TRANSPARENCY INTERNATIONAL
Korruptsioonivaba Eesti

Vihjeandjate kaitse Eestis: praktika ja kogemused

2026

PROJEKTI PARTNERID:

Delna
SABIEDRĪBA PAR ATKLĀTĪBU
TRANSPARENCY INTERNATIONAL
LATVIJAS NODAĻA

TRANSPARENCY INTERNATIONAL
Korruptsioonivaba Eesti

CENTRUL ROMÂN DE POLITICI EUROPENE
CRPE
DEBATING EUROPE, PROVIDING EXPERTISE

UNIVERSITÀ DI TORINO

INSTYTUT SPRAW OBYWATELSKICH

AMAPOLA
PROGETTI PER LA SICUREZZA DELLE PERSONE E DELLE COMUNITÀ

RAHASTAJA:

Kaasrahastanud Euroopa Liit

Sisukord

Lühiülevaade	1
1. Sissejuhatus	3
2. Riigi õiguslik ja regulatiivne taust	4
3. Teavituskanalite korraldus ja koostöö väliste osapooltega	7
4. Teadete arv, teemad ja tulemused	11
5. Vihjeandjate kaitsemeetmed ja tugi	15
6. Väljakutsed ja tugevused	19
Kokkuvõte	22
Soovitused vihjekanali haldajatele	25
Soovitused seadusandjale	28
Lisa 1. Intervjueeritud vihjekanalite haldajate nimekiri.	31
Kasutatud kirjandus	32
Kasulikke materjale	32

Lühiülevaade

Käesolev analüüs teeb ülevaate vihjeandjate kaitse praktilisest rakendamisest Eestis, tuginedes projekti WAKE UP (*Whistleblower Advocacy for Knowledge, Empowerment, Unity, and Protection*) raames vihjekanalite haldajatega läbiviidud intervjuudele. Kuigi Eesti on täitnud EL-i direktiivi miinimumnõuded, on rakendamise praktika veel välja kujunemas ja organisatsioonide lõikes üpris killustatud.

Peamised väljakutsed ja kitsaskohad

- **Kultuurilised barjäärid ja hoiakud:** vihjeandmist seostatakse endiselt kohati negatiivse "pealekaebamise" või nõukogude pärandiga, samuti võivad teavitamist pärssida juhtide hoiakud.
- **Seaduse kohaldamisala ja tegelikkuse vastuolu:** õigusraamistik keskendub peamiselt EL-i õiguse rikkumistele, jättes sageli seadusliku kaitseta siseriiklikest probleemidest (nt pettused, vargused, töövägivald) teavitajad, mis tekitab töötajates segadust ja võib vähendada usaldust vihjekanalite vastu.
- **Anonüümsuse haprus ja kättemaksuhirm:** väiksemates kollektiivides on vihjeandjat sageli võimalik kaudselt tuvastada. Kuigi otsest kättemaksu intervjuudes osalenud märganud ei ole, on hirm selle ees levinud ning asutustes puuduvad valdavalt süsteemsed järelkontrolli meetmed võimaliku kättemaksu ennetamiseks või tuvastamiseks.
- **Keskse toe ja juhendamise puudumine:** kanalite haldajad tunnevad puudust selgematest suunistest ja võimalusest jagada teiste asutustega parimaid praktikaid.

Peamised tugevused ja edutegurid

- **Turvalised tehnilised lahendused**: välised IT-platvormid on osutunud kriitiliseks tugevuseks, kuna need võimaldavad anonüümset kahepoolset suhtlust, mis parandab oluliselt menetluste kvaliteeti ja infovahetust.
- **Strateegiline menetlustaktika:** kõige tõhusamaks praktikaks peetakse vihjete "maskeerimist" – info kontrollimist muude protsesside (nt rutiinse siseauditi) kaudu, mis ei reeda vihjeandja olemasolu ja pakub talle seeläbi tugevat kaitset.
- **Sõltumatus ja "mõistlikkuse printsiip":** usaldust kasvatab asutusesisene nelja silma printsiip ja teadete käsitlemine eraldiseisva üksuse poolt (nt siseaudit või sisekontroll). Samuti on heaks tavaks kohaldamisala laiendamine, et julgustada teavitama ka sisekorra rikkumistest, mis teeb süsteemi töötajatele arusaadavamaks.

- **Juhtkonna eeskuju:** kultuurimuutuse vältimatuks eelduseks on tippjuhtkonna selged ja järjepidevad väärtussõnumid, mis kinnitavad, et vihjeandmine on organisatsioonikultuuri loomulik osa.

Kokkuvõttes näitavad intervjuud, et vihjeandmise praktikad on organisatsioonides erineval arengutasemel: osa on juba kogenud, samas kui teised alles otsivad oma asutusele sobivaimat lahendust. Eestis tuleks seejuures senisest enam panustada laiemale avalikkusele suunatud teavitustöösse ning juhtide koolitamisse, et kujundada hoiakuid ja toetada organisatsioonikultuuri muutust. Samuti on oluline kaaluda seaduse kohaldamisala laiendamist. Süsteemi laiemaks ja usaldusväärsemaks juurutamiseks on samal ajal hädavajalik pakkuda vihjekanalite menetlejatele tugevamat keskset tuge.

Soovitused

Läbiviidud intervjuude, rahvusvaheliste hinnangute ja parima praktika põhjal on aruande lõpus toodud soovitused vihjekanalite haldajatele (lk 25) ja seadusandjale (lk 28).

- **Soovitused vihjekanalite haldajatele:** Laiendada teavitatavate rikkumiste kohaldamisala, tagada turvaline kahepoolne anonüümne suhtlus ja menetluse konfidentsiaalsus, hoida teavitajat aktiivselt kursis ning ennetada kättemaksu süsteemse järelkontrolli ja juhtkonna toetatud avatud suhtluskultuuri kaudu.
- **Soovitused seadusandjale:** Laiendada vihjeandjate kaitset siseriikliku õiguse rikkumistele, seada miinimumnõuded kanalite struktuursele sõltumatusele, tõhustada kaitset kättemaksu eest läbi selgema tööandja tõendamiskoormise ja reaalsete hüvitiste ning kehtestada nõuded tsentraalseks järelevalveks ja ühtseks andmekogumiseks.

1. Sissejuhatus

Käesolev aruanne käsitleb vihjeandjate kaitse praktilist rakendamist Eestis. Euroopa Liidu vilepuhujate kaitse direktiiv 2019/1937[1] võeti Eesti õigusesse üle 1. septembril 2024, kui jõustus Tööalasest Euroopa Liidu õiguse rikkumisest teavitaja kaitse seadus[2]. Fookuses ei ole aga üksnes õigusraamistik, vaid selle rakendamine ja toimimine organisatsioonide igapäevatöös.

Aruanne tugineb Eestis vihjekanalite haldajatega läbiviidud intervjuudele, mis viidi läbi ajavahemikus november 2025 kuni veebruar 2026 (Lisa 1). Vestlused keskendusid vihjeandmise korraldusele asutustes, sealhulgas teadete vastuvõtmise ja menetlemise protsessidele, konfidentsiaalsuse tagamisele, koostööle väliste osapooltega ning kogemustele vihjeandjate kaitse meetmete rakendamisel. Lisaks käsitleti intervjuudes peamisi väljakutseid ja häid tavasid, mis on rakendamise käigus esile kerkinud.

Intervjueeritavate nimed ei ole aruandes avaldatud; nende rollid ja vastutusalad vihjeandmise süsteemis on esitatud üldistatud kujul. Intervjueeritud isikud esindasid erinevaid avaliku ja erasektori asutusi ning täitsid rolle, mis olid otseselt seotud vihjeandmise teadete vastuvõtmise, menetlemise või koordineerimisega. Selline valim võimaldas saada ülevaate vihjeandmise rakenduspraktikast eri tüüpi asutustes.

Aruanne on üles ehitatud temaatiliste peatükkidena. Pärast sissejuhatust antakse ülevaade Eesti vihjeandjate kaitse õiguslikust ja regulatiivsest taustast. Seejärel käsitletakse teavituskanalite korraldust ja koostööd väliste osapooltega, teadete arvu, teemasid ja menetluse tulemusi ning vihjeandjate kaitsemeetmeid ja tugisüsteeme. Eraldi peatükk on pühendatud peamistele väljakutsetele ja tugevustele, mis intervjuude põhjal esile kerkisid.

Tulemuste tõlgendamisel tuleb arvestada teatud piirangutega. Intervjuudel põhinev analüüs kajastab intervjueeritavate hinnanguid ja kogemusi ning ei pruugi hõlmata kõiki vihjeandmise süsteemi aspekte. Intervjuude valim koosneb asutustest, kus vihjeandmise süsteem on loodud ja kasutusel, mis võimaldas keskenduda praktilistele

[1] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2019/1937 liidu õiguse rikkumisest teavitavate isikute kaitse kohta https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A02019L1937-20241230

[2] Tööalasest Euroopa Liidu õiguse rikkumisest teavitaja kaitse seadus https://www.riigiteataja.ee/akt/117052025002

rakenduskogemustele. Samas ei ole Eestis kättesaadavad koondandmed selle kohta, kui paljudes avaliku või erasektori asutustes vihjeandmise kanalid üldse loodud on või millisel määral need toimivad. Seetõttu ei ole võimalik hinnata, mil määral on intervjueeritud asutused esinduslikud.

Vihjeandjate kaitse rakendus praktikad on kujunemisjärgus ning puuduvad koondandmed loodud kanalite ja nende toimimise kohta.

Lisaks on vihjeandjate kaitse süsteem Eestis suhteliselt uus ning paljud rakendus praktikad on alles kujunemisjärgus. Avaliku statistika ja koondandmete piiratud kättesaadavus raskendab süsteemi toimimise kvantitatiivset hindamist ja üldistuste tegemist. Sellest hoolimata pakub aruanne kasulikku ülevaadet vihjeandmise korraldusest ja kaitsemeetmete rakendamisest asutustes, kus vastavad süsteemid on kasutusel, ning aitab tuvastada valdkondi, kus võib olla vajadus täiendavate selgituste, juhendamise või edasise analüüsi järele.

