PRIVACY

POLICY FOR SUPPLIERS

tec·to

1. PURPOSE

Tecto Data Centers (“Tecto”) is committed to processing Personal Data with respect to your privacy, complying with privacy and data protection laws, regulations and under the terms of the Brazilian General Data Protection Law - Law No. 13,709/2018 (“LGPD”). Likewise, Tecto requires its Suppliers (“Supplier” or “You”) to also comply with legal requirements in the Processing of any and all Personal Data involved in their contractual relationship. Accordingly, the entire relationship between Tecto and its Suppliers shall comply with the provisions of this Supplier Privacy Policy (“Policy”), which shall apply to all Tecto’s Suppliers.

It should be noted that Tecto is a company specialized in offering data centers in the colocation modality, allowing companies to allocate their own servers and Information Technology (“IT”) equipment in a secure, resilient and highly connected environment. Tecto does not access, process or interfere with the data stored or trafficked by customers, acting exclusively as a provider of physical space, energy, air conditioning, security and connectivity.

The Policy is in force for an indefinite period of time and may be reviewed and updated whenever necessary.

2. DEFINITIONS

Anonymization: data relating to the Data Subject that cannot be identified, considering the use of reasonable technical means available at the time of its Processing.

Brazilian National Data Protection Authority (“ANPD”): body responsible for ensuring, supervising, and implementing compliance with the provisions of the LGPD in the national territory.

Controller: natural or legal person, under public or private law, who is responsible for decisions regarding the Processing of Personal Data, in accordance with article 5, VI of the LGPD.

Personal Data: information related to an identified or identifiable natural person, in accordance with article 5, I, of the LGPD.

Data Protection Officer (“DPO”): person appointed by each of the Controller and the Processor to act as their respective communication channel between the Data Subjects, and the ANPD.

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 in accordance with article 6, I of the LGPD.

Processor: natural or legal person, under public or private law, who carries out the Processing of Personal Data on behalf of the Controller.

Data subject: natural person to whom the Personal Data that is subject to Processing refers, in accordance with article 5, V of the LGPD.

International Data Transfer: transfer of Personal Data to a foreign country or international organization of which the country is a member, in accordance with article 5, XV of the LGPD.

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, in accordance with article 5, XI of the LGPD.

3. ROLES IN DATA PROCESSING

In the context of the relationship between Tecto and its Suppliers, it is essential to recognize that the roles and responsibilities related to the Processing of Personal Data may vary according to the nature and purpose of the Processing carried out by each party. In accordance with the LGPD, the parties may act, depending on the specific case, as Controllers, Processors or, eventually, Joint Controllers.

Considering that Tecto does not access, process or interfere with the data stored or trafficked by customers, limiting itself to the provision of physical infrastructure services, the processing of personal data carried out by Tecto is restricted to the activities necessary for the management of the relationship with customers and suppliers, the control of physical access to the data center premises, the traceability of physical connections (cross-connects) and the fulfillment of legal and regulatory obligations.

Thus, in general, Tecto will act as Controller of the personal data of customers and representatives, agents and employees of suppliers, determining the purposes and means of processing this data for the purposes of contractual management, access control, traceability, security, among others, while the Supplier acts as Processor, processing the data according to the instructions of Tecto. In specific cases, the Supplier may be the Controller and Tecto, the Processor, depending on who defines how and for what the data will be used. In these cases, the **Controller-Processor** relationship will be configured.

There may also be situations where Tecto and Supplier act as **Joint Controllers**, each making decisions independently about the data under its responsibility. In these cases, both have their own obligations under the LGPD, and must ensure transparency, security, and respect for the rights of the Data Subjects.

In view of this, it is essential that, for each operation involving the Processing of Personal Data, the parties clearly evaluate and define their respective roles, in order to ensure adequate compliance with legal and contractual obligations, as well as the protection of the rights of the Data Subjects.

The definition of the roles must be expressly contained in a contract or

equivalent instrument, detailing the responsibilities of each party, including the adoption of security measures, incident response and compliance with the rights of the Data Subjects. In any case, the Supplier undertakes to properly fulfill the roles that are applicable to it in accordance with the respective contract.

4. SUPPLIER EVALUATION PROCESS

Tecto may process the data of its Suppliers for evaluation and due diligence. The Supplier due diligence process is an essential step in the evaluation and selection process, aiming to ensure that Tecto hires partners who comply with legal, regulatory, and ethical requirements, in addition to mitigating risks for the company. During due diligence, Tecto may process Personal Data of the legal representatives, partners, managers and other stakeholders related to the Supplier.

