



Dokument obowiązujący

Umowa powierzenia przetwarzania danych osobowych (DPA)

Stanowi integralną część umowy o korzystanie z platformy NEXMA
zawartej pomiędzy klientem a SYLWESTER SZAFERSKI.

WYSTAWCA (PROCESOR)

SYLWESTER SZAFERSKI

DATA OBOWIĄZYWANIA

od 23 maja 2026

KONTAKT

legal@nexma.app

NUMER WERSJI

1.2

STAN PRAWNY

RODO (Rozporządzenie 2016/679)

STRONA DOKUMENTU

nexma.app/documents

Status procesora. Procesorem danych w rozumieniu niniejszej umowy jest **SYLWESTER SZAFERSKI** (NIP 5213906939, REGON 387026755, Dalekie 61a, 07-211 Długosiodło).

1. Strony umowy

PROCESOR

SYLWESTER SZAFERSKI

NIP: 5213906939

REGON: 387026755

Adres: Dalekie 61a, 07-211 Długosiodło

Reprezentant: Sylwester Szaferski

Kontakt: legal@nexma.app (umowa i dokumentacja prawna),

privacy@nexma.app (RODO, TOM, subprocesorzy), security@nexma.app (incydenty bezpieczeństwa).

ADMINISTRATOR

Klient — podmiot, który zawarł z NEXMA umowę o korzystanie z platformy (akceptując regulamin usługi lub na mocy indywidualnie podpisanej umowy).

Dane klienta identyfikowane są w panelu administracyjnym platformy oraz w dokumentach rozliczeniowych (fakturach) wystawianych na rzecz klienta.

2. Definicje

RODO

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

Umowa główna

Umowa o korzystanie z platformy NEXMA zawarta pomiędzy stronami (regulamin, umowa subskrypcyjna lub inny równoważny dokument).

Dane powierzone

Dane osobowe pracowników, współpracowników i innych osób związanych z Administratorem, które NEXMA przetwarza w imieniu Administratora w związku z wykonywaniem Umowy głównej. Szczegółowy zakres opisuje Załącznik nr 1.

Subprocesor

Dalszy podmiot przetwarzający zaangażowany przez NEXMA. Aktualna lista stanowi Załącznik nr 2.

Incydent

Naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO.

TOM

Środki techniczne i organizacyjne, o których mowa w art. 32 RODO, opisane w Załączniku nr 3 oraz w Polityce Bezpieczeństwa Informacji NEXMA dostępnej pod nexma.app/documents.

3. Przedmiot i cel powierzenia

Administrator powierza NEXMA, a NEXMA przyjmuje do przetwarzania dane powierzone wyłącznie w celu i zakresie niezbędnym do:

- świadczenia usługi NEXMA zgodnie z Umową główną,
- utrzymania, konfiguracji i rozwoju platformy,
- realizacji praw osób, których dane dotyczą, wykonywanych wobec Administratora,
- zapewnienia bezpieczeństwa platformy i reagowania na incydenty,
- spełnienia ewentualnych obowiązków prawnych ciążących na NEXMA.

NEXMA nie przetwarza danych powierzonych w celach własnych, w szczególności nie profiluje osób, których dane dotyczą, w celach marketingowych NEXMA oraz nie sprzedaje danych powierzonych.

4. Obowiązki procesora

NEXMA zobowiązuje się:

1. przetwarzać dane powierzone wyłącznie na udokumentowane polecenie Administratora, w tym w zakresie przekazywania danych do państwa trzeciego lub organizacji międzynarodowej, chyba że obowiązek taki nakłada na NEXMA prawo Unii lub prawo państwa członkowskiego — w takim przypadku NEXMA poinformuje Administratora o tym obowiązku przed rozpoczęciem przetwarzania, chyba że prawo to zabrania takiego poinformowania z uwagi na ważny interes publiczny;
2. zapewnić, by osoby upoważnione do przetwarzania danych powierzonych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
3. podjąć wszelkie środki wymagane na mocy art. 32 RODO (bezpieczeństwo przetwarzania), w zakresie opisanym w Załączniku nr 3;
4. przestrzegać warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w art. 28 ust. 2 i 4 RODO (patrz rozdział 7);
5. biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomagać Administratorowi — poprzez odpowiednie środki techniczne i organizacyjne — wywiązać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw (art. 12–22 RODO);