Aruanne on koostatud projekti WAKE UP (*Whistleblower Advocacy for Knowledge, Empowerment, Unity, and Protection*) raames ning selle koostamist on kaasrahastanud Euroopa Liit.

2. Riigi õiguslik ja regulatiivne taust

Eestis reguleerib vihjeandjate kaitset Tööalasest Euroopa Liidu õiguse rikkumisest teavitaja kaitse seadus, millega võeti üle Euroopa Parlamendi ja nõukogu direktiiv (EL) 2019/1937. Seadus loob raamistiku selleks, kuidas inimesed saavad tööalases kontekstis rikkumistest teada anda ja millist kaitset nad sellisel juhul saavad. Käesolevas peatükis antakse ülevaade seaduse peamistest põhimõtetest ja nõuetest, mis on vihjeandmise praktilise toimimise seisukohalt kõige olulisemad.

2.1. Keda ja milliseid rikkumisi seadus hõlmab

Seadus kaitseb eelkõige neid isikuid, kes annavad tööalases kontekstis teada Euroopa Liidu õiguse rikkumistest. See tähendab, et kaitse kehtib juhul, kui rikkumine on seotud näiteks avalike hangete, finantsteenuste, rahapesu tõkestamise, keskkonnakaitse, rahvatervise, tarbijakaitse või isikuandmete kaitsega. Puhtalt

siseriikliku õiguse rikkumiste puhul seadus üldjuhul ei kohaldu, kui need ei ole seotud seaduses mainitud Euroopa Liidu õigusega.

Seadus ei laiene ka teatud tundlikele valdkondadele, nagu riigikaitse ja riigisaladus, teatud kriminaalmenetluse aspektid ning kutsealase saladuse alla kuuluv teave (näiteks advokaadi ja kliendi vaheline suhtlus või meditsiiniline konfidentsiaalsus).

Isikute ring, keda seadus kaitseb, on seevastu suhteliselt lai. Kaitse laieneb mitte ainult töötajatele, vaid ka endistele töötajatele, tööotsijatele, füüsilisest isikust ettevõtjatele, praktikantidele ja vabatahtlikele. Samuti on kaitstud isikud, kes töötavad alltöövõtjate või tarnijate kaudu. Lisaks võib kaitse laieneda ka vihjeandjaga seotud kolmandatele isikutele, näiteks kolleegidele või pereliikmetele, kui nende suhtes rakendatakse survet või kahjulikke meetmeid seoses vihjeandmisega.

2.2. Avaliku sektori kohustused ja teavituskanalid

Seadus kohustab avaliku sektori asutusi looma asutusesisese teavituskanali, mille kaudu on võimalik tööalases kontekstis rikkumistest teada anda. Kohustus laieneb riigi ja kohaliku omavalitsuse ametiasutustele ning nende hallatavatele asutustele. Väiksematele kohaliku omavalitsuse üksustele kehtib erand, kui elanike arv jääb alla 10 000 või teenistujate arv alla seaduses sätestatud piirmäära. Samas peab igal juhul olema tagatud võimalus pöörduda rikkumisega asutusevälise pädeva asutuse poole.

Erasektoris on sisemise teavituskanali loomine kohustuslik juriidilistele isikutele, kus töötab vähemalt 50 töötajat. Teatud tegevusvaldkondades, eelkõige finantssektoris, võib kohustus tuleneda eriregulatsioonist sõltumata töötajate arvust. Väiksematel ettevõtjatel seadusest tulenevat üldist kohustust sisemist kanalit luua ei ole, kuid neil peab samuti olema võimalus pöörduda otse pädeva asutuse poole.

Sisemised teavituskanalid peavad võimaldama teadete esitamist nii kirjalikult kui ka suuliselt. Tagatud peab olema konfidentsiaalsus: vihjeandja isik ja teate sisu tuleb kaitsta ning juurdepääs piirata üksnes menetlusega seotud isikutega. Seadus sätestab ka menetlustähtajad — teate kättesaamine tuleb kinnitada seitsme päeva jooksul ning teavitajale tuleb anda tagasisidet hiljemalt kolme kuu jooksul alates teate saamisest.

2.3. Välised teavituskanalid ja pädevad asutused

Eestis ei ole loodud ühte keskset asutust, kuhu kõik vihjed koonduksid. Selle asemel toimib detsentraliseeritud süsteem, kus rikkumistest saab teatada erinevatele

pädevatele asutustele sõltuvalt rikkumise valdkonnast. Näiteks keskkonnaga seotud rikkumiste puhul on pädevaks asutuseks Keskkonnaamet, finantsvaldkonnas Finantsinspektsioon, tarbijakaitse või tooteohutuse teemadel Tarbijakaitse ja Tehnilise Järelevalve Amet. Valdkondades, kus järelevalvepädevus on kohalikul omavalitsusel (näiteks kasutus- ja ehitusload, jäätmehooldus jne), tuleks pöörduda nende poole.

Selline süsteem võimaldab kasutada asutuste olemasolevaid teadmisi ja pädevust. Samas tähendab see ka seda, et vihjeandja peab ise teadma või välja selgitama, milline asutus on konkreetse rikkumise puhul õigem, mis ei pruugi alati olla väga lihtne. Justiitsministeeriumil on vihjeandmise regulatsiooni üldine koordineeriv roll, kuid ta ei menetle üksikjuhtumeid ega teosta järelevalvet asutuste üle vihjeandjate kaitse küsimustes.

2.4. Kaitse kättemaksu eest

Seadus keelab igasuguse kättemaksu vihjeandja suhtes. Kättemaksuna käsitatakse mis tahes põhjendamatut ebasoodsat meedet, mis on seotud vihjeandmisega, näiteks vallandamist, töötingimuste halvendamist, ähvardusi või survet.

Kui vaidlus jõuab kohtusse, ei pea vihjeandja tõendama, et kahjulik meede rakendati just vihjeandmise tõttu. Piisab sellest, kui ta näitab, et ta andis rikkumisest teada ja et tema olukord pärast seda halvenes. Seejärel peab tööandja selgitama ja tõendama, et tema tegevus ei olnud seotud vihjeandmisega ning oli muul põhjusel põhjendatud.

Seadus näeb ette ka karistused juhtudel, kus vihjeandmist takistatakse, rikutakse konfidentsiaalsust või rakendatakse kättemaksu. Samas ei ole seaduses eraldi sätestatud karistusi olukordadeks, kus asutus jätab vihjeandmise kanali loomata või ei täida seaduses ette nähtud menetlustähtaegu. Samuti ei näe Eesti seadus ette hüvitisi survemeetmete ohvriks langenud isikutele.

2.5. Järelevalve ja tuvastatud lüngad

Eesti õigusraamistik ei näe ette ühtset sõltumatut asutust, kelle ülesanne oleks vihjeandjate kaitse süsteemi terviklik järelevalve. Samuti puudub kohustus koguda ja avaldada regulaarselt andmeid selle kohta, kui palju vihjeid esitatakse, milliseid teemasid need puudutavad ja milliste tulemusteni need viivad.

Kuigi seadus vastab direktiivi põhinõuetele, on mitmeid aspekte, mis võivad rakendamist keerulisemaks muuta. Nende hulka kuuluvad näiteks seaduse piiratud kohaldamisala, tegeliku õiguskaitse ja hüvitiste vähene reguleeritus ning keskse järelevalve ja andmekogumise puudumine. Need küsimused mõjutavad otseselt seda, kui selge, kättesaadav ja usaldusväärne on vihjeandmise süsteem praktikas nii asutuste kui ka võimalike vihjeandjate jaoks.

Kuigi Eesti seadus vastab direktiivi miinimumnõuetele, on selle rakendamine keeruline.

3. Teavituskanalite korraldus ja koostöö väliste osapooltega

Intervjuudest nähtub, et teavituskanalite korraldus erineb Eestis märkimisväärselt sõltuvalt asutuse suurusest, tüübist ja organisatsioonilisest ülesehitusest. Ühist mudelit ei ole, kuid mitmed lahendused ja praktikad korduvad erinevates asutustes ning annavad hea ülevaate sellest, kuidas vihjeandmise süsteeme praktikas korraldatakse.

3.1. Teadete vastuvõtt, menetlemine ja sõltumatuse tagamine

Valdavas osas intervjueeritud asutustest on vihjete vastuvõtmine ja menetlemine usaldatud siseauditi või sisekontrolli funktsioonile. Siseaudiitoreid nähakse organisatsioonis suhteliselt sõltumatute ja professionaalsete osapooltena, kes alluvad sageli otse asutuse tippjuhtkonnale (näiteks kantslerile, omavalitsuse juhile või auditikomiteele). See aruandlusliin on intervjueeritavate hinnangul üks peamisi sõltumatuse tagatisi.

Väiksemates asutustes ja kohalikes omavalitsustes, kus siseaudiitor puudub, on vihjete menetlemine sageli jaotatud teiste rollide vahel, näiteks vallasekretäri, kvaliteedijuhi või juristi ülesandeks. Sellistes olukordades rõhutati vajadust selgete rollijaotuste ja kokkulepete järele, et vältida huvide konflikte.

Sõltumatuse ja objektiivsuse tugevdamiseks kasutatakse mitmes asutuses nelja silma printsiipi, mille kohaselt tegeleb vihjetega vähemalt kaks isikut või vajavad olulised otsused teise menetleja kinnitust. Samuti on levinud praktika, et kui vihje puudutab allasutuse juhti või muud kõrget ametnikku, ei menetle juhtumit sama allasutus, vaid see suunatakse kõrgemalseisvale kesksele asutusele.

Mõnes organisatsioonis on teavituskanali haldamine ja menetlemine koondatud ühe konkreetse isiku kätte (nt siseaudiitor), kes võtab teated vastu, hindab nende vastavust seaduse kohaldamisalale, viib läbi menetluse ning vastutab ka vihjeandja kaitse tagamise eest. Selline lahendus võimaldab maksimeerida konfidentsiaalsust (nt ligipääs spetsiaalsele e-posti aadressile on vaid ühel isikul), kuid muudab süsteemi selgelt isikupõhiseks ning võib tekitada küsimusi asendatavuse ja töö järjepidevuse osas.