The due diligence process typically involves:

1. Information Collection

Request for documents and registration information from the Supplier's representatives, such as identity, CPF, proof of address, clearance certificates, information about the corporate structure and other relevant data.

2. Compliance Analysis

Verification of compliance with legal and regulatory requirements, such as fiscal, labor and environmental regularity, in addition to background checks and history checks of representatives.

3. Risk Assessment

Identification of potential risks related to integrity, reputation, involvement in legal proceedings, administrative or criminal sanctions, and exposure to situations of conflict of interest or corruption.

4. Verification of Specific Requirements

Depending on the nature of the contract, additional requirements may be required, such as technical certifications, presentation of internal documents and training, regulatory authorizations, or proof of experience.

5. Registration and Documentation

All information collected, and analyses carried out are recorded and documented, composing the Supplier's dossier, which will serve as a basis for the contracting decision and for any future audits.

Throughout the process, Tecto adopts measures to ensure the confidentiality, integrity and security of the Personal Data processed, limiting access only to authorized persons and using the data exclusively for the Purposes described.

5. SUPPLIER RESPONSIBILITIES

Once the due diligence process is concluded, Tecto must decide whether or not to hire the Supplier. Deciding to follow up on the contract, regardless of the role played by the Supplier in the contractual relationship with Tecto – whether as a Controller or Processor of Personal Data, the Supplier must strictly observe the following responsibilities and obligations:

Full Compliance with Applicable Legislation: The Supplier must comply with all laws and regulations applicable to privacy and data protection, especially the LGPD, as well as complementary rules, such as the Resolutions published by the ANPD and other guidelines issued by competent authorities.

Adoption of Technical and Organizational Measures: It is essential that the Supplier implements appropriate technical and organizational measures to ensure the security, confidentiality, integrity and availability of the Personal Data processed, preventing any form of unauthorized access, destruction, loss, alteration, disclosure or inappropriate Processing, whether accidentally or unlawfully. The topic of cybersecurity will be addressed in greater depth in item 9 of this Policy.

Incident Prevention and Response: The Supplier must adopt mechanisms for monitoring and responding to security incidents, immediately reporting to Tecto any event that may compromise the integrity, confidentiality or availability of personal data, including, but not limited to, unauthorized access, leaks, accidental or unlawful loss or destruction, whether in the physical or digital environment. It must also collaborate with Tecto in the investigation of the facts and in the implementation of corrective and mitigating measures. The topic of Incident Response will be addressed in greater depth in item 7 of this Policy.

Transfer of Personal Data: The Supplier declares that in any form of communication, integration and/or transfer of data, there will be the application of Triple A (Authentication, Authorization and Accounting), in addition to the use of encryption techniques, anonymization/masking of data and/or any other security measures that may be necessary to ensure the security and protection of Personal Data during the possible transfer, without prejudice to the prior consent of Tecto.

International Transfer of Personal Data: Any International Transfer of Personal Data, including to cloud storage, may only occur with prior and express authorization from Tecto, and must fully comply with the requirements of the LGPD, Resolution CD/ANPD No. 19/2024 and other applicable rules. The Supplier must ensure that, in such transfers, the Personal Data receives the same level of protection required by Brazilian law, including respect for the rights of the subjects.

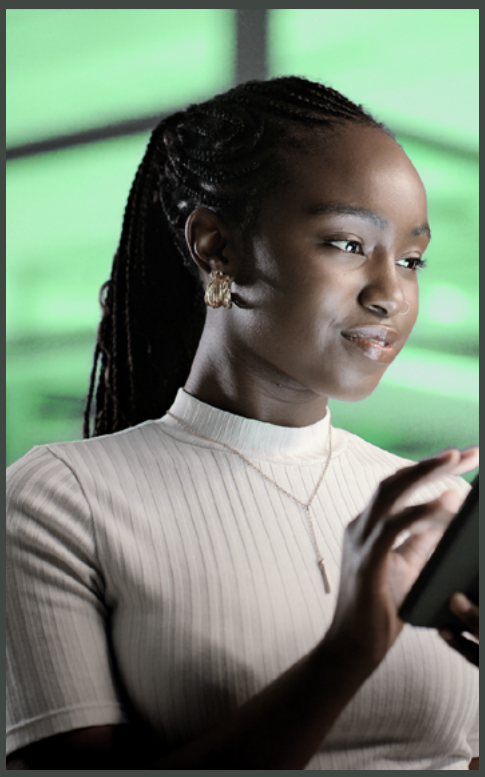
Respect for the Rights of Data Subjects: The Supplier must ensure that the rights of the Data Subjects are respected at all stages of the Processing, providing immediate and adequate support to Tecto to meet requests, such as access, correction, deletion, portability, opposition and other rights provided by law. The Supplier shall not respond directly to requests from data subjects but shall immediately forward them to Tecto and await specific guidance.

