Privacy Policy

Revision March 2026

Sigmine Ltd · Reg. 207785406 · Bulgaria

---

1. Data controller

Sigmine Ltd
Commercial register: 207785406 (Republic of Bulgaria)
Registered office: 2B Emiliyan Stanev str., Triaditsa Distr., Sofia 1407, Bulgaria
Contact: `support@sigmine.io`

2. Scope

This Privacy Policy describes how SigMine collects, uses, retains, shares, and protects the User's personal data when using the mobile application, website, or any associated service of SigMine (hereinafter, the "Services").

SigMine **does not sell personal data** to third parties.

3. Personal data we collect

3.1. Registration and account data

- Full name.
- Email address.
- Password (stored in encrypted form).

Purpose: account creation and management, authentication, communication, and technical support.
Legal basis: performance of a contract (Art. 6(1)(b) GDPR).

3.2. Identity verification data (KYC)

- **Identity document images:** photographs of the front and, where applicable, back of the User's official document, including the data therein (name, date of birth, document number, nationality, holder's photograph).
- **Data extracted from the document:** data obtained via optical character recognition (OCR) and machine-readable zone (MRZ) reading.
- **Tax identification number:** required under the DAC8 Directive.

Purpose: compliance with legal identification obligations, anti-money laundering, and tax compliance.
Legal basis: legal obligation (Art. 6(1)(c) GDPR); legitimate interest in fraud prevention (Art. 6(1)(f) GDPR).

3.3. Facial biometric data

During the identity verification process, SigMine collects and processes the following biometric data:

- **Facial images:** during the liveness check, the User's device camera captures a brief facial video from which photographic images of the User's face are extracted. These images are stored persistently in SigMine's systems.
- **Automated facial comparison:** the facial images are automatically compared with the photograph on the identity document. During this process, the software generates biometric vectors **transiently in memory**; these vectors are used exclusively for the comparison and are **not stored persistently**.
- **Derived data:** the software may derive data such as the User's estimated age, solely for identity validation purposes.
- **Verification result:** the comparison result (positive or negative), liveness confidence score, timestamps, session identifiers, and process duration.

Data stored persistently includes: facial images, identity document images, and liveness verification results.

Exclusive purpose: identity verification and fraud prevention. Biometric data is **not used** for advertising, personalisation, or commercial profiling purposes.

Legal basis: explicit consent of the User (Art. 9(2)(a) GDPR), given specifically before initiating the liveness check; supplemented by the legal obligation of customer identification (Art. 6(1)(c) GDPR).

Storage: data is stored **exclusively by SigMine** on servers located in the European Union (Germany). The identity verification technology provider (Regula Forensics) provides only the software and licence; it **does not store or have access to** the User's personal or biometric data.

Encryption: biometric data is encrypted in transit (TLS) and at rest.

3.4. Wallet and transaction data

- Public crypto-asset wallet addresses associated with the User.
- Transaction identifiers (hashes) related to fund withdrawals.
- Ownership certificate of the destination wallet.

Purpose: enabling withdrawals, traceability, auditability, and tax compliance (DAC8).
Legal basis: performance of a contract (Art. 6(1)(b) GDPR); legal obligation (Art. 6(1)(c) GDPR).

3.5. Device and usage data

- IP address, device identifiers, Application version, and operating system.
- Application interaction logs (access, authentication, and operational activity logs).

Purpose: security, fraud detection, operational control, technical auditing, and regulatory compliance.
Legal basis: legitimate interest (Art. 6(1)(f) GDPR); legal obligation when records are required by authorities (Art. 6(1)(c) GDPR).

4. Automated decisions

During identity verification, SigMine uses an **automated facial comparison** system that may reject the verification if the match does not reach the required confidence threshold.

Under Art. 22 of the GDPR, the User has the right to request **human review** of any automated decision that affects them, by contacting `support@sigmine.io`.

5. Disclosure of data to third parties

5.1. Tax authorities

Where legally required under the DAC8 Directive, SigMine will disclose identification data, tax identification numbers, wallet addresses, and asset information to the competent tax authorities. See the *DAC8 Directive Tax Information* document.

5.2. Service providers

- **Hosting infrastructure** (Amazon Web Services, Germany): storage and processing. Subject to contractual confidentiality obligations (Art. 28 GDPR).
- **Identity verification software** (Regula Forensics): provides only the software licence. Does not receive, store, or access the User's personal data.

5.3. Competent authorities

SigMine may disclose data to judicial, law enforcement, or regulatory authorities where a legal obligation exists.

6. International transfers

Personal data is stored on servers located in **Germany (European Union)**, operated by AWS. SigMine **does not transfer data outside the European Economic Area**. If necessary in the future, SigMine will apply the safeguards under Chapter V of the GDPR and inform the User in advance.

7. Retention periods

Data category	Period	Reason
Registration and account data	5 years after account closure	Legal and tax obligations
KYC data and facial images	5 years from collection	AML/KYC regulations
Tax identification number	5 years after account closure	DAC8 Directive
Wallet and transaction data	5 years after account closure	Tax obligations
Technical logs	5 years from generation	Security and auditing

After these periods, data is permanently deleted or irreversibly anonymised.

8. User rights

Under the GDPR, the User has the right to:

- **Access** (Art. 15): obtain confirmation and access to their data.
- **Rectification** (Art. 16): correct inaccurate or incomplete data.
- **Erasure** (Art. 17): request deletion, without prejudice to legal retention obligations.
- **Restriction of processing** (Art. 18): restrict processing in certain circumstances.
- **Portability** (Art. 20): receive their data in a structured, machine-readable format.
- **Objection** (Art. 21): object to processing based on legitimate interest.
- **Withdrawal of consent** (Art. 7(3)): withdraw consent at any time, without affecting the lawfulness of prior processing. Withdrawal of biometric consent may prevent use of services requiring identity verification.
- **Not to be subject to automated decisions** (Art. 22): request human review.

Contact for exercising rights: `support@sigmine.io`. Response period: **one (1) month**, extendable as provided by the GDPR.

8.1. Complaint to supervisory authority

The User may lodge a complaint with the **Commission for Personal Data Protection of Bulgaria (CPDP)** or with the data protection authority of their Member State of residence.

9. Minors

The Services are not directed at persons under **eighteen (18) years of age**. SigMine does not knowingly collect data from minors.

10. Security measures

SigMine implements appropriate technical and organisational measures, including encryption in transit and at rest, role-based access control, continuous monitoring, and incident response procedures. No system is completely secure; SigMine cannot guarantee absolute data security.

11. Modifications

Any substantial modification will be communicated to the User through the Services or by email before it takes effect.

12. Contact

Email: `support@sigmine.io`
Address: 2B Emiliyan Stanev str., Triaditsa Distr., Sofia 1407, Bulgaria