> *„Usaldust teenitakse aastaid, kuid kaotatakse hetkega.“*
>
> *- Kogenud siseauditi juht (intervjuu 12)*

Intervjueeritavad tõid ühtlasi esile, et tõsisemad rikkumised ei jõua sageli menetlejateni ametliku vihjekanali kaudu, vaid otsesuhtluse teel. Töötajate valmisolek rikkumistest teada anda sõltub suurel määral sellest, keda nad peavad usaldusväärseks. Seetõttu rõhutati korduvalt, et menetleja peab olema sõltumatu, professionaalne ja piisavalt julge keeruliste teemade käsitlemiseks.

Ministeeriumide tasandil on välja kujunenud ka tsentraalsed lahendused, kus ministeeriumi siseaudit haldab vihjeandmise kanalit mitte ainult ministeeriumi enda, vaid ka mitmete hallatavate asutuste jaoks. Seda peeti tõhusaks viisiks vähendada väiksemate asutuste halduskoormust ning tagada ühtlasem ja professionaalsem menetluspraktika.

3.2. Kirjalikud menetlused ja tehnilised lahendused

Enamikus intervjueeritud asutustes on vihjeandmise korraldus reguleeritud kirjalike dokumentidega, nagu käskkirjad, eeskirjad või menetlusjuhendid. Need määratlevad, kuidas vihjeid vastu võetakse, kes neid menetleb ja millised on menetluse etapid. Samas toodi esile, et mõnes väiksemas asutuses või kohaliku omavalitsuse üksuses tuginetakse pigem väljakujunenud tavale ja suulistele kokkulepetele ning eraldi kirjalikku dokumenti ei peeta asutuse väiksuse tõttu vajalikuks.

Tehniliste lahenduste osas jagunevad kasutatavad praktikad intervjuude põhjal kolme peamisse rühma.
Esiteks kasutavad mõned suuremad organisatsioonid (näiteks rahvusvaheliste kontsernide osad või ülikoolid) väliseid spetsiaalseid vihjeandmise platvorme, mida peetakse kõige turvalisemaks ja anonüümsust toetavamaks lahenduseks. Eriti hinnatakse võimalust pidada vihjeandjaga anonüümset kahepoolset dialoogi ning täiendavaid tehnilisi lahendusi, nagu hääle moonutamine.

Teiseks on avalikus sektoris levinud asutusesisesed veebivormid või infosüsteemid, mis on sageli integreeritud dokumendihaldussüsteemiga (näiteks SharePointi-põhised lahendused). Need võimaldavad suhteliselt lihtsat haldamist, kuid anonüümsuse tase sõltub konkreetsest tehnilisest seadistusest.

Kolmandaks kasutatakse väiksemates üksustes lihtsamaid lahendusi, nagu eraldi e-posti aadressid või veebipõhised ankeedid, mis on seadistatud nii, et saatja andmeid ei salvestata. Intervjueeritavate hinnangul täidavad need lahendused miinimumnõudeid, kuid ei pruugi pakkuda sama usaldusväärsust kui spetsiaalsed platvormid.

3.3. Koostöö väliste osapooltega ja juhtumite suunamine

Koostöö väliste osapooltega on intervjuude põhjal pigem piiratud ja erandlik. Enamasti püütakse vihjejuhtumid lahendada organisatsiooni sees. Mõned intervjueeritavad tõid ka välja, et kui vihje puudutab allasutust, edastatakse see vastava asutuse juhile või menetlejale kas krüpteeritult või eelnevalt kohandatuna, eemaldades võimaluse korral detailid, mis võiksid vihjeandja isikut otseselt või kaudselt tuvastada.

Sihtasutuse vormis tegutsevate organisatsioonide puhul joonistus välja ka omaniku (nt kohaliku omavalitsuse) roll võimaliku välise eskalatsioonikanalina. Kui teavitaja ei ole asutusesisese lahendusega rahul, on tal võimalik pöörduda omaniku poole subordinatsiooni korras. Selline lahendus ei ole klassikaline järelevalveasutuse poole pöördumine, kuid toimib institutsionaalse kontrollimehhanismina.

Õiguskaitseorganite kaasamist peetakse viimaseks abinõuks ning seda kasutatakse peamiselt juhul, kui ilmnevad selged kuriteo tunnused, näiteks korruptsiooni või varguse kahtlus. Mõnel juhul mainiti ka võimalust suunata teateid järelevalveasutustele, nagu Tööinspektsioon või Finantsinspektsioon, kui asutusesisene lahendus ei ole võimalik või ei anna tulemusi.

Väliste teenusepakkujatega tehakse koostööd peamiselt tehnilisel tasandil, näiteks IT-platvormide haldamisel. Sisulist vihjete menetlemist või uurimist väljast sisse ei osteta ning kodanikuühiskonna organisatsioonide või ametiühingute roll vihjete käsitlemisel jäi intervjuude põhjal marginaalseks.

3.4. Koostööd soodustavad ja takistavad tegurid

Intervjueeritavad tõid esile mitmeid tegureid, mis mõjutavad teavituskanalite toimimist ja koostööd. Koostööd soodustavad eelkõige tsentraalsed lahendused, kus suurem asutus pakub vihjeandmise kanalit ja menetlusvõimekust ka väiksematele üksustele. Samuti peetakse oluliseks head tehnilist võimekust, eriti lahendusi, mis võimaldavad anonüümset suhtlust vihjeandjaga menetluse käigus.

Takistusena mainiti ka allasutuste suletud organisatsioonikultuuri – probleeme eelistatakse lahendada majasiseselt ning välditakse info edastamist kesksele siseauditile. Väikestes kollektiivides toodi esile ka anonüümsuse praktiline haprus – isegi kui nimi ei ole teada, võib vihjeandja isik olla kaudselt tuletatav, mis vähendab valmisolekut infot jagada.

Lisaks mainiti segadust pädevuste osas. Mõnel juhul ei ole töötajatel selget arusaama sellest, kuhu vihje tegelikult jõuab ja kes seda menetleb, mis võib teavitamist ja koostööd oluliselt pärssida. Sellist probleemi aitab ennetada selgete kirjalike juhiste olemasolu, mis kirjeldavad läbipaistvalt kanali toimimist, menetlusprotsessi ning vastutavate isikute rolli. Kui töötajatele on arusaadav, kuidas vihjekanal toimib ja millised tagatised on kehtestatud, suureneb ka valmisolek süsteemi kasutada.

3.5 Kanalite paljusus ja killustumine

Ilmnes, et juba enne EL direktiivi rakendamist võis organisatsioonides olla kasutusel erinevaid vihjete esitamise kanaleid. Direktiivi ülevõtmise käigus kaaluti täiendava sisemise teavituskanali loomist tööalastest rikkumistest teavitamiseks, mis tõstatas küsimusi võimaliku dubleerimise ja ressursside otstarbeka kasutamise kohta. Ühes suuremas kohalikus omavalitsuses kerkis esile ka küsimus, kui palju paralleelseid kanaleid on mõistlik üleval pidada ning kas liigne killustatus võib vähendada süsteemi selgust ja kasutajasõbralikkust.

Mõnes organisatsioonis kerkis esile küsimus, kui palju erinevaid kanaleid on mõistlik üleval pidada.

Spetsiifilistes sektorites (nt meditsiin, finants, transport) toimivad lisaks ka valdkonnapõhised teavitusliinid (nt ravikvaliteet, lennundusohutus, kliendikaebused, töökeskkond). Tegemist ei ole otsese dubleerimisega, vaid funktsionaalse eristumisega. Praktikas tähendab see siiski, et osa rikkumisteabest liigub alternatiivsete kanalite kaudu ega kajastu vihjekanali statistikas. Menetleja rolliks kujuneb esmane „liikluskorraldus“ – hinnata, kas teade kvalifitseerub tööalaseks rikkumiseks või kuulub mõne muu menetlusraamistiku alla.

Väga levinud on olukord, kus formaalne IT-platvorm või veebivorm on küll olemas, kuid töötajad eelistavad pöörduda otse usaldusväärse isiku poole (nt siseaudiitori või sisekontrolöri töömeilile või telefoni teel). Selline praktika ei vähenda menetleja töö sisu, kuid muudab info haldamise keerulisemaks – konfidentsiaalsuse tagamine, dokumenteerimine ja statistika koondamine jäävad menetleja individuaalse vastutuse alla.

Sageli eelistavad töötajad formaalsele IT-platvormile otsesuhtlust usaldusväärse isikuga (nt siseaudiitoriga). See ei muuda menetluse sisu, kuid muudab info dokumenteerimise ja koondamise keerulisemaks. Mitme paralleelse pöördumisvõimaluse korral (juht, HR, siseaudit, väline platvorm) on vajalik keskne ülevaade, et vältida info hajumist.

Kanalite paljusus ei ole iseenesest probleem, kuid see tekitab praktilisi väljakutseid: statistika killustumist, läbipaistvuse vähenemist ja menetleja koordineerimisrolli suurenemist. Samas võib valdkonnapõhine diferentseerimine vähendada üldkanali koormust ja suunata spetsiifilised juhtumid kiiremini pädevasse menetlusse. Mõju sõltub sellest, kas organisatsioon suudab erinevad teavitusliinid tervikuks siduda.

4. Teadete arv, teemad ja tulemused

Käesolevas aruandes esitatud ülevaade põhineb intervjueeritud asutuste siseinfol ja hinnangutel. Eestis ei ole kättesaadavat koondatud riikliku tasandi statistikat vihjeandmise kanalite kasutamise kohta, mistõttu ei ole võimalik anda terviklikku ülevaadet teadete arvust või teemadest. Alljärgnevad tähelepanekud kajastavad seega praktikat nendes asutustes, kus intervjuud läbi viidi.

4.1 Kanalite kujunemisaeg ja küpsusaste

Intervjuude põhjal varieerub vihjekanalite vanus märkimisväärselt. Kõige pikema kogemusega on rahvusvahelised kontsernid ja mõned suuremad organisatsioonid, kus sarnastel põhimõtetel toimiv süsteem on olnud kasutusel juba üle kümne aasta ning menetluspraktika on ajas välja kujunenud. Samuti leidub asutusi, kus kanal on toiminud 3-5 aastat ning kus statistika pidamine ja protsessid on järk-järgult stabiliseerunud.

