NEXMA

Dokument obowiązujący

Polityka Bezpieczeństwa Informacji

Jak NEXMA chroni dane powierzone jej przez klientów oraz dane osobowe przetwarzane w imieniu administratorów danych.

WYSTAWCA
SYLWESTER SZAFERSKI

NUMER WERSJI
1.2

DATA OBOWIĄZYWANIA
od 23 maja 2026

NASTĘPNY PRZEGLĄD
w ciągu 12 miesięcy

KONTAKT (BEZPIECZEŃSTWO)
security@nexma.app

KONTAKT (RODO)
privacy@nexma.app

STRONA DOKUMENTU
nexma.app/documents

SPIS TREŚCI

1. Cel i zakres dokumentu
2. Definicje
3. Dane operatora i kontakt
4. Architektura i miejsce przetwarzania
5. Kontrola dostępu
6. Środki techniczne
7. Środki organizacyjne
8. Zarządzanie incydentami
9. Ciągłość działania i kopie zapasowe
10. Podprzetwarzający (subprocesorzy)
11. Rozwój oprogramowania
12. Audyty i przeglądy
13. Retencja i usunięcie danych
14. Zmiany w polityce

1. Cel i zakres dokumentu

Niniejsza Polityka Bezpieczeństwa Informacji (dalej: **Polityka**) opisuje środki techniczne i organizacyjne, które stosuje usługodawca platformy NEXMA — **SYLWESTER SZAFERSKI** — w celu ochrony poufności, integralności i dostępności danych powierzonych przez klientów korzystających z platformy. Dokument ma charakter publiczny — jest udostępniany klientom oraz ich działom bezpieczeństwa i compliance w celu oceny usługodawcy jako podprzetwarzającego dane osobowe w rozumieniu RODO.

Polityka obejmuje cały stos technologiczny platformy NEXMA: aplikację webową, bazę danych, mechanizm agenta instalowanego na stacjach roboczych klientów (dalej: **Nexma Connector**), kanały zdalnego zarządzania oraz procesy operacyjne zespołu NEXMA.

Polityka nie obejmuje:

- bezpieczeństwa środowiska Microsoft 365 klienta — tym zarządza klient jako administrator własnego tenantu;
- bezpieczeństwa stacji roboczych i serwerów klienta poza zakresem, który klient wprost powierzył do zarządzania przez Nexma Connector;
- bezpieczeństwa integracji stron trzecich, które klient samodzielnie dokonfiguruje poza standardowym zakresem NEXMA.

2. Definicje

Platforma NEXMA

Oprogramowanie typu SaaS dostępne pod domeną nexma.app, służące do samoobsługi pracowników, zarządzania wnioskami o dostęp, zarządzania stacjami roboczymi oraz procesami IT i HR opartymi o Microsoft 365.

Nexma Connector

Aplikacja instalowana przez klienta na stacjach roboczych (usługa Windows plus narzędzia administracyjne), pośrednicząca między platformą NEXMA a stacją — m.in. w zakresie inwentaryzacji oprogramowania, instalacji pakietów i zdalnych sesji wsparcia.

Dane osobowe

Wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej w rozumieniu art. 4 RODO.

Administrator danych

Klient korzystający z platformy NEXMA — podmiot, który decyduje o celach i sposobach przetwarzania danych swoich pracowników i współpracowników.

Procesor

SYLWESTER SZAFERSKI — podmiot przetwarzający dane osobowe w imieniu administratora na podstawie umowy powierzenia (DPA).

Subprocesor

Dalszy podmiot przetwarzający, którego NEXMA angażuje do realizacji usługi (np. dostawca hostingu).

Incydent bezpieczeństwa

Każde zdarzenie, które faktycznie lub potencjalnie naruszyło poufność, integralność lub dostępność danych klientów.

