GLOBAL TRADE INVEST LIMITED · WEBSITE LEGAL

Datenschutz & Datenverarbeitung

Öffentliche Website | Version PRE-LAUNCH | Wirksam ab: Kontrollierte Arbeitsfassung

Dieses öffentliche Rechtsdokument gehört zur Corporate- und Website-Dokumentation von GLOBAL FIX BOND. Programmspezifische Transaktionsdokumente werden zugelassenen Interessenten und Anlegern separat über autorisierte Kanäle oder das sichere Investor Portal bereitgestellt.

1. Geltungsbereich

Dieser Datenschutz- und Datenverarbeitungshinweis erläutert, wie GLOBAL TRADE INVEST LIMITED personenbezogene Daten im Zusammenhang mit der öffentlichen Website, Private-Offering-Anfragen, Onboarding, KYC/AML-Prüfung, Investor Portal, Note Administration, Payments, Redemptions, Kommunikation, Security und sonstigen Programme-Prozessen verarbeitet.

Er gilt für potenzielle und tatsächliche Investors sowie bei Legal Entities für relevante Directors, Authorised Representatives, Beneficial Owners, Controlling Persons und Signatories. Ergänzende kontrollierte Privacy Information kann während des Onboarding oder im Investor Portal bereitgestellt werden.

2. Verantwortlicher und Kontakt

Verantwortlicher ist GLOBAL TRADE INVEST LIMITED, Company No. 06874711, Registered Office 167-169 Great Portland Street, 5th Floor, London W1W 5PF, United Kingdom. Datenschutz- und Data-Rights-Anfragen: privacy@globalfix.bond.

Allgemeine Investor-Anfragen: investors@globalfix.bond.

3. Datenschutzrahmen

Je nach Umständen können UK GDPR, Data Protection Act 2018 in geänderter Fassung einschließlich der Änderungen durch den Data (Use and Access) Act 2025 sowie das Schweizer Bundesgesetz über den Datenschutz (DSG/FADP) Anwendung finden. Die EU GDPR kann zusätzlich gelten, wenn ihr territorialer Anwendungsbereich eröffnet ist.

Unabhängige Empfänger wie Banken, Professional Advisers, Swiss Escrow / Paying Agent oder Behörden können Daten aufgrund eigener rechtlicher Verantwortlichkeiten verarbeiten.

4. Verarbeitete Datenkategorien

Wir können Identity-, Contact-, Nationality-, Residence-, Tax- und Identification-Document-Daten; Beneficial-Ownership- und Corporate-Authority-Daten; KYC/AML-, PEP-, Sanctions-, Fraud-, Adverse-Information- und Risk-Review-Daten; Source-of-Funds- und Source-of-Wealth-Informationen; Bank- und verifizierte Wallet-Daten; Subscription-, Note-, Payment-, Fee- und Redemption-Records; Communications; Portal-, Authentication-, Device-, IP-, Session-, Security- und Audit-Log-Daten sowie begrenzte öffentliche Website-Analytics- und Performance-Informationen wie Page/Route, Referrer, Land auf aggregierter Ebene, Device-Kategorie, Browser, Betriebssystem und Web-Performance-Messwerte verarbeiten.

Es sollen nur Daten erhoben werden, die für den jeweiligen Zweck angemessen erforderlich sind.

5. Datenquellen

Daten können direkt von der betroffenen Person oder einem Authorised Representative, von Legal Entity Investors, über Website oder Portal, durch Sales Persons oder Introducers, von Banken und Professional Service Providers sowie aus rechtmäßigen öffentlichen und kommerziellen Quellen für Identity-, Company-, Beneficial-Ownership-, Sanctions-, PEP-, Fraud- und Adverse-Information-Prüfungen stammen.

Wer Daten über eine andere Person bereitstellt, sollte hierzu befugt sein und gegebenenfalls auf die relevante Privacy Information hinweisen.

6. Zwecke und Rechtsgrundlagen

Wir verarbeiten Daten zur Bearbeitung von Anfragen und Admissions; für Onboarding und KYC/AML-, Sanctions-, PEP-, Fraud-, Source-of-Funds- und Source-of-Wealth-Kontrollen; zur Administration von Subscriptions, Funding, Notes, Certificates, Payments und Redemptions; zur Pflege des Official Note Register und kontrollierter Dokumente; zum Betrieb und Schutz des Portals; zur aggregierten Analyse der Nutzung der öffentlichen Website und Messung realer Performance; für Incident Investigation, Audit Trails, Distribution Relationships, gesetzliche Pflichten und Rechtsansprüche.

Rechtsgrundlagen können vorvertragliche Maßnahmen, Vertragserfüllung, gesetzliche Verpflichtungen, berechtigte Interessen, Rechtsansprüche und in begrenzten Fällen Consent sein.

7. KYC, Screening und automatisierte Tools

Identity Documents und Verification Data können zur Bestätigung von Identität, Document Validity, Beneficial Ownership, Authority und Compliance Status verwendet werden. Spezialanbieter können Identity Verification, Sanctions-/PEP-Screening, Fraud Detection, Adverse-Information Review und Risk Scoring unterstützen.

Automated Tools können Matches, Scores oder Alerts erzeugen; materielle Onboarding- oder Compliance-Entscheidungen können Human Review unterliegen. Bei ausschließlich automatisierten erheblichen Entscheidungen werden die gesetzlich erforderlichen Informationen und Safeguards bereitgestellt.

