Nakmo Cloud

PRIVACY POLICY

Last updated: May 26, 2026

---

1. Introduction, Scope, and Data Controller

1.1 Data Controller and Framework

This Privacy Policy (the "Policy") defines and governs the protocols for the collection, processing, usage, storage, and protection of data by Nakmo Cloud, a legal entity incorporated and operating under the laws of the Republic of Armenia (hereinafter referred to as the **"Company"**, **"Nakmo Cloud"**, **"we"**, **"us"**, or **"our"**).

For the purposes of the European Union General Data Protection Regulation (GDPR) and the Republic of Armenia Law "On Protection of Personal Data" (HO-119-N), Nakmo Cloud acts as the **Data Controller** of your Personal Data.

Our Legal Address: Armenia, Yerevan, Minsk str. 17-19, Apr. 10
Contact Email: support@nakmo.net

1.2 Scope and Applicability

This Policy is a binding instrument that applies to all individuals ("User", "you", or "your") who download, install, register an account with, or otherwise access the Nakmo Cloud cloud-based media storage application via official mobile platforms (Apple App Store, Google Play Store) or the web application interface (collectively, the "Service").

By registering an account or interacting with the Service, you acknowledge that your information will be processed strictly in accordance with this Policy. This document serves as a compliance notice under Articles 13 and 14 of the GDPR, the Armenian Law HO-119-N, and incorporates applicable provisions of US state privacy laws (including the California Consumer Privacy Act - CCPA/CPRA) where relevant.

1.3 Critical Distinction: Personal Data vs. User Content

To ensure absolute clarity, this Policy distinguishes between two categories of information:

- **Personal Data:** Information relating to an identified or identifiable individual (e.g., email address, account settings, device identifiers, IP addresses, and billing logs).
- **User Content:** The actual media files (photos, videos, audio, and associated metadata like EXIF tags) uploaded and stored by you within your private cloud storage allocation.

The Company processes Personal Data for service administration and analytics, whereas User Content is treated with strict confidentiality as your private property and is subject to automated technical storage protocols described herein.

---

2. Definitions

2.1 Personal Data

"Personal Data" means any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (IP address), or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

2.2 User Content

"User Content" refers to any and all digital media files, including but not limited to photos, videos, images, screenshots, and audio recordings, uploaded, stored, or transmitted by the User to the Nakmo Cloud infrastructure for private backup and management.

2.3 Metadata

"Metadata" means technical information embedded in, appended to, or associated with User Content, including Exchangeable Image File Format (EXIF) data, GPS/geolocation coordinates, creation timestamps, camera model settings, file sizes, and structural device specifications. For the purposes of this Policy, Metadata of uploaded files is treated with the same strict confidentiality as User Content.

2.4 Processing

"Processing" means any operation or set of operations performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

2.5 Data Controller and Data Processor

- **"Data Controller"** means the legal entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. For this Service, the Data Controller is Nakmo Cloud.
- **"Data Processor"** means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Data Controller (e.g., cloud infrastructure providers or database operators).

2.6 Platform Store

"Platform Store" means the official digital distribution platforms — specifically the Apple App Store operated by Apple Inc. and the Google Play Store operated by Google LLC — through which the Nakmo Cloud application is distributed, updated, and through which In-App Purchases or Subscriptions are processed.

2.7 Advertising and Device Identifiers

"Advertising and Device Identifiers" means unique, resettable technical identifiers provided by the mobile operating system (such as Apple's Identifier for Advertisers - IDFA, and Google Advertising ID - GAID) used strictly to facilitate the reward mechanics within the Cloud Karma System via integrated third-party ad networks.

2.8 Automated Media Indexing (formerly AI Analysis)

"Automated Media Indexing" refers to the restricted use of automated technical algorithms, computer vision, and neural networks executing tasks solely to index, categorize, and detect objects or scenes within User Content. This operation is performed strictly to enable local searchability and automated categorization features for the User, and **never** to train external machine learning models or identify specific natural persons without explicit consent.

---

3. Identity of the Data Controller and Data Protection Officer

3.1 Legal Identity

The Data Controller responsible for the lawful, fair, and transparent processing of your Personal Data under this Policy is:

- **Entity Name:** Nakmo Cloud
- **Jurisdiction:** Incorporated and existing under the laws of the Republic of Armenia
- **Registered Address:** Republic of Armenia, Yerevan, Minsk str. 17-19, Apr. 10

3.2 Principles of Processing

As the Data Controller, Nakmo Cloud establishes the technical means and business purposes of data processing. We strictly adhere to core international data protection principles, ensuring that your Personal Data is:

- Processed lawfully, fairly, and transparently;
- Collected for specified, explicit, and legitimate purposes;
- Adequate, relevant, and limited to what is necessary (data minimization);
- Accurate and, where necessary, kept up to date;
- Stored in a form which permits identification for no longer than is necessary;
- Processed with appropriate security, integrity, and confidentiality measures.

3.3 Data Protection Officer (DPO)

To ensure the continuous alignment of our cloud services with global privacy standards, Nakmo Cloud has appointed an internal Data Protection Officer (DPO). The DPO independently oversees our privacy strategy, infrastructure risk assessments, and compliance implementation.

3.4 Privacy Inquiries and Direct Communication Channel

If you have any questions, concerns, or wish to exercise your legal rights regarding your Personal Data or this Privacy Policy, you may contact our DPO directly:

- **Dedicated Email Contact:** legal@nakmo.net
- **Postal Address:** Attn: Data Protection Officer, Nakmo Cloud, Republic of Armenia, Yerevan, Minsk str. 17-19, Apr. 10

The Company will investigate and attempt to resolve any complaints or requests regarding the use or disclosure of Personal Data within the statutory timeframes established by the GDPR and Armenian legislation (typically within thirty (30) days from receipt of a verified request).

---

4. Applicable Laws and Regulatory Framework

4.1 Dual-Layered Legal Foundation

The data processing operations conducted by Nakmo Cloud are governed by a robust, multi-jurisdictional legal framework designed to safeguard user privacy across global borders:

- **Domestic Law:** The Law of the Republic of Armenia "On Protection of Personal Data" (HO-119-N) constitutes the primary domestic legal basis, regulating all data operations executed by the Company as an Armenian legal entity.
- **European Union Law:** As a Service available globally, Nakmo Cloud offers its storage infrastructure to Data Subjects located within the European Union (EU) and the European Economic Area (EEA). Therefore, the Company strictly adheres to the **General Data Protection Regulation (Regulation (EU) 2016/679 - "GDPR")** pursuant to its Article 3(2) (extraterritorial applicability).

4.2 Additional Jurisdictions and US State Privacy Laws

Nakmo Cloud acknowledges the specific privacy rights of users residing in other global economic zones. Where mandatory and applicable under local legislation, the Company operates in compliance with United States privacy frameworks, including the **California Consumer Privacy Act (CCPA)** as amended by the **California Privacy Rights Act (CPRA)**, and equivalent US state-level privacy statutes.

