AROEIRA SALLES LAW FIRM'S PRIVACY AND PERSONAL DATA PROTECTION POLICY

I. INTRODUCTION

Aroeira Salles Law Firm ("Firm"), in its commitment to comply with Brazilian legislation on the protection of personal data, presents its Privacy and Personal Data Protection Policy ("Policy") to explain in a clear and accessible manner the regularity of the processing procedures carried out by the Firm or by third parties on its behalf.

II. OBJECTIVES

Without replacing or overriding the provisions of Federal Law No. 13,709/2018 (General Data Protection Law or "LGPD") and related regulations, neither Federal Law No. 8,906/1994 (Statute of Solicitors and Barristers and the Brazilian Bar Association) and other legal regulations applied to solicitors and barristers, this Policy aims to present the rules applicable to the processing of personal data carried out by the Firm or by third parties on its behalf in order to provide a clear understanding of the rules and principles regarding the subject, which are fundamental for the Firm.

Thus, this Policy formalizes and details the commitment of the Firm to (i) ensure the rights of data subjects in personal data processing; (ii) adopt processing, mechanisms, and rules in compliance with standards and good practices relating to privacy and the protection of personal data; (iii) promote transparency regarding personal data processing; (iv) protect the Firm, as well as its employees, clients, and partners, from risks involving incidents concerning personal data security; and (v) establish guidelines for the safeguarding, use, and sharing of personal data.

III. APLICABILITY AND RECIPIENTS

This Policy is applicable to everyone, whether they are members of the Firm, clients, service providers or any other stakeholders of the Firm in Brazil and abroad, that is, all natural and legal persons who have or may have contact with personal data processed by the Firm or on its behalf, on any type of physical or digital basis, including, but not limited to, personal data recorded on paper, maintained in computer systems or portable devices, as well as personal data transmitted by any means.

This Policy must be complied with the other policies that make up the Firm's Compliance Program.

IV. DEFINITIONS

The following definitions and descriptions should be considered for a better understanding of the purposes of this Policy:

a) **National Data Protection Agency (ANPD):** A federal public administration agency, linked to the Presidency of the Republic, with competencies as the central authority of the Brazilian personal data protection system;

b) **Personal Data:** Information related to a legal person (an individual) which can identity who the person is or to make this person identifiable;

c) **Sensitive Personal Data**: Personal data regarding more intimate aspects of an individual. According to the LGPD, sensitive data includes information related to racial or ethnic origin, religious beliefs, political opinions, membership in a trade union or religious, philosophical, or political organisation, data related to health or sexual life, genetic or biometric data when linked to a natural person;

d) **Anonymized Data:** Data that, during its processing, has undergone a specific process that rendered it unable to identify its owner, no longer being considered a personal data;

e) **Database:** A structured set of personal data maintained in one or more locations in either physical or digital form;

f) **Data Subject:** The individual to whom the personal data belongs;

g) **Data Processing Agents:** Controllers and processors, which are those who perform personal data processing. Individuals acting under instructions, such as the Firm's employees, are not considered controllers or processors;

h) **Controller**: The person responsible for taking decisions regarding the processing of personal data. It can be a natural or a legal person governed by public or private law;

i) **Processor:** The person who processes personal data on behalf of the controller. It can also be a natural or a legal person governed by public or private law;

j) **Sub-Processor:** The natural or legal person contracted by the processor to assist in processing personal data on behalf of the controller;

k) **Personal Data Processing:** It encompasses all operations carried out with personal data. Data processing may involve, among other activities, collecting, generating, receiving, classifying, using, accessing, reproducing, transmitting, distributing, processing, archiving, storing, deleting, accessing, controlling, modifying, communicating, transferring, disseminating, or extracting personal data. Data processing occurs when any of these activities are performed independently or in conjunction with the others;

l) **Personal Data Protection Officer:** The individual designated by the controller or the processor to work as a communication channel between the controller, data subjects, and the National Data Protection Authority (ANPD);

m) **Deletion:** The removal of data or a set of stored data. Deletion typically occurs after the data's storage period has expired, which depends on the purpose of the data processing;

n) **International Data Transfer:** It is the transfer of personal data to another country or to an international organisation of which Brazil is a member. This can take place physically or virtually, through servers hosted in different countries; and

o) **General Data Protection Regulation (GDPR):** European regulation on the protection of personal data.

