HIGH BINARY

PRIVACY POLICY

Information governance, security and user privacy rights

DOCUMENT Privacy Policy

VERSION 1.0

EFFECTIVE DATE 03 August 2026

WEBSITE https://highbinarytrading.com

CONTACT support@highbinarytrading.com

ABOUT THIS POLICY

This Privacy Policy describes what personal data HIGH BINARY processes, why it is processed, when it may be shared, how it is secured and retained, and the choices and rights available to users. It applies to the website and connected platform Services described below.

The data controller and contact details are identified in the publication information below.

PUBLICATION INFORMATION

Data controller / operator	HighBinary Technologies Ltd
Registered address	37th Floor, One Canada Square, Canary Wharf, London, E14 5AA, United Kingdom
Registration / identifier	17551319

CONTENTS

01 Information We Collect

02 How We Use Your Information

03 Data Protection & Security

04 Deposits, Withdrawals & Financial Information

05 Identity Verification (KYC)

06 Cookies & Tracking Technologies

07 Third-Party Services & Data Sharing

08 Data Retention & Deletion

09 User Privacy Rights

10 International Data Transfers

11 Children's Privacy & Age Restrictions

12 Privacy Policy Updates & Changes

13 Contact Information & Privacy Inquiries

14 Automated Decision-Making & Profiling

15 Legal Compliance & Governing Privacy Laws

This policy is organized for readable online publication and document distribution. The definitive effective date and legal operator details appear on the first page.

01 Information We Collect

1.1. Scope and sources of personal data

HIGH BINARY ("HIGH BINARY", "we", "us", or "our") processes personal data in connection with access to and use of its website, account features, demo and real trading environments, financial operations, account verification, customer support, and related services (together, the "Services"). This Privacy Policy applies to information provided by users, collected through their interactions with the Services, generated through their use of the platform, or obtained from authorized service providers and lawful verification sources.

1.2. Account, registration, and profile information

We collect information required to create, authenticate, and administer an account, such as name, email address, contact information, date of birth or age confirmation, account identifier, country or region, login credentials in protected form, account preferences, and details supplied when a profile is created or updated.

1.3. Identity verification and compliance information

Depending on the verification requirements applicable to an account, we may collect official identification documents, identification numbers, date of birth, nationality, address or residence information, document images, selfies or facial images used for identity matching, and information needed to confirm document authenticity, detect duplicate accounts, prevent fraud, and comply with identity-verification obligations. We may receive verification results or risk indicators from authorized providers rather than receiving all underlying documents directly.

1.4. Technical, device, and usage data

We may collect IP address, device and browser characteristics, operating system, language, approximate location inferred from network information, session and device identifiers, access timestamps, security events, login history, authentication attempts, settings, service logs, and interactions with platform features. We do not claim to collect precise location unless a relevant feature expressly requests and lawfully obtains it.

1.5. Trading and platform activity

We process trading account identifiers, selected instruments and currency pairs, order and trade records, transaction timestamps, order amounts, trade duration and outcomes, account balances, payout calculations, copy-trading settings, tournament participation, reward usage, demo-account activity, and other data generated by the Services. Where social, observer, copying, or leaderboard features exist, the information visible to other users is determined by the feature design and applicable privacy controls.

1.6. Financial, payment, and blockchain information

We collect or generate deposit and withdrawal requests, amounts, currencies, payment channels, processing status, reconciliation references, transaction identifiers, cryptocurrency wallet addresses, blockchain transaction hashes (TXIDs), and related verification and transaction-history records. We generally seek to limit payment-card or banking information to the data needed to coordinate a transaction; specialized payment providers may handle additional sensitive payment credentials.

1.7. Communications and preferences

We retain support tickets, chat and email correspondence, complaint histories, service inquiries, responses, notification preferences, consent records, and communications necessary to resolve service or financial issues. We also process cookie preferences and relevant account privacy settings.

1.8. Information from others and required disclosures

Where lawful and relevant, information may be obtained from identity-verification partners, payment processors, blockchain networks, security providers, fraud-prevention services, and other sources necessary to verify transactions or meet legal duties. Some information is required to establish an account, verify eligibility, execute a transaction, or comply with law; withholding it may prevent access to the relevant feature or Service. Optional information and consent-based activities will be identified as such where required.