4.3 Conflict of Laws and Higher Standard Principle

In the event of an operational or linguistic conflict between the provisions of the Armenian Law HO-119-N, the GDPR, or applicable US state privacy laws, Nakmo Cloud enforces a strict **"Higher Level of Protection" principle**.

This means the Company will automatically apply the legal provision, standard, or technical protocol that affords the maximum security, transparency, and structural protection to the Data Subject, unless the application of such a provision directly violates mandatory public policy or criminal statutes of the Republic of Armenia.

---

5. Categories of Personal Data and Content Collected

5.1 User Content and Special Categories of Data Disclaimer

The primary purpose of the Service is the private storage of User Content (high-resolution photographs, videos, and audio files).

- **No Active Collection of Sensitive Data:** Nakmo Cloud does not actively solicit, request, or intentionally process "Special Categories of Personal Data" under Article 9 of the GDPR (such as biometric data for unique identification, data concerning health, sexual orientation, political opinions, or religious beliefs).

- **Incidental Storage:** However, the Company acknowledges that private User Content uploaded voluntarily by the User may incidentally contain or visually reveal such sensitive details.
- **Operational Role:** Nakmo Cloud processes this content strictly as a passive, automated technical host. We do not scan, extract, catalog, or analyze your media files to isolate or utilize special categories of data for any secondary purposes.

5.2 Metadata, EXIF, and Geolocation Processing

The Service automatically extracts and processes technical Metadata embedded within your User Content (such as EXIF or IPTC tags) to provide core application functionality:

- **Geolocation Data:** GPS/location coordinates captured by your camera;
- **Chronological Data:** Exact timestamps of file creation, capture, and modification;
- **Technical Specifications:** Camera hardware models, lens types, and exposure settings (ISO, aperture, shutter speed).

Purpose of Processing: This processing is strictly limited to enabling automated sorting, search features, and chronological/geographical album mapping *solely within your private account interface*. Nakmo Cloud never extracts this metadata to track your live physical movement or build behavioral profiles. Users may strip metadata from their files prior to uploading or manage metadata preferences where supported in the Service settings.

5.3 Technical, Device, and Advertising Identifiers

When you interact with the Service via mobile applications or web interfaces, Nakmo Cloud automatically collects technical logs required for stability, optimization, and reward enforcement:

- **Network and Telemetry Data:** IP addresses, internet service provider logs, browser types, operating system versions, app performance metrics, and automated crash logs.
- **Hardware Identifiers:** Unique device tokens (such as UUID, Android ID, or secure installation tokens).
- **Advertising Identifiers:** Unique, user-resettable identifiers provided by your mobile operating system — specifically **Apple's Identifier for Advertisers (IDFA)** and **Google Advertising ID (GAID)**. These are collected strictly to validate and enforce the reward mechanics (e.g., tracking completed video views) within the Cloud Karma System via integrated secure advertising SDKs.

5.4 Account Identity Data

To establish, secure, and maintain your personal cloud storage allocation, the Company collects:

- Your email address and full name (or chosen username);

- Account security credentials (passwords, which are stored exclusively in an irreversible, encrypted, and cryptographically hashed form);
- Structural account metrics, including your subscription tier status, current storage utilization levels, and data traffic volume.

5.5 Subscription, Billing, and Anonymized Platform Tokens

All paid transactions are processed exclusively through the official billing layers of Apple Inc. or Google LLC. **Nakmo Cloud never collects, stores, or processes your credit card numbers, CVV codes, bank account details, or financial billing credentials.**

To manage your premium access status, the Platform Stores provide Nakmo Cloud with limited, strictly non-financial transactional telemetry:

- Subscription status (e.g., active, expired, trialing, cancelled);
- Selected subscription tier and billing frequency (monthly or annual);
- Transaction timestamps and upcoming renewal/expiration dates;
- An anonymized, unique platform token (used to link the purchase within the App Store or Google Play to your Nakmo Cloud account without revealing your external platform credentials).

This telemetry is used solely to audit account permissions, unlock expanded cloud storage tiers, and apply the corresponding Karma System exemptions.

5.6 Cloud Karma Operational Data

To ensure the integrity, security, and automated logic of the Cloud Karma system, Nakmo Cloud logs and processes the following activity metrics:

- Your current Karma Points balance and chronological ledger history (accruals, daily deductions, and activities completed);
- Timestamps of your first daily login (to trigger daily reward tokens);
- Cooldown tracking data for completed sponsored video views (to prevent system abuse and double-claiming);
- Promotional codes or referral tokens redeemed;
- The precise "Zero Karma Date" (the date your balance hit 0.0), used to dynamically calculate the accelerated or standard data retention windows prior to automated deletion.

---

6. Sources of Personal Data and Device Permissions

6.1 Direct Collection from the User

The primary source of information processed by the Service is you, the User. We collect data directly when you:

- Fill out the registration form to create an account;
- Manually select, upload, and backup your User Content (media files) to our cloud infrastructure;
- Adjust your account profile settings, preferences, or interact with the interface;
- Communicate directly with our customer support, technical engineering, or DPO channels.

6.2 Automated Telemetry and Third-Party Advertising Infrastructure

When you launch and interact with Nakmo Cloud, technical performance data and system metrics are automatically generated and logged by your device. Additionally, when you engage with the reward mechanics of the Cloud Karma System, validated event confirmations regarding completed video views are securely transmitted to us by our integrated third-party advertising SDK partners.

6.3 Third-Party Single Sign-On (SSO) Integrations

If you choose to register or log into the Service using integrated third-party identity providers (such as **Apple Sign-In** or **Google Sign-In**), Nakmo Cloud receives limited, structured profile data permitted by those platforms' secure OAuth API protocols. This is usually restricted to:

- A unique, obfuscated user identifier token;
- The verified email address associated with that third-party account;
- The name or username specified in that platform's profile.

6.4 Mobile Operating System Permissions

To provide core functionality, Nakmo Cloud requires access to specific native hardware and software features of your mobile device. These features are accessed **ONLY** after you grant explicit, affirmative consent through your operating system's standard permission prompts:

- **Photo Library / Storage Permission:** Required strictly to allow you to browse, select, and upload photographs and videos to Nakmo Cloud, or to download stored files back to your local device. The app never scans or indexes your local library in the background without your active interaction.
- **Location Services Permission (Optional):** Where supported or requested for advanced sorting, this permission allows the application to read location data during active uploads to enable geographical album mapping. You can disable this native permission at any time through your device settings without losing access to basic cloud storage.
- **Push Notifications Permission:** Used strictly to transmit automated alerts regarding your account status, system updates, and critical Cloud Karma warnings (such as notifications that your Karma balance is approaching zero or that your account has entered an Over-Limit State).

---

7. Purposes and Legal Bases for Processing Personal Data

Nakmo Cloud processes your Personal Data strictly under valid, lawful legal bases established by Article 6 of the GDPR and the Republic of Armenia Law HO-119-N. We never process data for unspecified or incompatible secondary purposes.

