

Privacy Policy

Last Updated: September 7, 2025

Beltic Inc. (“Beltic,” “we,” “us,” or “our”) provides fraud verification and compliance services (the “Service”). Individuals may be invited by our business customers to submit identification and proof-of-address documents, which we process on behalf of those customers. In that context, we act as their service provider/data processor and handle your information only on their documented instructions.

This Policy summarizes how we collect, use, and safeguard information. It is not a contract and does not create rights beyond applicable law. Your use of the Service is also governed by our Terms of Use.

Information We Collect

In short: We collect contact details, documents and the data they contain, verification results, and technical information necessary to operate and secure the Service.

Full explanation: When you or our business customers use the Service, we may process the following categories of personal information:

1. Contact Information

- **What this includes:** Your email address, as well as any communications you send us (such as support inquiries or responses).
- **Why we collect it:** To deliver verification results, provide updates, and respond to requests from you or our business customers.

2. Documents & Contained Data

- **What this includes:** Identification documents (such as passports, driver’s licenses, ID cards, visas, or tax identifiers) and proof-of-address files (such as utility bills, rental agreements, or official correspondence). We also extract necessary fields like your name, date of birth, address, document number, issuing country, and expiry date.
- **Why we collect it:** To perform verification checks, validate authenticity, and meet legal and regulatory compliance requirements.

3. Derived Verification Data

- **What this includes:** Automated and human-reviewed outcomes from the verification process, such as validation flags, match/tamper indicators, fraud or anomaly alerts, analyst notes, exception handling, and audit logs of verification activity.
- **Why we collect it:** To determine whether documents are authentic, maintain an audit trail, support fraud detection, and provide customers with accurate results.

4. Technical & Security Data

- **What this includes:** IP addresses, device and browser characteristics, session times, access history, navigation data, timestamps, and other metadata generated while using the Service.
- **Why we collect it:** To operate the platform reliably, enforce security, prevent misuse, troubleshoot errors, and generate logs for compliance and monitoring purposes.

How We Use Information

In short: We use your information to deliver and improve our verification Service, protect against fraud, provide support, comply with legal obligations, and strengthen our systems. We never sell personal information, use it for advertising, or train generalized AI models on it.

Full explanation: We process personal information strictly to provide the Service and meet our legal and contractual obligations. This includes:

1. Service Delivery

- **What this means:** We collect and process your documents and related data in order to verify accuracy, confirm authenticity, and deliver verification results to our business customer or to you directly.
- **Why we do it:** Without this processing, we would not be able to provide the core verification services you or our customers request.

2. Fraud Prevention & Integrity

- **What this means:** We analyze data to detect anomalies, prevent fraudulent submissions, and maintain secure and traceable audit trails.
- **Why we do it:** Fraud prevention is the foundation of our Service, and maintaining system integrity ensures trust for all customers and end-users.

3. Support & Troubleshooting

- **What this means:** We use contact information and activity logs to respond to support requests, investigate technical issues, and provide guidance to our business customers.
- **Why we do it:** Effective troubleshooting helps ensure smooth operation and timely resolution of problems.

4. Legal & Compliance

- **What this means:** We process information to comply with laws, regulations, and audit requirements related to anti-fraud, financial, and data protection obligations.
- **Why we do it:** Our customers often operate in regulated industries, and compliance is essential for us to provide lawful services.

5. Service Improvement

- **What this means:** We may use aggregated or de-identified information (never identifiable documents) to improve our fraud detection models, security practices, and operational efficiency.
- **Why we do it:** Continuous improvement ensures our Service remains effective and aligned with evolving fraud patterns and industry standards.

Sharing

In short: We share personal information only when necessary — with trusted vendors, lawful authorities, professional advisors, or as part of business transactions. Otherwise, we disclose data only if explicitly authorized by our customer.

Full explanation: Beltic may disclose personal information under limited and controlled circumstances:

1. Vendors & Service Providers

- **What this means:** We rely on carefully selected vendors to support our operations. This includes secure transfer through **SendSafely** and other subprocessors that may handle data strictly under our instructions.
- **Why we do it:** These providers enable us to deliver the Service effectively while maintaining required security standards.

2. Professional Advisors & Lawful Authorities

- **What this means:** We may disclose information to auditors, legal counsel, regulators, courts, or law enforcement agencies when it is legally required or otherwise appropriate under applicable law.
- **Why we do it:** This ensures compliance with our legal and regulatory obligations and provides transparency when responding to lawful requests.