02 How We Use Your Information

2.1. Purposes of processing

We use personal data only for specified, legitimate purposes connected with providing the Services, complying with applicable obligations, and protecting the platform and its users. Depending on the circumstances, these purposes include:

- Creating and administering accounts, authenticating access, maintaining balances and account settings, and providing requested functionality.
- Executing and recording trading operations, calculating results, enabling demo and real environments, and supporting copy-trading, tournaments, rewards, and related features.
- Receiving, verifying, processing, reconciling, and documenting deposits, withdrawals, and cryptocurrency transfers.
- Completing identity, age, and eligibility checks, performing KYC and other legally required due diligence, and detecting fraudulent or duplicate accounts.
- Protecting accounts, detecting unauthorized access, preventing fraud and abuse, monitoring suspicious transactions, and investigating security incidents.
- Responding to customer-support requests, disputes, complaints, and account or transaction inquiries.
- Sending essential service communications, verification codes, security alerts, financial status updates, and notices concerning the Services.
- Sending optional promotional communications only where a valid legal basis applies, including consent where required, and respecting opt-out choices.
- Maintaining, troubleshooting, testing, understanding, and improving platform availability, performance, and user experience through appropriate analytics.
- Establishing, exercising, or defending legal claims and fulfilling recordkeeping, regulatory, law-enforcement, and other applicable legal obligations.

2.2. Lawful grounds

Where the relevant data protection regime requires a legal basis, processing may rest on performance of or steps toward a contract, compliance with a legal obligation, legitimate interests that are not overridden by applicable individual rights, or valid consent. In limited circumstances other lawful grounds may apply. The specific basis depends on the nature, purpose, and jurisdiction of the processing activity. Where legitimate interests are relied upon, these may include securing the

Services, preventing misuse, ensuring reliable operations, and resolving disputes, subject to appropriate balancing and safeguards.

2.3. Consent and preferences

Optional marketing communications and non-essential cookies or comparable technologies will be managed using separate choices where required. A choice not to participate in optional processing will not be treated as a refusal of necessary account or security processing. Consent can be withdrawn through available controls or Customer Support, without affecting processing carried out lawfully before withdrawal.

2.4. Purpose changes and data minimization

We limit collection and use to information reasonably necessary for the relevant purpose. If we intend to use personal data for a materially different purpose, we will assess compatibility with the original purpose and provide any additional notice or consent required by applicable law.

03 Data Protection & Security

3.1. Security architecture

HIGH BINARY applies layered technical, organizational, and administrative safeguards intended to protect personal data against unauthorized access, misuse, loss, alteration, and disclosure. Safeguards are selected in view of the sensitivity of the information, associated risks, and operational requirements. No internet-based system can guarantee absolute security.

3.2. Safeguards applied

- Data encryption: encryption protects information in transit and stored information where appropriate, with controlled handling of cryptographic keys.
- Secure password storage: passwords are handled using secure, one-way password-verification methods rather than being retained as readable passwords.
- Two-factor authentication (2FA): additional authentication safeguards are supported for account access and related security workflows.
- Login activity monitoring: access attempts, relevant device or session changes, and unusual login activity may be logged and reviewed.
- Session management: controls are used to manage authenticated sessions and reduce unauthorized persistence of access.
- KYC document protection: identity records and documents are subject to additional access restrictions and handling protections.
- Financial transaction security: deposits, withdrawals, and associated account operations are subject to appropriate verification, security, and reconciliation controls.
- Restricted employee access: staff and authorized service personnel are granted access according to defined duties and least-privilege principles.
- Secure backups and recovery: backup and restoration controls support continuity, integrity, and recovery from operational incidents.
- Security incident response: processes support detection, investigation, containment, remediation, and legally required notifications of personal data incidents.

3.3. Review and security responsibilities

Security controls and operational protections are reviewed regularly and updated in response to changing risks. Users are responsible for protecting their credentials, enabling available account

security options, and reporting suspected unauthorized access through official support channels. HIGH BINARY may require additional verification before permitting sensitive account or financial actions.

3.4. Security notifications

Where a personal data breach or other security event requires notification under applicable law, HIGH BINARY will notify the relevant users and/or authorities as required, with information appropriate to the circumstances and legal reporting obligations.

