DATA RETENTION POLICY

This Data Retention policy was last updated on 2026-02-02.

1. Purpose

This Data Retention Policy defines Smile ID's practices for retaining and securely disposing of personal data collected through its services. This includes services such as identity (ID) verification, ID fraud detection, Know Your Customer (KYC) processes, and Anti-Money Laundering (AML) screening.

This policy ensures Smile ID's compliance with international and national data protection laws, including:

- General Data Protection Regulation (GDPR);
- Ghana: Data Protection Act, 2012 (Act 843);
- Nigeria: Nigeria Data Protection Act (NDPA), 2023;
- Kenya: Data Protection Act, 2019;
- Uganda: Data Protection and Privacy Act, 2019; and
- South Africa: Protection of Personal Information Act (POPIA), 2013.

2. Scope

This policy applies to all personal data processed by Smile ID in connection with:

- Identity verification and authentication services;
- KYC and AML screening;
- ID Fraud Detection Systems;
- SDK and API-based integrations and biometric services; and

It covers data received directly from individuals, business clients, and third-party data providers.

3. Retention Period

3.1. Personal data shall be retained only for as long as is necessary to achieve the purpose of its collection.

3.2. Full names, date of birth, address, phone numbers, image, IP address, ID information (ID number, type, and country), Email address, and document

photo shall be retained for no longer than 5 years from the date of collection or processing, unless a lawful exception applies.

3.3. Where retention periods cannot be strictly defined, Smile ID will apply reasonable criteria for determining the appropriate retention timeline.

3.4. Personal data that is no longer required will be securely deleted or irreversibly anonymized to prevent identification of any individual.

4. Legal Basis for Retention

Smile ID processes personal data under these legal bases:

4.1. **Performance of contracts** - we retain data that is necessary to fulfil our contractual obligations to our customers and users.

4.2. **Legitimate interests** – we retain personal data where it is necessary for fulfilling legitimate interests, including but not limited to fraud prevention, provided such interests are not overridden by the rights and freedoms of the data subject. We have conducted Legitimate Interests Assessments (LIAs) to ensure these interests are balanced and proportionate.

4.3. **Consent** – we retain personal data where informed consent is freely and explicitly given by the data subjects. We retain the relevant personal data only for as long as the consent remains valid unless otherwise required by law.

4.4. **Compliance with legal obligations** – we retain certain categories of data to comply with legal or statutory obligations, such as financial or regulatory requirements.

Each retention decision is justified with reference to the appropriate legal basis.

5. Data Disposal Methods

At the end of the retention period, personal data is securely removed using methods including:

- Encrypted deletion protocols;
- System-level purge or archival deletion;
- Data masking and anonymization; and
- Manual review for exception handling.
- Deletion logs will be maintained for audit purposes.

6. Exceptions

In the following cases, Smile ID may retain data beyond any specified retention period:

- To comply with applicable legal obligations
- To support ongoing or potential fraud or AML investigations
- To fulfil a lawful request or order from a regulatory or judicial authority
- Where necessary for the establishment, exercise, or defense of legal claims
- Where data retention is mandated by a contractual obligation with a client
- For audit, accounting, or compliance purposes where explicitly allowed by law

All exceptions must be documented and reviewed by Smile ID's Data Protection Officer (DPO).

7. Data Subject Rights

Data subjects may exercise the following rights under applicable data protection laws:

- Right to access, correct, and delete personal data
- Right to object to processing beyond the retention period
- Right to withdraw consent (where applicable)
- Right to lodge complaints with a relevant supervisory authority

Requests may be submitted to: dpo@usesmileid.com.

8. Review and Governance

This policy will be reviewed annually or earlier in response to:

- material legal or operational changes; or
- the introduction of new services or processing activities.

Policy updates are approved by the Data Protection Officer and Smile ID's executive compliance team, who are responsible for overseeing this policy, reviewing retention decisions, and ensuring alignment with data protection obligations.

Effective Date and Approval

Effective Date: 2026-02-02

Approved by: Data Protection Officer, Smile ID