõsiste probleemide tekkimise korral. Ka tööstaaži erinevus ei mõjutanud oluliselt teatamissagedust.

Arvestades nii teoreetilist käsitlust, uuringu tulemusi kui ka teenindusettevõtte X suurust ja selle valdkonna eripärasid, mis ilmnevad tegevuse hooajalisuses ja tööjõu suures voolavuses, on ettevõtte X puhul soovitatav luua lihtne, kulutõhus ja töötajatele turvatunnet pakkuv vihjekanal. Esiteks peab juhtkond üldse otsustama vihjekanaliloomise kasuks. Seejärel tuleb määrata vastutav isik: ettevõtte praeguses olukorras sobib selleks kõige paremini direktor, kes ei ole töötajate suhtes vahetu juht, välja arvatud keskastme juhtide puhul. Samal ajal tuleks laiendada rikkumiste loetelu, lisades seaduses nimetatule ka muid ebaseaduslikke, ebaeetilisi ja sisekorraeskirjade rikkumisega seotud juhtumeid.

Käesoleva magistritöö raames loodi vihjekanalil demoversioon, mille ettevõtte X saab soovil korral oma vihjekanaliloomisel aluseks võtta või mida edasi arendada. Demoversiooni loomisel kasutati tarkvara GlobaLeaks, sest see sobib kõige paremini ettevõtte X suuruse, vajaduste ja ressursidega. Valik tuleneb nii teoreetilisest käsitlusest, empiirilise uuringu tulemustest, tasuvabast ligipääsust kui ka Euroopa Komisjoni soovitusel, mis suurendab selle platvormi usaldusväärsust.

GlobaLeaks on kasutatav eesti ja vene keeles (GlobaLeaks, n.d.; European Commission, n.d.), mis on kakskeelse ettevõtte X jaoks tähtis. Lisaks pakub platvorm tehnilist anonüümsust ja konfidentsiaalsust ning võimalust vihjeandjal ja vihjesaajal suhelda ilma vihjeandja identiteeti avaldamata (GlobaLeaks, n.d.; European Commission, n.d.). See on võimalik tänu sellele, et veebivormi täitmise lõpetamisel tekitab süsteem unikaalse koodi, mille kaudu saab vihjeandja ligi vihjele ja sellega seotud teabele (GlobaLeaks, n.d.).

Otsus kasutada vihjekanalina veebivormi tulenes nii käesoleva töö teoreetilisest käsitlusest kui ka uuringu tulemustest, mille kohaselt on see kõige eelistatum vihjekanaliloomise vorm, edestades oluliselt teisi vorme. Samuti selgus olukordade teatamisvajaduse hindamisest, et töötajad peavad vihjeandmist vajavaks ka mittenõustumist juhi otsusega ja töötajate omavahelisi konflikte, mis võivad eristuda raskusastme poolest. See viitab vajadusele lisada veebivormis rikkumise kategooriate valiku jaotisse täpsed selgitused.

GlobaLeaksi platvormil demoversioon pakub ka lihtsustatud veebivormi malli, mis koosneb kaheksast avatud küsimusest ühel lehel, ilma et need oleks teemade kaupa jaotatud. Mallis küsitakse üldist teavet: lühike ja üksikasjalik kirjeldus juhtumist, juhtumi toimumise

koht ja aeg, kaebuse esitaja seotus juhtumiga, tõendite kättesaadavus, teave teiste organisatsioonide või üksikisikute teavitamise kohta ning oodatud tulemus. Kõik väljad on mõeldud vabateksti sisestamiseks, ajendades vihjeandjat teavet struktureerima ilma viipadeta. (GlobaLeaks, n.d.)

Teenindusettevõtte X vihjekanalil demoversioon töötati välja uuringu tulemuste ja teoreetiliste põhimõtete alusel. Vihjekanalil plokide koostamisel võeti arvesse Jatsa (2019) soovitusi ja eeskujuna kasutati Hiltoni vihjekanalit. Loodud vihjekanal koosnes viiest teemaplokist: rikkumise liik, toimumise koht ja aeg, seotud isikud, juhtumi kirjeldus ning teataja kontaktandmed. Valminud kanali demoversioon edastati hindamiseks teenindusettevõttele X, et saada lahenduse sobivuse kohta tagasisidet.

Ettevõttelt saadud tagasiside põhjal viidi demoversiooni sisse mitmeid muudatusi. Esiteks täpsustati rikkumiste loetelu ning küsimuste sõnastust, vältides keerulist terminoloogiat, et potentsiaalsetel vihjeandjatel oleks lihtsam veebivormi täita. Teiseks, kuna ettevõtte sisekultuur on suunatud vahetule suhtlusele, muudeti vihjekanalil keelekasutus isiklikumaks, asendades ametlik teietamine sinatamisega.

Loodud vihjekanalil demoversioon on kohandatud vastavaks teenindusettevõtte X olukorrale, sealsete töötajate eelistustele ja teoreetilistele soovistele. Vihjekanalil veebivorm on jagatud viieks eelmainitud etapiks: rikkumise liik, toimumise koht ja aeg, rikkumisega seotud pooled ja selle kirjeldus ning teataja kontaktandmed. Selline jaotus muudab veebivormi täitmise vihjeandja jaoks arusaadavamaks. Kasutatakse ka suletud küsimusi eelnevalt kindlaks määratud vastusevariantidega, mis selgitavad olulisi üksikasju, mis jäid GlobaLeaksi mallis küsimata. Näiteks küsitakse, kas rikkumine jätkub ja kuidas teave saadi. See aitab koguda vajalikku teavet, mida vihjeandja muidu mallikujulise veebivormi abil ei pruugiks esitada.

Rikkumise kategooria valimisel (vt joonis 4) pakub loodud vihjekanal nii vihjeandjate kaitse seaduses nimetatud kohustuslikke kategooriaid, näiteks keskkonda kahjustav tegevus ja andmekaitse rikkumine, kui ka uuringu käigus mainitud rikkumisi, näiteks ebaeetiline või sobimatu käitumine ja sisekorra rikkumine. Lisaks on täiendatud loetelu majutus- ja toitlustusvaldkonnale omaste rikkumistega. Kategooriad on koostud nii, et need kataksid võimalusel ka nii-öelda hallid alad Circle K näitel (Jatsa, 2019). Ühtlasi lisati kategooria „Muu“ juhaks, kui potentsiaalne vihjeandja peaks puutuma kokku ebamäärase olukorraga, mida tal on raske olemasolevate kategooriate alla liigitada.

Iga kategooria kohal hiirega liikudes kuvatakse lühike selgitus, mis põhineb Hiltoni hotelliketi eeskujul (Navex, n.d.). See vähendab potentsiaalsete vihjeandjate ebakindlust ja

aitab neil lihtsamini otsustada, kas murettekitav olukord kuulub vihjekanal kaudu käsitlemisele. Antud funktsiooni loomine on oluline, kuna küsitlusest selgus, et mitmed töötajad ei ole alati olnud kindlad, kas nende poolt märgatud olukord kvalifitseerub rikkumiseks või mitte.

1 Rikkumise Liik 2 Toimumise Koht Ja Aeg 3 Seotud Isikud

4 Juhtumi Kirjeldus 5 Kontaktandmed (Vabatahtlik)

Millist liiki rikkumist kirjeldate?

- ☐ Olukorrad, kus kedagi koheldakse ebaõiglaselt, esineb ahistamist või kiusamist
- ☒ Diskrimineerimine või ebaõiglane kohtlemine
- ☐ Finantsrikkumine
- ☐ Andmekaitse rikkumine
- ☐ Vara väärkasutamine
- ☐ Keskkonda kahjustav tegevus
- ☐ Seaduse või sisekorra rikkumine
- ☐ Muu

Joonis 4. Rikkumise kategooria valimise samm

Allikas: Autor koostanud GlobaLeaksi tarkvara abil.

Samuti sisaldab veebivorm võimaliku rikkumise aja ja asukoha märkimiseks ettenähtud välja (vt joonis 5) ning asjaosaliste kirjeldamise välja (vt joonis 6). See on kooskõlas Jatsa (2019) soovitusel koguda juba vihjeandmise etapis piisavalt teavet, et minimeerida vajadust anonüümse vihjeandja korduvate täpsustuste järele. See on oluline, kuna esineb oht, et vihjeandja ei pruugi hiljem oma vihje staatust jälgida ega täiendavatele küsimustele vastata.