04 Deposits, Withdrawals & Financial Information

4.1. Records associated with financial operations

To provide financial functionality and support accurate records, HIGH BINARY processes the following categories of data:

- Deposit information, including amounts, dates, payment channels, confirmation status, and account attribution.
- Withdrawal information, including requests, destinations, verification outcomes, processing status, and payment history.
- Cryptocurrency wallet addresses or destination details associated with deposits and withdrawals.
- Blockchain transaction identifiers (TXIDs), transaction confirmations, and network-related information.
- Limited payment-method information required to process and reconcile a transaction, such as method type and provider references.
- Transaction verification data used for security screening, compliance checks, and dispute resolution.
- Financial history, including balances, accounting entries, transfers, credits, debits, relevant fees, and transaction records.

4.2. Payment and cryptocurrency providers

Payment services may be delivered through a combined infrastructure comprising internal accounting and transaction-management systems and external payment or blockchain providers. A provider may process information according to its role as a service provider, processor, or independent controller and its own legally required privacy disclosures.

4.3. Blockchain transparency

Public blockchain networks may permanently record wallet addresses, transfer amounts, network timestamps, and TXIDs. Such records may be publicly observable, may be processed by independent network participants, and generally cannot be changed or deleted by HIGH BINARY. We cannot guarantee the deletion of information independently recorded on a public blockchain.

4.4. Verification, disclosure, and retention

Financial data may be checked to prevent fraud, verify ownership or control of payment destinations, address chargebacks or disputes, and meet applicable recordkeeping, anti-money-laundering, tax, or other legal duties. Records are retained in accordance with the applicable law and the retention principles in Section 8. Financial information is not used to authorize unrelated processing without a valid legal basis.

05 Identity Verification (KYC)

5.1. Why verification is required

HIGH BINARY uses identity verification to confirm eligibility, protect accounts and funds, prevent impersonation and multiple-account abuse, investigate suspicious activity, and satisfy applicable legal or regulatory requirements.

5.2. Information and verification methods

Identity checks may involve a passport, national identification card, or driver's license; a selfie or other facial image for identity matching; personal details such as name, date of birth and country of residence; checks of document validity and authenticity; fraud and duplicate-account detection; and additional information reasonably necessary to resolve verification discrepancies.

5.3. Internal and external verification

Verification may combine automated checks performed by external identity-verification partners with internal manual review, including review of exceptions, disputes, and suspected fraud. Access to source documents and verification results is restricted to authorized persons or systems.

5.4. Periodic and event-based reviews

Where justified by risk or law, HIGH BINARY may repeat or refresh verification, request updated documentation, or temporarily restrict relevant activities while material identity or compliance questions are resolved.

5.5. Protection and post-closure retention

KYC documents and associated verification records are subject to additional security controls. Following account closure, HIGH BINARY retains these records only for periods justified by applicable legal obligations, legitimate recordkeeping requirements, or lawful claims, after which they are securely deleted or de-identified where feasible and lawful.

06 Cookies & Tracking Technologies

6.1. Technologies and categories

HIGH BINARY may use cookies, local storage, session tokens, and comparable technologies to deliver the website and platform. The principal categories are:

- Essential cookies or technologies needed for core platform operation and technically necessary functions.
- Authentication and session technologies used to maintain secure sign-in and account sessions.
- Security technologies supporting misuse detection and account protection.
- Preference technologies remembering user-selected settings, language, or display choices.
- Analytics technologies used to understand aggregated performance and usage trends.
- Functional technologies that support optional conveniences and enhanced features.

6.2. No marketing cookies

HIGH BINARY does not use marketing or advertising cookies as part of the cookie configuration described in this Policy. Direct promotional emails, where enabled, are governed by separate marketing communication preferences and are not treated as cookie-based advertising.

6.3. Choice and consent

Where required by law, non-essential cookies and similar technologies are not activated until the user provides valid consent. The cookie interface provides "Accept All", "Reject Optional", and "Customize Settings" choices. Users may subsequently revisit privacy or cookie preferences and withdraw optional consent. Strictly necessary technologies may remain active without consent where permitted by law.

6.4. Cookie duration and third parties

Cookies may be session-based or persistent, depending on their function. Where applicable, specific cookie names, providers, lifetimes, and purposes are identified in the platform's cookie settings or a supplementary cookie notice. Browser controls may also restrict cookies, although disabling essential technologies can affect platform availability.