Enamik avaliku sektori asutusi on aga loonud või uuendanud oma kanali viimase 1-2 aasta jooksul seoses uue seaduse ja EL direktiivi nõuetega. Mitmed kanalid on olnud

kasutusel vaid mõne kuu kuni ühe aasta, mistõttu on nende praktika alles kujunemisjärgus. Samuti esineb eristuvaid lahendusi: mõnes väikeses omavalitsuses ei ole eraldi kanalit loodud ning tuginetakse varasemale avatud suhtluse praktikale, teistes on olemasolev rikkumiste vastuvõtmine formaliseeritud uue e-posti aadressi või veebivormina.

Kokkuvõttes peegeldab kanalite vanus organisatsioonide erinevat küpsusastet: osa süsteeme on institutsionaalselt juurdunud, samas kui paljud alles kohanevad uute regulatiivsete nõuetega.

4.2. Teadete arv ja kasutusaktiivsus

Läbiviidud intervjuudele tuginedes on teavituskanalite kasutusaktiivsus ja statistika pidamine väga ebaühtlane. Registreeritud teadete arv varieerub nullist kuni paarikümne teateni aastas, sõltudes organisatsiooni suurusest ning sellest, mida konkreetne asutus „teatena“ arvesse võtab.

Mitmes asutuses ei ole laekunud ühtegi sisulist tööalast rikkumist puudutavat teadet, kuigi kanal on olnud avatud üle aasta. Kanalitesse on jõudnud üksikuid ekslikke pöördumisi või rämpskirju, mida sisuliste teadetena ei käsitleta. Samuti esines juhtumeid, kus ainus laekunud teade ei kvalifitseerunud seaduse kohaldamisalasse või osutus kliendikaebuseks.

Suuremates organisatsioonides jääb registreeritud teadete arv tavaliselt vahemikku 10-20 aastas. Samas sisaldavad need numbrid sageli väga erineva sisuga pöördumisi. Paljud asutused arvestavad statistika hulka kõik kanalisse laekunud teated, sõltumata nende sisust, samas kui teised kajastavad ametlikult vaid menetlusse võetud potentsiaalseid rikkumisi. Mõnes asutuses hinnati, et tõsiseks seaduserikkumiseks, korruptsiooniks, pettuseks või tööalaseks väärkäitumiseks kvalifitseerub vaid 10-20% laekunud teadetest.

Seetõttu on asutustevaheline võrdlus keeruline ning suuremad numbrid ei tähenda tingimata suuremat korruptsiooniriski. Intervjuud viitavad, et reaalseid tööalaseid rikkumisi puudutavaid teateid esineb Eestis pigem harva ning vihjekanalid toimivad sageli ka üldise kaebe- ja tagasisidemehhanismina.

4.3. Teadete teemad

Intervjuude põhjal saab vihjekanalitesse laekuvad teated sisuliselt jagada kolme peamisse kategooriasse. Üldine tendents näitab, et klassikalisi seadusest tulenevaid

rikkumisi (nt finantspettused, keskkonnaalased rikkumised või tõsised korruptsioonijuhtumid) esineb harva. Domineerivad töökeskkonna ja inimsuhetega seotud probleemid ning erinevad olmelised või asjassepuutumatud pöördumised.

Tõsiseid seaduserikkumisi puudutavaid teateid esines intervjueeritud asutustes pigem harva.

Kõige sagedamini teavitatakse töökeskkonna pingetest, töökiusamisest, ebavõrdsest kohtlemisest ning juhtimisprobleemidest. Kaebused puudutavad nii kolleegidevahelisi konflikte kui ka juhtimisstiili, ametnike ebaviisakat käitumist või vastamata kirju. Intervjueeritavate hinnangul peegeldab see asjaolu, et vihjekanalit kasutatakse sageli üldise sisekliima „ventiilina".

Märkimisväärne osa teadetest kvalifitseerub nn „müraks". Nende hulka kuuluvad olmeprobleemid (nt katkised valgustid, logisevad toolid, taristumured), tehnilised rikked, isiklikud konfliktid või eksikombel saadetud päringud. Mõnes sektoris, näiteks meditsiinis või finantsvaldkonnas, aetakse vihjekanal sageli segi kliendikaebuste mehhanismiga ning sinna esitatakse ravikvaliteedi või teenindusega seotud pöördumisi.

Sisulisi tööalaseid rikkumisi käsitlevaid teateid esineb harvem, kuid need on menetlejate jaoks kõige olulisemad. Need puudutavad eelkõige huvide konflikte, kõrvaltegevusi, vara võimalikku väärkasutust ning hankemenetluste küsimusi. Mõnes valdkonnas toodi esile ka spetsiifilisi regulatiivseid rikkumisi, näiteks rahapesu tõkestamise nõuete ebapiisavat täitmist. Samas rõhutati, et esialgsed kahtlused ei pruugi kontrollimisel tõendamist leida ning osa juhtumeid osutub väheoluliseteks vigadeks või arusaamatusteks.

Kokkuvõttes näitavad intervjuud, et kuigi vihjekanalid on loodud eelkõige tõsiste rikkumiste avastamiseks, kasutatakse neid praktikas sageli laiemalt tööalaste ja organisatsiooniliste probleemide väljendamiseks. Tõsiseid seaduserikkumisi puudutavaid teateid esines intervjueeritud asutustes pigem harva.

4.4. Tüüpiline menetlusprotsess ja ajakava

Menetlusprotsess on intervjueeritud asutustes üldjoontes sarnane ning enamasti reguleeritud sisemiste kordade ja juhenditega. Tavapärane protsess koosneb mitmest etapist.

Esmalt saadetakse teavitajale kinnitus teate kättesaamise kohta, üldjuhul seitsme päeva jooksul. Seejärel viiakse läbi esmane kontroll ja analüüs, mida teevad tavaliselt siseauditi või vastavuskontrolli töötajad. Sageli on menetlusse kaasatud kaks kuni kolm isikut ning rakendatakse nelja silma printsiipi, et vähendada subjektiivsuse riski.

Kui teade puudutab allasutust või konkreetset struktuuriüksust, suunatakse see edasiseks lahendamiseks vastavale juhile või menetlejale. Seda tehakse võimaluse korral krüpteeritult või eelnevalt kohandatuna, eemaldades detailid, mis võiksid vihjeandja isikut tuvastada. Tõsisemate kahtluste korral viiakse läbi põhjalikum uurimine. Vihjeandja kaitsmiseks „maskeeritakse“ kontrolltoimingud mõnikord tavapäraste auditite või rutiinsete kontrollidena, et vältida infoallika avalikuks tulekut.

Menetluse käigus antakse teavitajale tagasisidet. Tähtajad varieeruvad, jäädes tavaliselt vahemikku 30 päeva kuni kolm kuud. Anonüümsete teadete puhul on tagasiside võimalik ainult siis, kui kasutatav IT-platvorm võimaldab turvalist ja anonüümset suhtlust.

4.5. Menetluste tulemused

Menetluste tulemused on intervjuude põhjal valdavalt mittekaristuslikud. Paljudel juhtudel selgub menetluse käigus, et rikkumist ei ole toimunud ning probleem tulenes pigem kommunikatsioonihäirest või erinevatest ootustest.

Kõige sagedasemaks tulemuseks on parandusmeetmete rakendamine, näiteks tööprotsesside korrigeerimine, sisekorra täiendamine, juhendite täpsustamine või koolituste korraldamine. Töökeskkonna ja inimsuhetega seotud juhtumite puhul kasutatakse sageli vestlusi ja vahendusmeetmeid.

Distsiplinaarmeetmed, sealhulgas töösuhte lõpetamine või kriminaalmenetluse algatamine, on harvad. Intervjueeritavate hinnangul pärinevad sellised juhtumid sagedamini mitte ametliku vihjeandmise kanali kaudu saadud teadetest, vaid otsestest vihjetest või muul viisil esile kerkinud asjaoludest.

4.6. Erinevused asutuste lõikes

Intervjuud kinnitavad, et nii menetlusprotsessi kui ka tulemusi mõjutavad oluliselt asutuse suurus ja võimekus. Suuremates organisatsioonides ja rahvusvahelistes kontsernides on kasutusel välised IT-platvormid, mis võimaldavad anonüümset dialoogi ja pakuvad paremaid tehnilisi lahendusi vihjeandja kaitseks. Väiksemates

asutustes ja kohalikes omavalitsustes kasutatakse sagedamini lihtsamaid lahendusi, nagu e-post, veebivormid või dokumendihaldussüsteemid.

Samuti erineb menetlusvõimekus. Suurtes asutustes on vihjete menetlemine siseauditi tavapärane tööosa, samas kui väiksemates üksustes tehakse seda sageli muude ülesannete kõrvalt, mis võib mõjutada menetluse kiirust ja põhjalikkust. Mõnes valdkonnas on kasutusele võetud tsentraliseeritud mudelid, kus ministeerium haldab vihjeandmise süsteemi ka oma allasutuste jaoks, vähendades viimaste halduskoormust ja ühtlustades praktikat.

5. Vihjeandjate kaitsemeetmed ja tugi

Intervjuudest ilmneb, et vihjeandjate kaitse tugineb Eestis eelkõige konfidentsiaalsuse tagamisele ning menetlejate professionaalsele ja ettevaatlikule tegutsemisele. Formaalsete ja eraldi struktureeritud kaitse- või tugimehhanismide roll on seevastu piiratud ning praktikas toetutakse sageli üldistele personalipoliitikatele ja mitteformaalsetele lahendustele. Olukorras, kus selged formaalsed mehhanismid puuduvad või neist mööda minnakse, muutub vihjeandja haavatavaks. See on eriti kriitiline tõsiste rikkumiste puhul, mida küll esineb harva, kuid mille tagajärjeks võib olla vihjeandja kiusamine, isolatsioon või juhtumi kinnimätsimine.

5.1. Konfidentsiaalsuse praktilised tagatised

Konfidentsiaalsuse tagamist peetakse intervjuude põhjal kõige olulisemaks ja tõhusamaks vihjeandjate kaitsemeetmeks. Praktikas kasutatakse selleks nii tehnilisi kui ka menetluslikke lahendusi.

