INDEX

1. OBJECTIVE

The purpose of this privacy and personal data protection policy is to guide TIVIT suppliers' and / or business partners on the privacy and data protection guidelines to be respected, in accordance with the Brazil's privacy regulations, as well as to describe their participation and responsibility, either as Operator or Controller, in compliance with necessary technical and organizational / administrative measures and other controls established by TIVIT as Controller. The instructions and rules described herein must be followed to ensure, in a consistent and efficient manner, the protection of personal data made available or collected in the name of TIVIT, or shared due to the provision of services and business partnerships, ensuring correct custody and avoiding deliberate or accidental personal data breaches.

2. APPLICABILITY AND INVOLVED AREAS

TIVIT suppliers and / or business partners.

3. DEFINITIONS AND ASSUMPTIONS

i. "AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD": Government Agency responsible for monitoring compliance with the provisions of the "Lei Geral de Proteção de Dados (LGPD)", Brazilian federal law nbr13.709/2018;

ii. "DATA SHARING": communication, dissemination, international transfer, interconnection of personal data or the shared processing of personal databases by public entities in compliance with their legal powers, or between public and private entities, reciprocally, with specific authorization, for one or more modalities of processing allowed by these public entities, or between private entities;

iii. "CONSENT": free, informed and unequivocal manifestation by which the data subject agrees with the processing of his/her personal data for a specific purpose;

iv. "CONTROLLER": the responsible for decisions regarding the processing of personal data, especially regarding the purposes and ways of processing personal data;

v. "ANONYMIZED DATA": data relating to a data subject who cannot be identified, considering the use of reasonable and available technical means at the time of processing;

vi. "PERSONAL DATA": any information obtained as a result of a contract or commercial agreement signed with TIVIT, related to an identified or identifiable natural person, such as: name, ID Number, home or business address, landline or mobile phone number, e-mail address, geolocation information, among others;

vii. "SENSITIVE PERSONAL DATA": personal data on racial or ethnic origin, religious belief, political opinion, union or religious, philosophical or of political nature organization membership, data relating to health or sexual life, genetic or biometric data, when linked to a natural person;

viii. "DUE DILIGENCE": process of searching for information about a company to carry out analysis that include aspects like risks, compliance, assets, organizational structure / size and activities carried out, from the perspective of future business;

ix. "SUPPLIERS": natural or legal person, of public or private law, including service providers and freelancers, who carry out activities for / or on behalf of TIVIT, producing, distributing and marketing goods, systems and services;

x. "SECURITY INCIDENTS": any event that makes it possible to break the principles of information confidentiality, integrity and availability;

xi. "OPERATOR": party that treats personal data in accordance with the Controller's instructions;

xii. "BUSINESS PARTNERS": institutions that work cooperatively with TIVIT to achieve common commercial interests;

xiii. "SERVICE PROVIDER": natural or legal person, who offers / provides specific services through specialized physical and / or intellectual labor;

xiv. "DATA SUBJECT": natural person to whom the personal data being processed refers;

xv. "PROCESSING": any operation or set of operations carried out on personal data or on personal data sets (data processing), by automated or non-automated ways, such as the collection, registration, organization, structuring, conservation, adaptation or alteration, retrieval, consultation, use, dissemination by transmission, diffusion or any other form of availability, comparison or interconnection, limitation, elimination or destruction;

xvi. "PERSONAL DATA BREACH": any accidental, illegal or unauthorized access, acquisition, use, modification, disclosure, loss, destruction or damage involving personal data.

4. RESPONSIBILITY

All TIVIT Suppliers and / or business partners must follow the general guidelines for privacy and personal data protection, whether in the role of controller or operator, contributing to the adoption of preventive measures and in the identification and mitigation of threats and risks to data subjects.