8. Portal-, Security- und Transaction-Daten

Invitation-, Account-Activation-, Authentication-, MFA-, Session-, Device-, Browser-, IP-, Login-, Security-Event- und Audit-Daten werden verarbeitet, um das Portal zu betreiben, Accounts zu schützen, suspicious activity zu untersuchen und sensitive Instructions nachzuweisen. Erstzugang und Recovery können zeitlich begrenzte Security-Links und eigene Activation Records verwenden; sensible Aktionen können erneute Authentifizierung oder eine separate E-Mail-Bestätigung erfordern.

Verifizierte Payment Destinations, Funding Records, Note Balances, Fee Records, Redemption Instructions und Settlement Evidence werden zur Programme-Administration und Reconciliation verarbeitet.

9. Empfänger und Distribution Relationships

Personenbezogene Daten werden nicht verkauft und KYC- oder Identitätsunterlagen nicht für unabhängiges Drittmarketing oder andere sachfremde kommerzielle Zwecke offengelegt. Soweit erforderlich und rechtmäßig, können Daten an Swiss Escrow / Paying Agent; Banken und Payment Providers; KYC/AML-, Identity-, Sanctions-, PEP- und Fraud-Provider; Cloud-, Hosting-, Authentication-, Cybersecurity-, Document-, E-Mail- und Communications-Provider; Professional Advisers; autorisierte Sales Persons oder Introducers auf strikter Need-to-Know-Basis sowie zuständige Gerichte, Regulators, Law-Enforcement Bodies oder Tax Authorities offengelegt werden.

Der einem Investor intern zugeordnete Sales Person, Family Office oder Introducer kann für Relationship-, Reporting- und Commission-Zwecke gespeichert werden. Diese Zuordnung gewährt für sich genommen keinen Zugriff auf KYC-Dokumente, Ausweisdaten, Bankkonto-Daten, Source-of-Funds- oder Source-of-Wealth-Unterlagen oder interne Compliance-Notizen. Jeder Partnerzugriff wird separat autorisiert und technisch beschränkt.

10. Internationale Datenübermittlungen

Das Programme ist grenzüberschreitend. Daten können im Vereinigten Königreich, in der Schweiz und in anderen Ländern zugelassener Service Provider verarbeitet werden. Soweit anwendbares Recht Safeguards verlangt, verwenden wir eine geeignete Adequacy-Grundlage, anerkannte Contractual Clauses oder einen anderen rechtmäßigen Transfermechanismus.

Soweit schweizerische Transparenzpflichten gelten, können Informationen zu Destination Countries und Safeguards in kontrollierter Privacy Information oder auf angemessene Anfrage bereitgestellt werden.

11. Blockchain und Digital Proof

Das Programme kann kryptographische Evidence für Certificates und wesentliche Lifecycle Events erzeugen. Investor Names, Addresses, Identity Documents, Principal Amounts, Note Unit Balances, Accrued Returns oder Redemption Amounts werden nach dem vorgesehenen Design nicht auf Ethereum Mainnet geschrieben.

Records können gehasht und in eine datenschutzschonende wöchentliche Merkle-Struktur aufgenommen werden; öffentlich verankert werden nur nicht lesbare Merkle Roots und zugehörige Public Transaction Data. Blockchain Evidence bestimmt nicht den Legal Title.

12. Aufbewahrung und Sicherheit

Daten werden so lange aufbewahrt, wie dies für den jeweiligen Zweck und für anwendbare Legal-, Contractual-, Accounting-, Tax-, KYC/AML-, Fraud-Prevention-, Audit-, Limitation-, Dispute- und Evidence-Anforderungen angemessen erforderlich ist.

Zum Schutz werden unter anderem Role-Based Access, MFA, Restricted Storage, Encryption soweit angemessen, Audit Logging, Secure Document Delivery, automatische Abmeldung bei Inaktivität, Backups, Monitoring, Vendor Controls und Incident-Response-Verfahren eingesetzt. Der Zugriff auf sensible Records wird nach Rolle und operativer Erforderlichkeit beschränkt; wesentliche Zugriffs- oder Lifecycle-Ereignisse können auditierbar protokolliert werden. Absolute Sicherheit kann nicht garantiert werden.

13. Rechte und Beschwerden

Vorbehaltlich anwendbaren Rechts und gesetzlicher Ausnahmen können Rechte auf Access, Correction, Erasure, Restriction, Objection, Portability und Informationen über bestimmte Automated Decisions bestehen. Rechte können eingeschränkt sein, wenn Records aus Legal-, Compliance-, Contractual-, Tax-, Accounting-, Fraud-Prevention-, Evidentiary- oder Legal-Claim-Gründen aufbewahrt werden müssen.

Datenschutzanfragen: privacy@globalfix.bond. Gesetzliche Beschwerderechte bei zuständigen Aufsichtsbehörden bleiben unberührt, einschließlich ICO bei anwendbarem UK-Recht und EDÖB/FDPIC bei anwendbarem Schweizer DSG.

14. Cookies, Marketing, Minderjährige und Updates

Website und Portal verwenden Cookies oder ähnliche Storage Technologies, soweit diese für Authentication, Security, Session Management, Language und Appearance erforderlich sind. Details enthält die Cookie & Browser Storage Policy. Optionale Analytics- oder Advertising-Technologien werden erforderlichenfalls mit Preference- bzw. Consent-Controls eingeführt.

Operational- und Servicing-Messages sind kein Marketing. Das Programme richtet sich an Erwachsene und Legal Entities, die durch Erwachsene handeln. Dieser Hinweis kann an Legal-, Regulatory-, Operational-, Security- oder Technology-Änderungen angepasst werden; die aktuelle Version und das Wirksamkeitsdatum werden veröffentlicht.