NEXMA

Effective document

Data Processing Agreement (DPA)

Integral part of the agreement for the use of the NEXMA platform concluded between the customer and SYLWESTER SZAFERSKI.

ISSUER (PROCESSOR)
SYLWESTER SZAFERSKI

VERSION
1.2

EFFECTIVE FROM
May 23, 2026

LEGAL FRAMEWORK
GDPR (Regulation 2016/679)

CONTACT
legal@nexma.app

DOCUMENT HOME
nexma.app/documents

Processor status. The processor under this agreement is **SYLWESTER SZAFERSKI** (NIP 5213906939, REGON 387026755, Dalekie 61a, 07-211 Długosiodło).

1. Parties

PROCESSOR

SYLWESTER SZAFERSKI
Tax ID (NIP): 5213906939
Statistical number (REGON): 387026755
Address: Dalekie 61a, 07-211 Długosiodło
Represented by: Sylwester Szaferski
Contact: legal@nexma.app (contract and legal documentation), privacy@nexma.app (GDPR, TOM, subprocessors), security@nexma.app (security incidents).

CONTROLLER

Customer — the entity that has entered into the agreement with NEXMA for the use of the platform (by accepting the terms of service or by signing an individual agreement).

The customer's data is identified in the platform's admin panel and on the invoices issued to the customer.

2. Definitions

GDPR
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Main agreement
The agreement for the use of the NEXMA platform concluded between the parties (terms of service, subscription contract or equivalent).

Entrusted data
Personal data of the controller's employees, contractors and other people connected to the controller, which NEXMA processes on behalf of the controller in connection with the performance of the main agreement. The detailed scope is described in Annex 1.

Subprocessor
A further processor engaged by NEXMA. The current list is in Annex 2.

Incident
A personal data breach within the meaning of Art. 4(12) GDPR.

TOM

Technical and organisational measures within the meaning of Art. 32 GDPR, described in Annex 3 and in the NEXMA Information Security Policy available at nexma.app/documents.

3. Subject and purpose of the processing

The controller entrusts NEXMA, and NEXMA accepts, the processing of the entrusted data solely for the purpose and to the extent necessary to:

- deliver the NEXMA service in accordance with the main agreement,
- maintain, configure and develop the platform,
- respond to data subject rights exercised against the controller,
- secure the platform and respond to incidents,
- comply with any legal obligations binding on NEXMA.

NEXMA does not process the entrusted data for its own purposes. In particular, NEXMA does not profile data subjects for its own marketing purposes and does not sell the entrusted data.

4. Processor's obligations

NEXMA undertakes to:

1. process the entrusted data only on documented instructions from the controller, including transfers to a third country or international organisation, unless required to do so by Union or Member State law — in which case NEXMA will inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
2. ensure that persons authorised to process the entrusted data have committed to confidentiality or are under an appropriate statutory obligation of confidentiality;
3. take all measures required pursuant to Art. 32 GDPR (security of processing), within the scope described in Annex 3;
4. comply with the conditions for engaging another processor referred to in Art. 28(2) and (4) GDPR (see section 7);
5. taking into account the nature of the processing, assist the controller by appropriate technical and organisational measures to fulfil its obligation to respond to requests for exercising data subject rights (Art. 12–22 GDPR);
6. assist the controller in complying with the obligations pursuant to Art. 32–36 GDPR, in particular regarding security, breach notification and data protection impact assessments;
7. at the end of the provision of services, return or delete the entrusted data in line with section 12;

8. make available to the controller all information necessary to demonstrate compliance with Art. 28 GDPR and allow for and contribute to audits by the controller (or an auditor) as described in section 11.

5. Controller's obligations

The controller undertakes to:

1. process personal data in accordance with GDPR and other applicable law;
2. issue processing instructions in a form that allows documentation — in particular, instructions resulting from the configuration of the platform are considered documented instructions of the controller;
3. inform users of the platform (data subjects) of the processing of their data to the extent required by GDPR — the information duty regarding processing within the NEXMA platform rests on the controller;
4. ensure a lawful legal basis for the processing of data transferred to NEXMA, including for obtaining data from third parties (for example Microsoft 365 integrations);
5. not transfer to NEXMA special categories of data (Art. 9 GDPR) or data relating to criminal convictions and offences (Art. 10 GDPR) unless necessary and previously agreed with NEXMA.

6. Security of processing

NEXMA applies technical and organisational measures providing a level of security appropriate to the risk to the rights and freedoms of natural persons, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing. The detailed description is set out in Annex 3 and in the published Information Security Policy.

