



TERMS & CONDITIONS

These Terms and Conditions were last updated on 2026-06-05.

1. CUSTOMER ACKNOWLEDGMENT

THIS SAAS AGREEMENT AND THE DATA PROCESSING AGREEMENT CONTAIN IMPORTANT INFORMATION ABOUT TERMS, CONDITIONS, RIGHTS AND OBLIGATIONS, AS WELL AS LIMITATIONS AND EXCLUSIONS OF PARTIES. BY CLICKING OR SIGNING THIS AGREEMENT, THE CUSTOMER IS CONSENTING TO BE BOUND BY AND IS BECOMING A PARTY TO THESE AGREEMENTS. THE CUSTOMER'S AUTHORISED REPRESENTATIVE REPRESENTS THAT HE/SHE IS DULY AUTHORISED TO COMMIT THE CUSTOMER TO THE TERMS AND CONDITIONS OF THE AGREEMENTS AND TO SIGN THE AGREEMENTS ON BEHALF OF THE CUSTOMER.

2. SAAS IMPLEMENTATION SERVICE

- 2.1. Smile ID will use commercially reasonable efforts to provide Customer the services described in the section SAAS SERVICES AND SUPPORT SERVICES.
- 2.2. The Service is offered subject to the terms of this Agreement, the Data Processing Agreement (DPA) and as may be contained in the Order Form(s).
- 2.3. The headings in this Agreement are for convenience only and shall not affect their interpretation.
- 2.4. In the interpretation of this Agreement, the *contra proferentem* rule of construction shall not apply (this Agreement being the product of negotiations between the Parties), nor shall this Agreement be construed in favour of, or against, either Party by reason of the extent to which either Party or its professional advisers participated in the preparation of this Agreement.

3. DEFINITIONS

- 3.1. **"Affiliate"** means, with respect to a Party, any entity or individual that directly or indirectly controls, is controlled by, is under common control with, or is otherwise contractually engaged by such Party in a manner that supports shared commercial, operational, or technological objectives relevant to this Agreement;

3.2. **"Authentication" or " Biometric Authentication"** is defined as the process or action whereby Smile ID attempts to verify biometric data, from or of, a User, against data captured at the time of Registration and may include:

- a. Proof of Liveness Check during Authentication.
- b. Compare Incoming Selfie to Registered Selfie and human review as needed

This service is designed to function as part of a multi-factor authentication framework and should not be used as a standalone method for user authentication. Customers are advised to implement their service accordingly"

3.3. **"Documentation"** means the specifications, user manuals and training materials or any other documentation that Smile ID makes generally available to all Customers relating to the use and operation of the Service.

3.4. **"Equipment"** means including, but not limited to, modems, hardware, servers, software, operating systems, networking, and web servers.

3.5. **"Human Review"** is the process or action whereby a human reviews or determines the result of a Registration or Verification, whether done manually by the human or otherwise.

3.6. **"ID Issuing Authority"** is defined as the Government or third-party authority or database which issues the identity card or identity credentials to a User in the country of operation.

3.7. **"Party"** refers to either Smile ID or the Customer in this agreement; both are jointly referred to as "Parties" in the Agreement.

3.8. **"Proof of Liveness Check"** is an anti-spoofing (anti-presentation attack) measure built into the Smile ID solution meant to identify whether the face submitted for authentication is real and the face is live.

3.9. **"Registration" or "User Registration"** are defined as a User who has been successfully registered into the Smile ID system.

3.10. **"Risk Intelligence Signals"** means algorithmic or rule-based indicators derived from previous Verifications, metadata from Users and Customers and other behavioural analytics, used to enhance the speed, security and continuity of subsequent Verifications and Services.

3.11. **"Services"** is defined as the usage of the Smile Identity (Smile ID) Platform, as available, to execute any or all the following ("Service(s)"):

- a. Authentication or Biometric Authentication
- b. Proof of Liveness Checks during Authentication.

- c. Verify the User ID number to the ID Issuing Authority and return of User Personal Information.
 - d. Face Matching - Matching of Selfie to the photo on file at the ID Issuing Authority, when available, with algorithmic confidence scores and human review as needed or comparison to a photo of the ID card provided by the User, when required.
- 3.12. **"Smile ID Terms"** means collectively, the SaaS Agreement, the Smile ID Data Processing Agreement, the Smile ID Privacy Policy, the Smile ID Usage Policy, the Smile ID Data Retention Policy and any other supplemental terms or guidelines governing use of the Services. Smile ID may update its Privacy Policy, Usage Policy, Data Retention Policy or other supplemental terms from time to time by posting the revised version at <https://smile.id> and such updates will become effective upon posting.
- 3.13. **"Customer"** means a corporate entity, company, or other legal entity with whom Smile ID enters into the Agreement and for whom Smile ID has agreed to provide the Services in accordance with these Terms. This includes a representative, employee, director, consultant, customer, client, or contracted third party of the Customer who is utilising the Smile ID Services.
- 3.14. **"User"** means a customer or client of the "Customer" who is utilising the Services.
- 3.15. **"Order Form"** means each fully executed Smile ID order form that incorporates the Smile ID Terms and forms part of the Agreement, and that specifies the Services, fees, payment terms, subscription duration, and other commercial details agreed by the parties. In the event of any conflict between an Order Form and other Smile ID Terms, (i) the Order Form shall prevail with respect to the Services described therein and all commercial terms (including fees, payments, and duration); and (ii) or all other matters, the Smile ID Terms shall prevail.
- 3.16. **"Version 2 (V2) APIs"** means Smile's legacy APIs providing standard responses.
- 3.17. **"Version 3 (V3) APIs"** means Smile's newest APIs providing Smile's Risk Intelligence response and scores.

The version of the Services applicable to the Customer shall be determined by the version of the SDK implemented by the Customer or by the integration method specified in the applicable Order Form or as enabled within the Smile ID platform.

4. TERMS & CONDITIONS.

4.1. SaaS Services

4.1.1. These terms and conditions govern the Customer's access to and the use of Smile ID's website and all services offered by Smile ID. Customer access to the Service is conditioned on acceptance of and compliance with these Terms.

4.1.2. Smile ID offers multiple API integration pathways, including legacy and enhanced configurations.

The enhanced V3 APIs incorporate Risk Intelligence Signals, adaptive risk modelling and expanded security telemetry. Smile ID designates the V3 APIs as its highest recommended security configuration.

4.1.3. With V3 APIs, Smile ID may optimize verification processes by reusing previously verified attributes and consented security signals for fraud-prevention and risk-mitigation purposes. Such optimisation is intended to enhance efficiency, reduce user friction and minimise redundant verification steps across lawful service contexts.

4.1.4. Optimised verification results are explicitly labelled and will include data freshness indicators. Customers on Version 3 (v3) APIs retain the option to request live verification results. Users who disagree with the outcome of a Verification reserve the right to request the re-verification, correction, or revocation of these results by contacting compliance@usesmileid.com.

4.1.5. The Service is offered subject to the terms of the ID Issuing Authorities and third-party providers (as set out in the [SMILE ID DATA PROCESSING AGREEMENT](#)) that may be utilised in the delivery of the Service and subject to acceptance of all the terms and conditions contained in these Terms and all other operating rules, policies, and procedures that may be published on the website by the Company, which are incorporated by reference, including operating rules, policies, and procedures of third-party service providers to the website that are referenced herein. These Terms apply to every User of the Service.

4.1.6. Fraud prevention constitutes a shared operational responsibility. Therefore, Customer agrees to implement enhanced Verification layers, including multi-factor authentication and behavioural safeguards where appropriate, in coordination with the security signals provided by the Services. Failure to implement

proportionate Verification controls may materially increase fraud exposure.


- 4.1.7. Customer is solely responsible for compliance with any and all laws, rules, regulations, and tax obligations that may apply to the use of the Services.

4.2. **Support Services**

- 4.2.1. Smile ID will provide a simulated server to facilitate SDK integration and testing prior to Customer integrating the Smile Identity API calls into Customer's private server.
- 4.2.2. As part of the registration process, Customer will create administrative usernames and passwords for Customer's Smile ID account. Smile ID reserves the right to refuse registration of or cancel passwords it deems inappropriate or insecure.
- 4.2.3. Smile ID will provide Customer access to an API to download images and associated Personal Data ("Customer Data") generated by any implementations of the Smile Platform.
- 4.2.4. Smile ID may choose to change support contacts or support communication methods over time, provided Smile ID gives Customer at least five (5) calendar days' notice prior to a change in customer support contact or communication method.
- 4.2.5. Smile ID may use a human/manual review process in provisioning the service under this agreement. Smile ID will use its best effort to complete a single manual review within three (3) minutes.
- 4.2.6. Smile ID may utilize machine learning models, AI-based systems, and statistical analysis of Customer and User activity to identify patterns and trends indicative of fraud or cybersecurity threats. Such processing may involve profiling and automated decision-making, in accordance with applicable data protection laws. Where necessary, Smile ID shall implement appropriate safeguards, including the right of human intervention.

