GLOBAL TRADE INVEST LIMITED · WEBSITE LEGAL

Privacy & Data Protection

Public Website | Version PRE-LAUNCH | Effective: Controlled working copy

This public legal document forms part of the corporate and website documentation of GLOBAL FIX BOND. Programme-specific Transaction Documents are provided separately to admitted prospective and actual investors through authorised channels or the secure Investor Portal.

1. Scope of this Privacy Notice

This Privacy & Data Protection Notice explains how GLOBAL TRADE INVEST LIMITED processes personal data in connection with the public website, private-offering enquiries, onboarding, KYC/AML review, the Investor Portal, Note administration, payments, redemptions, communications, security and related Programme operations.

It applies to prospective and actual investors and, for legal entities, relevant directors, authorised representatives, beneficial owners, controlling persons and signatories. More detailed controlled Programme privacy information may also be provided during onboarding or through the Investor Portal.

2. Controller and contact

The controller is GLOBAL TRADE INVEST LIMITED, company number 06874711, registered office 167-169 Great Portland Street, 5th Floor, London W1W 5PF, United Kingdom. Privacy and data-rights requests: privacy@globalfix.bond.

General investor enquiries may be sent to investors@globalfix.bond.

3. Privacy framework

Depending on the circumstances, processing may be subject to the UK GDPR, the Data Protection Act 2018 as amended including changes introduced by the Data (Use and Access) Act 2025, and the Swiss Federal Act on Data Protection (FADP). The EU GDPR may additionally apply where its territorial scope is engaged. Other mandatory privacy rules may also apply where required.

Independent recipients such as banks, professional advisers, the Swiss Escrow / Paying Agent or public authorities may process personal data under their own legal responsibilities.

4. Personal data we may process

We may process identity, contact, nationality, residence, tax and identification-document data; beneficial-ownership and corporate-authority data; KYC/AML, PEP, sanctions, fraud, adverse-information and risk-review data; Source of Funds and Source of Wealth information; bank-account information; subscription, Note, payment, fee and redemption records; communications; Portal, authentication, device, IP, session, security and audit-log data; and limited public-website analytics and performance information such as page or route, referrer, country-level location, device category, browser, operating system and web-performance measurements.

We seek to collect only information reasonably required for the relevant purpose.

5. Sources of data

Data may be obtained directly from the individual or an authorised representative, from a legal-entity investor, through the website or Portal, through Sales Persons or Introducers, from banks and professional service providers, or from lawful public and commercial sources used for identity, company, beneficial-ownership, sanctions, PEP, fraud and adverse-information checks.

Where another person provides information about an individual, that person should be authorised to do so and should direct the individual to relevant privacy information where appropriate.

6. Purposes and lawful bases

We process data to manage enquiries and admissions; conduct onboarding and KYC/AML, sanctions, PEP, fraud, Source of Funds and Source of Wealth controls; administer subscriptions, funding, Notes, Certificates, payments and redemptions; maintain the Official Note Register and document records; operate and secure the Portal; understand aggregate use of the public website and measure real-user performance; investigate incidents; maintain audit trails; manage distribution relationships; comply with legal obligations; and establish, exercise or defend legal claims.

Depending on the activity, lawful bases may include steps before entering a contract, performance of a contract, legal obligations, legitimate interests, legal claims and, in limited cases, consent where required.

7. KYC, screening and automated tools

Identity documents and verification data may be used to confirm identity, document validity, beneficial ownership, authority and compliance status. Specialist providers may support identity verification, sanctions/PEP screening, fraud detection, adverse-information review and risk scoring.

Automated tools may generate matches, scores or alerts, but material onboarding or compliance decisions may be subject to human review. If solely automated significant decision-making is introduced, additional legally required information and safeguards will be provided.

8. Portal, security and transaction data

Invitation, account-activation, authentication, MFA, session, device, browser, IP, login, security-event and audit data are processed to operate the Portal, protect accounts, investigate suspicious activity and evidence sensitive instructions. First-time access and recovery may use time-limited security links and dedicated activation records. Sensitive actions may require renewed authentication or separate email confirmation.

We also process verified payment destinations, funding records, Note balances, fee records, redemption instructions and settlement evidence to perform and reconcile Programme administration.

9. Recipients and distribution relationships

We do not sell personal data and do not disclose KYC or identity records for unrelated third-party marketing or other unrelated commercial purposes. Where necessary and lawful, data may be disclosed to the Swiss Escrow / Paying Agent; banks and payment providers; KYC/AML, identity, sanctions, PEP and fraud providers; cloud, hosting, authentication, cybersecurity, document, email and communications providers; professional advisers; authorised Sales Persons or Introducers on a strict need-to-know basis; and competent courts, regulators, law-enforcement bodies or tax authorities.

We may internally record the Sales Person, Family Office or Introducer associated with an investor for relationship, reporting and commission-administration purposes. That attribution does not itself grant access to KYC documents, identity evidence, bank-account details, Source of Funds or Source of Wealth records, or internal compliance notes. Any partner-facing access is separately authorised and technically restricted.

10. International transfers

The Programme is cross-border and data may be processed in the United Kingdom, Switzerland and other countries where approved service providers operate. Where applicable law requires a transfer mechanism or safeguard, we use an appropriate adequacy basis, recognised contractual clauses or another lawful transfer mechanism.

Where Swiss FADP transparency requirements apply, information about destination countries and relevant safeguards may be provided in controlled privacy information or on appropriate request.

11. Blockchain and digital-proof records

The Programme may create cryptographic evidence for Certificates and material lifecycle events. The intended public-chain design does not place investor names, addresses, identity documents, Principal Amounts, Note Unit balances, accrued returns or redemption amounts on Ethereum Mainnet.

Certificate or lifecycle records may be hashed and included in a privacy-preserving weekly Merkle structure, with only a non-readable Merkle root and related public transaction data anchored publicly. Blockchain evidence does not determine legal title.

12. Retention and security

We retain personal data for as long as reasonably required for the relevant purpose and for applicable legal, contractual, accounting, tax, KYC/AML, fraud-prevention, audit, limitation, dispute and evidentiary requirements. Different categories may have different retention periods.

We use technical and organisational measures designed to protect data, including role-based access, MFA, restricted storage, encryption where appropriate, audit logging, secure document delivery, automatic inactivity sign-out, backups, monitoring, vendor controls and incident-response procedures. Access to sensitive records is limited according to role and operational need, and material access or lifecycle events may be auditable. No internet-based system can be guaranteed absolutely secure.

13. Individual rights and complaints

Subject to applicable law and exemptions, individuals may have rights of access, correction, erasure, restriction, objection, portability and information about certain automated decisions. Rights may be limited where records must be retained for legal, compliance, contractual, tax, accounting, fraud-prevention, evidentiary or legal-claim purposes. We may verify identity before acting on a request.

Privacy concerns may be sent to privacy@globalfix.bond. This does not affect statutory rights to complain to a competent supervisory authority, including the UK Information Commissioner's Office where UK law applies or the Swiss FDPIC/EDOEB where the FADP applies.

14. Cookies, marketing, children and updates

The website and Portal use cookies or similar storage technologies where necessary for authentication, security, session management, language and appearance. More information is in the Cookie & Browser Storage Policy. Optional analytics or advertising technologies will be accompanied by appropriate transparency and preference or consent controls where required.

Operational and servicing messages are not marketing. Direct marketing is sent only where permitted by applicable law. The Programme is intended for adults and legal entities acting through adults and is not directed to children. We may update this notice for legal, regulatory, operational, security or technology changes; the current version and effective date will be published here.