Cookies Policy

Information about cookies and similar technologies used on fx-rails.com and related FX Rails web interfaces.

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. What this Policy covers

This Cookies Policy explains how FX Rails AG uses cookies, local storage, pixels, SDK-like web technologies and similar tools on fx-rails.com and related web interfaces. It should be read together with the FX Rails Privacy Policy.

The actual technologies used may change as the website, security controls, analytics stack and payment integrations evolve. Where required by law, optional technologies will not be used until you provide consent through the cookie banner or preference centre.

2. What cookies are

Cookies are small text files stored on a browser or device when a website is visited. Similar technologies can store or access identifiers in local storage, measure page interactions, support authentication or enable security functions. Some are set directly by FX Rails (first-party); others may be set by service providers whose components are used on the website (third-party).

3. Categories we may use

Category	Purpose	Consent	Typical duration
Strictly necessary	Authentication, session continuity, security, fraud prevention, load balancing, consent storage and core website functions.	Usually not required where strictly necessary for a service requested by the user.	Session or limited persistent period, depending on function.
Preferences	Remember language, display choices and optional interface preferences.	Consent may be required depending on jurisdiction and implementation.	From session-only to several months.
Analytics and performance	Understand page performance, navigation patterns, errors and aggregate usage so we can	Used only with consent where required.	Typically days to months, depending on provider/configuration.

	improve the service.		
Fraud and security signals	Identify suspicious sessions, automated abuse, account takeover and payment-related security risks.	May be treated as necessary where essential for security; otherwise consent rules apply.	Session to risk-appropriate retention period.
Marketing/measurement	Measure campaigns or personalise marketing if FX Rails enables such tools.	Consent required where applicable.	Provider-dependent; disclosed in the preference centre when enabled.

4. Payment and acquiring-related technologies

Checkout, card-transfer or merchant acquiring functionality may load components operated by payment gateways, acquirers, card schemes, authentication providers, fraud-prevention providers or banks. These components may use cookies, device identifiers, local storage or similar signals to authenticate a user, support 3-D Secure, prevent card testing, detect fraud, route a payment or maintain transaction security.

Where a third-party payment page or iframe is used, that provider may set technologies under its own privacy and cookie rules. Some security and payment technologies are necessary to provide the transaction requested by the user and may therefore be enabled independently of optional analytics or marketing choices, subject to applicable law.

5. Consent and preference management

Where consent is required, the website will provide a mechanism to accept, reject or manage non-essential technologies. Withdrawing consent does not affect the lawfulness of processing that occurred before withdrawal. Strictly necessary technologies may remain active because disabling them can prevent login, fraud protection or other core functionality.

You can also control cookies using browser settings. Blocking all cookies may prevent parts of the website, account or payment flow from functioning correctly. Deleting cookies may reset preferences and require re-authentication.

6. Cookie register and transparency

Because the precise set of cookies depends on the deployed production configuration, FX Rails should maintain an up-to-date cookie register in its consent-management tool or website settings. The register should identify, where applicable, the cookie/technology name, provider, purpose, category, retention period and whether data is transferred outside Switzerland or the EEA.

If the live website does not yet expose a detailed cookie list, this Policy does not create a representation that a particular analytics or marketing provider is currently in use. Users should rely on the live preference centre for the technologies actually deployed at the time of their visit.

7. Legal bases

Strictly necessary cookies are used where required to provide a service requested by the user or to support essential security and platform operations. Optional analytics, preference or marketing technologies are based on consent where applicable law requires it. In jurisdictions where another lawful basis is available, FX Rails will apply the basis permitted for the relevant technology and processing purpose.

8. International processing

Some cookie and technology providers may process information outside Switzerland or the EEA. Where required, FX Rails uses appropriate transfer safeguards or selects providers whose processing is covered by an applicable adequacy mechanism. More information about international transfers is provided in the Privacy Policy.

9. Do Not Track and similar browser signals

Browser-level privacy signals are interpreted in accordance with applicable law and the technical capabilities of the website. Because standards for some signals remain inconsistent, the FX Rails consent or preference interface is the primary method for managing optional cookies unless mandatory law requires a different mechanism.

10. Merchant websites using FX Rails

A merchant integrating FX Rails payment or acquiring components remains responsible for its own website cookie notice and consent mechanism. The merchant should accurately disclose any FX Rails or third-party payment components that set or access cookies or similar technologies through the merchant website and should configure the integration consistently with applicable e-privacy and data-protection rules.

11. Security

Cookies or local-storage values should never be treated as a substitute for secure authentication. FX Rails applies security measures intended to protect sessions and may rotate, expire or invalidate cookies when risk indicators are detected. Users should not share authentication cookies, session tokens or browser profiles with unauthorised persons.

12. Changes to this Policy

We may update this Policy when website functionality, consent requirements or technology providers change. The current version will be published on fx-rails.com with an updated effective date. Material changes will be presented through an appropriate notice where required.

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)