

Bitechchain

PRIVACY POLICY

Version 1.0 | Effective Date: 1 May 2026

Last Updated: May 2026

Document	Privacy Policy
Company	Bitechchain Platform
Jurisdiction	Canada (Ontario)
Address	940 Winterton Way, Mississauga, ON L5V 2M2
Contact	contact@bitechchain.com
Phone	+1 905-210-3928
Effective	1 May 2026

1. Introduction and Scope

This Privacy Policy ("Policy") describes how Bitechchain ("we", "us", "our", or the "Platform") collects, uses, stores, shares, and protects personal information provided by users ("you") of the Bitechchain mobile application and associated digital services.

This Policy applies to all users of the Platform regardless of location. By accessing or using the Platform, you acknowledge that you have read, understood, and agree to the data practices described in this Policy.

This Policy does not constitute financial advice and does not govern the terms of any financial products or services. Please refer to the applicable Terms of Service for the full scope of your agreement with the Platform.

1.1 Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person
Processing	Any operation performed on personal data, including collection, storage, use, and deletion

Data Controller	The entity that determines the purposes and means of processing personal data
Data Processor	A third party that processes personal data on behalf of the Data Controller
Sensitive Data	Personal data revealing racial origin, health information, financial details, or biometric data
User	Any individual who accesses or uses the Platform
Platform	The Bitechchain mobile application and associated web services

2. Data Controller Information

The data controller responsible for your personal data is:

Company Name	Bitechchain Platform
Legal Address	940 Winterton Way, Mississauga, ON L5V 2M2, Canada
Email	contact@bitechchain.com
Phone	+1 905-210-3928
Website	https://bitechchain.com

3. Information We Collect

We collect personal data through multiple channels. The following table outlines the categories of data we collect, how they are collected, and why.

3.1 Information You Provide Directly

Data Category	Examples	Purpose
Identity Data	Full name, date of birth	Account creation, verification
Contact Data	Email address, phone number	Communication, support
Account Credentials	Username, hashed password	Authentication, security
Verification Documents	Government-issued ID (where required)	Regulatory compliance (KYC/AML)
Financial Preferences	Asset class preferences, strategy settings	Platform personalisation

Support Communications	Messages, enquiries submitted via contact form	Customer support
------------------------	--	------------------

3.2 Information Collected Automatically

Data Category	Examples	Purpose
Device Information	Device model, OS version, app version	Compatibility, debugging
Network Information	IP address, mobile carrier, connection type	Security, fraud prevention
Usage Data	Features accessed, session duration, clicks	Platform improvement
Location Data	Country/region (derived from IP)	Compliance, language settings
Crash Reports	Error logs, stack traces	Bug fixing, stability
Performance Data	Load times, API response times	Platform optimisation

3.3 Information From Third Parties

We may receive data about you from the following third-party sources:

- Identity verification providers (KYC/AML compliance services)
- Analytics providers (anonymised aggregate usage data)
- Market data providers (no personal data received)
- Payment processors (transaction status only — no card data stored by us)

⚠ We do not collect special categories of sensitive personal data such as racial or ethnic origin, political opinions, religious beliefs, health information, or biometric data, unless explicitly required by law and with your prior consent.

4. Legal Basis for Processing

Under applicable data protection law (including Canada's PIPEDA and, where applicable, the EU General Data Protection Regulation), we process your personal data on the following legal bases:

Legal Basis	When We Use It	Examples
-------------	----------------	----------

Contractual Necessity	Processing required to fulfil our contract with you	Account management, service delivery
Legitimate Interests	Processing necessary for our legitimate business interests, balanced against your rights	Fraud prevention, security, analytics
Legal Obligation	Processing required to comply with applicable law	AML/KYC verification, tax reporting
Consent	Processing based on your explicit agreement	Marketing communications, optional analytics

5. How We Use Your Information

We use the personal data we collect for the following purposes:

5.1 Platform Operations

- Creating and managing your user account
- Authenticating your identity at each login session
- Providing access to platform features, tools, and market data
- Processing account-related requests and settings changes
- Maintaining the security and integrity of the Platform

5.2 Regulatory Compliance

- Conducting identity verification (Know Your Customer — KYC)
- Screening against anti-money laundering (AML) watchlists
- Maintaining records as required by applicable financial regulations
- Responding to lawful requests from regulatory authorities

5.3 Communication

- Responding to support enquiries and technical questions
- Sending transactional notifications (account changes, security alerts)
- Delivering service updates and policy change notices
- Sending marketing communications where you have provided consent

5.4 Platform Improvement

- Analysing aggregated usage patterns to improve features
- Diagnosing and fixing technical issues and crashes
- Conducting A/B testing to optimise user experience
- Measuring platform performance and reliability

We do not use your personal data to make fully automated decisions that have significant legal or similarly significant effects on you without human review.

