DATA PROTECTION

ONEOVA PRIVACY POLICY

Document ID: `ONV-LEGAL-PRIV-2026-V1`
Effective Date: October 25, 2026
Data Controller: THE CROWNED COLLECTIVE PRESSE (operating Oneova, "we", "us", or "our")
Data Protection Officer (DPO) & Trust Office: `thecrownedcollectivepress@gmail.com`
Web Portal: `https://oneova.app/privacy` · **Data Deletion:** `https://oneova.app/deletion`

Executive Summary ("In Short"):
1. **We never sell your personal data**—not your phone number, not your contacts, not your private chats, and not your videos.
2. **We never store mobile-money PINs** (M-Pesa, MTN MoMo, Airtel, Orange, Wave) or raw card CVVs.
3. **On-device first:** Hardware profiling (`Device Advisor`), thermal protection, and local Studio edits run on your device wherever possible to protect your privacy and save your mobile data bundle.
4. **Private stays private:** Private Chat messages, voice/video calls, KYC IDs, and unpublished Studio drafts are **never** used to train generative AI models.
5. **2-Tap Control:** Access, export, or permanently delete your account anytime in **Me → Settings → Privacy & Security**.

---

1. Scope and Global + African Data Protection Standards

This Privacy Policy explains how THE CROWNED COLLECTIVE PRESSE (operating Oneova) collects, uses, protects, shares, and deletes personal data across the Oneova mobile, desktop, and web applications (Reels, Stories, Chat & Calls, 4K Live, Studio, AI Lab, Ova Assistant, Wallet & Coins, and Biz Marketplace).

We engineer our privacy practices to comply with leading African and global data protection laws, including:

- **Kenya:** Data Protection Act, 2019 (ODPC)
- **Nigeria:** Nigeria Data Protection Act (NDPA), 2023 (NDPC)
- **South Africa:** Protection of Personal Information Act, 2013 (POPIA — Information Regulator)
- **Tanzania:** Personal Data Protection Act, 2022 (PDPC)
- **Uganda:** Data Protection and Privacy Act, 2019 (PDPO)
- **Rwanda:** Law No. 058/2021 Relating to the Protection of Personal Data and Privacy (NCSA)
- **Ghana:** Data Protection Act, 2012 (Act 843 — DPC)
- **Francophone & North Africa:** Côte d'Ivoire Law No. 2013-450 (ARTCI), Senegal Data Protection Law (CDP), Egypt PDPL No. 151/2020, Morocco Law 09-08 (CNDP), Ethiopia Proclamation No.

1321/2024, and the **African Union Malabo Convention**.

- **Global:** EU/EEA & UK General Data Protection Regulation (**GDPR**), California (**CCPA/CPRA**), and Brazil (**LGPD**).

---

2. Schedule of Personal Data We Collect, Purpose & Legal Basis

Data Category	Specific Data Elements	Purpose of Processing	Lawful Basis
1. Account & Identity	Username, display name, phone number or email, birth date / age bracket, password hash or WebAuthn passkey, profile bio & avatar	Create and authenticate your account, enforce teen age-safety defaults, prevent SIM-swap and bot takeovers	**Performance of Contract** & **Legal Obligation** (child safety)
2. Creative & Public Content	Reels, Stories, photos, captions, hashtags, comments, Live streams, custom Studio Looks (`.oneovapack`), Biz product listings	Host, transcode into adaptive bitrates, and distribute content to your selected audience	**Performance of Contract**
3. Private Messaging & Calls	Chat messages, media attachments, voice notes, call signaling/routing logs, read/delivery state	Deliver private communications reliably, synchronize across authorized devices, prevent spam/abuse	**Performance of Contract** & **Legitimate Interest** (network security)
4. Wallet, Coins & Biz Transactions	Coin purchase receipts, Gift ledger entries, payout mobile-money number or bank account, transaction IDs, KYC verification status (for 18+ payouts/merchants)	Process payments and creator payouts via licensed PSPs, maintain double-entry accounting, prevent fraud and money laundering	**Performance of Contract** & **Legal Obligation** (tax, AML/CTF & payment laws)
5. Device, Network & Thermal Telemetry	Device model, OS version, GPU/RAM/thermal capability tier (`Device Advisor`), app version, IP address, coarse country/region, crash diagnostics	Prevent phone overheating during 4K/Live use, optimize video streaming for 2G/3G/4G/Wi-Fi, fix crashes, block credential stuffing	**Legitimate Interest** (service reliability, device safety & security)
6. Engagement & Feed Signals	Watch completion, likes, saves, shares, follows, "Not Interested" taps, preferred app language	Rank relevant Reels and Biz items in your **For You** feed and honor content filters	**Performance of Contract** / **Legitimate Interest** (customizable in Settings)
7. Connected OAuth Channels	Encrypted OAuth access/refresh tokens and basic channel IDs when you link TikTok, YouTube, Instagram, or Meta	Execute 1-tap cross-platform video publishing strictly at your command	**Explicit Consent** (revocable anytime)
8. Optional Device Permissions	Camera, Microphone, Photo Library, Contacts (cryptographically hashed), Coarse/Precise Location (for optional Biz delivery or geo-tags)	Operate capture, voice chat, friend discovery, or local commerce **only when enabled by you**	**Explicit Consent** (revocable in OS or app settings)
9. AI Lab & Ova Assistant Inputs	Prompts, voice commands, captions, or media frames you actively submit to AI tools	Generate the color grade, cutout, caption, or assistant action you requested	**Performance of Contract** / **Consent**

