EXATO DIGITAL

DATA GOVERNANCE

Sets Exato Digital's Personal Data Governance Policy, establishing principles, guidelines, assignments and responsibilities for personal data management by its employees and third parties.

INTRODUCTION

The General Personal Data Protection Law ("LGPD" in Brazil) defined requirements and obligations to carry out Personal Data treatment activities.

A lot of these requirements and obligations focuses on guaranteeing Personal Data protection and decreasing the leakage risk or other internal issues that can generate damages to the Data Holder. There are plenty of measures that can be taken by the treatment agents to demonstrate that the activities are performed considering the best practices regarding the treatment, and with focus on the Data Holder protection.

That way, it can be said that responsibility and accountability in relation to the LGPD is more than complying with established obligations, but rather being able to demonstrate how the company complies with it.

EXATO DIGITAL LTDA. ("Exato Digital") is an organization with the address registered on Rua Da Consolação, nº 2302, 8th floor, Bairro Consolação, CEP 01302-001, São Paulo – SP, registered on the CNPJ/ME under the nº 12.387.530/0001-13 and collectively referred to as the "Company".

The Company collects and treats Personal Data in its daily operations, such as:

(i) Its employees' Personal Data treatment, for employees' obligations management reasons, including, but not limited to recruiting, onboarding, training, payment check, benefits management, etc.

(ii) Personal Data treatment of its clients, for carrying out its activities, such as user register and account management.

(iii) Personal Data treatment on services provision, under instruction of its clients;

(iv) Third party Personal Data treatment (as job candidates, suppliers, suppliers' employees, etc.), for relevant reasons, including, among others, job candidates' evaluation, contract management and relationship with suppliers, in addition to other necessary purposes to comply with its obligations as Personal Data Controller.

The Company respects the privacy of any Data Holder it collects and treats Personal Data and complies with the laws and regulations that protect Personal Data in Brazil. The Governance Policy explains the relevant privacy principles to Personal Data protection and how these principles should be implemented.

1.1 Scope and Applicability

This Governance Policy covers all collected, accessed, used, managed, stored, disclosed, transferred or treated in any other form by JUR_SP - 38568500v2 - 13124002.460510 Empresa. The Governance Policy applies to all Company directors, executive, managers and employees (current and former, including candidates, collectively referred as "Employees") and third parties that collect and treat Personal Data on behalf of the Company.

The Governance Policy can be complemented by procedures to guarantee the compliance with Personal Data protection local regulations.

If the applicable law and/or contracts impose less requirements than the ones supplied on this Governance Policy, the Privacy Committee can instruct the application of the requirements of this Governance Policy.

If there are any inconsistencies between this Governance Policy and legal obligations of any jurisdiction or agreement, the legal obligations or agreements between parts will prevail over this Governance Policy.

1.2 Updates

The Privacy Committee is responsible for approving any modifications to the Governance Policy and will conduct periodic reviews annually, at least, to account for law changes and applicable Personal Data privacy and protection, technology and business procedures regulations. The updated version of the Governance Policy can be obtained with the Privacy Committee, by contacting privacidade@exato.digital and will also be available on the corporate intranet.

1.3 Monitoring and Assessing compliance with Personal Data protection requirements

The Privacy Committee is responsible of monitoring the compliance with the requirements of this Governance Policy and local laws and regulations applicable on the Personal Data privacy and protection. The person in charge (“DPO”) is responsible for Personal Data privacy and protection periodic reviews. Any reviews and/or privacy audits to be conducted by third parties or individuals outside the Privacy Committee shall be pre-approved by the DPO. All the Employees, including the DPO, should cooperate totally with these Personal Data privacy and protection reviews and/or audits.

II. PERSONAL DATA PROTECTION PRINCIPLES AND RULES

2.1 Law compliance

The Company understands privacy and has a commitment with the protection of Personal Data belonging to Employees and other people, namely clients and suppliers, that provides their Personal Data to the Company. The Employees and third parties that act on behalf of the Company have the responsibility to respect his commitment, as described on the Governance Policy and on relevant Personal Data privacy and protection laws.

