

GLOBAL DATA PROTECTION POLICY

vital



1. INTRODUCTION

1.1. About Our Company and Our Privacy Governance

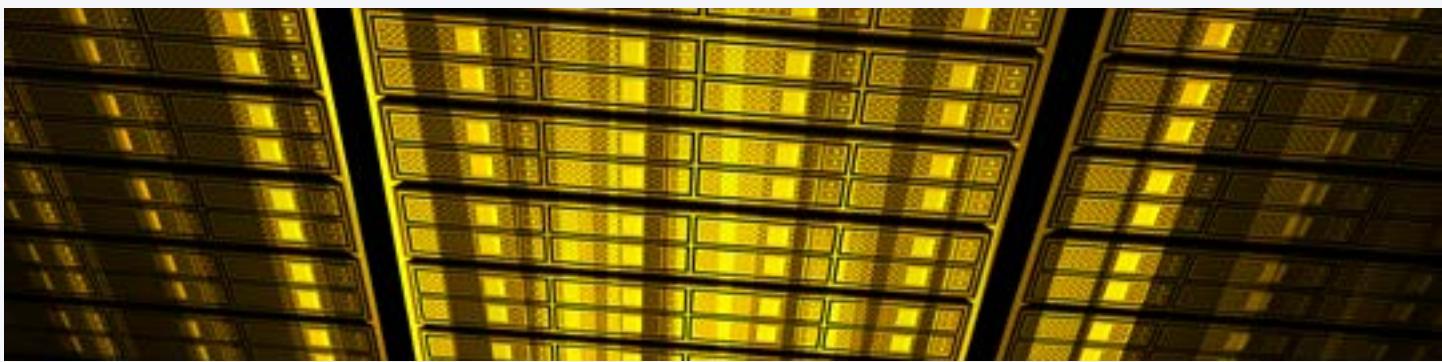
The V.tal Group constitutes a platform of infrastructure and digital solutions, operating different business units that serve both the wholesale and retail markets, ensuring service capillarity and the neutral operation of infrastructure. This Global Data Protection Policy (“Policy”) establishes the overarching principles, governance structure, and institutional commitments that guide the V.tal Group (“V.tal”, or “Group”) in protecting Personal Data throughout the life cycle of our submarine cable operations and related telecommunications services. Some companies are part of the V.tal Group, such as GlobeNet, Tec.to Data Centers and Nio. The activities of each of them are described in item 1.2 of this Policy.

GlobeNet is a wholesale telecommunications provider legally incorporated in the State of Delaware, with cable landing stations in Florida and New Jersey. The company was acquired in 2022 by V.tal, a global end-to-end digital infrastructure solutions company that owns and operates the largest neutral fiber optic network in Brazil, extensive subsea cable systems across the Americas, and a portfolio of edge data centers. As part of the V.tal Group, GlobeNet operates as an essential component of its international connectivity ecosystem, delivering sustainable on-ramps to the Internet through our wholly owned, dual ring-protected, subsea fiber optic cable system.

The business operations extend across multiple U.S. states, including California, Florida, Georgia, New Jersey, New York, Pennsylvania, Texas, and Virginia, where we maintain tax registration and engage with customers, partners, and employees. We operate exclusively under a business-to-business (B2B) model, without direct interaction with end users or consumers.

V.tal, as GlobeNet’s controlling shareholder, provides strategic oversight and alignment of privacy, security, and compliance objectives across the Group. Data flows between GlobeNet and V.tal will be governed by the principles set out in this Policy, which is designed to ensure consistent standards of data protection, privacy, and information security across all jurisdictions in which we operate.

This Policy is built upon internationally recognized privacy principles, applicable regulatory frameworks, and the commitments of V.tal as a signatory to the UN Global Compact on human rights, labor, environment, and anti-corruption.



1.2. V.tal Group Business

The business models of the Group's main companies are defined as follows:

V.tal (Neutral Digital Infrastructure)

V.tal is a comprehensive neutral digital infrastructure platform and the owner of the largest neutral fiber optic network in Brazil. V.tal operates on a strict B2B (Business-to-Business) wholesale model, serving as a critical enabler for the digital ecosystem across the Americas.

