GSMValve OÜ (Navirec)

Informācijas drošības politika

Dokumenta nosaukums	Informācijas drošības politika
Īpašnieks	GSMValve OÜ (Navirec) — IT nodaļa
Apstiprinājis (vadība)	Hans Alter
Pārskatījis (IT vadītājs)	Margus Paurson
Versija	1.0
Spēkā stāšanās datums	13.05.2026
Pārskatīšanas cikls	Reizi gadā vai būtisku izmaiņu gadījumā

1. Mērķis

Šī informācijas drošības politika nosaka principus, atbildību un minimālās prasības, kuras ievēro GSMValve OÜ (darbojoties ar preču zīmi Navirec), lai aizsargātu tās apstrādātās informācijas konfidencialitāti, integritāti un pieejamību — tostarp klientu un partneru vārdā apstrādātos personas datus. Šī ir uzņēmuma augstākā līmeņa informācijas drošības politika, kuru atbalsta pamatā esošās procedūras, tehniskie standarti un ieraksti.

Šī politika ir saskaņota ar attiecīgajiem ISO/IEC 27001:2022 un ISO/IEC 27002:2022 principiem, un tās mērķis ir apliecināt atbilstību piemērojamajiem datu aizsardzības tiesību aktiem, tostarp Eiropas Savienības Vispārīgajai datu aizsardzības regulai (VDAR).

2. Darbības joma

Šī politika attiecas uz:

- Visiem darbiniekiem, līgumdarbiniekiem, praktikantiem un trešajām personām, kas darbojas GSMValve OÜ vārdā.
- Visiem informācijas aktīviem, kas pieder GSMValve OÜ vai kurus tā apstrādā, glabā vai pārraida jebkurā formātā (digitālā, papīra, mutiskā).
- Visām IT sistēmām, lietojumprogrammām, tīkliem, mākoņpakalpojumiem un fiziskajām telpām, kas tiek izmantotas Navirec pakalpojuma nodrošināšanai.
- Visiem apakšapstrādātājiem un piegādātājiem, kuriem ir piekļuve GSMValve OÜ datiem vai sistēmām.

3. Lomas un atbildība

- **Vadība** ir atbildīga par informācijas drošību, apstiprina šo politiku un nodrošina pietiekamu resursu pieejamību.
- **IT vadītājs (Margus Paurson)** ir norīkotā drošības amatpersona, kas atbild par šīs politikas un to atbalstošo kontroles pasākumu ieviešanu, uzturēšanu un uzraudzību.
- **Visi darbinieki un līgumdarbinieki** ir atbildīgi par šīs politikas ievērošanu, nepieciešamo drošības izpratnes apmācību pabeigšanu, savu piekļuves datu aizsardzību un aizdomīgu drošības incidentu nekavējošu ziņošanu.
- **Izstrādātāji** ir atbildīgi par 9. sadaļā noteikto drošas izstrādes prasību ievērošanu.

4. Informācijas klasifikācija un apstrāde

GSMValve OÜ apstrādātā informācija tiek klasificēta kā publiska, iekšēja, konfidenciāla vai personas dati. Personas datiem un konfidenciālai informācijai drīkst piekļūt tikai pilnvaroti darbinieki, ievērojot nepieciešamības principu, tie jāglabā apstiprinātās sistēmās un tos nedrīkst nodot ārpus ES/EEZ, ja vien nav ieviesti atbilstoši aizsardzības pasākumi (piemēram, standarta līguma klauzulas vai lēmums par pietiekamības līmeni).

Klientu dati ir loģiski nodalīti lietojumprogrammas līmenī. Katrs klients darbojas kā atsevišķs īrnieks, un piekļuvi klienta datiem nosaka tiesības, kas piešķirtas attiecīgā klienta lietotājiem; datu sajaukšanos starp klientiem novērš lietojumprogrammas līmeņa piekļuves kontroles pasākumi.

Pirms jebkādas nepubliskas informācijas izpaušanas ārējai personai tiek pārbaudīta saņēmēja identitāte un pilnvarojums, izmantojot iedibinātu kanālu — piemēram, klienta norīkoto kontaktpersonu, parakstītu norādījumu vai iepriekš autentificētu saziņas kanālu. Konfidenciālas informācijas vai personas datu izpaušanai netiek izmantoti nejauši vai nepārbaudīti kanāli.

