| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sisestage siia registreeritud juriidilise isiku nimi | | | | | | |
| Dokumendi number:<br>P17 | | | | | Dokumendi pealkiri:<br>**Andmekaitse ja privaatsuspoliitika** | | | | | | |
| Versioon:<br>1.0 | | Jõustumiskuupäev:<br>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** |
| | | | |
| | | | |

Kooskõla standardite ja regulatsioonidega

| Standard/õigusnorm | Punkt/artikkel | Kommentaar |
|---|---|---|
| ISO/IEC 27001:2022 | Punktid 5.1, 6.1.3, 8.1, 10 | Asjakohased üldised, tehnilised ning pideva täiustamise ja andmekaitse kontrollimeetmed |
| ISO/IEC 27002:2022 | Kontrollimeetmed 5.34, 8.10, 8.11, 8.12 | Kontrollimeetmed isikut tuvastava teabe käitlemiseks, säilitamiseks, kustutamiseks, anonüümimiseks ja andmesubjekti õiguste tagamiseks |
| NIST SP 800-53 Rev.5 | AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23 | Juhtimise, riskijuhtimise, juurdepääsuhalduse, logimise, rikkumiste käsitlemise ja privaatsusprogrammi nõuded |
| ELi isikuandmete kaitse üldmäärus (GDPR) | Artiklid 5, 6, 12–23, 25, 28, 30, 32–34; põhjendus 78 | Kõik põhilised privaatsuse, vastutuse, andmesubjekti õiguste, andmesubjekti taotluste, rikkumiste ning kavandatud ja vaikimisi andmekaitse põhimõtted |
| ELi NIS2 direktiiv | Artikkel 21(2)(e), (f) | Riskipõhised turbekontrollid olulistele ja tähtsatele üksustele |
| ELi DORA määrus | Artiklid 6(2)(d), 11(1)(c), 15(1), 17 | Juhtimise, kolmanda osapoole riski ja turvalise töötlemise nõuded |
| COBIT 2019 | APO12, DSS01, DSS05, MEA | Riskijuhtimine, turvalised operatsioonid, vastavuse järelevalve |

## 1. Eesmärk

1.1 Käesolev poliitika kehtestab kohustuslikud organisatsioonilised põhimõtted ja tehnilised nõuded isikuandmete kaitseks ning kavandatud andmekaitse rakendamiseks kõigis keskkondades.

1.2 Käesolev poliitika formaliseerib ettevõtte kohustused rahvusvaheliste standardite ja regulatiivsete raamistike alusel, tagades, et isikuandmeid kogutakse, töödeldakse, säilitatakse, jagatakse ja kõrvaldatakse õiguspäraselt, turvaliselt ning läbipaistvalt.

1.3 Käesolev poliitika tugevdab ka vastavust kohaldatavatele andmekaitsealastele õigusnormidele ja raamistikele, sealhulgas ELi isikuandmete kaitse üldmäärusele (GDPR), ELi NIS2 direktiivile, ELi digitaalset tegevuskerksust käsitlevale määrusele (DORA), standardile ISO/IEC 27001:2022 ja COBIT 2019-le.

## 2. Kohaldamisala

**2.1 Käesolev poliitika kehtib kõigile organisatsiooni üksustele, töötajatele ja süsteemidele, mis osalevad isikuandmete töötlemises, sealhulgas järgmisele:**

2.1.1 töötajad, töövõtjad, konsultandid ja kolmandatest osapooltest teenuseosutajad;

2.1.2 sise- ja välistest allikatest kogutud andmed kõigis ärifunktsioonides;

2.1.3 füüsilised ja digitaalsed andmekandjad, sealhulgas pilveteenused, SaaS-platvormid, mobiilsed seadmed ja paberkandjal dokumendid;

2.1.4 kõik keskkonnad, sealhulgas tootmis-, arendus-, test- ja varundussüsteemid, kus võib esineda isikuandmeid.

**2.2 Poliitika hõlmab kõiki kohaldatavate andmekaitsealaste õigusnormide ja standardite kohaldamisalasse kuuluvaid töötlemistoiminguid, sealhulgas, kuid mitte ainult:**

2.2.1 isikuandmete kogumine, säilitamine, kasutamine, edastamine ja kõrvaldamine;

2.2.2 andmesubjekti õiguste tagamine, õigusliku aluse dokumenteerimine ja nõusolekute haldamine;

2.2.3 piiriülene edastamine, rikkumistest teavitamine ja andmete jagamine kolmandate osapooltega;

2.2.4 kavandatud ja vaikimisi andmekaitse rakendamine süsteemides ja protsessides.

## 3. Eesmärgid

3.1 Tagada isikuandmete õiguspärane, läbipaistev ja vastutustundlik töötlemine kooskõlas standardiga ISO/IEC 27001:2022 ja seotud õiguslike kohustustega.

