GSMValve OÜ (Navirec)

Infoturbe poliitika

Dokumendi pealkiri	Infoturbe poliitika
Omanik	GSMValve OÜ (Navirec) — IT-osakond
Kinnitanud (juhtkond)	Hans Alter
Üle vaadanud (IT-juht)	Margus Paurson
Versioon	1.0
Jõustumise kuupäev	13.05.2026
Ülevaatamise tsükkel	Kord aastas või oluliste muudatuste korral

1. Eesmärk

Käesolev infoturbe poliitika sätestab põhimõtted, vastutuse ja miinimumnõuded, mida GSMValve OÜ (tegutsedes kaubamärgi Navirec all) järgib, et kaitsta töödeldava teabe konfidentsiaalsust, terviklust ja käideldavust — sealhulgas klientide ja partnerite nimel töödeldavaid isikuandmeid. Tegemist on ettevõtte kõrgeima taseme infoturbe poliitikaga, mida toetavad alusdokumendid, tehnilised standardid ja registrid.

Käesolev poliitika lähtub standardite ISO/IEC 27001:2022 ja ISO/IEC 27002:2022 asjakohastest põhimõtetest ning selle eesmärk on tõendada vastavust kohaldatavatele andmekaitseõigusaktidele, sealhulgas Euroopa Liidu isikuandmete kaitse üldmäärusele (GDPR).

2. Kohaldamisala

Käesolev poliitika kehtib järgmiste suhtes:

- Kõik töötajad, lepingupartnerid, praktikandid ja kolmandad isikud, kes tegutsevad GSMValve OÜ nimel.
- Kõik teabevarad, mis kuuluvad GSMValve OÜ-le, mida ta töötleb, säilitab või edastab mistahes vormis (digitaalselt, paberil, suuliselt).
- Kõik IT-süsteemid, rakendused, võrgud, pilveteenused ja füüsilised ruumid, mida kasutatakse Navireci teenuse osutamiseks.
- Kõik alltöötlejad ja tarnijad, kellel on juurdepääs GSMValve OÜ andmetele või süsteemidele.

3. Rollid ja vastutus

- **Juhtkond** vastutab infoturbe eest, kinnitab käesoleva poliitika ja tagab selle rakendamiseks piisavate ressursside olemasolu.
- **IT-juht (Margus Paurson)** on määratud turbeametnik, kes vastutab käesoleva poliitika ja seda toetavate kontrollimeetmete rakendamise, hooldamise ja jälgimise eest.
- **Kõik töötajad ja lepingupartnerid** vastutavad käesoleva poliitika järgimise, nõutava infoturbe teadlikkuse koolituse läbimise, oma kasutajatunnuste kaitsmise ning kahtlastest turvaintsidentidest viivitamatu teatamise eest.
- **Arendajad** vastutavad punktis 9 sätestatud turvalise arenduse nõuete järgimise eest.

4. Teabe klassifitseerimine ja käitlemine

GSMValve OÜ töödeldav teave liigitatakse avalikuks, sisemiseks, konfidentsiaalseks või isikuandmeteks. Isikuandmetele ja konfidentsiaalsele teabele on juurdepääs ainult volitatud töötajatel teadmisvajaduse alusel, neid tuleb säilitada heakskiidetud süsteemides ning neid ei tohi edastada väljapoole EL-i/EMP-d, kui puuduvad asjakohased kaitsemeetmed (näiteks Euroopa Komisjoni standardsed lepingutingimused või adekvaatsusotsus).

Kliendiandmed on rakenduse tasandil loogiliselt eraldatud. Iga klient toimib eraldi üürnikuna ning juurdepääs kliendi andmetele määratakse kliendi enda kasutajatele antud õiguste alusel; klientide andmete segunemist takistavad rakenduse tasandi juurdepääsukontrollid.

Enne mitteavaliku teabe avaldamist väljapoolsele isikule kontrollitakse vastuvõtja isikut ja volitust väljakujunenud kanali kaudu — näiteks kliendi määratud kontaktisiku, allkirjastatud juhise või varem autenditud suhtluskanali kaudu. Konfidentsiaalse teabe või isikuandmete avaldamiseks ei kasutata juhuslikke ega kontrollimata kanaleid.

