

| | | | | | | | | | | | |
|----------------------------|-----------|---------------------------------|----------|---|------------|--|------|--|----------|--|-----|
| | | | | Sisestage siia registreeritud juriidilise isiku nimi | | | | | | | |
| Dokumendi number: PII13 | | | | Dokumendi pealkiri: Rahvusvahelise PII edastamise poliitika | | | | | | | |
| Versioon: 1.0 | | Jõustumiskuupäev: 01.01.2025 | | Dokumendi omanik: | | | | | | | |
| X | Poliitika | | Standard | | Protseduur | | Vorm | | Register | | Muu |

| Muudatuste ajalugu | | | | |
|--------------------|-------------------|------------|---------------|------------------|
| Muudatuse number | Muudatuse kuupäev | Muudatused | Läbi vaadanud | Protsessi omanik |
| | | | | |
| | | | | |

| Kinnitused | | | |
|------------|-----------|---------|---------|
| Nimi | Ametikoht | Kuupäev | Allkiri |
| | | | |
| | | | |

| |
|--|
| <p>Õiguslik teatis (autoriõigus ja kasutuspiirangud) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Käesolev dokument on Clarysec LLC intellektuaalomand. Selle dokumendi ühtegi osa ei tohi ilma eelneva selgesõnalise kirjaliku loata kopeerida, taaskasutada, levitada ega muuta äriilistel või rakendamise eesmärkidel.</p> <p>Loata kasutamine on rangelt keelatud ja võib kaasa tuua õiguslikke meetmeid.</p> <p>Litsentsimise küsimustes võtke ühendust: info@clarysec.com</p> |
|--|

Kooskõla standardite ja regulatsioonidega

| Standard / Regulation | Clause / Control / Article | Applicability | Coverage Type | Comment |
|-----------------------|---|-------------------------------|---------------|--|
| ISO/IEC 27701:2025 | Clause 7.5; Clause 8.1 | Both | Primary | Edastamise tõendusmaterjal ja tegevuslik kontroll |
| ISO/IEC 27701:2025 | Clause 9.1; Clause 10.2 | Both | Supporting | Seire, mittevastavus ja parandusmeetmed |
| ISO/IEC 27701:2025 | Annex A.1.2.8; Annex A.1.2.9 | Controller / Joint Controller | Supporting | Ühine vastutus ja töötlemiskirjed |
| ISO/IEC 27701:2025 | Annex A.1.5.2; Annex A.1.5.3 | Controller | Primary | Edastamise alus ja edastamise asukohad |
| ISO/IEC 27701:2025 | Annex A.1.5.4; Annex A.1.5.5 | Controller | Primary | Edastamise ja avalikustamise kirjed |
| ISO/IEC 27701:2025 | Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7 | Processor | Supporting | Kliendileping, juhised ja volitatud töötaja kirjed |
| ISO/IEC 27701:2025 | Annex A.2.5.2; Annex A.2.5.3 | Processor | Primary | Volitatud töötaja edastamise alus ja asukohad |
| ISO/IEC 27701:2025 | Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6 | Processor | Supporting | Volitatud töötaja avalikustamiskirjed ja õiguslikult siduvad avalikustamised |
| GDPR | Article 5(2); Article 24 | Controller | Supporting | Vastutus ja vastutava töötaja meetmed |
| GDPR | Article 26 | Joint Controller | Supporting | Ühise vastutuse jaotus |
| GDPR | Article 28 | Processor | Supporting | Volitatud töötaja juhised ja autoriseerimine |
| GDPR | Article 30 | Both | Supporting | Edastamiskirjed |
| GDPR | Article 44 | Both | Primary | Üldine edastamise põhimõte |
| GDPR | Article 45 | Controller | Primary | Piisavuse mehhanism |
| GDPR | Article 46 | Controller | Primary | Asjakohased kaitsemeetmed |
| GDPR | Article 47 | Controller | Supporting | Siduvad kontsernisisised eeskirjad |
| GDPR | Article 48 | Both | Supporting | Avaliku asutuse avalikustamistaotlused |
| GDPR | Article 49 | Controller | Supporting | Erandid konkreetsetes olukordades |

| | | | | |
|-----------------------|--|------|------------|--|
| ISO/IEC 29100:2020 | Clause 5.6; Clause 5.10; Clause 5.12 | Both | Supporting | Avalikustamise piiramine, vastutus ja privaatsusnõuetele vastavus |
| ISO/IEC 29151:2022 | Annex A.7 | Both | Supporting | Kasutamise, säilitamise, avalikustamise ja edastamise kaitse |