5. POLICY DESCRIPTION

5.1. ABOUT DATA PROCESSING

The supplier and / or business partner (in the role of Operator) must assume the commitment to this policy, developed by TIVIT (in the role of Controller), based on the applicable legislation on privacy and data protection, which are: Federal Constitution, Consumer Protection Code, Civil Code, Marco Civil da Internet (Federal Law n. 12.965/2014), its regulatory decree (Decree 8.771/2016), Lei Geral de Proteção de Dados (Federal Law n. 13.709/2018), and other industry or general rules on the topic.

During the performance of its activities, the supplier and / or business partner, who process personal data by, or on behalf of TIVIT, must:

- Ensure that any person, whether natural or legal, is committed to complying with the guidelines of this policy;
- Guarantee the restrictions to the unique purposes set out in this policy and or set out in a contract or commercial agreement, without authorization for the use of personal or private purposes;
- Ensure that data processing is in line with data protection and privacy laws, as well as the policies established by TIVIT, including the information security policy;
- Process personal data only to perform its obligations defined in the scope of the contract, or others, defined by TIVIT through service contracts and related amendments. In case of the need to processing personal data that is not in the obligations, it will be necessary to request science or formal authorization from TIVIT;
- Ensure even greater rigor in the processing of sensitive personal data, using it to comply with contractual provisions, adopting appropriate technical and organizational protections, in order to maintain the confidentiality, integrity and availability of that information. Examples of technical protections are anonymization or data masking.

Access, sharing and transfer of personal data by third parties (including contractors, authorized agents and branches) from a supplier and / or business partner will only be possible with the prior consent of TIVIT. The responsibility for all actions and omissions by such third parties, related to data processing, will remain with the supplier and / or business partner.

It is the commitment of the supplier and / or business partner, to create a privacy and governance program for personal data, that must define appropriate technical and administrative controls to guarantee the security of the processed personal data, in addition to ensuring compliance with the “Lei Geral de Proteção de Dados” and other rules that may be prepared by the ANPD. This includes implementing internal policies and practices that they may establish:

- how data subjects are informed about the processing of personal data;
- what are the security measures applied (technical and procedural) that guarantee the confidentiality, integrity and availability of information;
- how crisis management is carried out in the event of incidents involving personal data;
- which procedure has been put in place to ensure that these measures are constantly updated;

- how the mapping and management of personal data is maintained;
- access control to personal data;
- which channels are made available for the fulfillment of data subjects' rights;
- definition of a Data Protection Officer (DPO);
- conducting periodic training with company employees.

The supplier and / or business partner must keep properly updated the records of operations (processing) of personal data, including the category of the data, the users involved in the activity, the purpose (s) and processing and storage deadline. It should also ensure that the information handled remains correct and duly updated, allowing it to be corrected or deleted.

In addition to the personal data privacy and governance program, the supplier and / or business partner must have an information security policy. This policy should define, but not be limited to:

- conducting constant training for company employees; and
- consider security controls, when applicable, including at least:

  (i) intrusion or attempted intrusion detection system over the internet, including, but not limited to, virus containment;

  (ii) solution that enables the encryption of the personal data processed due to the provision of services, when necessary and according to the level of sensitivity and volume of the information established in the contract or other commercial agreement;

  (iii) systems that prevent or manage any mobile or related devices of uploading information; and

  (iv) a designated and instituted professional, to be the focal point responsible for the measures of privacy and protection of personal data.

5.1.1. SUPPLIER AND / OR BUSINESS PARTNER PERFORMING AS DATA CONTROLLER

The Parties understand that, eventually, according to the scope of the processing activities, provided for in the contractual instrument signed between them, the supplier and / or business partner, will act as an agent for the processing of personal data, under the terms of the LGPD, appearing sometimes as CONTROLLER and other as an OPERATOR.

Considering the coverage limits of each Party, each Party will be individually responsible for the fulfillment of its obligations under the LGPD and other regulations issued subsequently by the competent regulatory authority.