6. pomagać Administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO, w szczególności w obszarze bezpieczeństwa, zawiadamiania o naruszeniach oraz oceny skutków dla ochrony danych;
7. po zakończeniu świadczenia usług zwrócić lub usunąć dane powierzone zgodnie z rozdziałem 12 niniejszej umowy;
8. udostępnić Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków z art. 28 RODO oraz umożliwić Administratorowi (lub jego audytorowi) przeprowadzenie audytu, na zasadach opisanych w rozdziale 11.

5. Obowiązki administratora

Administrator zobowiązuje się:

1. przetwarzać dane osobowe zgodnie z RODO oraz innymi obowiązującymi przepisami prawa;
2. wydawać polecenia przetwarzania danych w formie pozwalającej na ich udokumentowanie — w szczególności polecenia wynikające z konfiguracji platformy uznaje się za udokumentowane polecenia Administratora;
3. informować użytkowników platformy (osoby, których dane dotyczą) o przetwarzaniu ich danych w zakresie wymaganym przez RODO — obowiązek informacyjny co do przetwarzania w ramach platformy NEXMA ciąży na Administratorze;
4. zapewnić legalną podstawę prawną dla przetwarzania danych przekazywanych NEXMA, w tym dla uzyskiwania danych od stron trzecich (np. integracji z Microsoft 365);
5. nie przekazywać NEXMA danych szczególnych kategorii (art. 9 RODO) ani danych dotyczących wyroków skazujących i naruszeń prawa (art. 10 RODO), o ile nie jest to niezbędne i wcześniej uzgodnione z NEXMA.

6. Bezpieczeństwo przetwarzania

NEXMA stosuje środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania. Szczegółowy opis środków stanowi Załącznik nr 3 oraz publikowana Polityka Bezpieczeństwa Informacji.

Strony przyjmują, że zakres środków opisany w Załączniku nr 3 jest zgodny z art. 32 RODO. NEXMA może modyfikować te środki, o ile zmiana nie obniży ogólnego poziomu bezpieczeństwa przetwarzania.

7. Korzystanie z subprocesorów

Administrator udziela NEXMA ogólnej zgody na powierzenie przetwarzania danych powierzonych subprocesorom wskazanym w Załączniku nr 2. NEXMA zapewnia, że każdy subprocesor będzie związany — na mocy umowy lub innego instrumentu prawnego — obowiązkami w zakresie ochrony danych tożsamymi z obowiązkami NEXMA wynikającymi z niniejszej umowy.

O planowanej zmianie lub dodaniu subprocesora NEXMA informuje Administratora z co najmniej 30-dniowym wyprzedzeniem drogą elektroniczną, umożliwiając złożenie uzasadnionego sprzeciwu. W przypadku wniesienia uzasadnionego sprzeciwu strony dołożą starań, aby osiągnąć porozumienie; jeżeli to nie nastąpi, Administrator ma prawo wypowiedzieć Umowę główną w zakresie dotkniętym zmianą, z zachowaniem 30-dniowego okresu wypowiedzenia.

8. Transfer danych poza EOG

NEXMA hostuje platformę na terytorium Polski (OVHcloud, region eu-central-waw). Jeżeli realizacja usługi wymaga transferu danych powierzonych poza EOG (np. z uwagi na globalny zasięg Microsoft 365 lub operatorów płatności), odbywa się to wyłącznie w oparciu o mechanizmy, o których mowa w rozdziale V RODO — w szczególności Standardowe Klauzule Umowne w wersji przyjętej decyzją wykonawczą Komisji (UE) 2021/914.