5. **RESTRICTIONS AND RESPONSIBILITIES**

- 5.1.1. Customer will not, directly or indirectly: reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas, know-how or algorithms relevant to the Services or any software, documentation or data related to the Services ("Software"); modify,



translate, or create derivative works based on the Services or any Software (except to the extent expressly permitted by Smile ID or authorised within the Services).

- 5.1.2. For the avoidance of doubt, “derivative works” are defined as any revisions, alterations, translations, or expansions of the Services or any other form in which Services or Documentation are transferred or adapted.
- 5.1.3. Customer will also not use the Services or any Software for time-sharing or service bureau purposes or otherwise for the benefit of a third party without the express approval of Smile ID; or remove any proprietary notices or labels.
- 5.1.4. With respect to any Software that is distributed or provided to Customer by Smile ID for use on Customer premises or devices, Smile ID hereby grants Customer a non-exclusive, non-transferable, non-sublicensable licence to use such Software during the term of the Agreement only in connection with the Services.
- 5.1.5. Further, Customer may not remove or export from the country of operation or allow the export or re-export of the Services, Software or anything related thereto, or any direct product thereof in violation of any restrictions, laws or regulations of the country of operation or without the prior written approval of Smile ID.
- 5.1.6. Customer warrants that it possesses the requisite licence, permits, authorizations, and regulations to perform its obligations under these Terms.
- 5.1.7. Customer represents, covenants, and warrants that Customer will use the services only in compliance with the [Smile ID Standard User Usage Policy](#) and all applicable local laws and regulations.
- 5.1.8. Customer represents and warrants that the person agreeing to the terms and conditions of this Agreement has been duly authorised to do so and has the power and capacity to bind the Customer.
- 5.1.9. Customer represents and warrants that the entry into and performance of these Terms will not:
 - (i) result in a breach or violate any instrument, judgement/law or decree of any court or governmental agency to which the Customer is a party to or by which it is bound;
 - (ii) result in or constitute a breach or default of any other instrument to which the Customer is bound; and/or

(iii) conflict with, result in a breach of, constitute a default under, or accelerate performance under the terms of any contract, agreement or deed to which the Customer may be bound or affected;

5.1.10. Customer shall be responsible for obtaining and maintaining any Equipment and ancillary services needed to connect to, access or otherwise use the Services. Customer shall also be responsible for maintaining the security of the Equipment, Customer account, passwords (including but not limited to administrative and Customer passwords) and files, and for all uses of Customer account or the Equipment with or without Customer's knowledge or consent.

5.1.11. Customer agrees to and is bound by the Smile ID Terms.

5.1.12. Customer grants Smile ID permission to use the Customer's name and logo in marketing materials of Smile ID.

5.1.13. Smile ID grants Customer permission to use Smile ID's name and logo in Customer's marketing materials. However, Smile ID reserves the right to request the immediate removal of its name and logo from any marketing material that Smile ID at its sole discretion deems inappropriate or misleading.

5.1.14. Customer represents and warrants that it has accurately disclosed the specific use case for which the Services are being utilized. In the event that the Customer fails to state the correct use case, or fails to provide Smile ID with prior written notice of any additional use case, change, or modification to the originally disclosed use case, Smile ID shall not be liable for any damages, losses, or regulatory non-compliance arising from such unauthorized use. Furthermore, Smile ID reserves the right to immediately suspend or terminate the Services if it determines, at its sole discretion, that the Customer's use of the Services deviates from the disclosed use case without prior authorization.

5.2. **Prohibited Activities**

5.2.1. Customer shall not utilize the website or the Services in connection with any transaction that is illegal or involves any illegal items, or is for any illegal purpose.

5.2.2. Smile ID may close, suspend, or limit your access to the website or services or refuse to complete a transaction that Smile ID has reason to believe is unauthorized or may violate any law, rule or regulation. Smile ID shall subsequently notify Customer of its


actions within twenty-four hours (24) of taking such action.

6. CONFIDENTIALITY AND PROPRIETARY RIGHTS

- 6.1. Parties understand that the other Party has disclosed or may disclose business, technical or financial information relating to the Party's business (hereinafter referred to as "Proprietary Information"). Proprietary Information of Smile ID includes non-public information regarding features, functionality and performance of the Service as well as all pricing and payment terms provided to the Customer. Proprietary Information of Customer includes non-public data and non-public information regarding features, functionality, performance and business information of Customer systems/platforms provided by Customer to Smile ID to enable the provision of the Services ("Customer Data"). The Party that receives such information (the "Receiving Party") agrees to take reasonable precautions to protect such Proprietary Information. The Party that shares the information (the "Disclosing Party") agrees that the foregoing shall not apply with respect to Proprietary Information that:
 - 6.1.1. is or becomes generally available to the public; or
 - 6.1.2. was in the Receiving Party's possession or known by it prior to receipt from the Disclosing Party; or
 - 6.1.3. was rightfully disclosed to the Receiving Party without restriction by a third party; or
 - 6.1.4. was independently developed without use of any Proprietary Information of the Disclosing Party; or
 - 6.1.5. is required to be disclosed by law.
- 6.2. Customer shall retain access to all Customer Data. As Smile ID shall own and retain the right to:
 - 6.2.1. the Services and Software, improvements, enhancements or modifications thereto,
 - 6.2.2. other technology developed by Smile ID in connection with Implementation Services, Services or support, and
 - 6.2.3. all intellectual property rights related to any of the foregoing. These rights will not include intellectual property developed by the Customer to implement Smile ID Services.


7. CUSTOMER DATA/ DATA ANALYTICS

- 7.1. Customer consents, agrees and warrants that Smile ID will be authorised, free and able (during and after the term of the Agreement) to:

- 
- 7.1.1. use such information and data, including Customer Data and data provided by Users, to improve and enhance the Services and for other development, diagnostic and corrective purposes in connection with the Services and other Smile ID offerings; and
 - 7.1.2. disclose such data solely in aggregate, encrypted or other de-identified form in connection with its business and with its Affiliates' business, provided that Smile ID shall be responsible for any misuse of that information and data.
 - 7.2. By using the Service, Customer acknowledges and agrees that Smile ID may carry out further processing activities aimed at ensuring the security and integrity of its Services, and may use aggregated and anonymized data for the improvement of its identity fraud detection and cybersecurity systems.
 - 7.3. Customer acknowledges that Smile ID may generate Risk Intelligence Signals derived from Customer Data and User data. For Customers using Version 3 (v3) APIs, these signals enhance fraud detection through the analysis of historical patterns and expedite Verifications for returning Users. By using the Services, Users consent and agree to their data being processed for these purposes.
 - 7.4. Smile ID maintains a multi-layered human review process to address high-uncertainty events where algorithmic confidence scores fall below pre-defined security thresholds. Smile ID shall conduct periodic integrity audits to identify and resolve potential algorithmic biases and gaps.

8. ORDERS AND PAYMENT (FEES)

- 8.1. Customer will pay the applicable fees as agreed in accordance with the terms therein indicated as Service Fees (the "Fees"). Customer may be invoiced for such usage, and the Customer agrees to pay Fees in the manner provided by Smile ID.
- 8.2. Invoices will be raised using the Customer's usage data from the Smile ID portal for each month. The Customer acknowledges that this usage data is definitive and takes precedence over any other sources. Customers are advised to reconcile their portal usage data at least fourteen (14) calendar days before the invoice payment is due. Where no dispute is raised, the Customer will be deemed to have accepted the accuracy of the Smile ID portal data for invoicing.
- 8.3. Fees are exclusive of taxes, and the Customer shall be responsible for all taxes (sales tax, use tax, GST, value-added tax, withholding, duties, levies,

- 
- etc.) that are applicable to or result from the User's purchase or use of the Services.
- 8.4. For local currency payments, Smile ID will use the prevailing official exchange rate provided by the central bank of the applicable country of operation accordingly.
 - 8.5. Smile ID reserves the sole right to change prices for the service provided that the Customer is issued fifteen (15) calendar days' notice of any such changes in advance.
 - 8.6. Pay-As-You-Go Customers shall pre-fund wallets to the value of the Services to be consumed.
 - 8.7. Except as otherwise expressly set forth in this Agreement, all Fees are non-refundable and are not subject to deduction or set off.