3. Business Transactions

- **What this means:** If Beltic is involved in a merger, acquisition, financing, or sale of assets, personal information may be shared with relevant parties under strict confidentiality protections.
- **Why we do it:** Such disclosures are a standard part of legitimate corporate transactions and are conducted with safeguards to protect individuals' data.

4. Customer Authorization

- **What this means:** We only share personal information with third parties outside of the categories above when our business customer (the data controller) explicitly instructs or authorizes us to do so.
- **Why we do it:** This reflects our role as a service provider/processor — we act only under our customers' documented instructions.

Security

In short: We apply strict administrative, technical, and organizational safeguards to protect your information, including encryption, access controls, monitoring, and employee training. While no system is completely secure, we take robust steps to minimize risks and respond quickly to incidents.

Full explanation: Because the Service involves sensitive verification data, Beltic implements layered security measures designed to prevent unauthorized access, misuse, or loss of information. These include:

1. Encryption

- **What this means:** All data is encrypted both in transit and at rest. This includes end-to-end encrypted intake via **SendSafely** for document submissions.
- **Why we do it:** Encryption ensures that sensitive information cannot be intercepted or accessed without authorization.

2. Access Controls

- **What this means:** We enforce strict role-based access and least-privilege policies, allowing employees or contractors to access only what is necessary for their role. Multi-factor authentication and secure credential practices are required.
- **Why we do it:** Limiting access reduces the likelihood of accidental or malicious misuse.

3. Monitoring & Logging

- **What this means:** We maintain continuous logging and monitoring of access, system activity, and changes, enabling full traceability and auditability.
- **Why we do it:** Monitoring provides visibility into unusual or suspicious activity and helps ensure accountability.

4. Network & System Security

- **What this means:** We use firewalls, intrusion detection systems, regular vulnerability scanning, and timely patch management.
- **Why we do it:** These measures reduce the risk of cyberattacks and system breaches.

5. Employee Training & Confidentiality

- **What this means:** All staff handling personal information receive mandatory training on data protection, fraud risks, and confidentiality obligations.
- **Why we do it:** Awareness and accountability are critical for preventing human error and maintaining compliance.

6. Incident Response

- **What this means:** We maintain formal procedures to detect, investigate, and remediate security incidents. This includes timely breach notifications in line with GDPR, LGPD, and CCPA requirements.
- **Why we do it:** Rapid response reduces harm and ensures compliance with global regulatory obligations.

Important to note: While Beltic takes extensive precautions, **no system is 100% secure**. To the maximum extent permitted by law, we are not responsible for unauthorized access outside our reasonable control (such as issues with your device, your personal network, or malicious third-party actions), except where caused by our gross negligence or willful misconduct.

Global Privacy Commitment

In short: We follow global privacy and data protection laws, including GDPR, CCPA/CPRA, and LGPD. If you submitted documents through one of our business customers, please contact them to exercise your rights. If you submitted directly to Beltic, you can contact us to request access, correction, deletion, or other rights available under law.

Full explanation: Beltic is committed to handling personal information in compliance with international privacy and data-protection frameworks, including but not limited to:

- **GDPR (EU/UK)** — General Data Protection Regulation.
- **CCPA/CPRA (US)** — California Consumer Privacy Act / California Privacy Rights Act.
- **LGPD (Brazil)** — Lei Geral de Proteção de Dados.
- Other national or sectoral privacy laws where our customers operate.

Your Rights Depend on Context

1. If you submitted documents at a customer's request

- **What this means:** We are acting as a service provider/processor on behalf of that business.
- **Your rights:** Please contact that business directly to exercise your rights (e.g., access, correction, deletion).

- **Our role:** We will fully support the customer in responding to your request in compliance with applicable law.

2. If you submitted directly to Beltic

- **What this means:** We may be the controller of your personal information.
- **Your rights:** Depending on the law that applies, you may request:
 - **Access** to a copy of your personal data.
 - **Correction** of inaccurate or incomplete data.
 - **Deletion/Erasure** of your information, subject to legal and contractual obligations.
 - **Restriction** of certain types of processing.
 - **Portability** to receive your data in a structured, machine-readable format.
 - **Objection** to processing carried out under legitimate interests.
 - **Withdrawal of consent**, where processing is based on consent.

How to exercise rights: You can submit these requests by contacting us at privacy@beltic.com. We will respond in accordance with applicable law.

International Transfers

In short: Your information may be transferred outside your country, including to the United States. We apply legal, contractual, and technical safeguards to ensure it remains protected wherever it goes.

