POLICY

PRIVACY FOR SUPPLIERS

V·tal

1. PURPOSE

V.tal Rede Neutra de Telecomunicações S/A ("V.tal" or "We") is committed to processing Personal Data in accordance with privacy and data protection laws and regulations, in particular the Brazilian General Data Protection Law – Law No. 13,709/2018 ("LGPD"). Similarly, V.tal 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 with us.

Thus, the entire relationship between V.tal and its Suppliers must comply with the dictates of this Privacy Policy for Suppliers ("Policy"), which is applicable to all V.tal Suppliers.

This Policy is in force for an indefinite period and may be reviewed and updated whenever necessary. The latest version will be available on the privacy page of the V.tal website.

2. TARGET AUDIENCE

This Policy covers all Suppliers who maintain any type of commercial relationship with V.tal in the national territory, regardless of the legal nature of the contract or the contractual formalization of the relationship.

3. GUIDELINES

3.1. ROLES IN DATA PROCESSING

In the context of the relationship between V.tal 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 of the contracting and the 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 Joint Controllers.

In general, V.tal will act as Controller of the Personal Data of its employees, customers and representatives, as well as agents and employees of the Suppliers when it has access to their Personal Data, determining the purposes and means of the Processing of this data for the purposes of contractual management, access control, traceability, security, among other purposes. The Supplier may act, as the case may be, as the Processor, processing the data in accordance with V.tal's instructions. In specific cases, the Supplier may be the Controller and V.tal, the Processor, depending on who defines how and for what the Personal Data will be used. In these cases, the **Controller-Processor** relationship will be configured.

There may also be situations where V.tal and the Supplier act as **Independent Controllers**, when each is responsible for making decisions independently about the Processing of Personal Data under their responsibility. In these cases, both have their own obligations under the LGPD and are responsible for ensuring transparency, security, and respect for the rights of Data Subjects.

If V.tal and the Supplier jointly establish the purposes and means of Processing Personal Data, obtaining mutual benefit from this joint action, both will be considered **Joint Controllers**.

In view of this, it is essential that, for each operation involving the Processing of Personal Data, V.tal and the Supplier clearly evaluate and define their respective roles, in order to ensure the proper allocation of legal and contractual obligations, as well as the protection of the rights of 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, You undertake to properly fulfill the obligations that are applicable to you in accordance with the role played.

3.2. SUPPLIER EVALUATION PROCESS

The due diligence process is an essential step in the evaluation and selection of Suppliers, which aims to ensure that V.tal only hires partners who comply with legal, regulatory and ethical requirements, mitigating legal, operational and reputational risks for the Company. During the due diligence, V.tal may process Personal Data of legal representatives, partners, administrators, employees and other Data Subjects related to the Supplier.

The due diligence process typically involves the following steps:

1. Information Collection

Request for documents and registration information of the Supplier and its legal 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 by the Supplier, such as fiscal, labor and environmental regularity, in addition to background checks and history checks of representatives.

3. Risk Assessment

Identification of potential risks of the Supplier 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 the basis for the contracting decision and for any future audits.

Throughout the process, V.tal 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.

3.3. CARE WITH THE PROCESSING OF PERSONAL DATA BY THE SUPPLIER

In order to carry out its activities within the scope of the relationship with V.tal, the Supplier may have access to and carry out the Processing of Personal Data controlled by V.tal, and must comply with all applicable legislation, especially the LGPD.

The instructions provided by V.tal must be strictly followed to ensure the protection of the Personal Data made available, collected or shared by V.tal, preventing any type of violation, whether deliberate or accidental. The Supplier undertakes to ensure that activities are carried out in compliance with privacy and data protection regulations, adopting preventive measures against undue destruction, unauthorized sharing, loss, alteration, access or any inappropriate Processing of Personal Data.

In addition, whenever requested, the Supplier must allow and collaborate, in a full and timely manner, with audits, inspections or evaluations carried out by V.tal or by third parties indicated by it, as well as with the provision of requested documents, with a view to verifying compliance with contractual and legal obligations related to the protection of Personal Data.