9. TERM AND TERMINATION

- 9.1. This Agreement is valid for three (3) years (calculated with effect from the Effective Date) and shall be automatically renewed for additional periods of the same duration unless:
 - 9.1.1. either party request's termination at least thirty (30) calendar days prior to the end of the then-current term.
 - 9.1.2. the Service is unused for ninety (90) calendar days, in which case the agreement shall be deemed terminated.
- 9.2. This Agreement may be terminated immediately with two (2) calendar days' notice in the event of:
 - a. non-payment;
 - b. material breach of this Agreement;
 - c. insolvency/bankruptcy of either Party;
 - d. the passing of a resolution to wind up either Party;
 - e. the appointment of an administrator or receiver;
 - f. the loss of the licence of either Party;
 - g. if required by applicable law or the relevant governing authority or competent authority;
 - h. if Smile ID, at its sole discretion, determines that not terminating would be harmful to Smile ID's business, goodwill or reputation.
- 9.3. Customer will pay in full for the services up to and including the last day on which the Services are provided. All sections of this Agreement will

survive this Agreement for two (2) years after termination, including, without limitation, accrued rights to payment, confidentiality obligations, warranty disclaimers, and limitations of liability.

- 9.4. In the case where the Customer subscribes for another service being provided by Smile ID, and the payment for the service is not currently covered by the existing Order Forms, Smile ID, at its discretion, reserves the right to call for and Customer agrees to execute a new Order Form to cover such services.
- 9.5. Upon any termination or expiration hereof, Customer will immediately cease access to and use of the service and delete (or, at Smile ID's request, return) any and all copies of the Documentation and any other Smile ID's Proprietary Information. Following termination or expiration of this Agreement, Smile ID may delete any data stored by Smile ID at any time.

10. WARRANTIES

- 10.1. Customer warrants that explicit consent shall be sought, received and documented from the User in accordance with the [Smile ID Data Processing Agreement](#) and the [Smile ID Standard User Usage Policy](#) before processing of personal data.
- 10.2. Customer hereby warrants and agrees that the Services will be utilized as a secondary factor within a multi-factor authentication framework. Customer acknowledges that the Services are not intended to be used as a standalone method or primary login solution and must be used alongside the Customer's internal KYB/KYC protocols and regulatory procedures.
- 10.3. Smile ID's Risk Intelligence Signals and verification results are advisory indicators of risk and do not constitute a full and final determination of user's eligibility for Customer's products or services. Customers shall remain the ultimate and final decision maker within their platforms.
- 10.4. Smile ID shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimises errors and interruptions in the Services. The Parties hereby acknowledge that industry standards in the context of the Services are non-static and may require the adoption of frontier technologies.
- 10.5. Smile ID shall perform its duties in a professional and workmanlike manner. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Smile ID or by third-party providers, or because of other causes beyond Smile

ID's reasonable control, but Smile ID shall use reasonable efforts to provide not less than seven (7) calendar days advance notice in writing or by e-mail of any scheduled service disruption.

- 10.6. SMILE ID DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, NOR DOES SMILE ID MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE SERVICES AND IMPLEMENTATION SERVICES ARE PROVIDED "AS IS."
- 10.7. WHILE Risk Intelligence Signals ARE OPTIMIZED FOR SECURITY AND IN COMBATING INCREASINGLY SOPHISTICATED FRAUD AND CYBERSECURITY ATTACKS, SMILE ID, TO THE MAXIMUM EXTENT PERMITTED BY LAW, MAKES NO GUARANTEES THAT THE SERVICES WILL BE ERROR-FREE.
- 10.8. SMILE ID DOES NOT GUARANTEE THE RECENCY OF Risk Intelligence Signals FOR UNRELATED PURPOSES, SUCH AS SECONDARY REGULATORY REPORTING OR NON-SECURITY-RELATED ACCOUNT UPDATES.

11. SECURITY

- 11.1. Smile ID implements and maintains commercially reasonable administrative, technical and organisational safeguards designed to protect the integrity, confidentiality and availability of the Services and associated data.
- 11.2. Customer acknowledges that fraud prevention and identity verification operate within an evolving threat environment. Accordingly, the Services constitute an adaptive security infrastructure that learns, adapts and improves over time in response to emerging risks and technological developments. Smile ID may refine analytical methodologies, risk models, Verification logic and related security mechanisms without requiring amendment to these Terms, provided the core functionality of the Services is materially maintained.
- 11.3. Smile ID may implement technological enhancements or shifts necessary to maintain industry-aligned protection standards and shall provide reasonable notice where such changes materially affect Customer's integration or operational processes.
- 11.4. Smile ID will use available technology, where appropriate, to protect the security of communications made as it offers the Services.
- 11.5. Notwithstanding the above, Smile ID does not accept liability for security, authenticity, integrity or confidentiality of any transactions and other communications made through their Service, provided that such liability is not borne out of negligence or omission on the part of Smile ID.

- 11.6. Customer is aware that internet connections may be susceptible to interference or interception by third parties. Despite its best efforts, Smile ID makes no warranties that the services it offers are free from interference and unlawful use.
- 11.7. Customer should take appropriate steps to keep information and any data in its possession as well as equipment secure.

12. INDEMNITY AND LIMITATION OF LIABILITY

- 12.1. Customer hereby agrees to indemnify and hold harmless Smile ID against any damages, losses, liabilities, settlements and expenses (including without limitation costs and attorneys' fees) in connection with any claim or action that arises from an alleged violation of the foregoing or otherwise from Customer's use of Services provided that same is not as a result of any negligence, default or breach on the part of Smile ID. Although Smile ID has no obligation to monitor Customer's use of the Services, Smile ID may do so and may prohibit any use of the Services it believes may be in violation of the foregoing.
- 12.2. Customer acknowledges that legacy integration pathways may not incorporate the most current fraud-mitigation methodologies, Risk Intelligence Signals or adaptive security enhancements.
- 12.3. Customers who elect to remain on Version 2 (v2) APIs acknowledge that such technology may not incorporate the latest advancements, including but not limited to liveness detection, anti-spoofing or generative AI/deepfake mitigation. Customer acknowledges that the continued use of legacy versions constitutes a waiver of any claim against Smile ID regarding the technical sufficiency of those versions against evolving fraud techniques.
- 12.4. Customer acknowledges that the V3 APIs utilise advanced risk scoring, automated signal generation and adaptive fraud-detection methodologies. Security signals may trigger automated actions within Customer systems, including step-up Verification, temporary restriction, or transaction denial.
- 12.5. Customer remains solely responsible for configuring, overseeing and validating any automated decisioning implemented within its own systems and for applying appropriate human oversight where required by law or internal policy.
- 12.6. Customer shall indemnify Smile ID against claims arising from Customer's reliance on automated outputs, failure to maintain independent human

oversight, or any adverse actions taken against end-users based on such signals.

- 12.7. Smile ID's liability to the Customer shall not exceed the amounts paid to Smile ID by the Customer under this Agreement during the twelve (12) month period immediately preceding the date a Party notifies the other of the claim. This limitation applies to all causes of action, including without limitation any action for breach of contract, breach of warranty, negligence, strict liability, misrepresentation and other tort.
- 12.8. SMILE ID SHALL HOLD CUSTOMER HARMLESS FROM LIABILITY TO THIRD PARTIES RESULTING FROM INFRINGEMENT BY THE SERVICE OF ANY REGISTERED PATENT IN THE COUNTRY OF OPERATION OR ANY COPYRIGHT OR MISAPPROPRIATION OF ANY TRADE SECRET, PROVIDED SMILE ID IS PROMPTLY NOTIFIED OF ANY AND ALL THREATS, CLAIMS AND PROCEEDINGS RELATED THERETO AND GIVEN REASONABLE ASSISTANCE AND THE OPPORTUNITY TO ASSUME SOLE CONTROL OVER DEFENCE AND SETTLEMENT; SMILE ID WILL NOT BE RESPONSIBLE FOR ANY SETTLEMENT IT DOES NOT APPROVE IN WRITING.

13. GENERAL PROVISIONS

13.1. Force Majeure

- 13.1.1. A Party hereof shall not be liable to the other for any delay or failure to perform its obligations under this Agreement if the delay or failure is due to causes beyond its reasonable control, including but not limited to acts of God, civil unrest, epidemics, pandemics, insurrection or civil disorder, war or military operations, national or local emergency, acts or omissions of government, or other competent authority, temporary or permanent disruptions, shutdowns or service failures or availability by ID Issuing Authorities, industrial disputes of any kind (whether or not involving the party's employees), fire, lightning, explosion, flood, subsidence, weather of exceptional severity, acts or omissions of persons for whom the Party is not responsible, or any other cause whether similar or dissimilar outside the Party's reasonable control.

13.2. Severability

- 13.2.1. If any provision of this Agreement is found to be unenforceable or invalid in whole or in part, that provision will be limited or eliminated to the minimum extent necessary so that this

Agreement will otherwise remain in full force and effect and enforceable.