9. Realizacja praw osób, których dane dotyczą

Jeżeli do NEXMA wpłynie żądanie od osoby, której dane powierzone dotyczą, NEXMA niezwłocznie przekazuje takie żądanie Administratorowi, bez podejmowania czynności merytorycznych samodzielnie, chyba że na żądanie Administratora.

NEXMA udostępnia Administratorowi narzędzia platformy pozwalające na obsługę takich żądań (wgląd w dane, ich sprostowanie, eksport, usunięcie konta). W zakresie, w jakim realizacja żądania wymaga po stronie NEXMA interwencji operacyjnej (np. trwałe usunięcie danych także z kopii zapasowych), NEXMA realizuje ją niezwłocznie po otrzymaniu pisemnego żądania Administratora.

10. Zgłaszanie naruszeń

NEXMA zawiadamia Administratora o każdym stwierdzonym incydencie dotyczącym danych powierzonych **bez zbędnej zwłoki, nie później niż w ciągu 72 godzin od jego stwierdzenia**. Zawiadomienie przekazywane jest drogą elektroniczną na adres kontaktowy wskazany przez Administratora w panelu platformy oraz zawiera elementy wskazane w art. 33 ust. 3 RODO, w zakresie, w jakim są znane NEXMA w chwili zawiadomienia. Dalsze informacje NEXMA przekazuje w miarę ich ustalania.

NEXMA zapewnia Administratorowi wsparcie niezbędne do wypełnienia przez Administratora obowiązku zawiadomienia organu nadzorczego oraz osób, których dane dotyczą, o naruszeniu ochrony danych osobowych (art. 33–34 RODO).

11. Audyty

NEXMA udostępnia Administratorowi, na jego żądanie, informacje potwierdzające wykonywanie niniejszej umowy oraz stosowanie TOM. Żądanie należy kierować na adres **privacy@nexma.app**.

Administrator ma prawo do audytu na zasadach opisanych poniżej:

1. W pierwszej kolejności Administrator korzysta z dokumentacji udostępnionej przez NEXMA (Polityka Bezpieczeństwa Informacji, odpowiedzi na kwestionariusze bezpieczeństwa, raporty o statusie platformy) — ta forma uznawana jest za wystarczający audyt dla większości przypadków.
2. W uzasadnionych przypadkach Administrator może przeprowadzić audyt w siedzibie NEXMA lub zdalnie, z co najmniej 30-dniowym wyprzedzeniem, w dniach roboczych, w zakresie niezbędnym do weryfikacji zgodności z art. 28 RODO. Koszty audytu wykonywanego na żądanie pojedynczego Administratora pokrywa Administrator, chyba że audyt ujawni istotne niezgodności po stronie NEXMA.
3. Audyt nie może zakłócać normalnej działalności NEXMA ani naruszać poufności danych innych klientów NEXMA.

12. Zakończenie powierzenia, zwrot i usunięcie danych

Po zakończeniu świadczenia usług na mocy Umowy głównej — w zależności od decyzji Administratora wyrażonej w pisemnym żądaniu doręczonym NEXMA nie później niż w ciągu 30 dni od zakończenia umowy — NEXMA:

- zwraca Administratorowi dane powierzone w standardowym formacie eksportu udostępnianym przez platformę, albo
- usuwa dane powierzone, potwierdzając ten fakt pisemnie (w tym drogą elektroniczną).

W braku wyraźnego żądania Administratora w tym terminie NEXMA usuwa dane powierzone zgodnie z polityką retencji opisaną w Polityce Bezpieczeństwa Informacji. NEXMA może zachować dane wyłącznie w zakresie, w jakim wymaga tego prawo Unii lub prawo państwa członkowskiego.

13. Odpowiedzialność

Odpowiedzialność stron za naruszenie niniejszej umowy określa Umowa główna, przy czym ograniczenia odpowiedzialności w niej zawarte nie stosują się do przypadków, w których zgodnie z prawem nie mogą one być skutecznie ograniczone (w szczególności roszczenia osób, których dane

dotyczą, dochodzone bezpośrednio na podstawie art. 82 RODO).

