

Compliance pack

Generated 2026-10-27. Describes the platform as it runs today.

1. The service

VerifyID verifies that a person is who they claim to be by comparing a photo of their identity document with a live capture of their face, checking that the capture comes from a live person, and reading the document's data. It is operated by Vyloxi and offered to businesses (our customers), who decide whom to verify and why. For the personal data of the people they verify, the customer is the controller and VerifyID acts as processor on the customer's instructions.

2. Data processed

Identity document images (front and, when provided, back) and the data read from them: name, document number, dates of birth and expiry, nationality, sex, and machine-readable zone check-digit results.

Face images from the live capture and a numeric face signature (512 numbers) derived from them. The signature is biometric data.

Device and network data from the capture: IP address, approximate country, browser/device description, whether the address is a Tor exit node.

Results: scores, reasons, reviewer decisions and notes, the consent record, and the case timeline.

Sanctions screening results for the name read from the document (OFAC SDN and UN consolidated lists).

3. Purposes

Verifying identity for the customer who requested it; detecting fraud (spoofed captures, the same face reappearing under another identity within the same customer account, sanctions matches); keeping an audit record of each decision. Data is not sold and is not used for advertising. It is not used across customer accounts: duplicate-face detection only compares faces within one account.

4. Consent

On hosted verification pages, the person must tick a consent statement naming the customer before any capture. The exact wording, its version, the time, IP address, browser and language are stored in the case timeline and printed in the case report. Customers who capture through the API or their dashboard collect consent themselves.

5. Retention

Images: each customer chooses from 'delete right after the decision' to 1 year (default: delete right after the decision). Images of a case waiting for manual review are kept until the review, then deleted on that schedule.

Verification records and the face signature: 30 days to 2 years, chosen by the customer (default 90 days).

Encrypted database backups: 14 days.

A daily job enforces these periods; each deletion is written to the case timeline.

6. Security measures

Encryption in transit with TLS; evidence images, support attachments, bot credentials and database backups are encrypted at rest with AES-256-GCM.

Passwords are stored as salted hashes; two-factor authentication (authenticator app) is available to every user; staff access is role-based.

Every staff and account action that changes data or settings is written to an audit log that can be exported as CSV. Staff views of customer accounts are logged.

Optional two-person approval: a customer can require two different people to approve a case in review; the platform can require two administrators to approve production access.

Nightly encrypted database backups, each verified by listing its contents after it is made; failures raise an alert to the operations team.

Rate limiting on the API and public forms; same-origin checks on state-changing browser requests; continuous server, database and error monitoring with alerts.

7. Sub-processors

Server hosting: a virtual private server operated for Vyloxi (application, database and encrypted files).

Email delivery: Hostinger (transactional email and the support mailbox).

Google: only when a user chooses 'Sign in with Google' (name, email, profile picture of that user).

Telegram: internal operations notifications and, when a customer chooses to contact support there, that support conversation. Verification images and document data are not sent to Telegram.

Anthropic: only if support-ticket translation is enabled, the text of that ticket message is sent for translation. It is off unless an administrator configures it.

Face analysis, liveness, document reading and sanctions screening run on VerifyID's own servers; no third-party biometric service receives the images.

8. Rights of the people verified

A person can ask for a copy of their data or for its deletion through the public form at /privacy/request, through the customer, or by email. Requests are confirmed by email, routed to the customer (the controller), tracked with a reference and a 30-day due date, and answered with a downloadable copy or a deletion record. Deletion removes images, the face signature and identifying fields; a bare record (type, status, dates) is kept so statistics and the audit trail stay consistent.

9. Incidents

Security incidents affecting customer data are investigated immediately; affected customers are told without undue delay, with what is known, so they can meet their own notification duties. Service incidents are published on the public status page, which customers can subscribe to.

10. Contact

Privacy and compliance questions: verifyid@vyloxi.com, or a ticket from the dashboard.

The master services agreement sent when production access is approved includes the data protection terms. Contact support for anything else your review needs.