13.3. Entire Agreement

13.3.1. This Agreement together with its schedules, annexures, Data Processing Agreement, and executed order form(s), contains the entire agreement between the Parties, and there are no other representations, promises or conditions, provided that nothing in this clause shall limit either Party's liability for fraudulent misrepresentation.

13.3.2. This Agreement is the complete and exclusive statement of the mutual understanding of the Parties and supersedes and cancels all previous written and oral agreements, communications and other understandings relating to the subject of this Agreement.

13.4. Assignment and Transfer

13.4.1. This Agreement is not assignable, transferrable or sub-licensable by either Party except with the other Party's prior written consent.

13.5. Variation

13.5.1. Smile ID reserves the right to change the terms under which the Services are offered. The most current version of the Smile ID Terms will supersede all previous versions. Smile ID will communicate any such changes in advance. However, Smile ID also encourages you to periodically review the terms to stay informed of updates.

13.6. Notices

13.6.1. All notices under this Agreement will be in writing and addressed to the other Party at such address as may at the relevant time have been notified pursuant to this provision to the Party giving the notice. Any such notice will be deemed to have been duly given:

- a. When the sender receives an automated delivery receipt from the recipient's mail server, or where no automated delivery failure message is received if transmitted by email;
- b. This amendment clarifies that confirmation that an email did not bounce back will be sufficient to consider notice duly served, regardless of whether the recipient provides an express receipt
- c. if sent by certified or registered mail, seven (7) calendar days after posting and proof that the envelope containing the notice of communication was properly addressed,

prepaid and registered, and a receipt to that effect shall be sufficient evidence that notice or communication has been duly served.

13.7. **Dispute Resolution**


- 13.7.1. Any dispute, controversy, difference, claim or question which may arise at any time between the parties touching upon the construction of this Agreement, on their respective rights and liabilities with respect hereto or otherwise arising in respect of matters the subject of this Agreement parties shall be dealt with amicably.
- 13.7.2. Any disputes arising under or in connection with the validity, interpretation and performance of the Terms between Smile ID, Customer or/and any third parties that cannot be resolved amicably by the parties through negotiation within thirty (30) calendar days shall be resolved by arbitration.
- 13.7.3. Where the Services are delivered in only one territory, the forum shall be any arbitration panel/tribunal or center established under applicable law (the "Domestic Tribunal"), and the rules of the Domestic Tribunal shall apply. The seat of arbitration shall be the territory in which the services are delivered. The number of arbitrators shall be one. The arbitrator shall be appointed by the Domestic Tribunal.
- 13.7.4. Where the Services are delivered in multiple territories, the dispute shall be resolved by the London Court of International Arbitration (LCIA) in accordance with the LCIA Rules and the seat of arbitration shall be London. The number of arbitrators shall be one. The arbitrator shall be appointed by the LCIA.

13.8. **Governing Law**

- 13.8.1. This Agreement shall be governed by the laws of the territory where the Service is delivered; however, where the Service is delivered in multiple territories, the laws of England and Wales shall apply.

13.9. **Miscellaneous**

- 13.9.1. No failure or delay by either party in exercising any of its rights under this Agreement shall be deemed to be a waiver of that right, and no waiver by either party of any breach of this Agreement by the other party shall be considered as a waiver of any subsequent breach of the same or any other provision.

- 
- 13.9.2. No agency or joint venture, franchise or employment is created as a result of this Agreement, and either party has no authority to bind the other Party in any respect whatsoever.
- 13.9.3. Except as otherwise set forth herein, no supplement, modification, or amendment of this Agreement will be binding unless accepted by each Party. Notwithstanding the foregoing, Smile ID may unilaterally vary terms where: (a) required to comply with Applicable Data Protection Laws; (b) necessary to implement enhanced security and fraud prevention protocols; (c) required by an ID Authority or other supervisory authority; or (d) where otherwise required for the performance of the Services. Customers shall be notified of any such changes.



DATA PROCESSING AGREEMENT


This Data Processing Agreement was last updated on 2026-06-05.


1. SUMMARY

Data security, protection and privacy are mission critical to our business. Our data protection policies spell out what we do with the information we collect from you when you visit our website or sign up for our service, and how we manage that information.

2. DEFINITIONS


- 2.1. **"Affiliate"** means, with respect to a Party, any entity or individual that directly or indirectly controls, is controlled by, is under common control with, or is otherwise contractually engaged by such Party in a manner that supports shared commercial, operational, or technological objectives relevant to this Agreement;
- 2.2. **"Applicable Law"** means any national, supranational, regional or local government or governmental, administrative, statute, law (including common law), regulation, rule, ruling, order, writ, injunction, decree or guidelines issued by any authority in the Territory;
- 2.3. **"Applicable Data Protection Laws"** means all data protection and privacy laws applicable to the processing of Personal Data under this Agreement, including but not limited to: (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("the GDPR"); (ii) the Data Protection Act, 2012 (Act 843) of Ghana; (iii) the Data Protection Act, 2019 of Kenya; (iv) the Nigeria Data Protection Act, 2023; (v) the Protection of Personal Information Act, 2013 of South Africa ("POPIA"); and any other relevant national or regional data protection laws or regulations. Any reference to such laws shall include all amendments, updates, consolidations, re-enactments or replacements thereof from time to time.
- 2.4. **"Business Purposes"** means Smile ID's Services and internal operational purposes, including identity verification, prevention of cybersecurity threats, identity fraud detection, identity fraud monitoring, research and development related to the Services, and any related or ancillary activities that are reasonably necessary and proportionate to achieve those purposes, or are otherwise compatible with the context in which the Personal Data was collected, or as otherwise permitted by Applicable Data Protection Laws;

- 
- 2.5. **“Consent”** means agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject’s wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of their Personal Data;
- 2.6. **“Controller”** shall have the meaning set out in the GDPR or Applicable Data Protection Laws;
- 2.7. **“Customer”** means a corporate entity, company, or other legal entity with whom Smile ID enters into the Agreement and for whom Smile ID has agreed to provide the Services in accordance with these Terms. This includes a representative, employee, director, consultant, customer, client, or contracted third party of the Customer who is utilising the Smile ID Services;
- 2.8. **“Data Subject”** shall have the meaning set out in the GDPR or Applicable Data Protection Laws and shall for the purposes of this Agreement, include Users as defined below;
- 2.9. **“Data Subject Rights”** means all rights granted to Data Subjects under the GDPR and other Applicable Data Protection Laws, which may include the right of access, the right to data portability, the right to raise complaints, the right to opt-out and the right to rectification or erasure of Personal Data as applicable.
- 2.10. **Fraud Intelligence Signals”** means algorithmic or rule-based indicators derived from previous Verifications, metadata from Users and Customers and other behavioural analytics, used to enhance the speed, security and continuity of subsequent Verifications and Services.
- 2.11. **“Order Form”** means each fully executed Smile ID order form that incorporates these Terms and the SaaS terms (together, the "Agreement") and describes the Services to be provided by Smile ID from time to time as agreed.
- 2.12. **“Party”** refers to either Smile ID or the Customer in this agreement; both are jointly referred to as the “Parties” in the Agreement.
- 2.13. **“Personal Data”** means any information identifying a Data Subject or information relating to a Data Subject. Personal Data specifically includes, but is not limited to: names, addresses or location data, photos, email addresses, bank details, posts on social networking websites, medical information, and other unique identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others;
- 2.14. **“Processing and Process”** shall have the meaning set out in the GDPR or Applicable Data Protection Laws;

- 
- 2.15. **“Personal Data Breach”** shall have the meaning set out in the GDPR or Applicable Data Protection Laws;
 - 2.16. **“Pseudonymisation”** means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure;
 - 2.17. **“Regulatory Authority”** means the regulating and enforcing authority responsible for regulating data protection and privacy of Data Subjects in the territory and as specifically described in the Applicable Data Protection Laws;
 - 2.18. **“Services”** means the data processing, identity-related fraud detection, identity verification services and identity-related fraud monitoring to be provided by Smile ID to the Customer under these Terms; and
 - 2.19. **“User”** means a customer or client of the “Customer” who is utilising the Services.


3. APPOINTMENT, PERSONAL DATA AND PROCESSING

- 3.1. The Customer acknowledges that it is an independent Controller and determines the purposes and means of processing for the Personal Data it collects from Users. The Customer shall remain responsible for its compliance obligations under the Applicable Data Protection Laws, including providing any required notices and obtaining any required consent for processing activities carried out under its instruction.
- 3.2. The Customer hereby appoints Smile ID to provide the Services.
- 3.3. For the purposes of executing specific Customer instructions for real-time verifications, Smile ID acts as a Data Processor.
- 3.4. Smile ID processes Personal Data for the Business Purposes and may utilise machine learning models, AI-based systems, and statistical analysis of User activity to identify patterns and trends indicative of fraud or cybersecurity threats. Such processing may involve profiling and automated decision-making, in accordance with Applicable Data Protection Laws. Where necessary, Smile ID shall implement appropriate safeguards, including the right of human intervention.
- 3.5. To the extent Smile ID processes Personal Data to generate Fraud Intelligence Signals, improve fraud-detection methodologies or enhance system integrity across its customer network, Smile ID acts as an independent Controller for those specific purposes.