The matrix below defines exactly why and on what legal grounds your data is handled:

Category of Processing Activity / Purpose	Specific Data Involved	Legal Basis under GDPR & Domestic Law
Provision of Storage Services Hosting, backup, and cross-device synchronization of your uploaded media files.	User Content, Account Identity Data, Storage utilization metrics.	**Performance of a Contract** (Art. 6(1)(b) GDPR). Necessary to fulfill our obligations under the Terms of Service.
Media Organization & Management Enabling custom albums, automated folder categorization, and timeline views.	User Content, Metadata (EXIF/GPS tags, capture timestamps).	**Performance of a Contract** (Art. 6(1)(b) GDPR). Core technical features of the cloud storage product requested by you.
Cloud Karma System Operation Tracking app engagement, ledger bookkeeping of Karma balances, managing daily login claims.	Cloud Karma Activity Data, Hardware/Device Identifiers.	**Performance of a Contract** (Art. 6(1)(b) GDPR). Required to calculate storage retention eligibility and run the platform's freemium mechanics.
Subscription Verification Validating payment confirmations and unlocking expanded storage limits for premium tiers.	Subscription and Billing Data, Anonymized Platform Tokens.	**Performance of a Contract** (Art. 6(1)(b) GDPR). Essential to deliver paid services and manage Karma exemptions.
Service Optimization & Bug Fixing Monitoring crash logs, API response times, server loads, and app stability.	Technical and Device Data, Telemetry logs, IP addresses.	**Legitimate Interest** (Art. 6(1)(f) GDPR). Our legitimate commercial interest in maintaining a stable, fast, and secure application interface.
Security & Fraud Prevention Detecting cyberattacks, account takeovers, multi-account abuse, and verifying infrastructure integrity.	Technical and Device Data, IP logs, Account metadata.	**Legitimate Interest** (Art. 6(1)(f) GDPR). Crucial for protecting our cloud architecture, our users' private data, and mitigating corporate liability.

Category of Processing Activity / Purpose	Specific Data Involved	Legal Basis under GDPR & Domestic Law
Monetization and Reward Video Tracking Validating completed sponsored video views to credit reward Karma Points.	Advertising Identifiers (IDFA, GAID).	**Consent** (Art. 6(1)(a) GDPR). Based on your explicit authorization granted via your device's native privacy prompts (e.g., Apple ATT).
Legal Compliance Responding to verified court orders, responding to valid government requests, and maintaining tax logs.	Account Data, Transactional telemetry, IP records.	**Legal Obligation** (Art. 6(1)(c) GDPR). Processing is mandatory to comply with statutory laws of the Republic of Armenia and applicable international regulations.

---

8. Data Retention Periods and Erasure Protocols

8.1 Retention Philosophy

Nakmo Cloud strictly applies the principle of storage limitation. We store your Personal Data and User Content only for the duration necessary to fulfill the operational purposes detailed in Section 7, or to comply with mandatory statutory laws.

8.2 Structured Retention Matrix

Different categories of information are subject to distinct retention lifecycles:

- **Active Account Data:** Your email, username, and account credentials are formats kept for the entire lifecycle of your active account.
- **Technical Logs and Telemetry:** IP address records, crash reports, and system telemetry logs are automatically rotated, anonymized, or deleted within **ninety (90) days** from collection.
- **Subscription and In-App Purchase Records:** Transaction histories received from Platform Stores are archived for **five (5) years** to satisfy corporate tax, accounting, and anti-fraud auditing laws of the Republic of Armenia.

8.3 Automated Deletion Triggered by Cloud Karma Depletion

Pursuant to Section 6 of our Terms of Service, the maintenance of your private cloud storage allocation depends directly on your active Cloud Karma balance:

- **The 0.0 Karma Threshold:** The exact calendar date your Karma balance hits zero is logged as the "Zero Karma Date".

- **The Grace Period and Permanent Deletion:** Nakmo Cloud provides a standard grace window following this date. Once this window expires without account reactivation or Karma accumulation, **all stored User Content (photos, videos, and associated metadata) will be permanently, automatically, and irreversibly deleted** from our live servers and edge networks (including Cloudflare R2 or equivalent cache stores).
- **Retention Post-Deletion:** We retain nothing but basic, non-identifying account metadata to prevent system exploitation.

8.4 Automated Deletion Triggered by Storage Over-Limit State

As established in Section 7.8 of the Terms of Service, accounts that enter an Over-Limit State due to a downgraded or expired subscription are subject to accelerated infrastructure clean-up:

- **The 7-to-30-Day Elimination Window:** If you do not clear your excess data or renew your premium tier within the specified **7-to-30-day notice period**, the automated system executes an irreversible erasure of the excess User Content.
- **Legal Rationale:** Nakmo Cloud cannot subsidize or permanently host unpaid over-limit infrastructure data.

8.5 Retention Upon Voluntary Account Deletion

If you choose to permanently close your account via the in-app "Delete Account" function, the deletion workflow triggers immediately. All your User Content, Account Identity Data, and active Karma logs are stripped from our primary application databases within **forty-eight (48) hours**.

> **Important Note on Backups:** Residual fragments of your data may remain securely stored inside encrypted, isolated system backup loops for up to **thirty (30) additional days** before being completely overwritten. These backups are entirely inaccessible for standard operational use.

---

9. Automated Processing and Automated Media Indexing (AI)

9.1 Two-Tiered Technical Isolation Architecture

To provide advanced searchability, chronological sorting, and structural categorization without compromising your fundamental right to privacy, Nakmo Cloud utilizes machine learning algorithms and computer vision models. To ensure maximum data safety, our technical architecture strictly isolates processing into two execution layers:

- **Local On-Device Processing (Strict Biometric Isolation):** Any features involving facial detection, facial clustering, recognition of specific individuals, or the analysis of sensitive biometric visual parameters are executed **strictly, exclusively, and locally on your physical device** (using native hardware neural engines). This visual identity data never leaves your local device, is never transmitted to our cloud infrastructure, and remains completely invisible and inaccessible to Nakmo Cloud, its engineers, or third-party vendors.
- **Cloud-Based Indexing (Object and Scene Classification):** When media files are transmitted to our secure cloud infrastructure, automated algorithms process the content **solely to detect general inanimate objects, visual patterns, textures, or scene environments** (e.g., classifying a file under "Beach," "Mountain," or "Document"). This is done at the exact moment of upload to generate private search indexes for your account.

9.2 Strict Prohibition on Machine Learning Model Training

Nakmo Cloud provides an absolute, legally binding guarantee that **we never use your personal media files (photographs, videos), associated metadata, or locally generated facial tokens to train, calibrate, evaluate, or optimize our own or any third-party machine learning models, computer vision systems, or generative neural networks.** Your private content is never shared with, sold to, or utilized by external AI vendors or data brokers for training or profiling purposes.

9.3 Scope of Automation and Article 22 GDPR Compliance

The Automated Media Indexing described in this Section is performed on a purely technical, programmatic basis to deliver product features. Nakmo Cloud explicitly certifies that these algorithms are **never** used to engage in automated decision-making or behavioral profiling that produces legal effects, significantly affects your user standing, or alters your contractual rights under Article 22 of the GDPR.

