

# Globridge Privacy Policy

Effective Date: April 1, 2026

This Privacy Policy describes how Globridge, Inc. (“Globridge,” “we,” “us,” or “our”) collects, uses, discloses, transfers, stores, and protects personal data when you access or use our websites, mobile applications, APIs, dashboards, payment orchestration tools, stablecoin wallet features, customer support channels, and related services (collectively, the “Services”). It also explains your rights and choices.

This Policy applies to information we collect about users, prospective users, recipients, beneficial owners, administrators, authorized users, website visitors, and other individuals whose information is processed in connection with the Services.

Some regulated products or features may be offered through banks, money transmitters, custodians, identity-verification providers, analytics vendors, or other partners that may provide separate privacy notices or process information as independent controllers. In those cases, their privacy notices apply to the information they process in their own capacity in addition to this Policy.

If you provide personal data about another person, such as a recipient or beneficial owner, you represent that you are authorized to do so and, where required by law, that you have provided them with any required notice.

## Contents

- 1. Who We Are
- 2. Personal Data We Collect
- 3. How We Collect Personal Data
- 4. How We Use Personal Data
- 5. How We Share Personal Data
- 6. International Data Transfers
- 7. Data Retention
- 8. Cookies and Similar Technologies
- 9. Automated Decision-Making and Profiling
- 10. Your Rights and Choices
- 11. Data Security
- 12. Children’s Privacy
- 13. Third-Party Services
- 14. Changes to This Policy and Contact Information

## **1. Who We Are**

Globridge, Inc. is generally the controller of personal data described in this Policy. For certain regulated financial services, a banking, custody, payout, or money transmission partner may separately control or co-control some information it receives to provide those services.

Privacy contact: [privacy@globridge.com](mailto:privacy@globridge.com)

## **2. Personal Data We Collect**

### **2.1 Identifiers and Contact Information**

We may collect your name, username, alias, email address, telephone number, mailing address, country of residence, nationality, date of birth, account identifiers, and similar contact or identifying details.

### **2.2 Identity, Tax, and Compliance Information**

We may collect government-issued identification information, Social Security number or tax identification number, passport or driver's license details, photos of your identification documents, selfie or liveness checks, biometric verification data or templates processed by our identity-verification providers where permitted by law, occupation, employer, tax residency, beneficial ownership information, source-of-funds or source-of-wealth information, and sanctions, politically exposed person, or fraud-screening results.

### **2.3 Financial, Payment, and Account Information**

We may collect linked bank account information, routing numbers, payment method details, card tokens, payment processor reference numbers, balances, transaction amounts, payout instructions, refund data, exchange-rate quotes, fee information, and records relating to chargebacks, returns, or disputes.

### **2.4 Recipient and Counterparty Information**

We may collect information about recipients, counterparties, beneficial owners, and authorized users, including names, bank or mobile wallet details, blockchain addresses, contact details, and the purpose of a payment or remittance where required.

### **2.5 Wallet, Blockchain, and Digital Asset Information**

We may collect wallet addresses, public keys, transaction hashes, network or chain information, asset types, on-chain interactions, blockchain screening or risk indicators, wallet-ownership or wallet-control data, and legally required originator and beneficiary information. Transactions recorded on public blockchains may be visible to other participants, validators, node operators, explorers, analytics providers, and the general public.

### **2.6 Device, Usage, and Technical Information**

We may collect IP address, device identifiers, operating system, browser type, app version, language, time zone, log data, cookie identifiers, local storage data, push-notification tokens, session data, crash reports, and approximate geolocation derived from IP or device information. Where permitted and enabled by you, we may also collect more precise location information.

### **2.7 Communications and Support Information**

We may collect emails, chat messages, customer support tickets, complaint records, survey responses, call recordings, and other communications you have with us or our service providers.

## **2.8 Marketing and Preference Information**

We may collect your communication preferences, referral or promotional participation data, survey responses, cookie choices, and information about your interactions with our emails, websites, or in-app messaging.