Full explanation: Because Beltic serves global customers, personal information may be processed in countries other than where it was originally collected. This includes transfers to the United States and other jurisdictions where our systems, service providers, or customers operate.

To protect your information, we apply the following safeguards:

1. Standard Contractual Clauses (SCCs)

- **What this means:** For transfers from the EU, UK, or other regions requiring adequacy, we use SCCs approved by regulators.
- **Why we do it:** SCCs are a recognized legal mechanism that ensures your data receives protections consistent with GDPR standards.

2. Vendor Contractual Commitments

- **What this means:** We require our subprocessors and service providers to contractually commit to equivalent protections, confidentiality, and compliance with applicable data protection laws.
- **Why we do it:** This ensures that any third party handling data on our behalf meets the same standards we apply internally.

3. Technical Safeguards

- **What this means:** We use encryption (in transit and at rest), access restrictions, and secure transmission channels for all international data transfers.
- **Why we do it:** Technical measures add an additional layer of protection beyond legal contracts, reducing the risk of unauthorized access during transfer.

These measures help ensure that, no matter where your data travels, it receives a consistent and lawful level of protection.

Retention

We retain personal information only as long as necessary to provide the Service, comply with law or contract, and maintain audit trails. Typical retention for uploaded documents and verification results is 30 days, after which we securely delete or irreversibly de-identify them (unless our customer instructs otherwise).

Your Responsibilities

Submit only the information requested, ensure it is accurate, and do not include unrelated sensitive data. If you submit information about others, you confirm you are authorized to do so.

Age Limit

The Service is intended for individuals aged 18+ (or the age required by local law). Do not use the Service or submit information if you do not meet this threshold.

Changes

We may update this Policy from time to time. The “Last Updated” date reflects the latest version. Continued use of the Service constitutes acknowledgment of the updated Policy.

Contact Us

Beltic Inc.
Email: privacy@beltic.com

Archived Versions:

Privacy Policy

Last Updated: September, 2025.

This Privacy Policy (“Policy”) explains how **Beltic Inc.** (“Beltic,” “we,” “our,” or “us”) collects, uses, processes, stores, and safeguards personal information in connection with the provision of our **fraud verification services** (the “Services”) to **Invisible** (“Customer,” “you,” or “your”).

Beltic’s Services combine technology and **agents verification tools** to analyze documents, records, and supporting data for the purpose of fraud detection and compliance. Because these Services handle **sensitive personal information** across jurisdictions worldwide, this Policy has been designed to comply with applicable international data protection laws and frameworks, including but not limited to:

- General Data Protection Regulation (GDPR) (EU/UK)
- California Consumer Privacy Act (CCPA/CPRA) (United States)
- Lei Geral de Proteção de Dados (LGPD) (Brazil)
- Other global privacy regulations where Customer operates

This Policy governs our processing of data as a **data processor**, acting on instructions provided by Customer (the data controller).

1. Scope of Processing

This Policy applies to all personal information processed by Beltic in connection with the Services. It covers:

- Data and documents uploaded by Customer or its authorized users;
- Personal information analyzed during fraud verification workflows;
- Metadata, logs, and system outputs generated by the Services;
- Processing carried out on behalf of Customer under contract.

Beltic does not determine the purposes of processing. Instead, we act strictly on Customer's documented instructions.

2. Categories of Information We Process

(a) Customer-Provided and Uploaded Information

The Services may involve processing of personal information contained in:

- **Government Identifiers:** passports, ID cards, driver's licenses, visas, national insurance/tax numbers from multiple countries.
- **Proof of Address Documents:** utility bills, rental agreements, official correspondence.
- **Contact and Identity Information:** full name, email, phone number, addresses, signatures.

(b) Service-Generated Information

When using the Services, Beltic may also generate or collect:

- **Audit Logs:** detailed records of access, changes, and decisions made by agents or systems.
- **Usage Data:** IP addresses, session times, access history, navigation within the platform.

- **Verification Metadata:** fraud detection outcomes, decision confidence scores, analyst notes, exceptions or flags.

(c) Third-Party Information

- Beltic relies on **Send Safely** for secure file transfer and upload. Information transmitted through Send Safely may include any of the categories above.

