NEXMA

Effective document

Information Security Policy

How NEXMA protects customer data and the personal data it processes on behalf of its customers as a data processor under GDPR.

ISSUER
SYLWESTER SZAFERSKI

VERSION
1.2

EFFECTIVE FROM
May 23, 2026

NEXT REVIEW
Within 12 months

SECURITY CONTACT
security@nexma.app

GDPR / PRIVACY
privacy@nexma.app

DOCUMENT HOME
nexma.app/documents

TABLE OF CONTENTS

1. Purpose and scope

This Information Security Policy (the **Policy**) describes the technical and organisational measures applied by the provider of the NEXMA platform — **SYLWESTER SZAFERSKI** — to safeguard the confidentiality, integrity and availability of data entrusted by customers using the platform. This document is public — it is made available to customers and to their security and compliance teams so that they can assess the service provider as a GDPR data processor.

The Policy covers the entire NEXMA technology stack: the web application, the database, the agent installed on customer workstations (the **Nexma Connector**), remote administration channels and the operational practices of the NEXMA team.

The Policy does not cover:

- the security of the customer's Microsoft 365 environment — this is managed by the customer as the administrator of its own tenant;
- the security of customer workstations and servers outside the scope the customer has explicitly entrusted to Nexma Connector;
- the security of third-party integrations that the customer configures beyond the standard NEXMA scope.

2. Definitions

NEXMA platform

The SaaS product available at nexma.app, used for employee self-service, access request management, workstation management and IT/HR processes built around Microsoft 365.

Nexma Connector

Software installed by the customer on its workstations (a Windows service plus administrative tools) that mediates between the NEXMA platform and the workstation, for example for software inventory, package deployment and remote support sessions.

Personal data

Any information relating to an identified or identifiable natural person as defined in Article 4 GDPR.

Data controller

The customer using the NEXMA platform — the entity that determines the purposes and means of processing the personal data of its employees and contractors.

Processor

SYLWESTER SZAFERSKI — the entity that processes personal data on behalf of the data controller on the basis of a data processing agreement (DPA).

Subprocessor

A further processor engaged by NEXMA to deliver the service (for example the hosting provider).

Security incident

Any event that has affected or might affect the confidentiality, integrity or availability of customer data.

3. Operator data and contact

The platform is operated by:

> **SYLWESTER SZAFERSKI**
>
> Tax ID (NIP): 5213906939
> Statistical number (REGON): 387026755
> Business address: Dalekie 61a, 07-211 Długosiodło

Security and data protection contact:

- email: **security@nexma.app** — monitored during business days 9:00–17:00 CET; critical reports (for example a suspected data breach) are also handled outside business hours.
- website: **nexma.app**

> **Data Protection Officer.** Given the scale of NEXMA's operations, appointing a DPO is not mandatory under Article 37 GDPR. Enquiries about personal data protection and data subject requests should be sent to **privacy@nexma.app**. Security incident reports (including suspected unauthorised access or technical data breaches) should be sent to **security@nexma.app**.

4. Architecture and hosting

4.1. Application hosting

The NEXMA application and its database are hosted with **OVHcloud** (OVH Groupe SAS, based in Roubaix, France), in the **eu-central-waw** region (Warsaw, Poland), availability zone **eu-central-waw-a**. This means that customer data is physically stored in a data centre located within the Republic of Poland and within the European Economic Area.

4.2. Database

Operational data is stored in a PostgreSQL relational database hosted in the same region, accessible only from inside the NEXMA network (no public endpoint). The database is accessed exclusively by named NEXMA administrator accounts.

4.3. Encryption

- **In transit:** all HTTP traffic is terminated with TLS 1.2 or newer using public certificates (Let's Encrypt or an equivalent certificate authority). Connections outside the supported range are rejected.
- **At rest:** virtual machine disks and backups are encrypted using the OVHcloud standard (AES-256 at the storage backend level).
- **Passwords:** NEXMA does not store end-user passwords — authentication of the customer's employees is handled through Microsoft 365 (Microsoft Entra ID) with MFA and Conditional Access enforced by the customer.

