INFORMATION SECURITY AND DATA PROTECTION POLICY - SALINA DIAMANTE BRANCO

SUMMARY

I. INTRODUCTION.

With the exponential increase in the use of personal data both by private sector as well as public bodies, the need for greater protection and guarantee of fundamental rights such as privacy, freedom and the free development of the personality of the natural person. It is in this context that, in 2018, it was created the General Personal Data Protection Law (LGPD, Law nº 13,709/2018) whose main objective is to regulate data protection in Brazil.

In this sense, the LGPD appears as a milestone in the beginning of a new culture, which aims at transparency centered on the individual, minimizing the impact and increasing the security applied to the processing of personal data. In force since 2020, the legislation establishes how companies carry out the collection, use, storage, sharing and control of personal data on national soil.

The impacts of the legislation are diverse, affecting all companies in greater or lesser degree, given that the law imposes a series of sanctions and requirements if it is not effectively complied with. In addition to the issue of legal compliance, being Adequate LGPD guarantees an improvement in the management, flow and structure of the company, as well as as a strengthening with business partners, customers and greater security and reliability in the market as a whole, highlighting the urgency of adapting to the provisions of the law.

II. BASIC CONCEPTS.

- **PERSONAL DATA: Information related to the identified natural person or identifiable. E.g.: name, CPF, ID, address, photographs, gender, etc.**

- **DATA HOLDER: The individual to whom the data refers, that is, the owner of personal data.**

- **SENSITIVE PERSONAL DATA: Data that reveals information related to racial or ethnic origin, religious conviction, political opinion, data relating to**

health or sexual life, genetic or biometric data when linked to a physical person. Such data have more restricted treatment hypotheses.

ÿ ANONYMIZED DATA: Data that refers to a holder who can no longer being identified, occurs when personal data or sensitive personal data loses its individuality. In general, anonymized data is used in statistical studies. E.g. generic data that identifies the individual as belonging to a certain group (man, 60 years old, retired), but who are unable to identify it individually

ÿ CONTROLLER: Individual or legal entity responsible for decisions relating to the processing of personal data. It is up to him to determine the purpose and form of processing of data, in addition to being responsible if there are any incidents involving the data. E.g. a company that collects data to employ employees, a school that collects student data

ÿ OPERATOR: Natural or legal person who processes the data personnel under the controller's command. Ex. an accounting consultancy that processes employee payments from various companies, a cloud system that hosts data.

ÿ PERSON IN CHARGE: Person appointed by the controller and operator to intermediate communication between the controller, data subjects, and the National Data Protection Authority (ANPD). Also called Date Protection Officer (DPO).

ÿ THIRD PARTY: Any natural or legal person hired by the company to develop or assist in the development of its activities, both in quality of suppliers of goods or services, as well as commercial partners.

ÿ PROCESSING: Any type of operation carried out with the personal data of an individual. Examples: collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, deletion, evaluation or control of information, modification, communication, transfer, diffusion or extraction.

- **ÿ CONSENT: It is a free, informed and unequivocal expression by the which the holder allows the processing of their personal data for a specific goal.**

- **ÿ LEGAL BASIS: A legal basis is a purpose provided for by law for which companies, entities and public authorities can process personal data. E.g. execution of an employment contract is an intended purpose to collect necessary employee data. Consent can be a legal basis for sending email marketing. Compliance with a legal obligation may require you to keep some collected data for a period of time. There are 10 legal bases giving different permissions for the use of personal data.**

III. OBJECTIVE AND APPLICATION.

This Privacy and Personal Data Protection Policy has the general objective of providing guidance on how to manage the various activities and existing personal data processing operations at Empresa Salina Diamante White.

In this sense, the document aims to establish the necessary guidelines to guide all team members on the precautions to be observed for the maintenance of Information, with reference to the General Data Protection Law Personal, among other national and international standards relating to privacy and protection of personal data.

The policy applies to (i) SDB employees; (ii) to all third parties, whether they are individuals or legal entities acting for or on behalf of SDB in operations that involve processing of personal data that is carried out within the scope of activities conducted by SDB; (iii) to personal data processing agents external to SDB who in any way are related to the Institution; and (iv) to holders of personal data, whose data is processed by the company.

That said, it is important to highlight that joining the the Company's compliance with personal data protection laws and diplomas regulations arising from it, including this Policy, is mandatory for all recipients indicated above insofar as they relate to SDB. All operations involving the processing of personal data that are carried out within the scope of the activities conducted by Salina are subject to such regulations.

IV. GENERAL RULES.

IV.1. PRINCIPLES.

Salina Diamante Branco must respect the following principles of protection of personal data when processing personal data:

- **ÿ PURPOSE: The Company will process personal data in a manner legitimate, specific, explicit and informed to the holder. Therefore, SDB must inform its intention in using that data and how it will be used, not being able to change this purpose during the treatment;**

- **ÿ ADEQUACY: The processing of personal data will be carried out in a manner compatible with the purposes informed to the data subject, and in accordance with the context of the processing;**

- **ÿ NEED: The use of data must be relevant, proportionate and strictly necessary. In other words, the company will only use what it actually it needs;**

- **ÿ FREE ACCESS: the Company will guarantee holders of personal data access facilitated and free information on the form and duration of treatment, as well as on the completeness of your data;**

- **DATA QUALITY: The data used in the processing must be accurate, clear, relevant to the purpose and correct. Being updated according to the needs of the context in which the treatment is inserted;**

- **TRANSPARENCY: The company will guarantee the data subject that they have clear and accurate information regarding the processing of their data. they will pass;**

- **SECURITY: The company will use technical and administrative measures capable of protect personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or dissemination;**

- **PREVENTION: Always adopt measures to prevent the occurrence of damage to virtue of the processing of personal data;**

- **NON-DISCRIMINATION: Guarantee the impossibility of using personal data, such as racial origin, religious belief or political positioning, to treatments for discriminatory and/or illicit purposes;**

- **RESPONSIBILITY AND ACCOUNTABILITY: Commitment to demonstrate the adoption of effective measures capable of proving compliance with personal data protection standards, and the effectiveness of these measures.**

IV.2. DUTIES AND RESPONSIBILITIES.

