Nakmo Cloud

DATA PROCESSING AGREEMENT (DPA)

Last updated: May 25, 2026

---

1. Nature and Scope of the Agreement

This Data Processing Agreement ("DPA") forms an integral part of the Service Agreement or other underlying agreement for the provision of services (the "Principal Agreement") between Nakmo Cloud, a legal entity registered under the laws of the Republic of Armenia (the "Controller"), and the service provider engaged to process data on behalf of the Controller (the "Processor").

This DPA sets out the parties' respective obligations and rights regarding the processing of personal data in accordance with the Republic of Armenia Law "On Protection of Personal Data" (HO-119-N) and the EU General Data Protection Regulation (GDPR, Regulation (EU) 2016/679). In the event of any conflict between the Principal Agreement and this DPA, the provisions of this DPA shall prevail with respect to the protection of personal data.

---

2. Definitions

The terms used in this DPA shall have the meanings set forth in the GDPR and the RA Law "On Protection of Personal Data."

"Instruction" means a written direction issued by the Controller to the Processor, directing the Processor to perform specific actions with regard to personal data (including, but not limited to, modifying, deleting, or transferring data).

"Sub-processor" means any third party appointed by or on behalf of the Processor to process personal data on behalf of the Controller.

"Technical and Organizational Measures" means measures aimed at protecting personal data against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure, or access.

"Platform Store Processors" means Apple Inc. (Apple App Store) and Google LLC (Google Play Store), which process payment and transaction data exclusively and independently on behalf of end-users in connection with In-App Purchases. Platform Store Processors act as independent data controllers with respect to payment processing and are not sub-processors of the Controller under this DPA.

---

3. Subject Matter and Duration

3.1 Subject Matter

The Processor shall process personal data only for the purpose of providing cloud storage, media processing, analytics, and related infrastructure services as defined in the Principal Agreement. This excludes payment processing, which is handled exclusively by Platform Store Processors independently of this DPA.

3.2 Duration

Processing shall be performed for the duration of the Principal Agreement and until final deletion or return of data as required by the Controller's retention policy or applicable law.

---

4. Type of Data and Categories of Data Subjects

Data Subjects: Users of the Nakmo Cloud application, including international consumers and EU citizens.

Data Categories:

- Media files (photos and videos) uploaded by users;
- EXIF metadata (GPS coordinates, timestamps, device information);
- Account identifiers (name, email address, encrypted credentials);
- Technical telemetry (device identifiers, IP addresses, crash logs, app usage data);
- Cloud Karma activity data (Karma balance, daily login timestamps, video completion records);
- Subscription status data (active/expired/cancelled status, subscription tier, renewal date, and anonymized Platform Store user tokens received from Apple or Google). **Payment card details, bank account numbers, and full payment credentials are not processed by the Controller and are not within the scope of this DPA.**

---

5. Obligations of the Processor

The Processor agrees to:

Compliance with Instructions: Process personal data only on documented instructions from the Controller, unless required to do otherwise by applicable law. In such cases, the Processor shall inform the Controller of the legal requirement before processing, unless legally prohibited from doing so.

Confidentiality: Ensure that all personnel authorized to process personal data are subject to binding confidentiality obligations. Access to personal data shall be limited to personnel who require it for the performance of their duties.

Security: Implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, without limitation:

- Encryption of personal data at rest (AES-256) and in transit (TLS 1.3);
- Pseudonymization of data where appropriate;
- Procedures for testing, assessing, and evaluating the effectiveness of security measures on a regular basis;
- Physical security controls for data centers and systems.

Assistance: Assist the Controller in responding to requests from data subjects exercising their rights under the GDPR and Armenian law (access, rectification, erasure, portability, restriction, objection). With respect to payment-related data held by Platform Store Processors, the Processor shall direct data subjects to the applicable Platform Store for such requests.

Breach Notification: Notify the Controller **without undue delay** after becoming aware of any personal data incident or breach, or immediately upon receiving a corresponding breach notification from a Sub-processor (e.g., an underlying infrastructure supplier). The Processor shall provide the Controller with all available and necessary technical details to enable the Controller to meet its legal reporting obligations toward supervisory authorities and affected users.

Data Protection Impact Assessment: Assist the Controller in conducting data protection impact assessments (DPIAs) and prior consultations with supervisory authorities where required under Article 35-36 GDPR.

---

6. Sub-processing

The Processor shall not engage another sub-processor without prior written authorization from the Controller. Where general written authorization is given, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of sub-processors, giving the Controller a reasonable opportunity to object.

The following sub-processors are authorized as of the date of this DPA:

- **Amazon Web Services (AWS)** — cloud infrastructure and storage;
- **Google Cloud Platform (GCP)** — cloud infrastructure;
- **Hetzner Online GmbH** — cloud infrastructure;
- **Cloudflare, Inc.** — edge caching and content delivery (Cloudflare R2);
- **SendGrid / Twilio** — transactional email delivery;
- **Google Firebase / Mixpanel** — analytics and performance monitoring.

Note on Platform Store Processors: Apple Inc. and Google LLC act as independent data controllers with respect to payment processing for In-App Purchases. They are not sub-processors of Nakmo Cloud under this DPA. Their processing of payment data is governed exclusively by their own terms of service and privacy policies.

---

7. International Data Transfers

Any transfer of personal data outside the Republic of Armenia or the EEA shall comply with:

- Standard Contractual Clauses (SCCs) approved by the European Commission;
- Bilateral agreements ensuring an adequate level of protection as mandated by the RA Personal Data Protection Agency;
- Any applicable adequacy decision or equivalent safeguard recognized under GDPR.

The Processor shall not transfer personal data to a third country or an international organization unless such transfer is made on the basis of one of the mechanisms listed above. Platform Store Processors (Apple and Google) manage their own international transfer compliance independently.

---

8. Audit Rights

The Processor shall make available all information reasonably necessary to demonstrate compliance with the obligations set out in this DPA and Article 28 of the GDPR. The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or a Controller-mandated auditor, subject to reasonable advance notice and the Processor's reasonable security and confidentiality requirements.

---

9. Deletion or Return of Data

Upon termination of services or the Principal Agreement, the Processor shall, at the Controller's written choice:

- Delete all personal data and confirm in writing that deletion has been completed; or
- Return all personal data to the Controller in a structured, commonly used, and machine-readable format.

This obligation shall apply to all copies of personal data held by the Processor, including in backups, unless applicable law requires continued storage. In such cases, the Processor shall inform the Controller and ensure the data remains subject to appropriate protective measures.

---

10. Record of Processing Activities

The Processor shall maintain, to the extent required under Article 30(2) GDPR, a record of all categories of processing activities carried out on behalf of the Controller, including the information specified in Article 30(2)(a)-(d) GDPR.

---

11. Governing Law and Jurisdiction

This DPA is governed by the laws of the Republic of Armenia. Any disputes arising out of or in connection with this DPA shall be subject to the exclusive jurisdiction of the competent courts in Yerevan, Republic of Armenia.

---

12. Contact Information

Nakmo Cloud (Data Controller)

Armenia, Yerevan, Minsk str. 17-19, Apr. 10

Email: support@nakmo.net

Phone: +374 44 16 66 20

Data Protection Officer: support@nakmo.net