

TECTRIL

INTEGRITY REPORTING CHANNEL PRIVACY NOTICE

How we process personal data related to reports, investigations and integrity measures

TRANSPARENCY AND PROTECTION. Tectril processes Integrity Reporting Channel data for defined purposes, with restricted access, confidentiality and proportionate security. This Notice explains what data may be processed, why it is needed and the rights of the persons involved.

Document	Version	Effective date
Integrity Reporting Channel Privacy Notice	Revision 0	July 18, 2026

TECTRIL SOLUÇÕES EM LOGÍSTICA E COMÉRCIO LTDA
Caieiras — São Paulo — Brazil

Document control

Field	Definition
Controller	Tectril Soluções em Logística e Comércio Ltda
Owner	Tectril Management
Management	Person formally appointed for Integrity and Compliance, supported by the data protection function
Approval	Tectril Management
Review	Annually or following a relevant change to the Channel, processing operations or law
Related documents	Code of Business Ethics and Conduct; Integrity Reporting Channel Policy; Information Security Policy; Records Management Policy

1. Who is responsible for the data

Tectril Soluções em Logística e Comércio Ltda is the controller of personal data processed through the Integrity Reporting Channel because it determines the purposes and principal means of receiving, assessing, investigating, deciding, remediating and retaining reports.

Technology, hosting, security, investigation, legal, audit and other providers may act as processors or independent controllers depending on the activity and applicable contract.

The official contact for privacy matters and data subject requests is privacidade@tectril.com.br. The recommended subject line is “Privacy — Integrity Reporting Channel” to support secure routing.

2. Who this Notice covers

This Notice covers personal data related to:

- persons submitting identified reports;
- persons choosing not to identify themselves where the report or technical data permits direct or indirect identification;
- persons accused, mentioned or connected with the facts;
- witnesses, employees, representatives and consulted third parties;
- investigators, screening officers and persons deciding or implementing measures;
- persons appearing in documents, messages, images, audio, video or other attachments.

3. Personal data we may process

3.1. Reporting person data

- name, position, company and relationship with Tectril;
- email, telephone number and contact preference;
- statements, opinions, documents and evidence submitted;
- information needed to assess protection against retaliation;

- communication records and supplements.

3.2. Data about involved persons

- identity, role, company and connection with the facts;
- alleged conduct, statements and accounts provided;
- relevant professional, contractual, financial, operational, tax, customs or system records;
- preservation, investigation, remediation or accountability measures;
- witness and other relevant-source information.

3.3. Sensitive and higher-risk data

Where relevant, a report may contain health, biometric, racial or ethnic origin, religion, political opinion, trade union membership, sex life, sexual orientation or other data receiving enhanced legal protection.

It may also contain allegations of fraud, harassment, discrimination, corruption, offenses, proceedings or sanctions, as well as financial data, identification documents and other high-impact information.

Such data must not be included out of curiosity. It will only be processed where necessary, appropriate and related to the report or the exercise of rights.

3.4. Technical data and attachments

Use of the form may generate date and time, session identifiers, browser, device, security logs and, depending on technical configuration, IP address information.

Attachments may contain metadata, authorship, history, geolocation, image, voice or other identifying data. A person wishing not to be identified should review attachments and avoid including information revealing their identity.

4. Sources of data

Data may be obtained directly from the reporting person; interviewed or consulted persons; documents and evidence provided by involved persons; authorized corporate systems, records, devices, emails and files; clients, suppliers, partners, carriers, agents and providers; legitimate public sources and authorities; and authorized advisers, auditors or investigators.

5. Purposes of processing

We may process data to:

- receive, record and acknowledge reports;
- screen, preliminarily assess and evaluate risks;
- identify conflicts and arrange independent routing;
- seek clarification and receive supplements;
- preserve records, systems and evidence;
- investigate facts and interview persons;
- prevent, detect, stop and remediate misconduct;
- protect reporting persons, witnesses and others against retaliation;
- decide and implement corrective, disciplinary, contractual or legal measures;
- cooperate with audits, inspections and competent authorities;

- exercise rights in administrative, arbitral or judicial proceedings;
- comply with legal, regulatory and contractual duties;
- assess the Integrity Program through aggregate information;
- protect Channel security and prevent abuse, fraud and unauthorized access.

6. Legal bases

Consent is generally not the primary legal basis because withdrawal could compromise duties, investigations and the exercise of rights.

Depending on the circumstances, processing may rely on:

Category	Possible legal bases
Personal data generally	Compliance with a legal or regulatory obligation; performance of a contract or related procedures; regular exercise of rights; legitimate interests of Tectril or a third party, subject to necessity assessment and safeguards; protection of life or physical integrity where applicable.
Sensitive personal data	Compliance with legal or regulatory obligations; regular exercise of rights; protection of life or physical integrity; fraud prevention and data subject security in identification processes where applicable; other situations authorized by the LGPD.
Children's and adolescents' data	Exceptional processing limited to what is necessary and guided by the child's or adolescent's best interests, protection and safety.

The applicable basis will be assessed according to the purpose, data type, relationship and context.