1 Rikkumise Liik **2 Toimumise Koht Ja Aeg** 3 Seotud Isikud

4 Juhtumi Kirjeldus 5 Kontaktandmed (Vabatahtlik)

Kus see juhtus? *

Millal see juhtus? *

Kas rikkumine kestab endiselt? *

- ☐ Jah
- ☐ Ei
- ☐ Pole kindel

Joonis 5. Arvatava rikkumise toimumiskoha ja -aja kirjeldamise samm

Allikas: Autor koostanud GlobaLeaksi tarkvara abil.

Veebivormis on kasutatud veel nutikat lahendust (vt joonis 6), mille korral küsimus „Kas oled sellest juba kellelegi rääkinud?“ avab täpsustava küsimuse vaid siis, kui vastaja valib „Jah“. Kui vastus on „Ei“, siis lisaküsimust ei kuvata. Nii ei koormata veebivormi täitjat üleliigse küsimusega, mis tema olukorraga ei sobi.

1 Rikkumise Liik 2 Toimumise Koht Ja Aeg 3 Seotud Isikud 4 Juhtumi Kirjeldus 5 Kontaktandmed (Vabatahtlik)

Kes pani rikkumise toime? (ees- ja perekonnanimi, ametinimetus ning osakond) *

Kas oled sellest juba kellelegi rääkinud? *

☒ Jah
☐ Ei

Kui jah, siis palun kirjuta, kellele ja millal Sa sellest teavitasid? Mis pärast seda juhtus? *

Joonis 6. Arvatava rikkumisega seotud osapoolte kirjeldamise samm

Allikas: Autor koostanud GlobaLeaksi tarkvara abil.

Järgmine funktsioon on failide lisamine (vt joonis 7), mis võimaldab vihjeandjal edastada arvatava rikkumise kohta tõendeid, näiteks fotosid või dokumente. Samal lehel palutakse vihjeandjal olukorda ka detailsemalt kirjeldada ning märkida, kuidas ta juhtunust teada sai.

4 Juhtumi Kirjeldus 5 Kontaktandmed (Vabatahtlik)

Kirjelda palun, mis täpsemalt juhtus. *

Kuidas Sa sellest teada said? *

☐ Olin seda isikult pealt näinud
☐ See juhtus minuga
☐ Sain teada kelleltki teiselt
☐ Avastasin selle dokumentidest või töövoogudest
☐ Muu

Kui Sul on dokumente või muid tõendeid, laadi need siia.

Valige fail või lohistage see siia.

Joonis 7. Arvatava rikkumise kirjeldamise samm

Allikas: Autor koostanud GlobaLeaksi tarkvara abil.

Viimane samm (vt joonis 8) võimaldab vihjeandjal valida, kas esitada oma kontaktandmed konfidentsiaalseks suhtluseks või jääda täiesti anonüümseks. Pärast vihje edastamist genereerib süsteem igale vihjeandjale unikaalse jälgimiskoodi (GlobaLeaks, n.d.). See võimaldab vihjeandjal jälgida menetluse staatust ja saada tagasisidet, ilma et peaks oma identiteeti paljastama. Siinkohal on oluline rõhutada seadusest tulenevat nõuet anda vihjeandjale tagasisidet hiljemalt 7 päeva jooksul alates vihje kättesaamisest (TÕRTKS, 2024). Unikaalse koodi genereerimine tagab selle nõude täitmise ka anonüümsete vihjete puhul.

The screenshot shows a web interface with two tabs: '4 Juhtumi Kirjeldus' and '5 Kontaktandmed (Vabatahtlik)'. The '5' tab is active. Below the tabs, there is a paragraph of text explaining the choice between confidential and anonymous reporting. Below the text, there are three input fields: 'Sinu ees- ja perekonnanimi:', 'Sinu telefoninumber:', and 'Sinu e-posti aadress:'. Each input field has a light blue border and a small blue icon on the left.

4 Juhtumi Kirjeldus 5 Kontaktandmed (Vabatahtlik)

Võid jääda täielikult anonüümseks. Sellisel juhul toimub suhtlus siinsamas keskkonnas. Pärast vihje esitamist loob süsteem Sulle unikaalse koodi. Palun kirjuta see üles, et saaksid hiljem oma vihje staatust kontrollida ja vajadusel meie küsimustele vastata.

Kui aga soovid, et saaksime Sinuga otse ühendust võtta, jätta siia oma andmed:

Sinu ees- ja perekonnanimi:

Sinu telefoninumber:

Sinu e-posti aadress:

Joonis 8. Anonüümse või konfidentsiaalse teatamisviisi vahel valimise samm

Allikas: Autor koostanud GlobaLeaksi tarkvara abil.

Pärast tehnilise lahenduse seadistamist on teenindusettevõttel X soovitatav koostada selged juhised, mis võib lisada ka sisekorraeeskirjadesse. Lähtuvalt nii Jatsa (2019) kui ka Terracoli (2022) soovitustest peaksid need selgitama järgmist: kellel on õigus võimalikust rikkumisest teatada; milliste olukordade kohta tuleb vihje anda; kuidas vihjet esitada; millist tagasisidet saadakse ja millal seda antakse; kuidas tagatakse konfidentsiaalsus ja kaitse. Juhistes tuleks samuti eraldi rõhutada, et vihjekanal ei ole mõeldud isiklike kaebuste lahendamiseks. Täiendavalt tuleb kirjeldada, kes vihjeid kogub ja menetleb, kuidas andmeid hoiustatakse, kellel on ligipääs nendele andmetele ning mis põhimõtetel kogutud andmeid kustutatakse.

Kasulik on lisada juhistesse lihtsad näited arvatavate rikkumistega seotud olukordadest, nagu on tehtud Hiltoni (n.d.a) käitumisjuhendis, et aidata töötajatel otsustada, kas tegemist on vihjeandmist vajava olukorraga või pigem mitte. Lisaks võib esitada otsust tegema suunavaid küsimusi, mis samuti aitavad aru saada, kas tegemist on tõesti rikkumisega. Needki on välja toodud Hiltoni (n.d.a) käitumisjuhendis ja on heaks eeskujuks.

Järgmise sammuna tuleb teenindusettevõttel X vihjekanal töötajatele nähtavaks teha. Selleks sobivad QR-koodiga infovoldikud puhkeruumides ning ettevõtte siseveebi paigutatud lingid, mis suunavad vihjekanalit tutvustavale lehele ja vihjekanal juurde (Smirnova, 2024; Terracol, 2022; Jatsa, 2019). Samuti on soovitatav korraldada regulaarseid koolitusi (Terracol, 2022; Jatsa, 2019). Need vähendavad hirmu ning suurendavad teadlikkust vihjeandmise olemusest, selle olulisusest, vajalikkusest ja kasutamisevõimalustest.

Lõpetuseks tuleb pärast vihjeandmissüsteemi käivitamist seda regulaarselt jälgida (Jatsa, 2019; Terracol, 2022). Vähemalt kord aastas tuleb vaadata, kuidas vihjekanal toimib, koguda töötajatelt tagasisidet ja vajaduse korral süsteemi täiendada, lisades näiteks uusi kategooriaid või lihtsustades veebivormi ülesehitust.

Nende soovitude järgimine võimaldab teenindusettevõttel X luua vihjekanal, mis vastaks seaduse nõuetele, arvestaks töötajate tegelikke vajadusi ja oleks piisavalt lihtne, et selle saaks edukalt kasutusele võtta. Ettevõttesisesse vihjeandmissüsteemi loomine aitab vähendada rikkumiste avastamata jätmise riski, parandada töökeskkonda ja täita seadusest tulenevat kohustust. Töötajate regulaarne teavitamine ja koolitamine ning protsessi pidev täiustamine tagavad, et vihjekanal ei jää üksnes formaalsuseks, vaid muutub tõeliseks tööriistaks ettevõtte eetilise keskkonna loomisel, töötajate turvalisuse kaitsmisel ja teenuse hea kvaliteedi hoidmisel.

Kokkuvõte

Organisatsioonides võib aeg-ajalt esineda tegevusi, millega rikutakse seadusi, eetikanorme või ettevõtte sisekorraeskirju. Need tegevused võivad olla seotud näiteks diskrimineerimise, ahistamise, ressursside väärkasutamise ja ohutusnõuete eiramisega, aga ka muude probleemidega. Kõik need probleemid võivad kahjustada nii töötajate kui ka ettevõtte mainet ja finantsseisu.