Każda ze stron ponosi własną odpowiedzialność za naruszenia RODO, których się dopuściła w ramach swojej roli — Administratora albo Procesora.

14. Postanowienia końcowe

1. Niniejsza umowa wchodzi w życie z chwilą zawarcia Umowy głównej (albo z chwilą akceptacji regulaminu, jeżeli stanowi ona integralną część regulaminu) i obowiązuje przez okres trwania Umowy głównej oraz tak długo, jak długo NEXMA przetwarza dane powierzone.
2. W sprawach nieuregulowanych stosuje się przepisy RODO oraz polskiego prawa powszechnie obowiązującego.
3. Sądem właściwym dla sporów wynikających z niniejszej umowy jest sąd właściwy dla siedziby NEXMA, chyba że bezwzględnie obowiązujące przepisy stanowią inaczej.
4. Wszelkie zmiany umowy wymagają formy pisemnej lub dokumentowej pod rygorem nieważności; za zmianę nie uznaje się aktualizacji załączników dokonywanej w trybie opisanym w rozdziale 7 (aktualizacja listy subprocessorów).
5. Jeżeli którekolwiek z postanowień umowy zostanie uznane za nieważne lub bezskuteczne, nie wpływa to na ważność pozostałych postanowień.

A. Załącznik nr 1 — Opis przetwarzania

Przedmiot, charakter i cel przetwarzania

Świadczenie usługi NEXMA jako platformy do samoobsługi pracowników i zarządzania IT w środowisku Microsoft 365. Przetwarzanie ma charakter zautomatyzowanego przetwarzania danych osobowych w systemie teleinformatycznym oraz — w zakresie sesji zdalnego wsparcia — charakter ograniczonego dostępu człowieka do stacji roboczych użytkowników pod ich nadzorem.

Czas trwania przetwarzania

Czas obowiązywania Umowy głównej oraz okres retencji opisany w Polityce Bezpieczeństwa Informacji (do 30 dni w produkcji i do 90 dni w kopiach zapasowych po zakończeniu umowy).

Rodzaj i kategorie danych

- dane identyfikacyjne (imię, nazwisko, e-mail służbowy, identyfikator w Microsoft Entra ID, identyfikator tenantu);
- dane organizacyjne (stanowisko, dział, przełożony, lokalizacja);
- dane dotyczące uprawnień w Microsoft 365;
- dane urządzeń przypisanych do użytkownika i stanu oprogramowania;
- logi aktywności w platformie;
- treść wniosków i zgłoszeń wprowadzanych przez użytkownika;
- metadane i zapisy sesji zdalnego wsparcia technicznego.

Kategorie osób

- pracownicy Administratora,
- współpracownicy i wykonawcy Administratora, którym Administrator nada dostęp do platformy,
- użytkownicy zewnętrzni (gościnni), jeżeli Administrator udostępnia im zasoby za pośrednictwem platformy.

B. Załącznik nr 2 — Lista subprocesorów

PODMIOT	ROLA	LOKALIZACJA DANYCH	STATUS
Microsoft Ireland Operations Ltd.	Microsoft 365, Microsoft Entra ID, Graph API — źródło danych pracowników Administratora.	Data residency zgodnie z wyborem tenantu Administratora (typowo UE).	Aktywny
OVH Groupe SAS (OVHcloud)	Dostawca hostingu aplikacji i bazy danych NEXMA.	Warszawa, Polska — region eu-central-waw, strefa eu-central-waw-a (EOG).	Aktywny
Wasabi Technologies, Inc.	Przechowywanie szyfrowanych kopii zapasowych bazy danych i środowiska platformy (Wasabi Hot Cloud Storage, region eu-central-2).	Frankfurt, Niemcy — region eu-central-2 (EOG); dane nie opuszczają 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 (132 Hawthorne St., San Francisco, CA 94107, USA)	Monitoring błędów aplikacji (usługa Sentry, region EU). Otrzymuje wyłącznie zminimalizowane dane techniczne błędu (rodzaj wyjątku, ślad stosu, identyfikator wersji, znacznik czasu, adres URL trasy aplikacji i nagłówek user-agent), bez adresu IP użytkownika i bez identyfikatorów osobowych. Nagłówki autoryzacyjne i sekrety w adresach URL są filtrowane po stronie NEXMA przed wysyłką.	Frankfurt, Niemcy — region EU (de.sentry.io). Dane nie opuszczają EOG. Pomimo siedziby spółki-matki w USA wybrany region przetwarzania pozostaje w EOG; w razie potrzeby zastosowanie mają Standardowe Klauzule Umowne (decyzja KE 2021/914) na podstawie Online DPA Sentry.	Aktywny