5. Piekļuves kontrole un autentifikācija

- Katram lietotājam ir unikāls personiskais konts. Koplietošanas konti ir aizliegti.
- Piekļuve sistēmām un datiem tiek piešķirta, ievērojot mazāko privilēģiju un nepieciešamības principu, un tiek pārskatīta vismaz reizi gadā.
- Parolēm jāatbilst dokumentētam sarežģītības standartam (minimālais garums, rakstzīmju daudzveidība, izplatītu paroļu bloķēšana), un to ievērošanu nodrošina platforma.
- Attālināta piekļuve iekšējām sistēmām ir atļauta tikai, izmantojot uzņēmuma VPN un personiskos piekļuves datus.
- Ar darbinieku pievienošanos, lomas maiņu un aiziešanu saistītas izmaiņas (konta izveide, lomas maiņa, tiesību atsaukšana) tiek veiktas nekavējoties un dokumentētas.
- Ja ārējām personām (piemēram, IT atbalstam, līgumdarbiniekiem, piegādātājiem) ir nepieciešama piekļuve GSMValve OÜ sistēmām, piekļuve tiek piešķirta uz vārdā piesaistīta konta pamata, tā ir laika ziņā ierobežota, tiek dokumentēta un ir atkarīga no rakstiska konfidencialitātes līguma esamības. Ārējā piekļuve tiek regulāri pārskatīta un atsaukta, kad tā vairs nav nepieciešama.

6. Kriptogrāfija

- **Dati pārraides laikā:** visa piekļuve Navirec pakalpojumiem un API tiek šifrēta, izmantojot TLS 1.2 vai jaunāku versiju. Administratīvā piekļuve notiek, izmantojot šifrētu VPN.
- **Dati miera stāvoklī:** uzņēmuma sistēmās glabātie personas dati tiek aizsargāti ar atbilstošiem tehniskiem pasākumiem. Uzņēmuma izsniegtajās galiekārtās tiek izmantota pilna diska šifrēšana.
- **Atslēgu pārvaldība:** kriptogrāfiskās atslēgas un noslēpumi tiek glabāti aizsargātās atslēgu glabātuvēs un netiek iekļauti pirmkodā.

7. Fiziskā un vides drošība

Ražošanas serverus uztur Elisa Eesti AS, galvenais mitināšanas un pārvaldītās infrastruktūras nodrošinātājs, un tie fiziski atrodas Greenergy datu centrā (Tallinā) — objektā ar visu diennakti uzraudzītu piekļuvi, biometriskajām un ID balstītajām ieejas kontrolēm, vides kontroles pasākumiem un nepārtrauktās barošanas avotu (UPS). Fiziska piekļuve serveru statīviem ir ierobežota tikai pilnvarotam personālam. Biroja darbstacijas tiek aizsargātas, izmantojot ekrāna bloķēšanu, tīra galda praksi un slēdzamas glabātuves papīra dokumentiem, kur tas ir piemērojams.

8. Darbības drošība

- **Ielāpu un ievainojamību pārvaldība:** operētājsistēmas, atkarības un konteineru attēli tiek uzturēti atjauninātā stāvoklī. Zināmās ievainojamības tiek izsekotas un novērstas atbilstoši riska līmenim.
- **Aizsardzība pret ļaunprogrammatūru:** visās uzņēmuma izsniegtajās galiekārtās darbojas apstiprināts galiekārtu drošības risinājums (pašlaik ESET Small Business Security).
- **Žurnalēšana un uzraudzība:** ar drošību saistīti notikumi no ražošanas sistēmām tiek centralizēti reģistrēti, aizsargāti pret neatļautu labošanu un glabāti kriminālistiskajai analīzei atbilstoši dokumentētajam glabāšanas standartam (mērķis: vismaz 180 dienas drošības žurnāliem).
- **Rezerves kopijas:** ražošanas dati tiek regulāri dublēti, replicēti un tiek testēta to atjaunošana.
- **Droša iznīcināšana:** datu nesēji, kas satur personas datus vai konfidenciālu informāciju, tiek droši dzēsti vai iznīcināti pirms atkārtotas izmantošanas vai likvidēšanas.

9. Droša programmatūras izstrāde

- Izstrādes, testēšanas un ražošanas vides ir loģiski nodalītas.
- Izstrādātājiem nav tiešas rakstīšanas piekļuves ražošanas videi; visas izmaiņas iziet kontrolētu izmaiņu pārvaldības procesu, kas ietver pārskatīšanu, testēšanu un iespēju atgriezties iepriekšējā stāvoklī.

- Izstrādes process risina vismaz aktuālos OWASP Top 10 riskus (piemēram, ievadīšanas uzbrukumus, nepareizu piekļuves kontroli, drošības nepareizu konfigurāciju).
- Atkarības tiek pārbaudītas attiecībā uz zināmām ievainojamībām; atjauninājumi tiek ieviesti kā daļa no regulārā izlaiduma cikla.