9.4 Data Isolation and Contractual Necessity

The descriptive tags and index maps generated by our cloud infrastructure are treated with the exact same level of strict confidentiality as your original User Content. They are cryptographically linked to your specific account, remain completely isolated from other users, and are never shared with external parties.

Technical Inseparability Notice: Because automated scene and object indexing is a fundamental, structurally inseparable component of Nakmo Cloud's core database architecture (required to display, organize, and retrieve your files within a cloud environment), **it cannot be disabled individually while the account remains active.**

This processing is legally justified under Article 6(1)(b) of the GDPR as necessary for the performance of our contract with you. If you do not wish your files to undergo this basic automated cloud indexing, your

sole remedy is to refrain from uploading media or to permanently delete your account via the Service settings, which will trigger the immediate erasure of all your indexed metadata within forty-eight (48) hours.

---

10. Data Storage, Cloud Infrastructure, and International Data Transfers

10.1 Infrastructure and Storage Partners

To ensure multi-regional availability, low latency, and enterprise-grade infrastructure resilience, Nakmo Cloud utilizes the storage and hosting services of premier third-party cloud infrastructure networks.

Our core infrastructure operates across environments provided by **Cloudflare (including Cloudflare R2 object storage), Amazon Web Services (AWS), Google Cloud Platform (GCP), and Hetzner Online GmbH**. These partners act strictly as **Data Processors** executing storage commands under our direct oversight. They are legally and contractually prohibited from accessing, using, or disclosing your data for any independent marketing, telemetry, or analytical training operations.

10.2 Global Data Localization and Server Regions

While Nakmo Cloud is legally incorporated in the Republic of Armenia, our server nodes, Content Delivery Networks (CDNs), and primary cloud storage buckets are strategically distributed across multi-regional availability zones.

Your Personal Data and User Content may be hosted and processed on physical systems located within the **European Union (EU), the United Kingdom (UK), and the United States (US)**. We ensure that our physical servers are localized exclusively within jurisdictions that maintain robust, stable data protection infrastructures and are fully compliant with applicable international compliance regimes.

10.3 Legal Mechanisms for International Transfers (GDPR Compliance)

For users residing within the EU/EEA, transferring data to infrastructure located outside the European Economic Area (such as servers based in Armenia or the United States) requires strict adherence to Chapter V of the GDPR. Nakmo Cloud enforces the following legal compliance layers:

- **Standard Contractual Clauses (SCCs):** Where data is routed to or stored in jurisdictions without a formal EU adequacy decision (including the US and Armenia), Nakmo Cloud ensures that its agreements with data centers incorporate the latest **Standard Contractual Clauses** approved by the European Commission, guaranteeing an equivalent level of individual data protection.

- **Armenian Framework:** Pursuant to Article 26 of the Republic of Armenia Law HO-119-N, international data transfers executed under this Policy are protected by established corporate data security agreements.

10.4 Infrastructure Security and Cryptographic Safeguards

We choose storage partners that hold leading global security verifications, including **ISO/IEC 27001, SOC 2 Type II, and PCI-DSS compliance**.

Furthermore, to mitigate intercept and breach risks, Nakmo Cloud applies robust cryptographic measures across the entire data stream:

- **Data in Transit:** All files and account metadata transmitted between your device and our cloud infrastructure are protected using secure, industry-standard **Transport Layer Security (TLS/HTTPS)** encryption protocols.
- **Data at Rest:** Once stored within our cloud allocation (e.g., inside Cloudflare R2 or AWS blocks), User Content is isolated and guarded via advanced logical firewalls and encrypted using commercial-grade **Advanced Encryption Standard (AES-256)** encryption algorithms.

---

11. Third-Party Data Disclosure and Integrated Third-Party Services (SDKs)

11.1 Strict Non-Commercialization Policy

Nakmo Cloud enforces a strict policy regarding the commercialization of user data. **We do not sell, rent, lease, trade, or distribute your Personal Data, Metadata, or private User Content to data brokers, advertising agencies, or any external third parties for marketing or independent financial gain.**

11.2 Authorized Third-Party Service Providers (Sub-Processors)

To deliver core application features, process reward events, and maintain service stability, Nakmo Cloud embeds limited third-party Software Development Kits (SDKs) and developer tools. Data is shared only with vetted providers who act as our sub-processors and are contractually bound to implement strict technical and organizational security measures:

- **Infrastructure & Content Delivery: Cloudflare, Inc.** (USA/EU) — used to run our edge networks, cache optimization, and securely route and host encrypted data blocks via Cloudflare R2 object storage.
- **Infrastructure & Database Hosting: Hetzner Online GmbH** (Germany), **Amazon Web Services, Inc.** (USA/EU), and **Google LLC** (USA/EU) — utilized for backend application operations, encrypted

database management, and server compute allocation.

- **Application Performance & Analytics: Google Firebase / Crashlytics** (USA) — integrated into our mobile apps strictly to log operational bugs, monitor real-time server response errors, and analyze application stability. This data is entirely aggregated and anonymized.
- **Monetization & Cloud Karma Video Networks:** Authorized programmatic mobile ad networks (such as **Google AdMob**, **Unity Ads**, or equivalent certified networks) — integrated exclusively to serve sponsored reward video streams within the Cloud Karma System. These networks receive only resettable Advertising Identifiers (IDFA/GAID) and limited technical device telemetry to prevent fraudulent ad interactions and manage capping cooldowns.

11.3 Law Enforcement and Compulsory Disclosures

Nakmo Cloud may disclose basic operational Personal Data or infrastructure transaction logs to external public authorities, law enforcement agencies, or courts if and when such disclosure becomes mandatory to:

- Comply with a legally binding subpoena, warrant, or court order issued by a competent judicial authority of the Republic of Armenia;
- Detect, prevent, or address active infrastructure cyberattacks, financial fraud, or severe systemic application security threats;
- Enforce our Terms of Service or defend the legal rights and corporate safety of Nakmo Cloud, its employees, and its infrastructure assets.

> **Critical Caveat on User Content:** Pursuant to Section 5 of our Terms of Service, Nakmo Cloud will never voluntarily grant law enforcement agencies backdoor access to your private photographs or videos unless presented with a verified, non-appealable judicial warrant issued under the criminal procedure laws of the Republic of Armenia, or in compliance with mandatory global urgent emergency protocols regarding child exploitation materials (CSAM).

---

12. Master Data Retention Schedule and Automated Erasure Metrics

12.1 Core Retention Philosophy

In strict alignment with the data minimization and storage limitation principles of the GDPR (Article 5(1)(e)) and Armenian Law HO-119-N, Nakmo Cloud establishes deterministic lifecycles for all handled data. No information is stored indefinitely without a valid operational or legal justification.