07 Third-Party Services & Data Sharing

7.1. General approach to sharing

HIGH BINARY does not disclose personal data to third parties merely because they request it. Information is shared only where necessary for specified Services, authorized processing, legitimate security purposes, legally justified business operations, or legal compliance, and subject to appropriate controls. The role of a third party may vary; some act under our instructions while others have independent legal obligations.

7.2. Service-provider categories

- Payment processing providers: external processors and internal financial systems together support payment initiation, settlement, reconciliation, and risk checks.
- Cryptocurrency and blockchain services: a hybrid infrastructure uses internal transaction records together with external wallets, payment networks, network observers, or blockchain services as needed.
- Identity verification providers: external automated identity-document and verification tools may be combined with internal manual review.
- Cloud hosting and infrastructure: cloud and dedicated infrastructure may be used to store, transmit, operate, and protect the Services.
- Email and communication providers: internal workflows and external mailbox or message-delivery services support service messages, security notifications, and Customer Support.
- Analytics and performance services: internal analytics and approved external services may be used for reliability, performance, diagnostics, and product improvement.
- Security and fraud prevention providers: internal controls may operate together with external anti-abuse, threat detection, and security technologies.
- Customer support services: support is managed through HIGH BINARY channels, with hosting or communication providers supporting the underlying systems where applicable.

7.3. Email service channels

HIGH BINARY uses dedicated communication channels for distinct purposes: support@highbinarytrading.com for customer inquiries and privacy requests; security@highbinarytrading.com for relevant security-related communications; and notifications@highbinarytrading.com for platform notices and permitted promotional communications. Email infrastructure may be supplied by third-party email service providers.

7.4. Other lawful disclosures

Personal data may be disclosed to competent courts, regulators, supervisory bodies, law-enforcement agencies, auditors, professional advisers, or other recipients where disclosure is required or permitted by applicable law. If the business is reorganized or transferred, personal data may be disclosed to relevant counterparties subject to lawful safeguards and appropriate notification requirements.

7.5. Contractual controls and transparency

Where required, providers are subject to appropriate confidentiality, security, data-processing, and international-transfer arrangements. HIGH BINARY evaluates provider access according to business need and risk. We will provide information about recipients or categories of recipients, and applicable transfer safeguards, in response to valid requests as required by law.

08 Data Retention & Deletion

8.1. Retention principles

HIGH BINARY keeps personal data only for as long as reasonably necessary for the purpose for which it was collected, subject to applicable legal retention periods, pending disputes, fraud investigations, security needs, and the establishment, exercise, or defense of legal claims. Retention is determined by the nature of the record, the applicable jurisdiction, operational necessity, and legal requirements; different categories may be retained for different periods.

8.2. Retention by record category

- Account and profile records: generally retained while the account is active and for any justified post-closure administration or legal period.
- KYC and compliance records: maintained for the statutory or otherwise lawful period applicable to identity-verification, financial-compliance, and dispute requirements.
- Deposits, withdrawals, and other financial records: retained for applicable financial, tax, accounting, regulatory, and claims-related periods.
- Trading and transaction history: retained for account administration, investigation, reconciliation, and legally necessary records.
- Login, device, session, and security records: retained for a proportionate security, incident-response, and fraud-prevention period.
- Support and complaint communications: retained for case administration, service quality, dispute resolution, and lawful recordkeeping.
- Cookie preferences, consent records, and relevant analytics data: retained according to their purpose, technical configuration, and proof-of-consent or legal requirements.
- Backups and disaster-recovery copies: retained under controlled backup lifecycles and removed through scheduled rotation or secure recovery procedures.

8.3. Closing an account

When an account is closed, access to ordinary active-account functionality is terminated as appropriate. Personal data not subject to continued lawful retention will be deleted, anonymized, or otherwise removed through the normal deletion process. Closure does not automatically erase records that must legally be kept, including certain identity, financial, transaction, or security records.

8.4. Deletion requests and controls

Users may initiate deletion requests through available Account Settings and by contacting Customer Support. HIGH BINARY may ask for reasonable identity verification and will inform the user if a

particular category cannot be erased immediately because of legal or legitimate grounds recognized by applicable law.

