

Privacy Policy

Bright Carrier Technology Pvt. Ltd. / BriteX

1. Introduction

Bright Carrier Technology Pvt. Ltd., operating as BriteX, respects your privacy and is committed to protecting your personal data. This Privacy Policy explains what information we collect, how we use it, when we share it, how we protect it, and the rights available to you.

This Policy applies to users who access or use our website, mobile application, trading platform, wallet services, customer support channels, and related services.

By using BriteX services, you acknowledge that your personal data will be handled in accordance with this Privacy Policy and applicable laws.

2. Information We Collect

2.1 Personal and Identity Information

- Full name, date of birth, photograph, selfie, and other identity verification information.
- Email address, phone number, residential address, and communication details.
- Government-issued identification details, including Aadhaar, PAN, or other KYC documents, where required by law.
- Bank account details, payment information, and payout or deposit information.

2.2 Trading, Wallet, and Transaction Information

- Transaction history, order activity, deposits, withdrawals, trades, and related records.
- Wallet addresses, portfolio information, trading preferences, and account activity.
- Staking, rewards, referral, promotional, and incentive-related information.

2.3 Technical and Usage Information

- IP address, device identifiers, browser type, operating system, and app version.
- Login history, security events, usage data, pages viewed, features used, and error logs.
- Cookies, analytics identifiers, and similar technologies used to improve security and performance.

3. How We Use Your Information

We process personal data for lawful, specific, and necessary purposes, including to:

- Verify identity and complete KYC, AML, fraud-prevention, and compliance checks.
- Create, operate, secure, and maintain your BriteX account.
- Process trades, deposits, withdrawals, payments, settlements, and wallet-related activities.
- Provide customer support, respond to queries, and resolve disputes.
- Send service messages, security alerts, account notifications, and important updates.
- Improve platform functionality, user experience, analytics, risk controls, and service quality.
- Detect, prevent, investigate, and respond to fraud, cyber incidents, misuse, suspicious activity, and legal violations.
- Comply with applicable laws, regulatory requirements, court orders, tax obligations, and lawful requests from authorities.

4. Legal Basis and Consent

Where required, we collect and process personal data based on your consent. We may also process personal data where it is necessary for providing requested services, meeting legal obligations, preventing fraud, protecting platform security, enforcing agreements, or responding to lawful requests.

You may withdraw consent where processing is based on consent, subject to legal, regulatory, contractual, and operational limitations. Withdrawal of consent may affect our ability to provide certain services.

5. Data Sharing and Disclosure

We do not sell your personal data. We may share personal data only where necessary and appropriate with:

- Regulatory authorities, law enforcement agencies, courts, tax authorities, or government bodies where required or permitted by law.
- Banking, payment, settlement, custody, wallet, and financial service partners.
- KYC, identity verification, AML screening, blockchain analytics, fraud monitoring, cybersecurity, and compliance service providers.
- Cloud hosting, technology, analytics, communication, customer support, and operational service providers.

- Professional advisors, including lawyers, auditors, consultants, insurers, and accountants.
- Group companies, business partners, successors, or transferees in connection with restructuring, merger, acquisition, financing, or sale of business assets, subject to appropriate safeguards.

6. Data Security

We use reasonable technical, organisational, and administrative safeguards to protect personal data and digital assets, including:

- Encryption in transit and appropriate encryption or protection for stored information.
- Two-factor authentication, access controls, and internal authorisation procedures.
- Cold storage or other risk-reduction measures for eligible digital assets.
- Security monitoring, incident response procedures, vulnerability management, and periodic audits.
- Employee confidentiality obligations and role-based access restrictions.
- Secure infrastructure, backups, logging, and business continuity practices.

No method of electronic transmission or storage is completely secure. You are responsible for maintaining the confidentiality of your account credentials, passwords, OTPs, private keys, recovery phrases, and devices.

7. Data Retention

We retain personal data only for as long as necessary for the purposes described in this Policy, unless a longer retention period is required or permitted by law. Typical retention periods include:

- Account and KYC records: for the duration of the account and for at least five years after closure, or longer where required by law.
- Transaction, trading, and compliance records: for at least five years, or longer where required by law or regulatory requirements.
- Marketing preferences: until you opt out or withdraw consent, subject to suppression-list requirements.
- Technical logs: generally for up to 90 days, unless needed for security, fraud prevention, investigation, audit, or legal purposes.

8. Your Rights

Subject to applicable law, you may have the right to:

- Access information about the personal data we process about you.
- Request correction, completion, updating, or erasure of personal data, where permitted.
- Request portability of certain personal data, where applicable.
- Withdraw consent where processing is based on consent.
- Nominate another individual to exercise your rights in the event of death or incapacity, where applicable.
- Raise grievances with us and, where permitted by law, approach the appropriate authority.

To exercise your rights, please contact us using the details provided in the “Contact Us” section. We may need to verify your identity before responding to a request.

9. Cookies and Similar Technologies

We use cookies and similar technologies to support authentication, security, preferences, analytics, performance, service improvement, and marketing where permitted by law or based on consent.

You may manage cookies through your browser or device settings. Disabling some cookies may affect the functionality, security, or availability of certain services.

10. International Transfers

Your personal data may be processed, stored, or transferred outside India where necessary for cloud hosting, service provider operations, security monitoring, compliance, customer support, analytics, or business continuity.

Where we transfer personal data internationally, we seek to use appropriate safeguards and comply with applicable legal requirements.

11. Children’s Privacy

Our services are intended only for users who are legally eligible to use them. We do not knowingly provide trading or exchange services to children or collect children’s personal data except where legally permitted and with required verifiable consent.

12. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or services. The updated version will be effective when published or otherwise communicated to you.

13. Contact Us

Data Protection Officer / Grievance Contact:

Email: bctechpvtltd0120@gmail.com

Phone: 03474 353034

Note: This Privacy Policy is intended as a general policy document and should be reviewed by a qualified legal professional to confirm compliance with all laws and regulations applicable to BC Exchange's specific business model, licences, operations, and jurisdictions.