

SARTORI DE CASTRO



## **PRIVACY AND PERSONAL DATA PROTECTION POLICY**

## INTRODUCTION

### PURPOSE

This Privacy and Personal Data Protection Policy forms part of the internal body of rules of SARTORI DE CASTRO ADVOGADOS (the “Firm”) and supplements the Compliance, Secrecy, and Confidentiality Guidelines set out in its Code of Ethics and Conduct, as well as the Compliance and the Anti-Corruption and Anti-Bribery Policies already in place.

Its purpose is to establish the principles, criteria, limits, responsibilities, and controls applicable to the collection, processing, storage, sharing, retention, and protection of personal data, in accordance with Law No. 13,709/2018 (the Brazilian General Data Protection Law – LGPD) and with national and international best practices, notably ISO/IEC 27701 (Privacy Information Management System – PIMS), in conjunction with ISO/IEC 27001 and ISO 37301.

Through this Policy, the Firm reaffirms its institutional commitment to the ethical, responsible, diligent, and proportionate processing of personal data, respecting privacy, informational self-determination, professional confidentiality, and the fundamental rights of data subjects.

### SCOPE

The provisions of this Policy apply, mandatorily and without restriction, to all professionals and staff associated with the Firm, regardless of the role they perform or the nature of their relationship, including partners, attorneys, interns, employees, service providers, outsourced personnel, and correspondent attorneys, in Brazil or abroad.

It applies equally to third parties and business partners that process personal data in the name, interest, or benefit of the Firm, who must observe data protection standards compatible with this Policy, with applicable law, and with the contractual instruments entered into.

## **CHAPTER I**

### **CONTEXT, ORGANIZATION, AND RESPONSIBILITIES**

SARTORI DE CASTRO ADVOGADOS specializes in legal representation and advice in contentious and advisory matters, notably in the areas of Criminal Law, Economic Criminal Law, Digital Law, Administrative Disciplinary Law, Compliance, and Regulatory Matters.

In carrying out its activities, the Firm processes personal data and sensitive personal data and may act either as Controller or as Processor, within the meaning of the LGPD, depending on the nature of the legal relationship established and the purposes of the processing.

The Firm's organizational structure comprises equity partners, service partners, attorneys, interns, and administrative staff, all of whom are responsible for observing this Policy and the controls and procedures deriving from it.

## **CHAPTER II**

### **LEGAL AND NORMATIVE REFERENCES**

This Policy is based, among other instruments, on the following rules and references:

- Law No. 13,709/2018 (the Brazilian General Data Protection Law – LGPD);
- Regulations, guides, and guidance issued by the Brazilian National Data Protection Authority (Autoridade Nacional de Proteção de Dados – ANPD);
- ISO/IEC 27701 – Privacy Information Management System;
- ISO/IEC 27001 – Information Security Management System;
- ISO 37301 – Compliance Management System.

This Policy forms part of the Firm's SGCAA (Compliance, Anti-Corruption and Anti-Bribery Management System) and is directly linked to the Compliance and Privacy Risk Matrix, a technical instrument for the identification, assessment, treatment, and continuous monitoring of risks relating to the processing of personal data.

## **CHAPTER III**

### **PRINCIPLES OF PRIVACY AND DATA PROTECTION**

The processing of personal data by the Firm will at all times observe the principles set out in Article 6 of the LGPD, as well as the principles of governance, accountability, and continuous improvement set out in ISO/IEC 27701, including: lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy and currency; storage limitation; integrity and confidentiality; and accountability.

## **CHAPTER IV**

### **COLLECTION, PROCESSING, AND SHARING OF DATA**

The Firm may collect and process the personal data necessary for the performance of its institutional, professional, contractual, and legal activities, including identification data, contact data, professional qualifications, financial information, data relating to judicial or administrative proceedings, and other data strictly necessary for the legitimate purposes of the processing.

Collection and processing will observe the criteria of necessity, proportionality, and adequacy; excessive processing, or processing incompatible with the stated purposes, is prohibited.