- 
- 3.6. Such processing is undertaken for fraud-prevention and security purposes and may rely on legitimate interests and/or contractual necessity as the applicable lawful basis, subject to applicable data protection law. Each party remains responsible for documenting and maintaining its own lawful basis for processing.
 - 3.7. Each Party hereby acknowledges that it is responsible for establishing and documenting its lawful basis for processing under Applicable Data Protection Laws.


4. SMILE ID'S OBLIGATIONS

- 4.1. Smile ID will process the Personal Data in accordance with the Customer's instructions, and only to the extent necessary for the Business Purposes. Smile ID shall not Process the Personal Data in a manner incompatible with those purposes, unless required or permitted by Applicable Data Protection Laws.
- 4.2. Unless otherwise required by law, and in line with Smile ID's [Data Retention Policy](#), Smile ID will retain and securely store Personal Data only for as long as is necessary to fulfil the Business Purpose and, where feasible, shall apply appropriate data minimisation techniques, including Pseudonymisation.
- 4.3. Smile ID shall at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, reproduction, or display of Personal Data in its possession, and against accidental or unlawful loss, destruction, alteration, or damage of such Personal Data.
- 4.4. Smile ID shall implement measures to ensure a level of security appropriate to the risk involved, including as appropriate:
 - 4.4.1. the Pseudonymisation and encryption of Personal Data;
 - 4.4.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - 4.4.3. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
 - 4.4.4. a process for regularly testing, assessing and evaluating the effectiveness of security measures.
- 4.5. Smile ID will ensure that all employees are informed of the confidential nature of the Personal Data and are bound by the necessary confidentiality obligations and use restrictions in respect of the Personal Data.

- 
- 4.6. The obligations under this clause shall survive the termination of the Agreement.

5. THE CUSTOMER'S OBLIGATIONS

- 5.1. The parties understand and acknowledge that Smile ID reaches Users through the Customer and its platforms and thus must rely on the adequacy of Consent which the Customer shall obtain from the User. The Customer shall ensure that, where applicable, it has obtained the requisite Consent (of the Data subject) using a notice or method which contains:
- 5.1.1. an approved data processing notice informing the Data Subject of appointment of Smile ID at the time of collecting the Personal Data;
 - 5.1.2. the purpose for which their Personal Data will be Processed, including notification that the Personal Data may be Processed for the Business Purposes, and their right to opt-out;
 - 5.1.3. information that the Personal Data may be transferred outside the territory of collection for Processing;
 - 5.1.4. information that the Personal Data may be Processed by a third-party controller or processor; and
 - 5.1.5. any other information that, having regard to the specific circumstances of the collection and expected processing, is required to enable fair Processing and performance of the Services.
- 5.2. Additionally, Smile ID may provide a consent screen to be integrated into the Customer's Consent collection mechanisms, or, may request the transmission of a formal record of Consent to verify the adequacy of Consent collected.
- 5.3. Where Smile ID provides a consent screen, the Customer shall not obscure, alter, bypass or otherwise circumvent the consent screen. Any attempt to do so would constitute a material breach of this Agreement and entitle Smile ID to be fully indemnified by the Customer in respect of all costs, claims, damages, expenses, fines or penalties arising from this breach.
- 5.4. Where Smile ID requests the Customer to transmit a formal record of Consent, the Parties hereby acknowledge and agree that the Customer assumes strict liability for the accuracy and lawfulness of such records. Smile ID shall not be held responsible for any false or inaccurate records,



and shall be fully indemnified by the Customer in respect of all costs, claims, damages, expenses, fines or penalties arising from such.


- 5.5. The Customer shall at all times implement appropriate technical, organisational and security measures against unauthorised or unlawful processing and access of Personal Data in its possession.
- 5.6. The obligations under this clause shall survive the termination of the Agreement.


6. OBLIGATIONS OF THE PARTIES

- 6.1. Each Party shall remain responsible for complying with Applicable Data Protection Laws in respect of the Personal Data it controls.
- 6.2. Each Party shall treat all Personal Data and any non-public information shared under this Agreement as confidential and shall not disclose it to any third party except (i) as required by law; (ii) as required for the performance of the Business Purposes; or (iii) with the other Party's prior written consent.
- 6.3. Each Party acknowledges that it is individually responsible for handling Data Subject requests applicable to the data it controls and must put in place mechanisms which allow Data Subjects to exercise their Data Subject Rights. Each Party further acknowledges and agrees that where a request requires cooperation from the other Party, the Parties shall reasonably assist each other in good faith to enable full and timely compliance with individual Data Subject requests, regulatory directives, or other obligations under Applicable Data Protection Laws.
- 6.4. Each Party agrees to promptly notify the other Party if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data held by the other Party or to either Party's compliance with the Applicable Data Protection Laws.
- 6.5. The obligations under this clause shall survive the termination of the Agreement.

7. PERSONAL DATA BREACH

- 7.1. Smile ID will promptly and without undue delay notify the Customer if any Personal Data in its possession is lost or destroyed or becomes damaged, corrupted, or unusable.
- 7.2. Smile ID will immediately and without undue delay notify the Customer if it becomes aware of:

- 
- 7.2.1. any accidental, unauthorised or unlawful processing of the Personal Data; or
 - 7.2.2. any Personal Data Breach.
 - 7.3. Immediately following any Personal Data Breach, the Parties will coordinate with each other to investigate the matter. Smile ID will reasonably cooperate with the Customer in the Customer's handling of the matter, including:
 - 7.3.1. assisting with any investigation;
 - 7.3.2. providing the Customer with access to any facilities and operations affected if necessary;
 - 7.3.3. facilitating interviews with Smile ID's employees, former employees and others involved in the matter;
 - 7.3.4. making available all relevant records, logs, files, data reporting and other materials required to comply with the Applicable Data Protection Laws or as otherwise reasonably required by the Customer; and
 - 7.3.5. taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data Processing.
 - 7.4. The Customer must, to the extent permitted by Applicable Data Protection Laws, obtain the written approval of Smile ID prior to the publication or communication of any filings, communications, notices, press releases or reports related to any Personal Data Breach that expressly mentions Smile ID or its Affiliates. This obligation does not extend to:
 - 7.4.1. disclosures required by law, a court order, or a Regulatory Authority, provided Smile ID is promptly notified, where permissible, and consulted in advance of such disclosure;
 - 7.4.2. internal communications with the Customer's personnel, stakeholders, or professional advisers, insofar as the Customer ensures that such communication is made with the greatest of confidentiality and in good faith; and
 - 7.4.3. communications with affected Data Subjects or Regulatory Authorities, provided that Smile ID or its Affiliates are not referred to by name or clearly identifiable implication.
 - 7.5. The Customer acknowledges and agrees that a violation of the above clause may cause immediate and irreparable harm to Smile ID for which damages may not constitute an adequate remedy and as such, Smile ID



may seek injunctive or other equitable relief for any such violation or incident, in addition to its remedies at law, without proof of actual damages.

8. CROSS-BORDER TRANSFERS OF PERSONAL DATA

- 8.1. The Customer agrees that Smile ID may transfer the Personal Data outside the territory of collection for the purpose of Processing and performance of the Services.
- 8.2. Where the Processing to be carried out by Smile ID includes a transfer to a country which is not recognized by the relevant Regulatory Authority to have adequate level of protection, Smile ID shall ensure that there are appropriate safeguards and that the Personal Data will be protected with the same level of protection as provided under the Applicable Data Protection Laws and this Agreement.
- 8.3. The Customer shall ensure that the Data Subject has provided Consent for the transfer of Personal Data outside the territory of collection, after having been informed:
 - 8.3.1. of the possible risks of such transfers for the Data Subject due to the absence of an adequate level of data protection for the privacy rights of individuals;
 - 8.3.2. that Smile ID shall remain bound by the Applicable Data Protection Laws;
 - 8.3.3. that there are no alternatives; and
 - 8.3.4. that the transfer is necessary for the performance of a contract between the Data Subject and the Customer.

9. SUBCONTRACTORS

- 9.1. Smile ID may only authorise a third-party (subcontractor) to process the Personal Data if:
 - 9.1.1. Smile ID enters into a written contract with the subcontractor that contains terms substantially the same as those set out in these Terms, in particular, in relation to requiring appropriate technical and organisational data security measures; and
 - 9.1.2. Smile ID maintains control over all Personal Data it entrusts to the subcontractor.