Töötajad on sageli võtmeisikud potentsiaalsete rikkumiste ja muude probleemide märkamisel, kuid mitte alati ei julge või ei soovi nad neist teada anda. Kui siiski julgetakse teatada, on tegemist vihjeandmisega. Vihjeandmise käigus annab organisatsiooniga seotud isik teada väärkäitumisest, et ennetada või leevendada kahjusid.

Käesolevas magistritöös uuriti vihjeandmise teoreetilisi aluseid ja õiguslikku raamistikku ning vihjeandmissüsteemi loomise võimalusi ja rakendamist teenindusettevõttes X, mis tegutseb majutus- ja toidlustusvaldkonnas. Teoreetilises osas selgitati vihjeandmise olemust varasemate teadustööde põhjal. Eri autorid defineerivad vihjeandmist kui teavitamist organisatsioonisisestest ebaeetilistest, ebaseaduslikest või kahjulikest tegevustest, mille eesmärk on ennetada kahjusid või leevendada nende mõju.

Euroopa Liidu vihjeandjate kaitse direktiivi miinimumnõuded ja Eesti vihjeandja kaitse seadus sätestavad, et ettevõtted, kus töötab vähemalt 51 inimest, peavad looma sisemise vihjekanalit. Need õigusaktid rõhutavad, et vihjekanal peab tagama vihjeandja konfidentsiaalsuse ja et vihjeandja peab olema kaitstud kättemaksu eest. Samuti on õigusaktides sätestatud kohustus, mille järgi peab vihjekanalit menetlemise eest vastutav isik andma kõikides vihjeandmise etappides vihjeandjale tagasisidet.

Hästi toimiv vihjeandmissüsteem peab võimaldama nii anonüümset kui ka konfidentsiaalset vihjeandmist, pakkuma võimaluse korral mitut erisugust vihjekanalit vormi ning tagama vihjekanalit eest vastutava isiku sõltumatuse. Tõhus süsteem peab põhinema selgel protsessil alates vihje vastuvõtmisest, hindamisest ja uurimisest ning lõpetades rikkumise lahendamisega. Lisaks on oluline anda vihjeandjale regulaarset tagasisidet, nagu rõhutab ka seadus. Tagasiside tähtsus tuleneb soovist tagada süsteemi sujuv toimimine ja vältida välist vihjeandmist. Tagasisidestamise käigus kinnitatakse vihje kättesaamist ja hiljem tutvustatakse uurimise tulemusi.

Sisemise vihjeandmissüsteemi loomine aitab organisatsioonil rikkumisi varakult avastada ja vähendada oluliselt riski, et tõsised probleemid jäävad märkamata. See tugevdab organisatsiooni läbipaistvust, suurendab usaldust ja edendab eetilist kultuuri. Samas takistavad vihjeandmist mitmesugused tegurid, millest üks olulisimaid on hirm kättemaksu ees. Survemeetmed võivad väljenduda vallandamises ja suhete halvenemises, aga ka muudes negatiivsetes tagajärgedes. Paljud töötajad ei anna vihjet seetõttu, et nad ei usu, et vihjega midagi ette võetakse, või kardavad, et võimalikku rikkumist püütakse varjata või ignoreeritakse.

Vihjeandmist soodustavatest teguritest üks olulisimaid on vihjeandja turvatunne. Turvatunnet aitavad luua ja tugevdada kaitse kättemaksu eest, võimalus teatada arvatavast rikkumisest anonüümselt või konfidentsiaalselt, sõltumatu vastutava isiku olemasolu ning regulaarne tagasiside menetluse käigu kohta. Olulist rolli mängib ka töötajate teadlikkus, mis tuleneb ettevõtte loodavatest stiimulitest. Kui ettevõttes on vihjeandmise kohta kehtestatud selged juhised, korraldatakse teemakohaseid koolitusi ja suhtlus on avatud, kasvab valmidus arvatavatest rikkumistest teatada.

Magistritöö empiirilises osas viidi läbi anonüümne küsitlus teenindusettevõtte X töötajate ja juhtide seas, mille valimis oli 44 inimest. Tulemused kinnitasid paljuski teoreetilisi seisukohti. Pooled vastajad olid töökohal kokku puutunud olukorraga, mida nad pidasid rikkumiseks. Enim mainiti ebaetilist käitumist ja sisekorraeskirjade rikkumist. Osa rikkumise märkajatest teatas sellest otse juhile, nagu on ette nähtud ettevõtte X

sisekorraeeskirjades. Peamised mitteteatamise põhjused olid hirm negatiivsete tagajärgede ees ja usk, et muudatusi ei tule. Töötajad hindasid kõrgelt konfidentsiaalsust, kaitset ja protsessi selgust ning eelistasid vihjekanalina veebivormi.

Uuringu tulemuste ja teema teoreetilise käsitluse põhjal töötati GlobaLeaksi tarkvara abil välja vihjekanalide demoversioon. See lahendus hõlmab üsna laia valikut rikkumiste kategooriaid, mida vihjekanalide kaudu menetletakse, sisaldab iga kategooria kohta lühiselgitusi, et rikkumise kategooria valimist lihtsustada, ning võimaldab tõendite esitamiseks faile üles laadida.

Magistritöö eesmärgi saavutamiseks anti teenindusettevõttele X vihjeandmissüsteemi loomiseks soovitusi. Esiteks tuleb tal luua sisemine vihjekanal, mis vastab seaduse nõuetele ja vihjeandmist käsitleva teaduskirjanduse soovitudele. Teiseks on ettevõttel vaja koostada selged juhised, mis kirjeldaksid vihjeandmise protsessi ja suunaksid sellega seotud tegevust. Kolmandaks tuleb töötajaid vihjekanalide olemasolust aktiivselt teavitada, kasutades selleks infovoldikuid, QR-koode, siseveebi bannereid ja regulaarseid koolitusi. Neljandaks on soovitatav määrata vihjesaajaks teenindusettevõtte X direktor, kes töötajaid ise otseselt ei juhi, välja arvatud keskastme juhte. Lõpuks tuleb vihjeandmissüsteemi toimimist vähemalt kord aastas üle vaadata ja täiendada nii kogemuste kui ka töötajate tagasiside alusel.

Vihjekanalide loomine on teenindusettevõtte X jaoks mitte ainult seadusest tulenev kohustus, vaid ka kasulik tööriist julgustamiseks töötajaid võimalike rikkumiste kohta vihjet andma. See võimaldab ettevõttel X probleeme varakult märgata ning parandada organisatsiooni üldist töökeskkonda. Vajadust vihjekanalide järele näitavad ka käesoleva töö raames läbi viidud uuringu tulemused, mille kohaselt ei jõua paljud probleemid juhtideni, sest töötajad kardavad teatamisega kaasnevaid negatiivseid tagajärgi või ei usu, et vihjeandmisega mingisugune muutus kaasneks.

Käesolevat magistritööd on võimalik edasi arendada, uurides, kuidas vihjekanalide loomine ja kasutuselevõtt tegelikult mõjutab rikkumiste avastamist ning töötajate valmidust neist teatada. Võrdlev analüüs selliste ettevõtete vahel, kus vihjekanal on juba aktiivselt kasutusel ning kus seda alles luuakse, aitaks selgitada välja parimad praktikad ja peamised takistused, mis vihjekanalide tõhusust vähendavad.