5. Juurdepääsu kontroll ja autentimine

- Igal kasutajal on unikaalne isiklik konto. Jagatud kontod on keelatud.
- Juurdepääs süsteemidele ja andmetele antakse minimaalsete õiguste ja teadmisvajaduse põhimõttel ning see vaadatakse üle vähemalt kord aastas.
- Paroolid peavad vastama dokumenteeritud keerukusstandardile (minimaalne pikkus, märgivariatiivsus, levinud paroolide blokeerimine), mida platvorm rakendab.
- Kaugjuurdepääs sisemistele süsteemidele on lubatud ainult ettevõtte VPN-i kaudu, kasutades isiklikke kasutajatunnuseid.
- Töötajate liitumise, rolli muutmise ja lahkumisega seotud muudatused (konto loomine, rolli muutmine, õiguste tühistamine) tehakse viivitamatult ja dokumenteeritakse.
- Kui välised osapooled (nt IT-tugi, lepingupartnerid, tarnijad) vajavad juurdepääsu GSMValve OÜ süsteemidele, antakse juurdepääs nimelise konto alusel, see on ajaliselt piiratud, dokumenteeritud ning eeldab kirjaliku konfidentsiaalsuslepingu olemasolu. Välist juurdepääsu vaadatakse regulaarselt üle ja see tühistatakse, kui seda enam ei vajata.

6. Krüptograafia

- **Andmed edastamisel:** kogu juurdepääs Navireci teenustele ja API-dele on krüpteeritud, kasutades TLS 1.2 või uuemat versiooni. Administratiivne juurdepääs toimub krüpteeritud VPN-i kaudu.
- **Andmed puhkeolekus:** ettevõtte süsteemides säilitatavad isikuandmed on kaitstud asjakohaste tehniliste meetmetega. Ettevõtte poolt väljastatud seadmed kasutavad täisketta krüpteerimist.
- **Võtmehaldus:** krüptograafilised võtmed ja saladused hoitakse kaitstud võtmehoidlates ega ole lisatud lähtekoodi.

7. Füüsiline ja keskkonnaturve

Tootmisservereid haldab Elisa Eesti AS, peamine majutuse ja hallatava infrastruktuuri pakkuja, ning need asuvad füüsiliselt Greenergy andmekeskuses (Tallinn) — rajatises, kus on ööpäevaringne jälgitav juurdepääs, biomeetrilised ja ID-põhised sissepääsukontrollid, keskkonnakontrollid ning katkematu toiteallikas (UPS). Füüsiline juurdepääs serveririiulitele on piiratud volitatud töötajatega. Kontori töökohti kaitsevad ekraaniluku kasutamine, puhta laua põhimõte ja lukustatud hoiukohad paberdokumentide jaoks, kus see on asjakohane.

8. Käitamisturve

- **Turvapaikade ja haavatavuste haldus:** operatsioonisüsteemid, sõltuvused ja konteineritõmmised hoitakse ajakohasena. Teadaolevaid haavatavusi jälgitakse ja kõrvaldatakse vastavalt riskitasemele.
- **Pahavaratõrje:** kõikides ettevõtte poolt väljastatud seadmetes töötab heakskiidetud lõpp-punkti turvalahendus (praegu ESET Small Business Security).
- **Logimine ja jälgimine:** tootmissüsteemide turvaga seotud sündmusi logitakse tsentraalselt, kaitstakse manipuleerimise eest ning säilitatakse kohtueksperti isiks vastavalt dokumenteeritud säilitusstandardile (eesmärk: vähemalt 180 päeva turvalogide puhul).
- **Varukoopiad:** tootmisandmeid varundatakse, replikeeritakse ja taastetestitakse regulaarselt.
- **Turvaline hävitamine:** isikuandmeid või konfidentsiaalset teavet sisaldavad andmekandjad kustutatakse turvaliselt või hävitatakse enne taaskasutust või kõrvaldamist.

9. Turvaline tarkvaraarendus

- Arendus-, testimis- ja tootmiskeskkonnad on loogiliselt eraldatud.

- Arendajatel puudub otsene kirjutusõigus tootmiskeskkonda; kõik muudatused läbivad kontrollitud muudatuste haldamise protsessi, mis hõlmab ülevaatust, testimist ja tagasipööramise võimalust.
- Arendusprotsess käsitleb vähemalt kehtivaid OWASP Top 10 riske (nt süstimisrünnakud, puudulik juurdepääsukontroll, vale turvakonfiguratsioon).
- Sõltuvusi kontrollitakse teadaolevate haavatavuste suhtes; uuendused rakendatakse regulaarse väljalasketsükli osana.