7. Identified, confidential and non-identified reports

In an identified report, Tectril knows the reporting person's identity but restricts access to persons who need it for case handling.

For a report without identification, name, email and telephone are not required. However, narrative content, attachments and certain technical logs may permit indirect identification. Tectril therefore uses the expression "without identification" and does not promise absolute technical anonymity.

Without contact or tracking functionality, Tectril may be unable to seek clarification, communicate closure or respond to requests connected with the report.

8. Data sharing

Sharing will be limited to what is necessary and may involve:

- the Channel Officer, formally appointed alternate and authorized investigators;
- non-conflicted Management or decision makers;
- legal advisers, auditors, experts and independent investigators;
- form, hosting, storage, security, communications and technical-support providers;
- insurers, financial institutions or partners where strictly necessary and lawful;
- competent police, administrative, tax, customs, judicial or regulatory authorities;
- other persons or organizations where needed to protect rights, safety or legal compliance.

A person mentioned in a report does not receive the reporting person's identity merely because they were mentioned. Information will be provided consistently with defense rights, third-party protection, confidentiality and investigation integrity.

9. International transfers

Technology, storage, security or support providers may process data in other countries. Where an international transfer occurs, Tectril will seek providers, contracts and mechanisms compatible with the LGPD and limit data to what is necessary.

Server and subprocessor locations must be confirmed before publication and retained in Tectril's processing records.

10. Retention

Data will be retained for as long as needed for Channel purposes, remediation, the Integrity Program, exercise of rights and compliance duties.

As an initial internal rule, a case file will be retained for five years after closure, subject to periodic necessity review. The period may be extended for an ongoing investigation, legal or contractual obligation, preservation measure, audit, inspection, judicial, administrative or arbitral proceeding, or documented legal risk.

When the period expires and no basis remains, data will be securely deleted or anonymized. Backups follow the applicable technical replacement cycle.

11. Security and access control

Tectril will apply risk-based measures such as need-to-know access, individual permissions, authentication, periodic access review, segregation of sensitive cases and conflicted persons, protected transmission and storage, backup protection, access logging where available, confidentiality commitments, vulnerability remediation, incident response and evidence chain-of-custody controls.

No system is completely risk free. If an incident may create relevant risk or harm, Tectril will assess it and make communications required by the LGPD and ANPD regulations.

12. Automated decisions

Tectril does not intend to impose sanctions or determine responsibility solely through automated decisions. Tools may assist with organization, security, classification or research, but material decisions require appropriate human review.

13. Data subject rights

Subject to applicable law, a data subject may request:

- confirmation that processing exists;
- access to their own data, subject to third-party rights;
- correction of incomplete, inaccurate or outdated data;
- information on sharing;

- anonymization, blocking or deletion of unnecessary or unlawfully processed data;
- objection or review where applicable;
- information on consequences of not providing certain data;
- petition before Brazil's National Data Protection Authority.

Rights may be lawfully limited to protect another person's identity, preserve evidence, avoid compromising an investigation, comply with an obligation or exercise rights. Tectril will explain the applicable reason where a request cannot be fully granted.

Reasonable information may be requested to verify identity and prevent unauthorized access. Requests by representatives or concerning deceased persons require proof of authority.

14. Responsibilities of Channel users

Anyone submitting a report must act in good faith, provide only relevant information and avoid excessive, intimate or unrelated personal data.

Where possible, third-party documents should be limited to the necessary portions. The Channel must not be used to expose persons publicly, share illegal content or replace emergency services.

15. Updates

This Notice may be updated due to legal, regulatory, technical or operational changes. The current version will show the revision date and be available with the Integrity Reporting Channel. Material changes may be communicated by additional means where appropriate.

16. Contact and exercise of rights

For privacy questions or data subject requests concerning Channel data, use:

- Privacy contact: privacidade@tectril.com.br;
- Recommended subject: "Privacy — Integrity Reporting Channel";
- Official website: www.tectril.com.br.

canaldeetica@tectril.com.br may be used for questions about Channel operation, but it must not be presented as anonymous or replace the dedicated privacy contact after formal designation.

17. Approval

Responsibility	Name/Position	Date	Signature
Preparation			
Legal/LGPD review			
Validation of privacy contact			
Approval			

Legal references

- BRAZIL. Law No. 13,709/2018 — Brazilian General Data Protection Law — LGPD, as amended.
- BRAZILIAN NATIONAL DATA PROTECTION AUTHORITY. Resolution CD/ANPD No. 15/2024 — Security Incident Communication Regulation.
- BRAZILIAN NATIONAL DATA PROTECTION AUTHORITY. Resolution CD/ANPD No. 18/2024 — Data Protection Officer Regulation.
- BRAZILIAN NATIONAL DATA PROTECTION AUTHORITY. Guidance on controllers, processors and data protection officers.
- BRAZILIAN NATIONAL DATA PROTECTION AUTHORITY. Information Security Guide for Small Processing Agents.

VALIDATION NOTE. Before publication, this Notice must be legally reviewed and aligned with the actual form, technical logging and provider configuration used for the Channel.