Viidatud allikad

1. 2019/1937. (2019). *Euroopa Parlamendi ja nõukogu direktiiv (EL) 2019/1937, 23. oktoober 2019, liidu õiguse rikkumisest teavitavate isikute kaitse kohta*. European Union law. Vaadatud 17.09.2025. <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32019L1937>
2. ACFE. (2024). *Occupational fraud 2024: a report to the nations®*. Association of Certified Fraud Examiners. Vaadatud 07.01.2026. <https://www.acfe.com/-/media/files/acfe/pdfs/rtnn/2024/2024-report-to-the-nations.pdf>
3. Adli Roslan, M.S., Hamid, M.H., Said, R., & Mohd Razali, F. (2025). Whistleblowing Effectiveness: The Role of Ethical Climate and Regulatory Strength in Shaping the Whistleblowing Index. *Advanced International Journal of Business Entrepreneurship and SMEs*, 7, 209-223. DOI: 10.35631/AIJBES.724014.
4. Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211. DOI: 10.1016/0749-5978(91)90020-T
5. Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Hum Behav & Emerg Tech*, 2, 314–324. DOI: 10.1002/hbe2.195.
6. Aren, K. (2025). *Asutusesisese vilepuhumise protsessi parendamine Eesti avalikus sektoris*. Magistritöö. Tallinna Tehnikaülikool, infotehnoloogia teaduskond. Vaadatud 31.01.2026. <https://www.corporatecrime.co.uk/post/ecthr-luxleaks-whistleblower>
7. Banisar, D. (2023). *The European Court of Human Rights protects LuxLeaks whistleblower*. Corporate Crime Observatory. Vaadatud 02.04.2026.
8. Bishop-Monroe, R., Cockrell, S.R., Di Paolo Harrison, B.M. & Miller, G.J. (2021). Thank you whistleblower! How organizations can cultivate whistleblower activity to enhance business success. *Organizational Dynamics*, 50(4), DOI: 10.1016/j.orgdyn.2020.100814.
9. Ciuapala, D. (2024). *Clarifications on Whistleblower Protection and Internal Reporting Channels in Corporate Groups*. Peterka & Partners. Vaadatud 05.02.2026. <https://blog.peterkapartners.com/clarifications-on-whistleblower-protection-and-internal-reporting-channels-in-corporate-groups/>
10. Cordis, A.S., & Lambert, E.M. (2017). Whistleblower laws and corporate fraud: Evidence from the United States. *Accounting Forum*, 41(4), 289-299. DOI: 10.1016/j.accfor.2017.10.003.
11. Daroglou, G., Barkoukis, V., Fairs, L.R.W., Toner, J., Jones, L., Perry, J.L., Micle, A.V., Theodorou, N.C., Shakhverdieva, S., Stoicescu, M., Constantin, P.-N., Vesic, M.V., Dikic, N., Andjelkovic, M., Muñoz-Guerra Revilla, J., García Grimau, E., Martínez, M.A.E.,

- Amigo, J.A., Schomöller, A., & Nicholls, A.R. (2025). Athletes' beliefs about whistleblowing doping misconduct from six European countries: A social cognitive perspective. *Emerging Trends in Drugs, Addictions, and Health*, 5. DOI: 10.1016/j.etdah.2025.100181.
12. Djawadi, B.M., Plaß, S., & Loer, S. (2025). "I don't believe that you believe what I believe": an experiment on misperceptions of social norms and whistleblowing. *European Economic Review*, 180. DOI: 10.1016/j.euroecorev.2025.105189.
13. Dungan, J., Waytz, A., & Young, L. (2015). The psychology of whistleblowing. *Current Opinion in Psychology*, 6, 129-133. DOI: 10.1016/j.copsyc.2015.07.005.
14. Erikson, M. (2021). *Rikkumisest teavitaja kaitse töösuhtes*. Juridica. Vaadatud 04.01.2026.
https://www.juridica.ee/article_full.php?uri=2021_1_rikkumisest_teavitaja_kaitse_t_suhtes&pdf=1
15. European Commision. (n.d.). *EU Open Source Solutions Catalogue*. Interoperable Europe. Vaadatud 29.01.2026. <https://interoperable-europe.ec.europa.eu/eu-oss-catalogue/solutions/globaleaks>
16. Eurostat. (2025). *Accidents at work statistics*. Vaadatud 20.02.2026.
https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Accidents_at_work_statistics
17. Evchenko, O. (2016). Моральная проблема сигнализаторства. [Signaliseerimise moraalne probleem]. *TRAEKTORIÁ NAUKI*, 2(3), ISSN: 2413-9009, 6.1-6.5. Vaadatud 22.10.2025. <https://pathofscience.org/index.php/pVOLTRIs/article/view/45/122>
18. EWR Online. (2025). *Eesti sai viivitamise eest Euroopa Liidu käest trahvi*. Vaadatud 17.09.2025. <https://www.eesti.ca/eesti-sai-viivitamise-eest-euroopa-liidu-kaest-trahvi/article61471>
19. Fischer, M., & Gollwitzer, M. (2025). Personality Effects on Two Types of Whistleblowing Decisions. *Social Psychological Bulletin*, 20. DOI: 10.32872/spb.12243.
20. Furlow, B. (2011). US physician whistleblowers face intimidation and retaliation. *The Lancet Oncology*, 12(8), 727. DOI: 10.1016/S1470-2045(11)70180-2.
21. GlobaLeaks. (n.d.). *Reporting*. Vaadatud 07.02.2026.
<https://docs.globaleaks.org/en/stable/reporting/reporting.html#save-your-access-code>
22. Goh, E., & Lee, C. (2018). A workforce to be reckoned with: The emerging pivotal Generation Z hospitality workforce. *International Journal of Hospitality Management*, 73, 20-28. DOI: 10.1016/j.ijhm.2018.01.016.

23. Hilton. (n.d.a). *Code of Conduct*. Vaadatud 05.02.2026.
<https://ir.hilton.com/~media/Files/H/Hilton-Worldwide-IR-V3/committee-composition/HW-Code-Of-Conduct-OCT2015-L26.pdf>
24. Hilton. (n.d.b). *Explore the world with Hilton*. Vaadatud 05.02.2026.
<https://www.hilton.com/en/locations/>
25. Hilton. (n.d.c). *Privacy Notice for Hilton Worldwide Holdings Inc. Hotline*. Vaadatud 02.03.2026.
<https://secure.ethicspoint.com/domain/media/en/gui/23073/consent.html?clientid=23091&CMlocationid=100339&companylocation=Estonia&override=yes&agreement=no&companyname=Hilton&RedirectClientId=23091>
26. Hilton. (n.d.d). *Raise a Concern Online*. Vaadatud 02.03.2026.
<https://secure.ethicspoint.com/domain/media/en/gui/23073/report.html>
27. Hilton. (n.d.e). *Select an Issue Type*. Vaadatud 02.03.2026.
<https://secure.ethicspoint.com/domain/media/en/gui/23073/issues.html?clientid=23091&CMlocationid=100339&companylocation=Estonia&override=yes&agreement=no&companyname=Hilton&RedirectClientId=23091>
28. Hakim Z., A., Safira, & Mahmudah, H. (2019). Whistleblowing Intention: A Study of Situation Factors. *SSRG International Journal of Economics and Management Studies*, 6(12), 132-140. DOI: 10.14445/23939125/IJEMS-V6I12P115.
29. Hersh, M.A. (2002). Whistleblowers - Heroes or Traitors?: Individual and Collective Responsibility for Ethical Behaviour. *Annual Reviews in Control* 26, 243-262. DOI: 10.1016/S1367-5788(02)00025-1.
30. Ibrahim, I.A., Doddanavar, I., Abdelrahim, S.M., & Abou Zeid, M.A.G. (2025). The role of ethical leadership in promoting internal whistleblowing among nurses: A dual-mediation model analysis of psychological safety and reporting attitudes. *International Journal of Nursing Sciences*, 12(5), 431-437. DOI: 10.1016/j.ijnss.2025.08.004.
31. Jatsa, A. (2019). *Vihjeandmise mehhanism ettevõttes*. Tööriistakast. Korruptsioonivaba Eesti. Vaadatud 30.01.2026. <https://transparency.ee/publikatsioonid/vihjeandmise-mehhanism-ettevottes-tooriistakast>
32. Komisarof, A., & Akaliyski, P. (2025). New developments in Hofstede's Individualism-Collectivism: A guide for scholars, educators, trainers, and other practitioners. *International Journal of Intercultural Relations*, 107. DOI: 10.1016/j.ijintrel.2025.102200.
33. Korruptsioonivaba Eesti. (n.d.). *Whistleblower protection*. Vaadatud 04.01.2026.
<https://www.transparency.ee/en/whistleblower-protection-1>