It's expected that Employees and third parties that act on behalf of the company recognizes if they are collecting, accessing, using, managing, disclosing, storing, transferring, or treating Personal Data in any other way. They shall be aware of privacy general requirements and principles that govern the Personal Data treatment and know when to forward problems.

By the Privacy Committee and the DPO, the Company provides guidance about its policies and training about Personal Data privacy and protection to help the Employees and third parties directly involved in the Personal Data treatment on behalf of the company on the understanding and fulfillment of its obligations.

2.2 Legal and fair Personal Data collect and use

Principles and Rules

A fundamental principle for Personal Data protection requires that the Company treats Personal Data in a fair and legal way. Besides the Governance Policy, when treating Personal Data, the Company shall consider the laws and relevant regulations.

The following principles shall be followed by those subjected at the Governance Policy:

(i) Purpose: carrying out treatment for legitimate, specific, explicit and informed to the Data Holder reasons;

(ii) Suitability: treatment compatibility with the purposes informed to the Data Holder, according with the treatment context;

(iii) Necessity: limiting the treatment to the minimum needed, including only relevant, proportional and non-excessive data in relation with the purpose of the data treatment;

(iv) Free Access: free access to the information treated by the Controller for the Data Holder;

(v) Data Quality: guarantee, to the Data Holder, of accuracy, clarity and updated data, according to necessity;

(vi) Transparency: guarantee, to the Data Holder, of clear, precise and easily accessible information about the treatment, observed the commercial and industry secrets;

(vii) Security: utilization of technical and administrative measures to protect Personal Data of unauthorize access and accidental or illegal destruction, loss, change, communication or diffusion situations;

(viii) Prevention: adoption of measures to prevent damage occurred by the Personal Data treatment;

(ix) Non-Discrimination: impossibility of treatment for abusive and illegal discriminatory reasons;

(x) Accountability and Responsibility: demonstration of the adoption of effective measures that are capable to prove the fulfillment of Personal Data protection standards, and also the effectiveness of these measures.

The compliance with the principles above can also be guaranteed by carrying out a Data Protection Impact Report ("DPIA"), when (a) the legal base is legitimate interest and (b) upon request by the competent authority, especially if the treatment is considered high risk.

2.3 Personal Data maintenance and administration responsibility

Principles and Rules

A responsible administration of the Personal Data is necessary to protect privacy and comply with the Personal Data protection laws.

Every Employee is responsible for complying with the data protection obligations related to Personal Data. The Employees that treat Personal Data shall take appropriate measures to:

(i) Comply with the company policies to collect, access, use, manage, disclose, store, transfer and, in any other way, treat Personal Data.

(ii) Prevent the improper use of Personal Data for a purpose that's not compatible with the original purpose for which they were collected.

(iii) Keep Personal Data precise and updated during all information lifecycle (meaning from collect to destruction).

(iv) Respond promptly to access requests on the legal deadline if applicable, modification or removal of Personal Data kept by Company (for an example, disposition for “elimination” for marketing communications); requests to exercise a Data Holder’s right to portability of Personal Data.

(v) Protect Personal Data so it won’t be shared with other people that do not have a legitimate reason to access the information.

(vi) Guarantee the traceability of Personal Data during all its lifecycle.

(vii) Keep Personal Data only for the necessary time for the specific purpose or as required by law.

(viii) Report any violation of Personal Data to the Privacy Committee or to the DPO.

Compliance with the principles above can be guaranteed by completing a Privacy by Design document and, depending on the case, a DPIA before the development and marketing of new products or services, that allows changes to the Personal Data treatment or the implementation of new technologies involving Personal Data.

The Privacy Committee or the DPO are responsible of developing, communicating, and providing training on the Company’s privacy program.