## **2.9 Inferences and Risk Data**

We may generate or receive risk scores, fraud indicators, compliance alerts, transaction-pattern analysis, and other inferences used to protect the Services, comply with law, and assess eligibility or risk.

Not all categories of personal data are collected from every individual, and the specific data we collect depends on how you interact with the Services and what products or corridors you use.

## **3. How We Collect Personal Data**

We collect personal data:

- directly from you, such as when you create an account, complete onboarding, link a bank account, connect a wallet, initiate a transaction, contact support, complete a survey, or submit compliance documents;
- automatically when you use the Services, such as through cookies, local storage, device logs, app analytics, session records, and network monitoring;
- from third parties, such as banks, payment processors, card networks, money transmitters, custody or wallet providers, identity-verification vendors, fraud-prevention vendors, sanctions or blockchain-analytics vendors, affiliates, public blockchains, public records, regulators, and law-enforcement or governmental sources where lawful;
- from other users or businesses, such as when someone lists you as a recipient, authorized user, beneficial owner, or business contact; and
- from integrations or APIs that you authorize us to connect to.

## **4. How We Use Personal Data**

Where required by law, we rely on one or more of the following legal bases to process personal data: performance of a contract with you, compliance with legal obligations, our legitimate interests in operating a safe and effective financial services platform, and your consent where required.

### **4.1 To Provide and Operate the Services**

We use personal data to create and administer accounts, verify access, connect payment methods, enable wallet features, process funding and payout instructions, settle fiat and digital asset transactions, manage APIs and integrations, provide receipts and transaction history, and deliver customer support.

### **4.2 To Comply with Legal and Regulatory Obligations**

We use personal data to satisfy obligations relating to customer due diligence, know-your-customer and know-your-business requirements, anti-money laundering, counter-terrorist financing, sanctions screening, fraud prevention, recordkeeping, tax reporting, consumer protection, remittance regulation, lawful requests, and audit or examination requirements.

#### **4.3 To Protect Security and Prevent Abuse**

We use personal data to detect, investigate, prevent, and respond to fraud, account compromise, suspicious transactions, abuse of the Services, cyber threats, theft, and other unlawful or harmful conduct; to authenticate users; and to enforce our Terms and other policies.

#### **4.4 To Improve, Develop, and Maintain the Services**

We use personal data to monitor performance, analyze usage, troubleshoot issues, perform testing, improve our user experience, develop new features, train support personnel, measure corridor or product performance, and manage risk and operations.

#### **4.5 To Communicate With You**

We use personal data to send service notices, security alerts, transaction confirmations, account updates, policy changes, educational materials, support responses, surveys, and, where permitted, marketing or promotional communications.

#### **4.6 To Market and Personalize**

Where permitted by law, we use personal data to understand interest in our products, personalize content, measure campaign effectiveness, administer referral or promotional programs, and send offers that may be relevant to you. You can opt out of marketing communications at any time.

#### **4.7 For Corporate Transactions and Legal Claims**

We may use personal data in connection with actual or proposed mergers, acquisitions, financing, insolvency, restructuring, or asset sales, and to establish, exercise, defend, or settle legal claims.

#### **4.8 Sensitive Personal Data**

We process sensitive personal data, such as government-issued identification, biometric verification data, and compliance or fraud-screening data, only where necessary to provide the Services, comply with law, protect against fraud or financial crime, or where required and based on your consent.

If we need certain personal data to comply with law or to perform a contract with you and you do not provide it, we may be unable to open or maintain your account or complete your requested transaction.

### **5. How We Share Personal Data**

We may share personal data with the following categories of recipients:

#### **5.1 Affiliates and Group Companies**

We may share information with our affiliates and related companies for internal administration, customer support, security, legal compliance, analytics, and product operations.

#### **5.2 Banking, Payments, Custody, and Settlement Partners**

We may share personal data with banks, licensed money transmitters, payment processors, card networks, liquidity providers, FX providers, disbursement partners, stablecoin or wallet infrastructure providers, custody providers, and recipient institutions to fund, route, settle, reconcile, reverse, investigate, or complete your transactions.