3. Purposes of Processing

Beltic processes personal information solely to provide the Services to Customer, including:

1. **Fraud Verification:** To validate documents and identities, detect anomalies, and flag fraudulent activity.
2. **Human-in-the-Loop Operations:** To enable authorized analysts to review, validate, and escalate cases requiring judgment.
3. **Service Delivery and Maintenance:** To operate, maintain, and enhance the Services.
4. **Security and Integrity:** To protect against unauthorized access, misuse, or fraud, and to ensure traceability.
5. **Compliance:** To satisfy legal, regulatory, and contractual requirements applicable to fraud prevention.
6. **Support and Communication:** To respond to Customer inquiries, provide technical support, and share relevant updates.
7. **Research and Improvement:** To analyze aggregated or anonymized usage data for improving fraud detection models.

We do not sell, rent, or use personal information for advertising or unrelated commercial purposes.

4. Legal Basis for Processing

When required by law (e.g., GDPR, LGPD), the legal grounds on which Beltic relies include:

- **Performance of Contract:** Processing necessary to deliver the Services.

- **Legal Compliance:** Processing necessary to comply with anti-fraud, financial, and regulatory obligations.
- **Legitimate Interests:** Processing necessary for fraud prevention, information security, and operational improvement, provided such interests are not overridden by individuals' rights.
- **Consent:** In cases where a customer obtains consent from individuals for specific processing.

5. Disclosure of Personal Information

Beltic may disclose personal information under the following circumstances:

- **Vendors and Service Providers:** We use **Send Safely** as a secure document transfer service provider. Additional subprocessors may be engaged only with Customer's authorization.
- **Legal Requirements:** To law enforcement, courts, regulators, or competent authorities when legally required.
- **Business Transactions:** In connection with a merger, acquisition, financing, or sale of assets, under confidentiality safeguards.
- **Consent or Direction:** When explicitly authorized by Customer.

Beltic does not disclose personal information to unauthorized third parties or any other party not previously authorized by the Customer.

6. International Transfers

Personal information may be transferred and processed outside of the country where it was originally collected, including to the United States. Beltic ensures such transfers are subject to appropriate safeguards, such as:

- Standard Contractual Clauses (SCCs) approved by the European Commission or UK authorities;
- Contractual commitments with vendors ensuring equivalent protection;

- Technical measures including encryption and access restrictions.

7. Security Measures

Given the sensitivity of fraud verification data, Beltic implements robust administrative, technical, and organizational measures, including:

- Encryption: Data encrypted in transit and at rest, including via Send Safely transfers.
- Access Controls: Role-based permissions, least-privilege policies, and authentication safeguards.
- Monitoring & Logging: Continuous logging of access and activity for traceability and auditing.
- Network Security: Firewalls, intrusion detection, and vulnerability management.
- Employee Training: Mandatory training on data protection, confidentiality, and fraud risks.
- Incident Response: Established breach detection, reporting, and remediation procedures aligned with GDPR, LGPD, and CCPA obligations.

8. Data Retention

We retain personal information only as long as necessary to:

- Provide the Services and complete verification workflows;
- Comply with legal, regulatory, and contractual obligations;
- Maintain audit trails for fraud prevention and compliance.

After retention periods expire, data is securely deleted or anonymized, unless further retention is legally required.

9. Rights of Individuals

Depending on applicable law, individuals whose data is processed may have the right to:

- Access: Obtain confirmation and a copy of personal information.
- Correction: Request updates to inaccurate or incomplete data.
- Deletion: Request erasure of personal information, subject to legal requirements.
- Restriction: Limit processing in certain circumstances.
- Portability: Receive data in a structured, machine-readable format.
- Objection: Object to processing carried out under legitimate interests.
- Withdraw Consent: Revoke consent previously provided.

Beltic will support Customer in responding to such requests, as Customer is the data controller responsible for fulfilling them.

10. Processor Obligations

When acting as a data processor on behalf of Customer:

- Beltic processes personal information only in accordance with Customer's documented instructions;
- Beltic ensures confidentiality obligations for all employees and agents;
- Beltic engages subprocessors only with notice and contractual safeguards;
- Beltic assists Customer in meeting compliance requirements (e.g., data subject requests, breach notifications, audits);
- Beltic makes available necessary information to demonstrate compliance.

11. Updates to this Policy

We may amend this Policy from time to time to reflect changes in law, technology, or operational practices. Updates will include a revised "Last Updated" date and will be communicated to Customer. Continued use of the Services constitutes acknowledgment of the updated Policy.

12. Contact Us

If you have questions or requests regarding this Privacy Policy or our data practices, please contact:

Beltic Inc.

Email: **privacy@beltic.com**