The parties agree that the measures described in Annex 3 comply with Art. 32 GDPR. NEXMA may modify those measures as long as the change does not lower the overall level of security of the processing.

7. Use of subprocessors

The controller grants NEXMA general authorisation to engage the subprocessors listed in Annex 2. NEXMA ensures that each subprocessor is bound — by contract or another legal instrument — by data protection obligations equivalent to those of NEXMA under this agreement.

NEXMA notifies the controller of any intended addition or replacement of a subprocessor at least 30 days in advance by email and allows reasoned objections. If a reasoned objection is raised, the parties will endeavour to agree; if they do not, the controller may terminate the main agreement with regard to the affected scope upon 30 days' notice.

8. Transfers outside the EEA

NEXMA hosts the platform within Poland (OVHcloud, region eu-central-waw). If delivery of the service requires a transfer of the entrusted data outside the EEA (for example due to the global footprint of Microsoft 365 or payment processors), it is based solely on the mechanisms referred to in Chapter V of GDPR — in particular the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914.

9. Data subject rights

If NEXMA receives a request from a data subject whose entrusted data it processes, NEXMA forwards the request to the controller without undue delay, without taking substantive action on its own, unless requested to do so by the controller.

NEXMA provides the controller with platform tools that allow it to service such requests (access, correction, export, account deletion). Where serving a request requires operational action from NEXMA (for example permanent deletion from backups), NEXMA carries it out promptly upon the controller's written request.

10. Incident notification

NEXMA notifies the controller of every confirmed incident affecting the entrusted data **without undue delay and no later than 72 hours after becoming aware of it**. The notification is sent by email to the contact address designated by the controller in the platform's admin panel and contains the elements listed in Art. 33(3) GDPR, to the extent known to NEXMA at the time of notification. Further information is provided as soon as it becomes available.

NEXMA provides the controller with the assistance necessary for the controller to comply with its obligation to notify the supervisory authority and the data subjects of a personal data breach (Art. 33–34 GDPR).

11. Audits

Upon request, NEXMA provides the controller with information demonstrating performance of this agreement and application of the TOM. Requests should be sent to **privacy@nexma.app**.

The controller has the right to audit on the following terms:

1. First, the controller relies on the documentation provided by NEXMA (Information Security Policy, replies to security questionnaires, platform status reports) — this form is considered a sufficient audit for most cases.
2. In justified cases the controller may conduct an audit at NEXMA's premises or remotely, with at least 30 days' advance notice, on business days, to the extent necessary to verify compliance

with Art. 28 GDPR. The cost of an audit requested by an individual controller is borne by the controller, unless the audit reveals material non-compliance on the NEXMA side.

3. The audit must not disrupt NEXMA's normal operations or compromise the confidentiality of data of other NEXMA customers.

12. End of processing, return and deletion of data

After the provision of services under the main agreement ends — depending on the controller's instruction expressed in a written request delivered to NEXMA no later than within 30 days of termination — NEXMA will:

- return the entrusted data to the controller in the standard export format provided by the platform, or
- delete the entrusted data and confirm deletion in writing (including by email).

In the absence of an explicit instruction within that period, NEXMA deletes the entrusted data in accordance with the retention policy described in the Information Security Policy. NEXMA may retain data only to the extent required by Union or Member State law.

13. Liability

The liability of the parties for a breach of this agreement is governed by the main agreement, provided that any limitations of liability it contains do not apply in cases where by law they cannot be effectively limited (in particular claims of data subjects brought directly under Art. 82 GDPR).

Each party bears its own responsibility for any GDPR infringements committed within its role — controller or processor.

14. Final provisions

1. This agreement enters into force upon conclusion of the main agreement (or upon acceptance of the terms of service, if it forms an integral part of them) and remains in force for the duration of the main agreement and as long as NEXMA processes the entrusted data.
2. Matters not regulated here are governed by GDPR and by Polish law applicable to the extent relevant.
3. The court competent for disputes arising from this agreement is the court with jurisdiction over NEXMA's registered office, unless mandatory provisions provide otherwise.
4. Any modification of the agreement requires written or documentary form on pain of nullity; updates of annexes performed under section 7 (updates of the subprocessor list) are not considered modifications.

5. If any provision of this agreement is held to be invalid or ineffective, this does not affect the validity of the remaining provisions.

