



Effective document

# Privacy Policy

What personal data NEXMA processes, on what legal basis, for how long, and the rights available to data subjects.

---

ISSUER

SYLWESTER SZAFERSKI

VERSION

1.2

EFFECTIVE FROM

May 23, 2026

NEXT REVIEW

Within 12 months

GDPR CONTACT

[privacy@nexma.app](mailto:privacy@nexma.app)

DOCUMENT HOME

[nexma.app/documents](https://nexma.app/documents)

## TABLE OF CONTENTS

- |  |  |
|--|--|
| <a href="#">1. Who this document is for</a>  | <a href="#">8. Rights of data subjects</a>           |
| <a href="#">2. Controller and processor</a>  | <a href="#">9. Automated decisions and profiling</a> |
| <a href="#">3. What data we process</a>      | <a href="#">10. Cookies and technical logs</a>       |
| <a href="#">4. Purposes and legal bases</a>  | <a href="#">11. Data security</a>                    |
| <a href="#">5. Retention periods</a>         | <a href="#">12. Contact and complaints</a>           |
| <a href="#">6. With whom we share data</a>   | <a href="#">13. Changes to this policy</a>           |
| <a href="#">7. Transfers outside the EEA</a> |  |

## 1. Who this document is for

This policy describes how NEXMA processes personal data in two main scenarios:

- 1. Data of users of the NEXMA platform** — employees and contractors of companies that use our application. With respect to this data NEXMA acts as a data processor on behalf of the employer, who is the controller.
- 2. Data of people who contact NEXMA directly** — for example through the contact form, by email or in connection with subscription sales and support. Here NEXMA acts as an independent controller.

The principles described below apply to both scenarios. Where differences exist, we point them out explicitly.

## 2. Controller and processor

The issuer of this policy:

### **SYLWESTER SZAFERSKI**

Tax ID (NIP): 5213906939

Statistical number (REGON): 387026755

Business address: Dalekie 61a, 07-211 Długosiodło

Contact: [privacy@nexma.app](mailto:privacy@nexma.app)

**Please note.** If you are an employee of a company that uses NEXMA and want to know more about how your data is processed in the application, please contact your employer's HR or IT department first — your employer is the controller of your data. NEXMA acts on behalf of your employer and can provide information through them.

### 3. What data we process

#### 3.1. Employee data of customers (NEXMA acting as processor)

In the course of delivering the service NEXMA may process the following categories of customer-employee data, synchronised from the customer's Microsoft 365 or entered when using the platform:

- identification data: first name, last name, work email, Microsoft Entra ID identifier (UPN, objectId), tenant id;
- organisational data: job title, department, manager, location, work phone number (if present in M365);
- permission data: membership in Microsoft 365 groups, Teams, shared mailboxes and SharePoint sites;
- device data assigned to the user: host name, serial number, Intune id, BitLocker status, IP address, installed software state — to the extent the customer uses the workstation-management modules;
- activity data: sign-in logs to the platform, history of administrative actions, access-request history and status, helpdesk ticket history;
- content of requests and tickets entered by users in the application (for example a description of requested access, a message to a manager, attachments);
- recordings of remote desktop and remote-support sessions performed through Nexma Connector, together with metadata (who connected, when, for how long and to which workstation).

The actual scope of data depends on how the customer configures the platform — the customer decides which modules to enable and which Microsoft 365 data to expose to NEXMA.

#### 3.2. Data of people contacting NEXMA (NEXMA acting as controller)

If you contact NEXMA outside the scope of using the platform, we may process:

- contact data: first name, last name, email, phone number, company name, job title;
- contents and history of correspondence;
- billing data — to the extent required for invoicing and payment processing (entity name, address, tax id, bank account);
- data related to your use of the nexma.app website (see section 10).

## 4. Purposes and legal bases

PURPOSE	WHO IT CONCERNS	LEGAL BASIS (GDPR)
Delivery of the NEXMA service on behalf of the customer (employee self-service, access requests, workstation management).	Customer's employees and contractors.	Art. 28 GDPR in conjunction with Art. 6(1)(b) or (f) GDPR on the side of the controller (customer).
Entering into and performing the contract with the customer, subscription and invoicing.	Customer contact persons.	Art. 6(1)(b) GDPR (contract performance) and Art. 6(1)(c) GDPR (tax and accounting obligations).
Responding to enquiries addressed to NEXMA (contact form, email).	People contacting NEXMA.	Art. 6(1)(f) GDPR — legitimate interest of handling correspondence.
Ensuring the security of the application, incident response, defence against abuse.	All platform users.	Art. 6(1)(f) GDPR — legitimate interest of NEXMA and of the customer.
Direct marketing (newsletter, product updates) — only after opt-in consent.	People who gave consent.	Art. 6(1)(a) GDPR — consent, revocable at any time.

## 5. Retention periods

- **Customer employee data processed as processor** — for the duration of the contract with the customer. After termination the data is deleted within the timeframe described in the Information Security Policy (within 30 days from the production database; within 90 days from backups through normal rotation), unless the customer requests earlier deletion or return under the DPA.
- **Data of people contacting NEXMA** — for as long as necessary to handle the matter and additionally for the limitation period of any possible claims.
- **Billing and accounting data** — for as long as required by law (typically five years from the end of the fiscal year in which the document was issued).
- **Security logs** — up to 12 months, unless they form part of an ongoing investigation, in which case until its conclusion.
- **Data processed on the basis of consent** — until consent is withdrawn.