Operations and Clients: V.tal provides an extensive portfolio of connectivity and infrastructure solutions. Its clients include telecommunications operators, internet service providers (ISPs), global content companies (Big Techs and OTTs), and enterprises from diverse sectors. V.tal offers end-to-end Fiber to the Home (FTTH) network services, high-capacity data transport, and infrastructure solutions for mobile networks (including 4G and 5G). Our commitment to network neutrality ensures that all client traffic is handled with equal priority and security, without discrimination.

Infrastructure: The company's vast infrastructure includes over 450,000 kilometers of terrestrial fiber optic cable, with a network passing more than 22 million homes available for FTTH services across thousands of Brazilian municipalities. This terrestrial network is seamlessly integrated with the group's international submarine cable system and data center ecosystem.

GlobeNet (International Wholesale Telecommunications Provider)

GlobeNet is a wholesale telecommunications provider. Although it was acquired and integrated by V.tal in 2022, it maintains its specific segment as an essential component of V.tal's international connectivity ecosystem.

Operations and Clients: GlobeNet operates exclusively under a B2B (Business-to-Business) model. Its clients consist of telecom operators, global carriers, and large enterprises requiring robust, high-capacity international connectivity.

Infrastructure and Geographic Scope: GlobeNet owns and operates a resilient, 26,000-kilometer submarine cable network. This critical infrastructure has landing points in Brazil, the United States, Colombia, Venezuela, Bermuda, Argentina, and Chile, forming the backbone of the V.tal Group's pan-American operations. The network is engineered for high availability and low latency, ensuring the secure and efficient transport of data.

Tec.to (Data Centers)

Tecto Data Centers (Tec.to) was created in October 2024 as an independent business unit of V.tal Group, reinforcing specialization and growth in data infrastructure.

Operations and Services: Tec.to's business model is focused on providing Edge and Hyperscale Data Center solutions. Its core services include Colocation, offering secure and resilient physical space, power, and cooling for client-owned IT infrastructure, and Interconnection, facilitating high-performance, low-latency connectivity within a neutral ecosystem.

Infrastructure: Tec.to operates and is developing a growing portfolio of data centers in strategic locations in Brazil (Fortaleza, Porto Alegre, Santana de Parnaíba/SP, Rio CLS, Fortaleza CLS) and Colombia (Barranquilla, BDC-1 and BDC-2), serving as international gateways and regional hubs. These facilities are fully integrated into V.tal's extensive terrestrial and submarine fiber optic network, creating a seamless ecosystem for data storage and transport.

Nio (Fiber Optic Internet Service Provider - Retail)

Nio is a new fiber optic internet brand that operates as a retail service provider. Born from a consumer-centric model, Nio is a new and distinct company focused on delivering a high-quality digital experience directly to residential customers and small and medium-sized businesses across Brazil.

Operations and Clients: Nio provides high-speed internet services and related digital solutions to its customers. While establishing and maintaining a direct relationship with its clients, including for Purposes of account registration, service delivery, billing, and customer support, Nio collects and processes Personal Data within a B2C relationship.

Relationship with V.tal Group Infrastructure: To deliver its services, Nio utilizes the neutral, open-access fiber optic network operated by V.tal. In this arrangement, Nio is a client of V.tal's wholesale infrastructure, ensuring a clear operational separation that maintains the neutrality of the core network.

1.3. Commitment to Data Protection and Privacy

The V.tal Group recognizes privacy as a fundamental right and a strategic business imperative. We are committed to Processing Personal Data in a lawful, fair, transparent, and secure manner, embedding privacy considerations into all corporate decisions, technologies, and processes.



1.4. Purpose of the Policy

The Policy is designed to:

- Support the trust of our customers, partners, employees and stakeholders while demonstrating to supervisory authorities, auditors, and the public that V.tal Group maintains a robust and unified data protection framework;
- Ensure that all Group entities act consistently with applicable data-protection legislation in every jurisdiction where we operate, while aligning our data handling practices with the best global practices and legal requirements;
- Ensure transparency and accountability in our Processing of Personal Data; and
- Articulate foundational rules that will be further detailed in supplemental standards, procedures, and bilateral or multilateral data-sharing agreements within the Group.



