PRIVACY POLICY

Last updated: 23.09.2026

This Privacy Policy applies exclusively to personal data of natural persons (including individuals connected to a business customer in B2B relationships).

Our Website and Services are not directed at individuals under the age of 18 (or the applicable age of majority). We do not knowingly collect personal data from minors.

1. DATA CONTROLLER

Foxo Solutions AG ("**Company**", "**we**", "**us**" or "**our**") is a company incorporated under the laws of Switzerland, with registered office at Office 13, Turmstrasse 28, 6312 Steinhausen, registered in the Commercial Register of the Canton of Zug under number CHE238.153.127.

For purposes of the Swiss Federal Act on Data Protection ("**FADP**"), Company acts as the controller of personal data covered by this Privacy Policy where Company determines the purposes and means of processing.

As used in this Privacy Policy, "you" and "your" refer to the individual whose personal data we process.

2. SCOPE OF THIS PRIVACY POLICY

This Privacy Policy applies to personal data relating to:

- customers who use this website and any related webpages or online interfaces made available by the Company ("**Website")** directly;
- individuals connected to a customer in the Business-to-Business ("**B2B**") relationships, such as directors, officers, beneficial owners, authorized signatories, personal guarantors, and employees
- prospective customers and business contacts;
- individuals who communicate with us; and
- visitors to our Website.

This Privacy Policy applies to personal data that we process in connection with:

- our websites and online platforms;
- applications for our services;
- communications with us; and
- business development and prospective customer relationships.

This Privacy Policy also applies to data processing conducted in the context of contractual B2B relationships, in addition to any separate agreement(s) governing such relationships. Where, in the context of a B2B relationship, Company processes personal data solely on behalf of and in accordance with its documented instructions of business customer, Company may act as a processor rather than as an independent controller.

3. PERSONAL DATA WE PROCESS

We process personal data that is necessary and proportionate for the purposes described in this Privacy Policy.

The categories of personal data we process depend on your relationship with us.

3.1 Personal data provided by you

Depending on the circumstances, this may include:

Contact information

- full name;
- business or personal email address;
- telephone number;
- postal or residential address;
- country of residence;
- job title; and
- other contact details.

Your communications and correspondence

We may process:

- emails;
- support requests;
- messages;
- information provided to our sales or compliance teams;
- complaints;
- feedback;
- documents and files you provide; and
- other information contained in communications with us.

3.2 Personal data provided in the context of contractual B2B relationships

If you, or someone at a business customer, initiates communication with us, we collect the same categories listed above (Section 3.1) in relation to the business customer's representatives (for example, directors, signing officers, or beneficial owners) with **Contact Information** additionally including employer and job title, as well as the following information specific to B2B relationships:

- ownership and control information (shareholding percentage, control chain).
- personal information you give us about co-workers, contractors, or vendors, such as their name, email, phone number, employer, or job title.

3.3 Personal data we collect automatically

When you use our Website or online services, we may automatically collect certain technical and usage information.

This may include:

- IP address;
- browser type and version;
- operating system;
- device type;
- language and regional settings;
- date and time of access;
- pages and content accessed;
- referring website;
- technical identifiers;
- login and authentication information;
- security and fraud-prevention information;
- information concerning interaction with our Website or services; and
- technical logs generated by our systems.

We use this information primarily to:

- operate and secure our Website;
- authenticate users;
- prevent fraud and abuse;
- investigate security incidents;
- maintain system reliability;
- diagnose technical problems;
- monitor and improve performance; and
- understand how our Website is used.

3.4 Sources of personal data (Data collected from third parties) In addition to the data you provide directly to us and the data we collect automatically, we may obtain personal data about you from third-party sources. Such sources may include:

- publicly available sources (e.g., commercial registers, professional networks, public media);
- business partners, affiliates, or subcontractors;
- credit reference agencies, identity verification services, or compliance screening providers; and
- other third parties, to the extent permitted by applicable law.

This Privacy Policy itself provides the information required under Article 19 FADP in respect of personal data we obtain from sources other than you: the third-party sources listed above (including identity-verification and compliance-screening providers) and the categories of such data, which include identity and verification data and screening results such as sanctions, politically exposed person (PEP) and adverse-media information. We do not provide separate individual notice in addition to this Privacy Policy. Where an exception under Article 20 FADP applies, in particular in connection with our legal and anti-money-laundering obligations, the duty to inform may be restricted or may not apply.