10. AUDIT

- 10.1. To the extent permitted by Applicable Law and access protocols, each Party shall, from time to time, permit the other Party and its duly authorised third-party representatives to audit the other Party's compliance with its obligations under these Terms, on at least thirty (30) Business Days' notice. Each Party will give the other Party, and its duly authorised third-party representatives, all necessary assistance to conduct such audits.
- 10.2. The Parties shall cooperate in good faith and provide access limited to such documentation, personnel, and systems that are reasonably necessary to verify compliance with the obligations under this Agreement.
- 10.3. Audits shall be conducted during normal business hours and in a manner that minimises disruption to the Party's operations.
- 10.4. The Parties agree that audits shall be limited to one (1) per calendar year. Nonetheless, additional audits may be conducted in response to data breaches, regulatory inquiries, or substantiated compliance concerns.
- 10.5. All audit-related information shall be treated as confidential information and used solely for compliance purposes.

11. INDEMNIFICATION

- 11.1. The Customer shall indemnify and keep indemnified Smile ID in respect of costs, claims, damages, expenses, fines or penalties arising from losses suffered or incurred by, awarded against or agreed to be paid by Smile ID or any of its sub-contractors arising from or in connection with any:
 - 11.1.1. Non-compliance by the Customer with the Applicable Data Protection Laws;
 - 11.1.2. Processing carried out by Smile ID or any of its sub-contractors pursuant to any Processing instruction from the Customer that infringes any provision of the Applicable Data Protection Laws;
 - 11.1.3. Personal Data Breaches directly attributable to the Customer with regard to the Personal Data it controls; or
 - 11.1.4. Breach by the Customer of its obligations under these Terms.
- 11.2. Smile ID shall indemnify and keep indemnified the Customer in respect of costs, claims, damages, expenses, fines or penalties arising from losses suffered or incurred by or awarded against the Customer arising from or in connection with any:

- 11.2.1. Non-compliance by Smile ID with the Applicable Data Protection Laws;
- 11.2.2. Personal Data Breaches directly attributable to Smile ID or any of its sub-contractors with regard to the Personal Data it controls; or
- 11.2.3. Breach by Smile ID of its obligations under these Terms.

12. GOVERNING LAW

- 12.1. This Agreement shall be governed by the Applicable Law of the Territory where the Service is delivered; however, where the Service is delivered in multiple territories, the laws of England and Wales shall apply.
- 12.2. For questions or more information on our data protection and privacy policies contact us at dpo@usesmileid.com with the subject line: Data Protection.

13. DISPUTE RESOLUTION

- 13.1. Any dispute, controversy, difference, claim or question which may arise at any time between the Parties touching upon the construction of this Agreement, on their respective rights and liabilities with respect hereto or otherwise arising in respect of matters the subject of this Agreement shall be dealt with amicably between the Parties.
- 13.2. Any disputes arising under or in connection with the validity, interpretation and performance of this Agreement between Smile ID, Customer or/and any third parties that cannot be resolved amicably by the Parties through negotiation within thirty (30) calendar days shall be resolved by arbitration.
- 13.3. Where the Services are delivered in only one territory, the forum shall be any arbitration panel/tribunal or centre established under Applicable Law (the "Domestic Tribunal"), and the rules of the Domestic Tribunal shall apply. The seat of arbitration shall be the territory in which the services are delivered. The number of arbitrators shall be one. The arbitrator shall be appointed by the Domestic Tribunal.
- 13.4. Where the Services are delivered in multiple territories, the dispute shall be resolved by the London Court of International Arbitration (LCIA) in accordance with the LCIA Rules and the seat of arbitration shall be London. The number of arbitrators shall be one. The arbitrator shall be appointed by the LCIA.



STANDARD USER USAGE POLICY

This Standard User Usage Policy was last updated on 2026-06-05.

1. SMILE ID USAGE PRINCIPLES

At Smile ID we require our “Customers” (organizations that use our products) to adhere to basic principles of transparency and responsibility.

- 1.1. We believe privacy means people knowing what they are signing up for — in plain language or clear illustrations.
- 1.2. We require that our Customers adhere to local laws around data collection and storage.
- 1.3. We require that our Customers do not collect information on Users who are children or under the age of 16.

2. INFORMED CONSENT

- 2.1. Users of data capture applications powered by Smile ID must be informed about the information that is collected from them and be given an opportunity to provide or withhold consent for that information to be collected.
- 2.2. Users must be provided with a mechanism to withdraw their consent at any time. The procedure for User consent withdrawal should be as straightforward as the consent collection process and should result in the cessation of data processing and deletion of their data, unless retention is required by law.
- 2.3. This includes letting Users know that using the product will involve taking and uploading “selfies” and in some cases, taking photos of identity documents.
- 2.4. Customers must make the Terms and Conditions of any application powered by Smile ID easily available to end users, inside the User’s application, in the predominant local language(s) of the Users. Swahili, Arabic and French have been included as a sample translation due to Smile ID’s operational footprint in East and Francophone Africa . In compliance with our obligations under data protection laws, Smile ID reserves the right to request and review a copy of your current Privacy Policy, or any other terms that contain this information, at any time to ensure alignment. If we determine, in our sole discretion, that your policy does not sufficiently meet our privacy standards or applicable data

protection laws, we may request or provide recommendations for amendment. Continued use of our services may be contingent upon the implementation of these recommendations.

2.4.1. **SAMPLE NOTICE IN ENGLISH**

“By using this product, you consent to Smile Identity Inc, a U.S.-based data controller, and [Customer, a company based in _____], collecting images and device information about you and/or your identity documents for the purpose of identification, authentication and fraud prevention.

Smile ID may securely collect and process your information to detect and prevent identity-related fraud.

When you interact with our systems, we collect the information you provide, as well as metadata, network information like IP addresses, device identifiers, location data from your device which we analyse and use in our fraud detection systems.

This may include the use of artificial intelligence (AI) technologies and automated decision-making systems. These systems may automatically determine the authenticity of identity documents, match biometric features, or help us identify patterns and anomalies. No significant legal decisions will be made without human oversight. Your personal data may be processed by Smile ID for security monitoring, pattern recognition, and to improve verification systems. Smile ID may transfer your data to another territory for processing in accordance with the Data Protection Laws applicable to your information. You retain all your data subject rights, including the right to data portability, rectification, and the right to opt-out of having your information processed in this regard. If you do not consent to the processing of your Personal Data as described above, please refrain from using this product. For more details, you can review Smile ID’s privacy policy at <https://smile.id/privacy-policy>

Smile ID provides support to [Customer] and as such, [Customer] remains the ultimate decision-maker regarding your eligibility for use of its services.”

2.4.2. **SAMPLE NOTICE IN SWAHILI**

“Kwa kutumia bidhaa hii, unakubali kwamba Smile Identity Inc, mdhibiti wa data aliye nchini Marekani, na [Customer, kampuni

iliyoko _____], watakusanya picha pamoja na taarifa za kifaa chako na/au nyaraka zako za utambulisho kwa madhumuni ya utambulisho, uthibitishaji na kuzuia udanganyifu.

Smile ID inaweza kukusanya na kuchakata taarifa zako kwa usalama ili kugundua na kuzuia udanganyifu unaohusiana na utambulisho.

Unapowasiliana na mifumo yetu, tunakusanya taarifa unazotupatia, pamoja na metadata, taarifa za mtandao kama vile anwani za IP, vitambulisho vya kifaa, na data ya eneo [...] kutoka kwenye kifaa chako, ambazo tunachambua na kuzitumia katika mifumo yetu ya kugundua udanganyifu.

Hii inaweza kujumuisha matumizi ya teknolojia za akili bandia (AI) na mifumo ya kufanya maamuzi kiotomatiki. Mifumo hii inaweza kuamua kiotomatiki uhalisia wa nyaraka za utambulisho, kulinganisha sifa za kibayometriki, au kutusaidia kutambua mifumo na tofauti zisizo za kawaida. Hakuna maamuzi muhimu ya kisheria yatakayofanywa bila usimamizi wa binadamu. Data yako ya kibinafsi inaweza kuchakatwa na Smile ID kwa madhumuni ya ufuatiliaji wa usalama, utambuzi wa mifumo, na kuboresha mifumo ya uthibitishaji.

Smile ID inaweza kuhamisha data yako kwenda eneo jingine kwa ajili ya uchakataji kwa mujibu wa Sheria za Ulinzi wa Data zinazotumika kwa taarifa zako. Unabaki na haki zako zote kama mhusika wa data, ikiwa ni pamoja na haki ya kuhamisha data, kurekebisha data, na haki ya kujiondoa kwenye uchakataji wa taarifa zako kwa namna ilivyoelezwa hapa.