Any impossibility of complying with the LGPD or significant changes in the Processing standards must be immediately notified to V.tal, so that corrective measures can be adopted.

3.3.1. International Transfer of Personal Data

The International Transfer of Personal Data, including cloud storage physically located abroad, is only allowed when strictly necessary for the execution of the object of the contract with V.tal and must adopt appropriate mechanisms to legitimize such transfers, pursuant to article 33 of the LGPD, Resolution CD/ANPD No. 19/2024 and other applicable legislation. The Supplier must ensure that the principles of the LGPD and the rights of the Data Subjects are fully respected in any transfer abroad.

3.3.2. Respect for the Rights of Data Subjects

Whenever necessary, the Supplier shall cooperate and provide adequate support to V.tal to meet the demands and requests of the Data Subjects, complying with all instructions of V.tal and not directly responding to requests regarding Personal Data controlled by V.tal.

3.3.3. Responsibilities

The Supplier is aware and 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 is obliged to repair it. Thus, the Supplier will be jointly and severally liable for the damages generated when it fails to comply with the obligations of the legislation for the protection of data or, acting as a Processor, fails to comply with V.tal's lawful instructions, equating it to the Controller, except in the cases of exclusion of liability 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 liable.

3.3.4. Return and/or Deletion of Personal Data

At the end of the contractual relationship between the Supplier and V.tal, or once the purpose of the processing of Personal Data has been achieved, the Personal Data processed on behalf of V.tal must be returned and/or destroyed in a secure and definitive manner, ensuring that there is no undue retention of information. The Supplier is prohibited from integrating and/or enriching V.tal's Personal Data into its databases, except with the express authorization of V.tal.

3.3.5. Governance

The Supplier must adopt and maintain governance measures in the protection of Personal Data, including the preparation and implementation of internal policies, procedures and regulations that ensure compliance with the LGPD.

In addition, it is essential that all Employees and Collaborators of the Supplier involved in the Processing receive adequate training on the protection of Personal Data and on the obligations provided for by the LGPD. This training should cover cibersecurity best practices, compliance procedures, and the legal responsibilities associated with the Processing of Personal Data.

3.4. WITH WHOM CAN THE SUPPLIER SHARE V.TAL'S DATA?

Information owned by V.tal 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, for example, if it is necessary to the execution of the contract signed with V.tal. In such cases, such partners must be included in the contract between the Supplier and V.tal or have the subcontracting authorized by V.tal.

3.5. INCIDENT RESPONSE AND COOPERATION BETWEEN THE PARTIES

In order to ensure the proper management and response to security incidents involving Personal Data, guidelines and responsibilities are established, observing the definitions and obligations provided for in the applicable legislation, especially the LGPD and ANPD Resolutions.

The Supplier undertakes to notify V.tal, promptly and in detail, of any security incident involving V.tal's data, systems, assets or information, including, but not limited to, unauthorized access, data

leaks, loss, destruction, alteration, disclosure or any other form of compromise of cibersegurity. 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.

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

The Supplier, as an 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 the prior, express and written authorization of V.tal. It is exclusively up to V.tal, as Controller, to assess the need and make communications to Data Subjects, to the ANPD and other competent bodies, as required by law, and the Supplier must strictly follow the guidelines and determinations of V.tal 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 incident response, 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.

All actions, communications and measures related to the incident taken by the Supplier must be duly recorded and documented, being available to V.tal 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 V.tal in full.

3.6. INTELLECTUAL PROPERTY

At V.tal, we value and protect all of 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 fundamental to our business and belong exclusively to V.tal or our licensors.

If you, as a Supplier, need to access or use any of these assets in order to provide the contracted services, it is important to remember that such use must always be limited to what is necessary for the performance of the contract and must strictly follow V.tal's guidelines and authorizations. It is not permitted to use these assets for any other purposes, whether for your own benefit or that of third parties, nor for any benefit 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 V.tal's security or intellectual property rights.