A. Annex 1 — Description of the processing

Subject matter, nature and purpose of the processing

Delivery of the NEXMA service as a platform for employee self-service and IT management around Microsoft 365. The processing is an automated processing of personal data in an IT system and, in the scope of remote-support sessions, a supervised human access to user workstations.

Duration of the processing

Duration of the main agreement and the retention period described in the Information Security Policy (up to 30 days in production and up to 90 days in backups after termination).

Types and categories of data

- identification data (first name, last name, work email, Microsoft Entra ID identifier, tenant id);
- organisational data (job title, department, manager, location);
- permission data in Microsoft 365;
- device data assigned to the user and software state;
- activity logs in the platform;
- content of requests and tickets entered by the user;
- metadata and recordings of remote-support sessions.

Categories of data subjects

- the controller's employees,
- the controller's contractors and vendors granted access to the platform by the controller,
- external (guest) users, if the controller shares resources with them through the platform.

B. Annex 2 — List of subprocessors

ENTITY	ROLE	DATA LOCATION	STATUS
Microsoft Ireland Operations Ltd.	Microsoft 365, Microsoft Entra ID, Graph API — source of the controller's employee data.	Data residency per the controller tenant (typically EU).	Active
OVH Groupe SAS (OVHcloud)	Hosting of the NEXMA application and database.	Warsaw, Poland — region eu-central-waw, zone eu-central-waw-a (EEA).	Active
Wasabi Technologies, Inc.	Storage of encrypted database and platform environment backups (Wasabi Hot Cloud Storage, region eu-central-2).	Frankfurt, Germany — region eu-central-2 (EEA); data does not leave the EEA.	Active
Stripe Payments Europe Ltd.	Card payments and subscription billing (Stripe Billing); fees in EUR net; VAT via Stripe Tax.	Ireland (EEA); possible transfers to the USA under Standard Contractual Clauses.	Active
Functional Software, Inc. d/b/a Sentry (132 Hawthorne St., San Francisco, CA 94107, USA)	Application error monitoring (Sentry SaaS, EU region). Receives only minimised technical error data (exception type, stack trace, release identifier, timestamp, application route URL and the user-agent header) without the end-user IP address and without personal identifiers. Authorisation headers and secret URL parameters are filtered on the NEXMA side before transmission.	Frankfurt, Germany — EU region (de.sentry.io). Data does not leave the EEA. Despite the parent company's seat in the USA, the chosen processing region remains within the EEA; where required, Standard Contractual Clauses (Commission Decision 2021/914) apply on the basis of Sentry's online DPA.	Active

Sub-processor statuses may evolve as the platform develops. Archived billing records may include historical entries from former payment providers, only as needed for accounting and compliance.

C. Annex 3 — Technical and organisational measures

The measures listed below correspond to the requirements of Art. 32 GDPR. The full description is set out in the published Information Security Policy (nexma.app/documents).

ACCESS CONTROL

- role-based access control (RBAC) at the application level;
- integration with Microsoft Entra ID for end-user authentication — MFA and Conditional Access enforced by the customer;
- mandatory MFA for NEXMA personnel;
- named, non-shared administrative accounts;
- least-privilege principle.

ENCRYPTION

- TLS 1.2+ for all client–platform traffic and for traffic between the platform and Nexma Connector;
- encryption at rest at the storage backend level of the cloud provider (AES-256);
- encrypted backups.

TENANT SEPARATION

- logical separation of customer data at the database and API level;
- every application query is filtered by tenant id;
- no shared operational resources directly exposed between tenants.

MONITORING AND INCIDENT RESPONSE

- collection of security-relevant event logs;
- incident handling procedure with 72-hour notification to the controller;
- reporting channel: security@nexma.app.

BUSINESS CONTINUITY

- automated backups at least once every 24 hours;
- target RPO 24 hours, RTO 24 hours;
- annual restore test.

ORGANISATION

- written confidentiality obligations for people with access to data;
- data protection training for team members;
- secure configuration of NEXMA team workstations (disk encryption, screen lock, updates);
- code review and controlled production deployments.

15. Signatures

This agreement is concluded in documentary form by accepting the NEXMA terms of service. If an individual written or qualified-signature contract is used instead, the parties sign below.

Processor	Controller
SYLWESTER SZAFERSKI Sylwester Szaferski	[customer data] [representative name]
date and signature	date and signature

This data processing agreement is an integral part of the NEXMA terms of service. In case of any conflict between its content and the terms of service regarding the processing of personal data, the provisions of this agreement prevail.