Personal data may be shared, when strictly necessary and always subject to the duty of professional confidentiality:

- I – with contracted third parties or partners, subject to contractual obligations of confidentiality and data protection;
- II – with public authorities, in order to comply with legal or regulatory obligations or court orders;
- III – for the regular exercise of rights in judicial, administrative, or arbitral proceedings;
- IV – with clients, when the processing arises from services engaged by them.

## **CHAPTER V**

### **DATA PROTECTION**

The Firm adopts appropriate technical and organizational measures to protect the personal data in its custody against unauthorized access, loss, destruction, improper alteration, or any form of irregular processing.

These measures include, without limitation: control of access to systems by means of individual credentials; the use of information security solutions, such as antivirus software; formal secrecy and confidentiality undertakings; and the storage and processing of personal data on the Firm's own servers or on servers contracted from providers recognized as reliable, including in cloud computing environments, which may involve the international transfer of data, provided that an adequate level of protection is ensured, compatible with the General Data Protection Law, with this Policy, and with the controls defined in the Compliance and Privacy Risk Matrix.

Personal data will be kept only for the period necessary to fulfill the purposes of the processing, to perform contracts, or to comply with legal and regulatory obligations. Once those purposes have ended, or where there is no legal basis for retention, the data will be securely deleted or anonymized by means of appropriate technical procedures.

The Firm undertakes to remain permanently up to date on best practices in data protection, promoting the continuous review of its processes and controls.

## **CHAPTER VI**

### **ESSENTIAL PRIVACY CONTROLS**

The technical and organizational measures adopted by the Firm are defined, prioritized, and reviewed on the basis of the risks identified in the Compliance and Privacy Risk Matrix, observing the criteria of proportionality, likelihood, and impact.

The following essential controls, among others, are adopted:

I – clear definition of roles and responsibilities in data processing;

- II – logical and physical access control over information;
- III – formal confidentiality and secrecy undertakings;
- IV – management of third parties and suppliers with data protection clauses;
- V – identification, assessment, and treatment of privacy risks;
- VI – procedures for responding to data subjects' rights requests;
- VII – mechanisms for incident prevention, detection, and response;
- VIII – periodic training and awareness-raising;
- IX – periodic review of the related policies and controls.

## **CHAPTER VII**

### **SECURITY INCIDENTS AND DATA BREACHES**

The Firm will maintain internal procedures for identifying, containing, assessing, and responding to security incidents that may compromise personal data, including for the purpose of notifying the National Data Protection Authority and data subjects, where applicable.

## **CHAPTER VIII**

### **PERSONS RESPONSIBLE FOR DATA**

The Firm designates its managing partners as its Data Protection Officers (DPO), responsible for liaising with data subjects and with the National Data Protection Authority, in accordance with applicable law.

## **CHAPTER IX**

### **RIGHTS OF THE DATA SUBJECT**

The Firm ensures the full exercise of the data subjects' rights set out in Article 18 of the LGPD, including, among others, the rights of confirmation, access, correction, anonymization, portability, deletion, information, and withdrawal of consent.

The exercise of these rights must be expressly requested by the data subject or by his or her legal representative, by means of a communication addressed to the Data Protection Officers at [contato@sartoridecastro.com](mailto:contato@sartoridecastro.com), indicating in the subject line that the request relates to Data Protection.

## **CHAPTER X EFFECTIVE DATE AND UPDATES**

This Policy takes effect on the date of its approval and will be reviewed periodically, or whenever there are significant changes in the legislation, in the organizational structure, in the risk profile reflected in the Compliance and Privacy Risk Matrix, or in the Firm's processes, in keeping with the principles of continuous improvement set out in the applicable ISO standards.

São Paulo, February 10, 2026.

**SARTORI DE CASTRO ADVOGADOS**

---

*This document is a translation of the original Portuguese version. In the event of any discrepancy or conflict between this translation and the Portuguese version, the Portuguese version shall prevail.*