Archonite Privacy Policy

Last updated on January 1, 2025

1. Introduction

Archonite Inc. ("Archonite", "We", "Us", "Provider") respects your privacy and is committed to protecting it through our compliance with this policy. This Privacy Policy describes the types of information we may collect from you or that you may provide when you visit our website or use our identity verification APIs, SDKs, and Dashboard ("Services").

We act primarily as a Data Processor on behalf of our Customers (the businesses requesting your verification). However, we act as a Data Controller regarding our direct Customer account information and website analytics.

Role Definitions:

- **Data Processor:** When we verify an identity on behalf of a business client (our "Customer"), Archonite acts as a Data Processor.
- **Data Controller:** When you visit our marketing website, sign up for a developer account, or contact our support, Archonite acts as the Data Controller of your account information.

This policy adheres to the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA/CPRA), and the Philippine Data Privacy Act of 2012 (RA 10173).

2. Information We Collect

(a) End-User Data (Verification Subjects)

When an individual undergoes verification, we collect strictly what is necessary to perform the service:

- **Government ID Images:** Front and back images of passports, driver's licenses, or national IDs.
- **Extracted PII:** Data parsed via OCR such as Full Name, Date of Birth, Address, Nationality, Document Number, and Expiry Date.
- **Biometric Inputs:** Selfie video or static images used for liveness analysis.
- **Device Metadata:** IP address, User-Agent, device model, and OS version (used exclusively for fraud detection and risk scoring).

(b) Customer Data (Business Clients)

To manage your access to the Archonite platform, we collect:

- **Account Info:** Business email, hashed passwords, and company details.
- **Billing Details:** Payment tokens (via PayMongo) and billing addresses. We do not store raw credit card numbers.
- **Integration Logs:** API usage patterns, webhook endpoints, and developer activity logs.

3. Biometric Data Policy

Archonite processes "Biometric Data" (facial geometry and liveness vectors) which is classified as Sensitive Personal Information. We adhere to the strictest standards regarding this data.

(a) Definition & Nature

We generate a mathematical representation (a "template" or "vector") of your facial features. This template is used to compare your selfie against the photo on your ID document. This template is proprietary and cannot be reverse-engineered into a photograph.

(b) Explicit Consent (BIPA/GDPR)

Biometric processing never occurs without affirmative consent. Our SDKs include a mandatory consent screen where End-Users must explicitly agree to the collection of biometric data before the camera is activated.

(c) Prohibited Uses

Archonite creates biometric templates solely for identity verification and fraud prevention. We do not, and will not, sell, lease, trade, or profit from biometric data. We do not use biometric data for surveillance or behavioral advertising.

(d) Retention Schedule

Biometric templates are transient by default. They are permanently destroyed immediately upon the completion of the verification session or within a maximum of 30 days, unless a valid legal order requires preservation.

4. Purposes of Processing

We process data based on the following legal grounds:

- **Contractual Necessity:** To fulfill the verification requests initiated by our Customers.
- **Legal Obligation:** To comply with Anti-Money Laundering (AML), Know Your Customer (KYC), and Counter-Terrorism Financing (CTF) regulations.
- **Legitimate Interests:** To detect and prevent fraud across our network (e.g., identifying a fake ID used across multiple clients) and to ensure network security (DDoS mitigation).
- **Consent:** For specific sensitive data processing (Biometrics) or optional marketing communications.

Model Improvement: We may use de-identified, anonymized, and aggregated data to train and improve our computer vision models (e.g., to reduce bias in facial recognition). This data cannot be linked back to any specific individual.

5. Automated Decision Making

Our Services employ automated decision-making logic to determine the validity of an ID document and the liveness of a user.

(a) Logic Involved

The system analyzes visual security features (holograms, fonts), metadata consistency, and facial similarity scores. A "Fraud Score" is generated. If the score exceeds a threshold, the verification is automatically rejected.

(b) Human Review

While we offer fully automated flows, Customers typically configure a "Hybrid" workflow where rejected or low-confidence verifications are routed to a human Review Officer for Enterprise plan subscriptions. End-Users have the right (under GDPR) to request human intervention if a decision has legal consequences.