8.5. Backups and completion confirmation

Data in backup systems may persist until the relevant controlled backup expires, subject to restricted access and restoration controls. Where a valid erasure request is completed, HIGH BINARY may confirm the result through email and/or an in-platform notification. Anonymized information that can no longer reasonably identify a person may be retained where lawful.

09 User Privacy Rights

9.1. Rights available under applicable law

Depending on the user's location, the nature of the processing, and applicable law, users may have some or all of the following rights:

- Right to be informed: receive clear information about collection and use of personal data.
- Right of access: request confirmation of processing and a copy of eligible personal data.
- Right to rectification: request correction of inaccurate or incomplete information.
- Right to erasure: request deletion where an applicable ground exists and no overriding lawful obligation requires retention.
- Right to restriction: ask us to limit processing in the circumstances provided by law.
- Right to data portability: receive eligible data in a structured, commonly used, machine-readable format and, where technically feasible and legally applicable, have it transmitted to another controller.
- Right to object: oppose certain processing, including processing based on legitimate interests where the law provides an objection right.
- Right to withdraw consent: withdraw consent at any time for processing that relies on it, without retroactively invalidating earlier lawful processing.
- Rights concerning certain automated decisions: request the protections, explanations, human intervention, review, or challenge available under applicable law.
- Right to lodge a complaint: contact HIGH BINARY and, where applicable, the competent data protection or privacy supervisory authority.

9.2. How to submit a request

Users may exercise available rights through Account Settings, the platform's Privacy Preferences controls, or Customer Support at support@highbinarytrading.com. Self-service options may permit users to access or correct account details, manage optional consents, initiate deletion, or export eligible data. Customer Support assists with requests that cannot reasonably be fulfilled through self-service.

9.3. Timing and identity verification

Requests are assessed and answered within the timeframes established by applicable law. Where reasonably necessary to protect user information, HIGH BINARY may verify the identity or authority of the requester using a risk-based and proportionate approach. Additional verification should not exceed what is necessary for the relevant request.

9.4. Export, review, and appeal

Where a valid portability or access request is made, we may offer a downloadable export and/or a Customer Support-assisted delivery of eligible records. Users may request human review of legally significant automated decisions where applicable. If a request is refused or limited, we will provide an

explanation and information about available internal escalation and external remedies where legally required.

9.5. Request tracking and communications

Where available, users may track a privacy request through the platform and receive status updates through registered email and/or in-app notifications. HIGH BINARY will not discriminate against users for exercising protected privacy rights where such non-discrimination is required by law.

10 International Data Transfers

10.1. International hosting and processing

HIGH BINARY may operate using multiple geographic hosting and processing regions. Personal data may be stored, accessed, transmitted, or otherwise processed in countries other than the country in which a user resides, including by authorized providers supporting platform operations, security, payments, verification, analytics, and communication services.

10.2. Safeguards for international transfers

Where an international transfer is subject to legal restrictions, HIGH BINARY evaluates the applicable transfer rules and implements appropriate legal, contractual, technical, and organizational safeguards. These measures may include recognized adequacy mechanisms, approved standard contractual clauses (SCCs), other lawful transfer instruments, documented assessments, and supplementary controls where necessary.

10.3. International provider governance

International providers are managed through a centralized approach to service-provider oversight, including risk assessment, appropriate contractual terms, access restrictions, and review of their role in processing personal data. A provider is permitted to process only information appropriate to its function and applicable legal responsibilities.

10.4. Restricted cross-border access

Access to personal data from different countries or regions is governed by role-based restrictions and a zero-trust approach, including verification of users and systems, least-privilege permissions, session safeguards, monitoring, and additional controls for sensitive financial and identity records.

10.5. Encryption and secure transmission

HIGH BINARY applies encryption and secure transmission protocols appropriate to the sensitivity of transferred information. Measures may include TLS-protected connections, authenticated APIs, strong certificate and key management, and mutual TLS (mTLS) where suitable for specific systems or connections.

10.6. SCCs and adequacy decisions

Where a relevant jurisdiction recognizes an adequacy decision for the destination country and processing circumstances, HIGH BINARY may rely on that mechanism where applicable. Otherwise, recognized contractual or other legal safeguards, including SCCs where relevant, may be used following the required assessment. HIGH BINARY does not treat a transfer as legally authorized merely because encryption is in place.