Iwapo hukubaliani na uchakataji wa Data yako ya Kibinafsi kama ilivyoelezwa hapo juu, tafadhali usitumie bidhaa hii. Kwa maelezo zaidi, unaweza kupitia sera ya faragha ya Smile ID katika <https://smile.id/privacy-policy>

Smile ID hutoa msaada kwa [Customer], na hivyo [Customer] ndiye anayebaki kuwa mtoa maamuzi wa mwisho kuhusu ustahiki wako wa kutumia huduma zake.”

2.4.3. SAMPLE NOTICE IN ARABIC

وهي جهة متحكمة، Smile Identity Inc باستخدامك هذا المنتج، فإنك تمنح موافقتك لشركة“ بالبيانات مقرها الولايات المتحدة الأمريكية، و[العميل، وهي شركة مقرها _____]، على جمع الصور ومعلومات الجهاز الخاصة بك و/أو مستندات هويتك لغرض التعريف، والتحقق، ومنع الاحتيال.

بجمع ومعالجة معلوماتك بأمان لاكتشاف ومنع الاحتيال المتعلق بالهوية. عند Smile ID قد تقوم تفاعل مع أنظمتنا، نجمع المعلومات التي تقدمها، بالإضافة إلى البيانات الوصفية، ومعلومات الشبكة ومعرفات الأجهزة، وبيانات الموقع [...] من جهازك، والتي نقوم بتحليلها واستخدامها، IP مثل عناوين في أنظمة اكتشاف الاحتيال وأنظمة اتخاذ القرار الآلي. هذه الأنظمة قد تحدد (AI) قد يشمل ذلك استخدام تقنيات الذكاء الاصطناعي تلقائيًا مدى صحة مستندات الهوية، أو تطابق السمات البيومترية، أو تساعدنا في التعرف على الأنماط والشذوذات. لن يتم اتخاذ أي قرارات قانونية هامة دون إشراف بشري لمراقبة الأمان، والتعرف على الأنماط، وتحسين Smile ID قد تتم معالجة بياناتك الشخصية بواسطة بنقل بياناتك إلى أراضٍ أخرى للمعالجة وفقًا لقوانين حماية Smile ID أنظمة التحقق. وقد تقوم البيانات المعومول بها فيما يخص معلوماتك أنت تحتفظ بجميع حقوقك المتعلقة بالبيانات، بما في ذلك الحق في نقل البيانات، والتصحيح، والحق في رفض معالجة معلوماتك في هذا الصدد. إذا كنت لا توافق على معالجة بياناتك الشخصية كما هو موضح أعلاه، يرجى الامتناع عن استخدام هذا المنتج. لمزيد من التفاصيل، يمكنك مراجعة سياسة <https://smile.id/privacy-policy> على الرابط Smile ID الخصوصية الخاصة بـ الدعم لـ [العميل]، وبناءً عليه يظل [العميل] هو صاحب القرار النهائي بشأن أهليتك Smile ID تقدم "لاستخدام خدماته".

2.4.4. SAMPLE NOTICE IN FRENCH

"En utilisant ce produit, vous consentez à ce que Smile Identity Inc, responsable du traitement des données basé aux États-Unis, ainsi que [Customer, une société basée à _____], collectent des images ainsi que des informations relatives à votre appareil et/ou à vos documents d'identité dans le but d'assurer l'identification, l'authentification et la prévention de la fraude.

Smile ID peut collecter et traiter vos informations de manière sécurisée afin de détecter et prévenir la fraude liée à l'identité.

Lorsque vous interagissez avec nos systèmes, nous collectons les informations que vous fournissez, ainsi que des métadonnées et des informations réseau telles que les adresses IP, les identifiants d'appareil et les données de localisation [...] provenant de votre appareil, que nous analysons et utilisons dans nos systèmes de détection de fraude.

Cela peut inclure l'utilisation de technologies d'intelligence artificielle (IA) et de systèmes de prise de décision automatisés. Ces systèmes peuvent déterminer automatiquement l'authenticité des documents d'identité, faire correspondre des caractéristiques

biométriques ou nous aider à identifier des schémas et anomalies. Aucune décision juridique importante ne sera prise sans supervision humaine. Vos données personnelles peuvent être traitées par Smile ID à des fins de surveillance de la sécurité, de reconnaissance de schémas et d'amélioration des systèmes de vérification.

Smile ID peut transférer vos données vers un autre territoire pour traitement conformément aux lois sur la protection des données applicables à vos informations. Vous conservez tous vos droits en tant que personne concernée, y compris le droit à la portabilité des données, le droit de rectification et le droit de vous opposer au traitement de vos informations tel que décrit ci-dessus.

Si vous ne consentez pas au traitement de vos données personnelles tel que décrit ci-dessus, veuillez vous abstenir d'utiliser ce produit. Pour plus de détails, vous pouvez consulter la politique de confidentialité de Smile ID à l'adresse suivante :

<https://smile.id/privacy-policy>

3. ADHERENCE TO LOCAL LAWS

- 3.1. Different countries have different policies around the collection, processing and storage of personal information.
- 3.2. Wherever a Smile ID Customer operates, they must adhere to Applicable Data Protection Laws regarding the collection, handling or storage of personal information.
- 3.3. Customers shall ensure that all Users are provided with clear and accessible mechanisms to exercise their rights under Applicable Data Protection Laws. This includes providing end users with the contact details of Smile ID's Data Protection Officer at dpo@usesmileidentity.com as well as informing Users of available escalation pathways, including their right to lodge complaints with the relevant data protection supervisory authority.

4. NO USERS UNDER 16

- 4.1. If a Smile ID Customer believes that they have collected images of users who are under the age of 16, or Users who have not provided consent, they are required to notify Smile ID immediately.
- 4.2. Upon request from Smile ID, Customers may be required to destroy any data or images collected from or about those Users, unless otherwise



prescribed by law.

5. NO DISCRIMINATION

- 5.1. Customers shall ensure that all identity verification processes, including those involving automated decision-making or biometric analysis, are designed and implemented in a manner that prevents discriminatory outcomes. Specifically:
 - 5.1.1. processing shall not result in unfair or biased treatment of Users based on race, ethnicity, gender, age, nationality, disability, or any other protected characteristic under applicable laws;
 - 5.1.2. Customers must regularly assess and mitigate risks of algorithmic bias or disparate impact, particularly in relation to demographic attributes; and
 - 5.1.3. where automated systems are used, Customers shall implement appropriate safeguards, including human oversight, to ensure fairness, accuracy, and non-discrimination in identity verification outcomes.



PRIVACY POLICY

This Privacy Policy was last updated on 2026-06-05.

1. SUMMARY

- 1.1. This Privacy Policy ("Policy") describes how Smile Identity Inc. and its Affiliates ("Smile ID," "we," "our," "us") collects, processes, uses, and discloses certain information obtained through your use of our website (the "Site"), as well as information that we collect through our services or if you apply for a job with us (collectively with the Site, the "Services").
- 1.2. Smile ID acts as a data controller for the personal data it collects and processes in connection with its services, including identity verification, ID fraud detection, and Anti-Money Laundering (AML) screening.

2. DEFINITIONS

- 2.1. "**Affiliates**" refers means, with respect to a Party, any entity or individual that directly or indirectly controls, is controlled by, is under common control with, or is otherwise contractually engaged by such Party in a manner that supports shared commercial, operational, or technological objectives relevant to this Agreement.
- 2.2. "**Server logs**" refers to a document that automatically records information and details about online interactions with our sites. For example, server logs may record information about a person's visit to our Site at a particular time and day and collect information such as device ID or IP address.
- 2.3. "**Cookies**" refer to small files that are stored on a user's device through the use of our websites. A cookie allows the Site to recognize users who have visited and may store user preferences and other information. For example, cookies can be used to collect or store information about use of our website during a session and over time (including the pages viewed, and the files downloaded), the device's operating system, device ID, IP address, and users general geographic location.
- 2.4. "**Personal Information**" refers to information that can be used to identify, locate, or contact an individual, alone or when combined with other personal or identifying information.

3. INFORMATION WE COLLECT AND MAINTAIN

3.1. Third Party Collection

We collect information directly from you when you use the services and from third parties who provide it to us through the Services.

We may also collect information from Customers and third parties pursuant to the explicit consent of the data subjects where required. We further automatically collect certain information about persons from their smartphone or other device when they use, access, or interact with our Services. This includes but is not limited to technical data like IP addresses, device identifiers, location data . Additionally, we collect information when persons use any of the devices related to our ID verification, fraud detection and KYC services.

3.2. Cooperation with Partners for Data Subject Rights

Where Smile ID delivers services in partnership with trusted third parties, we may coordinate with these partners to ensure that data subject rights requests (for example, access, correction, or deletion) are handled in a timely and effective manner. The partner responsible for fulfilling a specific request will be identified to you, and Smile ID will facilitate the process to make sure your rights are respected. The detailed cooperation process between Smile ID and its partners is documented in our contractual arrangements and is available to supervisory authorities upon request.