2.4 Know how to share Personal Data to third parties or other Company’s affiliates

Principles and Rules

Personal Data can be shared with other Company’s affiliates and subsidiaries (when applicable), governmental agencies and third parties for legitimate reasons or as allowed or required by law.

The Employees responsible of creating of managing relationships with third parties on behalf of the Company must obtain guarantees by writing that the third party is capable and has the intention of protecting Personal Data, according to the principles contained in this Governance Policy. This can be made by third party due diligence, risk evaluation and/or a formal written contract.

It’s necessary the creation of an Annex, a Term or a Data Protection Agreement (“DPA”) whenever access to Personal Data is granted to a third party on behalf of the Company. These agreements may take the form of agreements between affiliates or standard contracts with third parties. All contracts must include the Personal Data protection principles and instructions for its treatment.

Based on risk assessments carried out on third parties, appropriate technical safeguards (e.g., cryptography) or other corrective measures may be planned in contract to guarantee Personal Data adequate protection.

2.5 International Transfer of Personal Data

Principles and Rules

The Personal Data treatment made by third parties can involve the international transfer of these Personal Data (e.g., in cases of services located outside of Brazil). Consult the DPO at all stages of a potential or real international transfer. Personal Data Transfer means any access, visualization or other processing of Personal Data that occur outside of the Brazilian border.

When transferring Personal Data internationally:

(i) Determine if there's a legitimate explanation for the Personal Data transfer (e.g., valid commercial motive);

(ii) Follow the LGPD requirements (e.g., standard clauses established by competent authority).

Before transferring Personal Data internationally, the Employees must get approval of the Privacy Committee or from the DPO.

2.6 Query handling

From the Personal Data Protection Regulators

The Company can receive Personal Data privacy and protection inquiries (for example, questions or complaints related to privacy) from an Inspection Authority. These questions must be sent immediately to the DPO and without unreasonable delay. In certain cases, an inquiry from an Inspection Authority may trigger monitoring, evaluation, or audit activities.

When a privacy inquiry is received from an Inspection Authority, the DPO reviews any and all responses before submission to the Inspection Authority.

Inquiries must be treated in a timely manner, in accordance with applicable law, and the DPO must supervise remediation activities, if any, related to these Inspection Authority inquiries.

From Personal Data Holders

We can receive inquiries or worries from a Data Holder. The Company adopted applicable procedures to guarantee an appropriate response to people that are exercising their individual rights to, among others: (a) know which Personal Data about them are being treated, (b) object to the treatment and/or (c) request correction, deletion or blocking of their Personal Data in certain circumstances determined by the law.

In certain cases, the circumstances related to a Data Holder inquiry, worry or requisition may trigger monitoring, evaluation, or audit activities.

The Employees that collect Personal Data or develop systems that contain Personal Data must guarantee that those rights can be exercised in a timely manner or as required by the local law (usually in 15 days).

The DPO must be immediately notified of any inquiries from Data Holder that are sent to the Inspection Authority and/or ANPD. The DPO must supervise the response activities to the Data Holder.

III. PERSONAL DATA SAFETY AND CONFIDENTIALITY

3.1 Personal Data Protection

The Company protects the Personal Data it treats and implements technical and organization measures for this protection. These measures are used to mitigate destruction, accidental or illegal loss, change, disclosure or unauthorized access or any kind of illegal or unauthorized treatment risk. Sensitive Personal Data, for example, must be subjected to improved security measures.

These standards include safeguards, as strict access controls to IT, to protect Personal Data against a variety of threats, including:

(i) Loss or theft;

(ii) Unauthorized access, use or disclosure;

(iii) Inadequate copy, modification or tampering;

(iv) Inadequate retention or destruction;

(v) Integrity loss.