10.7. Transparency and access to safeguards

Users may request information about relevant categories of international recipients, destination regions, and applicable safeguards through the contact channel in Section 13, subject to legitimate confidentiality, security, and legal limitations. We provide information and access to transfer safeguards as required by applicable law.

10.8. Monitoring and legal requirements

International transfer practices are reviewed when the Services, providers, risks, or legal requirements change. HIGH BINARY maintains organizational measures intended to address cross-border compliance obligations and to protect personal data throughout its processing lifecycle.

11 Children's Privacy & Age Restrictions

11.1. Minimum eligible age

HIGH BINARY is intended exclusively for adults who are at least 18 years old or the higher age of legal eligibility required by the law applicable to them. Persons below the applicable minimum age must not register for, access, or use the Services.

11.2. Age verification

Eligibility checks may combine an age declaration at registration with verification of official identity documents and other KYC information. Where applicable, further checks may be performed if discrepancies or underage-use indicators arise.

11.3. No parental-consent exception

HIGH BINARY does not permit a minor to open or maintain an account on the basis of parental or guardian consent. The prohibition applies to both real-money and demo accounts and to associated platform features.

11.4. Detection and response

HIGH BINARY may use relevant account, identity-verification, risk, and support information to detect suspected underage registration or use. Where credible evidence indicates that a person is underage, the account may be suspended promptly while the facts are verified.

11.5. Closure and lawful handling of balances

Where underage status is confirmed, HIGH BINARY will take appropriate steps to close the account, prevent further prohibited activity, and handle any associated balance or financial obligations in accordance with applicable law, contractual duties, and fraud-prevention requirements. Where a suspension results from an error, we will provide an appropriate process to correct the record and restore access when lawful.

11.6. Data deletion and retention

Personal data relating to confirmed minors is prioritized for deletion or de-identification unless continued retention is legally necessary, for example to document a prohibited transaction, meet a legal obligation, protect rights, or investigate misuse. Retained information is subject to access restrictions and the retention principles in Section 8.

11.7. Reporting concerns

Anyone who believes that an underage person has accessed the Services may contact HIGH BINARY at support@highbinarytrading.com so that the concern can be reviewed through the appropriate verification process.

12 Privacy Policy Updates & Changes

12.1. Right to Update the Privacy Policy

HIGH BINARY reserves the right to review, amend, or update this Privacy Policy from time to time to reflect changes in applicable laws and regulatory requirements, our services and trading features, technological developments, payment and withdrawal infrastructure, identity verification procedures, security practices, international operations, data processing activities, or other legitimate operational requirements.

Any amendments will be made in accordance with applicable data protection laws and the principles of lawfulness, fairness, transparency, and accountability. Updates to this Privacy Policy do not, by themselves, establish a new lawful basis for processing personal data or authorize processing that would otherwise require additional notice or consent.

12.2. Notification of Policy Changes

HIGH BINARY will communicate updates to this Privacy Policy through a combined notification system, using registered email addresses and notifications within the HIGH BINARY platform, as appropriate to the nature of the changes.

The current version of this Privacy Policy will remain accessible through our official website. Notifications may include a description of the changes, a link to the updated Privacy Policy, and relevant information regarding their effective date.

12.3. Notification of Material Changes

Where changes materially affect how personal data is collected, used, disclosed, retained, transferred, or otherwise processed, HIGH BINARY will provide an enhanced notification explaining the relevant changes.

Such notifications will ordinarily include:

- A clear summary of the material changes.
- A link to the updated Privacy Policy.
- The effective date of the revised provisions.
- Information about any actions users may need to take.
- A separate consent request where required by applicable law.

Material changes may include the introduction of new processing purposes, significant modifications to data-sharing practices, changes affecting international data transfers, or other developments that materially affect users' privacy rights.

Where legally required, users will receive advance notice and an appropriate opportunity to exercise their rights before the relevant changes take effect.

12.4. Effective Date of Changes

The effective date of each updated Privacy Policy will be clearly identified in the published document.

Minor editorial, administrative, or clarifying changes may become effective upon publication, provided that applicable law does not require additional notice or other measures.