1. Kohaldamisala

- 1.1 See poliitika kehtestab organisatsiooni nõuded PII rahvusvaheliste edastuste tuvastamiseks, heakskiitmiseks, registreerimiseks, läbivaatamiseks, piiramiseks ja peatamiseks.
- 1.2 Seda poliitikat kohaldatakse vastutava töötleja, kaasvastutava töötleja, volitatud töötleja ja alltöötleja tegevustele, mille käigus PII tehakse kättesaadavaks, sellele pääsetakse juurde, seda säilitatakse, majutatakse, avalikustatakse või muul viisil edastatakse riiki, territooriumile, rahvusvahelisele organisatsioonile või vastuvõtjale väljaspool REG02-s või REG09-s registreeritud heakskiidetud töötlemispiiri.
- 1.3 Seda poliitikat kohaldatakse edastustele, mis hõlmavad sisemisi sidusettevõtteid, väliseid vastuvõtjaid, volitatud töötlejaid, alltöötlejaid, teenuseosutajaid, tugijuurdepääsu, majutusasukohti, kaughaldust, edasiedastusi, avaliku asutuse avalikustamisaotlusi ja edastamisega seotud teenusemuudatusi.
- 1.4 See poliitika ei anna õigusnõu, ei määratle standardsete lepingutingimuste teksti, ei loo eraldi edastamise mõjuhindamise registrit, ei loo eraldi SCC registrit, ei määratle turbekontrollide arhitektuuri, ei määratle volitatud töötleja elutsükli juhtimist ega intsidendihalduse töövoogu. Neid küsimusi käsitletakse seotud poliitikate, kliendipõhise õigusliku konfiguratsiooni või heakskiidetud REG09 tõendusmaterjali kaudu.
- 1.5 Käesoleva poliitika tähenduses on oluline edastamismuudatus mis tahes muudatus edastamise sihtkohas, vastuvõtjas, töötlemisrollis, majutusasukohas, tugijuurdepääsu asukohas, edastusmehhanismis, edasiedastamise teekonnas, volitatud töötleja või alltöötleja korralduses, õiguslikus või regulatiivses edastamistingimuses, edastamise kaitsemeetmes või edastamise jääkriskis.

2. Eesmärk

- 2.1 Selle poliitika eesmärk on tagada, et PII rahvusvahelised edastused tuvastatakse enne nende toimumist, neid toetab heakskiidetud edastusmehhanismi tõendusmaterjal, nende edastamisrisk vaadatakse läbi, nende edasiedastusi juhitakse ning need peatatakse või korrigeeritakse, kui nõutavat tõendusmaterjali või kaitsemeetmeid ei säilitata.
- 2.2 See poliitika võimaldab organisatsioonil tõendada vastutuspõhist edastamise juhtimist, kasutades REG09-t peamise edastamise tõendusobjektina ning REG02, REG08 ja REG12 toetavate tõendusobjektidena.

3. Eesmärgid

3.1 Selle poliitika eesmärgid on:

- 3.1.1 tuvastada PII rahvusvahelised edastused enne töötlemise algust või muutmist;
- 3.1.2 säilitada heakskiidetud edastamiskirjed REG09-s;
- 3.1.3 dokumenteerida edastusmehhanismid ja toetav tõendusmaterjal;
- 3.1.4 määratleda edastamisriski läbivaatamise ja heakskiitmise nõuded;
- 3.1.5 kontrollida volitatud töötleja, alltöötleja ja edasiedastamise autoriseerimist;
- 3.1.6 vaadata aktiivsed edastused läbi kindlaksmääratud sagedusega;
- 3.1.7 peatada või korrigeerida edastused, kui nõutavat tõendusmaterjali, autoriseerimist või kaitsemeetmeid ei säilitata;
- 3.1.8 vältida tarbetut õigusnõu teksti, dubleerivaid registreid ja dubleerivaid tarnijajuhtimise kontrollimeetmeid.