6. Data Sharing and Disclosure

We do not sell, rent, or trade your personal data. We may share your data in the following limited circumstances:

6.1 Service Providers

We engage trusted third-party service providers who process personal data on our behalf, subject to strict data processing agreements:

Service Type	Examples of Providers	Data Shared
Cloud Infrastructure	AWS, Google Cloud	Encrypted user data, logs
Analytics	Firebase Analytics	Anonymised usage data
Identity Verification	Third-party KYC providers	Identity documents (encrypted)
Customer Support	Support ticketing platforms	Name, email, support messages
Crash Reporting	Error monitoring services	Device info, anonymised logs

6.2 Legal Requirements

We may disclose personal data where required by applicable law, court order, or governmental authority, including:

- Compliance with anti-money laundering (AML) regulations
- Response to valid legal process (subpoenas, court orders)
- Protection of the rights, property, or safety of our users or the public

6.3 Business Transfers

In the event of a merger, acquisition, restructuring, or sale of assets, your personal data may be transferred to the successor entity. We will notify you in advance of any such transfer and provide the opportunity to delete your account if you do not wish your data to be transferred.

6.4 With Your Consent

We may share data with third parties for any other purpose with your explicit prior consent, which you may withdraw at any time.

7. International Data Transfers

Your personal data may be transferred to and processed in countries other than your country of residence. These countries may have data protection laws that differ from those in your jurisdiction.

Where we transfer personal data internationally, we ensure appropriate safeguards are in place, including:

- Standard Contractual Clauses (SCCs) approved by relevant authorities
- Adequacy decisions recognising equivalent protection standards
- Binding Corporate Rules (where applicable)
- Your explicit consent (where no other safeguard applies)

Users located in the European Economic Area (EEA) or United Kingdom should be aware that their data may be transferred to Canada (which has an EU adequacy decision) and potentially other jurisdictions with appropriate safeguards.

8. Data Retention

We retain personal data for as long as necessary to fulfil the purposes for which it was collected, comply with legal obligations, resolve disputes, and enforce agreements.

Data Type	Retention Period	Reason
Account Data	Duration of account + 7 years post-closure	Legal obligation, dispute resolution
Identity Documents	5–10 years post-account closure	AML/KYC regulatory requirements
Transaction Records	7 years from transaction date	Financial regulatory requirements

Support Communications	3 years from resolution	Service improvement, dispute records
Usage & Analytics Data	24 months (anonymised thereafter)	Platform improvement
Crash & Error Logs	12 months	Debugging, stability
Marketing Consents	Until withdrawal of consent	Compliance

Upon account deletion, we will delete or anonymise your personal data within 30 days, except where retention is required by law or legitimate business interest.

9. Data Security

We implement comprehensive technical and organisational security measures to protect your personal data against unauthorised access, alteration, disclosure, loss, or destruction.

9.1 Technical Measures

- Transport Layer Security (TLS 1.3) for all data in transit
- AES-256 encryption for sensitive data at rest
- Multi-factor authentication (MFA) for all account access
- Secure API endpoints with rate limiting and anomaly detection
- Regular penetration testing and vulnerability assessments
- Automated threat detection and incident response systems

9.2 Organisational Measures

- Role-based access controls limiting data access to authorised personnel
- Regular staff training on data protection and security practices
- Data protection impact assessments for new features and integrations
- Documented incident response and breach notification procedures
- Vendor due diligence and contractual data protection obligations

⚠ No method of electronic transmission or storage is 100% secure. While we apply industry-standard measures, we cannot guarantee absolute security. You are responsible for maintaining the confidentiality of your account credentials.

10. Your Rights and Choices

Depending on your location and applicable law, you have the following rights regarding your personal data:

Right	Description	How to Exercise
Access	Obtain a copy of your personal data we hold	Submit request to contact@bitechchain.com
Rectification	Correct inaccurate or incomplete data	Via account settings or email
Erasure	Request deletion of your personal data	Submit request to contact@bitechchain.com
Restriction	Limit processing in certain circumstances	Submit request to contact@bitechchain.com
Portability	Receive your data in a structured, machine-readable format	Submit request to contact@bitechchain.com
Objection	Object to processing based on legitimate interests	Submit request to contact@bitechchain.com
Withdraw Consent	Withdraw consent at any time for consent-based processing	Via account settings or email
Lodge Complaint	File a complaint with your local data protection authority	Contact your national DPA

We will respond to all data rights requests within 30 days. In complex cases, we may extend this period by a further 60 days with prior notice.