Any third party that treats Personal Data on behalf of the Company is bound to a contract including, among other safeguards, an obligation of confidentiality in relation of these Personal Data (e.g., on the contract of third party services, employment contracts, etc.), and the obligation to take adequate measures to avoid misuse or Personal Data loss and to prevent the unauthorized access to them. Furthermore, third parties have the obligation to immediately report any known or suspected case of misuse, loss, or unauthorized access to Personal Data to the DPO.

3.2 Personal Data violation management

A Personal Data violation occurs when there is a security breach that leads to the destruction, loss, alteration, unauthorized, illegal, or accidental disclosure of Personal Data transmitted, stored or treated in another form. “Unauthorized” means the treatment that occurs in violation of the applicable privacy law or applicable privacy policies.

Some of the most common privacy breaches occurs when the Employees or clients Personal Data are stolen, lost, or disclosed by mistake. A Personal Data violation can also happen because of a defective commercial procedure or an operational breakdown.

If there is any suspect of a Personal Data violation, the Employees must notify immediately the Privacy Committee and the DPO.

IV. TRAINING

4.1 Training and awareness

The Employees must become familiar with this Governance Policy and any other Company document related to privacy, developed by the Privacy Committee and/or the DPO. Each Employee must participate in trainings that can be given periodically. These trainings will allow interested parties to identify risks related to Personal Data protection and recognize the privacy principles of each project as part of the development and marketing of new products and services.

Directly contact the Privacy Committee with questions about the training or by e-mail **privacidade@exato.digital**.

4.2 Reporting misconduct / potential non-retaliation

Any Employee who becomes aware of a possible violation of the laws applicable to Personal Data and/or this Governance Policy must report it immediately. The Employees that report potential misconduct or that supply information or assist in any investigation or misconduct investigation will be protected against retaliation according with Company policies.

4.3 Responsibilities and Implementation

All Company's Employees have the responsibility to adhere to this Governance Policy in their functional responsibility, for example, leading and providing guidance to other Employees who report to them. All Employees are responsible for adhering to the principles and rules established on this Governance Policy. The Governance Policy must be adopted as part of the Company's internal code of conduct.

V. REFERENCES

Company's internal policies for reference:

1. Security Incident Response Policy

2. Privacy Policy

If you have any questions about privacy or data protection, contact a Privacy Committee member or the DPO (consult the Annex 2 to obtain more details of Privacy Committee contacts).

ANNEX 1 - DEFINITIONS

Definitions

"Anonymization" means the process by which Personal Data are irreversibly removed from all identifiers and can no longer be linked to a person. Once this is done, it will no longer be considered Personal Data.

"Consent" means any freely given, specific, informed indication of a person's agreement with the processing of their Personal Data.

"In Charge" or **"DPO"** is named by the company. Responsible for complying with applicable laws and regulations related to Personal Data protection and for monitoring the organization's compliance with the applicable laws.

"Data Holder" is every identified or identifiable person whose Personal Data is being treated.

"Employees" are Company's employees, temporary employees, interns and unit business contractors.

"Personal Data" are any information related to an identified or identifiable individual.

"Personal Data Violation" means any disclosure, acquisition, access, unauthorized destruction or alteration or any similar action involving Personal Data, or any other incident in which the confidentiality of Personal Data may have been compromised.

"Privacy Committee" means the Company's multidisciplinary committee dedicated to deal with Personal Data privacy and protection issues.

"Sensitive Personal Data" are any personal data about ethnic or race background, religious conviction, political opinion, syndicate or religious, philosophical or political organization affiliation, health or sexual life data, genetics or biometric data, when linked to a person.

"National Data Protection Authority" ("ANPD") is the National Data Protection Authority, created by the law 13.853/19, responsible for privacy and protection of Personal Data issues in Brazil.

"Inspection Authorities" means any authority, including judicial, competent to inspect, judge and apply the pertinent legislation, including, but not limited to, ANPD.

"User": any individual or entity registered on Exato Digital's platforms.

ANNEX 2 - PRIVACY COMMITTEE

privacidade@exato.digital