Status podmiotów z listy może ewoluować wraz z rozwojem platformy. Archiwalne rozliczenia mogą obejmować historyczne wpisy po wcześniejszych operatorach — wyłącznie w zakresie niezbędnym do rozliczeń i compliance.

C. Załącznik nr 3 — Środki techniczne i organizacyjne

Wyszczególnione poniżej środki odpowiadają wymaganiom art. 32 RODO. Pełny opis środków zawiera publikowana Polityka Bezpieczeństwa Informacji (nexma.app/documents).

KONTROLA DOSTĘPU

- model kontroli dostępu opartej o role (RBAC) po stronie aplikacji;
- integracja z Microsoft Entra ID po stronie uwierzytelniania użytkowników klienta — obsługa MFA i Conditional Access zgodnie z polityką klienta;
- obowiązkowe MFA dla personelu NEXMA;
- imienne, nieudostępniane konta administracyjne;
- zasada najmniejszych uprawnień.

SZYFROWANIE

- TLS 1.2+ dla ruchu między klientem a platformą oraz pomiędzy platformą a Nexma Connector;
- szyfrowanie danych w spoczynku na poziomie storage backendu dostawcy chmury (AES-256);
- szyfrowane kopie zapasowe.

ROZDZIELNOŚĆ TENANTÓW

- logiczna separacja danych klientów na poziomie bazy danych i API;
- każde zapytanie aplikacyjne jest filtrowane po identyfikatorze tenantu;
- brak wspólnych zasobów operacyjnych udostępnianych bezpośrednio między tenantami.

MONITOROWANIE I REAGOWANIE NA INCYDENTY

- zbieranie logów zdarzeń istotnych dla bezpieczeństwa;
- procedura obsługi incydentów z zawiadomieniem Administratora w ciągu 72 godzin;
- kanał zgłoszeń: security@nexma.app.

CIĄGŁOŚĆ DZIAŁANIA

- automatyczne kopie zapasowe co najmniej raz dobowo;
- docelowe RPO 24 godziny, RTO 24 godziny;
- coroczny test odtworzenia danych z kopii.

ORGANIZACJA

- pisemne zobowiązanie do poufności osób mających dostęp do danych;
- szkolenia z ochrony danych dla członków zespołu;
- bezpieczna konfiguracja stacji roboczych zespołu NEXMA (szyfrowanie dysku, blokada ekranu, aktualizacje);

- review kodu i kontrolowane wdrożenia produkcyjne.

15. Podpisy stron

Niniejsza umowa zawierana jest w formie dokumentowej w drodze akceptacji regulaminu usługi NEXMA. W przypadku zawarcia indywidualnej umowy pisemnej lub podpisu kwalifikowanego, strony podpisują dokument w poniższych miejscach.

Procesor

SYLWESTER SZAFERSKI
Sylwester Szaferski

data i podpis

Administrator

[dane klienta]

[imię i nazwisko reprezentanta]

data i podpis

Niniejsza umowa powierzenia stanowi integralną część regulaminu korzystania z platformy NEXMA. W przypadku rozbieżności pomiędzy jej treścią a regulaminem w zakresie przetwarzania danych osobowych pierwszeństwo mają postanowienia niniejszej umowy.