4. Poliitika põhimõtted

4.1 Edastamise tuvastamine ja registreerimine

- 4.1.1 [Controller] Process Owner / Business Owner PEAB tuvastama PII rahvusvahelise edastamise sihtkohad, vastuvõtjate kategooriad ja juurdepääsu asukohad REG02-s enne töötlemistoimingu algust või olulist muutmist.
- 4.1.2 [Controller] Privacy Lead / PIMS Manager PEAB looma või ajakohastama REG09 edastamiskirje enne iga uue või oluliselt muudetud vastutava töötleja PII rahvusvahelise edastamise algust.
- 4.1.3 [Processor] Vendor / Procurement Owner PEAB registreerima kliendi autoriseeritud volitatud töötleja edastamise sihtkohad, teenuse asukohad ja kaugjuurdepääsu asukohad REG08-s ja REG09-s enne volitatud töötleja edastamistegevuse algust või muutmist.
- 4.1.4 [Joint Controller] Privacy Lead / PIMS Manager PEAB registreerima kaasvastutava töötleja vastutusvaldkondade jaotuse rahvusvahelise edastamise otsuste puhul REG08-s ja REG09-s enne ühise edastamistegevuse algust või muutmist.
- 4.1.5 [Both] Process Owner / Business Owner PEAB tuvastama edasiedastamise marsruudid, edasiste vastuvõtjate kategooriad ja edasiedastamise tingimused REG09-s enne edasiedastamise heakskiitmist.

4.2 Edastusmehhanismi valik ja heakskiitmine

- 4.2.1 [Controller] Privacy Lead / PIMS Manager PEAB registreerima heakskiidetud edastusmehhanismi ja toetava tõendusmaterjali REG09-s enne vastutava töötleja PII rahvusvahelise edastamise algust.
- 4.2.2 [Controller] Data Protection Officer / Privacy Advisor PEAB läbi vaatama edastusmehhanismi tõendusmaterjali REG09-s enne uue, oluliselt muudetud või kõrgema riskiga PII rahvusvahelise edastamise heakskiitmist.
- 4.2.3 [Processor] Vendor / Procurement Owner PEAB hankima dokumenteeritud kliendi autoriseeringu või juhise REG08-s ja REG09-s enne mis tahes volitatud töötleja PII rahvusvahelise edastamise algatamist.
- 4.2.4 [Subprocessor] Vendor / Procurement Owner PEAB registreerima alltöötleja edastamise autoriseerimise ja kohaldatavad edasiantavad edastamistingimused REG08-s ja REG09-s enne alltöötleja edastamistegevuse algust.
- 4.2.5 [Both] Privacy Lead / PIMS Manager PEAB blokeerima või edasi lükkama PII rahvusvahelise edastamise REG09-s, kui edastusmehhanism, sihtkoht, vastuvõtja, rollijaotus või toetav tõendusmaterjal on enne kavandatud edastamise algust puudulik.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Erandid

- 9.1.1 [All] Process Owner / Business Owner PEAB esitama iga taotluse jätkata puuduliku, viibiva või erandliku edastamise tõendusmaterjaliga REG12-s enne erandi aktiveerumist.
- 9.1.2 [All] Privacy Lead / PIMS Manager PEAB heaks kiitma või tagasi lükkama edastamiserandi taotlused REG12-s enne erandi aktiveerumist.
- 9.1.3 [All] Data Protection Officer / Privacy Advisor PEAB registreerima nõuande REG12-s enne iga edastamiserandi heakskiitmist, mis hõlmab kõrgema riskiga töötlemist, puuduvat edastusmehhanismi tõendusmaterjali, avaliku asutuse avalikustamist, edasiedastamist või sertifitseerimismõju.
- 9.1.4 [All] Top Management PEAB heaks kiitma edastamiserandid, mis ületavad 90 päeva, mõjutavad kõrgema riskiga töötlemist, mõjutavad korduvat edastamistegevust või mõjutavad välist kindlustandmist, REG12-s enne erandi aktiveerumist.

