



**MANUAL IN TERMS OF SECTION 51 OF THE
PROMOTION OF ACCESS TO INFORMATION ACT
2 OF 2000**

Smile Identity

Document attribute	Detail
Document reference	SID-ZA-PAIA-MAN-001
Version	1.0
Effective date	1 July 2025
Last updated	June 2026
Review cycle	Annual
Classification	PUBLIC — Available on request, free of charge
Contact	dpo@usesmileid.com

Public document notice — PAIA s.51(3)

This Manual is available to any person on request, free of charge, in accordance with section 51(3) of the Promotion of Access to Information Act, 2 of 2000 ("PAIA"). It is also published on the Smile ID website at www.smile.id/paia-manual. Requests for access to records held by Smile ID must be submitted in accordance with the procedure set out in this Manual.

Part A: Introduction and Company Information

A.1 About Smile ID

Smile Identity is Africa's leading digital identity verification and KYC compliance provider. Founded with a mission to unlock digital access for every African, Smile ID has completed over 200 million identity verification checks across more than 35 countries on the continent. We serve clients in financial services, fintech, telecommunications, e-commerce, and regulated industries, providing biometric identity verification, document verification, ID fraud detection, and Anti-Money Laundering (AML) screening services through our API and SDK products.

Our South African subsidiary, Smile Identity, is incorporated and registered with the Companies and Intellectual Property Commission (CIPC). Our physical and registered presence in South Africa makes us a "private body" for the purposes of PAIA, and our processing of personal information in South Africa makes us a Responsible Party under the Protection of Personal Information Act, 4 of 2013 ("POPIA").

A.2 Registered Details

Attribute	Detail
Company name	Smile Identity
Registration number	2018/068222/10
Registered address	BLOCK D OFFICE D7 CARPE DIEM 26 QUANTUM STREET TECHNO PARK STELLENBOSCH WESTERN CAPE 7600
Postal address	PO BOX 1206 STELLENBOSCH STELLENBOSCH WESTERN CAPE 7599
Website	www.smile.id
Group parent	Smile Identity Inc. (USA)
Services	Identity verification, biometric KYC, document verification, AML screening, ID fraud detection
Jurisdictions of operation	South Africa and 35+ African countries

A.3 Information Officer

Smile ID has designated a registered Information Officer in terms of section 55 of POPIA, who is responsible for encouraging and ensuring POPIA compliance, processing data subject requests, liaising with the Information Regulator, and maintaining this Manual.

Role	Detail
Designation	Information Officer (registered with the Information Regulator)
Name	Mark Straub
Title / position	CEO
Email	dpo@usesmileid.com
Telephone	0781985145
Physical address	Stemantom Agencies, 79 5th Street, Springs, New Springs, 1559,
Deputy Information Officer(s)	Talita Van Niekerk , 0720327836

Dual obligation — PAIA and POPIA

This Manual serves two complementary purposes: (1) it enables members of the public to exercise their right of access to records held by Smile ID; and (2) it demonstrates how Smile ID's POPIA obligations — including data subject rights, security safeguards, the Information Officer designation, and breach notification requirements — are integrated into our governance. Where a request constitutes a data subject exercising rights under POPIA (sections 23–25), Smile ID processes the request under both PAIA and POPIA without requiring separate submissions.

A.4 Guide on Using PAIA

The South African Human Rights Commission (SAHRC) has published a guide on how to use PAIA (the section 10 guide). This guide is available in all 11 official languages from the SAHRC at www.sahrc.org.za and from the Government Printer. The guide explains the procedure for submitting access requests and the circumstances under which access may be refused.

Part B: Records Held by Smile ID

B.1 Categories of Records

Smile ID holds the following categories of records. Certain records are subject to grounds for refusal under sections 62 to 70 of PAIA (see Part D). The availability column indicates the general accessibility position before any grounds for refusal are assessed.