Thus, when the supplier and / or business partner acts and / or appears as a CONTROLLER in addition to the other conditions applicable to the relationship provided for in this Policy, it must:

a. make all decisions related to the activities of processing personal data, which includes the definition of purpose, scope, storage timeframe, forms and means of processing, in an appropriate way to LGPD, communicating to TIVIT in a timely manner when related to the contractual instrument signed with TIVIT;

b. ensure the existence of a legal basis that authorizes the processing of personal data resulting from a contractual instrument signed with TIVIT, under the terms of articles 7 and 11 of the LGPD, being certain that:

i. in cases based on consent, you must collect the free, informed and unequivocal manifestation of the data subject for the treatment of personal data, as well as specific and highlighted one for the treatment of sensitive personal data;

ii. in cases based on legitimate interests, you must prepare a Legitimate Interest Assessment (LIA) and keep the assessment stored for possible demonstration needs; and

iii. for cases in which the processing of personal data may generate risks to civil liberties and fundamental rights, prepare a Data Protection Impact Assessment (DPIA or RIPD) and keep it stored for possible need of demonstration;

c. comply with requests from data subjects regarding the exercise of their rights; and

d. communicate to TIVIT, in writing, when TIVIT acts as OPERATOR of the data, all information and guidance necessary for the data processing to be properly carried out under the terms of the LGPD.

e. This instrument does not modify or transfer ownership or control over the personal data made available, obtained or collected under this instrument, which will remain the property of its original owner.

In relationships in which the supplier and / or business partner acts exclusively as a CONTROLLER, the obligations to be considered during the relationship are restricted to that described in this item.

5.2. ABOUT AUDITS AND DUE DILIGENCE

The necessary documentation to demonstrate compliance with the obligations established in this policy or in the applicable data protection legislation must be made available by the supplier and / or business partner, being TIVIT allowed to carry out audits limited to the scope of service or systems contracted.

TIVIT, by hiring a third party or not, in a previously agreed period, will carry out the audits with the objective of verifying information security measures and controls, and the adequacy of the processing of personal data. Therefore, a confidentiality agreement between the parties will be signed, considering that the company hired to perform the audit, is not a competitor of the supplier and / or business partner in question.

If TIVIT is sued by any person, authority or entity, public or private, due to the leakage of data that was under the responsibility or storage by the supplier and / or business partner, TIVIT is guaranteed the right to denounce the supplier and / or service provider.

Any contract, of an auditor or outsourced security company contracted by TIVIT, must include, in case of access to confidential information or strategy of the supplier and / or business partner, the following requirements:

(i) use for inspection or audit purposes only;

(ii) preservation of business secrets;

(iii) protection of confidential information of the supplier and / or business partner (including any information relating to its other customers); and

(iv) processing of personal data in compliance with the rules established herein.

5.3. INTERNATIONAL TRANSFER OF PERSONAL DATA

When applicable, the supplier and / or business partner must enter into international personal data transfer agreements in order to meet the requirements imposed by data protection laws for other countries. TIVIT must previously consent to the international transfer or sharing of data by the supplier and / or business partner. When there is a need to transfer data outside the country, both TIVIT and the supplier and / or business partner must observe whether the destination countries have compatible privacy regulations and / or adopt Adequacy Contracts or Binding Corporate Rules.

5.4. DATA SUBJECT'S RIGHTS

When TIVIT requests, through a request from the data subject, the supplier and / or business partner must eliminate, correct, anonymize and / or block access to the data, whether permanently or not, that have been treated as a result of contracts of services provisioning, extending to possible copies, with the exception of a different instruction from TIVIT.

In case of legal obligation or systemic impossibility, the supplier and / or business partner may reserve the right to keep personal data for as long as required by law or until the data can be definitively eliminated from the system, seeking to undertake the necessary efforts to ensure their confidentiality until the exclusion within its operational routines is feasible.