4.4. Nexma Connector

Nexma Connector communicates with the platform only outbound (HTTPS to nexma.app). No inbound ports need to be opened on workstations or inside the customer's network. Remote administration sessions and remote desktop are delivered through the open-source engine MeshCentral; remote desktop sessions are recorded in the NEXMA audit module (who connected, to which workstation, when and for how long).

5. Access control

5.1. Customer user access

The NEXMA platform enforces role-based access control (RBAC). Every user can only see the data and actions permitted by their role within their employer's tenant. Tenants are logically separated at both the database and API layer — data belonging to one customer is never exposed to another.

5.2. NEXMA personnel access

Access to customer data is granted only to NEXMA employees and contractors who need it to perform their duties (least-privilege principle). Every such access is:

- named — no shared accounts;
- protected by a strong password and a second factor (MFA);
- time-limited where possible (ad-hoc, task-scoped);
- recorded in application or system logs.

5.3. Infrastructure access

SSH access, database administration and the OVHcloud console are restricted to people who hold the platform administrator role. Accounts used to access infrastructure are protected with MFA. SSH keys are unique to each person — never shared and never stored in the code repository.

6. Technical measures

In addition to the controls described in the previous sections, NEXMA applies the following technical security measures:

- **Environment isolation** — production is separated from development and test environments at the network and authorisation level; production data is never used for testing.
- **Secrets and keys** — database passwords, API keys and tokens are stored outside the code repository, in environment variables on the hardened production server; keys are rotated whenever the team with access to them changes.
- **System updates** — the operating system, database and application libraries are kept up to date; critical security patches are deployed without undue delay after publication.
- **Event logging** — the application logs security-relevant events (sign-ins, administrative operations, access to personal data, remote sessions). Logs are protected against unauthorised modification.
- **Attack protection** — the application applies standard defensive mechanisms: input validation, parametrised database queries, CSRF/XSS protection, HTTP security headers and rate limiting on sensitive operations.
- **Data separation** — each customer (tenant) has its own isolated dataset identified by the Microsoft 365 tenant id; database queries are filtered by tenant id at every layer.
- **Application error monitoring** — NEXMA uses the Sentry service (EU region, Frankfurt) for centralised reporting of application exceptions and errors. The Sentry SDK runs server-side (Node.js + Edge runtime) and in the end-user browser. Privacy and configuration:
  - the `sendDefaultPii` option is **disabled** — Sentry does not collect IP addresses, cookies or request bodies;
  - before any event is sent, a NEXMA-side filter (*scrubber*) strips authorisation headers (including `Authorization`, `Cookie`, `x-cron-secret`, `x-mailbox-webhook-secret`) and secret URL parameters (such as `?secret=`, `?token=`, `?code=`, `?password=`) — both from the main request and from the breadcrumb history;

- the "Session Replay" feature (browser session recording) is disabled;
- tracing sample rate on the server side defaults to 10%; client-side tracing is disabled — only errors are transmitted.

7. Organisational measures

- **Confidentiality obligations** — everyone with access to customer data is bound in writing to confidentiality, with terms that survive the end of the engagement.
- **Training** — the NEXMA team undergoes internal training on data protection and application security; new team members are trained before being granted access to production data.
- **Clean desk and clean screen** — team workstations are encrypted (BitLocker or equivalent), require session lock after idle time, and are protected by a strong password and MFA for critical applications.
- **Secure development policy** — see section 11.

8. Incident management

8.1. External reports

Security reports (including potential vulnerabilities, unusual application behaviour or suspected unauthorised access) can be submitted to **security@nexma.app**. We encourage responsible disclosure with enough detail to reproduce the issue. NEXMA will not pursue legal action against good-faith researchers who follow generally accepted responsible-disclosure guidelines.

8.2. Response procedure

1. **Intake and acknowledgement** — every report is acknowledged within one business day and assigned a case number.
2. **Classification** — we assess the impact on confidentiality, integrity and availability and the number of potentially affected customers.
3. **Containment** — remediation starts immediately after classification; if needed we cut access, rotate keys and disable the affected feature.
4. **Analysis** — reconstruction of the event, data scope and root cause.
5. **Communication** — see 8.3.
6. **Corrective action** — technical or process changes designed to prevent recurrence.