V. GUIDING PRINCIPLES OF DATA PROTECTION

The Firm will adhere to the following principles in the processing of personal data it carries out, and it will also require that all third parties processing personal data on behalf of the Firm also adhere to them:

a) **Purpose:** Personal data processing will be carried out only for legitimate, specific, explicit, and informed purposes to the data subject, with no possibility of subsequent processing that is incompatible with these purposes;

b) **Adequacy:** Personal data processing shall happen in a manner consistent with the purposes informed regarding the data subject and with the context of the processing;

c) **Necessity:** Personal data processing shall happen in a manner consistent with the purposes informed regarding the data subject and with the context of the processing;

d) **Free Access:** Data subjects shall have facilitated and free access to information regarding the manner and duration of the data processing and to the totality of their data;

e) **Data Quality:** Data subjects shall be ensured accuracy, clarity, relevance, and updates of data as needed and for the purpose of data processing;

f) **Transparency:** Clear, accurate, and easily accessible information shall be provided to data subjects regarding the processing and the respective data processing agents, while respecting trade and industrial secrets;

g) **Security:** Technical and administrative measures shall be adopted to protect personal data from unauthorised access and from accidental or unlawful destruction, loss, alteration, communication, or dissemination;

h) **Prevention:** Measures shall be adopted to prevent harm to data subjects due to the processing of their personal data;

i) **Non-Discrimination:** No personal data shall be processed in any way for unlawful, discriminatory, or abusive purposes; and

j) **Responsibility and accountability**: The adoption of effective measures capable of proving compliance with personal data protection rules must be demonstrated, as well as the effectiveness of these measures.

VI. RIGHTS OF DATA SUBJECTS

The Firm will proactively work to ensure that data subjects exercise their rights guaranteed by current legislation, including:

Your Rights	Explanation

Confirmation and Access	The data subject has the right to confirm the existence of processing of his/her personal data and may request and receive a copy of all personal data that belongs to him/her and is subject to processing by the Firm.
Correction	The data subject can request the correction of personal data that is incomplete, inaccurate, or outdated.
Anonymization, Blocking, or Deletion	The data subject may request (a) anonymization of his/her data, which is the process by which personal data loses the capacity to generate direct or indirect association with the data subject; (b) the blocking of his/her Personal Data, temporarily suspending its processing for certain purposes; and (c) the deletion of personal data that is processed based on his/her consent, except in cases where maintenance is allowed by the law, in which case the Firm reserves the right to choose the procedure to be adopted.
Portability	The data subject may request his/her personal data to be made available to another provider or service provider. This request is subject to the technical limitations of the Firm's infrastructure, ANPD regulations, and professional and commercial secrecy.
Information about the Possibility of Not Consenting	The data subject has the right to receive clear and complete information about the possibility and consequences of not giving consent when requested by the Company. Consent, when necessary, must be freely given and informed. Therefore, whenever consent is requested, the data subject will be free to deny it - in these cases, some services may not be provided.
Revocation of Consent	The data subject has the right to revoke his/her consent, with the treatments carried out up to the moment of revocation remaining valid. The data subject will be informed about the consequences of revoking his/her consent and about possible alternatives.
Opposition	In some cases, the law authorises the processing of personal data even without the consent of the data subject. Thus, if the data subject does not agree with any purpose for which his/ her personal data is processed, they may object under the terms of the LGPD.

VII. DUTIES FOR THE PROPER USE OF PERSONAL DATA

The duties of care, attention, and proper use of personal data extend to all recipients of this Policy without prejudice to specific duties applicable to each recipient according to his/her situation.

VII.1. Duties of all recipients of this Policy:

All recipients of this Policy must act in good faith and in compliance with the current legislation, refrain from causing hindrances to the regular exercise of data subject rights, and contact the Firm´s Data Protection Officer when there is a suspicion or occurrence of personal data processing operations contrary to this Policy, the LGPD, and related regulations.

VII.2. Specific duties of data subjects:

Data subjects shall always provide correct and up-to-date information to the Firm regarding their personal data, always acting in good faith.

VII.3. Specific duties of Firm members:

Members of the Firm must respect the principles for the processing of personal data collected by the Firm, especially the need for it, the purpose for which it is processed and the legal basis supporting its processing. In addition, professional confidentiality inherent to the practice of law must be observed throughout the course of activities, with personal data processing always limited to activities authorised by the Firm.

Furthermore, it is the responsibility of Firm employees to:

a) Be aware of, respect, and enforce this privacy and personal data protection policy;

b) Respect the workspaces of other colleagues;

c) Carry out personal data processing in accordance with the current legislation;

d) Inform the Data Protection Officer in case of changes in existing processing procedures or the creation or discontinuation of any processing procedure;

e) Participate in training on this policy and personal data protection legislation;

f) Maintain confidentiality regarding personal data to which they have access, refraining from any unauthorised or improper sharing;

g) Submit any doubts regarding the legality of a specific processing procedure to the Data Protection Officer; and

h) Report any irregularities related to the processing of personal data through the available internal channels.