Category of records	Description	General availability
Statutory and corporate	Memorandum of Incorporation, board minutes, CIPC filings, share register, annual financial statements	Certain records are publicly available at CIPC; others are subject to commercial privilege
Human resources and employment	Employment contracts, payroll, leave, performance, disciplinary, health and medical records for employees	Restricted — employee privacy; third-party personal information
Client and commercial contracts	Service agreements, data processing agreements (DPAs), operator agreements, SLAs, non-disclosure agreements	Confidential — commercial and legal privilege
Financial and accounting	Invoices, bank records, VAT returns, management accounts, audit records	Restricted — commercial confidentiality; statutory retention obligation
Identity verification and KYC records (Operator context)	Biometric data (facial geometry), identity document images, verification outcomes, liveness results — processed on behalf of the client's Responsible Parties	Restricted — subject to client Responsible Party instructions; protected as special personal information under POPIA s.26
Smile ID client account data (Responsible Party context)	Business contact details, CRM records, usage logs, and billing records for Smile ID's own clients	Restricted — third-party commercial information; personal information of client contacts
Information security records	Information Security Policy, audit reports, penetration test results, vulnerability assessments, Security Compromise Register	Restricted — security sensitivity; disclosure would undermine safeguards
POPIA compliance records	POPIA Compliance Framework, Record of Processing Activities (ROPA), PIIA reports, training register	Partially available — framework available on request; operational detail restricted
Direct marketing and consent records	Campaign records, consent register, Do-Not-Contact list, opt-out register	Available to data subjects in respect of their own records on a valid POPIA s.23 request
Website and analytics data	Server logs, IP address logs, cookie consent records, analytics data	Restricted — technical security; pseudonymised data
Job applications and recruitment	CVs, assessments, reference checks, interview notes	Available to the data subject in respect of their own records
Correspondence and communications	Emails, support tickets, data subject request correspondence	Restricted — third-party privacy; legal privilege where applicable

B.2 Records Available Without a Formal Request

The following records are published or publicly available and do not require a formal PAIA request:

- Privacy Policy — www.smile.id/privacy-policy

- Cookie Policy — www.smile.id/cookie-policy
- This PAIA Manual — www.smile.id/paia-manual
- Data subject rights request form — www.smile.id/dsr-request-form
- CIPC public filings — www.cipc.co.za
- SAHRC guide on PAIA — www.sahrc.org.za

B.3 POPIA Integration — Data Subject Access to Own Personal Information

Unified access channel

Where a request for access to records constitutes a data subject exercising their right of access under section 23 of POPIA (access to own personal information), Smile ID processes the request under both PAIA and POPIA. The data subject does not need to submit separate requests. No fee is charged for data subject access requests under POPIA. Requests may be submitted through any of the channels in Part C below, including WhatsApp and SMS, as required by the April 2025 POPIA Amendment Regulations.

Part C: How to Submit an Access Request

C.1 Submission Channels

Access requests may be submitted through any of the following channels. In accordance with the April 2025 POPIA Amendment Regulations, all channels listed below are available free of charge and are treated as equally valid:

Channel	Details
Email (primary)	dpo@usesmileid.com — include "PAIA/POPIA Access Request" in the subject line
Web form	www.smile.id/dsr-request-form
WhatsApp	0720327836
SMS	0720327836
Telephone	0720327836
Postal	Attention: Information Officer, P O BOX 1233, SPRINGS, 1560
In person	Stemantom Agencies, 79 5th Street, Springs New, Springs, 1559,— by appointment only; contact dpo@usesmileid.com to arrange

C.2 Information Required

A request should include the following information to enable Smile ID to locate the relevant records and verify the requester's identity:

- The requester's full name, identity number, and contact details;
- A description of the records requested with sufficient particularity to enable identification;
- The form in which access is required (copy, inspection, electronic copy, etc.);
- If acting on behalf of another person: written proof of authority (power of attorney, parental consent for a minor, or executor authority);
- Any additional information to assist in locating the record (e.g. verification date range, account number, product used);
- The reason for the request — note: not required for requests by a data subject about their own personal information under POPIA s.23.

C.3 Identity Verification

Smile ID verifies the identity of every requester before processing a request, protecting personal information from unauthorised disclosure. The verification standard is proportionate to the sensitivity of the records requested:

Record sensitivity	Verification method
--------------------	---------------------

Standard personal information (contact data, account data)	Verification from a registered email address or matching against the account record
Sensitive records (employment, financial, health data)	Verified email plus copy of government-issued ID (last 4 digits of ID number)
Special personal information (biometric data)	Enhanced: government-issued ID plus one additional authenticating factor (account credentials or verification transaction reference)
Requests on behalf of a minor	Proof of parental authority or legal guardianship required in all cases
Requests by authorised representative	Written authority plus identity verification of both the requester and the representative

C.4 Fees

Fee type	Amount
Request fee (third-party access requests under PAIA)	R35.00 (waived for data subjects requesting access to their own personal information under POPIA)
Search and preparation fee	As prescribed by PAIA Regulations 2 of 2002 (as amended) — estimated costs communicated in advance
Reproduction fees	As prescribed by PAIA Regulations — per page for paper copies; standard rate for electronic copies
Indigent requester	Fee waiver available on application — contact the Information Officer
Data subject access requests (POPIA s.23)	No fee charged — POPIA data subject access requests are free of charge