4. COOKIES AND SIMILAR TECHNOLOGIES

We use cookies, local storage and similar technologies on the Website for the following purposes:

- operating the Website;
- maintaining secure sessions;
- authenticating users;
- maintaining security;
- remembering necessary technical settings;
- providing functionality requested by you; and
- analysing the use of the Website.

You may reject or disable cookies and similar technologies through the mechanisms made available on the Website or through your browser settings, as applicable under Article 45c of the Swiss Telecommunications Act (TCA). Disabling certain technologies may affect the functionality of the Website.

5. PURPOSES OF PROCESSING

We process personal data only for specific purposes that are recognizable to you and only to the extent necessary and proportionate for those purposes.

Depending on the circumstances, we may process personal data to:

5.1 Establish and manage relationships

We may process personal data to:

- assess prospective customers;
- communicate with prospective customers;
- conduct onboarding;
- conduct due diligence;
- negotiate and enter into agreements;
- manage customer relationships; and
- maintain appropriate business records.

5.2 Security and fraud prevention

We may process personal data to:

- protect our systems;
- detect unauthorized access;
- investigate security incidents;
- prevent fraud;
- protect our customers and counterparties;
- monitor unusual activity; and
- maintain the integrity and security of our services.

5.3 Communications

We may use personal data to:

- respond to enquiries;
- provide customer support;
- provide information concerning the Services;
- notify you about material changes to the Services;
- communicate about accounts; and
- communicate about our business relationship with you.

Where we send promotional communications, we will comply with applicable law, including applicable requirements under Article 3(1)(o) of the Swiss Federal Act on Unfair Competition (UCA), and provide any required means to object or unsubscribe.

5.4 Legal claims and corporate matters

We may process personal data where necessary to:

- establish;
- exercise;
- enforce; or
- defend legal claims or rights.

We may also process personal data in connection with mergers, acquisitions, restructurings, financing transactions, asset transfers or similar corporate transactions, subject to applicable law.

In connection with security, fraud prevention and AML/compliance screening, we may carry out profiling. We do not, however, take decisions producing legal effects concerning you or similarly significantly affecting you based solely on automated processing within the meaning of Article 21 FADP; where automated processing is used for such purposes, it is subject to human review.

We process personal data based on your consent, the necessity to perform a contract with you, our overriding legitimate interests (such as security and IT administration), or legal obligations.

6. DISCLOSURE OF PERSONAL DATA

We may disclose personal data where necessary for the purposes described in this Privacy Policy.

Recipients may include the following categories.

6.1 Affiliated Companies

We may disclose personal data to affiliated companies where necessary for:

- offering and promoting our Services;
- managing relationships with prospective customers;
- internal administration and management;
- compliance and risk management;
- information security; or
- other purposes described in this Privacy Policy.

6.2 Service Providers and Processors

We may use service providers for:

- hosting;
- cloud infrastructure;
- IT;
- cybersecurity;
- communications;
- customer support;
- identity verification;
- fraud prevention;
- compliance screening;
- document management;
- professional services; and
- other operational functions.

Where a service provider acts as our processor, we require it to process personal data in accordance with our instructions and applicable data protection requirements.

6.3 Professional Advisers

We may disclose personal data to:

- lawyers;

- accountants;
- auditors;
- compliance advisers;
- consultants; and
- other professional advisers

where necessary for the provision of their services to us.

6.4 Potential Buyers or Investors

We may disclose personal data to potential buyers, investors, financing parties or their professional advisers where necessary in connection with a proposed or actual:

- merger;
- acquisition;
- investment;
- financing;
- restructuring;
- sale of assets; or
- other corporate transaction.

Such disclosure will be limited to information necessary for the relevant transaction and carried out in accordance with applicable law.

6.5 Public Authorities

We may disclose personal data to:

- courts;
- regulators;
- supervisory authorities;
- law enforcement authorities;
- tax authorities;
- the Money Laundering Reporting Office Switzerland (MROS), where applicable; and
- other competent public authorities

where disclosure is required or permitted by applicable law or legal process.

Where applicable, disclosures to foreign authorities will be made subject to applicable Swiss legal requirements and restrictions.

7. INTERNATIONAL DATA TRANSFERS

We may process or disclose personal data outside Switzerland.

Where personal data is disclosed abroad, we comply with the requirements applicable to international transfers under Articles 16 and 17 of the FADP.