1.5. Scope and Applicability

This Policy applies to every company part of the Group, department, employee, contractor, and third party acting on our behalf when Processing Personal Data. It covers any process of Personal Data, such as collection, storage, use, disclosure, transfer, retention, and deletion.

1.6. Audience

The primary audiences are:

- Data-protection authorities and regulators (ANPD – Brazil, FTC – United States, CCPA – California, other U.S. State Attorneys General, PrivCom – Bermuda, Agencia de Protección de Datos Personales – Chile, URCDP – Uruguay, SIC – Colombia, and AAIP – Argentina, and any other applicable data-protection regulator);
- External and internal auditors; and
- Customers, partners, vendors, and employees seeking transparency into our privacy governance.

2. APPLICABLE DATA-PROTECTION LEGISLATION

2.1. Country-by-Country Data Protection Frameworks

Each country is governed by its own data protection legislation (the “Applicable Legislation”), which is outlined below.



United States / North America

- Delaware** – Delaware Personal Data Privacy Act;
- Georgia** – Law of Georgia on Personal Data Protection;
- New Jersey** – New Jersey Personal Data Privacy Act;
- Texas** – Texas Data Privacy and Security Act;
- California** – California Consumer Privacy Act and California Privacy Rights Act;
- Florida** – Florida Information Protection Act;
- Virginia** – Virginia Consumer Data Protection Act; and
- Bermuda** – Personal Information Protection Act 2016.

In the case of GlobeNet, it also operates in New York and Pennsylvania, two states that have yet to enact comprehensive data privacy legislation.



South America

- Brazil** – Law 13.709/2018 on Brazilian Data Protection Law;
- Chile** – Law 19.628 on Protection of Private Life;
- Uruguay** – Law 18.331 on Protection of Personal Data and Habeas Data Action, regulated by Decree 414/009;
- Colombia** – Law 1581/2012 and Decree 1377/2013, complemented by SIC guidelines;
- Argentina** – Law 25.326 on Protection of Personal Data and Decree 1558/2001; and
- Venezuela** – Constitutional protections (Art. 28), Telecommunications Law, and sector-specific regulations.

2.2. Cross-Border Data Transfers

The Group engages in cross-border transfers of Personal Data exclusively where a lawful ground is firmly established and robust safeguards are demonstrably in place, relying, where appropriate, on:

- I. Adequacy determinations issued by competent supervisory authorities, confirming that the destination jurisdiction affords a level of protection essentially equivalent to that of the originating country;
- II. The execution of Standard Contractual Clauses, or any local equivalents approved by the relevant regulator, to contractually bind all parties to data-protection obligations that mirror those imposed under applicable law; or, exceptionally,
- III. Specific derogations or exemptions expressly sanctioned by Applicable Legislation ensuring that every international transfer aligns with prevailing data-protection regimes.



3. DATA-PROTECTION GOVERNANCE

3.1. Data-Protection Principles

The V.tal Group adopts the following foundational principles, applicable to every Processing activity:

- Lawfulness, Fairness, and Transparency** – Personal Data is processed on a lawful basis, in a manner that is fair and transparent to Data Subjects;
- Purpose Limitation** – Data is collected for specific, explicit, and legitimate Purposes and not further processed in a manner incompatible with those Purposes;
- Data Minimization** – Only data that is adequate, relevant, and limited to what is necessary for the stated Purposes is processed;
- Accuracy** – Reasonable steps are taken to ensure data is accurate and, where necessary, kept up to date;
- Storage Limitation** – Data is retained no longer than necessary for the Purposes for which it is processed or to comply with legal obligations;
- Integrity and Confidentiality** – Appropriate technical and organizational measures protect data against unauthorized or unlawful Processing and against accidental loss, destruction, or damage; and
- Accountability** – The Group is also responsible for, and able to demonstrate, compliance with all the above principles.

3.2. Training and Awareness Initiatives

The Group is committed to fostering a culture of privacy and accountability throughout its global operations and, to that end, conducts periodic training sessions for all employees covering the principles, requirements, and best practices of Applicable Legislation and this Policy.