10. Piegādātāju un apakšapstrādātāju drošība

Uz piegādātājiem un apakšapstrādātājiem, kas apstrādā personas datus GSMValve OÜ vārdā, attiecas rakstisks datu apstrādes līgums un, ja nepieciešams, ES standarta līguma klauzulas. Tiek uzturēts aktuāls apakšapstrādātāju saraksts, kas pēc pieprasījuma tiek sniegts klientiem.

11. Incidentu pārvaldība

Visiem darbiniekiem un līgumdarbiniekiem nekavējoties jāziņo IT vadītājam par jebkuru aizdomīgu vai apstiprinātu drošības incidentu. Incidenti tiek reģistrēti, ierobežoti, izmeklēti un novērsti, un no tiem gūtā pieredze tiek atspoguļota šajā politikā un to atbalstošajās procedūrās. Par personas datu aizsardzības pārkāpumiem, kas var radīt risku datu subjektiem, 72 stundu laikā tiek ziņots attiecīgajai datu aizsardzības uzraudzības iestādei, un skartie klienti (pārziņi) tiek informēti saskaņā ar līgumiskajām saistībām.

12. Uzņēmējdarbības nepārtrauktība un avārijas atjaunošana

GSMValve OÜ uztur uzņēmējdarbības nepārtrauktības un avārijas atjaunošanas pasākumus, kas ir samērīgi ar tās darbības riskiem, tostarp datu replikāciju, UPS aizsargātu mitināšanu un periodisku atjaunošanas testēšanu. Nepārtrauktības pasākumi tiek regulāri pārskatīti un testēti, kā arī atjaunināti būtisku izmaiņu gadījumā.

13. Personāla drošība, izpratne un apmācība

Pirms piekļuves piešķiršanas sistēmām vai personas datiem kandidāti tiek pakļauti identitātes pārbaudei un, ja tas ir piemēroti amatam, ieteikumu un pagātnes pārbaudei. Darba un līgumdarbinieku līgumi ietver rakstiskas konfidencialitātes un informācijas drošības saistības, kas stājas spēkā pirmajā piekļuves dienā un paliek spēkā arī pēc darba attiecību izbeigšanas.

Visi darbinieki, kuriem ir piekļuve personas datiem, saņem drošības izpratnes apmācību darba uzsākšanas laikā un pēc tam vismaz reizi gadā. Apmācība aptver pieļaujamu lietošanu, paroļu un piekļuves datu higiēnu, pikšķerēšanu, datu apstrādes noteikumus, drošu attālināto darbu, kā arī drošības incidentu atpazīšanu un ziņošanu par tiem.

14. Konfidencialitāte

Uz visiem darbiniekiem un līgumdarbiniekiem attiecas rakstiskas konfidencialitātes saistības, kas aptver klientu un personas datus. Šīs saistības paliek spēkā arī pēc darba vai līgumattiecību izbeigšanas.

15. Atbilstība, audits un pārskatīšana

Šīs politikas ievērošanu uzrauga IT vadītājs. Ar drošību saistītām darbībām, kas ietekmē klientu datus, tiek uzturēti pret manipulācijām aizsargāti audita pieraksti, kas ir aizsargāti pret nesankcionētu grozīšanu vai dzēšanu.

Papildus ikgadējai politikas pārskatīšanai IT vadītājs veic periodiskas izlases veida pārbaudes attiecībā uz piekļuves žurnāliem, konta atļaujām, izmaiņu pārvaldības ierakstiem un rezerves kopiju atjaunošanas pierādījumiem, lai apstiprinātu, ka drošības kontroles pasākumi darbojas paredzētajā veidā. Šo pārbaužu rezultāti tiek dokumentēti, un nepieciešamie koriģējošie pasākumi tiek izsekoti līdz to pabeigšanai.

Politika un to atbalstošie kontroles pasākumi tiek pārskatīti vismaz reizi gadā, pēc jebkura būtiska incidenta, kā arī tad, kad notiek nozīmīgas izmaiņas tehnoloģijā, organizācijā vai piemērojamajā regulējumā. Šīs politikas neievērošana var izraisīt disciplināru rīcību, tostarp darba attiecību izbeigšanu, bet līgumdarbinieku gadījumā — sadarbības izbeigšanu.

16. Apstiprināšana

Šo informācijas drošības politiku ir apstiprinājusi GSMValve OÜ vadība, un tā stājas spēkā zemāk norādītajā datumā.

Loma	Vārds, uzvārds	Paraksts / Datums

Apstiprinājis (vadība)	Hans Alter	*digitāli parakstīts*
Pārskatījis (IT vadītājs)	Margus Paurson	*digitāli parakstīts*