Privacy Policy

How FX Rails AG collects, uses, shares and protects personal data across consumer transfer and merchant acquiring services.

Effective date: 17 August 2026
Operator: FX Rails AG | UID: CHE-403.817.123 | Seefeldstrasse 219, 8008 Zurich, Switzerland
Website: https://fx-rails.com/ | Contact: customer@silvo.io

REGULATORY CONTEXT	SERVICES COVERED
FX Rails AG states that it is affiliated with VQF Financial Services Standards Association (membership no. 101231) for Swiss AML self-regulatory supervision. This document does not represent that such affiliation is an EU payment institution or banking licence.	Digital payment platform services, EUR card-to-card or card-directed transfers where available, account and dashboard functions, and merchant acquiring/payment processing features when separately approved, contracted and technically enabled.

1. Purpose and scope

This Privacy Policy explains how FX Rails AG ("FX Rails", "we", "us" or "our") processes personal data when individuals visit fx-rails.com, create or use an account, initiate or receive payment-related services, communicate with us, act for a business customer, or interact with merchant acquiring and payment-processing services made available by us or through our regulated banking, payment, acquiring, card-network and technology partners.

This Policy is intended to address the Swiss Federal Act on Data Protection (FADP) and, where the processing falls within its territorial scope, the EU General Data Protection Regulation (GDPR) and applicable e-privacy rules. Additional notices may apply to a specific product, merchant, partner integration or jurisdiction. If an additional notice conflicts with this Policy for a specific service, the more specific notice applies to that service.

Some payment services are delivered with or through third-party financial institutions, payment processors, acquirers, issuers, card schemes or technical service providers. Depending on the service and data flow, such parties may act as independent controllers or processors. Their own privacy notices may also apply.

2. Who is covered

- Visitors to the FX Rails website and web applications.
- Registered individual users and prospective users.
- Senders, recipients and beneficiaries of card-directed or other supported transfers.
- Directors, shareholders, beneficial owners, authorised signatories, employees and representatives of business customers and merchants.
- Merchant customers that use acquiring, payment gateway, payment processing, settlement, reconciliation or reporting functionality.
- Cardholders and purchasers whose payments are processed for a merchant, where FX Rails receives transaction or fraud-prevention data.
- Persons who contact customer support, submit complaints, complete forms, attend onboarding or otherwise communicate with us.

3. Categories of personal data we may process

Identity and verification data

Name, date and place of birth, nationality, citizenship or residence information, identity-document type and number, document images, selfie/liveness results, signature, tax identifiers where relevant, and verification outcomes.

Contact and profile data

Email address, telephone number, postal address, account profile, preferred language, communication preferences and customer identifiers.

Business and KYB data

Company name, registration number, registered office, operating address, corporate documents, website/domain information, business activity, licences or permits, ownership and control structure, beneficial owners, directors, authorised persons, expected volumes and transaction profiles.

Payment and transaction data

Transaction amount, currency, timestamps, sender and recipient references, merchant identifiers, terminal or account identifiers, masked or tokenised card information, bank or payment-account references, authorisation and settlement status, refunds, reversals, disputes and chargebacks.

Merchant acquiring data

Merchant category, MCC, descriptors, product/service information, checkout and payment-page data, acquirer/processor references, card-scheme data elements, settlement instructions, reserve information, payout reports, fraud indicators, dispute evidence and reconciliation records.

Financial and source-of-funds data

Funding source, bank statements or other supporting documents, expected and actual activity, source of wealth/source of funds information where required, invoices, contracts and evidence of underlying transactions.

Compliance and risk data

KYC/KYB results, sanctions and PEP screening results, adverse-media indicators, fraud scores, transaction-monitoring alerts, device-risk indicators, case-management notes and communications with competent authorities where legally permitted.

Device and technical data

IP address, browser and device type, operating system, device/session identifiers, timestamps, security logs, authentication events, cookies, SDK or analytics identifiers and diagnostic data.

Support and communications data

Messages, forms, complaints, call or chat notes, attachments, feedback and information necessary to investigate a service issue or dispute.

Marketing data

Newsletter subscription, consent records, campaign engagement, referral data and preferences, where marketing is used.

We do not intentionally store full card security codes (CVV/CVC) after authorisation. Card data may be tokenised, masked or processed by PCI DSS-compliant service providers depending on the integration model. The exact card-data environment depends on the merchant integration and payment partner used.