### **5.3 Identity, Compliance, and Fraud Vendors**

We may share personal data with identity-verification vendors, KYC or KYB vendors, sanctions-screening providers, fraud-prevention vendors, risk-scoring providers, travel-rule solution providers, blockchain-analytics vendors, and similar compliance providers.

### **5.4 Technology and Operational Service Providers**

We may share personal data with cloud hosting providers, communications vendors, analytics providers, customer relationship management vendors, software providers, security vendors, consultants, customer-support providers, auditors, and other service providers that process personal data on our behalf.

### **5.5 Professional Advisers and Transaction Counterparties**

We may share personal data with legal counsel, accountants, auditors, insurers, financing sources, prospective investors or acquirers, and counterparties in a corporate transaction, subject to confidentiality and legal restrictions.

### **5.6 Regulators, Courts, and Authorities**

We may disclose personal data to regulators, law-enforcement agencies, courts, arbitrators, tax authorities, government agencies, and self-regulatory organizations where required or permitted by law, legal process, examination, investigation, or to protect the rights, safety, or property of Globridge, its users, or others.

### **5.7 Authorized Integrations and Directions**

We may share personal data with API partners, software integrations, or other third parties when you instruct us to do so, connect their services, or authorize them to access your account or transaction information.

### **5.8 Public Blockchains**

When you initiate or receive a blockchain transaction through the Services, certain information may be written to a public ledger, where it may be accessible to the public indefinitely. We do not control how other parties use data visible on public blockchains.

Some recipients of your personal data act as processors on our behalf; others, such as banks, payment providers, custody providers, recipient institutions, and certain compliance vendors, may act as independent controllers and process your data under their own privacy notices.

We do not sell personal data for monetary consideration. In limited cases, certain cookie or analytics disclosures may be treated as “sharing,” targeted advertising, or similar activity under some U.S. state privacy laws, and we provide rights or choices where required.

## **6. International Data Transfers**

Globridge operates internationally and may transfer, store, or process personal data in countries other than the country where it was collected, including the United States, the Philippines, and other jurisdictions where we or our service providers operate.

Where applicable law requires safeguards for international transfers, we use appropriate measures, which may include standard contractual clauses, intra-group transfer agreements, contractual protections with service providers, adequacy mechanisms, or other lawful transfer tools recognized by the relevant jurisdiction.

Cross-border transfers are also inherent in the nature of international payments and remittances. When you send or receive a cross-border payment, we may need to share personal data with counterparties and providers in the relevant destination or origin country.

## **7. Data Retention**

We retain personal data for as long as necessary to provide the Services, fulfill the purposes described in this Policy, and comply with applicable law.

Because Globridge is a financial-services business and works with regulated financial partners, we generally retain identity, onboarding, account, and transaction records for at least five (5) years after your relationship with us ends and, in some cases, up to ten (10) years or longer where required or permitted by law, regulation, audit requirements, sanctions or fraud controls, litigation holds, tax rules, or contractual obligations.

We may retain:

- onboarding and verification records even if you do not complete registration, where needed for fraud prevention, sanctions compliance, or recordkeeping;
- support and complaint records for as long as needed to address the issue and meet legal obligations;
- security logs and technical records for operational, fraud-prevention, and security purposes; and
- de-identified or aggregated information for analytics, reporting, and product improvement where lawful.

Please note that blockchain records, transaction hashes, wallet addresses, and data held by decentralized networks or public explorers may persist indefinitely and are not within our control.

## **8. Cookies and Similar Technologies**

We use cookies, local storage, SDKs, pixels, and similar technologies to authenticate users, maintain sessions, remember preferences, detect fraud, protect security, analyze traffic, troubleshoot problems, measure product usage, and, where permitted, support marketing or attribution.

You can manage cookie preferences through your browser, device settings, any cookie banner or in-app privacy controls we make available, or by contacting us. If you disable certain cookies or tracking technologies, some features of the Services may not function properly.