12.2 The Cloud Karma Retention Protocol (Free-Tier Infrastructure)

For Users utilizing the Service under the Free-Tier framework, data persistence is tied directly to the automated Cloud Karma System:

- **Immediate Edge Purge:** The exact calendar day your Karma Point balance drops to 0.0 is logged as the "Zero Karma Date". Upon this event, all cached preview files and temporary media representations are immediately and completely purged from our global edge servers and Content Delivery Networks (including Cloudflare R2 caches).
- **The 150-Day Preservation Window:** Your original, full-resolution User Content (photos, videos) remains securely archived in our cold-storage layer for exactly **one hundred and fifty (150) calendar days** from the Zero Karma Date.
- **Permanent Automated Erasure:** If you do not accumulate Karma Points or reactivate your account within this 150-day window, the system executes an **irreversible, permanent technical deletion** of all original files and associated cloud metadata.

12.3 System Alerts and Lifecycle Warnings

To prevent accidental data loss, the Company operates an automated warning infrastructure that transmits critical push notifications and email alerts:

- **First System Warning:** Triggered automatically when your account reaches a threshold of **14.0 Karma Points** (approximately seven (7) calendar days prior to projected depletion based on standard system burn rates).
- **Suspension Notice:** Triggered instantly on the Zero Karma Date, notifying you that the account has officially entered the 150-day deletion countdown.

12.4 Paid Premium Subscribers Exemption

Users maintaining an active, verified paid Subscription are completely exempt from the activity-based Cloud Karma depletion and retention metrics. Your Personal Data and User Content will be safely preserved for the entire uninterrupted duration of your premium billing lifecycle.

12.5 Financial Compliance and Administrative Logs

Pursuant to statutory tax, corporate reporting, and anti-money laundering laws of the Republic of Armenia, the non-payment transactional telemetry and anonymized Platform Store tokens received from Apple Inc. or Google LLC (as described in Section 5.5) are securely archived for **five (5) years** following the formal closure or deletion of your Nakmo Cloud account.

12.6 Voluntary Account Deletion and Backup Lifecycle

When you execute the "Delete Account" function within the Service interface, the application triggers an immediate data teardown:

- **Live Database Eviction:** All live account profiles, validation logs, and original User Content are wiped from our active operational databases within **forty-eight (48) hours**.
- **Disaster Recovery Backups:** For business continuity and disaster recovery purposes, isolated, cryptographically encrypted snapshots of our infrastructure may persist in offline, non-operational backup loops for a maximum of **ninety (90) additional days**. Once this cycle rotates, all fragments are permanently overwritten and completely unrecoverable.

---

13. Technical Data Deletion and Absolute Irreversibility

13.1 Immediate Operational Cessation

When a deletion workflow is triggered — whether via your voluntary execution of the "Delete Account" function, the expiration of the 150-day Cloud Karma grace period, or the enforcement of the Storage Over-Limit State clean-up — Nakmo Cloud immediately disconnects that data from the active application layer.

Within **forty-eight (48) hours**, your user profile is deactivated, and your stored User Content (original photos, videos, and associated metadata) is systematically unlinked from our live database indexes and purged from all active Content Delivery Network (CDN) edge caches.

13.2 Technical Isolation of Backup Snapshots

As detailed in Section 12.6, encrypted, compressed multi-tenant snapshots of our entire cloud infrastructure are generated automatically for emergency disaster recovery and business continuity.

- **No Individual Extraction:** Because these archival snapshots copy the entire system state as a single, indivisible, and cryptographically encrypted block, it is technically impossible to isolate, extract, or restore the files of one specific individual user from them.
- **Passive Preservation:** Any data remaining inside these backup loops is completely passive, entirely inaccessible to regular system operations, and is never used for any analytical or operational purposes.

13.3 Absolute Irreversibility and Disclaimer of Liability

Nakmo Cloud strictly operates a zero-recovery architecture post-deletion. Once the 48-hour live database eviction window closes:

- **Permanent Loss:** Your User Content, account history, accumulated Cloud Karma balances, and metadata are considered permanently destroyed and mathematically unrecoverable.
- **Support Limitations:** Nakmo Cloud's customer support and engineering teams **do not possess the technical means, tools, or backdoors to restore** your media files under any circumstances.

- **Limitation of Liability:** By utilizing the Service or executing an account deletion request, the User acknowledges and agrees that Nakmo Cloud shall bear zero corporate, financial, or legal liability for any permanent loss of data resulting from automated lifecycle enforcement or user-initiated deletion.

13.4 Legal Retention Exception

Pursuant to Article 17(3) of the GDPR and applicable laws of the Republic of Armenia, the only information that survives an account deletion workflow is limited, non-identifying accounting logs, tax transaction telemetry from the Platform Stores (as described in Section 5.5), and legal consent records. These are kept strictly in an isolated archive to fulfill mandatory statutory reporting obligations.

---

14. Data Subject Rights and Exercise Mechanisms

Pursuant to Chapter III of the GDPR and the Law of the Republic of Armenia "On Protection of Personal Data" (HO-119-N), Users possess comprehensive legal rights regarding their Personal Data. Nakmo Cloud ensures that these rights can be exercised efficiently and transparently.

14.1 Core Statutory Rights

- **Right of Access (Art. 15 GDPR):** You have the right to obtain formal confirmation from us as to whether your Personal Data is being processed, and, where applicable, receive a structured overview and a digital copy of the specific data points we hold.
- **Right to Rectification (Art. 16 GDPR):** You have the right to demand the immediate correction of inaccurate Personal Data or the completion of incomplete profile records associated with your account.
- **Right to Erasure / "Right to be Forgotten" (Art. 17 GDPR):** You may request the permanent elimination of your Personal Data and User Content, subject to the irreversible technical protocols and legal exceptions defined in Section 13 of this Policy.
- **Right to Restriction of Processing (Art. 18 GDPR):** You have the right to restrict or "freeze" the processing of your data under specific statutory conditions (e.g., if you contest the accuracy of the data, while we verify it).
- **Right to Data Portability (Art. 20 GDPR):** You have the right to export your account profile and uploaded User Content in a structured, commonly used, and machine-readable format.
- **Right to Object (Art. 21 GDPR):** You possess an absolute right to object at any time to the processing of your data based on our "Legitimate Interests" framework or where data is utilized for direct operational telemetry.
- **Right to Withdraw Consent:** Where data processing is technically grounded on your explicit consent (such as mobile Advertising Identifiers for the Cloud Karma System), you may withdraw

your consent at any time via your device settings. Withdrawal does not affect the lawfulness of any processing executed prior to such action.

14.2 Engineering and Execution Protocols for Data Portability

Due to the significant technical infrastructure loads and massive file sizes associated with high-resolution photographic and video archives:

- **Processing Window:** The generation and compilation of a full data portability archive may take up to **seventy-two (72) hours** from the date of a verified request.
- **Delivery Method:** Once compiled, the user will receive a secure, cryptographically signed, and time-limited download URL (delivered via Cloudflare R2 or equivalent secure infrastructure). For security purposes, this download link will automatically expire and become invalid after **seven (7) calendar days**.