3. Dane operatora i kontakt

Platforma jest prowadzona przez:

> **SYLWESTER SZAFERSKI**
>
> NIP: 5213906939
> REGON: 387026755
> Adres działalności: Dalekie 61a, 07-211 Długosiodło

Kontakt w sprawach bezpieczeństwa i naruszeń ochrony danych:

- adres e-mail: **security@nexma.app** — monitorowany w dni robocze w godzinach 9:00–17:00 czasu środkowoeuropejskiego; zgłoszenia o charakterze krytycznym (np. podejrzenie wycieku danych) obsługiwane są także poza tymi godzinami.
- adres serwisu: **nexma.app**

> **Inspektor Ochrony Danych.** Z uwagi na skalę działania NEXMA nie ma obowiązku powołania IOD w rozumieniu art. 37 RODO. Zapytania dotyczące ochrony danych osobowych oraz żądania praw podmiotów danych kieruj na **privacy@nexma.app**. Zgłoszenia incydentów bezpieczeństwa (w tym podejrzenia nieuprawnionego dostępu lub wycieku danych w warstwie technicznej) kieruj na **security@nexma.app**.

4. Architektura i miejsce przetwarzania

4.1. Hosting aplikacji

Aplikacja NEXMA oraz jej baza danych są uruchamiane w chmurze publicznej dostawcy **OVHcloud** (OVH Groupe SAS, siedziba: Roubaix, Francja), w regionie **eu-central-waw** (Warszawa, Polska), strefa dostępności **eu-central-waw-a**. Oznacza to, że dane klienta są fizycznie przechowywane w centrum danych zlokalizowanym na terytorium Rzeczypospolitej Polskiej, w granicach Europejskiego Obszaru Gospodarczego.

4.2. Baza danych

Dane operacyjne są zapisywane w relacyjnej bazie danych PostgreSQL utrzymywanej w tym samym regionie, z dostępem wyłącznie z wnętrza sieci NEXMA (brak publicznego endpointu). Dostęp do bazy mają wyłącznie imiennie wskazane konta administracyjne NEXMA.

4.3. Szyfrowanie danych

- **W transporcie:** cały ruch HTTP jest terminowany na TLS 1.2 lub nowszym z użyciem certyfikatów publicznych (Let's Encrypt lub równoważny urząd certyfikacji). Połączenia poza wspieranym zakresem są odrzucane.
- **W spoczynku:** dyski maszyn wirtualnych oraz kopie zapasowe są szyfrowane zgodnie ze standardem OVHcloud (AES-256 na poziomie storage backendu).
- **Hasła:** NEXMA nie przechowuje haseł użytkowników biznesowych — uwierzytelnianie pracowników klienta odbywa się przez Microsoft 365 (Microsoft Entra ID), z obsługą mechanizmów MFA i Conditional Access po stronie klienta.

4.4. Nexma Connector

Nexma Connector komunikuje się z platformą wyłącznie w trybie wychodzącym (outbound HTTPS do nexma.app). Nie wymaga otwierania portów przychodzących na stacjach ani w sieci klienta. Zdalne sesje administracyjne oraz zdalny pulpit realizowane są przez silnik open-source MeshCentral; sesje zdalnego pulpitu są rejestrowane w module audytu NEXMA (kto się połączył, do której stacji, kiedy i jak długo trwała sesja).

5. Kontrola dostępu

5.1. Dostęp użytkowników klienta

Platforma NEXMA stosuje model kontroli dostępu opartej o role (RBAC). Oznacza to, że każdy użytkownik widzi wyłącznie te dane i operacje, do których jego rola daje mu uprawnienia w ramach tenantu jego pracodawcy. Podział tenantów jest logiczny, realizowany na poziomie bazy danych i API — dane jednego klienta nie są widoczne dla innych klientów.

5.2. Dostęp personelu NEXMA

Do danych klientów mają dostęp wyłącznie pracownicy i współpracownicy NEXMA, którym taki dostęp jest niezbędny do realizacji obowiązków (zasada najmniejszych uprawnień). Każdy taki dostęp jest:

- imienny — nie używamy kont współdzielonych;
- uwierzytelniany silnym hasłem oraz drugim składnikiem (MFA);
- ograniczony czasowo tam, gdzie to możliwe (ad-hoc, pod konkretne zadanie);
- odnotowany w dziennikach zdarzeń aplikacji lub systemu.