In addition, the V.tal Group deploys complementary awareness initiatives to ensure that every member of its workforce remains continuously informed, competent, and aligned with the Group's privacy obligations.

4. DATA-SUBJECT RIGHTS AND INSTITUTIONAL COMMITMENTS

Depending on the jurisdiction, Data Subjects may exercise rights of access, confirmation of Processing, rectification, deletion/erasure, restriction, portability, objection, withdrawal of consent, review of automated decisions and any other rights provided under Applicable Legislation. The V.tal Group respects these rights in accordance with Applicable Legislation and, where feasible, applies a harmonized approach to provide an equivalent level of protection across the Group. All companies within the V.tal Group operate on a B2B basis, except for Nio.

Data-subject requests can be submitted via e-mail to the Group DPO (see Section 6).

We will acknowledge receipt of requests and make our best efforts to address them within the timeframes established by the Applicable Legislation.

5. DATA SECURITY AND RISK MANAGEMENT

We implement appropriate technical and organizational measures to protect Personal Data against unauthorized access, loss, misuse, alteration, disclosure, or destruction. These measures are designed considering the nature of the data, the risks associated with the Processing, and industry standards for information security.

Our safeguards may include encryption, pseudonymization, firewalls, access controls, secure storage environments, monitoring systems, regular vulnerability assessments, and employee training on data-protection responsibilities.



While we strive to protect all Personal Data within our systems and networks, no method of transmission or storage is entirely secure. For this reason, we continuously review and enhance our security controls to minimize potential risks. All Personal Data Processing activities carried out by V.tal Group are duly registered and subjected to risk assessments that are proportional to the nature, volume, and criticality of the operations involved. If the results of these assessments indicate a high risk to the rights and freedoms of Data Subjects, we will evaluate and, if necessary, conduct a Data Protection Impact Assessment or Privacy Impact Assessment (“DPIA” or “PIA”) as required by the applicable laws of each jurisdiction. The findings of the DPIA or PIA will guide the definition and implementation of additional technical and organizational safeguards, ensuring that risks are properly mitigated and compliance with data protection requirements is maintained.

Any indication or confirmation of a security incident involving Personal Data must be reported immediately to the DPO. The DPO and their team will promptly assess the severity of the event, take measures to contain its impact, and, when applicable, notify the competent supervisory authority and affected Data Subjects within the legal deadlines.

In addition, vendors who have or may have access to Personal Data will only be engaged following risk-based due diligence procedures and will remain subject to ongoing monitoring. All relevant contracts will include mandatory data protection clauses, such as audit rights, incident notification obligations, and minimum-security requirements, ensuring alignment with the Group standards and applicable legislation.



6. DATA ACCURACY AND STORAGE LIMITATION

We take reasonable steps to ensure that the Personal Data we process is accurate, complete, and up to date, considering the Purposes for which it is collected and used. We encourage individuals to inform us of any changes to their Personal Data to help maintain accuracy.

Personal Data is retained only for as long as necessary to fulfill the Purposes for which it was collected, to comply with legal, regulatory, or contractual obligations, or to resolve disputes and enforce our rights. Once data is no longer required, we apply secure deletion, anonymization, or archiving procedures in accordance with our internal policies and applicable law.

7. CONTACT INFORMATION

For any questions or matters involving your Personal Data, please contact the DPO, Maria Cecília Oliveira Gomes, through the Data Protection channel: pp-privacidadevtal@vtal.com

8. DEFINITIONS

Personal Data: information related to an identified or identifiable natural person.

Data Protection Officer (“DPO”): person appointed by each of the data Processing agents to act as their respective communication channel between the Data Subjects, and the applicable data-protection regulator.

Purpose: carrying out the Processing for legitimate, specific, explicit and informed Purposes to the Data Subject, without the possibility of further Processing in a way that is incompatible with these Purposes.

Data Subject: natural person to whom the Personal Data that is subject to Processing refers.

International Data Transfer: transfer of Personal Data to a foreign country or international organization of which the country is a member.

Processing: any operation carried out with Personal Data, such as those referring to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, Processing, filing, storage, elimination, evaluation or control of information, modification, communication, transfer, dissemination or extraction.