SwissFox Privacy Policy

This Privacy Policy explains how we collect, use, disclose, secure, and retain personal data when you interact with our websites, mobile apps, communications, and services (collectively, the "Services"). It applies to visitors, applicants, verified customers, and business contacts.

1) Summary (executive snapshot)

- We collect KYC/AML data, account & transaction data, and technical telemetry to run the SwissFox platform and comply with Swiss law.
- We share data with banking/payment partners, cloud & security vendors, and compliance providers (e.g., sanctions/PEP screening, chain analytics), and with counterparties/financial intermediaries for Travel Rule compliance.
- We retain business and AML records for 10 years after the end of the relationship/transaction, and keep other data for proportionate periods.
- You can access, correct, port, and request deletion of your data (subject to legal holds). We respond within 30 days.
- We provide a cookie/SDK preference center for non-essential tracking.
- If a personal-data breach poses high risk, we will notify the FDPIC and affected users as soon as possible.

2) What we collect

2.1 Data you provide directly

- Identification & onboarding: full name, date of birth, nationality, residential address, government ID/passport details, occupation, PEP status, beneficial ownership (for entities), and—where applicable—video/online identification artifacts.
- Account & profile: email, phone number, password hashes/MFA artifacts, preferences.
- Financial crime controls: information about source of funds/wealth, risk questionnaires, declarations.
- Communications: support tickets, emails, optional call recordings (if we activate recordings, we will inform you at the start of the call).
- Marketing consent: newsletter/alerts preferences; referral features (see §10.2).

2.2 Data we generate or collect automatically

- Account & transaction metadata: account status, login timestamps, session identifiers, order and funding/withdrawal history, wallet addresses you use with the Service, device/IP, approximate location derived from IP.
- Telemetry & analytics: app and browser type/version, OS, device identifiers (e.g., IDFV/IDFA on iOS, AAID on Android), event logs, crash diagnostics, email open/click signals (pixels).
- Security signals: device fingerprinting, anomaly and abuse indicators, access logs.

2.3 Data from third parties

- Compliance datasets: sanctions/PEP lists, adverse-media data, fraud and risk data from specialist vendors; blockchain analytics for compliance.
- Financial partners: payment institutions and banks (e.g., KeaBank (Gulliver Pay Inc)) provide status/settlement confirmations and reconciliation data.
- Corporate data: commercial registers, KYC/KYB service providers.
- Public sources: government registers, publicly available websites and media.

Sensitive data. If we use video/online identification, we may process biometric templates or liveness data strictly to verify your identity and to combat fraud. Where we do, we apply enhanced safeguards and minimal retention.

3) Why we use personal data (purposes)

We process personal data to:

1. Deliver and operate the Services (create/maintain accounts, facilitate orders/wallet activity, provide support).
2. Comply with law and regulation (AMLA/AMLO-FINMA, VQF rules, sanctions/embargo regimes, bookkeeping/CO 958f).
3. Financial-crime risk management (KYC/KYB, sanctions/PEP screening, monitoring, investigations, regulatory reporting to MROS/authorities).
4. Travel Rule compliance: collect and exchange originator/beneficiary information with counterpart financial intermediaries/VASPs when required.
5. Security (detect, investigate, and mitigate fraud, abuse, and cyber threats; maintain logs and evidence chains).

6. Product analytics & service improvement (aggregate usage analytics, performance tuning).
7. Communications & marketing (transactional messages; marketing only with consent or within statutory allowances; opt-out anytime).
8. Corporate operations (audits, accounting, mergers & acquisitions due diligence).

Swiss legal justification. We rely on the principles of good faith, proportionality, purpose limitation, and transparency under Swiss law. Processing is justified by contract necessity, legal obligations (e.g., AML), and/or overriding private/public interests; where required, we obtain consent (e.g., for non-essential cookies/SDKs or certain marketing).

4) Cookies, SDKs, and similar technologies

- We use cookies and SDKs to operate the site/app, secure sessions, measure performance, and—if you opt in—support analytics/marketing.
- On first visit and thereafter, you can set preferences in our Cookie/SDK Preference Center. Essential cookies are always active; non-essential tracking is off by default unless you opt in.
- Email communications may include tracking pixels to measure deliverability and engagement; you can opt out of marketing any time.
- Do Not Track (DNT): we currently rely on the preference center rather than browser DNT signals.