Return or Deletion of Personal Data: At the end of the contractual relationship, or whenever requested by Tecto, the Supplier must return or delete all Personal Data processed on behalf of Tecto, making sure that there is no undue retention of information, except when there is a legal or regulatory obligation to retain it.

Training and Awareness: All employees, collaborators, agents and subcontractors of the Supplier who have access to Personal Data must receive continuous and adequate training in data protection, information security, best compliance practices and legal obligations arising from the LGPD and other applicable regulations. The Supplier must keep records of these trainings and ensure that everyone is aware of their responsibilities.

Supervision and Audit: The Supplier must allow and collaborate with any audits, inspections or evaluations carried out by Tecto or by third parties indicated by it, to verify compliance with contractual and legal obligations related to the protection of Personal Data.

Joint and several liability and Compensation for Damages: The Supplier acknowledges that, pursuant to article 42 of the LGPD, the Controller or Processor who, due to the Processing of Personal Data, causes property, moral, individual or collective damage to third parties, including through its employees, collaborators, agents and subcontractors, is obliged to repair it. The Supplier will be jointly and severally liable for the damages caused when it fails to comply with the obligations of the data protection legislation or does not follow the lawful instructions of Tecto, being equivalent to the controller, except in the cases provided for in article 43 of the LGPD. Likewise, the controllers directly involved in the Processing that results in damage to the data subject will be jointly and severally liable, as provided for in the legislation.



6. WITH WHOM THE SUPPLIER CAN SHARE TECTO'S DATA TO?

Information owned by Tecto may only be shared with companies in the Supplier's economic group and with national or international business partners when there is a real need for sharing, such as for the execution of the signed contract and in accordance with the applicable legal basis. Such partners must be included in the contract signed with the Supplier or have the subcontracting authorized by Tecto.

In the event that Personal Data is shared with Supplier's partners outside Brazil, the processing, analysis, Processing, use and sharing of such data will be carried out in accordance with applicable laws and the terms and conditions stipulated in the signed contract, and it is the responsibility of the Supplier to hire its partners.

7. INCIDENT RESPONSE AND COOPERATION BETWEEN THE PARTIES

In order to ensure the proper management and response to security incidents involving Personal Data or not, guidelines and responsibilities are established, observing the definitions and obligations provided for in the applicable legislation, especially the LGPD and ANPD Resolutions.

Supplier undertakes to notify Tecto, promptly and in detail, of any security incident involving Tecto's data, systems, assets, or information, including, but not limited to, unauthorized access, leaks, loss, destruction, alteration, disclosure, or any other form of compromise of information security. The notification shall contain, as a minimum, a description of the incident, the nature of the data affected, the containment measures taken, the preliminary risk assessment and the remediation plans.

Supplier shall fully cooperate with Tecto in the investigation, mitigation, and resolution of the incident by providing all necessary information, records, logs, evidence, and technical support.

The Supplier, as Processor, may not, under any circumstances, communicate directly with Personal Data Subjects, public authorities, regulatory bodies (including the ANPD) or any third parties about the incident, except with prior, express and written authorization from Tecto. It is the sole responsibility of Tecto, as Controller, to assess the need and make communications to Data Subjects, the ANPD and other competent bodies, as required by law, and the Supplier must strictly follow the guidelines and determinations of Tecto regarding the conduct of the incident and response measures.

If the Parties act as joint Controllers, they must define, in the signed contract or in their own instrument, the specific responsibilities of each one regarding the communication, response and mitigation of incidents, as well as communication with Data Subjects and authorities. In any event, the Parties shall cooperate with each other, in a transparent and timely manner, to ensure compliance with legal obligations and the protection of the rights of the Data Subjects.

All actions, communications and measures related to the incident taken by the Supplier must be duly recorded and documented, being available to Tecto for audit and proof of compliance with contractual and legal obligations.

The Supplier shall be liable for all damages, losses, costs, expenses, fines and convictions arising from security incidents caused by its action or omission, including the faults of its employees, subcontractors or third parties under its responsibility, and shall indemnify Tecto in full.