5.3. Dostęp do infrastruktury

Dostęp SSH, administracja bazą danych i konsola OVHcloud są ograniczone do osób pełniących rolę administratora platformy. Konta służące do dostępu do infrastruktury są chronione MFA. Klucze SSH są unikalne dla każdej osoby — nie dzielone, nie zapisywane w repozytorium kodu.

6. Środki techniczne

Niezależnie od środków opisanych w poprzednich rozdziałach, NEXMA stosuje następujące techniczne środki bezpieczeństwa:

- **Izolacja środowisk** — środowisko produkcyjne jest oddzielone od środowisk deweloperskich i testowych na poziomie sieciowym i autoryzacyjnym; dane produkcyjne nigdy nie są używane do testów.
- **Sekrety i klucze** — hasła do baz, klucze API i tokeny są przechowywane poza repozytorium kodu, w zmiennych środowiskowych chronionego serwera; rotacja kluczy odbywa się przy zmianach składu zespołu mającego do nich dostęp.
- **Aktualizacje systemowe** — system operacyjny, baza danych i biblioteki aplikacji są regularnie aktualizowane; krytyczne poprawki bezpieczeństwa wdrażamy niezwłocznie po ich publikacji.
- **Logowanie zdarzeń** — aplikacja rejestruje zdarzenia istotne z perspektywy bezpieczeństwa (logowania, operacje administracyjne, dostęp do danych osobowych, sesje zdalne). Logi są chronione przed nieuprawnioną modyfikacją.

- **Ochrona przed atakami** — aplikacja stosuje standardowe mechanizmy obronne: walidacja danych wejściowych, parametryzacja zapytań do bazy, zabezpieczenie przed CSRF/XSS, nagłówki bezpieczeństwa HTTP, ograniczenie liczby zapytań (rate limiting) dla operacji wrażliwych.
- **Separacja danych** — każdy klient (tenant) ma własny izolowany zestaw danych, identyfikowany po identyfikatorze tenantu Microsoft 365; zapytania do bazy są filtrowane przez identyfikator tenantu na każdym poziomie.
- **Monitoring błędów aplikacji** — NEXMA korzysta z usługi Sentry (region EU, Frankfurt) do centralnego raportowania wyjątków i błędów aplikacji. SDK Sentry działa po stronie serwera (Node.js + Edge runtime) oraz w przeglądarce użytkownika. Polityka prywatności i konfiguracja:
  - opcja `sendDefaultPii` jest **wyłączona** — Sentry nie zbiera adresu IP, ciasteczek ani treści żądania;
  - przed wysyłką każdego zdarzenia zaplikany jest filtr po stronie NEXMA (*scrubber*) usuwający nagłówki autoryzacyjne (m.in. `Authorization`, `Cookie`, `x-cron-secret`, `x-mailbox-webhook-secret`) oraz parametry sekretów w adresach URL (m.in. `?secret=`, `?token=`, `?code=`, `?password=`) — zarówno z głównego żądania, jak i z historii (*breadcrumbs*);
  - funkcja „Session Replay" (nagrywanie sesji przeglądarki) jest wyłączona;
  - próbkowanie zdarzeń diagnostycznych (*tracing*) po stronie serwera ustawione jest domyślnie na 10%; po stronie klienta tracing jest wyłączony — przekazywane są wyłącznie błędy.

7. Środki organizacyjne

- **Zobowiązanie do poufności** — każda osoba mająca dostęp do danych klientów jest pisemnie zobowiązana do zachowania poufności, z klauzulami obowiązującymi również po zakończeniu współpracy.
- **Szkolenia** — zespół NEXMA przechodzi wewnętrzne szkolenia z zakresu ochrony danych i bezpieczeństwa aplikacji; nowi członkowie zespołu są szkoleni przed uzyskaniem dostępu do danych produkcyjnych.
- **Zasada czystego biurka i czystego ekranu** — stacje robocze zespołu są szyfrowane (BitLocker lub równoważne), wymagają blokady po okresie bezczynności, dostęp do nich chroniony jest silnym hasłem oraz MFA dla krytycznych aplikacji.
- **Polityka bezpiecznego rozwoju oprogramowania** — patrz rozdział 11.