Valdavas osas asutustest on ligipääs vihjeandmise kanalite kaudu saadud infole rangelt piiratud, olles kättesaadav vaid väga kitsale ringile, tavaliselt ühele kuni kolmele isikule. Enamasti on nendeks siseauditi juht, riskijuht või vastavuskontrolli eest vastutav töötaja. Samas tuuakse mitmes intervjuus välja, et dokumendihaldussüsteemide praktiline turvalisus ei ole alati absoluutne: isegi piiratud ligipääsudega kasutadesse võivad tehniliselt ligi pääseda administraatorid või peakasutajad. Selliste riskide maandamiseks on kasutusel logide jälgimine (volitatud juurdepääsust kõrvalekalded käsitletakse töökohustuste rikkumisena) ning pseudonüümimise praktikad (nt ainult initsiaalide või anonüümsete märgetega salvestamine).

Tehniliste meetmete osas kasutavad suuremad organisatsioonid ja rahvusvahelised kontsernid väliseid spetsiaalseid platvorme, mis ei salvesta IP-aadresse, krüpteerivad andmeid ning võimaldavad anonüümset suhtlust, sealhulgas hääle moonutamist. Riigiasutused ja väiksemad üksused tuginevad sagedamini asutusesisestele lahendustele, nagu piiratud ligipääsuga dokumendihaldussüsteemid või krüpteeritud e-post.

Olulise praktilise kaitsemeetmena toodi mitmes intervjuus esile ka nn menetlustaktika „maskeerimine“. Selle käigus kontrollitakse vihjes toodud infot näiteks plaanilise auditi või rutiinse kontrolli kaudu, et mitte jätta uuritavale muljet, nagu oleks menetlus alguse saanud konkreetsest vihjest. Intervjueeritavate hinnangul on see üks tõhusamaid viise vihjeandja kaitsmiseks.

Samas toodi intervjuudes välja ka vastupidiseid näiteid, kus asutuse vihjeandmise korras on läbipaistvuse huvides sätestatud, et menetluse lõppedes teavitatakse vihje saabumisest isikuid, keda see oluliselt puudutab, eelkõige neid, kelle kohta vihje esitati. Teavitamisest loobutakse erandlikel juhtudel. Intervjueeritavate hinnangul aitab selline lähenemine vältida arusaama „varjatud toimikute“ kogumisest. Samal ajal võib see suurendada riske vihjeandja konfidentsiaalsuse tagamisel, eriti väiksemates kollektiivides, kus isegi piiratud teave võib võimaldada vihjeandja isiku kaudset tuvastamist.

Lisaks kasutatakse info filtreerimist ja kohandamist. Kui juhtum vajab edasist menetlemist teises osakonnas või allasutuses, edastatakse teave sageli ümber sõnastatuna või detailidest „puhastatuna“, et vältida vihjeandja isiku tuvastamist tema väljendusviisi, ajastuse või spetsiifiliste viidete kaudu.

5.2. Anonüümsete teadete käsitlemine

Kõik intervjueeritud asutused aktsepteerivad anonüümseid teateid, kuid nende menetlemise praktiline võimekus varieerub oluliselt. Peamine erinevus seisneb selles, kas ja kuidas on võimalik vihjeandjaga edaspidi suhelda.

Spetsiaalsete IT-platvormide kaudu on võimalik küsida täpsustavaid küsimusi vihjeandja isikut paljastamata.

Asutustes, mis kasutavad spetsiaalseid IT-platvorme, on võimalik pidada anonüümset kahepoolset dialoogi turvalise postkasti kaudu. Seda peeti menetluse edukuse seisukohalt kriitiliseks, kuna see võimaldab esitada täpsustavaid küsimusi ja saada lisainfot ilma vihjeandja isikut paljastamata.

Lihtsamate veebivormide, anonüümsete e-kirjade või kirjalike pöördumiste puhul puudub sageli võimalus teavitajale vastata või anda tagasisidet menetluse käigu ja tulemuste kohta. See piirab menetluse sügavust ning võib viia juhtumi lõpetamiseni ebapiisava info tõttu.

Mõnes asutuses on anonüümsete teadete osas uurimise alustamise otsustusõigus viidud juhatuse tasandile, sest piiratud informatsiooni tingimustes peetakse vajalikuks kollegiaalset riski- ja olulisushinnangut.

Samuti mainisid mõned intervjueeritavad, et lähtuvad põhimõttest, et anonüümsuse säilitamine on olulisem kui menetluse lõpuleviimine. Kui uurimise jätkamine tooks kaasa anonüümse vihjeandja isiku paljastamise, võidakse loobuda konkreetse juhtumi menetlemisest ning käsitleda probleemi laiemalt, näiteks üldiste koolituste või protsessimuudatuste kaudu.

5.3. Meetmed kättemaksu ennetamiseks ja sellele reageerimiseks

Peamine kättemaksu ennetamise meede on intervjuude põhjal samuti konfidentsiaalsus. Loogika on lihtne: kui vihjeandja isik ei ole teada, ei ole võimalik talle ka kätte maksta.

Väiksemates kollektiivides on vihjeandjat sageli võimalik kaudselt tuvastada.

Suuremates asutustes toetavad seda nelja silma printsiip ning huvide konflikti vältimise reeglid, mis vähendavad riski, et menetleja tegutseb kallutatult või avaldab infot sobimatult. Samas tunnistati mitmes intervjuus, et väikestes kollektiivides või väga spetsiifiliste juhtumite korral on vihjeandja isik sageli kaudselt tuletatav, hoolimata kõigist ettevaatusmeetmetest. Väikeses omavalitsuses lisandub tööalase kättemaksu hirmule ka hirm sotsiaalse tõrjutuse ees (naabrid/kogukond).

Otseseid ja formaalseid protseduure kättemaksujuhtumitele reageerimiseks peale üldise tööõiguse normide enamasti ei ole. Kui siiski tuvastatakse tagakiusamine või ebasoodne kohtlemine, ollakse valmis sekkuma mitteformaalsete meetmete kaudu, näiteks vestluste, vahendamise või vajaduse korral distsiplinaarmeetmete rakendamisega.

5.4. Raporteeritud kogemused kättemaksuga

Valdav enamik intervjueeritavaid kinnitas, et nad ei ole oma praktikas kokku puutunud otseste ja selgelt tuvastatavate kättemaksujuhtumitega. Samas mainiti üksikuid olukordi, kus konfliktid pärast teavitamist süvenesid või kus vihjeandja lahkus organisatsioonist kas omal soovil või koondamise teel.

Kuigi konkreetseid juhtumeid intervjueeritavad välja ei toonud, on hirm kättemaksu ees intervjuude põhjal läbiv teema. Just see hirm on üks peamisi põhjuseid, miks töötajad eelistavad anonüümsust või otsesuhtlust usaldusisikutega ametlike kanalite asemel.

Kuigi otseseid juhtumeid intervjuudes välja ei toodud, on hirm kättemaksu ees läbiv teema.

Intervjuudest ilmneb siiski, et kättemaksuvastane kaitse ei paku vihjeandjatele alati piisavat õiguskindlust. Kirjeldati juhtumeid, kus vihjeandjad lahkusid organisatsioonist koondamise või muude formaalselt põhjendatud meetmete kaudu ka siis, kui vihje osutus sisuliselt põhjendatuks. Samuti möönsid intervjueeritavad, et nad ei vii läbi süsteemset järelkontrolli võimaliku kättemaksu tuvastamiseks, mistõttu tugineb kaitse pigem üksikute menetlejate tähelepanelikkusele kui läbimõeldud ja ühtsele süsteemile.

5.5. Kättemaksu tuvastamise seiremehhanismid

Süstemaatilisi ja formaalseid seiremehhanisme kättemaksu tuvastamiseks intervjuude põhjal enamasti ei kasutata. Näiteks ei ole tavapärane automaatne järelkontroll teatud aja möödudes pärast menetluse lõppu.

Jälgimine toimub pigem mitteformaalselt ja inimlikul tasandil. Tundlikemate juhtumite puhul, eriti töökiusuga seotud teemades, hoiavad menetlejad olukorral silma peal, suhtlevad vihjeandjaga pärast menetluse lõppu või paluvad tal ise märku anda, kui olukord peaks halvenema.

5.6. Tugimeetmete kättesaadavus

Spetsiaalselt vihjeandjatele suunatud tugipakette intervjuude põhjal üldjuhul ei ole. Tugimeetmete pakkumisel tuginetakse eelkõige organisatsiooni üldistele töötajatele mõeldud hüvedele.

Kõige kättesaadavamaks toetusvormiks on psühholoogiline tugi. Paljudes organisatsioonides on töötajatel võimalus kasutada psühholoogi teenust töötervishoiu, tervisetoetuste platvormide või lepinguliste partnerite kaudu ning see võimalus laieneb ka vihjeandjatele.

Organisatsioonipoolset tasuta õigusabi vihjeandjatele üldjuhul ei pakuta. Mõnel juhul on sisejurist või menetleja andnud praktilist nõu, kuid seda peeti pigem erandlikuks ja mitteformaalseks. Riigi õigusabi võimalustest ollakse teadlikud, kuid intervjuude põhjal ei ole praktikas vajadust nende kasutamiseks tekkinud.

Olulise toetusena tõsteti esile menetleja rolli, keda nähakse sageli mitte üksnes formaalse uurijana, vaid ka usaldusliku ärakuulaja ja nõustajana. See, et inimesed eelistavad tihti pöörduda otse usaldusisikute poole, rõhutab menetleja tähtsust toetava ja turvalise kontaktina. Seetõttu ei piisa üksnes tehnilisest konfidentsiaalsusest — sama oluline on, et menetleja oleks koolitatud, kättesaadav ning suudaks suhelda diskreetselt ja toetavalt. Just selline professionaalne ja inimlik lähenemine aitab maandada pingeid ning suurendab tõenäosust, et tõsisemad rikkumised jõuavad avalikuks ega jää varju.