14.3 Mandatory User Verification and Anti-Fraud Security

To prevent social engineering, identity theft, and unauthorized data leaks, Nakmo Cloud enforces a strict identity validation protocol:

- **Source of Request:** All requests to exercise privacy rights must be submitted directly from the **verified email address** explicitly linked to the active Nakmo Cloud account.
- **Identity Audits:** Nakmo Cloud reserves the right to demand additional non-intrusive identity verification parameters (such as device installation tokens or subscription purchase receipt numbers from the Platform Store) to verify ownership. Anonymous, unverified, or third-party proxy requests will be rejected immediately to protect user privacy.

14.4 Response Timelines and Communication Channel

To exercise any of your legal privacy rights, please submit a structured request to our Data Protection Officer at:

- **Email:** legal@nakmo.net

Pursuant to international compliance standards, Nakmo Cloud will provide a substantive response and execute the validated request within **thirty (30) calendar days** of receipt. This period may be extended by an additional sixty (60) days for exceptionally complex multi-terabyte data extraction workflows, in which case the user will be notified within the initial 30-day window.

14.5 Right to Lodge a Complaint with Regulatory Authorities

If you believe that Nakmo Cloud has infringed upon your privacy rights or failed to process your data in compliance with applicable law, you have the right to lodge a formal complaint with a competent supervisory authority:

- **In the Republic of Armenia:** The Personal Data Protection Agency of the Ministry of Justice of the Republic of Armenia.
- **In the European Union:** Any national Data Protection Authority (DPA) within the EU Member State of your habitual residence, place of work, or place of the alleged infringement (pursuant to Article 77 GDPR).

—

15. Technical, Organizational, and Infrastructure Data Security

15.1 Corporate Commitment to Security

Nakmo Cloud places the highest operational priority on the security, integrity, and confidentiality of your Personal Data and User Content. We implement and continuously update advanced technical and organizational security measures designed to protect our cloud ecosystem against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or malicious access.

15.2 Cryptographic Safeguards and Access Controls

To guarantee that your private photographs, videos, and account credentials remain completely isolated, Nakmo Cloud enforces strict cryptographic and access limitations across its architecture:

- **Transport Encryption (TLS):** All data moving between your mobile application or web interface and our servers is encrypted in transit using industry-standard Transport Layer Security (TLS 1.2 or TLS 1.3) protocols, protecting your files from interception on public Wi-Fi networks.
- **Storage Encryption (AES-256):** Once static user media blocks are committed to our object storage infrastructure (such as Cloudflare R2 or AWS S3), they are encrypted at rest using commercial-grade Advanced Encryption Standard (AES-256) algorithms.
- **Irreversible Hashing:** User passwords are encrypted on the client side and stored in our databases exclusively using advanced, non-reversible cryptographic hashing algorithms. Nakmo Cloud employees cannot read or reconstruct your actual password text.
- **Strict Internal Access Controls (Least Privilege Principle):** We enforce a rigid internal permission hierarchy. No employee or engineer at Nakmo Cloud has general or unmonitored access to view your private photos or videos. Access to database management layers is restricted to specific core infrastructure engineers solely for emergency system maintenance, and every access event is permanently logged in an unalterable security audit trail.

15.3 Network Security and Perimeter Defense

Our server networks, API gateways, and cloud compute nodes are deployed behind enterprise-grade infrastructure firewalls and managed security layers (including **Cloudflare's Advanced DDoS Protection and Web Application Firewall (WAF)**). These systems continuously monitor, flag, and mitigate automated brute-force attacks, SQL injections, server-side exploits, and structural network anomalies.

15.4 Security Disclaimer and User Responsibility

While Nakmo Cloud deploys cutting-edge infrastructure defenses, no cloud storage system, database cluster, or internet data transmission can be guaranteed to be 100% secure against highly sophisticated state-sponsored cyber threats or advanced social engineering.

Your Role in Security: The ultimate security of your data also depends on your personal security hygiene. You are strictly responsible for maintaining the absolute confidentiality of your Nakmo Cloud account credentials and choosing a strong, unique password. If you suspect that your login credentials or linked email address have been compromised, you must update your security settings immediately and contact our team.

---

16. Policy Amendments, Children's Privacy, and Contact Information

16.1 Automated Version Control and Policy Updates

Nakmo Cloud reserves the right to amend, update, or modify this Privacy Policy at any time to reflect structural changes in our cloud infrastructure, adjustments to the Cloud Karma System metrics, or evolving international legal compliance standards.

- **Notice of Changes:** When material changes are executed, we will update the "Effective Date" at the top of this document and transmit a prominent notification via the Nakmo Cloud mobile application interface or to your verified email address.
- **Acceptance:** Continued interaction with the Service following the publication of an updated version constitutes your explicit, binding acknowledgment of the revised data practices. If you do not agree with the updated terms, your sole and exclusive remedy is to discontinue use and execute an account deletion request.

16.2 Strict Protection of Children's Privacy (COPPA & GDPR Compliance)

Nakmo Cloud delivers a private cloud storage utility intended exclusively for a general adult audience and users who have reached the legal age of digital consent.

- **Age Restriction:** We do not knowingly solicit, request, or collect personal information from children under the age of **thirteen (13)** in the United States (under the Children's Online Privacy Protection Act - COPPA) or under the age of **sixteen (16)** in the European Union (pursuant to Article 8 GDPR).
- **Remediation:** If we discover that a minor below these statutory thresholds has bypassed registration controls and established a Nakmo Cloud account without verifiable parental consent, our infrastructure systems will immediately freeze the account and permanently erase all associated files and telemetry logs within forty-eight (48) hours. If you suspect a minor has created an account, please contact us at **legal@nakmo.net**.

16.3 Regulatory Contacts and Data Protection Officer (DPO)

For any questions regarding this Privacy Policy, your statutory user rights under Armenian law HO-119-N, or to report a suspected security vulnerability, please contact our dedicated Data Protection and Legal Compliance department:

- **Company Name:** Nakmo Cloud LLC
- **Legal Address:** Republic of Armenia, Yerevan
- **Data Protection Officer Email:** legal@nakmo.net
- **General Technical Support:** support@nakmo.net

Our legal team will audit, verify, and substantively respond to all formal inquiries within thirty (30) calendar days from receipt.

---

17. Personal Data Breach Management and Notification Procedures

17.1 Incident Response and Containment

Nakmo Cloud operates an automated intrusion detection infrastructure and a strict incident response protocol. In the unfortunate event of a systemic security anomaly, unauthorized infrastructure access, or a verified personal data breach, our engineering and security teams will immediately initiate emergency containment protocols to isolate the affected database clusters, revoke compromised access tokens, and close identified vulnerabilities.

17.2 Mandatory Notification to Supervisory Authorities

Pursuant to Article 33 of the GDPR and applicable provisions of the Republic of Armenia Law HO-119-N, if a data breach occurs that is likely to result in a risk to the fundamental rights and freedoms of natural persons:

- **The 72-Hour Window:** Nakmo Cloud will formally document the incident and lodge an official notification with the competent regulatory authorities — specifically the **Personal Data Protection Agency of the Ministry of Justice of the Republic of Armenia** and, where applicable, leading European Data Protection Authorities (DPAs) — within **seventy-two (72) hours** of becoming aware of the breach.