The duties of caution, attention and appropriate use of personal data are extend this Policy to all recipients in the development of their work and activities at Salina Diamante Branco, with a commitment to contribute to ensuring that the Company fulfills its obligations in implementing its privacy and protection of personal data.

It is the duty of data holders to notify SDB of any modifications to your personal data in your relationship with the Institution, whether by email institutional, in person at a specific sector or any other appropriate means.

It is the responsibility of SDB employees, personal data processing agents and third parties to obtain the necessary authorization for data processing and to have the necessary documents that demonstrate the designation of their competence for the carrying out the personal data processing operation. Furthermore, it is the duty of such parties not share or guarantee access to personal data held by the Company to any unauthorized or competent person in accordance with the rules of the Company. Institution.

IV.3. DATA PROTECTION OFFICER - DPO.

The so-called Data Protection Officer, or person in charge, is the person appointed by the Controller (natural or legal person responsible for managing and making decisions about the processing of personal data) to act in communication between the controller, data holders and the National Data Protection Authority (ANDP).

In this sense, the DPO is responsible for carrying out the activities, documents and programs related to the protection of personal data in the company, being your duty:

- **ÿ Ensure that all rules and this policy are put into practice by all SDB members;**
- **ÿ Provide guidance and be available to clarify any doubts regarding protection company data;**
- **ÿ Ensure that everyone carries out their activities in accordance with the principles listed in the item above;**

- **Prepare review of documents and impact reports regarding protection data;**

- **Solve any problems relating to data security, mainly related to the personal data processing operation carried out without legal basis, in non-compliance with the Company's Security Policy SDB Information or any other violation of this Policy.**

IV.4. PROHIBITIONS.

Aiming for greater information security and data protection in the company, it is essential to highlight some points that should be prohibited to employees and employees of the Salina Diamante Branco Company. Let's see:

- **Access to any customer information is expressly prohibited, employees or any record in SDB's information systems without a clear business purpose, and directly linked to the exercise of functions assigned in the employment relationship between the employee and the company;**

- **Access to customer data out of mere curiosity is expressly prohibited;**

- **It is expressly prohibited to send information classified as "internal" and "confidential" for email addresses from domains other than the Company, except for third parties (customers or suppliers) directly involved in the respective subject of the message;**

- **Use programs that circumvent the security and control controls imposed by the SDB or its regulations;**

- **Store personal files and/or files not relevant to SDB's business (photos, music, videos, etc.) to network drives as they may overload the storage on servers and accumulating personal data not necessary for the Company's activities.**

IV.5. RISKS THAT MUST BE AVOIDED.

In general, the typical risks that this security policy seeks to avoid are:

- **ÿ Disclosure of sensitive information to unauthorized third parties;**
- **ÿ Disclosure of personal information to unauthorized third parties;**
- **ÿ Improper modifications of data and programs;**
- **ÿ Loss of data and programs;**
- **ÿ Destruction or loss of resources and facilities;**
- **ÿ Theft/theft of personal data;**
- **ÿ Improper use of collected data;**
- **ÿ Unauthorized access.**

IV.6. RELATIONSHIP WITH THIRD PARTIES.

Analyzing the General Data Protection Law, it is clear that the liability in the case of property, moral, individual or collective damages arising from violations of personal data protection legislation is joint, that is, all agents in the chain involving the processing of personal data can be liable for any damages caused.

For this reason, it is essential that efforts are made to verify, evaluate and ensure that such third parties comply with data protection legislation

applicable data, taking into account the possibility of SDB being held responsible for such actions.

Given this point, all contracts with third parties must contain clauses dealing with the protection of personal data, stipulating duties and obligations involving this point, and guaranteeing the commitment of third parties to the legislation of applicable personal data protection. Furthermore, it is necessary to explain from the beginning of negotiations, the security policy established by the company, making the third party aware of the importance of being in line with the LGPD.

IV.7. SANCTIONS.

It is essential to highlight that the General Data Protection Law stipulates a series of sanctions for data processing agents, due to infractions committed to the standards set out in the Law, being subject to some sanctions administrative provisions applicable by the national authority, such as:

- **ÿ Warning, indicating a deadline for adopting corrective measures;**
- **ÿ Simple fine, of up to 2% (two percent) of the revenue of the legal entity of private law, group or conglomerate in Brazil in its last year, excluding taxes, limited in total to R$ 50,000,000.00 (fifty million reais) for infraction;**
- **ÿ Daily fine, subject to the total limit referred to in item II;**
- **ÿ Publication of the infraction after its duly investigated and confirmed occurrence;**
- **ÿ Blocking of personal data to which the infringement refers until its regularization;**
- **ÿ Deletion of personal data to which the infringement refers;**

- **ÿ Partial suspension of the operation of the database to which the infraction refers for a maximum period of 6 (six) months, extendable for an equal period, until regularization of the processing activity by the controller;**

- **ÿ Suspension of the exercise of the personal data processing activity to which the infringement refers for a maximum period of 6 (six) months, extendable for equal period;**

- **ÿ Partial or total prohibition on carrying out activities related to the treatment of data.**

In this sense, violation of this Policy may result in sanctions administrative and/or legal, without prejudice to the termination of the employment contract and/or any other service provision relationship contract between the employee, associate, consultant and/or partner.