8. INTELLECTUAL PROPERTY

At Tecto, we value and protect all our intellectual property assets, such as trademarks, patents, copyrights, trade secrets, know-how, software, databases, methodologies, processes, technical specifications, documentation and confidential information. These assets are critical to our business and belong solely to Tecto or our licensors.

If you, the Supplier, need to access or use any of these assets to provide the contracted services, it is important to remember that this use must always be restricted to what is necessary for the execution of the contract and strictly follow the guidelines and authorizations of Tecto. It is not allowed to use these assets for other purposes, own or third-party, nor for any benefit that is not directly related to the contract.

We expect you to take all possible measures to protect our assets and systems, preventing any misuse, unauthorized access, disclosure, copying, modification, destruction, misappropriation, reverse engineering, or any other action that may compromise the security or intellectual property rights of Tecto.

Anything developed, improved, customized, adapted or created by the Supplier during the performance of the contract – whether alone or in conjunction with Tecto – shall be the exclusive property of Tecto. If necessary, the Supplier shall take all steps to ensure that these rights are properly transferred or registered in the name of Tecto at no additional charge.

It is not allowed to register, license, transfer, market, disclose or exploit any asset, right, trademark, patent, software, domain, industrial design, methodology, process, information or other intellectual property of Tecto, in Brazil or abroad, without prior written authorization from Tecto.

In the event of any violation of Tecto's intellectual property rights, including by employees, subcontractors or third parties connected to the Supplier, the Supplier shall be responsible for all resulting damage, costs and expenses and shall reimburse Tecto in full.

At the end of the contract, or whenever requested, the Supplier must return all materials, documents, equipment, credentials, copies, backups and any other assets of Tecto, in addition to eliminating from its systems all related information and data, ensuring that nothing is improperly retained, unless there is a legal obligation to the contrary.

Finally, Tecto relies on the Supplier's collaboration to protect and defend its intellectual property rights, providing information, documents and support whenever necessary.

The objective of Tecto is to ensure a transparent, secure relationship in line with the best practices for the protection of intellectual property. If you have any questions, we are available to guide and support.

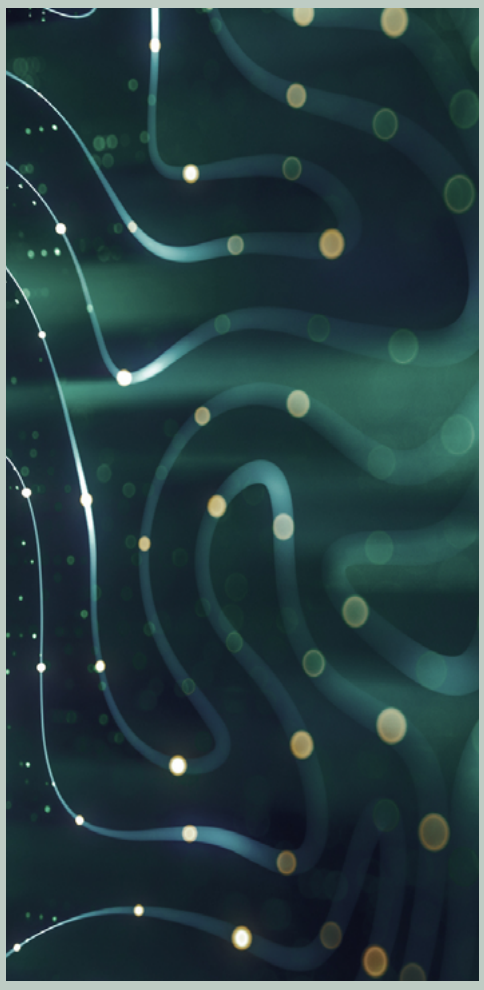
9. CYBERSECURITY

In addition to the provisions of the LGPD, Tecto requires its Suppliers to adopt robust cybersecurity measures, in line with regulatory standards and best practices in the technology and critical infrastructure sector.

The Supplier shall adopt robust technical and organizational measures to ensure the physical and logical security of the Personal Data, infrastructure, and equipment used in the provision of services to Tecto. When applicable, Tecto may request the availability of an Information Security Policy, evidence of its implementation and audit reports; continuous monitoring of assets; maintenance of audit records; immediate notification of incidents; carrying out vulnerability tests; performing backups; using antivirus, firewalls, and access lists; adopting confidentiality contractual clauses; using strong authentication with MFA; secure access via VPN; timely revocation of former employee access; documentation of infrastructure and software processes; training in personal data protection and cybersecurity; and identification and protection of confidential information.