3.2 Rakendada kavandatud ja vaikimisi andmekaitse põhimõtteid kõigis infosüsteemides, teenustes ja äriprotsessides.

3.3 Rakendada tehnilised ja korralduslikud meetmed (TOM-id), mis kaitsevad isikuandmete konfidentsiaalsust, terviklust ja käideldavust kogu nende elutsükli jooksul.

3.4 Määratleda andmekaitse juhtimisrollid ja vastutusstruktuurid, sealhulgas andmekaitseametniku, infoturbe, õigusfunktsiooni ja andmeomanike vastutus.

3.5 Tagada täielik vastavus GDPR-i artiklitele 5, 6, 25, 30 ja 32 ning NIS2 ja DORA kohastele riskide maandamise ja toimepidevuse nõuetele.

3.6 Tagada andmesubjekti õigused, sealhulgas õigus tutvuda andmetega, andmete parandamine, kustutamine, töötlemise piiramine, andmete ülekantavus, vastuväidete esitamine ning kaitse automatiseeritud otsuste tegemise eest.

3.7 Maandada regulatiivseid, maine-, õiguslikke ja operatiivseid riske, mis tulenevad isikuandmete loata juurdepääsust, väärkasutusest või kaost.

## 4. Rollid ja vastutused

### 4.1 Tippjuhtkond

4.1.1 Tagab strateegilise järelevalve ja eraldab piisavad ressursid privaatsusprogrammi toetamiseks.

4.1.2 Kinnitab käesoleva poliitika ja tagab selle rakendamise kogu organisatsioonis.

### 4.2 Andmekaitseametnik

4.2.1 Tegutseb sõltumatult, et teha järelevalvet andmekaitsenõuetele vastavuse üle.

4.2.2 Hoiab GDPR-i artikli 30 kohast töötlemistoimingute registrit (RoPA).

4.2.3 Juhib suhtlust järelevalveasutustega, viib läbi andmekaitsealaseid mõjuhindamisi (DPIA-d) ja haldab rikkumistest teavitamise protsesse.

4.2.4 Vaatab läbi privaatsuserandid ja peab privaatsuserandite registrit.

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

## 9. Läbivaatamise ja ajakohastamise nõuded

### 9.1 Käesolev poliitika tuleb läbi vaadata vähemalt kord aastas või varem järgmistel juhtudel:

9.1.1 olulised õiguslikud või regulatiivsed muudatused (nt GDPR-i muudatused, DORA tähtajad);

9.1.2 uued süsteemid või töötlemistoimingud, mis hõlmavad isikuandmeid;

9.1.3 siseauditi leiud, mis viitavad puudustele poliitikas;

9.1.4 oluline rikkumine või järelevalveasutuse tagasiside.

### 9.2 Läbivaatamise vastutus

9.2.1 Andmekaitseametnik algatab poliitika läbivaatamise, koordineerides tegevusi õigus- ja vastavusfunktsiooni, riskijuhtimise, infoturbe ja tippjuhtkonnaga.

9.2.2 Kõik ajakohastused tuleb registreerida ISMS-i dokumendihalduse registris ja edastada mõjutatud sidusrühmadele.

**9.3 Muudatuste kontroll**

9.3.1 Kõik käesoleva poliitika muudatused peab formaalselt kinnitama tippjuhtkond.

9.3.2 Kehtetud versioonid tuleb turvaliselt arhiveerida ning ajakohastatud versioon peab sisaldama dokumenteeritud muudatuste ajalugu.

## 10. Seotud poliitikad ja seosed

10.1 P1 – Infoturbepoliitika. Määratleb üldised turbejuhtimise põhimõtted, millele käesolev andmekaitsepoliitika tugineb. P1 toetab isikuandmete konfidentsiaalsust, terviklust ja käideldavust kõigis süsteemides ja teenustes.

10.2 P6 – Riskijuhtimise poliitika. Määratleb organisatsiooni riskikäsitluse metoodika, mis on vajalik andmekaitseriskide, andmekaitsealaste mõjuhindamiste ja GDPR-i ning ISO/IEC 27001 punkti 6.1.3 alusel nõutavate jääkriski hinnangute tegemiseks.

10.3 P13 – Andmete klassifitseerimise ja märgistamise poliitika. Annab suunised isikuandmete ja tundlike andmete kategoriseerimiseks ning loob aluse asjakohaste andmekaitse kontrollimeetmete rakendamiseks, sealhulgas säilitamise jõustamiseks, juurdepääsu piiramiseks ja turvaliseks kõrvaldamiseks.

10.4 P14 – Andmete säilitamise ja kõrvaldamise poliitika. Toetab otseselt GDPR-i artikli 5 lõike 1 punkti e ja artikli 17 kohaseid andmekaitsenõudeid, tagades, et isikuandmeid säilitatakse ainult nii kaua, kui see on vajalik, ning kõrvaldatakse turvaliselt kooskõlas õiguslike kohustustega.

10.5 P16 – Andmete maskeerimise ja pseudonüümimise poliitika. Kehtestab kontrollimeetmed isikuandmete tuvastatavuse vähendamiseks tehniliste meetmete abil, nagu tokeniseerimine, dünaamiline maskeerimine ja pseudonüümimine, tagades seeläbi GDPR-i artikli 32 ja ISO/IEC 27002 kontrollimeetme 5.34 täitmise.