3.3. Personal information provided directly by you through the Site

We collect personal information from Users who create an account on the Site, log into their account on the Site, or apply to a job with us. We may collect the following categories of information from these users:

- Full name
- The password you create for your account
- Email address
- Phone number
- Organization name
- Information about your customers
- Payment card information

- Resume information (including experiences and education information)
- Any personal information you provide in your cover letter
- Information we collect through your social media profiles or personal website

3.4. **Personal information collected through our identity verification services**

We may collect the following categories of information about Users who are subject to our identity verification, ID fraud detection, authentication or KYC services through our Customers and partners:

- Full name
- Contact Information
- Biometric information (facial geometry)
- Government ID number (from a national database)
- A photo of your face (selfie)

4. **HOW WE USE YOUR INFORMATION**

4.1. We use the information that we collect for a variety of purposes. Our legal bases for processing personal information are:

- our legitimate interest in running and maintaining our business;
- our legitimate interest in providing secure authentication and preventing fraud;
- the performance and fulfilment of our contracts;
- consent; and
- compliance with our legal obligations.

In many instances, more than one of these legal basis apply to the processing of your personal information.

4.2. The purposes for which we use personal information include to:

- provide Users with our Services;
- help detect and prevent fraud which may include the use of artificial intelligence and machine learning technologies and maintaining secure anti-fraud databases;
- analyze behavioural patterns and technical anomalies to generate advanced fraud-protection signals (Smile ID Risk Intelligence Signals) and improve our fraud networks;

- respond to questions or requests concerning the Services;
- fulfill the terms of any agreement requiring processing of personal data;
- fulfill requests for our Services or otherwise complete a transaction that persons initiate;
- send information about our Services and other topics that are likely to be of interest, including newsletters, updates, or other communications, including promotional emails;
- improve our artificial intelligence and machine learning technology;
- deliver confirmations, account information, notifications, and similar operational communications;
- improve User experience and the quality of our products and Services;
- comply with legal and/or regulatory requirements;
- aggregate and de-identify information;
- serve advertisements;
- analyze how visitors use the Services and various Services features, including to count and recognize visitors to the Services;
- create new products and Services; and
- manage our business.

5. WITH WHOM AND WHY WE SHARE YOUR INFORMATION


5.1. We share personal information with third parties for a variety of purposes, as described below.

5.1.1. **Businesses who sign up for our Services**

We may share personal information, which includes your identity verification status, with the businesses who utilize our verification KYC services. In addition to this privacy policy, information collected from persons by businesses who use our services may be subject to the privacy policies of these businesses.

5.1.2. **Fraud prevention**

We process personal data for fraud prevention and identity Verification. This includes creating and maintaining a secure, hashed database used by us and select partners, comparing customer data with the database to detect anomalies using Artificial Intelligence systems and models developed by the Smile ID team, and deploying human review to evaluate the decisions of



the machine following a rule-based system. We only process data points strictly necessary for fraud prevention, use secure storage, apply strict access controls, and conduct regular reviews to ensure data accuracy and proportionality.

5.1.3. Data sharing

We may share personal information, including identity verification data, with our Affiliates and partners to facilitate fraud prevention, identity verification, and secure transaction processing, or to develop new products to improve identity verification and fraud prevention in accordance with applicable laws and regulations.

5.1.4. Third-party service providers

Smile ID uses third-party service providers that perform services on our behalf, including web-hosting companies and mailing vendors. These service providers may collect and/or use personal information we process, including information that identifies persons, to assist us in achieving the purposes discussed above. We may also share personal information with third parties when necessary to fulfill requests for Services; to complete a transaction initiated by persons through third parties; to meet the terms of any agreement that persons may have with third parties or with us; or to manage our business.

5.1.5. Analytics

We partner with certain third parties to obtain the automatically collected information discussed above and to engage in analysis, auditing, research, and reporting. These third parties may use pixels or server logs, and they may set and access device IDs and IP addresses from your device.

5.1.6. Interest-based Advertising

The Services also enable third-party tracking mechanisms to collect information about persons and personal computing devices for use in online interest-based advertising. For example, third parties, such as Facebook, may use personal information deposited in our app to target online ads to persons who may have used our apps. In addition, our third-party advertising networks might use personal information obtained from use of our Services to help target advertisements based on mobile activity in general. For information about interest-based advertising practices, including privacy and confidentiality, visit the Network Advertising Initiative website or the Digital Advertising Alliance website.

- 5.2. We share personal information with third parties for a variety of purposes, as described above. The use of online tracking mechanisms by third parties is subject to those third parties' own privacy policies, and not this Policy. Persons who prefer to prevent third parties from setting and accessing cookies on their computer or other device may set their browser to block cookies.
- 5.3. Additionally, persons may remove themselves from the targeted advertising of companies within the Network Advertising Initiative by opting out [here](#), or of companies participating in the Digital Advertising Alliance by opting out [here](#). Although our Site currently does not respond to "do not track" browser headers, persons can limit tracking through these third-party programs and by taking the other steps discussed above.

6. YOUR CHOICES

- 6.1. Persons who may wish to access, correct, or delete the personal information we have on file, may contact us at dpo@usesmileid.com.
- 6.2. Residents of the EU, UK, or other jurisdictions with Applicable Data Protection Laws, may have certain rights. These rights may include:
 - The right to be informed about our data collection practices;
 - The right to access and rectify your data;
 - The right to erase or delete your data;
 - The right to data portability;
 - The right to restrict and object to the processing of your data (including for direct marketing purposes);
 - The right to opt-out of marketing emails and text messages;
 - The right to limit our use of any automated decision-making processes;
 - The right to lodge a complaint to your local data protection authority; and
 - The right to withdraw consent (to the extent applicable).
- 6.3. To exercise any of the rights listed above, please contact us via email at compliance@usesmileid.com. We will respond to your request as soon as reasonably possible but no longer than thirty (30) calendar days.

7. EXTERNAL LINKS

- 7.1. We do not warrant, endorse, guarantee, or assume responsibility for the accuracy or reliability of any information offered by third-party websites linked through the site or any website or feature linked in any banner or other advertising.

8. DATA SECURITY


- 8.1. We employ physical, technical, and administrative procedures to safeguard the personal information we collect both online and offline. However, no website or platform is 100% secure, and we cannot ensure or warrant the security of any information you transmit through the Services or to us, and therefore you transmit such information at your own risk.

9. DATA RETENTION

- 9.1. We retain personal information about you only for as long as is necessary to fulfil the purpose for which that information was collected or as required or permitted by law [, for example, under Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) laws where applicable]. We may also retain certain data points for fraud prevention and identity Verification purposes. This is based on our legitimate interest in maintaining the security and integrity of our systems and services, as well as preventing ID-related fraud for Users and third-party service providers. We do not retain personal information longer than is necessary to achieve this purpose. Individuals reserve their rights to object to this processing or request the erasure of their information under applicable data protection laws. We may however, continue to retain the data where: (i) in compliance with a legal obligation; (ii) required for legal claims; (iii) necessary for reasons of substantial public interest; (iv) necessary for preventing or detecting unlawful behaviour; or (v) as otherwise lawfully permitted by Applicable Data Protection Laws. When we destroy personal information which no longer needs to be retained, we do so in a way that prevents that information from being restored or reconstructed. Further information about our data retention practices is outlined in the Smile ID Data Retention Policy [here](#).

10. INTERNATIONAL USERS

- 10.1. The information that we collect through or in connection with the Services is transferred to and processed in the United States of America for the purposes described above. We may also subcontract the processing of your data to, or otherwise share your data with, Affiliates or third parties in countries other than your country of residence. The data-protection laws



in these countries may be different from, and less stringent than, those in your country of residence. However, we comply with all Applicable Data Protection Law regarding international data transfers.

- 10.2. By using the Services or by providing any information to us, persons expressly consent to such transfer and processing.

11. CHILDREN

- 11.1. Content on the Services is directed at individuals over the age of 18 and is not directed at children under the age of 13. We do not knowingly collect personally identifiable information from children under the age of 13.

12. CHANGES TO THIS POLICY

- 12.1. We may make changes to the Services in the future and as a consequence will need to revise this Policy to reflect those changes. We will notify you and post all such changes on the Services, and we encourage users to review this page periodically.

13. HOW TO CONTACT US

- 13.1. If there are questions or concerns about this Policy, we can be contacted by email at compliance@usesmileid.com.



DATA RETENTION POLICY

This Data Retention Policy was last updated on 2026-06-05.

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 or as required or permitted by law.

3.2.

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
Device information such as IP address, location data, 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 days after account deletion
V3 optimised pre-verified results	Retained for no longer than 5 years except 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: 2026-06-05.

Approved by: Data Protection Officer, Smile ID