GSMValve OÜ (Navirec)

Polityka Bezpieczeństwa Informacji

Tytuł dokumentu	Polityka Bezpieczeństwa Informacji
Właściciel	GSMValve OÜ (Navirec) — Dział IT
Zatwierdził (Zarząd)	Hans Alter
Zweryfikował (Kierownik IT)	Margus Paurson
Wersja	1.0
Data wejścia w życie	13.05.2026
Cykl przeglądu	Raz w roku lub w przypadku istotnej zmiany

1. Cel

Niniejsza Polityka Bezpieczeństwa Informacji określa zasady, obowiązki i minimalne wymagania, których przestrzega GSMValve OÜ (działająca pod marką Navirec) w celu ochrony poufności, integralności i dostępności przetwarzanych przez nią informacji — w tym danych osobowych przetwarzanych w imieniu klientów i partnerów. Jest to nadrzędna polityka bezpieczeństwa informacji spółki, wspierana przez powiązane procedury, standardy techniczne i rejestry.

Niniejsza polityka jest zgodna z odpowiednimi zasadami norm ISO/IEC 27001:2022 oraz ISO/IEC 27002:2022 i ma na celu wykazanie zgodności z obowiązującymi przepisami o ochronie danych, w tym z ogólnym rozporządzeniem o ochronie danych UE (RODO).

2. Zakres

Niniejsza polityka ma zastosowanie do:

- Wszystkich pracowników, podwykonawców, stażystów oraz osób trzecich działających w imieniu GSMValve OÜ.
- Wszystkich zasobów informacyjnych będących własnością GSMValve OÜ lub przez nią przetwarzanych, przechowywanych bądź przekazywanych w dowolnej formie (cyfrowej, papierowej, ustnej).
- Wszystkich systemów IT, aplikacji, sieci, usług chmurowych oraz obiektów fizycznych wykorzystywanych do świadczenia usługi Navirec.
- Wszystkich podwykonawców przetwarzania i dostawców posiadających dostęp do danych lub systemów GSMValve OÜ.

3. Role i odpowiedzialność

- **Zarząd** odpowiada za bezpieczeństwo informacji, zatwierdza niniejszą politykę i zapewnia dostępność wystarczających zasobów.
- **Kierownik IT (Margus Paurson)** pełni funkcję wyznaczonego oficera bezpieczeństwa, odpowiedzialnego za wdrażanie, utrzymywanie i monitorowanie niniejszej polityki oraz wspierających ją mechanizmów kontroli.
- **Wszyscy pracownicy i podwykonawcy** są odpowiedzialni za przestrzeganie niniejszej polityki, ukończenie wymaganych szkoleń z zakresu świadomości bezpieczeństwa, ochronę swoich danych dostępowych oraz niezwłoczne zgłaszanie podejrzeń wystąpienia incydentów bezpieczeństwa.
- **Deweloperzy** są odpowiedzialni za przestrzeganie wymogów bezpiecznego tworzenia oprogramowania określonych w punkcie 9.

4. Klasyfikacja i przetwarzanie informacji

Informacje przetwarzane przez GSMValve OÜ są klasyfikowane jako publiczne, wewnętrzne, poufne lub dane osobowe. Dostęp do danych osobowych i informacji poufnych mogą mieć wyłącznie upoważnieni pracownicy, zgodnie z zasadą wiedzy koniecznej; informacje te muszą być przechowywane w zatwierdzonych systemach i nie mogą być przekazywane

poza obszar UE/EOG, chyba że wdrożono odpowiednie zabezpieczenia (takie jak standardowe klauzule umowne lub decyzja stwierdzająca odpowiedni stopień ochrony).

Dane klientów są logicznie odseparowane na poziomie warstwy aplikacji. Każdy klient funkcjonuje jako odrębny najemca, a dostęp do danych klienta jest determinowany przez uprawnienia nadane użytkownikom tego klienta; mieszanie się danych pomiędzy klientami jest uniemożliwione przez mechanizmy kontroli dostępu na poziomie aplikacji.

Przed ujawnieniem jakichkolwiek informacji niepublicznych podmiotowi zewnętrznemu weryfikowana jest tożsamość i uprawnienia odbiorcy za pośrednictwem ustalonego kanału — na przykład wyznaczonej osoby kontaktowej klienta, podpisanego polecenia lub uprzednio uwierzytelnionego kanału komunikacji. Do ujawniania informacji poufnych lub danych osobowych nie wykorzystuje się kanałów przypadkowych ani niezweryfikowanych.