34. Kusmierz, J. (2024). *Is whistleblowing protection possible in multinational businesses?*. Global Alliance. Vaadatud 04.02.2026. <https://www.ggi.com/news/auditing/is-whistleblowing-protection-possible-in-multinational-businesses>
35. Kүүts, A. (2024). *Töölasest Euroopa Liidu õiguse rikkumisest teavitajad saavad parema kaitse*. Justiits- ja Digiministeerium. Vaadatud 17.09.2025. <https://www.justdigi.ee/uudised/toolasest-euroopa-liidu-oiguse-rikkumisest-teavitajad-saavad-parema-kaitse>
36. Lata, M., & Chaudhary, R. (2020). Workplace Spirituality and Experienced Incivility at Work: Modeling Dark Triad as a Moderator. *J Bus Ethics*, 174, 645–667. DOI: 10.1007/s10551-020-04617-y.
37. LOI n° 2022-401. (2022). *LOI n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte (1)*. [21. märtsi 2022. aasta seadus nr 2022-401, mille eesmärk on parandada vilepuhujate kaitset (1)]. Journal officiel "Lois et Décrets". Vaadatud 22.10.2025. <https://www.legifrance.gouv.fr/jorf/id/JORFARTI000045388750>
38. Lõvi, S. (2023). *Government goes for new try with whistleblower protection bill*. ERR. Vaadatud 22.09.2025. <https://news.err.ee/1609075649/government-goes-for-new-try-with-whistleblower-protection-bill>
39. Mechtenberg, L., Muehlheusser, G., & Roider, A. (2020). Whistleblower protection: Theory and experimental evidence. *European Economic Review*, 126. DOI: 10.1016/j.eurocorev.2020.103447.
40. National Whistleblower Center. (n.d.). *The European Union Whistleblower Directive*. Vaadatud 04.01.2026. <https://www.whistleblowers.org/what-is-the-european-whistleblower-directive/>
41. Navex. (n.d.). *File a Report*. Vaadatud 02.03.2026. https://secure.ethicspoint.com/domain/en/report_information.asp?clientid=23091&CMlocation=100339&companylocation=Estonia&override=yes&agreement=no&companyname=Hilton&RedirectClientId=23091&violationtypeid=17480
42. Nur'aini, R.Y., & Pujiningsih, S. (2021). What factors affect students' whistleblowing intentions?. *Jurnal Studi Akuntansi dan Keuangan*, 4(2), 151 - 162. DOI: 10.29303/akurasi.v4i2.102.
43. Paatsi, K., & Haabu, H. (2024). *Vilepuhujat kaitsev seadus sai lõpuks vastu võetud*. Cobalt. Vaadatud 04.01.2026. <https://www.cobalt.legal/et/news-cases/vilepuhujat-kaitsev-seadus-sai-lopuks-vastu-voetud/>

44. Palojärv, K. (2021). *Vihjeandmine ja selle teavitustiini loomise võimalused Eesti kohalikes omavalitsustes*. Magistritöö. Eesti Maaülikool, majandus- ja sotsiaalinstituut, majandusarvestuse ja finantsjuhtimise õppekava. Vaadatud 25.01.2026.
<https://dspace.emu.ee/server/api/core/bitstreams/066988b9-5269-4b6b-aa71-85297447dae5/content>
45. Puh, K., ja Tökke, M. (2024). *Employee attitudes and intentions towards whistleblowing in Estonia*. Magistritöö. Tartu Ülikool, majandusteaduse õppekava. Vaadatud 07.11.2025.
<https://dspace.ut.ee/server/api/core/bitstreams/3c60fe4c-5899-43de-95fa-7032649c44a3/content>
46. Putri, C.M. (2018). Does Type of Fraudulent Act Have an Impact On Whistleblowing Intention?. *Journal of Accounting and Investment*, 19(2), 210-225. DOI: 10.18196/jai.1902102.
47. Qasem, F. (2025). Whistleblower protections and their impact on reducing corruption in public and private sectors. *E-Journal VFU*, 341-350. DOI: 10.53606/evfu.24.341-350.
48. Ramazanov, K. (2016). Развитие института добровольного информирования о коррупционных правонарушениях. [Korruptsioonikuritegude vabatahtliku teavitamise institutsiooni arendamine]. *Противодействие коррупции: государственная политика и гражданское общество*. Vaadatud 14.01.2026. <https://ssrn.com/abstract=2756485>
49. Ratner, B. (2009). The correlation coefficient: Its values range between +1/-1, or do they?. *J Target Meas Anal Mark* 17, 139–142 (2009). DOI: 10.1057/jt.2009.5.
50. Saaremägi, R. (2021). *Väärkäitumisest teavitajate kaitse Eestis ja selle kooskõla rahvusvaheliste aktidega*. Magistritöö. Tartu Ülikool, õigusteaduskond, karistusõiguse osakond. Vaadatud 24.11.2025. <https://dspace.ut.ee/server/api/core/bitstreams/49a9673b-6639-44ce-bb98-da4dbc4f9984/content>
51. Scopus. (n.d.). *Document search results*. Vaadatud 20.02.2026.
<https://www.scopus.com/results/results.uri?st1=whistleblowing&st2=&s=TITLE-ABS-KEY%28whistleblowing%29&limit=10&origin=searchbasic&sort=plf-f&src=s&sot=b&sdt=b&sessionSearchId=04d8070400a5c6e168f47ee42670e72d>
52. Smirnova, E. (2024). *Väärkäitumisest teavitamine teenindusettevõtte näitel*. Bakalaureusetöö. Tartu Ülikool, majandusteaduse õppekava. Vaadatud 12.03.2026.
<https://dspace.ut.ee/server/api/core/bitstreams/2143d60a-a5a4-41ec-845c-31d5651b5682/content>
53. Statistikaamet. (n.d.). *Teenindus*. Vaadatud 28.01.2026. <https://www.stat.ee/et/avasta-statistikat/valdkonnad/majandus/teenindus>

54. *Suhtlus kontaktisikuga*. (2026.a). 09.03.2026 isiklik suhtlus telefoni teel täiendava teabe täpsustamiseks.
55. *Suhtlus kontaktisikuga*. (2026.b). 24.04.2026 isiklik suhtlus telefoni teel täiendava teabe täpsustamiseks.
56. Sullivan, G.M., & Artino Jr, A.R. (2013). Analyzing and Interpreting Data From Likert-Type Scales. *Journal of Graduate Medical Education*, 5, 4, 541-542. DOI: 10.4300/JGME-5-4-18.
57. Terracol, M. (2019). *Building on the EU directive for whistleblower protection. Analysis and recommendations*. Transparency International. Vaadatud 04.01.2026.
https://transparency.eu/wp-content/uploads/2024/07/2019_EU_whistleblowing_EN.pdf
58. Terracol, M. (2022). *Internal whistleblowing systems. Best practice principles for public and private organisations*. Transparency International. Vaadatud 20.01.2026.
https://files.transparencycdn.org/images/2022_Internal-Whistleblowing-Systems_English.pdf
59. Terracol, M. (2023). *How well do EU countries protect whistleblowers?*. Transparency International. Vaadatud 14.01.2026. https://files.transparencycdn.org/images/2023_How-well-do-EU-countries-protect-whistleblowers_EN.pdf
60. Terracol. (2024). *Internal whistleblowing systems. Self-assessment framework*. Transparency International. Vaadatud 17.05.2026.
https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Ffiles.transparencycdn.org%2Fimages%2FInternal-whistleblowing-systems-Self-assessment-framework-for-public-and-private-organisations_Excel_Word.docx&wdOrigin=BROWSELINK
61. Tiits, T. (2014). *Rikkumisest teavitamisega seonduvaid probleeme Eestis*. Juridica. Number 2014/6, 443-453. Vaadatud 03.11.2025.
https://www.juridica.ee/article.php?uri=2014_6_rikkumisest_teavitamisega_seonduvaid_probleeme_ee_tis
62. Transparency International. (n.d.). *Whistleblowing*. Vaadatud 23.10.2025.
<https://www.transparency.org/en/our-priorities/whistleblowing>
63. Transparency International. (2020). *Exposing the truth to save taxpayers' money*. Vaadatud 22.10.2025. <https://www.transparency.org/en/news/world-whistleblower-day-cost-of-exposing-facts-age-of-misinformation>
64. Transparency International. (2025). *World Whistleblower Day: The cost of exposing facts in the age of misinformation*. Vaadatud 22.10.2025.
<https://www.transparency.org/en/news/world-whistleblower-day-cost-of-exposing-facts-age-of-misinformation>