6. Väljakutsed ja tugevused

Intervjuudest joonistusid selgelt välja nii peamised takistused kui ka toimivad praktikad, mis mõjutavad vihjeandmise süsteemide rakendamist Eestis. Mitmed väljakutsed on seotud laiemate kultuuriliste ja organisatsiooniliste hoiakutega, samas kui tugevused tulenevad eelkõige teadlikest menetlusvalikutest, tehnilistest lahendustest ja juhtkonna rollist.

6.1. Peamised väljakutsed

Ajalooline ja kultuuriline taust. Rikkumistest teavitamist seostatakse endiselt negatiivse „pealekaebamisega“. Intervjueeritavad viitasid nn totalitarismi või „nõukogude kultuuri“ pärandile, mille mõju on küll ajas vähenemas, kuid püsib eriti vanema põlvkonna ja teatud asutuste puhul. Nooremate töötajate seas nähakse vihjeandmist üha enam tavapärase osana organisatsioonikultuurist, kuid üldine hoiak ei ole veel ühtlaselt muutunud.

Vihjeandmist seostatakse endiselt pealekaebamisega.

Anonüümsuse praktiline haprus väikestes kollektiivides. Kuigi tehnilised ja menetluslikud meetmed võivad olla korrektselt rakendatud, on vihjeandja isik väikestes kogukondades või väga spetsiifiliste probleemide korral sageli kaudselt tuletatav. See tekitab hirmu sotsiaalse tõrjutuse või varjatud kättemaksu ees ning vähendab valmisolekut vihjekanaleid kasutada.

Seaduse kohaldamisala ja töötajate tegelike kogemuste vaheline vastuolu. Kuigi töötajad võivad praktikas anda teada ka Eesti siseriiklike õigusnormide rikkumistest, ei pruugi selliste teadete puhul vihjeandjatele seadusest tulenev kaitse kohalduda. Kehtiv õigusraamistik keskendub eelkõige Euroopa Liidu õiguse rikkumistele ning annab kaitse näiteks riigihangete, keskkonnakaitse või finantsteenustega seotud vihjete esitajatele. Samas puudutavad tegelikud probleemid sagedamini siseriiklikke teemasid nagu pettused, vargused, vara omastamine, töövägivald või huvide konflikt. Intervjueeritavate hinnangul jätab see töötajatele mulje, et kaitse on ette nähtud pigem teoreetiliste või nende asutuse jaoks ebaoluliste rikkumiste puhul, samal ajal kui tõsistest ja igapäevastest probleemidest teavitamine ei pruugi olla kaitstud. See omakorda muudab süsteemi raskesti mõistetavaks ja vähendab usaldust vihjeandmise mehhanismide vastu.

Rakendusliku toe ja juhendamise puudumine vihjekanalite haldajatele. Kuigi menetlejad tegutsevad üldjuhul heas usus ja parima äranägemise järgi, tuntakse puudust selgematest suunistest ning võimalusest oma praktikat teiste organisatsioonidega võrrelda. Intervjueeritavad soovisid rohkem infot selle kohta, kas nende kogemused – näiteks vihjete vähesus või töötajate kõhklus – on sarnased ka mujal, ning huvitusid teiste asutuste lahendustest ja statistikast. Samuti mainiti korduvalt segadust seaduse tõlgendamisel ning vajadust lihtsustatud selgituste ja nõu järele, kuidas vihjeandmist töötajatele paremini tutvustada ja süsteemi toimimist järjepidevalt parandada. Intervjuudest saab järeldada, et keskse juhendamise ja nõustamisvõimaluse puudumine süvendab praktika ebaühtlust asutuste lõikes.

Keskse juhandamise ja praktilise toe puudumine takistab vihjekanalite ühtlast ja tõhusat toimimist organisatsioonides.

Teadete sisu ja kvaliteet. Mitmed kanalid on kas alakasutatud või koormatud teadetega, mis ei ole sisulised rikkumised, vaid olmeprobleemid või üldised rahulolematuse väljendused. Eriti keeruline on töökiusu ja inimsuhetega seotud teadete anonüümne menetlemine, kuna sellised juhtumid nõuavad sageli dialoogi ja

konteksti. Anonüümsete teadete puhul lisandub raskus, kui teavitaja ei tule platvormile tagasi või ei ole võimalik temaga ühendust võtta.

Juhtide hoiakud ja „maja sees lahendamise“ kultuur. Mõnes organisatsioonis eelistavad allasutuste juhid probleeme lahendada oma meeskonna sees ning väldivad info jõudmist siseauditi või sisekontrollini. Intervjueeritavate hinnangul pärsivad teavitamist eelkõige autoritaarsed või „vanakooli“ juhtimisstiilid, kus kriitikat ei tajuta konstruktiivsena.

6.2. Peamised tugevused ja head tavad

Vihjete „maskeerimine“. Kõige tõhusamaks praktikaks peetakse intervjuude põhjal strateegilist menetlustaktikat, kus vihjes toodud infot kontrollitakse muude protsesside kaudu, näiteks plaanilise siseauditi või rutiinse kontrolli käigus. Selline lähenemine võimaldab probleemidele reageerida ilma, et uuritav seostaks menetlust konkreetse vihjega, ning pakub vihjeandjale tugevat kaitset.

Kõige tõhusamaks praktikaks peetakse vihjete „maskeerimist“ – info kontrollimist näiteks rutiinse siseauditi kaudu, et mitte reeta vihjeandja olemasolu.

Turvalised IT-lahendused. Oluliseks tugevuseks on osutunud ka tehnilised lahendused, mis võimaldavad anonüümset kahepoolset suhtlust. Välised IT-platvormid, mis pakuvad turvalist postkasti ja täiendavaid anonüümsust toetavaid funktsioone, on intervjuude põhjal märkimisväärselt parandanud menetluste kvaliteeti. Võimalus küsida täpsustavaid küsimusi ilma vihjeandja isikut paljastamata on paljudel juhtudel otsustava tähtsusega.

Kanali kohaldamisala laiendamine. Mitmed asutused on läinud seaduse miinimumnõuetest kaugemale ja laiendanud vihjeandmise kanali kohaldamisala. Selline „mõistlikkuse printsiibil“ põhinev lähenemine, kus julgustatakse teavitama ka sisekorra rikkumistest või muudest probleemidest, muudab süsteemi töötajate jaoks arusaadavamaks ja suurendab selle praktilist väärtust. Samas tuleb arvestada, et kui teade ei kuulu seaduse kohaldamisalasse, ei pruugi teavitajale laieneda seaduslik kaitse. Sellisel juhul võib ta jääda haavatavaks ning riskida kättemaksu või muude ebasoodsate tagajärgedega.

Nelja silma printsiip ja sõltumatus. Teadmine, et vihjeid menetlevad alati vähemalt kaks sõltumatut isikut ning et vastuvõtjaks on eraldiseisev üksus, näiteks siseaudit, vähendab hirmu info kuritarvitamise või mahavaikimise ees.

Läbipaistev suhtlus ja ootuste juhtimine. Intervjueeritavad rõhutasid, et töötajatele tuleb selgelt selgitada, mida vihjeandmise kanal võimaldab ja mida mitte.

Juhtkonna eeskuju ja selged väärtussõnumid. Kultuurimuutuse eelduseks on see, et tippjuhid väljendavad oma sõnades ja tegudes üheselt, et vihjeandmine on lubatud, aktsepteeritud ja vajalik organisatsiooni väärtuste ning aususe kaitsmiseks. Seda toetavad juhid oma järjepideva kommunikatsiooniga, sealhulgas regulaarsete sõnumite, infopäevade ning teema käsitlemisega organisatsioonisisestes kanalites.

Kokkuvõte

Käesolev uurimus analüüsib vihjeandjate kaitse praktilist rakendamist Eestis ning põhineb intervjuudel, mis viidi läbi ajavahemikus november 2025 - veebruar 2026 vihjekanalite haldajate ja menetlejatega eri tüüpi avaliku ja erasektori asutustest. Intervjuude valim koosnes asutustest, kus vihjeandmise mehhanism juba eksisteerib; riiklikku koondstatistikat kanalite leviku või kasutuse kohta ei ole, mistõttu esitatud tähelepanekud kajastavad eelkõige praktikat nende asutuste kontekstis.

Õigusraamistiku osas on Eesti täitnud direktiivi miinimumnõuded: tööalasest EL-õiguse rikkumisest teavitaja kaitse seadus loob aluse teatamiseks ja kättemaksuvastaseks kaitseks. Samas on seaduse materiaalne kohaldamisala kitsas – keskendumine EL-õiguse rikkumistele tähendab, et paljud töötajate mured, nagu korruptsioon, pettused, vargused või sisekorra rikkumised, ei pruugi seadusest tulenevalt automaatselt kaitstud olla. See vastuolu tekitab praktikas segadust ja võib vähendada usaldust vihjeandmise mehhanismide vastu.

Rakendamise tasandil on olukord killustatud. Organisatsioonide lahendused on väga erinevad: mõnel on pikalt toimivad, väliste platvormidega süsteemid (>10 aastat), teistes on kanalid loodud alles 1-2 aasta jooksul. Suuremad organisatsioonid ja rahvusvahelised ettevõtted on paljudes aspektides edumeelsemad: kasutusel on tsentraliseeritud menetlused, spetsiaalsed turvalised IT-platvormid ning püsiv sisemine menetlusvõimekus. Väiksemates asutustes ja kohalikes omavalitsustes kasutatakse sagedamini lihtsamaid

Õigusraamistik keskendub peamiselt EL õiguse rikkumistele, jättes sageli seadusliku kaitseta siseriiklikest probleemidest teavitajad.

lahendusi (nt e-post, veebivormid või dokumendihaldus) ning vihjete käsitlemine toimub muude tööülesannete kõrval.

Intervjuude põhjal on konfidentsiaalsus selgelt keskne kaitsemehhanism. Praktikas rakendatakse ligipääsu piiramist, andmete krüpteerimist, info „puhastamist“ ning menetlustaktikaid, näiteks vihjete „maskeerimist“ rutiinsete kontrollide või auditite kaudu, et vähendada vihjeandja tuvastamise riski. Samas sõltub anonüümsuse praktiline tase tugevalt kasutatavast tehnoloogiast ja asutuse suurusest: välised platvormid võimaldavad anonüümset kahepoolset suhtlust ning parandavad menetluste kvaliteeti, samas kui lihtsamad lahendused seda sageli ei võimalda.