For material changes, HIGH BINARY will provide reasonable advance notice, taking into account the nature of the changes, their potential impact on users, and applicable legal requirements.

Where urgent changes are necessary to address legal obligations, security vulnerabilities, fraud prevention, or other legitimate and time-sensitive circumstances, changes may take effect sooner where permitted by law. HIGH BINARY will provide appropriate notice as required.

12.5. User Consent for Significant Changes

Where an update introduces or modifies personal data processing activities that require consent under applicable law, HIGH BINARY will request the necessary consent before carrying out the relevant processing.

HIGH BINARY may provide granular consent controls through its Privacy Preferences functionality, allowing users to manage consent for specific optional processing activities, including marketing communications and non-essential cookies, where applicable.

Where required, consent will be obtained through a clear, affirmative action and will be recorded in accordance with applicable legal requirements.

Users may withdraw their consent through the available privacy controls or by contacting Customer Support, subject to applicable legal conditions.

Acknowledgment of an updated Privacy Policy, continued use of the platform, or failure to object will not be treated as a substitute for valid consent where an affirmative consent mechanism is legally required.

12.6. Previous Versions and Change History

HIGH BINARY will maintain a structured version management system for its Privacy Policy to support transparency, accountability, and accurate recordkeeping.

Where available, users will be able to access previously published versions through a public policy archive containing relevant version numbers, effective dates, and summaries of material changes.

HIGH BINARY will also maintain internal publication and revision records for compliance, administrative, and audit purposes.

The current version of the Privacy Policy will be clearly identified to help users distinguish it from previous editions.

12.7. User Responsibility to Review

Users are encouraged to review this Privacy Policy periodically and to read notifications concerning updates that may affect their personal data or privacy rights.

HIGH BINARY will make the current version reasonably accessible and will provide notifications of changes in accordance with this section and applicable legal requirements.

A user's responsibility to remain informed does not relieve HIGH BINARY of its legal obligations to provide appropriate privacy notices, obtain required consent, or respect applicable data protection rights.

12.8. Continued Use of Services Following Changes

Following the effective date of an updated Privacy Policy, the processing of personal data associated with continued use of HIGH BINARY will be governed by the applicable version of the Privacy Policy, subject to applicable law and any required notices, lawful bases, or consent.

For certain material changes, HIGH BINARY may request that users acknowledge the updated Privacy Policy before accessing or continuing to use relevant platform features.

Where separate consent is legally required for a particular processing activity, HIGH BINARY will request that consent independently. Continued use of the platform alone will not be considered sufficient to establish such consent.

Where a user declines an optional processing activity, HIGH BINARY will respect that choice in accordance with applicable law. Any resulting limitations on specific features will be communicated where relevant and legally permissible.

Users who have questions or concerns regarding changes to this Privacy Policy may contact HIGH BINARY Customer Support through the official support channels.

13 Contact Information & Privacy Inquiries

13.1. Contacting HIGH BINARY about privacy

For questions about this Privacy Policy, the processing of personal data, an account privacy setting, or the exercise of a privacy right, users may contact HIGH BINARY through Customer Support at support@highbinarytrading.com or through the official in-platform support channel.

13.2. Data protection responsibility

HIGH BINARY assigns responsibility for handling privacy inquiries and coordinating appropriate internal review. Where applicable law requires appointment of a Data Protection Officer (DPO) or another designated privacy representative, the relevant contact details will be made available through official privacy notices or contact channels.

13.3. Privacy rights requests

Users may submit access, correction, deletion, restriction, portability, objection, consent-withdrawal, and other applicable privacy requests through Account Settings or Customer Support. Requests should describe the desired action sufficiently to permit secure processing without unnecessarily disclosing additional sensitive data.

13.4. Complaints and escalation

Privacy concerns and complaints may be reviewed through an internal escalation process. If a user disputes the handling of a request, HIGH BINARY will explain the available review process and, where required, the right to challenge the outcome or raise the matter with a competent authority.

13.5. Response timeframes

HIGH BINARY processes privacy requests within time limits imposed by applicable law. If clarification, lawful identity checks, or a permitted extension is necessary, we will provide appropriate information about the request status or the applicable extension when required.

13.6. Verification of the requester

Before disclosing, changing, or deleting personal data, HIGH BINARY may verify the requester's identity or lawful authority using a proportionate, risk-based method. Additional documents are requested only where necessary for the relevant privacy or security purpose.