Depending on the destination, a disclosure may be based on:

- an adequate level of data protection recognized under Swiss law in the destination state, as determined by the Federal Council (Article 16(1) FADP);
- appropriate safeguards recognized under Swiss law providing sufficient protection under Article 16(2) FADP, in particular standard data protection clauses approved, issued or recognized by the Federal Data Protection and Information Commissioner (FDPIC);
- binding corporate rules, where applicable;
- another recognized safeguard; or
- an exception permitted by applicable law under Article 17 FADP (for example, your express consent or the necessity of the disclosure for the performance of a contract).

Our service providers may operate infrastructure in Switzerland, the European Economic Area, the United Kingdom or other jurisdictions.

The actual countries involved depend on the service providers and technologies used by Company.

Where a destination country does not provide an adequate level of protection under Swiss law, we will take the measures required by the FADP before making the relevant disclosure, unless an applicable statutory exception applies.

8. DATA RETENTION

Retention periods therefore vary depending on the category of data and the purpose of processing.

Indicative periods include:

Category	Indicative retention
Customer contact information	24 months after the end of the use of the Website or termination of the relationship
Customer support communications	24 months after the resolution of the request
Consent records	10 years after the withdrawal of consent
Security and access logs	10 months (or longer if required for an ongoing security investigation)

Website technical logs	7 days
AML/KYC records (where the Company acts as a financial intermediary)	10 years after the end of the business relationship or completion of the transaction (Article 7 AMLA/GwG)

Where applicable law imposes a mandatory retention period, that period prevails.

After the applicable retention period expires, we securely delete, destroy or anonymize the relevant personal data unless further retention is required by law or necessary to establish, exercise or defend legal claims.

9. YOUR RIGHTS UNDER SWISS DATA PROTECTION LAW

Subject to the conditions and limitations established by Swiss law, you may have the right to:

- request information on whether we process personal data concerning you and the information you need to assert your rights (right of access, Article 25 FADP);
- request correction of inaccurate personal data;
- request deletion or destruction of personal data where the legal requirements for deletion are satisfied;
- object expressly to specific processing activities (further processing will then require a justification under Article 31 FADP);
- request that specific processing or specific disclosures to third parties be prohibited, or that a note of dispute be added where the accuracy of data cannot be established (Article 32 FADP);
- request the delivery or transfer of your personal data in a commonly used electronic format (data portability) where the requirements of Articles 28 and 29 FADP are met;
- withdraw your consent at any time, where processing is based on consent, without affecting the lawfulness of processing based on consent before its withdrawal; and
- exercise any other rights available under applicable Swiss law.

These rights are not absolute.

For example, we may be entitled or required to continue processing or retaining personal data because of legal, regulatory, contractual, security or evidentiary requirements.

To exercise a data protection right or ask a question about our processing of your personal data, contact us. We will process requests within 30 days.

To protect against unauthorized disclosure of personal data, we may request reasonable information necessary to verify your identity before responding to a request.

Where a request cannot be fulfilled in whole or in part, we will explain the applicable reason to the extent permitted by law.

10. DATA SECURITY

We maintain appropriate technical and organizational measures designed to protect personal data against unauthorized access, unauthorized disclosure, loss, destruction, alteration, misuse, and other unlawful or unauthorized processing, depending on the nature of the processing and the risks involved. No method of transmission or storage can be guaranteed to be completely secure.

In the event of a data breach that is likely to result in significant harm to you, we will notify the Federal Data Protection and Information Commissioner (FDPIC) and, where required by applicable law, inform you without undue delay.

11. COMPLAINTS AND THE FDPIC

If you have any questions or concerns about how we process your personal data, or if you wish to exercise your rights under Swiss law, please contact us at:

Email: info@foxosolutions.ch

You may also contact the competent Swiss supervisory authority:

Federal Data Protection and Information Commissioner (FDPIC)
Feldeggweg 1, 3003 Bern, Switzerland

Website: edoeb.admin.ch.

12. APPLICABLE DATA PROTECTION LAW

This Privacy Policy is primarily intended to explain our processing of personal data under applicable Swiss data protection law, including:

- the Swiss Federal Act on Data Protection (FADP);
- the Data Protection Ordinance (DPO); and
- other Swiss laws applicable to particular processing activities.

Where other mandatory data protection laws apply to a particular processing activity, we will comply with those laws to the extent applicable.

This Privacy Policy does not limit any mandatory rights or protections available to data subjects under applicable law.

13. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time.

We will publish the updated version on our Website and indicate the date on which it was last updated.

Where a change materially affects the manner in which we process personal data and applicable law requires additional notice, we will provide the required notice.

Where processing requires consent under applicable law, we will obtain the required consent before carrying out the relevant processing.