Privacy Policy

This privacy notice ("Privacy Policy") explains how we collect, use, store, and share personal information at Beltic Inc. ("we," "our," or "us"). It applies to your interactions with us, including when you:

- Visit our website;
- Use our services directly;
- Are an end user of a client who integrates our technology (e.g., via API or SDK);
- Engage with us in other ways, such as through sales, support, or events.

If you have any questions, contact us at privacy@beltic.com.

1. Information We Collect

We may collect or receive the following categories of personal information:

From individuals or their devices:

- Full name
- Email address
- Phone number
- Mailing address
- Job title or role
- Username and password (if applicable)
- Government-issued ID details (e.g., driver's license, passport)
- Financial data (e.g., account numbers, creditworthiness, payment instrument details)
- Selfie or biometric data for identity verification (e.g., facial images, facial geometry, document scans). Such data is processed only with explicit user consent and used solely for the purpose of verifying identity or detecting fraud. We apply industry-standard

safeguards including encryption, access controls, and retention limits in line with applicable laws. Biometric data is not shared with third parties except with subprocessors operating under strict confidentiality and only to the extent necessary to provide verification services. Retention of biometric information is limited to the shortest duration necessary for processing, unless otherwise required by contractual, regulatory, or legal obligations. Upon request or expiration of the retention period, biometric data is securely deleted.

- Device information (IP address, browser type, OS, language, hardware identifiers)
- Geolocation and time zone
- Typing patterns, device behavior, and interaction metadata
- Transaction details, risk signals, and behavioral patterns, including device motion, typing cadence, mouse movement, screen interaction timing, swipe velocity, tap frequency, and indicators of coordinated or scripted activity. These data points may be used to establish behavioral baselines, detect anomalies, identify automated or bot-like usage, and prevent fraud across sessions and devices.
- Social media data, if login via social platforms is enabled

From clients, businesses, and third parties:

- KYC/KYB onboarding documentation
- Business registration, beneficial ownership, and incorporation records
- Business address and contact information
- Tax ID or business license numbers
- Risk scores or fraud indicators
- Information from data providers, sanctions lists, or public databases
- Chargeback, dispute, or suspicious activity metadata
- Information from device fingerprinting or behavioral analytics tools
- Fraud history or watchlist match status from external partners

© 2025. Beltic, Inc.

We collect this information either directly from you, from our clients (including regulated institutions), or from integrated third-party sources, depending on the use case. We take reasonable steps to ensure the accuracy, completeness, and relevance of the data we collect.

2. How We Use Your Information

We use personal data to:

- Facilitate identity and business verification (KYC/KYB)
- Conduct AML screening against sanctions, PEP, and watchlists
- Detect fraud, duplicate accounts, or suspicious activity
- Score transactions, users, or businesses for fraud or risk
- Monitor behavioral signals (e.g., typing cadence, geolocation, device motion)
- Analyze device fingerprinting and session metadata
- Cross-reference data with fraud consortiums and external blacklists
- Identify account takeovers, bot activity, or coordinated abuse
- Track prior fraud activity, chargeback or dispute trends
- Maintain security of accounts and infrastructure
- Provide and maintain services, integrations, and infrastructure
- Inform product improvement or business decision-making
- Support client compliance with applicable laws and regulations
- Comply with legal, regulatory, or contractual obligations

We implement strict internal controls to ensure personal data is only accessed by authorized personnel for approved use cases.

We do **not** sell personal data. We do **not** use data for advertising or marketing purposes. Most of our data processing occurs behind the scenes and is not visible to the end user. However, in

some flows—such as when document uploads or selfies are required—users will interact directly with our tools.

We may aggregate or anonymize data for statistical or research purposes, product development, or fraud benchmarking, ensuring it is no longer identifiable.

3. How We Share Information

We do not sell personal data. We only share information as follows:

- With service providers or subprocessors under contract who assist with infrastructure, identity verification, device fingerprinting, fraud analytics, biometric authentication, behavioral analytics, storage, customer support, and other operational functions
- With clients, in the course of providing our services (including risk scoring, verification outcomes, audit logs, and fraud signal data)
- With fraud consortiums or external databases for fraud detection, risk intelligence, or sanctions screening
- With affiliates or subsidiaries under common ownership, for internal administrative purposes
- In the event of a business transfer, merger, divestiture, or acquisition
- When required to comply with law, regulation, subpoena, court order, or law enforcement request

We require all third parties with whom we share data to adhere to strict confidentiality, security, and data handling standards. We review contracts, conduct diligence, and limit onward sharing by such parties. Information is not used beyond what is necessary to fulfill their function. We may disclose anonymized or aggregated information without restriction.

