

# Privacy Policy

HelveticPay AG

Last updated: January 2026

## 1. Who we are

HelveticPay AG  
Kolinplatz 17  
6300 Zug  
Switzerland

HelveticPay AG is a Swiss financial intermediary subject to the Swiss Anti-Money Laundering Act (AMLA) and supervised by a Swiss self-regulatory organization (SRO). HelveticPay does not act as a bank, does not execute payments in its own name, and does not hold or safeguard client funds.

For questions regarding data protection, you may contact us at the contact details published on our website.

## 2. Scope of this Privacy Policy

This Privacy Policy explains how HelveticPay AG processes personal data of:

- Corporate customers and their representatives
- Beneficial owners, controlling persons, directors, and authorized signatories
- Prospective customers during onboarding
- Website users and business contacts

It applies to all processing activities carried out by HelveticPay AG in connection with customer due diligence, onboarding, monitoring, and compliance activities.

## 3. Categories of personal data we process

Depending on the relationship and legal requirements, we may process the following categories of personal data:

### 3.1 Identification and contact data

- Full name
- Date of birth
- Nationality or nationalities
- Residential address
- Contact details
- Identification document data (including document number, issuing authority, validity, and MRZ data)

### 3.2 Corporate and professional data

- Company name and registered address
- Business activities and place of business
- Role, position, and authority within an entity
- Information on ownership and control structures

### 3.3 Compliance and risk-related data

- Beneficial ownership and controlling person declarations
- Source of funds and source of assets information
- Financial and transactional context information required for AML purposes
- Risk classification data
- Results of sanctions, PEP, and adverse media screenings

### 3.4 Technical and verification data

- Video and image data collected during video or online identification
- Biometric verification results derived from identification documents
- IP address and geolocation checks where legally required

## 4. Purposes of data processing

We process personal data exclusively for legitimate, defined purposes, including:

- Customer identification and verification
- Performance of know-your-customer (KYC) and know-your-business (KYB) checks
- Compliance with AMLA, AMLO, AMLO-FINMA, SRO regulations, and sanctions regimes
- Risk classification and ongoing monitoring of business relationships
- Detection and prevention of money laundering, terrorism financing, and sanctions circumvention
- Fulfillment of reporting, record-keeping, and audit obligations
- Communication with customers and competent authorities

We do not use personal data for profiling, marketing, or automated decision-making unrelated to regulatory compliance.

## 5. Legal basis for processing

Personal data is processed on one or more of the following legal bases:

- Compliance with Swiss legal and regulatory obligations
- Performance of contractual or pre-contractual measures
- Legitimate interests in maintaining a compliant, secure, and lawful business operation
- Explicit consent, where required by law (for example for video identification)

Where processing is required by law, consent is not required and cannot be withdrawn.

## 6. Data sharing and recipients

We may share personal data with the following categories of recipients, strictly on a need-to-know basis:

- Regulated partner banks and payment institutions
- External identification, screening, and AML service providers meeting Swiss standards
- Auditors and compliance advisors
- Swiss and foreign authorities, including MROS, SECO, FINMA, or prosecuting authorities, where legally required

We do not sell personal data and do not allow third parties to use personal data for their own purposes.

## 7. Cross-border data transfers

Where personal data is transferred outside Switzerland, we ensure that:

- The transfer is legally required or necessary for compliance purposes, and
- Appropriate safeguards are in place, such as adequacy decisions, contractual protections, or equivalent regulatory obligations

## 8. Data retention

Personal data and related documentation are retained for **ten years** after the end of the business relationship or completion of a transaction, in accordance with Swiss AML and accounting regulations.

After expiry of the retention period, data is securely deleted or anonymized unless further retention is required by law.

## 9. Data security

We implement appropriate technical and organizational measures to protect personal data against unauthorized access, loss, alteration, or disclosure. These measures include:

- Restricted access controls
- Secure storage systems located in Switzerland
- Audit trails and backup procedures
- Confidentiality obligations for employees and service providers

## 10. Your rights

Subject to applicable law, you may have the right to:

- Request access to your personal data
- Request correction of inaccurate or incomplete data

- Request deletion or restriction of processing where legally permitted
- Object to certain processing activities

Please note that these rights may be limited or excluded where processing is required by law, particularly under AML regulations.

## **11. Obligation to provide data**

Providing personal data is mandatory where required by law or regulation. Failure to provide requested information may result in refusal or termination of a business relationship.

## **12. Changes to this Privacy Policy**

We may update this Privacy Policy to reflect changes in legal, regulatory, or operational requirements. The current version will always be made available through our official communication channels.