Finally, to ensure compliance with regulatory standards and information security best practices, Supplier shall conduct periodically independent audits of its cybersecurity policy and practices. The Supplier also undertakes to make the reports and results of these audits available to Tecto whenever requested.

10. SUPPLIER DATA PROCESSED BY TECTO



Supplier, you also have employees, whose Personal Data may be processed by Tecto during the business relationship. In this way, Tecto processes the Personal Data of its Suppliers and their representatives in order to ensure the proper management of the business relationship, compliance with legal and regulatory obligations, and the protection of its legitimate interests. The processing of this data is essential both for contracting and for maintaining and monitoring the services provided by the Suppliers.

The Personal Data of Suppliers that Tecto processes may include, but is not limited to, registration data, such as name, CPF, RG, date of birth, gender, profession, age, marital status, nationality, place of birth, affiliation, telephone/cell phone, e-mail, class registration, address, among other Personal Data that may be sent during the process of contracting and maintaining the relationship with the Supplier.

This data may be provided directly by the Supplier or its representative, obtained from third parties (such as consultants, companies in the same economic group, marketing agencies), or collected automatically through cookies and similar technologies, in case there is interaction with Tecto's digital systems or platforms.

The Personal Data of the Suppliers and their representatives will be processed for the following purposes:

- **Commercial Relationship Management:** Administration and implementation of the contract, analysis and approval of registration, execution and termination of contracts and amendments, records in systems, making payments, monitoring the execution of services or supply of products, carrying out due diligences, among others.
- **Communication with the Supplier:** Carrying out communications, sending requests, receiving information and clarifying doubts related to the supply of products or services.
- **Legal and Regulatory Obligations:** Compliance with legal or regulatory obligations, compliance with internal policies and standards, meeting requests from regulatory bodies, governmental or judicial authorities.
- **Exercise of Rights:** Collection and payment of amounts due, defense in judicial or administrative proceedings, and exercise of other rights provided for by law.
- **Control and monitoring of physical access to data center premises.**

11. HOW TECTO PROTECTS YOUR DATA

Tecto adopts appropriate technical and organizational measures to protect the Personal Data of its Suppliers against unauthorized or unlawful Processing, as well as against accidental loss, destruction or damage. Suppliers' Personal Data is stored securely in protected environments, which will be accessed by a restricted number of people with legitimate reasons for this access.

Despite Tecto's best efforts to protect and preserve Suppliers' Personal Data, it is critical to understand that no transmission of information is absolutely secure. Therefore, Tecto cannot guarantee that all information received and sent is free from unauthorized access, which may occur through illicit methods, such as viruses or database invasions. In the event of a breach of the Personal Data under our responsibility, we undertake to apply all necessary efforts to correct and mitigate the consequences of such an incident.

However, Tecto's liability will be limited to direct damages proven to be caused by failures in its security measures, and it will not be liable for indirect damages, loss of profits or any other losses arising from events beyond its reasonable control, such as cyber-attacks, third-party system failures or unforeseeable circumstances and force majeure.

12. WHO DO WE SHARE VENDOR PERSONAL DATA WITH?

There is a possibility for Tecto to share the Personal Data of Suppliers with third parties, competent authorities or business partners that are relevant to the performance of the contract signed. Such sharing will take place based on the criteria and for the purposes described below.

Service Providers or Business Partners: We may share Suppliers' Personal Data with service providers engaged by Tecto or business partners for the following purposes: (a) providing software and systems used by Tecto in the performance of its functions and/or other information technologies; (b) defense in administrative or judicial proceedings involving Tecto and/or the Supplier; (c) hiring consultancies, advisors, specialists and service providers to support Tecto's activities related to the signed contract (such as law firms, credit and collection companies, third-party valuation, security and fraud prevention companies); and (d) administration of contracts and obligations with other third parties involved in the supply chain.

Competent Authority Request: Tecto may also share Vendor Personal Data with third parties (including government agencies) to respond to investigations, lawsuits, legal processes, or to investigate, prevent, or take action regarding illegal activities, suspected fraud, or situations that pose potential threats to the physical safety of any individual, or as otherwise required by law.

13. CHANGES TO THIS PRIVACY POLICY

Tecto reserves the right to modify this Privacy Policy for Suppliers at any time by posting the updated version. If there are material changes to this Privacy Policy for Vendors, Vendor will be notified thereof.

14. DATA PROTECTION OFFICER

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