5. Kontrola dostępu i uwierzytelnianie

- Każdy użytkownik posiada unikalne, indywidualne konto. Konta współdzielone są zabronione.
- Dostęp do systemów i danych jest przyznawany zgodnie z zasadą najmniejszych uprawnień i wiedzy koniecznej oraz jest weryfikowany co najmniej raz w roku.
- Hasła muszą spełniać udokumentowany standard złożoności (minimalna długość, różnorodność znaków, blokowanie popularnych haseł), którego przestrzeganie wymusza platforma.
- Zdalny dostęp do systemów wewnętrznych jest dozwolony wyłącznie za pośrednictwem firmowej sieci VPN, przy użyciu indywidualnych danych dostępowych.
- Zmiany związane z zatrudnieniem, zmianą stanowiska oraz odejściem pracownika (utworzenie konta, zmiana roli, odebranie uprawnień) są przeprowadzane niezwłocznie i dokumentowane.
- Jeżeli podmioty zewnętrzne (np. wsparcie IT, podwykonawcy, dostawcy) wymagają dostępu do systemów GSMValve OÜ, dostęp jest przyznawany na podstawie imiennego konta, ograniczony czasowo, rejestrowany oraz uzależniony od zawarcia pisemnej umowy o zachowaniu poufności. Dostęp zewnętrzny jest regularnie weryfikowany i cofany, gdy przestaje być potrzebny.

6. Kryptografia

- **Dane w tranzycie:** cały dostęp do usług i API Navirec jest szyfrowany przy użyciu protokołu TLS 1.2 lub wyższego. Dostęp administracyjny odbywa się za pośrednictwem szyfrowanego połączenia VPN.
- **Dane w spoczynku:** dane osobowe przechowywane w systemach spółki są chronione odpowiednimi zabezpieczeniami technicznymi. Urządzenia końcowe wydawane przez spółkę wykorzystują szyfrowanie całego dysku.
- **Zarządzanie kluczami:** klucze kryptograficzne i inne poufne dane są przechowywane w zabezpieczonych magazynach kluczy i nie są umieszczane w kodzie źródłowym.

7. Bezpieczeństwo fizyczne i środowiskowe

Serwery produkcyjne są obsługiwane przez Elisa Eesti AS, głównego dostawcę hostingu i zarządzanej infrastruktury, i znajdują się fizycznie w centrum danych Greenergy (Tallin) — obiekcie z całodobowo monitorowanym dostępem, kontrolą wejścia opartą na biometrii i identyfikatorach, kontrolą warunków środowiskowych oraz zasilaniem awaryjnym (UPS). Fizyczny dostęp do szaf serwerowych jest ograniczony do upoważnionego personelu. Stacje robocze w biurze są chronione poprzez blokowanie ekranu, zasadę czystego biurka oraz zamykane miejsca przechowywania dokumentów papierowych, tam gdzie ma to zastosowanie.

8. Bezpieczeństwo operacyjne

- **Zarządzanie poprawkami i podatnościami:** systemy operacyjne, zależności oraz obrazy kontenerów są utrzymywane w aktualnym stanie. Znane podatności są monitorowane i usuwane zgodnie z poziomem ryzyka.
- **Ochrona przed złośliwym oprogramowaniem:** wszystkie urządzenia końcowe wydawane przez spółkę korzystają z zatwierdzonego rozwiązania ochrony punktów końcowych (obecnie ESET Small Business Security).
- **Rejestrowanie zdarzeń i monitorowanie:** zdarzenia istotne dla bezpieczeństwa pochodzące z systemów produkcyjnych są rejestrowane centralnie, chronione przed manipulacją i przechowywane do celów analizy

śledczej zgodnie z udokumentowanym standardem retencji (cel: co najmniej 180 dni dla dzienników bezpieczeństwa).

- **Kopie zapasowe:** dane produkcyjne są regularnie archiwizowane, replikowane, a proces ich odtwarzania jest cyklicznie testowany.
- **Bezpieczne niszczenie danych:** nośniki danych zawierające dane osobowe lub informacje poufne są bezpiecznie usuwane lub niszczone przed ponownym użyciem lub utylizacją.

9. Bezpieczne tworzenie oprogramowania

- Środowiska programistyczne, testowe i produkcyjne są logicznie rozdzielone.
- Deweloperzy nie posiadają bezpośredniego dostępu do zapisu w środowisku produkcyjnym; wszystkie zmiany przechodzą przez kontrolowany proces zarządzania zmianą, obejmujący przegląd, testowanie oraz możliwość wycofania zmian.
- Proces programistyczny uwzględnia co najmniej aktualne ryzyka z listy OWASP Top 10 (np. ataki iniekcyjne, nieprawidłową kontrolę dostępu, błędną konfigurację zabezpieczeń).
- Zależności są weryfikowane pod kątem znanych podatności; aktualizacje są wdrażane w ramach regularnego cyklu wydawniczego.