10. Tarnijate ja alltöötlejate turvalisus

Tarnijate ja alltöötlejate suhtes, kes töötlevad isikuandmeid GSMValve OÜ nimel, kehtib kirjalik andmetöötlusleping ning vajaduse korral Euroopa Liidu standardsed lepingutingimused. Ajakohast alltöötlejate loetelu hoitakse ja see esitatakse klientidele nõudmisel.

11. Intsidentide haldus

Kõik töötajad ja lepingupartnerid on kohustatud teatama igast kahtlustatavast või kinnitatud turvaintsidendist IT-juhile viivitamatult. Intsidendid registreeritakse, piiratakse, uuritakse ja kõrvaldatakse ning saadud õppetunnid kajastuvad käesolevas poliitikas ja seda toetavates protseduurides. Isikuandmetega seotud rikkumistest, mis võivad tõenäoliselt kaasa tuua riski andmesubjektidele, teatatakse pädevale andmekaitseasutusele 72 tunni jooksul ning mõjutatud kliente (vastutavaid töötlejaid) teavitatakse vastavalt lepingulistele kohustustele.

12. Äritegevuse jätkuvus ja taastumine

GSMValve OÜ rakendab äritegevuse jätkuvuse ja katastroofijärgse taastumise korda, mis on vastavuses ettevõtte tegevusega kaasnevate riskidega, sealhulgas andmete replikeerimine, UPS-iga kaitstud majutus ja regulaarne taastetestimine. Jätkuvuskorda vaadatakse üle ja testitakse regulaarselt ning seda uuendatakse oluliste muudatuste korral.

13. Personaliturve, teadlikkus ja koolitus

Enne süsteemidele või isikuandmetele juurdepääsu andmist läbivad kandidaadid isikusamasuse kontrolli ning vajaduse korral, sõltuvalt ametikohast, soovituste ja tausta kontrolli. Töö- ja käsunduslepingud sisaldavad kirjalikke konfidentsiaalsus- ja infoturbekohustusi, mis jõustuvad juurdepääsu esimesel päeval ja kehtivad ka pärast lepingu lõppemist.

Kõik isikuandmetele juurdepääsu omavad töötajad läbivad infoturbe teadlikkuse koolituse tööle asudes ning seejärel vähemalt kord aastas. Koolitus hõlmab lubatud kasutust, paroolide ja kasutajatunnuste hügieeni, andmepüüki, andmete käitlemise reegleid, turvalist kaugtööd ning turvaintsidentide äratundmist ja neist teatamist.

14. Konfidentsiaalsus

Kõik töötajad ja lepingupartnerid on seotud kirjalike konfidentsiaalsuskohustustega, mis hõlmavad kliendi- ja isikuandmeid. Need kohustused kehtivad ka pärast töö- või lepingusuhte lõppemist.

15. Vastavus, audit ja ülevaatamine

Käesoleva poliitika täitmist jälgib IT-juht. Kliendiandmeid mõjutavate turvaga seotud toimingute kohta säilitatakse manipuleerimiskindlaid auditijälgi, mis on kaitstud loata muutmise või kustutamise eest.

Lisaks poliitika iga-aastasele ülevaatamisele teeb IT-juht perioodilisi pistelisi kontrolle juurdepääsulogide, kontoõiguste, muudatuste halduse dokumentide ja varundamise-taastamise tõendite üle, et kinnitada turvakontrollide nõuetekohast toimimist. Nende kontrollide tulemused registreeritakse ning vajalikud parandusmeetmed viiakse lõpuni ja neid jälgitakse.

Poliitika ja seda toetavad kontrollimeetmed vaadatakse üle vähemalt kord aastas, pärast igat olulist intsidenti ning tehnoloogias, organisatsioonis või kohaldatavas õigusaktis toimuvate oluliste muudatuste korral. Käesoleva poliitika rikkumine võib kaasa tuua distsiplinaarmeetmed, sealhulgas töösuhte lõpetamise, ning lepingupartnerite puhul koostöö lõpetamise.

16. Kinnitamine

Käesoleva infoturbe poliitika on kinnitanud GSMValve OÜ juhtkond ning see jõustub allpool märgitud kuupäeval.

Roll	Nimi	Allkiri / Kuupäev
Kinnitanud (juhtkond)	Hans Alter	*digitaalselt allkirjastatud*
Üle vaadanud (IT-juht)	Margus Paurson	*digitaalselt allkirjastatud*