4. Data Retention

We retain personal information only as long as necessary to:

- Fulfill the purposes it was collected for
- Maintain a user, developer, or customer account

- Support compliance investigations, chargeback analysis, and audit logs
- Meet fraud prevention, AML screening, and sanctions monitoring obligations
- Comply with legal, regulatory, tax, and contractual requirements

When no longer needed, we securely delete or irreversibly anonymize the data, unless a longer retention period is required or permitted by law. If we process data on behalf of a client (such as a bank or enterprise), retention may follow their internal policy or regulatory schedule. For biometric or sensitive data, we retain information only for the duration permitted by applicable law, contractual obligations, or your explicit consent.

Retention periods may also depend on factors such as ongoing investigations, litigation holds, audit requirements, or fraud review needs.

5. Security Measures

We implement appropriate technical and organizational measures to protect personal data, including:

- Encryption in transit and at rest
- Access control and authentication protocols
- Regular vulnerability scanning and penetration testing
- Logging and monitoring for anomalous access
- Data segregation, backup, and recovery systems

Despite our safeguards, no method of transmission over the Internet or electronic storage is 100% secure. We maintain incident response and breach notification procedures in accordance with applicable laws.

6. Your Rights and Choices

Depending on your location and applicable law (such as GDPR, CCPA, or VCDPA), you may have rights that include:

- Requesting access to the personal data we hold about you (we will review and share it upon validation)
- Requesting correction or deletion of inaccurate or outdated information
- Objecting to or restricting certain processing activities
- Withdrawing consent where processing is based on consent
- Requesting a copy of your data in a portable format
- Requesting information about categories of personal data we collect, use, and share
- Appealing decisions we make regarding your data rights requests

To exercise any of these rights, contact us at privacy@beltic.com. We may require you to verify your identity before processing your request. We will respond within the timeframe required by applicable law, typically within 30 days. If we deny a request, we will provide a justification and offer an opportunity to appeal.

We do not discriminate against users for exercising privacy rights.

7. Minors and Age Restrictions

Our services are not directed to individuals under 18. We do not knowingly collect or solicit personal information from individuals under the age of 18. If you believe that a minor may have provided us with personal information without proper consent, please contact us immediately at privacy@beltic.com. Upon receiving such notice, we will take reasonable steps to verify the identity of the reporting party and promptly delete any associated data if applicable. Parents or legal guardians may also request access to, or deletion of, their child's information if it was inadvertently collected. We do not knowingly collect data from minors. If we become aware of such data collection, we will delete it promptly.

8. Embedded Use and White Labeling

We may provide services in embedded or white-labeled forms through clients. In these scenarios, we operate under contractual obligations with our clients, and they are primarily responsible for managing the relationship with end users. Any access, correction, or deletion requests regarding user data should be routed through the respective client, who may then submit a verified request to us for processing. We do not directly interact with end users in such cases, nor do we assume liability for client-side disclosures or consent collection. However, we

take appropriate steps to ensure data is handled securely, processed solely for the purposes authorized by the client, and retained only for as long as necessary to fulfill those purposes or meet legal obligations. In such cases:

- We may process user data without direct interaction
- Our clients are responsible for surfacing appropriate privacy notices and collecting user consent
- We operate under contractual obligations with clients, and any rights requests should be submitted to the client when they are the primary interface with end users

9. Do Not Track

Our services do not respond to Do Not Track signals at this time. If a standard is adopted in the future, we will update this policy accordingly.

10. Regional Disclosures

If you reside in California, Virginia, or the European Economic Area, you may be entitled to additional privacy rights under CCPA, VCDPA, or GDPR, respectively. You may request:

- Information about how your data is collected and used
- A list of categories of personal data processed
- Deletion or correction of data
- Appeals if your data request is denied

Please contact us at privacy@beltic.com for more information. We cooperate with regulators and supervisory authorities as required.

11. Updates to This Policy

We may update this policy from time to time. When we do, we will revise the "Last Updated" date. If we make material changes to how we handle your personal data or your rights, we will notify you by sending an email to the address associated with your account (if applicable) or by displaying a prominent notice within our service or on our website prior to the changes taking

effect. When we do, we will revise the "Last Updated" date. Material changes will be communicated appropriately.

12. Contact Us

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

Beltic Inc.
751 Duncan St, San Francisco, CA 94131
Email: privacy@beltic.com

Last Updated: July 16th, 2025.