DATA RETENTION POLICY

This Data Retention policy was last updated on 2026-07-10.

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. For South African data subjects, this Policy operates under the Protection of Personal Information Act, 4 of 2013 ("POPIA"), under which Smile ID acts as a Responsible Party, and its designated Information Officer is accountable for retention decisions.

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), 4 of 2013 — retention and destruction governed by sections 13–14 of POPIA.

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 or as required or permitted by law. Under sections 13–14 of POPIA, personal information may not be retained longer than is necessary to achieve the purpose of collection; once the purpose has lapsed, the information must be destroyed, deleted, or de-identified.

3.2. **POPIA — Children's Biometric Data:** Under section 35 of POPIA, a child is any person under 18 years of age. The processing of a child's personal information, including biometric data, requires parental or guardian consent and is subject to additional restrictions. Where Smile ID processes biometric data that may relate to a minor, enhanced retention controls and parental consent verification are applied.

3.3.

Categories Of Personal Data Collected	Retention Period
Personal information such as name, date of birth, address, phone numbers	Retained for no longer than 5 years from the date of collection or processing, unless a lawful exception applies
Biometric information such as live capture images, document photos	Retained for no longer than 5 years from the date of collection or processing, unless a lawful exception applies Note: under POPIA section 14, biometric information (special personal information under section 26(1)(b)) must be destroyed or de-identified as soon as the verification purpose lapses. Smile ID applies a default 90-day post-verification retention period for biometric data in its Operator capacity, reverting to the 5-year maximum only where a specific lawful basis under section 27 of POPIA requires longer retention.
Device information such as IP address, location data, and online activity	Retained for no longer than 5 years from the date of collection
Account information such as usernames, email addresses,	Retained for no longer than 5 years after account deletion
V3 optimised pre-verified results	Retained for no longer than 5 years, except where a lawful exception applies.

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

3.5. Personal data that is no longer required will be securely deleted or irreversibly anonymized to prevent identification of any individual. In accordance with section 14(2) of POPIA, destruction of personal information must be done in a manner that prevents its restoration or reconstruction.

4. Legal Basis for Retention

Smile ID processes personal data under these legal bases: For South African data subjects, these legal bases correspond to the conditions for lawful processing in section 11 of POPIA.

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

4.2. **Legitimate interests** – we retain personal data where necessary to fulfil legitimate interests, including, but not limited to, fraud prevention, provided such interests are not overridden by the data subject's rights and freedoms. 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) and, for South African processing activities, the designated Information Officer (IO) as required by section 55 of POPIA.

7. Data Subject Rights

Data subjects may exercise the following rights under applicable data protection laws: Under POPIA, these include the rights in sections 23–25: the right of access (section 23), the right to correction or deletion (section 24), and the right to object to processing (section 11(3)). Under section 69 of POPIA, data subjects may object to direct marketing at any time and processing must cease immediately on receipt.

- 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 — for South African data subjects, this is the Information Regulator: inforeg@justice.gov.za | www.inforegulator.org.za

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: 2026-07-10

Approved by: Data Protection Officer, Smile ID