4. Where data comes from

- Directly from you during registration, verification, account use, support or merchant onboarding.
- From a business customer, merchant, employer or authorised representative that identifies you as a director, employee, beneficial owner, recipient, customer or contact person.

- From banks, card issuers, acquirers, payment processors, card schemes, payment gateways and other financial institutions involved in a transaction.
- From identity-verification, fraud-prevention, sanctions/PEP screening and compliance providers.
- From public registers, corporate registries, sanctions lists and other legally accessible sources used for due diligence.
- Automatically from devices, browsers, cookies, logs and security systems when you use our services.

5. Purposes and legal bases

Purpose	Examples	Typical legal basis
Provide and administer services	Account creation, authentication, transfer execution, merchant acquiring, payment processing, settlement, reconciliation, support and reporting.	Contract performance; steps requested before entering a contract; legitimate interests.
KYC/KYB, AML and sanctions compliance	Identity verification, beneficial-owner checks, transaction monitoring, sanctions/PEP screening, investigation and record-keeping.	Legal obligations; substantial public interest where applicable; legitimate interests in compliance and risk management.
Fraud and security	Device risk, behavioural indicators, authentication, anomaly detection, account protection, dispute investigation.	Legitimate interests; legal obligations; contract performance.
Card acquiring and scheme compliance	Authorisation, clearing, settlement, chargebacks, refunds, retrieval requests, scheme monitoring and merchant risk management.	Contract performance; legal obligations; legitimate interests; card-scheme and partner requirements.
Customer communication	Service messages, incident notices, complaints, support and material legal updates.	Contract performance; legal obligations; legitimate interests.
Product improvement and analytics	Performance metrics, debugging, capacity planning, usability and service improvement.	Legitimate interests; consent where required for non-essential cookies/analytics.
Marketing	Optional product updates and promotions.	Consent where required; legitimate interests where permitted, subject to opt-out rights.
Legal claims and governance	Audits, risk management, legal proceedings, responding to authorities, corporate transactions.	Legal obligations; legitimate interests; establishment/exercise/defence of legal claims.

6. Payment and merchant acquiring data

When FX Rails provides or facilitates merchant acquiring or card-payment processing, we may receive transaction data from the merchant, payment page, gateway, processor, acquirer, issuer and card scheme. The information may include the data needed to route, authorise, authenticate, clear, settle, refund, reconcile and dispute a payment. We may also use such data to detect fraud, enforce merchant risk controls and satisfy AML, sanctions, card-scheme or partner obligations.

Merchants are independently responsible for providing cardholders and website visitors with their own legally compliant privacy notices and for establishing a lawful basis for transferring personal data to FX Rails and relevant payment participants. Where we act as a processor on documented merchant instructions, the applicable merchant agreement or data-processing terms will govern that processing. Where we determine purposes required for compliance, fraud prevention, card-scheme operation, settlement or legal obligations, we may act as an independent controller.

7. Sharing and recipients

- Banks, safeguarding or settlement institutions, card issuers, acquirers and correspondent/payment institutions involved in executing or settling a transaction.
- Card schemes and payment networks, including for authorisation, clearing, dispute handling, fraud monitoring and scheme compliance.
- Payment gateways, processors, tokenisation providers, 3-D Secure/authentication providers and other technical payment vendors.
- Identity-verification, sanctions/PEP screening, fraud-prevention and compliance service providers.
- Cloud hosting, cybersecurity, monitoring, communications, CRM, customer-support, analytics and professional service providers.
- Auditors, legal advisers, insurers, consultants and potential transaction counterparties under appropriate confidentiality safeguards.
- Competent regulators, law-enforcement bodies, courts, tax authorities, financial-intelligence units or other public authorities where disclosure is required or legally permitted.
- A successor, purchaser or reorganisation participant in connection with a merger, acquisition, financing, asset transfer or restructuring, subject to applicable law.

We do not sell personal data as a standalone product. We do not disclose personal data to advertisers for their own unrelated direct-marketing purposes without an appropriate legal basis.