Part D: Processing of Requests and Response Timeframes

D.1 Standard Timeframes

Stage	Timeframe
Acknowledgement of request	Within 3 business days of receipt
Identity verification (where required)	Within 5 business days of receipt of verification documents
Decision on access (PAIA)	Within 30 calendar days of receipt (extendable by a further 30 days on written notice to the requester)
Data subject access response (POPIA s.23)	Within 30 calendar days of receipt (extendable by a further 30 days with notice and reason)
Direct marketing opt-out (POPIA s.69)	Immediate — all marketing must cease on receipt; platform suppression within 24 hours
Notice of extension	Before the expiry of the initial 30-day period, with a reason for extension
Appeal or review	30 days from the date of notice of refusal to approach the Information Regulator or the High Court

D.2 Grounds for Refusal

Access to records may be refused on the grounds set out in sections 62 to 70 of PAIA. The primary grounds applicable to Smile ID's records include:

- **Protection of personal information of a third party (s.63)** — disclosure would involve unreasonable infringement of another individual's right to privacy;
- **Commercial information/trade secrets (s.64)** — records containing commercially sensitive information, proprietary algorithms, or confidential client information;
- **Confidential third-party communications (s.65)** — information supplied in confidence by a third party that would prejudice their future supply of information;
- **Safety of individuals (s.66)** — disclosure would endanger the life, physical safety, or wellbeing of an individual;
- **Legally privileged information (s.67)** — records protected by attorney-client or litigation privilege;
- **Operations of private bodies (s.68)** — records that would prejudice a pending, current, or anticipated legal proceeding;
- **Research information (s.69)** — research records where premature disclosure would compromise the research.

Where access is refused on any ground, the Information Officer will provide written notice stating the ground of refusal, the right to appeal to the Information Regulator, and the right to apply to the High Court for relief under section 78 of PAIA.

D.3 Mandatory Disclosure Despite Grounds for Refusal

In terms of section 46 of PAIA, Smile ID must disclose a record — despite a ground for refusal otherwise applying — if the record reveals evidence of a substantial contravention of, or failure to comply with, the law or an imminent and serious public safety or environmental risk, and the public

interest in disclosure clearly outweighs the harm. This provision reflects PAIA's constitutional underpinning in the right of access to information under section 32 of the Constitution.

Part E: Data Subject Rights Under POPIA

E.1 Rights Available to Data Subjects

In addition to the right of access to information under PAIA, data subjects have the following rights under POPIA in relation to their personal information held by Smile ID in its capacity as Responsible Party:

Right	POPIA provision	How to exercise
Right of access — confirm processing and obtain a copy of personal information	s.23	Submit request via any channel in Part C — no fee applies; response within 30 days
Right to correction — correct inaccurate, misleading, or out-of-date personal information	s.24(1)	Submit a correction request via dpo@usesmileid.com with details of the inaccuracy
Right to deletion — destroy or delete personal information no longer lawfully retained	s.24(2)	Submit a deletion request; Smile ID will confirm which records are deleted and advise on any statutory retention obligation
Right to object to processing — object to processing based on legitimate interest	s.11(3)	Submit an objection in writing to dpo@usesmileid.com ; processing ceases pending assessment unless compelling grounds exist
Right to object to direct marketing — absolute right to opt out at any time	s.69	Submit via any channel in Part C, including WhatsApp or SMS; all marketing ceases immediately on receipt
Right re automated decision-making — right not to be subject to decisions based solely on automated processing with significant effects	s.71	Contact dpo@usesmileid.com to request an explanation of the automated decision and a human review
Right to withdraw consent — withdraw consent at any time without penalty	s.11(1)(a)	Notify dpo@usesmileid.com ; withdrawal does not affect the lawfulness of prior processing
Right to lodge a complaint with the Information Regulator	s.74	See Part F — Information Regulator contact details

E.2 Operator Context — End-User Verification Data

Important — identity verification end-users

When Smile ID verifies the identity of an individual on behalf of a client business (such as a bank or fintech), Smile ID acts as an Operator, and the client is the Responsible Party. In this context, data subject rights requests in respect of verification data should be directed to the client Responsible Party in the first instance. Smile ID will identify the relevant client and facilitate the process. Where the client has given Smile ID authority to respond directly, Smile ID will do so. Contact dpo@usesmileid.com for assistance in identifying the correct Responsible Party.

E.3 Special Personal Information

Smile ID processes biometric information (facial geometry) as its primary product function. Biometric information is special personal information under section 26(1)(b) of POPIA. Data subject requests relating to biometric data are subject to enhanced identity verification (see Part C.3) and are processed jointly with the relevant client Responsible Party where Smile ID acts as Operator. Data subjects may request human review of any automated verification outcome by contacting dpo@usesmileid.com.