10.6 P30 – Intsidentidele reageerimise poliitika (P30). Määratleb kohustuslikud rikkumistele reageerimise protokollid, mis on kooskõlas GDPR-i artiklite 33 ja 34 alusel nõutavate andmekaitserikkumiste käsitlemise ja teavitamise tähtaegadega.

10.7 P33 – Auditi ja vastavuse seire poliitika. Rakendab planeeritud hindamised andmekaitseprogrammi tõhususe, poliitika rakendamise ja parandusmeetmete jälgimise kohta organisatsiooni üksustes ja kolmandatest osapooltest volitatud töötlejate puhul.

## 11. Viitestandardid ja raamistikud

**11.1 ISO/IEC 27001**

11.1.1 Punkt 5.1 – Juhtimine ja pühendumine: määratleb tippjuhtkonna vastutuse isikuandmete kaitsmisel ja andmekaitsepõhimõtete rakendamisel.

11.1.2 Punkt 6.1.3 – Infoturbe riskijuhtimine: toetab andmekaitseriskide tuvastamist, hindamist ja käsitlemist andmekaitsealaste mõjuhindamiste ning erandite kaudu.

11.1.3 Punkt 8.1 – Operatiivne planeerimine ja kontroll: nõuab tehnilisi ja protseduurilisi kaitsemeetmeid, et tagada isikuandmete turvaline töötlemine.

11.1.4 Punkt 10.1 – Pidev täiustamine: nõuab andmekaitseprogrammi perioodilist hindamist ja kohandamist.

11.2 ISO/IEC 27002:2022 kontrollimeetmed 5.34, 8.10, 8.11, 8.12: annavad suunised isikut tuvastava teabe käitlemiseks ning säilitamise, kustutamise, anonüümimise ja andmesubjekti õiguste läbipaistvuse tagamiseks.

**11.3 NIST SP 800-53 Rev.5**

11.3.1 AR-1, AR-2, AR-4, AR-5: määratlevad juhtimise, rollid, vastutuse ja andmekaitsealase koolituse kohustused.

11.3.2 PL-2, PL-8: nõuavad andmekaitse kontrollimeetmete integreerimist süsteemi elutsüklisse ja ettevõtte arhitektuuri.

11.3.3 AC-2, AC-6: rakendavad vähimate õiguste põhimõtet ja kontohaldust isikuandmete kaitseks.

11.3.4 AU-2, AU-6, AU-9: nõuavad logimist, jälgitavust ja auditi tervikluse tagamist isikuandmetele juurdepääsu korral.

11.3.5 IR-4, IR-5, IR-6: määratlevad struktureeritud tuvastamise, analüüsi ja teavitamise protsessid andmekaitserikkumiste korral.

11.3.6 PM-1, PM-21, PM-23: loovad tervikliku andmekaitseprogrammi, mis on kooskõlas strateegilise riski ja andmehalduse eesmärkidega.

**11.4 ELi GDPR (2016/679)**

11.4.1 Artiklid 5, 6, 12–23, 25, 28, 30, 32–34: reguleerivad õiguspärast töötlemist, eesmärgi piirangut, andmesubjekti õigusi, vastutust, kavandatud ja vaikimisi andmekaitset, kolmandate osapoolte kohustusi ning rikkumiste käsitlemist.

11.4.2 Põhjendus 78: tugevdab kavandatud andmekaitse põhimõtteid.

**11.5 ELi NIS2 direktiiv (2022/2555)**

11.5.1 Artikkel 21(2)(e) ja (f): nõuab riskipõhiste turbekontrollide rakendamist ja isikuandmete kaitset oluliste ja tähtsate üksuste kohaldamisalas.

**11.6 ELi DORA (2022/2554)**

11.6.1 Artikkel 6(2)(d): kehtestab andmekäitlusega seotud IKT-riskide sisemise juhtimise nõuded.

11.6.2 Artikkel 11(1)(c): nõuab andmetega seotud teenuste kolmanda osapoole riskide järelevalvet.

11.6.3 Artiklid 15(1) ja 17: nõuavad teenuseosutajate turvalist andmetöötlust ja õigeaegset teavitamist järelevalveasutustele IKT-ga seotud intsidentide järel.

**11.7 COBIT 2019**

11.7.1 APO12 – Riskijuhtimine: lõimib andmekaitseriski laiemasse ettevõtte riskijuhtimise järelevalvesse.

11.7.2 DSS01 – Hallatud operatsioonid ja DSS05 – Turvateenused: tagavad turvalised operatsioonid, sealhulgas juurdepääsukontrolli, säilitamise ja süsteemi tervikluse.

11.7.3 MEA03 – Vastavuse seire: nõuab pidevat vastavuse staatuse läbivaatamist regulatiivsete ja poliitikapõhiste andmekaitsekohustuste suhtes.