Everything that is developed, improved, customized, adapted or created by the Supplier during the performance of the contract - whether alone or together with V.tal - will be the exclusive property of V.tal. If necessary, the Supplier undertakes to take all steps to ensure that these rights are duly transferred or registered in the name of V.tal, at no additional cost.

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 V.tal, in Brazil or abroad, without prior written authorization from V.tal.

In the event of any violation of V.tal's intellectual property rights, including by employees, subcontractors or third parties connected to the Supplier, the Supplier will be responsible for all losses, costs and expenses arising therefrom, and must fully reimburse V.tal.

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 V.tal, 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, V.tal relies on the collaboration of the Supplier to protect and defend its intellectual property rights , providing information, documents and support whenever necessary.

V.tal's objective 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.

3.7. GOVERNANCE OF ARTIFICIAL INTELLIGENCE SYSTEMS

In the event of the use, development, or delivery of artificial intelligence ("AI") systems within the scope of the relationship with V.tal, the Supplier must observe the principles of ethical and responsible use of such systems, including but not limited to: safety, reliability, robustness, non-discrimination, transparency, explainability, and accountability. The Supplier must also ensure that the processing of personal data through AI systems is in compliance with all applicable laws and regulations.

The Supplier will be responsible for conducting due diligence in relation to the third parties involved in the supply, development or operation of AI systems used within the scope of the relationship with V.tal, in order to ensure that the systems employed are adequate and meet the minimum requirements of security, accuracy, protection of personal data and other necessary technical and legal guarantees.

The Supplier shall implement governance measures and mechanisms for assessing impacts and mitigating ethical, legal and social risks related to AI systems, including conducting continuous testing and validation throughout the system's life cycle with the aim of preventing failures, unlawful or abusive discriminatory results, misuse, and malicious access or manipulation.

Finally, the Supplier undertakes to notify V.tal in advance of the adoption of a tool, model or resource based on an AI system within the scope of the relationship with V.tal.

3.8. HOW THE SUPPLIER SHOULD PROTECT V.TAL DATA

In addition to the provisions of the LGPD, V.tal requires its Suppliers to adopt robust information security 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, infrastructures and equipment used in the provision of services to V.tal. Such measures must include, as applicable, the provision of an Cibersecurity Policy; continuous monitoring of assets; maintenance of audit records; carrying out vulnerability tests; performing backups; using antivirus, firewalls, and lists access; adoption of confidentiality clauses; use of 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 cibersecurity; and identification and protection of confidential information.

Finally, to ensure compliance with regulatory standards and information security best practices, the Supplier shall conduct periodic audits on its cibersecurity policy and practices. The Supplier also undertakes to make the reports and results of these audits available to V.tal whenever requested.

3.9. PROCESSING OF THE SUPPLIER'S PERSONAL DATA BY V.TAL

Supplier, You also have employees and representatives whose Personal Data may be processed by V.tal during the business relationship. V.tal needs to process this Personal Data for the fulfillment and management of contracts, payment processing, service monitoring, legal or regulatory obligation, and to exercise its rights on a regular basis.

The Personal Data of Suppliers that V.tal 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 submitted during the hiring process.

The Personal Data mentioned above may be provided directly by the Data Subject during the process of

registration, negotiation, and execution of contracts, in the sending of proposals, in communications by e-mail or telephone, or in other interactions necessary for the relationship commercial. In addition, we may obtain the data from third parties, such as consultants, companies within the same economic group, and marketing agencies. There is also the collection of automatic information, made through cookies and related technologies, if You use our systems or digital platforms.

The data mentioned above will be processed by V.tal for the following purposes:

- **Business Relationship Management:** We may process the data for the administration and implementation of the contract signed with the Supplier, covering all actions necessary to carry out V.tal's activities, including, but not limited to, the analysis and approval of registration, execution and termination of contracts and amendments, registrations in systems, execution of payments, monitoring the execution of services or supply of products, among others;
- **Supplier Evaluation and Selection:** The data can be used for compliance analysis, risk assessment, verification of legal and regulatory requirements, and other procedures necessary for the selection and maintenance of Suppliers;
- **Communication with the Supplier:** The data may be processed to carry out communications, send requests, receive information and clarify doubts related to the supply of products or services;
- **Legal and Regulatory Obligations:** We may also process data to comply with legal or regulatory obligations, as well as V.tal's internal policies and rules, including responding to requests from regulatory bodies, government or judicial authorities; and
- **Exercise of Rights:** The data may be processed for the collection and payment of amounts due, as well as to exercise other rights provided for by law, such as, for example, defense in judicial or administrative proceedings.