8. International transfers

Because payments and card networks operate internationally, personal data may be processed in Switzerland, the European Economic Area, the United Kingdom and other jurisdictions in which our payment, banking, compliance or technology partners operate. Where required, we use recognised transfer mechanisms such as adequacy decisions, contractual safeguards (including standard contractual clauses), or other lawful transfer bases. Transaction data may also be transmitted internationally where necessary to execute a payment or comply with legal and network requirements.

9. Retention

We keep personal data only for as long as reasonably necessary for the purposes for which it was collected and for any longer period required by financial-services, AML, tax, accounting, card-scheme, dispute, limitation or other applicable rules. Retention periods therefore vary by data category and service.

- Account and contract records: generally for the customer relationship and applicable legal limitation/record-retention periods thereafter.

- KYC/KYB and AML records: for the period required by applicable Swiss AML obligations and any other law governing the service.
- Transaction, settlement, refund and chargeback records: for the period needed to complete processing, reconciliation, card-scheme disputes, audits and legal record-keeping.
- Security logs: for a period proportionate to cybersecurity, fraud and incident-investigation needs.
- Consent and marketing-preference records: while relevant and for an appropriate evidentiary period after withdrawal or opt-out.
- Cookie identifiers: according to the lifespan described in the Cookies Policy or the settings of the relevant provider.

10. Automated monitoring and decisions

We may use automated tools to score transaction, account, device or merchant risk and to identify activity requiring additional verification or review. These tools can result in a transaction being paused, challenged, declined or sent for manual review. Where applicable law grants a right relating to decisions based solely on automated processing that produce legal or similarly significant effects, you may request appropriate human review and exercise the rights available under that law.

11. Security

- Encryption in transit and appropriate encryption or protection at rest where relevant.
- Role-based access controls, authentication controls and least-privilege access.
- Logging, monitoring, vulnerability management, incident response and security testing.
- Tokenisation or masking of card data where supported by the payment architecture.
- Segregation of production environments and controls over administrative access.
- Vendor due diligence and contractual security/data-protection requirements where appropriate.

No system can be guaranteed to be completely secure. Users and merchants must also protect their credentials, devices, integration secrets and API keys, and must notify us promptly of suspected compromise.

12. Your rights

Depending on your location and the law applicable to the processing, you may have rights to request access, correction, deletion, restriction, objection, data portability, withdrawal of consent, or information about certain disclosures or automated processing. These rights are subject to legal exceptions, including financial-services record-retention and AML restrictions.

To make a request, contact us using the details below. We may need to verify your identity before acting on a request. If we cannot comply, we will explain the applicable reason where the law permits us to do so.

13. Children and vulnerable users

The services are not directed to children and may be used only by persons who have the legal capacity required for the relevant service. We do not knowingly open payment accounts or merchant accounts for minors unless a specific service and applicable law expressly permit it.

14. Cookies and similar technologies

The website and web applications may use strictly necessary cookies and similar technologies for authentication, security, load balancing and session management, and may use preference, analytics or other optional technologies subject to applicable consent requirements. More information is provided in the FX Rails Cookies Policy.

15. Merchant responsibilities for personal data

- Provide transparent privacy notices to cardholders, customers and website visitors.
- Collect and transmit only the data necessary for legitimate payment and business purposes.
- Maintain appropriate PCI DSS scope and security controls for the selected integration model.
- Use personal data received through FX Rails only for lawful purposes connected with the underlying transaction and customer relationship.
- Respond to data-subject requests where the merchant is the relevant controller and cooperate with FX Rails where responsibilities overlap.
- Notify FX Rails without undue delay of a security incident that could affect payment data, credentials, integration keys or personal data exchanged with FX Rails.

16. Complaints and supervisory authorities

You may contact us first so that we can investigate a privacy concern. Depending on the applicable law, you may also have the right to contact a competent data-protection authority. Nothing in this Policy limits rights that cannot lawfully be waived.

17. Changes to this Policy

We may update this Policy to reflect changes in law, regulation, payment functionality, technology, counterparties or business practices. We will publish the updated version and change the effective date. Where required, we will provide additional notice before a material change takes effect.

Company information and contact

Legal name	FX Rails AG
Swiss UID / registration number	CHE-403.817.123
Registered address	Seefeldstrasse 219, 8008 Zurich, Switzerland
Website	https://fx-rails.com/
Customer contact	customer@silvo.io
SRO information	VQF; membership no. 101231 (per FX Rails corporate website)