6. Disclosure & Sharing

We disclose Personal Information only in the following controlled scenarios:

(a) To the Customer

The Business Client who initiated the request receives the full verification report. They act as an independent Controller of this data once received.

(b) Trusted Sub-processors

We engage third-party vendors who are bound by Data Processing Agreements (DPAs) and confidentiality clauses.

- **AWS/Vercel (US West):** Infrastructure hosting and domain provider.
- **PayMongo (Philippines):** Payment Processor for handling billing transactions.
- **Hostinger:** Transactional email service provider.
- **Global Watchlists (Classified):** For PEP/Sanctions screening (only if requested by Customer).

(c) Legal Requirements

We may disclose data to law enforcement if compelled by a valid court order, subpoena, or search warrant. We challenge such requests if they are overly broad or lack legal basis.

(d) Corporate Transactions

In the event of a merger, acquisition, or sale of assets, customer data may be transferred as a business asset, subject to the acquirer respecting this privacy policy.

7. Security & Incident Response

We implement a defense-in-depth security strategy designed to protect data against unauthorized access, alteration, and destruction.

- **Encryption:** All of the payloads are hashed via Archonite Signed Payload to ensure all data are protected.
- **Access Control:** We use Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) for all internal systems. No engineer has standing access to production customer data.
- **Penetration Testing:** We conduct annual third-party audits and maintain a private Bug Bounty program.
- **Incident Response:** In the event of a data breach, we will notify affected Customers and regulatory authorities within 72 hours of becoming aware of the breach, in accordance with GDPR/PDPA requirements.

8. Data Retention & Archival

We retain data only as long as necessary. Default retention periods are defined below, but Enterprise Customers may configure shorter periods via the API.

Data Type	**Retention Period**	**Purpose**
Biometric Vectors	Max 30 Days	Verification & Fraud prevention window
Document Images	90 Days (Default)	Dispute resolution & Audit
Transaction Logs	5 Years	Financial, AML, and CTF regulatory compliance

9. Cross-Border Transfers

Archonite is a global company. Data collected in the EEA, UK, or Switzerland may be transferred to, and stored at, a destination outside the European Economic Area (specifically the Philippines and the USA).

In addition, our Privacy Policy incorporates the EU Commission's latest Standard Contractual Clauses (SCCs) for transfers to third countries.

10. Rights of Data Subjects

Depending on your jurisdiction (GDPR, CCPA, PDPA), you possess specific rights regarding your personal data:

The Right to Access

You have the right to request copies of your personal data.

The Right to Rectification

You have the right to request that we correct any information you believe is inaccurate.

The Right to Erasure

You have the right to request that we erase your personal data ("Right to be Forgotten"), subject to overriding legal obligations (e.g., maintaining fraud records).

The Right to Object

You have the right to object to our processing of your personal data for direct marketing purposes.

Exercising Your Rights

If you verified your identity with an Archonite Customer, please contact them directly, as they are the Data Controller. If you contact us, we are legally required to redirect your request to the Customer. For direct inquiries regarding Archonite's own data handling, email privacy@archonite.xyz.

11. Cookies & Tracking

We use cookies and similar tracking technologies to track the activity on our Service and hold certain information.

- **Essential Cookies:** Required for the operation of the Dashboard (e.g., session tokens).
- **Security Cookies:** Used to detect unusual login behavior.
- **Analytics Cookies:** We use minimal, privacy-focused analytics to understand SDK performance. We do not use third-party advertising pixels on our verification interfaces.

12. Children's Privacy

Our Service is strictly intended for individuals 18 years of age or older. We do not knowingly collect, use, or disclose personal data from children under 18. If we identify that a verification attempt involves a minor (via OCR of the Date of Birth), the system is configured to automatically reject the transaction and purge the data immediately, unless the Customer has configured specific "Parental Consent" flows compliant with COPPA/GDPR-K.

13. Updates to Policy

We may update this Privacy Policy from time to time. We will notify you of any material changes by posting the new Privacy Policy on this page and updating the "Effective Date."

For Enterprise customers, we provide email notifications 30 days prior to material changes affecting data processing terms.

14. Contact & Address

Email: privacy@archonite.xyz

Mailing Address: Archonite Inc., 842-B Sapphire Lane, Phase 4, San Miguel, Pasig City, Philippines