65. Trofimov, J. (2021). *Антикоррупционная денунциация: методологические проблемы, зарубежный опыт и Российские перспективы*. [Korruptsioonivastane vihjeandmine: metodoloogilised probleemid, rahvusvaheline kogemus ja Venemaa väljavaated]. Vaadatud 23.10.2025. <https://cyberleninka.ru/article/n/antikorrupsionnaya-denuntsiatsiya-metodologicheskie-problemy-zarubezhnyy-opyt-i-rossiyskie-perspektivy>
66. TÕRTKS. (2024). *Töölalasest Euroopa Liidu õiguse rikkumisest teavitaja kaitse seadus (lühend - TÕRTKS)*. RT I, 30.05.2024, 1. Riigi teataja. Vaadatud 17.09.2025. <https://www.riigiteataja.ee/akt/130052024001>
67. United Nations. (2004). *United Nations Convention Against Corruption*. United Nations office on drugs and crime, Vienna. Vaadatud 01.02.2026. https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf
68. United Nations. (2019). *Introduction of the Note of the Secretary-General on the report of the Joint Inspection Unit entitled: "Review of whistle-blower policies and practices in United Nations system organizations"*. United Nations System Chief Executives Board for Coordination. United Nations General Assembly Seventy-third Session Fifth Committee. Vaadatud 01.02.2026. https://www.un.org/en/ga/fifth/73/statements/135.%20142.%20Accountability%20JIU/C5_73_1r_ST_2019_03_22_Item_135_Accountablity_142_JIU_CEB.pdf
69. Uus, M. (2016). *Rikkumisest teatamine aitab meil paremaks saada*. nki blogi. Vaadatud 29.01.2026. <https://blog.nk.ee/tulevik/rikkumisest-teatamine-aitab-meil-paremaks-saada#:~:text=nki-suurusel%20ettev%C3%B5ttel%20peab%20olema%20toimiv%20kord%2C%20mis%20aitab,N%20%C3%A4iteks%20v%C3%B5ivad%20need%20olla%20korruptsioon%20v%C3%B5i%20huvide%20konflikt>
70. Vesterinen, A. (2024). *Exploring 9 Typical Whistleblowing Cases in Hotels*. Falcony. Vaadatud 05.02.2026. <https://blog.falcons.io/en/9-typical-whistleblowing-cases-in-hotels>
71. Whistleblowing International Network. (n.d.). *EU Whistleblowing Monitor*. Vaadatud 22.09.2025. <https://whistleblowingmonitor.eu/>
72. Voltri, J., & Whyte, A. (2023). *EU demands substantial fines for late directive implementation in Estonia*. ERR. Vaadatud 22.09.2025. <https://news.err.ee/1609070813/eu-demands-substantial-fines-for-late-directive-implementation-in-estonia>
73. Whistlelink. (2024). *Whistleblowing in the Hospitality Industry: Protecting customers, employees, businesses, and reputation*. Vaadatud 04.02.2026.

<https://www.whistlelink.com/blog/whistleblowing-in-the-hospitality-industry-protecting-customers-employees-businesses-and-reputation/>

74. Zopiatis, A., Constanti, P., & Theocharous, A.L. (2014). Job involvement, commitment, satisfaction and turnover: Evidence from hotel employees in Cyprus. *Tourism Management*, 41, 129-140. DOI: 10.1016/j.tourman.2013.09.013.

LISA A

Vihjeandmise mõiste kasutus kirjanduses

Allikas	Tsitaat	Vihjeandja	Vihjesaaja	Teatamist nõudev tegevus	Eesmärk	Kontekst
Qasem, 2025, lk 341	„Vihjeandmine on tegevus, mille käigus paljastatakse teavet organisatsiooni sees toimuvate ebaseaduslike, ebaeetiliste või kahjulike tegevuste kohta, sageli hõlmates väärkäitumist, mis on kahjulik avalikkusele või aktsionäridele.“	Täpsustamata	Täpsustamata	Ebaseaduslik, ebaeetiline või kahjulik tegevus	Kaitsta avalikkust ja aktsionäre	Organisatsioonis isene
Evchenko, 2016, lk 6.1	„Signaliseerimine (teatamine) on üks moraali- ja õigusnormide rikkumiste vastase võitluse vorme, üks võimalikke vorme üksikisiku ja ühiskonna huvide ning inimväärikuse kaitsmiseks.“	Üksikisik	Täpsustamata	Ebaeetiline või ebaseaduslik tegevus	Kaitsta ennast ja ühiskonda	Üldine
Tiits, 2014	„Mõistet „rikkumisest teavitamine“ /.../ võib lühidalt defineerida kui vahetu ülemuse, muu pädeva isiku või pädeva ametiasutuse, aga ka meedia kaudu laiema avalikkuse teavitamist kindlat liiki ohust, riskist, tulevikus toimuvast või juba toimepandud väärkäitumisest ehk rikkumisest ettevõttes, avaliku sektori asutuses või muudes organisatsioonides.“	Täpsustamata	Vahetu ülemus, pädev isik või asutus, meedia	Tulevane või toimunud rikkumine	Pöörata tähelepanu riskidele, ohtudele ja väärtegadele	Organisatsioonis isene

Hersh, 2002, lk 243	„Vihjeandmine hõlmab tahtlikku teabe avalikustamist mittetriviaalsete tegevuste kohta, mida peetakse ohtlikuks, ebaseaduslikuks, ebaeetiliseks, diskrimineerivaks või muul viisil väärtegudega seonduvaks, üldiselt organisatsiooni praeguste või endiste liikmete poolt.“	Organisatsiooni praegused või endised liikmed	Täpsustamata	Ohtlik, ebaseaduslik, ebaeetiline, diskrimineeriv või muu väärtegevus	Pöörata tähelepanu väärtegudele	Organisatsioonis isene
---------------------------	--	---	--------------	---	---------------------------------	------------------------

Allikas: Autor koostanud järgmiste allikate põhjal: Qasem, 2025; Evchenko, 2016; Tiits, 2014; Hersh, 2002.

LISA B

Vihjeandmist eeldavad rikkumised

Kategooria	Direktiiv nõuab	Organisatsioon võib lisaks nõuda
Finants- ja majanduslikud rikkumised	Euroopa Liidule rahalist kahju põhjustavad tegevused või siseturu ja ettevõtte tulumaksu eeskirjade rikkumised Finantsteenuste, -toodete ja -turgude rikkumised Rahapesu ja terrorismi rahastamine Riigihangetega seotud rikkumised	Rahaliste vahendite, vara või ressursside ilma loata kasutamine Finantsaruannete võltsimine Korruptsioon
Organisatsiooni käitumiseetika rikkumised		Seksuaalne ahistamine, kiusamine, diskrimineerimine Võimu kuritarvitamine Organisatsiooni sisemise eetika- või käitumiskodeksi rikkumine Huvide konflikt Tõsine hooletus või halb juhtimine
Ohutuse ja tervisega seotud rikkumised	Kiirgus- ja tuumaohutuse eeskirjade rikkumised Tooteohutusnõuete rikkumised Transpordiohutuse eeskirjade rikkumised Toidu- ja söödaohutuse ning loomade tervise ja heaolu eeskirjade rikkumised Inimeste tervist tegelikult või tõenäoliselt kahjustavad tegevused	
Keskkonna ja ühiskonnaga seotud rikkumised	Keskkonda kahjustavad tegevused	Laste ärakasutamine või väärkohtlemine

Tarbija ja andmekaitsega
seotud rikkumised

Privaatsuse, isikuandmete kaitse ja infosüsteemi turvalisuse
rikkumised
Tarbijaõiguste rikkumised

Üldised seaduserikkumised

Kõik seaduserikkumised

Allikas: Autor koostanud järgmiste allikate põhjal: TÕRTKS, 2024; Terracol, 2022; Whistlelink, 2024; Vesterinen, 2024.

LISA C

Küsimustik

Vihjeandmise uuring

Olen Tartu Ülikooli kaasaegse majanduse õppekava magistrant ja viin magistritöö raames läbi uurimuse.

Vihjeandmine ehk rikkumisest teavitamine on olukord, kus töötaja annab teada organisatsioonis toimunud või toimuvast rikkumisest, näiteks ebaeetilisest või seadusevastasest tegevusest.

Selle küsitluse eesmärk on mõista töötajate arvamust selle kohta, kuidas ettevõttes rikkumistest teatada ning millised tingimused on vajalikud turvalise ja tõhusa vihjeandmiskanali loomiseks.

Küsitluses ei ole õigeid ega valesid vastuseid. Oluline on ainult Teie isiklik arvamus ja kogemus.

Küsitlus on täiesti anonüümne, seega ei saa vastaja isikut tuvastada.

Andmeid kasutatakse ainult minu magistritöö jaoks ja neid säilitatakse Tartu Ülikooli turvalises OneDrive'i keskkonnas. Andmetele on juurdepääs ainult minul kui küsitluse autoril.

Küsitlus sisaldab 18 küsimust. Selle täitmine võtab aega umbes 5–10 minutit. Osalemine on vabatahtlik, seega võite osalemisest igal ajal loobuda.

Küsimuste korral võtke minuga julgelt ühendust.

Nimi: Erika Smirnova

E-post: erikasm@ut.ee

Klõpsates nupul „Esita“, kinnitate oma vabatahtliku nõusoleku osalemiseks.

Täna Teid panuse eest!