9.1.5 [All] Privacy Lead / PIMS Manager PEAB määrama iga heakskiidetud edastamiserandi jaoks omaniku, aegumiskuupäeva, kompenseeriva kontrollimeetme ja läbivaatamise sageduse REG12-s.

9.1.6 [All] Privacy Lead / PIMS Manager PEAB läbi vaatama iga avatud edastamiserandi REG12-s vähemalt kord kuus kuni sulgemiseni.

10. Jõustamine

10.1.1 [All] Privacy Lead / PIMS Manager PEAB registreerima mittevastavuse REG12-s viie tööpäeva jooksul pärast registreerimata edastamise, toetamata edastusmehhanismi, puuduva volitatud töötaja autoriseeringu, tähtaja ületanud läbivaatamise, puuduva edasiedastamise tõendusmaterjali või autoriseerimata edastamise jätkamise tuvastamist.

10.1.2 [Controller] Privacy Lead / PIMS Manager PEAB peatama vastutava töötaja PII rahvusvahelise edastamise REG09-s, kui nõutav edastusmehhanismi tõendusmaterjal puudub enne kavandatud edastamise algust.

10.1.3 [Processor] Vendor / Procurement Owner PEAB peatama volitatud töötaja rahvusvahelise edastamise tegevuse REG08-s ja REG09-s, kui nõutav kliendi autoriseering puudub enne edastamistegevuse algust.

10.1.4 [Subprocessor] Vendor / Procurement Owner PEAB eskaleerima autoriseerimata alltöötaja rahvusvahelise edastamise tegevuse REG08-s ja REG12-s viie tööpäeva jooksul selle tuvastamisest.

10.1.5 [All] Top Management PEAB määrama REG12-s parandusmeetme omaniku 10 tööpäeva jooksul korduvate, pikaajaliste, kõrge riskiga või sertifitseerimise seisukohast oluliste edastamistõrgete puhul.

10.1.6 [All] Internal Audit / Compliance Reviewer PEAB kontrollima edastamisega seotud mittevastavuste parandusmeetmete tõhusust REG12-s järgmisel kavandatud auditiil või 60 päeva jooksul sulgemisest, olenevalt sellest, kumb toimub varem.

11. Lävivaatamine ja ajakohastamine

11.1.1 [All] Privacy Lead / PIMS Manager PEAB läbi vaatama selle poliitika kord aastas ja registreerima läbivaatamise tulemuse REG12-s.

11.1.2 [All] Privacy Lead / PIMS Manager PEAB läbi vaatama selle poliitika 30 päeva jooksul olulisest muudatusest edastamist käsitlevas õiguses, edastusmehhanismi kättesaadavuses, volitatud töötaja teenusemudelis, majutusasukohas, tugijuurdepääsu asukohas, alltöötaja korralduses, edastamise kaitsemeetmes või PIMS sertifitseerimisnõuetes.

11.1.3 [All] Data Protection Officer / Privacy Advisor PEAB läbi vaatama selle poliitika privaatsuse seisukohast olulised muudatused REG12-s enne heakskiitmist.

11.1.4 [All] Top Management PEAB heaks kiitma selle poliitika olulised muudatused REG12-s enne avaldamist.

11.1.5 [All] Privacy Lead / PIMS Manager PEAB registreerima heakskiidetud poliitikamuudatuste teavitamise REG11-s 30 päeva jooksul avaldamisest.