Strict Exclusions — Data We NEVER Collect

1. **Never Mobile-Money PINs or Card CVVs:** We never request, see, or store your M-Pesa PIN, MTN MoMo PIN, Airtel/Orange PIN, bank password, or raw payment card CVV. All payment authentication happens inside regulated PCI-DSS / central-bank-licensed gateways.
2. **Never Covert Recording:** Oneova never activates your camera or microphone in the background without an active recording, call, Live broadcast, or explicit voice-assistant session initiated by you.
3. **Never Unconsented Contact Harvesting:** Your phone address book is never uploaded unless you explicitly grant Contacts permission.

---

3. How We Protect AI, Biometrics & Facial Landmarks

3.1 On-Device AR & Beauty Processing. When you use Studio Looks, Boost Beauty, or AR camera lenses, facial/pose landmark alignment runs in volatile device memory in real time to position visual effects. **Oneova does not build or sell a facial-recognition identity database from camera effects.**

3.2 App Biometric Lock. When you enable Fingerprint or Face Unlock in **Privacy & Security**, authentication is performed strictly by your operating system's secure hardware enclave (`Android Keystore` / `Apple Secure Enclave`). Oneova never receives or stores your fingerprint image or facial scan.

3.3 AI Firewall & Zero Private Training. Inputs handled by Oneova AI tools pass through `AiSecurityGateway` prompt-injection isolation. Private Chat messages, calls, KYC documents, and unpublished Studio drafts are **never** used to train generative AI models or shared with external advertisers.

---

4. How and When Information Is Shared

We **never sell or rent** personal data to data brokers or third parties. We share limited data only in five strictly controlled situations:

1. **According to Your Audience Settings:** Other users see your profile, public Reels, Live broadcasts, or Biz store according to whether you choose **Public**, **Followers Only**, or **Private**.
2. **Biz Order Fulfillment:** When you order a physical item from a Biz Seller, that seller receives only the order details, name, delivery address, and contact number needed to deliver your order.
3. **Contractually Bound Infrastructure Processors:** Trusted cloud, streaming, and payment processors—such as Google Cloud / Firebase (database, auth, storage), LiveKit (low-latency Live WebRTC relay), Flutterwave, Stripe, licensed mobile-money aggregators, Apple, and Google Play—acting strictly under written **Data Processing Agreements (DPAs)** with confidentiality and security mandates.
4. **Valid Legal Process & Emergency Child/Life Protection:** We disclose non-public records to law enforcement or regulators **only** in response to a legally valid warrant, court order, or statutory mandate (such as confirmed CSAM reporting under child-protection laws), subject to human-rights and legality review under our **Law Enforcement Guidelines**. Unless legally prohibited, we notify affected users prior to disclosure.

5. **Corporate Transactions:** In a merger, acquisition, or financing, data remains subject to protections at least as strong as this Privacy Policy, with advance notice to users before any material change.