8.3. Customer notification

If an incident constitutes a personal data breach under GDPR, NEXMA notifies the customer (data controller) **without undue delay and no later than 72 hours** after becoming aware of it. The notification includes:

- a description of the nature of the breach and, where possible, the categories and approximate number of data subjects and records concerned;
- a description of the likely consequences;
- a description of measures taken or planned to address the breach;
- contact details of the person handling the case at NEXMA.

9. Business continuity and backups

- **Database backups** are performed automatically at least once every 24 hours; they are encrypted and stored outside the production environment with **Wasabi Hot Cloud Storage** (Wasabi Technologies, Inc., region **eu-central-2** — Frankfurt, Germany, EEA), independently of the OVHcloud application hosting location.
- **RPO** (acceptable data-loss window) — at most 24 hours.
- **RTO** (time to restore service after a major failure) — target 24 hours for all key platform features.
- **Restore tests** — the database restore procedure is tested at least once every 12 months.
- **Escalation path** — in case of a major outage NEXMA publishes status updates and communicates with customers through the admin email address and the status page.

10. Subprocessors

NEXMA uses the following service providers that may have access to customer data to the extent necessary to deliver their services. The list is updated whenever the stack changes; earlier versions are available on request at privacy@nexma.app.

ENTITY	ROLE	DATA LOCATION	STATUS
Microsoft Ireland Operations Ltd. (Microsoft 365, Microsoft Entra ID, Graph API)	Identity provider and source of customer employee data; integrated on the customer side.	Data residency per the customer tenant (typically EU).	Active
OVH Groupe SAS (OVHcloud, region eu-central-waw)	Hosting provider for the NEXMA application and database.	Warsaw, Poland (EEA).	Active
Wasabi Technologies, Inc. (Wasabi Hot Cloud Storage, region eu-central-2)	Off-site storage of encrypted backups (database and backup files).	Frankfurt, Germany (EEA).	Active
Stripe Payments Europe Ltd.	Card payments and subscription billing (Stripe Billing); EUR net pricing; VAT via Stripe Tax.	Ireland (EEA); possible transfers to the USA under Standard Contractual Clauses.	Active
Functional Software, Inc. d/b/a Sentry	Centralised application error monitoring (Sentry, EU region). Scope described in section 6 — no IP address, with active secret filtering on the NEXMA side.	Frankfurt, Germany — EU region (EEA). Data does not leave the EEA.	Active

NEXMA gives customers at least 30 days' advance notice by email of any planned change to or addition of a subprocessor, and allows reasoned objections.

11. Software development

- the application code lives in a private repository with access controls and full change history;
- production changes go through technical review before deployment;
- production deployments are tracked and can be rolled back quickly if needed;
- external dependencies are updated and scanned for known vulnerabilities;
- access to the production environment from developer tooling is restricted to authorised people only.

12. Audits and reviews

NEXMA internally reviews this Policy at least once every 12 months and after every material change to the architecture, the subprocessor list or a significant security incident. Customers may request information about the current state of security controls at **security@nexma.app**. For justified requests — in particular those driven by the customer's compliance team — NEXMA shares detailed documentation under a non-disclosure agreement.

13. Data retention and deletion

- operational data (accounts, requests, events) is retained for the duration of the contract and for 30 days after it ends;
- afterwards, production data is deleted and backups are overwritten through normal rotation no later than within the following 90 days;
- on written request from the customer (sent from the administrative address) NEXMA confirms deletion in writing or by email;
- detailed rules for data deletion and return are set out in the Data Processing Agreement (DPA).

14. Changes to this policy

NEXMA may update this Policy to reflect changes to the service, the applicable law or the security controls in place. Material changes are communicated by email and published at **nexma.app/documents**. The effective date of the latest update is shown on the cover page.

This document is owned by **SYLWESTER SZAFERSKI** and has been prepared in good faith based on the architecture of the platform as of the publication date. In case of any conflict between the Policy and the Data Processing Agreement (DPA) signed with the customer, the DPA prevails.