Menetluste sisu näitab, et enamik juhtumeid ei lõpe karistuslike meetmetega, vaid suunatakse pigem süsteemsete või töökeskkonna parenduste poole, näiteks protseduuride täpsustamise või koolituste kaudu. Tõsisemad rikkumised jõuavad menetlejateni sageli otsesuhtluse, mitte ametlike vihjekanalite kaudu, mis peegeldab usalduse rolli teavitamispraktikas.

Samas ilmnesid mitmed olulised väljakutsed. Peamisteks takistusteks on kultuurilised ja organisatsioonilised barjäärid, sealhulgas ajalooline stigma „pealekaebamise“ suhtes, juhtide eelistus probleeme „maja sees“ lahendada, anonüümsuse haprus väikestes kollektiivides ning segadus pädevuste ja kanalite toimimise osas. Kuigi intervjuude põhjal esines otseseid kättemaksujuhtumeid harva, on hirm kättemaksu ees töötajate seas levinud ning enamikus asutustes puuduvad süsteemsed meetmed, millega pärast menetluse lõppu võimalikke probleeme jälgida või ennetada.

Intervjuud viitavad ka sellele, et kättemaksuvastane kaitse ei paku vihjeandjatele alati piisavat õiguskindlust. Kirjeldati juhtumeid, kus vihjeandjad lahkusid organisatsioonist koondamise või muude formaalselt põhjendatud meetmete kaudu. Süsteemne järelkontroll võimaliku kättemaksu tuvastamiseks on valdavalt puudu, mistõttu tugineb kaitse pigem üksikute menetlejate tähelepanelikkusele kui läbimõeldud ja ühtsele süsteemile.

Juhtkonna selge eeskuju ja järjepidevad väärtussõnumid on kultuurimuutuse vältimatu eeldus.

Samal ajal ilmnesid ka konkreetsed tugevused ja head praktikad, mida tasub säilitada ja laiendada. Nendeks on tsentraalsed kanalid ja menetlusressursid, nelja silma printsiip ja sõltumatu siseauditina toimiv vastuvõtustruktuur, väliste turvaliste platvormide kasutamine anonüümseks kahepoolseks suhtluseks ning

juhtkonna selge eeskuju ja väärtussõnumite järjepidev esiletoomine. Need tegurid suurendavad usaldust ja parandavad menetluste kvaliteeti.

Intervjuudest ilmneb lisaks selge vajadus täiendava toe ja juhendamise järele vihjekanalite haldajatele. Kuigi menetlejad tegutsevad üldjuhul heas usus ja parima äranägemise järgi, tuntakse puudust selgematest suunistest, võimalusest võrrelda oma praktikat teiste asutustega ning ligipääsust headele näidetele. Samuti toodi esile segadust seaduse tõlgendamisel ning vajadust lihtsustatud selgituste ja nõu järele, kuidas vihjeandmist töötajatele paremini tutvustada ja süsteemi toimimist järjepidevalt parandada.

Soovitused vihjekanali haldajatele

Järgnevad soovitused tuginevad käesoleva Eesti aruande järeldustele ja Transparency Internationali rahvusvahelistele parimatele praktikatele[3].

1. Laiendada kanali kohaldamisala ja juhtida selgelt töötajate ootusi

Probleem: Eesti uuringust selgub, et vaid EL-i õiguse rikkumistega seotud teavituste vastuvõtmine tekitab töötajates segadust ja ebakindlust, kuna tegelikud probleemid ei pruugi seaduses mainitud valdkondadesse kuuluda või ei oska teavitaja ise seda hinnata. Transparency International soovitab kaasata vihjesüsteemi igasugused kahtlustatavad rikkumised (sh korruptsioon, inimõiguste rikkumised, ahistamine), kuna vastasel juhul ei pruugi potentsiaalsed vihjeandjad aru saada, kas nende mure kuulub seaduse kaitse alla.

Soovitus: Laiendada teavituskanali kohaldamisala. Eestis on häid tulemusi andnud "mõistlikkuse printsiip", kus asutus laiendab teavituskanali kohaldamisala ka näiteks sisekorra rikkumistele, muutes süsteemi töötajatele arusaadavamaks. Samas tuleb arvestada, et kehtiv Eesti seadusandlus võib sellistel juhtudel jätta vihjeandja formaalselt seadusliku kaitseta. Seetõttu on organisatsioonidel oluline rakendada täiendavaid sisemisi meetmeid, et tagada vihjeandja isiku maksimaalne konfidentsiaalsus ning pakkuda talle praktilist kaitset organisatsiooni sees.

2. Tagada anonüümne, kuid kahepoolne suhtlusvõimalus

Probleem: Kuigi kohustust selleks pole, siis intervjueeritud asutuste vihjekanalid võtavad enamasti vastu ka anonüümseid teateid. Sageli on probleemiks (eriti e-posti või lihtsate veebivormide puhul), et vihjeandjaga ei saa hiljem ühendust võtta ja uurimine sumbub menetlejate sõnul info puudumise tõttu.

Soovitus: Nii Transparency Internationali poolt soovitatav kui ka Eesti praktika näitavad, et parimaks lahenduseks on turvalised IT-lahendused, mis võimaldavad menetlejal pidada teavitajaga kahepoolset dialoogi ilma vihjeandja isikut tuvastamata. Vihjekanali haldajana soodustage selliste lahenduste kasutuselevõttu ja pakkuge vähemalt ühte täiesti anonüümset kanalit.

[3]Internal Whistleblowing Systems. Best practice principles for public and private organisations. (2022) Transparency International https://transparency.ee/publikatsioonid/internal-whistleblowing-systems-best-practice-principles-public-and-private

3. Rakendada uurimisel „maskeerimist“ ja nelja silma printsiipi

Probleem: Väiksemates kollektiivides on anonüümsus väga habras ja vihjeandja isik on tihti kaudselt tuletatav, mis tekitab tugevat hirmu kättemaksu ees.

Soovitus: Eesti asutuste kõige tõhusamaks taktikaks on osutunud vihjete "maskeerimine" – saadud info kontrollimine nii, nagu see oleks avastatud rutiinse siseauditi või plaanilise kontrolli käigus. See kaitseb vihjeandja identiteeti. Usalduse tõstmiseks tuleks kasutada ka nelja silma printsiipi (vähemalt kaks sõltumatut menetlejat) ning vältida huvide konflikte, kaasates menetlusse organisatsiooni sõltumatu üksuse (nt siseaudit).

4. Hoida vihjeandjat aktiivselt kursis ja tagada sisuline tagasiside

Probleem: Pika vaikuse korral võib vihjeandja tunda, et tema teadet ignoreeritakse, mis vähendab usaldust kogu süsteemi vastu.

Soovitus: Transparency International soovitab kinnitada teate kättesaamist lühikese aja, soovitavalt seitsme päeva jooksul. Esimene sisuline tagasiside tuleks anda hiljemalt kolme kuu jooksul, kuid kommunikatsioon vihjeandjaga peaks toimuma regulaarselt ka edaspidi. Vihjeandjat tuleks teavitada plaanitavatest sammudest, kaitsemeetmetest ning uurimise lõpptulemustest.

5. Hinnata kättemaksuriske süsteemselt ja seada sisse järelkontroll

Probleem: Eestis puuduvad asutustes valdavalt süsteemsed järelkontrolli meetmed ja kättemaksuvastane kaitse tugineb pigem üksikute menetlejate tähelepanelikkusele. Kättemaks võib olla ka varjatud (nt sotsiaalne tõrjutus, koolitustest ilmajätmine, koondamine).

Soovitus: Vihjekanali haldajana tuleks riske hinnata kohe teate saamisel ja pidevalt uurimise vältel. Sisse tuleks viia süstemaatiline järelkontroll (näiteks 3, 6, 12 kuud pärast menetluse lõppu), et veenduda, ega vihjeandja ei ole langenud varjatud kättemaksu ohvriks. Ennetavate meetmete kasutuselevõtt aitab võimalikke kättemaksujuhtumeid ära hoida.

6. Toetada kultuurimuutust läbi juhtide aktiivse kaasamise (*tone from the top)*

Probleem: Eestis valitseb kohati veel "pealekaebamise" stigma ning osad juhid eelistavad probleeme vaikselt "maja sees" lahendada.

Soovitus: Kultuurimuutuse peamine eeldus on tippjuhtkonna selge eeskuju. Kanali haldajana nõustage ja suunake organisatsiooni tippjuhte, et nad väljendaksid järjepidevalt tugevat toetust *speak up* (julge rääkida) kultuurile. Samuti on oluline regulaarne teavitustöö ning vihjeandmist soosiva kultuuri ja väärtuste edendamine. Kuna paljud töötajad pöörduvad esimesena oma juhi poole, tuleb otseseid juhte koolitada, kuidas vihjet ära tunda, info konfidentsiaalsust kaitsta ja kuidas teavitajat edasi suunata. Samas ei tohiks töötajatele teha ettekirjutust ("kõigepealt räägi otsese juhiga"), vaid neile tuleb selgitada, et nad on igati oodatud kasutama vajadusel ametlikku vihjekanalit kohe, eriti olukorras, kus nad ei tunne ennast juhiga rääkides mugavalt või kui kahtlus puudutabki nende otsest juhti.

Soovitused seadusandjale

Järgnevad soovitused põhinevad käesoleva uuringu raames läbi viidud intervjuudel, kahel erineval Transparency Internationali poolt tehtud analüüsil EU direktiivi ülevõtmisest erinevates riikides[4&5] ning GRECO VI hindamisvooru raames Eestile tehtud soovitustel[6].