12. Seotud poliitikad

- 12.1 Seda poliitikat toetavad järgmised seotud poliitikad:
- 12.2 PII01 - Privaatsusteabe haldussüsteemi poliitika
- 12.3 PII02 - Privaatsusrollide, vastutuste ja vastutuse poliitika
- 12.4 PII03 - PII töötlemise inventari ja õigusliku aluse poliitika
- 12.5 PII04 - Privaatsusteate ja läbipaistvuse poliitika
- 12.6 PII07 - Privaatsusriskide hindamise ja DPIA poliitika

- 12.7 PII08 - Lõimitud ja vaikimisi andmekaitse poliitika
- 12.8 PII09 - PII kogumise, kasutamise, avalikustamise ja jagamise poliitika
- 12.9 PII12 - Volitatud töötajate, alltöötajate ja kolmandate osapoolte privaatsushalduse poliitika
- 12.10 PII14 - PII turbe ja juurdepääsukontrolli poliitika
- 12.11 PII17 - PIMS dokumenteeritud teabe ja tõendusmaterjali halduse poliitika
- 12.12 PII18 - PIMS seire, auditi ja täiustamise poliitika

13. Viitestandardid ja raamistikud

- 13.1 See poliitika on vastendatud järgmiste standardite ja regulatsioonidega. Vastendus selgitab, kuidas poliitika toetab viidatud nõudeid, ning tuvastab sisemised punktid, mis neid rakendavad või toetavad.

13.2 ISO/IEC 27701:2025

- 13.2.1 **Clause 7.5; Clause 8.1** - Vastendatud dokumenteeritud edastamise tõendusmaterjalile, edastamise tegevuslikule kontrollile, REG09 edastamisväljadele, edastamise heakskiitudele, edastamise rakendamise kirjetele ja edastamise tõendusmaterjali kooskõlastamisele. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.5; 7.1.1; 7.1.2; 7.1.3; 7.1.5; 7.1.6].
- 13.2.2 **Clause 9.1; Clause 10.2** - Vastendatud rahvusvahelise edastamise kontrollimeetmete seirele, mõõdikutele, läbivaatamisele, peatamisele, mittevastavusele ja parandusmeetmetele. Addressed by clauses [4.3.4; 4.5.1; 4.5.3; 6.1.1; 6.1.2; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.6; 10.1.1; 10.1.5; 10.1.6].
- 13.2.3 **Annex A.1.2.8; Annex A.1.2.9** - Vastendatud kaasvastutava töötaja vastutuse tõendusmaterjalile ja vastutava töötaja töötlemiskirjetele, mis sisaldavad rahvusvahelise edastamise teavet. Addressed by clauses [4.1.1; 4.1.4; 4.1.5; 4.5.5; 6.1.4; 7.1.5].
- 13.2.4 **Annex A.1.5.2; Annex A.1.5.3** - Vastendatud vastutava töötaja edastamise alusele, edastusmehhanismi tõendusmaterjalile, riikidele, rahvusvahelistele organisatsioonidele, sihtkohtadele ja edastamise läbivaatamise tõendusmaterjalile REG09-s. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.3.1; 4.5.1].
- 13.2.5 **Annex A.1.5.4; Annex A.1.5.5** - Vastendatud edastamise ja avalikustamise kirjetele, edasiedastamise marsruudi tuvastamisele ning lõpuleviidud edastamise või avalikustamise tõendusmaterjalile. Addressed by clauses [4.1.5; 4.4.3; 4.4.5; 7.1.7].
- 13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Vastendatud volitatud töötaja kliendilepingutele, dokumenteeritud kliendi juhistele, volitatud töötaja kirjetele ja autoriseerimise tõendusmaterjalile volitatud töötaja rahvusvaheliste edastuste puhul. Addressed by clauses [4.1.3; 4.2.3; 4.2.4; 4.4.2; 6.1.5; 7.1.6; 10.1.3].
- 13.2.7 **Annex A.2.5.2; Annex A.2.5.3** - Vastendatud volitatud töötaja edastamise alusele, kliendi autoriseeritud edastamise sihtkohtadele, teenuse asukohtadele ja edastamiskoha tõendusmaterjalile. Addressed by clauses [4.1.3; 4.2.3; 4.2.4; 4.5.2; 7.1.6].
- 13.2.8 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Vastendatud volitatud töötaja avalikustamiskirjetele, avalikustamistaotluste käsitlemise tõendusmaterjalile, avaliku asutuse avalikustamistaotluste suunamisele ja edasiedastamise tõendusmaterjalile. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 10.1.4].