5) How we share personal data

We disclose personal data to:

- Group entities and contractors supporting SwissFox operations (on a need-to-know basis under binding data-processing terms).
- Financial partners for fiat flows and settlement (e.g., KeaBank (Gulliver Pay Inc)), card/payment processors, and correspondent banks.
- Compliance and security vendors (KYC/KYB, sanctions/PEP screening, blockchain analytics, fraud-prevention, secure communications, document verification).
- Cloud/IT providers (infrastructure, storage, monitoring, email/SMS, customer support tooling).
- Counterpart institutions (financial intermediaries/VASPs) for Travel Rule information exchange when required by law/regulation.

- Auditors, advisors, insurers (professional confidentiality applies).
- Authorities and courts where legally required or permitted (e.g., MROS filings, supervisory inquiries, lawful requests).
- Corporate transactions (merger, acquisition, financing, or asset transfer), subject to confidentiality controls.

We do not sell personal data.

6) International data transfers

Your data may be accessed from or transferred to countries outside Switzerland. We use the following safeguards:

- Adequacy decisions by the Swiss Federal Council where available.
- For transfers to the United States: if the recipient is certified, we may rely on the Swiss-US Data Privacy Framework; otherwise we use Standard Contractual Clauses with the Swiss addendum, plus transfer-impact assessments and supplementary measures as needed.
- Remote support access from abroad is treated as an international transfer and is subject to the same safeguards.

7) Retention

We retain personal data only as long as necessary for the purposes described here or as required by law. Illustrative periods:

- AML/KYC and business records: generally 10 years after the end of the business relationship or the completion of the one-off transaction (in line with Swiss record-keeping norms).
- Operational logs & security telemetry: typically 12–24 months (longer if investigating incidents).
- Marketing consents & suppression lists: kept as long as necessary to demonstrate compliance and to honor opt-out.
- Backups: retained for limited cycles and then overwritten; where deletion is not immediately feasible, data is put beyond routine business use until expunged.

When retention ends, we delete or irreversibly anonymize the data.

8) Security

We implement risk-appropriate technical and organisational measures, including access controls, encryption in transit and at rest where applicable, network segmentation, monitoring/logging, secure development practices, vendor due diligence, and employee confidentiality obligations.
No method of transmission or storage is 100% secure, but we continuously improve our controls and test for efficacy.

9) Automated decision-making and profiling

We may use automated systems and risk-scoring (e.g., sanctions screening, fraud/AML analytics) that can produce decisions with legal or similarly significant effects. When we make a solely automated decision with such effects, you may request human review, express your point of view, and contest the decision—subject to legal/AML constraints.

10) Your choices

10.1 Marketing preferences

You can opt in/out of marketing at signup and any time thereafter (links in our emails or in-app settings). Transactional communications are not marketing and you cannot opt out of those.

10.2 Referrals

If you provide third-party contact details for a referral, you must have their consent. We will not send repeated marketing to a referral without their own consent.

10.3 Cookies/SDKs

Use the Preference Center to manage non-essential cookies/SDKs at any time.

11) Your rights (Swiss data protection)

Subject to legal exceptions (e.g., AML obligations, overriding interests), you have the right to:

- Access the personal data we hold about you;
- Rectify inaccurate or incomplete personal data;
- Erase personal data where no legal basis requires continued processing;
- Port data you provided to us, in commonly used electronic format, where technically feasible;
- Object to processing based on overriding private interests; and

- Withdraw consent at any time for processing based on consent (e.g., non-essential cookies, marketing).

How to exercise your rights: contact support@swissfox.com from your registered email and be prepared to verify your identity. We generally respond within 30 days.

Regulator contact: you may contact the Swiss Federal Data Protection and Information Commissioner (FDPIC) about concerns. We recommend contacting us first so we can address them promptly.

12) Personal-data breaches

If a breach is likely to pose a high risk to your personality or fundamental rights, we will notify the FDPIC as soon as possible and, where required, inform you without undue delay, describing the nature of the breach, likely consequences, and measures taken.

13) Account closure & data after deletion

You can request account deletion via in-app settings (where available) or by emailing support@swissfox.com. After deletion:

- Your login will be disabled and access removed.
- We will retain only the data we must keep to comply with law (e.g., AML/business records), resolve disputes, prevent fraud, or enforce our terms, and will delete/anonymize when retention expires.
- We will continue to protect retained data with appropriate security and limit access to personnel with a need-to-know.

14) Changes to this Privacy Policy

We may update this Policy from time to time. Material changes will be announced in-app or by email at least 30 days before they take effect. The “Effective date” above is the latest revision date.

15) How to contact us

- Privacy & DSAR requests: support@swissfox.com
- Postal: Helvetia Chain GmbH (SwissFox), Gartenstrasse 6, 6300 Zug, Switzerland