To exercise any of these rights, please contact us at contact@bitechchain.com with the subject line "Data Rights Request" and include sufficient information to verify your identity.

11. Cookies and Tracking Technologies

The Platform uses cookies and similar tracking technologies to enhance functionality, analyse usage, and support security measures.

Cookie Type	Purpose	Opt-Out
Essential	Platform functionality, authentication, session management	Cannot be disabled

Security	Fraud detection, bot prevention, session integrity	Cannot be disabled
Analytics	Usage patterns, performance measurement (anonymised)	Via settings or cookie consent
Preference	Remembering language, layout, and display settings	Via account settings
Marketing	Personalised content (only with explicit consent)	Withdraw consent at any time

You can manage cookie preferences through the Platform settings. Disabling essential cookies will impair Platform functionality.

12. Children's Privacy

The Platform is not directed at or intended for use by individuals under the age of 18. We do not knowingly collect personal data from minors.

If we become aware that we have inadvertently collected personal data from a person under 18, we will take immediate steps to delete that data. If you believe we have collected data from a minor, please contact us immediately at contact@bitechchain.com.

⚠ Parents and guardians are responsible for monitoring their children's use of digital services. If you are under 18, please do not use the Platform or provide any personal information.

13. Third-Party Links and Services

The Platform may contain links to third-party websites, services, or applications. This Policy does not apply to those third-party services. We are not responsible for the privacy practices of third parties and encourage you to review their privacy policies before providing any personal data.

14. 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 other factors. We will notify you of material changes by:

- Posting the updated Policy within the Platform with a revised "Last Updated" date
- Sending an email notification to your registered email address

- Displaying an in-app notification upon next login

Your continued use of the Platform after the effective date of any changes constitutes your acceptance of the updated Policy. If you do not agree with the changes, you should discontinue use and may request account deletion.

15. Specific Disclosures for App Store Compliance

15.1 Apple App Store — iOS Users

The following disclosures are required under Apple's App Store Review Guidelines and App Privacy nutrition label requirements:

Data Type	Collected	Linked to Identity
Contact Info (name, email, phone)	Yes	Yes
Usage Data (app interactions)	Yes	No (anonymised)
Diagnostics (crash logs)	Yes	No
Identifiers (device ID)	Yes	No
Financial Info	No	N/A
Health & Fitness	No	N/A
Location (precise)	No	N/A
Location (coarse)	Yes	No (country level only)

15.2 Google Play — Android Users

The following disclosures are required under Google Play's Data Safety section requirements:

- Data collected: Name, email address, phone number, country/region
- Data sharing: With service providers under data processing agreements only
- Security practices: Data encrypted in transit and at rest
- Users can request data deletion by contacting contact@bitechchain.com
- Data collection is required for core Platform functionality

16. Financial Regulatory Compliance

As an operator of a trading analytics platform, we are subject to certain financial data protection requirements in addition to general privacy law:

- We conduct Know Your Customer (KYC) and Anti-Money Laundering (AML) checks as required
- Identity documents collected for regulatory purposes are subject to specific retention requirements
- We may be required to disclose personal data to financial regulators without prior notice to you
- Transaction data may be shared with clearing partners or payment processors as required

⚠ If you are in a jurisdiction with specific financial data protection requirements (e.g., GDPR Article 9 in the EU, CCPA in California), additional rights and protections may apply. Contact us to exercise jurisdiction-specific rights.

17. Contact Information and Complaints

If you have questions, concerns, or complaints about this Privacy Policy or our data practices, please contact us:

Contact Method	Details
Email	contact@bitechchain.com
Phone	+1 905-210-3928
Post	940 Winterton Way, Mississauga, ON L5V 2M2, Canada
Subject Line	"Privacy Enquiry" or "Data Rights Request"
Response Time	Within 5 business days for general enquiries; 30 days for data rights requests

If you are located in the European Economic Area and are not satisfied with our response, you have the right to lodge a complaint with your local data protection supervisory authority. In the UK, this is the Information Commissioner's Office (ICO) at ico.org.uk.

18. Governing Law

This Privacy Policy is governed by the laws of the Province of Ontario and the federal laws of Canada applicable therein, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and successor legislation.

Where applicable, this Policy is also intended to comply with the EU General Data Protection Regulation (GDPR), the UK GDPR, the California Consumer Privacy Act (CCPA), and other applicable regional privacy laws.

BY USING THE Bitechchain PLATFORM, YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTOOD, AND AGREE TO THIS PRIVACY POLICY.

Document Version: 1.0

Effective Date: 1 May 2026

© 2026 Bitechchain. All rights reserved.