13.3 GDPR

- 13.3.1 **Article 5(2); Article 24** - Vastendatud vastutusele, vastutava töötaja juhtimisele, edastamise tõendusmaterjalile, edastamisriski läbivaatamisele, erandite käsitlemisele ja parandusmeetmetele. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.3.4; 4.3.5; 6.1.2; 8.1.1; 9.1.2; 9.1.3; 10.1.1; 11.1.1].

- 13.3.2 **Article 26** - Vastendatud kaasvastutava töötleja rahvusvahelise edastamise vastutusvaldkondade jaotusele. Addressed by clauses [4.1.4; 6.1.4].
- 13.3.3 **Article 28** - Vastendatud volitatud töötleja ja alltöötaja edastamise autoriseerimisele, kliendi juhiste, edasiantavate kohustuste tõendusmaterjalile ja peatamisele, kui autoriseering puudub. Addressed by clauses [4.1.3; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 6.1.5; 10.1.3; 10.1.4].
- 13.3.4 **Article 30** - Vastendatud töötlemistoimingute kirjetele ja edastamiskirjetele REG02-s, REG08-s ja REG09-s. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.5; 4.5.5; 7.1.5].
- 13.3.5 **Article 44** - Vastendatud üldisele edastamise juhtimisele, edastusmehhanismi heakskiitmisele, edastamisriski läbivaatamisele, puuduva tõendusmaterjali korral peatamisele ja edastamise kordushindamisele. Addressed by clauses [4.1.2; 4.2.1; 4.2.5; 4.3.1; 4.5.3; 4.5.4].
- 13.3.6 **Article 45** - Vastendatud piisavusel põhineva edastusmehhanismi tõendusmaterjalile, läbivaatamisele ja heakskiitmisele REG09-s. Addressed by clauses [4.2.1; 4.2.2; 4.5.1].
- 13.3.7 **Article 46** - Vastendatud asjakohastele kaitsemeetmetele, kaitsemeetmete tõendusmaterjalile, tehniliste kaitsemeetmete sõltuvuste suunamisele ja edastamise peatamisele, kui kaitsemeetmed puuduvad või ei kehti. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.5.4].
- 13.3.8 **Article 47** - Vastendatud siduvatele kontsernisestele eeskirjadele edastusmehhanismi võimalusena, kui need on kohaldatavad ja REG09-s registreeritud. Addressed by clauses [4.2.1; 4.2.2; 4.3.1].
- 13.3.9 **Article 48** - Vastendatud välisriigi avaliku asutuse avalikustamistaotluse registreerimisele ja privaatsusnõuandele enne vastamist, kui see on teostatav. Addressed by clauses [4.4.3; 4.4.4].
- 13.3.10 **Article 49** - Vastendatud erandliku edastusmehhanismi tõendusmaterjalile ja erandi heakskiitmisele, kui kasutatakse konkreetse olukorra erandeid. Addressed by clauses [4.2.1; 4.2.2; 9.1.3].

13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 5.6; Clause 5.10; Clause 5.12** - Vastendatud avalikustamise piiramisele, vastutuspõhisele edastamise juhtimisele, edastamise vastavuse tõendusmaterjalile, läbivaatamisele ja parandusmeetmetele. Addressed by clauses [4.1.2; 4.1.5; 4.3.5; 4.4.1; 4.5.1; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

- 13.5.1 **Annex A.7** - Vastendatud edastamise kaitsele, avalikustamise piiramisele, edastamise kaitsemeetmete tõendusmaterjalile, edasiedastamise kontrollile ja peatamisele, kui edastamise kaitsemeetmed puuduvad või ei kehti. Addressed by clauses [4.2.1; 4.3.2; 4.3.3; 4.4.1; 4.5.3; 7.1.4].