17.3 Direct Notification to Affected Users

Where a personal data breach is assessed to present a high risk to your personal security, data integrity, or privacy, Nakmo Cloud will notify all affected Users directly and without undue delay via their verified, registered email addresses.

17.4 Content of the Security Notification

To ensure you can take immediate protective action, our direct security notification will be written in clear, plain language and will explicitly provide:

- The name and direct contact details of our Data Protection Officer or legal compliance team;
- A transparent description of the nature of the security incident, including the approximate categories and volume of Personal Data records involved;
- The projected or likely consequences of the data breach;
- A comprehensive overview of the technical remediation measures already executed or planned by Nakmo Cloud to mitigate the event;
- Specific, actionable recommendations and security hygiene instructions for the User (such as triggering an immediate password reset or verifying the security settings of your linked external identity providers).

---

18. Age Restrictions and Protection of Minors (Children's Privacy)

18.1 General Prohibition and Thresholds

Nakmo Cloud operates a strict adult-oriented cloud infrastructure environment. The Service is not engineered, intended, or marketed for children. In absolute alignment with Article 8 of the GDPR, the

Children's Online Privacy Protection Act (COPPA), and the Republic of Armenia Law HO-119-N, we enforce the following strict age thresholds:

- **EEA and Armenian Residents:** Access is strictly prohibited to individuals under **sixteen (16) years of age**.
- **US and Global Residents:** Access is strictly prohibited to individuals under **thirteen (13) years of age**.

18.2 Absolute Disclaimer of Verification Capability and User Liability

Nakmo Cloud processes age parameters purely based on the self-declared input provided by the individual during the signup process.

- **No Technical Mandate:** The User acknowledges and agrees that Nakmo Cloud **does not possess the technical capability, infrastructure hooks, or legal authority to verify the absolute authenticity** of the age specified during registration (such as cross-referencing national ID databases).
- **Sole User Responsibility:** The legal, financial, and moral responsibility for providing fraudulent or falsified age telemetry lies **solely and exclusively with the individual User** (and, where applicable, their parents or legal guardians). Nakmo Cloud explicitly disclaims all corporate liability for unauthorized registrations executed via deceptive age inputs.

18.3 Immediate Remediation and Purge Protocol

If Nakmo Cloud's legal compliance team or data monitoring algorithms discover, or are notified by verified third parties, that an active cloud account belongs to a minor below the permissible age limits specified in Section 18.1:

- **Immediate Freeze:** The account will be immediately locked and disconnected from the network to prevent further data processing.
- **Permanent Erasure:** Within **forty-eight (48) hours**, Nakmo Cloud will execute a complete, irreversible, and permanent technical erasure of that account, its user profile, all accumulated Cloud Karma points, and all uploaded User Content (photos, videos, and associated metadata) across all operational live systems and disaster recovery backups, to the maximum extent technically feasible.

18.4 Parental Control and Reporting Escalation

Parents or legal guardians who maintain a reasonable suspicion or possess material proof that their child has bypassed our gateway controls and provided Personal Data or media files to the Service are strongly urged to contact us immediately.

Upon receipt of a verified parental report, we will prioritize and expedite the absolute deletion of the minor's infrastructure footprint.

- **Dedicated Reporting Channel: legal@nakmo.net** *(or support@nakmo.net)*

---

19. Advertising SDKs and Cloud Karma Program sandboxing

19.1 Programmatic Advertising Framework

To sustain, finance, and technically validate the freemium reward mechanics of our Free Tier — specifically the accumulation of Karma Points via the completion of sponsored programmatic video streams — Nakmo Cloud embeds limited, verified third-party advertising networks and Software Development Kits (SDKs) into the mobile application architecture.

19.2 Strict Data Isolation and Sandboxing Guarantee

Nakmo Cloud enforces an absolute, structurally hardcoded barrier between your private life and external ad platforms. **We explicitly guarantee that all integrated advertising trackers, programmatic networks, and monetization SDKs are strictly sandboxed, isolated, and computationally decoupled from your core account infrastructure.**

These external advertising systems do not possess, do not request, and are contractually, technically, and structurally incapable of obtaining access to:

- Your uploaded User Content (private photographs, videos, or documents);
- File names, custom folder organization, or user-defined tags;
- Embedded metadata layers (including EXIF parameters, GPS capture coordinates, or camera hardware profiles);
- Your private cloud database allocation indexes.

19.3 Scope of Limited Telemetry Collection

Data harvesting executed by these integrated monetization SDKs is strictly confined to industry-standard mobile identifiers and localized technical metrics required solely to credit your Karma balance and maintain ecosystem stability. Collected data points include:

- **Resettable Hardware Identifiers:** Apple's Identifier for Advertisers (IDFA) or Google's Advertising ID (GAID / AAID);
- **Device Telemetry:** Operating system version, device model, language settings, and IP address;

- **Interaction Telemetry:** Video playback events (start, 25%, 50%, 75%, and 100% completion states), click-through rates, and session timestamps.

19.4 Legal Basis, Ad Fraud Prevention, and User Control

The processing of technical advertising metrics is governed by a dual legal framework:

- **Ad Fraud Mitigation:** Tracking interaction telemetry is justified under our **Legitimate Interest** (Art. 6(1)(f) GDPR) to detect automated bot networks, prevent click-fraud exploitation, enforce cooldown capping rules, and protect Nakmo Cloud from financial liability.
- **Consent-Driven Tracking:** The activation and collection of your unique mobile advertising identifiers (IDFA/GAID) are strictly conditional upon your explicit authorization. Nakmo Cloud fully respects your device's native privacy controls (e.g., Apple's App Tracking Transparency framework).

> **User Control Notice:** If you opt out of tracking via your smartphone's global privacy settings, the integrated SDKs will automatically receive a string of non-identifying zeros. In this state, you can still view sponsored videos to earn Cloud Karma, but the advertisements served to you will be purely generic and contextual rather than personalized.

---

20. Authorized Third-Party Processors and Sub-Processors Register

20.1 Statutory Framework for Sub-Processing

To deliver a high-availability cloud environment, process microtransactions, and maintain application performance, Nakmo Cloud delegates specific technical operations to third-party sub-processors. Pursuant to Article 28 of the GDPR and the Republic of Armenia Law HO-119-N, all listed partners are legally bound by strict Data Processing Addendums (DPAs). They are contractually mandated to enforce security safeguards equivalent to those maintained by Nakmo Cloud and are strictly prohibited from utilizing your data for any independent or secondary commercial purposes.

20.2 Categorized Sub-Processor Registry

- **Cloud Infrastructure and Content Routing:**
  - **Cloudflare, Inc. (USA/EU):** Operates edge networks, DDoS protection, Web Application Firewalls (WAF), and manages encrypted data block delivery via Cloudflare R2 object storage.