## 6. With whom we share data

Personal data is shared only with entities that provide an adequate level of protection and that are bound by appropriate contracts. Current list of our subprocessors:

ENTITY	ROLE	LOCATION
Microsoft Ireland Operations Ltd.	Provider of Microsoft 365, Microsoft Entra ID, Graph API — source of customer employee data.	Ireland (EEA); data residency depends on the customer tenant.
OVH Groupe SAS (OVHcloud)	Hosting for the NEXMA application and database (region eu-central-waw, zone eu-central-waw-a).	Warsaw, Poland (EEA).
Wasabi Technologies, Inc.	Storage of encrypted database and platform environment backups (Wasabi Hot Cloud Storage, region eu-central-2).	Frankfurt, Germany (EEA); data does not leave the EEA.
Stripe Payments Europe Ltd.	Card payments and recurring subscription billing (Stripe Billing); EUR net fees; VAT via Stripe Tax based on buyer details.	Ireland (EEA); possible transfers to the USA — see section 7.
Functional Software, Inc. d/b/a Sentry	Application error monitoring (Sentry SaaS, EU region). Receives only minimised technical error data — no end-user IP address and no personal identifiers, after automatic secret filtering performed by NEXMA before transmission (see section 10 and the <b>Information Security Policy</b> ).	Frankfurt, Germany (EU region; data does not leave the EEA).

Additionally, data may be disclosed to public authorities upon their request, to the extent and in the form required by law.

## 7. Transfers outside the EEA

The primary NEXMA environment is located in Poland, within the European Economic Area (EEA). The Sentry error monitoring service is used in the EU region (data centre in Frankfurt, Germany) — diagnostic data does not leave the EEA. If the delivery of the service causes any transfer of data outside the EEA (for example when using Microsoft or Stripe services), such transfer is based solely on mechanisms ensuring an adequate level of protection within the meaning of Art. 46 GDPR, in particular:

- European Commission adequacy decisions where applicable;
- Standard Contractual Clauses approved by the European Commission;

- additional safeguards implemented by the supplier (encryption, pseudonymisation).

## 8. Rights of data subjects

Under GDPR you have the right:

- **of access** — to learn whether and what data we process about you;
- **of rectification** — to have inaccurate or incomplete data corrected;
- **of erasure** (*right to be forgotten*) — in the situations set out in Art. 17 GDPR;
- **to restrict processing** — in the situations set out in Art. 18 GDPR;
- **to object** — to processing based on legitimate interest;
- **to data portability** — to receive your data in a machine-readable format;
- **to withdraw consent** at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

To exercise any of these rights, write to **privacy@nexma.app**. If we process your data on behalf of your employer (as processor), we will forward your request to the controller (your employer) and let you know we have done so.

You also have the right to lodge a complaint with the President of the Personal Data Protection Office (Prezes UODO, ul. Stawki 2, 00-193 Warszawa, Poland) if you believe that the processing of your personal data infringes GDPR.

## 9. Automated decisions and profiling

NEXMA does not take automated decisions about you that produce legal effects concerning you or that similarly significantly affect you. The platform supports decision processes (for example access requests), but the actual decision to approve or reject access is always taken by a human designated by the controller (a manager, a system administrator, an HR manager).

## 10. Cookies and technical logs

The nexma.app website and the application panel may use cookies and similar technologies in a limited scope:

- **Technical and session cookies** — necessary for the authenticated session to work. Without them the application cannot function; they do not require consent.
- **Preference cookies** — remember the language and light/dark theme. You can disable them in your browser settings.

- **Server technical logs** — IP address, user-agent header, request timestamp; collected for security and troubleshooting. Retained for the period described in section 5.
- **Application error monitoring (Sentry)** — when an application error occurs, a minimal set of technical data is sent to the Sentry service (EU region, Frankfurt): exception type, stack trace, application release identifier, timestamp, application route URL and the browser user-agent header. The end-user IP address is **not** transmitted (the `sendDefaultPii` option is disabled). Authorisation headers (such as `Authorization`, `Cookie`) and secret URL parameters are stripped on the NEXMA side before transmission. The "Session Replay" feature (browser session recording) is not enabled. Data does not leave the EEA.

NEXMA does not currently use marketing cookies or third-party trackers. If that changes, we will update this policy and introduce a consent mechanism (cookie banner).

## 11. Data security

The technical and organisational measures used by NEXMA to protect personal data are described in detail in the **Information Security Policy** available at [nexma.app/documents](https://nexma.app/documents). They include, among others, encryption in transit and at rest, role-based access control, mandatory multi-factor authentication for NEXMA personnel, logging of security-relevant events and incident-response procedures.

## 12. Contact and complaints

Questions and requests related to this policy or to the processing of personal data should be sent to:

**privacy@nexma.app**

We respond within the timeframe set by GDPR — without undue delay and no later than 30 days after receiving the request (extendable by 60 days for complex cases).

## 13. Changes to this policy

This policy may change in connection with changes in law, the scope of the service or the list of subprocessors. Each version is dated and available at [nexma.app/documents](https://nexma.app/documents). Material changes will be communicated directly to customers by email.

---

This document has been prepared by **SYLWESTER SZAFERSKI** and becomes effective on its publication at [nexma.app/documents](https://nexma.app/documents). In case of any conflict between the Privacy Policy and the Data Processing Agreement (DPA) concluded with the customer regarding the processing of customer employee data, the DPA prevails.