---

5. International & Intra-African Data Transfers

Because Oneova connects creators and businesses across Africa and the world, personal data may be processed on secure cloud servers outside your country of residence. Whenever data is transferred internationally, we implement legally recognized transfer safeguards:

- **Adequacy & Regulator Whitelists** recognized under your national data protection law;
- **Standard Contractual Clauses (SCCs)** and binding Data Transfer Agreements enforcing equivalent technical and legal protections;
- **Statutory Registration & Prior Authorization** where required for specific data categories under **Kenya DPA Part VI**, **Nigeria NDPA Part VI**, **South Africa POPIA s.72**, **Tanzania PDPA**, **Rwanda Law No. 058/2021**, **Côte d'Ivoire ARTCI**, and **Morocco CNDP**; and
- **End-to-end TLS 1.3 encryption in transit** and **AES-256 encryption at rest**.

---

6. Data Retention & Deletion Schedule

Record Type	Retention Period
Active Account & Published Posts	Retained while your account remains open and until you delete the item
User-Deleted Posts or Deleted Account	Removed from public visibility **immediately**; purged from active production clusters within **24 hours to 30 days**, and rotated out of encrypted backups within **90 days**
24-Hour Stories	Automatically expire from Story rings after **24 hours** (unless saved by you to Archive/Highlights)
Connected Social OAuth Tokens	Deleted **immediately** when you disconnect the channel or delete your account
Wallet, Coin & Biz Tax/AML Ledgers	Retained in restricted accounting storage for **5 to 7 years** strictly as mandated by tax, central-bank, and anti-money-laundering laws
Confirmed CSAM / Severe Fraud Ban Records	Hashed identifiers and preserved evidence retained for the statutory period required by cybercrime laws and to prevent ban evasion
Diagnostic, Security & Crash Logs	Automatically rotated or anonymized within **90 to 180 days**

---

7. Security Architecture & 72-Hour Breach Commitment

Oneova enforces defense-in-depth engineering controls:

- **Cryptographic Tenant Isolation** (`users/{uid}`) and explicit `allowedViewers` access control lists preventing cross-account data leaks;

- **Passkeys, 2FA, App PIN / Biometrics, and Active Session Controls** allowing instant remote sign-out of lost or stolen phones;
- **Zero Standing Staff Access** to private messages, audited break-glass controls, and mandatory hardware MFA across internal infrastructure;
- **Breach Notification Guarantee:** In the event of a personal data breach posing a risk to user rights and freedoms, Oneova notifies competent Data Protection Authorities within **72 hours** (or shorter national deadline) and promptly notifies affected users in plain language.

---

8. Your Privacy Rights & How to Exercise Them

We extend strong data rights to **every Oneova user worldwide**:

1. **Right of Access & Information:** Know what personal data we process about you.
2. **Right to Data Portability (Export):** Download a structured copy of your profile, settings, and content (**Me → Settings → Privacy & Security → Export Data**).
3. **Right to Rectification:** Update or correct inaccurate account details anytime.
4. **Right to Erasure (Account & Data Deletion):** Permanently delete individual items or your entire account in-app or via `https://oneova.app/deletion`.
5. **Right to Withdraw Consent:** Revoke Camera, Microphone, Location, Contacts, Connected Channels, or marketing notifications at any time without penalty.
6. **Right to Object / Restrict Automated Profiling:** Reset feed recommendations or opt out of personalized promotional targeting in Settings.
7. **Right to Lodge a Regulatory Complaint:** You may contact our DPO at `thecrownedcollectivepress@gmail.com` (free response within **21 days**, and always within statutory 30-day limits) or contact your national supervisory authority:

- **Kenya:** Office of the Data Protection Commissioner (`odpc.go.ke`)
- **Nigeria:** Nigeria Data Protection Commission (`ndpc.gov.ng`)
- **South Africa:** Information Regulator (`inforegulator.org.za`)
- **Tanzania:** Personal Data Protection Commission (`pdpc.go.tz`)
- **Uganda:** Personal Data Protection Office (`pdpo.go.ug`)
- **Rwanda:** National Cyber Security Authority — Data Protection Office (`dpo.gov.rw`)
- **Ghana:** Data Protection Commission (`dataprotection.org.gh`)
- **EU / EEA / UK:** Your local Data Protection Authority or UK ICO (`ico.org.uk`).

---

9. Children's & Teen Privacy

Oneova does not permit accounts for children under **13**. Users aged **13 to 17** receive privacy-by-design defaults—including private-by-default profiles for ages 13–15, mutual-follower DM protections, disabled targeted ad profiling, and blocked Wallet/Live monetization. Full details are set out in our **Child & Teen Safety Policy**.

© 2026 THE CROWNED COLLECTIVE PRESSE (operating Oneova). All rights reserved.

Official Trust & Legal Office: thecrownedcollectivepress@gmail.com