3.9.1. WITH WHOM DOES V.TAL SHARE PERSONAL DATA?

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

Service providers or business partners:

We may share your Personal Data with service providers hired by V.tal or business partners for the following purposes: (a) provision of software and systems used by V.tal in the exercise of its functions and/or other information technologies; (b) defense in administrative or judicial proceedings involving V.tal and/or the Supplier; (c) Hiring consultancies, advisors, specialists and service providers to support V.tal's activities related to the contract entered into with You (such as law firms, credit and collection companies, and third-party assessment, security and fraud prevention companies); and (d) administration of contracts and obligations with other third parties involved in the supply chain.

Request from competent authority:

V.tal may also share your Personal Data with third parties (including government agencies) to respond to investigations, lawsuits, legal process 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 required by law.

Additionally, V.tal may transfer Personal Data to service providers located abroad, including communication systems, email, cloud storage, among other services.

V.tal will ensure that the transfers of Personal Data to foreign countries are in compliance with the requirements established by the LGPD and the regulations of the ANPD on the subject. Furthermore, V.tal is committed to adopting best practices in cybersecurity to protect your Personal Data during international transfers.

3.9.2. HOW LONG WILL WE RETAIN PERSONAL DATA?

We store and maintain Personal Data: (i) for the period required by law; (ii) until the Processing of Personal Data is concluded, as mentioned below, or (iii) when one of the hypotheses provided for in article 16 of the LGPD is applicable. In this way, we will process Personal Data, for example, during limitation periods applicable or as long as necessary for compliance with legal or regulatory obligations.

The Processing of Personal Data will be terminated in the following cases:

- When the purpose for which the Personal Data was collected is achieved and/or the Personal Data collected is no longer necessary or relevant to achieve that purpose;
- Where the Supplier exercises its right to request the cessation of Processing and the deletion of its Personal Data and makes such a request; and
- When there is a legal order to that effect.

In these situations where the Processing of Personal Data is terminated, except in the cases of retention and/or storage provided for by applicable legislation or by this Supplier Privacy Policy, Personal Data will be deleted.

3.9.3. HOW DOES V.TAL PROTECT PERSONAL DATA?

V.tal adopts appropriate technical and organizational measures to protect your Personal Data against unauthorized or unlawful Processing, as well as against accidental loss, destruction or damage. Your Personal Data is stored securely on protected devices, which will be accessed by a restricted number of people with legitimate reasons for this access.

Despite our best efforts to protect your privacy and preserve your Personal Data, it is essential that you are aware that no transmission of information is absolutely secure. Therefore, we cannot guarantee that all information we receive and/or send is free from unauthorized access, which may occur through unauthorized and illicit methods, such as viruses or database breaches. In the event

of a breach of Personal Data under our responsibility, we are committed to making every necessary effort to correct and mitigate the consequences of such an incident.

However, V.tal's liability will be limited to direct damages that are proven to have been caused by failures in its security measures, and it will not be liable for indirect damages, loss of profits, or any other losses resulting from events beyond its reasonable control, such as cyberattacks, failures of third-party systems, or acts of God and force majeure.

3.10. CHANGES TO THIS PRIVACY POLICY

V.tal reserves the right to modify this Privacy Policy for Suppliers at any time, through the disclosure of the updated version.

If there are material changes to this Privacy Policy for Vendors, Vendor will be notified thereof.

3.11. DATA PROTECTION OFFICER

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

4. GLOSSÁRIO

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.

THIS DOCUMENT REVOKES PREVIOUS VERSIONS