1. Laiendada vihjeandjate kaitse kohaldamisala väljapoole EL õigust

Probleem: Kehtiv seadus piirab kaitse EL õiguse rikkumistega. Transparency International toob välja, et kui kohaldamisala on killustatud või piiratud, ei pruugi potentsiaalsed vihjeandjad aru saada, kas nende mure kuulub seaduse kaitse alla, mis toob kaasa vaikimise ning rikkumiste avastamata jäämise. Intervjuud kinnitavad, et enamik reaalseid vihjeid puudutab Eesti siseriikliku õiguse rikkumisi. EL direktiiv lubab ja Euroopa Komisjon soovitab ühtse horisontaalse süsteemi loomist. GRECO teeb Eestile otsese soovituse muuta seadust nii, et selle kohaldamisala laieneks ka siseriikliku õiguse rikkumistele (lõik 113).

Soovitus: Laiendada seaduse kohaldamisala vähemalt tööalases kontekstis ka siseriikliku õiguse rikkumistele.

2. Tagada vihjekanalite struktuurne sõltumatus ja huvide konflikti vältimine

Probleem: Eesti seadus nõuab kanalite loomist, kuid ei sätesta nende struktuurse sõltumatuse nõudeid. See on oluline vastavuslünk EL direktiivi suhtes, mille kohaselt asutusesiseselt on oluline vihjekanali eest vastutava isiku erapooletus teadete menetlemisel ja asutusevälise teavituskanali puhul peab see olema sõltumatu ja eraldiseisev. Transparency International toob välja, et vihjekanalite sõltumatuse

[4] How well do EU countries protect whistleblowers? (2023) Transparency International https://transparency.ee/en/how-well-do-eu-countries-protect-whistleblowers-0

[5] How effective is whistleblower protection in the EU? Trends, gaps and emerging practices across member states. (2026) Transparency International https://www.transparency.org/en/publications/whistleblower-protection-eu-trends-gaps-practices-member-states

[6] GRECO's Sixth Evaluation Round. Preventing corruption and promoting integrity at the sub-national level. Estonia, including Tallinn and Tartu. (2026) https://www.coe.int/en/web/greco/evaluations/estonia

puudumine, nõrgad konfidentsiaalsuse tagatised ja asutusesisesed hierarhilised sõltuvused õõnestavad tõsiselt vihjeandjate usaldust süsteemi vastu. Eesti intervjuud kinnitasid, et usaldus kanalite vastu sõltub otseselt sellest, kes vihjeid menetleb.

Soovitus: Sätestada seaduses või rakendusaktides miinimumnõuded vihjekanalite sõltumatusele, näiteks alluvus otse tippjuhtkonnale, mitte personalifunktsioonile. Et väiksemate asutuste puhul ressursipuudusel halduskoormust jagada, siis intervjuudes toodi hea praktikana välja, et suurem struktuuriüksus (nt ministeerium või omavalitsus) haldab allasutuste kanaleid.

3. Parandada kättemaksu vastase kaitse tõhusust ja tõendamiskoormust

Probleem: Kuigi seadus näeb ette ümberpööratud tõendamiskoormise, võimaldab see tööandjal õigustada meetmeid ka põhjustega, mis ei ole sõltumatud vihjeandmisest. See loob soodsa pinnase varjatud kättemaksuks – näiteks võib kättemaks toimuda näiliselt neutraalsete struktuurimuudatuste varjus või töökeskkonna väljakannatamatuks muutmises. Direktiiv näeb ette, et liikmesriigid võtavad vajalikud meetmed, et tagada vihjeandjate kaitse survemeetmete eest. Mitmed intervjueeritud vihjekanalite eest vastutajad kirjeldavad juhtumeid, kus vihjeandjad lahkusid organisatsioonist koondamise või muude formaalselt põhjendatud meetmete kaudu. Transparency International soovitab tungivalt, et liikmesriigid täpsustaksid oma seadusi nii, et tööandjal lasuks kohustus tõendada, et rakendatud kahjulik meede oli vihjeandmisest täielikult sõltumatu.

Soovitus: Täpsustada seadust selliselt, et tööandjal lasub kohustus tõendada, et võetud meede ei olnud kuidagi seotud vihjeandmisega.

4. Tagada vihjeandjatele tegelik õiguskaitse ja hüvitised

Probleem: Eesti seadus ei reguleeri piisavalt õiguskaitsevahendeid, esialgset õiguskaitset, hüvitisi ega õigusabikulude katmist, millele osutab ka GRECO raport (lõik 110). See on oluline vastavuslünk EL direktiivi suhtes, mis näeb ette, et survemeetmete ohvriks langenud isikutele tuleb tagada õiguskaitsevahendite olemasolu ning kantud kahju täielik hüvitamine. Transparency International lisab, et vihjeandjad peaksid saama täieliku kompensatsiooni nii varalise kui ka mittevaralise (nt emotsionaalse) kahju eest ning kättemaksumeetmed (nt vallandamine) tuleks

tühistada või isik ametisse ennistada. Intervjuudest ilmnes, et vihjeandjad sõltuvad sageli menetleja heast tahtest, mitte süsteemsest toest.

Soovitus: Sätestada selged õigused esialgsele õiguskaitsele, et pakkuda kaitset poolelioleva vaidluse või menetluse ajaks. Täiendada seadust, et tagada kantud kahju täielik hüvitamine taastamaks vihjeandja olukord võimalikult lähedaseks kättemaksueelsele seisule.

5. Tagada keskne järelevalve ja ühtne andmekogumine

Probleem: Eestis puudub sõltumatu keskne asutus, mis koordineeriks vihjeandjate kaitse toimimist ning tagaks süsteemse andmekogumise ja analüüsi. Intervjuudest ilmneb, et ilma keskse koordineeriva toeta jääb vihjekanalite toimimine suurel määral üksikute menetlejate teadmiste ja initsiatiivi kanda, mis süvendab praktika ebaühtlust. Samuti ei koguta ega avaldata Eestis järjepidevalt andmeid vihjete arvu, teemade, menetluste ega rakendatud kaitsemeetmete kohta, kuigi nii EL direktiiv, Transparency International kui ka GRECO rõhutavad, et seaduse tõhususe hindamiseks on selline andmestik hädavajalik. Andmete puudumine vähendab süsteemi läbipaistvust ja usaldusväärsust ning raskendab ka tulevaste poliitikamuudatuste kavandamist.

Soovitus: Kehtestada kohustus, et kõik vihjekanalite omanikud koguvad ja edastavad regulaarselt (vähemalt kord aastas) anonüümseid koondandmeid vihjete, nende sisu, menetluste ja rakendatud kaitsemeetmete kohta. Paralleelselt määrata sõltumatu keskne riiklik üksus, kelle ülesanne on neid andmeid süstemaatiliselt koondada, analüüsida ja avaldada ning hinnata vihjeandjate kaitsesüsteemi toimimist tervikuna. Kogutud andmeid tuleks kasutada nii järelevalveks kui ka koolituste ja juhendmaterjalide arendamiseks ning avalikkusele selgelt näitamiseks, et vihjeandmine viib sisuliste tulemusteni ja toimiva kaitsesüsteemini.

Lisa 1. Intervjueeritud vihjekanalite haldajate nimekiri.

Intervjuu	Asutus	Intervjueeritud isiku roll
1	Kohalik omavalitsus	sisekontrolör
2	Ministeerium	siseauditi juht
3	Eraettevõte	siseauditi juht
4	Ministeerium	siseauditi juht
5	Kohalik omavalitsus	vallasekretär
6	Kohalik omavalitsus	sisekontrolör
7	Ministeerium	nõunik
8	Kohalik omavalitsus	sisekontrolör
9	Riigi äriühing	vastavuskontrolli juht
10	Riigiasutus	jurist
11	Avalik-õiguslik ülikool	kantselei juhataja
12	Eraettevõte (finantssektor)	siseauditi juht
13	Riigi äriühing	siseauditi juht
14	Avalik-õiguslik ülikool	siseaudiitor
15	Riigiasutus	riskijuhtimise osakonna juhataja
16	Avaliku sektori tervishoiuasutus (haigla)	siseauditi juht

Kasutatud kirjandus

Euroopa Parlamendi ja nõukogu direktiiv (EL) 2019/1937 liidu õiguse rikkumisest teavitavate isikute kaitse kohta (30.12.2024). *EUR-Lex*. Kasutatud 07.04.2026, https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A02019L1937-20241230

GRECO's Sixth Evaluation Round. Preventing corruption and promoting integrity at the sub-national level. Estonia, including Tallinn and Tartu (2026). Council of Europe. Kasutatud 10.04.2026, https://www.coe.int/en/web/greco/evaluations/estonia

How effective is whistleblower protection in the EU? Trends, gaps and emerging practices across member states. (2026) Transparency International. Kasutatud 24.04.2026, https://www.transparency.org/en/publications/whistleblower-protection-eu-trends-gaps-practices-member-states

How well do EU countries protect whistleblowers? Assessing the transposition of the EU Whistleblower Protection Directive (2023). Transparency International. Kasutatud 07.04.2026, https://transparency.ee/en/how-well-do-eu-countries-protect-whistleblowers-0

Internal Whistleblowing Systems. Best practice principles for public and private organisations. (2022). Transparency International. Kasutatud 07.04.2026, https://transparency.ee/publikatsioonid/internal-whistleblowing-systems-best-practice-principles-public-and-private

Tööalasest Euroopa Liidu õiguse rikkumisest teavitaja kaitse seadus (17.05.2025). *Riigi Teataja I*. Kasutatud 07.04.2026, https://www.riigiteataja.ee/akt/117052025002

Kasulikke materjale

Vihjeandmise mehhanism ettevõttes. Tööriistakast (2019). Ühing Korruptsioonivaba Eesti. Kasutatud 07.04.2026, https://transparency.ee/publikatsioonid/vihjeandmise-mehhanism-ettevottes-tooriistakast

Vihjeandmise meetmed: e-kursus praktikutele (2021). Ühing Korruptsioonivaba Eesti. Kasutatud 07.04.2026, https://kve-vihjeandmise-meetmed.thinkific.com/courses/vihjeandmise-meetmed-e-kursus-praktikutele

Kaasrahastanud Euroopa Liit. Väljendatud seisukohad ja arvamused on siiski üksnes autori(te) omad ega pruugi kajastada Euroopa Liidu või rahastava asutuse seisukohti ja arvamusi. Euroopa Liit ega rahastav asutus ei vastuta nende eest.

Kaasrahastanud Euroopa Liit

CC BY NC SA