Part F: Remedies and Supervisory Authorities

F.1 Internal Review

There is no formal internal appeal mechanism beyond the initial Information Officer decision. A data subject or requester who is dissatisfied with a decision may request that the Information Officer conduct a personal review of the matter by submitting a written request to dpo@usesmileid.com within 30 days of receiving the decision. The Information Officer will acknowledge within 3 business days and complete the review within 30 days.

F.2 Information Regulator — PAIA and POPIA Complaints

Any person who is dissatisfied with Smile ID's response to a PAIA access request, or who believes that Smile ID has interfered with their rights under POPIA, may lodge a complaint with the Information Regulator. The right to lodge a complaint exists independently of any internal review and may be exercised without exhausting internal remedies.

Information Regulator (South Africa)

Physical address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
Email: inforeg@justice.gov.za
PAIA enquiries: POPIAComplaints@inforegulator.org.za
Website: www.inforegulator.org.za
Telephone: +27 (0)10 023 5200
eServices Portal (breach reporting): <https://eservices.inforegulator.org.za>

F.3 High Court

Where access to a record has been refused or not provided within the required timeframe, a requester may apply to the High Court of South Africa for relief in terms of section 78 of PAIA. Applications must be made within 30 days of receiving notice of refusal. The court may, on application, make any order that is just and equitable, including ordering Smile ID to disclose the record.

F.4 Other Supervisory Authorities — International Data Subjects

Smile ID processes personal information of data subjects across Africa and internationally. The following supervisory authorities are relevant to data subjects in other jurisdictions:

Jurisdiction	Supervisory authority and contact
European Union / EEA (GDPR)	Lead supervisory authority at Smile ID's EU establishment, or local DPA of data subject — see edpb.europa.eu
United Kingdom (UK GDPR)	Information Commissioner's Office (ICO) — www.ico.org.uk
Nigeria (NDPA)	Nigeria Data Protection Commission (NDPC) — www.ndpc.gov.ng
Kenya (Data Protection Act 2019)	Office of the Data Protection Commissioner (ODPC) — www.odpc.go.ke
Ghana (Data Protection Act 2012)	Data Protection Commission — www.dataprotection.org.gh

**Uganda (Data Protection Act
2019)**

Personal Data Protection Office — www.pdpo.go.ug

Part G: Security Compromises and Breach Notification

In the event of a security compromise (data breach) that poses a real risk of harm to affected data subjects, Smile ID will:

- **Notify the Information Regulator** via the eServices Portal (mandatory since April 2025) as soon as reasonably possible after becoming aware of the compromise (section 22 of POPIA);
- **Notify affected data subjects directly** where the Regulator determines notification is required or where the risk of harm warrants direct notice;
- **Document the compromise** in Smile ID's Security Compromise Register and conduct a post-incident review;
- **Provide information** to data subjects about the nature of the compromise, the categories of data affected, and the steps taken to mitigate harm.

Smile ID's Security Compromise Response Procedure is maintained internally and available to the Information Regulator upon request. To report a suspected compromise involving your personal information, contact security@usesmileid.com.

Part H: Availability, Related Documents, and Document Control

H.1 Availability of This Manual

This Manual is available:

- Online at www.smile.id/paia-manual — available at any time, free of charge;
- On request to the Information Officer at dpo@usesmileid.com — provided free of charge within 5 business days;
- In physical copy at Smile ID's South African office — by appointment;
- In all 11 official languages, on request, the Information Officer will arrange translation where feasible.

H.2 Related Documents

The following Smile ID documents should be read together with this Manual:

Document	Location / Reference
Privacy Policy	www.smile.id/privacy-policy SID-ZA-PP-001
Cookie Policy	www.smile.id/cookie-policy SID-ZA-CP-001
Data Retention Policy	Available on request SID-ZA-DRDP-001
POPIA Compliance Framework	Internal SID-ZA-POPIA-CF-001
Data Subject Rights Policy	Available on request SID-ZA-DSRP-001
Information Security Policy	Internal SID-ZA-ISP-001
Data Subject Rights Request Form	www.smile.id/dsr-request-form
SAHRC Guide on PAIA	www.sahrc.org.za (all official languages)

H.3 Document Control

Attribute	Detail
Version	1.0
Effective date	1 July 2025
Next review date	30 June 2026 (or earlier on material regulatory or operational change)
Approved by	Information Officer, Smile Identity
Document owner	Information Officer

Sign-off	Name	Signature / Date
Information Officer	Mark Straub	<i>Mark Straub</i> / 25 June 2026
Chief Executive Officer	Mark Straub	<i>Mark Straub</i> / 25 June 2026

Director, Regulatory & Governmental Affairs	Kasim Sodangi	<i>Kasim Sodangi/1 July 2025</i>
---	---------------	----------------------------------