* Tärniga tähistatud küsimused on vastamiseks kohustuslikud.

1. Palun märkige oma tööstaaž ettevõttes.*

- ☐ Alla 1 aasta
- ☐ 1–4 aastat
- ☐ 5–9 aastat
- ☐ 10–14 aastat
- ☐ Üle 15 aasta
- ☐ Ei soovi täpsustada

2. Palun märkige oma roll ettevõttes.*

- ☐ Töötaja
- ☐ Juht
- ☐ Ei soovi täpsustada

- Muu:

3. Kas olete kunagi töökohal kokku puutunud olukorraga, mida olete pidanud rikkumiseks (nt reeglite rikkumine, ebaeetiline käitumine või muu)?*

- Jah
- Ei
- Pole kindel

4. Kui vastasite „Jah“ või „Pole kindel“, siis palun täpsustage üldsõnaliselt, millise olukorraga oli tegemist.

*(Kui see küsimus Teie kohta ei kehti, siis palun märkige „–“)**

5. Kui sellisesse olukorda sattusite, kas teatasite sellest?*

- Jah
- Ei
- Ei ole kokku puutunud

6. Kui vastasite „Jah“, siis palun kirjeldage üldiselt, kuidas Te rikkumisest teatasite ja milline oli selle tulemus.

*(Kui see küsimus Teie kohta ei kehti, siis palun märkige „–“)**

7. Kui Te rikkumisest EI teatanud, siis miks?

*(Võite valida mitu varianti)**

- Ei ole kokku puutunud
- Ma polnud kindel, kas see oli rikkumine
- Ma ei teadnud, kellele sellest teatada
- Ma kartsin negatiivseid tagajärgi (nt suhete halvenemist, tagakiusamist)
- Ma ei uskunud, et midagi muutub
- Ma arvasin, et see pole minu asi
- Muu:

8. Kui oleksite töökohal rikkumise tunnistajaks, kuidas Te tõenäoliselt esmalt tegutseksite?*

- Ma ei võtaks midagi ette
- Teataksin sellest oma otsesele juhile
- Teataksin sellest kõrgemale juhtkonnale
- Kasutaksin spetsiaalset vihjeandmiskanalit (kui see oleks olemas)
- Teavitaksin ettevõtteväliseid osapooli (nt politseid, meediat)
- Arutaksin olukorda kaastöötajate, sõprade või pereliikmetega
- Muu:

9. Kujutage ette, et avastate meie ettevõttes ühe alljärgnevatest olukordadest. Palun märkige, kas Teie hinnangul tuleks sellest teavitada ning keda tuleks teavitada.*

	Ei tuleks teavitada	Tuleks teavitada ettevõtte sees (nt teavitada juhtkonda või kasutada vihjeandmiskanalit)	Tuleks teavitada ettevõtteväliselt (nt politseid, meediat)
Seaduserikkumine	☐	☐	☐
Tegevus, mis ohustab inimeste tervist või ohutust	☐	☐	☐
Töötajatevaheline konflikt	☐	☐	☐
Finantsrikkumine või ressursside väärkasutamine	☐	☐	☐
Diskrimineerimine või ebavõrdne kohtlemine	☐	☐	☐
Juhtkonna otsus, millega töötaja ei nõustu	☐	☐	☐
Isikuandmetega seotud rikkumine	☐	☐	☐
Finantsaruannete võltsimine	☐	☐	☐
Ettevõtte käitumiskodeksi rikkumine	☐	☐	☐
Korruptsioon	☐	☐	☐

10. Kui soovite mõnda 9. küsimuse vastust täpsustada, siis palun kirjutage siia.

11. Kui olulised on Teie jaoks järgmised potentsiaalsed riskid rikkumisest teatamisel?
(Palun hinnake iga valikut skaalal 1 kuni 5, kus 1 – üldse mitte oluline, 2 – pigem ebaoluline, 3 – nii ja naa, 4 – pigem oluline ja 5 – väga oluline)*

	1 – üldse mitte oluline	2	3 – nii ja naa	4	5 – väga oluline
Vallandamine või koondamine	☐	☐	☐	☐	☐
Töölalasesse „musta nimekirja“ kandmine	☐	☐	☐	☐	☐
Tööülesannete muutmine	☐	☐	☐	☐	☐
Sotsiaalne isolatsioon (nt väärkohtlemine, teabest ilma jätmine)	☐	☐	☐	☐	☐
Kohtumenetluse alustamise ähvardused	☐	☐	☐	☐	☐
Kaastöötajate või juhtide negatiivne reageering	☐	☐	☐	☐	☐
Teavituse ignoreerimine	☐	☐	☐	☐	☐

12. Kui olulised on Teie jaoks järgmised vihjeandmiskanali omadused?

(Palun hinnake iga valikut skaalal 1 kuni 5, kus 1 – üldse mitte oluline, 2 – pigem ebaoluline, 3 – nii ja naa, 4 – pigem oluline ja 5 – väga oluline)*

	1 – üldse mitte oluline	2	3 – nii ja naa	4	5 – väga oluline
Võimalus teatada anonüümselt	☐	☐	☐	☐	☐
Teabe konfidentsiaalsus	☐	☐	☐	☐	☐
Kaitse negatiivsete tagajärgede eest (nt vallandamine, väärkohtlemine)	☐	☐	☐	☐	☐
Teate saaja sõltumatus	☐	☐	☐	☐	☐
Selge teavitusprotsess (nt juhiste olemasolu, koolitused)	☐	☐	☐	☐	☐
Tagasiside saamine (nt teate kättesaamise ja uurimise tulemuste kohta)	☐	☐	☐	☐	☐
Võimalus teatada ilma oma otsese juhi vahendusega	☐	☐	☐	☐	☐
Selged tagasisidestamise tähtsused	☐	☐	☐	☐	☐

13. Kui vajalik on meie ettevõttes vihjeandmiskanali olemasolu?*

- ☐ Üldse mitte vajalik
- ☐ Pigem mitte vajalik
- ☐ Nii ja naa
- ☐ Pigem vajalik
- ☐ Väga vajalik

14. Kui meie ettevõtte loob spetsiaalse vihjeandmiskanali, siis kui tõenäoline on, et Te seda kasutate?*

- ☐ Väga ebatõenäoline
- ☐ Üsna ebatõenäoline
- ☐ Üsna tõenäoline
- ☐ Väga tõenäoline

15. Kui meie ettevõtte loob vihjeandmiskanali, siis kui sobivaks peate järgmisi teatamisviise? (Palun hinnake iga valikut skaalal 1 kuni 5, kus 1 – üldse ei sobi, 2 – pigem sobimatu, 3 – nii ja naa, 4 – pigem sobib ja 5 – väga sobiv)*

	1 – üldse ei sobi	2	3 – nii ja naa	4	5 – väga sobiv
Konfidentsiaalne veebivorm	☐	☐	☐	☐	☐
E-post	☐	☐	☐	☐	☐
Telefon	☐	☐	☐	☐	☐
Spetsiaalne sõnumikast	☐	☐	☐	☐	☐
Isiklik kohtumine vastutava isikuga	☐	☐	☐	☐	☐

16. Kui teil on täiendavaid mõtteid või ettepanekuid seoses vihjeandmiskanali või teatamisviisidega, siis palun kirjutage need siia.

17. Millist vihjeandmiskanali korraldust peate kõige sobivamaks?*

- ☐ Kanal, mis toimib kogu grupi ulatuses
- ☐ Kanal, mis toimib ainult meie ettevõtte sees
- ☐ Mõlema rakendamine

18. Palun põhjendage 17. küsimusele antud vastust.*

LISA D

Vastajate kokkupuutumine tööalaste rikkumistega

Rikkumise kategooria	Alamkategooria	Vastuste arv
Eetikavastane käitumine ja sobimatu suhtlemine	Naeruvääristamine, töökaaslaste klatš, solvavad naljad	2
	Ebaviisakus, solvangud, karjumine	3
	Vaidlused ja konfliktsituatsioonid	1
	Töötajate üldine ebaetiline käitumine	2
Psühholoogiline surve ja kiusamine	Ebasoodsa töökeskkonna loomine, töölt tähelepanu kõrvalejuhtimine	2
	Psühholoogiline surve, eelarvamused	2
	Töökaaslaste kiusamine	1
Tööõiguse, töökorralduse ja sisekorra rikkumised	Tööõiguse rikkumised ja ebavõrdne kohtlemine	1
	Tööaja, puhkusegraafiku ja palgaküsimused	2
	Dokumentatsiooni ja tööülesannete rikkumised	3
	Murtud lubadused ja ebaselged vastutuspiirid	1
	Tööle ilmumine joobes olekus	2
Üldised või täpsustamata olukorrad		4

Märkus: Avatud küsimuses mainisid mõned vastajad rohkem kui ühte olukorda, seega on tabelis esitatud rohkem olukordi kui nende vastajate arv, kes rikkumisi tegelikult kogesid.