13.7. Supervisory authorities

Depending on the applicable jurisdiction, users may lodge a complaint with a competent data protection or privacy authority, including an authority responsible for their place of habitual residence, work, or an alleged infringement where the law provides that option. Contacting HIGH BINARY first is encouraged but does not remove a statutory right to lodge a regulatory complaint.

13.8. Official channels

The official website is https://highbinarytrading.com/. Privacy-related communications should be sent through the support address or the authenticated support features made available by HIGH BINARY. Security-related notifications may also be delivered through security@highbinarytrading.com; general platform notices may be delivered through notifications@highbinarytrading.com. Users should verify the sender and avoid disclosing credentials or sensitive identification documents to unverified contacts.

14 Automated Decision-Making & Profiling

14.1. Use of automated tools

HIGH BINARY may use rule-based or automated tools, and where applicable authorized provider technologies, to support identity verification, age and eligibility checks, fraud prevention, account security, transaction monitoring, service reliability, and other legitimate operational or compliance purposes. Some checks may help flag activity for manual review rather than making a final decision.

14.2. Data and factors considered

Depending on the specific process, automated assessments may consider account and verification status, identity-document validity, login or device anomalies, transaction patterns, technical signals, or compliance-related indicators. Such systems are subject to the data minimization, access, and security requirements described in this Policy.

14.3. Decisions with significant effects

Where applicable law restricts decisions based solely on automated processing that produce legal or similarly significant effects, HIGH BINARY will apply the necessary lawful conditions and safeguards. These may include meaningful information about the relevant decision process, the opportunity to provide additional context, human intervention, and the right to express a view or contest the decision, as required.

14.4. Human review and correction

Users who believe an automated or partially automated assessment is inaccurate or unfair may contact Customer Support. Where applicable, a trained person may review the relevant information, consider additional evidence, and correct, reverse, or maintain an outcome according to the facts, security obligations, and governing law.

14.5. Transparency and review of systems

HIGH BINARY seeks to identify and address inaccurate information, undue bias, unnecessary processing, and disproportionate outcomes in significant automated workflows. The fact that a system supports a process does not automatically mean that a legally significant decision is taken solely by automated means. Where a particular automated decision requires more detailed disclosure, it will be provided through the relevant notice or user request process, subject to lawful security and confidentiality restrictions.

15 Legal Compliance & Governing Privacy Laws

15.1. Applicable data protection requirements

HIGH BINARY processes personal data in accordance with the privacy, data protection, electronic communications, financial recordkeeping, and other legal requirements applicable to the relevant entity, processing activity, and user. The applicability of particular laws and individual rights may differ according to the user's location, the location of processing, and the nature of the Services.

15.2. Accountability and compliance practices

HIGH BINARY maintains policies and organizational measures intended to support lawful processing, access controls, appropriate security, consent administration where required, recordkeeping, data-subject requests, risk-based provider management, and the secure handling of personal data incidents. Compliance measures are reviewed as laws, services, and operational circumstances evolve.

15.3. Lawful requests and preservation

Where required or permitted by applicable law, HIGH BINARY may preserve or disclose relevant information in response to valid court orders, lawful regulatory requests, investigations, or legal proceedings. Such requests are handled with regard to their legal basis, scope, confidentiality, and proportionality.

15.4. No waiver of mandatory privacy rights

Nothing in this Privacy Policy is intended to exclude, restrict, or waive rights or protections that cannot lawfully be limited under applicable data protection or consumer laws. Any dispute-resolution or choice-of-law provisions in other platform documents operate subject to mandatory privacy rights and competent supervisory-authority powers.

15.5. Relationship to other documents

This Privacy Policy explains the handling of personal data. It should be read together with the Terms of Service, any applicable Cookie Notice, and specific privacy notices provided when users activate a particular feature. Where a separate notice is necessary for a legally significant processing activity, HIGH BINARY will provide that notice as required.

15.6. Privacy contact and policy interpretation

For information about how applicable privacy laws affect your data or the exercise of your rights, contact support@highbinarytrading.com. In the event of an inconsistency between this Policy and a mandatory legal requirement, that legal requirement prevails to the extent of the inconsistency.