    - **Amazon Web Services, Inc. (AWS) (USA/EU), Google Cloud Platform (GCP) (USA/EU), and Hetzner Online GmbH (Germany):** Provide core multi-regional cloud servers, encrypted database storage arrays, and backend computational power.
- **Transactional and Billing Infrastructure (Absolute Payment Isolation):**
    - **Apple Inc. (Apple App Store) & Google LLC (Google Play Store):** Handle all premium subscription billing, in-app purchases, and payment validation loops.
    - *Security Isolation Guarantee:* Nakmo Cloud operates a strict zero-access billing pipeline. We never receive, process, or store your full credit card numbers, bank details, or CVV codes. All financial transactions are managed independently by the Platform Stores under their respective autonomous privacy policies.
- **System Notifications and Lifecycle Emails:**
    - **SendGrid (Twilio, Inc.) / Mailchimp (Intuit, Inc.) (USA):** Utilized strictly to transmit critical transactional system emails, such as account verification codes, password reset links, and automated Cloud Karma depletion alerts (as detailed in Section 12.3).
- **Application Performance and Telemetry Analytics:**
    - **Google Firebase / Crashlytics (USA) & Mixpanel, Inc. (USA):** Embedded to monitor real-time mobile application crashes, server latency anomalies, and feature interaction metrics. All data routed to these systems is heavily aggregated and pseudonymized.
    - **Proprietary Analytics Infrastructure:** Nakmo Cloud's internal telemetry monitoring systems log strictly non-identifying operational behaviors (e.g., UI button clicks, storage capacity ratios). Our proprietary analytics tools are programmatically isolated and possess **zero technical visibility into the actual contents of your uploaded media files**.

20.3 Onward Transfer Responsibility

Nakmo Cloud monitors the compliance status of its sub-processors. In accordance with international data protection frameworks, Nakmo Cloud maintains ultimate accountability for ensuring that all integrated third-party sub-processors process individual Personal Data strictly within the boundaries of the specific authorizations set forth in this Privacy Policy.

---

21. Regulatory Oversight and Formal Complaint Mechanisms

21.1 Commitment to Mutual Resolution

Nakmo Cloud maintains a dedicated, internal data privacy compliance infrastructure. If you maintain any anxieties, disputes, or complaints regarding how your private photographs, metadata, or account telemetry are processed, we strongly encourage you to first contact our Data Protection department directly at **legal@nakmo.net**. We commit to auditing your concern, investigating potential

infrastructure anomalies, and working transparently to reach an amicable, non-judicial resolution within our standard 30-day processing window.

21.2 Right to Lodge Formal Complaints (Statutory Recourse)

Pursuant to Article 77 of the GDPR and applicable administrative provisions of the Republic of Armenia Law HO-119-N, you possess an absolute, non-restrictable legal right to bypass internal resolution paths and lodge a formal complaint directly with an official public supervisory authority if you believe that Nakmo Cloud's processing operations infringe upon applicable data protection laws.

21.3 Competent Supervisory Registries

- **Within the Jurisdiction of the Republic of Armenia:**
  - **Authority:** The Personal Data Protection Agency of the Ministry of Justice of the Republic of Armenia.
  - **Core Mandate:** Enforces individual privacy compliance under Law HO-119-N, handles localized infrastructure security audits, and investigates domestic user data disclosures.
- **Within the Jurisdiction of the European Union (EU) and European Economic Area (EEA):**
  - **Authority:** Any national Data Protection Authority (DPA) operating within the specific EU Member State of your habitual residence, your primary place of work, or the physical location where the alleged data privacy infringement occurred.
  - **Core Mandate:** A comprehensive register and direct contact portals for all independent European DPAs are maintained and publicly updated by the European Data Protection Board (EDPB).

21.4 Judicial Recourse Exception

The right to file a complaint with a regulatory supervisor operates in parallel with, and does not prejudice, any constitutional or statutory rights you may hold to initiate independent civil litigation or seek judicial remedies against the Company before a court of competent jurisdiction in the Republic of Armenia.

---

22. Amendments, Version Control, and Policy Evolution

22.1 Right to Modify and Update

Nakmo Cloud reserves the absolute corporate right to modify, amend, rewrite, or update this Privacy Policy at any discretion. This is necessary to accommodate structural enhancements to our cloud node

architecture, balance optimization metrics within the Cloud Karma System, or maintain continuous compliance with shifting international data protection regimes.

22.2 Material vs. Non-Material Notifications

- **Material Changes:** If we execute adjustments that substantively alter your individual privacy rights, data retention schedules, or third-party disclosure protocols, we will transmit a prominent notification. This will be delivered via a system-wide banner inside the Nakmo Cloud application or distributed directly to the verified email address linked to your user profile at least **fourteen (14) calendar days** before the updated policy takes effect.
- **Non-Material Changes:** Minor grammatical corrections, stylistic edits, or updates to the sub-processor registry that do not degrade your security stance will be updated instantly on our public website without formal proactive notification.

22.3 Binding Acceptance and Sole Remedy

The updated version of the Privacy Policy supersedes all previous iterations, communications, or verbal understandings.

- **Implied Consent:** Your continued interaction with our cloud servers, API endpoints, or mobile interfaces following the formal publication or notice of an updated Policy constitutes your unconditional, legally binding acceptance of the revised data processing operations.
- **The Opt-Out Remedy:** If you object to any element of an updated Policy, you must immediately cease uploading files and exercise your right to erasure. Your sole and exclusive remedy is to permanently delete your account through the application settings, which will trigger the immediate eviction protocols defined in Section 13.

22.4 Historical Archives and Document Integrity

Nakmo Cloud maintains a strict, internal chronological archive of all past versions of this Privacy Policy. Users or legal compliance officers may request a historical text copy for comparative purposes by submitting an inquiry to **legal@nakmo.net**.

---

23. Corporate Identification and Contact Channels

23.1 Official Corporate Roster

For the purposes of the General Data Protection Regulation (GDPR), the Republic of Armenia Law "On Protection of Personal Data" (HO-119-N), and other applicable regional privacy frameworks, the legal

entity acting as the **Data Controller** responsible for your Personal Data, account telemetry, and cloud storage infrastructure is:

- **Company Name:** Nakmo Cloud LLC
- **Registered Legal Address:** Republic of Armenia, Yerevan, Minsk Street 17-19, Apt. 10
- **Corporate Phone Line:** +374 44 16 66 20
- **Primary Corporate Email:** support@nakmo.net
- **Dedicated Legal & Privacy Desk:** legal@nakmo.net

23.2 Scope of Communications

You are encouraged to utilize the communication channels established in Section 23.1 to submit any inquiries regarding the following operational and legal categories:

- Submission of statutory Data Subject Requests (including rights to access, data portability, or account erasure as defined in Section 14);
- Technical reporting of suspected infrastructure vulnerabilities, data leaks, or unauthorized system access;
- Reporting of unauthorized registrations executed by minors below the permissible age thresholds (as defined in Section 18);
- Service of formal administrative notifications, regulatory audits, or judicial process documents.

23.3 Document Archival Status

- **Current Edition:** Version 1.1
- **Effective Operational Date:** May 26, 2026
- **Status:** Officially Ratified and Publicly Active