Allikas: Autor koostanud küsitluse vastuste põhjal.

LISA E

Vastajate hinnang teatamisvajadusele ja -viisile

Olukord	Ei tuleks teatada	Tuleks teatada ettevõttesiseselt	Tuleks teatada ettevõtteväliselt
Seaduserikkumine	2%	82%	16%
Inimest ohustav tegevus	0%	66%	34%
Töötajatevaheline konflikt	48%	52%	0%
Finantsrikkumine või ressursside väärkasutamine	5%	77%	18%
Diskrimineerimine või ebavõrdne kohtlemine	4,5%	91%	4,5%
Mittenõustumine juhtkonna otsusega	34%	61%	5%
Isikuandmetega seotud rikkumine	7%	79%	14%
Finantsaruannete võltsimine	5%	61%	34%
Käitumisjuhendi rikkumine	9%	80%	11%
Korruptsioon	5%	45%	50%

Allikas: Autor koostanud küsitluse vastuste põhjal.

LISA F

Vihjekanali omaduste korrelatsioonimaatriks

Tegurid	1.	2.	3.	4.	5.	6.	7.	8.
1. Anonüümsus	1							
2. Konfidentsiaalsus	0,81**	1						
3. Kaitse survemeetmete eest	0,24	0,46**	1					
4. Vihjesaaja sõltumatus	0,34*	0,31*	0,48**	1				
5. Selge protsess	0,25	0,40**	0,48**	0,44**	1			
6. Tagasisidestamine	0,27	0,41**	0,58**	0,40**	0,66**	1		
7. Juhi vahendusest teatamine	0,09	0,20	0,25	0,05	0,20	0,38*	1	
8. Selged tagasisidestamise tähtsused	0,15	0,22	0,52**	0,27	0,60**	0,70**	0,42**	1

Märkus: Märgiga „***“ on tähistatud statistiliselt oluline korrelatsioon olulisuse nivoo 0,01 korral ja märgiga „**“ olulisuse nivoo 0,05 korral. Tugevad seosed on esitatud paksemas kirjas. Tegureid tähistatakse veerus täisnimetusega ning reas ainult numbriga vastavalt tegurite veeru järjestusele.

Allikas: Autor koostanud küsitluse vastuste põhjal ning Exceli funktsiooni Data Analysis korrelatsiooni- ja regressioonanalüüsi abil.

LISA G

Uuringu tulemuste ja teoreetiliste seisukohtade võrdlus

Allikas	Teoreetiline käsitlus	Uuringu tulemus
Bishop-Monroe et al. (2021), Terracol (2022), Korruptsioonivaba Eesti (n.d.), Saaremägi (2021)	Rikkumiste varajane avastamine vähendab kahjusid.	Vastajad rõhutasid vihjeandmise eelistena maine säilitamist ja probleemide kiiret lahendamist.
Terracol (2023), Terracol (2022)	Seaduses sätestatud piiratud loetelu tuleb ettevõtte äranägemise järgi laiendada.	Vastajad tõid esile laiema hulga probleeme, mida peeti vihjeandmist vajavaks.
Saaremägi (2021), Putri (2018)	Töötajad teavitavad esimesena sageli juhte.	Enamik vastajaid, kes rikkumist märkas, pöördus esmalt oma vahetu juhi poole.
Terracol (2024)	Vihjesaaja peab olema sõltumatu.	Vastutava isiku sõltumatus oli vastajate hulgas kõrgelt hinnatud.
Jatsa (2019), Terracol (2022)	Regulaarne tagasiside on oluline.	Tagasisidestamine sai kõrge hinnangu, kuid selged tagasisidestamise tähtsajad said vastupidi üsna madala hinnangu.
Saaremägi (2021), Jatsa (2019), Palojärv (2021)	Hirm kättemaksu ja vihje ignoreerimise ees vähendab valmidust vihjet anda.	Peamised mitteteatamise põhjused olid survemeetmete kartus ja usk, et midagi ei muutu.
Djawadi, Plaß & Loer (2025), Dungan, Waytz & Young (2015), Daroglou et al. (2025)	Grupi positiivne suhtumine ja sotsiaalse surve vähendamine suurendab vihjeandmise kavatsust.	Töötajad kardavad negatiivseid tagajärgi, sealhulgas suhete halvenemist kaastöötajatega, mis kinnitab sotsiaalse surve olulisust.
Hakim Z., Safira & Mahmudah (2019), Dungan, Waytz & Young (2015), Puh & Tökke (2024)	Kõrgemal ametikohal töötavad inimesed teatavad rikkumisest tõenäolisemalt.	Ei leidnud kinnitust, kuna juhid ei teatanud probleemidest, vaid püüdsid ise neid reguleerida. Ka tööstaaži osas ei leitud märgatavaid erinevusi.

Allikas: Autor koostanud järgmiste allikate põhjal: Bishop-Monroe et al., 2021; Terracol, 2022; Terracol, 2024; Korruptsioonivaba Eesti, n.d.; Saaremägi, 2021; Terracol, 2023; Putri, 2018; ACFE, 2024; Jatsa, 2019; Palojärv, 2021; Djawadi, Plaß & Loer, 2025; Dungan, Waytz & Young, 2015; Daroglou et al., 2025; Ajzen, 2020; Hakim Z., Safira & Mahmudah, 2019; Puh & Tökke, 2024.

Summary

CREATING A WHISTLEBLOWING CHANNEL USING SERVICE COMPANY X AS AN EXAMPLE

Erika Smirnova

Misconduct can occur in any organization, ranging from unethical behaviour and discrimination to fraud and breaches of internal rules. Such incidents damage both employees and the company, causing reputational harm, financial losses, and legal risks.

Employees are usually the first to notice problems as they work within the daily processes. However, many hesitate to report violations due to fear of negative consequences. This thesis uses the term “whistleblowing” to describe the reporting of potential or actual misconduct within an organization.

The topic has gained significant importance after the adoption of the European Union’s directive, which sets minimum standards for the protection of whistleblowers. In Estonia, the relevant law entered into force on 1 September 2024. From January 1, 2025, companies with more than 50 employees are required to create an internal confidential whistleblowing channel.

This master’s thesis aims to develop practical recommendations for creating an effective whistleblowing system for service company X, operating in the accommodation and catering sector, and to create a demo version based on theoretical analysis and empirical findings. The theoretical part examines the definition of whistleblowing, the requirements of the European Union directive and Estonian law, as well as the key conditions for a well-functioning reporting channel. Factors influencing people’s willingness to report were also examined, including legal protection, organizational culture, and individual employee characteristics.

The empirical part is based on an anonymous online survey conducted among 44 employees and managers of service company X. The results showed that every second respondent had encountered situations at work that they considered violations. Most often, these included unethical behaviour or breaches of internal procedures. Only 45% of those who noticed a problem reported it, usually to their immediate supervisor. The main reasons for silence were fear of negative consequences and disbelief that anything would change.

Respondents highly valued confidentiality, protection from negative consequences, and the independence of the person receiving reports. A confidential web form was clearly the most preferred reporting channel.

Based on the theory and survey results, a demo version of the channel was created using the free GlobaLeaks platform. It offers violation categories with explanations, detailed questions, a file upload option, and both anonymous and confidential reporting methods.

Practical recommendations for service company X include appointing the company director as responsible for the reporting channel, expanding the list of reportable violations, developing clear instructions with examples and guiding questions, informing staff through posters, QR-codes, and regular training, and reviewing the system annually.

Creating such a channel will help the service company X not only meet legal requirements but also detect problems early, improve the work environment, build trust, and reduce business risk. In a sector with high staff turnover and seasonal employment, it will enable faster responses to issues and support a more trusting work environment.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Erika Smirnova,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose

„Vihjekanali loomine teenindusettevõtte X näitel“,

mille juhendaja on Anne Reino,

reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada Tartu Ülikooli digitaalarhiivi kuni autoriõiguse kehtivuse lõppemiseni;

2. annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi kaudu Creative Commons litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni;
3. olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile;
4. kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Erika Smirnova

18.05.2026