10. Bezpieczeństwo dostawców i podwykonawców przetwarzania

Dostawcy i podwykonawcy przetwarzający dane osobowe w imieniu GSMValve OÜ podlegają pisemnej umowie powierzenia przetwarzania danych oraz, w stosownych przypadkach, standardowym klauzulom umownym UE. Prowadzona jest aktualna lista podwykonawców przetwarzania, która jest udostępniana klientom na żądanie.

11. Zarządzanie incydentami

Wszyscy pracownicy i podwykonawcy są zobowiązani niezwłocznie zgłaszać Kierownikowi IT wszelkie podejrzewane lub potwierdzone incydenty bezpieczeństwa. Incydenty są rejestrowane, ograniczane, badane i usuwane, a wnioski z nich wyciągane są uwzględniane w niniejszej polityce oraz wspierających ją procedurach. Naruszenia ochrony danych osobowych, które mogą powodować ryzyko dla osób, których dane dotyczą, są zgłaszane właściwemu organowi nadzorczemu ds. ochrony danych w ciągu 72 godzin, a dotknięci klienci (administratorzy danych) są informowani zgodnie ze zobowiązaniami umownymi.

12. Ciągłość działania i odzyskiwanie po awarii

GSMValve OÜ utrzymuje mechanizmy zapewnienia ciągłości działania i odzyskiwania po awarii proporcjonalne do ryzyk związanych z jej działalnością, obejmujące replikację danych, hosting zabezpieczony zasilaniem awaryjnym (UPS) oraz okresowe testowanie procesu odtwarzania. Mechanizmy zapewnienia ciągłości są regularnie przeglądane i testowane oraz aktualizowane w przypadku istotnych zmian.

13. Bezpieczeństwo, świadomość i szkolenia personelu

Przed przyznaniem dostępu do systemów lub danych osobowych kandydaci przechodzą weryfikację tożsamości, a jeśli jest to odpowiednie dla danego stanowiska — również weryfikację referencji oraz przeszłości. Umowy o pracę i umowy z podwykonawcami zawierają pisemne zobowiązania dotyczące poufności i bezpieczeństwa informacji, które wchodzą w życie w pierwszym dniu uzyskania dostępu i pozostają w mocy po zakończeniu współpracy.

Cały personel posiadający dostęp do danych osobowych przechodzi szkolenie z zakresu świadomości bezpieczeństwa podczas wdrożenia oraz co najmniej raz w roku w kolejnych latach. Szkolenie obejmuje dopuszczalne korzystanie z zasobów, higienę haseł i danych dostępowych, phishing, zasady przetwarzania danych, bezpieczną pracę zdalną oraz sposoby rozpoznawania i zgłaszania incydentów bezpieczeństwa.

14. Poufność

Wszyscy pracownicy i podwykonawcy są związani pisemnymi zobowiązaniami do zachowania poufności obejmującymi dane klientów oraz dane osobowe. Zobowiązania te pozostają w mocy również po zakończeniu stosunku pracy lub współpracy.

15. Zgodność, audyt i przegląd

Przestrzeganie niniejszej polityki jest monitorowane przez Kierownika IT. Dla działań istotnych dla bezpieczeństwa, mających wpływ na dane klientów, prowadzone są dzienniki audytowe odporne na manipulację, chronione przed nieuprawnioną modyfikacją lub usunięciem.

Oprócz corocznego przeglądu polityki, Kierownik IT przeprowadza okresowe, wyrywkowe kontrole dzienników dostępu, uprawnień kont, zapisów zarządzania zmianą oraz dowodów odtwarzania kopii zapasowych, aby potwierdzić, że mechanizmy kontroli bezpieczeństwa działają zgodnie z założeniami. Wyniki tych kontroli są dokumentowane, a wymagane działania naprawcze są monitorowane aż do ich zakończenia.

Polityka oraz wspierające ją mechanizmy kontroli są przeglądane co najmniej raz w roku, po każdym istotnym incydencie oraz w przypadku znaczących zmian w technologii, organizacji lub obowiązujących przepisach. Nieprzestrzeganie niniejszej polityki może skutkować działaniami dyscyplinarnymi, łącznie z rozwiązaniem stosunku pracy, a w przypadku podwykonawców — zakończeniem współpracy.

16. Zatwierdzenie

Niniejsza Polityka Bezpieczeństwa Informacji została zatwierdzona przez zarząd GSMValve OÜ i obowiązuje od daty wskazanej poniżej.

Rola	Imię i nazwisko	Podpis / Data
Zatwierdził (Zarząd)	Hans Alter	*podpisano cyfrowo*
Zweryfikował (Kierownik IT)	Margus Paurson	*podpisano cyfrowo*