5.5. COOPERATION BETWEEN PROCESSING AGENTS

Each party, whether the Controller or Operator, will be individually responsible for the ethical and legitimate use of the data collected and processed, observing the limits and exclusions provided in contracts, commercial agreements or legal obligations.

The supplier and / or business partner, together with TIVIT, must guarantee the exercise of the rights of the data subjects and / or provide support for its realization, when it requires joint action, including necessarily all the rights provided in the LGPD, in the Código de Defesa do Consumidor (Consumer Protection Code, Brazilian law n. 8.078/1990) and other rules applicable to the contracted service model.

If any data subject requests the exercise of his/her rights, the supplier and / or business partner must immediately communicate to TIVIT through communication channels defined in the contract or operational procedures, and if none is defined, an email must be sent to: lgpd@tivit.com.

5.6. SECURITY INCIDENTS AND DATA LEAKAGE

The supplier and / or business partner must have structured plans for cases of incidents involving breaches of personal data. The security incident response plan should provide for immediate notification to TIVIT.

In the event of an incident, regardless of the reason that caused it, and which involves personal data that has been shared or collected on behalf of TIVIT, the supplier and / or business partner must communicate to TIVIT by e-mail to lgpd@tivit.com or in any other way previously agreed, making sure that it is received as soon as possible after the knowledge of the leak. The communication must contain, at least, the following information:

(i) date and time of the incident;

(ii) date and time that the supplier and / or business partner became aware of the incident;

(iii) list of data types affected by the incident;

(iv) number of data subjects affected;

(v) list of data subjects affected by the leak;

(vi) contact details of the Data Protection Officer (DPO) or other person from whom it is possible to obtain more information about the incident;

(vii) description of the possible consequences of the accident; and

(viii) indication of measures being taken to repair the damage and prevent further incidents.

The communication may not exceed the maximum timeframe established in the current regulation, or in the absence of a regulatory definition, the supplier and / or business partner must pay attention to the period of up to 48 hours of awareness of the incident, regardless of the reasons.

If the supplier and / or business partner does not have all the information listed at the time of sending the communication, it should be sent gradually, in order to share the information obtained as quickly as possible, being certain that you will need to keep the communications with TIVIT until all information is made available.

After TIVIT's prior consent, the supplier and / or business partner must also provide:

- Notification to affected individuals (subject to prior approval of the text by TIVIT);
- Notification to ANPD (subject to prior approval of the text by TIVIT);
- The adoption of an action plan, which considers the factors that led to the cause of the incident and that applies measures to ensure the non-recurrence of this event.

For incidents involving personal data caused solely by the supplier and / or business partner, the latter will be responsible for adopting the measures described above, as well as, assuming and complying with any sanctions determined by the ANPD.

5.7. DESTRUCTION OR RETURN OF PERSONAL DATA

The supplier and / or business partner shall, under the command of TIVIT, or when the contractual link or other obligation is terminated, return the shared personal data and perform the definitive deletion of such data, except for those that are under other existing obligations. Exceptions will be allowed only in the case of express command from TIVIT, and the supplier and / or business

partner should extend the retention period of the shared personal data, in order to fulfill possible purposes expressed in additives or other contractual instruments.

5.8. COMPLIANCE WITH LEGAL OBLIGATION

If the supplier and / or business partner is the recipient of any court order or official communication that determines the provision or disclosure of personal information that has been shared or collected on behalf of TIVIT, TIVIT must be notified, within a maximum of 24 (twenty-four) hours, on what happened in a timely manner, so that TIVIT can adopt legal measures to prevent or mitigate the effects resulting from the disclosure of personal data related to this request.

The supplier and / or business partner obligations in the role of OPERATOR will remain for as long as the party continues to have access, is in possession, acquire or carry out any processing of personal data, obtained as a result of the contractual and / or commercial relationship with TIVIT, even if all commercial contracts and agreements between the parties have expired or been terminated.

6. REFERENCE TO OTHER DOCUMENTS

"There is no reference to other documents"