8. Zarządzanie incydentami

8.1. Zgłoszenia zewnętrzne

Zgłoszenia dotyczące bezpieczeństwa (w tym potencjalne podatności, nietypowe działanie aplikacji, podejrzenie nieuprawnionego dostępu) przyjmujemy pod adresem **security@nexma.app**. Zachęcamy do zgłaszania problemów odpowiedzialnie, z opisem kroków umożliwiających reprodukcję. NEXMA nie pozywa za działania w dobrej wierze, zgodne z ogólnie przyjętymi zasadami responsible disclosure.

8.2. Procedura reakcji

1. **Przyjęcie i potwierdzenie** — każde zgłoszenie potwierdzamy w ciągu 1 dnia roboczego, przypisując mu numer sprawy.
2. **Klasyfikacja** — oceniamy wpływ na poufność, integralność i dostępność danych oraz liczbę potencjalnie dotkniętych klientów.
3. **Ograniczenie skutków** — działania naprawcze uruchamiamy niezwłocznie po klasyfikacji; w razie potrzeby odcinamy dostęp, wymieniamy klucze, wyłączamy podatną funkcję.
4. **Analiza** — rekonstrukcja zdarzenia, zakresu danych, przyczyny korzeniowej.
5. **Komunikacja** — patrz punkt 8.3.
6. **Działania korygujące** — wdrożenie zmian technicznych lub procesowych, które wykluczają powtórzenie incydentu.

8.3. Zawiadomienie klienta

Jeżeli dany incydent stanowi naruszenie ochrony danych osobowych w rozumieniu RODO, NEXMA zawiadamia o tym klienta (administratora danych) **bez zbędnej zwłoki, nie później niż w ciągu 72 godzin** od stwierdzenia naruszenia. Zawiadomienie zawiera:

- opis charakteru naruszenia oraz — w miarę możliwości — kategorii i przybliżonej liczby osób i rekordów, których naruszenie dotyczy;
- opis możliwych konsekwencji naruszenia;
- opis zastosowanych lub planowanych środków zaradczych;
- dane kontaktowe osoby prowadzącej sprawę po stronie NEXMA.

9. Ciągłość działania i kopie zapasowe

- **Kopie zapasowe bazy danych** wykonywane są automatycznie co najmniej raz na dobę; są szyfrowane i przechowywane poza środowiskiem produkcyjnym u dostawcy **Wasabi Hot Cloud Storage** (Wasabi Technologies, Inc., region **eu-central-2** — Frankfurt, Niemcy, EOG), niezależnie od lokalizacji aplikacji w OVHcloud.
- **RPO** (akceptowalny horyzont utraty danych) — maksymalnie 24 godziny.

- **RTO** (czas na przywrócenie działania po poważnej awarii) — cel 24 godziny dla wszystkich kluczowych funkcji platformy.
- **Testy odtworzenia** — procedura odtworzenia bazy z kopii testowana jest nie rzadziej niż raz na 12 miesięcy.
- **Ścieżka eskalacji** — w razie poważnej awarii NEXMA publikuje aktualizacje statusu oraz komunikuje się z klientami przez adres e-mail wskazany w panelu administracyjnym i na stronie statusowej.

10. Podprzetwarzający (subprocesorzy)

NEXMA korzysta z następujących dostawców usług, którzy mogą mieć dostęp do danych klientów w zakresie niezbędnym do świadczenia swoich usług. Lista aktualizowana jest wraz ze zmianami stosu; historyczne wersje dostępne są na żądanie pod adresem privacy@nexma.app.