## **9. Automated Decision-Making and Profiling**

We may use automated systems to help verify identity, assess eligibility, screen sanctions and fraud risk, monitor transactions and wallet activity, and decide whether to approve, delay, restrict, or decline an account or transaction. These systems may use information such as identity data, funding history, device signals, transaction patterns, public-blockchain data, and compliance alerts.

Where required by law, you may request human review of a decision that produces legal or similarly significant effects. Even where not legally required, we will review reasonable requests for additional information about a blocked or declined account or transaction, subject to security, law-enforcement, or regulatory restrictions.

## **10. Your Rights and Choices**

### **10.1 General Rights**

Depending on where you live and subject to applicable law, you may have the right to:

- know whether we process your personal data and obtain a copy of it;
- correct inaccurate or incomplete personal data;
- request deletion of personal data;
- request portability of certain personal data;
- object to or request restriction of certain processing;
- withdraw consent where processing is based on consent;
- opt out of marketing communications;
- request human review of certain automated decisions; and
- lodge a complaint with a supervisory authority or regulator.

### **10.2 Rights for EEA, UK, and Similar Jurisdictions**

If you are located in the European Economic Area, the United Kingdom, Switzerland, or another jurisdiction with similar privacy laws, you may have rights to access, rectification, erasure, restriction, objection, portability, and complaint to your local supervisory authority. We may continue to retain or process certain information where necessary to comply with legal obligations, establish or defend legal claims, prevent fraud or financial crime, or because deletion is not technically possible, including with respect to public-blockchain data.

### **10.3 U.S. State Privacy Rights**

If you are a resident of California or another U.S. state with applicable privacy rights, you may have rights to know or access categories and specific pieces of personal information, correct information, delete information, obtain a portable copy, opt out of certain sharing or targeted advertising, and appeal certain denials. We will not discriminate against you for exercising applicable privacy rights.

Certain personal information we process in connection with financial products or services may be exempt from some U.S. state privacy laws to the extent covered by federal financial privacy laws such as the Gramm-Leach-Bliley Act. We do not sell personal data for monetary consideration. We do not use sensitive personal data to infer characteristics about you.

### **10.4 How to Exercise Your Rights**

To exercise privacy rights, contact us at [privacy@globridge.com](mailto:privacy@globridge.com). We may need to verify your identity before responding, and we may request additional information for that purpose. You may also designate an authorized agent where permitted by law. If we deny a request, we will explain the basis for the denial where required.

### **10.5 Marketing Choices**

You may opt out of promotional emails by using the unsubscribe link in the message or contacting us. We may still send you service-related, legal, security, and transaction-related communications.

## **11. Data Security**

We use administrative, technical, and physical safeguards designed to protect personal data from unauthorized access, loss, misuse, or alteration. These measures may include encryption in transit and at rest where appropriate, access controls, vendor due diligence, monitoring, logging, and workforce training.

No method of transmission over the internet or method of electronic storage is completely secure. You are responsible for protecting your credentials, devices, and connected email accounts and for notifying us promptly of any suspected unauthorized access or security incident involving your account.

## **12. Children's Privacy**

The Services are not directed to children under eighteen (18), and we do not knowingly collect personal data directly from children. If we learn that we have collected personal data from a child in violation of applicable law, we will take appropriate steps to delete or restrict that information.

## **13. Third-Party Services**

The Services may contain links to, or integrations with, third-party websites, wallets, exchanges, applications, or services. We are not responsible for the privacy practices of those third parties. Their own terms and privacy notices apply when they process your information in their own capacity.

## **14. Changes to This Policy and Contact Information**

We may update this Privacy Policy from time to time. If we make a material change, we will provide notice as required by law, such as by posting the updated Policy in the Services, updating the effective date, or contacting you through the account information we have on file.

Privacy requests: [privacy@globridge.com](mailto:privacy@globridge.com)

Customer support: [support@globridge.com](mailto:support@globridge.com)

Legal notices: [legal@globridge.com](mailto:legal@globridge.com)