PODMIOT	ROLA	LOKALIZACJA DANYCH	STATUS
Microsoft Ireland Operations Ltd. (Microsoft 365, Microsoft Entra ID, Graph API)	Dostawca systemu tożsamości oraz źródła danych pracowników klienta; integracja po stronie klienta.	Data residency zgodnie z wyborem tenantu klienta (typowo UE).	Aktywny
OVH Groupe SAS (OVHcloud, region eu-central-waw)	Dostawca hostingu aplikacji i bazy danych.	Warszawa, Polska (EOG).	Aktywny
Wasabi Technologies, Inc. (Wasabi Hot Cloud Storage, region eu-central-2)	Off-site przechowywanie szyfrowanych kopii zapasowych (baza danych i pliki kopii).	Frankfurt, Niemcy (EOG).	Aktywny
Stripe Payments Europe Ltd.	Operator płatności kartowych i rozliczeń subskrypcyjnych (Stripe Billing); rozliczenia w EUR netto; VAT przez Stripe Tax.	Irlandia (EOG); możliwe transfery do USA na podstawie Standardowych Klauzul Umownych.	Aktywny
Functional Software, Inc. d/b/a Sentry	Centralny monitoring błędów aplikacji (Sentry, region EU). Zakres opisany w rozdziale 6 — bez adresu IP, z aktywnym filtrowaniem sekretów po stronie NEXMA.	Frankfurt, Niemcy — region EU (EOG). Dane nie opuszczają EOG.	Aktywny

O planowanej zmianie lub dodaniu subprocesora NEXMA informuje klienta z co najmniej 30-dniowym wyprzedzeniem pocztowym, z możliwością złożenia uzasadnionego sprzeciwu.

11. Rozwój oprogramowania

- kod aplikacji przechowywany jest w prywatnym repozytorium z kontrolą dostępu i historią zmian;
- zmiany w kodzie produkcyjnym przechodzą przez review techniczny przed wdrożeniem;
- wdrożenia produkcyjne są odnotowywane, istnieje możliwość szybkiego wycofania zmiany (rollback);
- zależności zewnętrzne (biblioteki) są aktualizowane i skanowane pod kątem znanych podatności;
- dostęp do środowiska produkcyjnego z poziomu narzędzi deweloperskich jest ograniczony wyłącznie do osób upoważnionych.

12. Audyty i przeglądy

NEXMA wewnętrznie przegląda niniejszą Politykę co najmniej raz na 12 miesięcy oraz po każdej istotnej zmianie w architekturze, liście subprocesorów lub po poważnym incydencie bezpieczeństwa. Klient ma prawo zażądać informacji o aktualnym stanie środków bezpieczeństwa pod adresem **security@nexma.app**. W uzasadnionych przypadkach, zwłaszcza w związku z wymaganiami działu compliance klienta, NEXMA udostępnia szczegółową dokumentację na podstawie umowy o zachowaniu poufności.

13. Retencja i usunięcie danych

- dane operacyjne (konta, wnioski, zdarzenia) przechowywane są przez czas trwania umowy oraz 30 dni po jej wygaśnięciu;
- po tym okresie dane produkcyjne są usuwane, a kopie zapasowe są nadpisywane w ramach normalnej rotacji nie później niż w ciągu kolejnych 90 dni;
- na pisemne żądanie klienta (wysłane z adresu administracyjnego) NEXMA potwierdza fakt usunięcia danych na piśmie lub drogą e-mail;
- szczegółowe zasady dotyczące usunięcia i zwrotu danych osobowych opisuje umowa powierzenia (DPA).

14. Zmiany w polityce

NEXMA ma prawo aktualizować niniejszą Politykę w celu odzwierciedlenia zmian w usługach, obowiązującym prawie lub stosowanych środkach bezpieczeństwa. O istotnych zmianach klient jest informowany drogą e-mail oraz przez opublikowanie zaktualizowanej wersji dokumentu pod adresem **nexma.app/documents**. Data obowiązywania ostatniej aktualizacji widoczna jest na okładce dokumentu.

Niniejszy dokument jest własnością **SYLWESTER SZAFERSKI** i został przygotowany w dobrej wierze, w oparciu o wiedzę o architekturze platformy na dzień publikacji. W przypadku rozbieżności między treścią Polityki a postanowieniami umowy powierzenia (DPA) pierwszeństwo mają postanowienia DPA.