VII.4. Specific duties of third parties processing personal data

All third parties processing personal data on behalf of or at the request of the Firm, whether as a controller or processor, assume the following duties without prejudice to others arising from law or contract:

a) Comply with the Firm ´s rules, recommendations, and guidance on information security and the prevention of security incidents;

b) Not provide access to the personal data processed by the Firm to any unauthorised persons;

c) Conduct processing in accordance with the current legislation, observing the principles listed in the LGPD;

d) Participate in training on this policy and personal data protection legislation when invited;

e) After the termination of the contract and the fulfilment of the data processing purpose, delete the personal data provided by the Office, or adopt an effective anonymization process using secure, reasonable, and disclosed technical means, and may only retain the data in their systems if, by legal or regulatory obligation, such retention is necessary;

f) Take all necessary and reasonable measures to ensure a satisfactory level of security in the personal data processing as established in the contract and require such measures to be also observed by their representatives and/or service providers involved in data processing;

g) Maintain confidentiality, secrecy, and integrity of all information and/or personal data to which there is access by virtue of the contract;

h) Notify the Firm in advance in cases of international transfer of personal data, observing, in any case, the provisions of current legislation and this policy on the subject; and

i) Immediately and in writing, report to the Firm any data breach incident and/or other personal data violation, as well as in the event of any administrative civil or criminal investigation related to non-compliance with obligations related to the protection of personal data, from the moment they become aware of the fact or its suspicion, also providing information on the measures taken to mitigate risks and damages.

VIII. PERSONAL DATA PROCESSED

In the provision of legal services, the Firm may have access to and process different types and quantities of personal data depending on the relationship between the data subject and the Firm as well as the basis that underlies this connection. Personal data collected for the defense of one of our clients 'rights will differentiate from those of our employees.

Regardless of this, in any processing carried out, the Firm always processes personal data with the support of one of the legal bases provided in Article 7 of the LGPD and, when processing sensitive personal data, in Article 11.

Personal data may be collected in various ways, either through direct provision by the data subjects themselves, or through someone related to the data subject, such as the employing company contracting with the Firm. Personal data may also be accessed from publicly accessible sources.

Therefore, to bring transparency to its actions, the Firm sets out the purposes and contexts for which it processes the personal data collected:

VIII.1 Service Provision

For the provision of our professional services, within the limits of applicable law and in compliance with the ethical and confidentiality principles applied to solicitors and barristers, we collect and process personal data with the purpose of supporting our clients in various areas of law, seeking to achieve the desired legal objectives.

This personal data is provided directly by the data subject, by third parties appointed by him/her, or it is obtained from public sources. Among the data that the Firm may process, there are:

a) Registration data: Such as name, address, CPF (Brazilian tax ID), RG (identity card), company for which they work;

b) Financial data: Such as remuneration, transaction history, bank account number;

c) Contact data: Such as email, telephone number;

d) Authentication data: Such as signature and digital signature;

e) Sensitive data: Depending on the service to be provided, health information and union membership;

f) Identity data: Such as photos and videos;

g) Other personal data necessary for the provision of services by the Firm.

VIII.2. Contracts

The firm signs contracts with other companies for activities other than its core business and that are necessary for it to function properly. In these contracts, sometimes, there is a need to process the personal data of employees and third parties, which is done within the limits of the principles of the law and the objectives pursued.

This personal data is provided directly by the data subject or by a third party appointed by him/her and may include registration data, contact information, financial data, among other personal data necessary for hiring.

VIII.3. Selection Processes

In conducting its selection processes, the Firm processes personal data of candidates who are interested in working at the Firm. The information to participate in the selection processes is sent by the data subjects themselves and may include various types of personal data, mostly résumés containing identification data, contact details, academic and professional records, and, eventually, photographs.

After the selection process period, the documents are kept in the Firm's Human Resources department for a maximum period of 6 (six) months for potential future opportunities and are discarded after that period.

VIII.4. Collection and Use of Cookies

The Firm 's website does not directly store cookies; however, Google Analytics collects and stores them strictly to analyse traffic volume and browsing patterns, in compliance with Article 15 of the Brazilian Civil Rights Framework for the Internet (Law No. 12.965/14).

This information is necessary for the website's operation and measuring access to content on the Firm's website. It is not possible to identify the data subject from the collected data.

IX. PERSONAL DATA SECURITY

IX.1. Proportionality and Necessity

The personal data processed by the Firm can only be accessed by duly authorised professionals and for predetermined purposes in accordance with the principles of proportionality and necessity. Additionally, the Firm has protection against unauthorised access to its systems.

IX.2. Processing of Personal Data by Third Parties

As provided in this Policy, third parties who process personal data on behalf of or at the request of the Firm must commit to respecting the personal data protection laws, the conditions stipulated in this Policy, and other applicable privacy and information security regulations. This commitment will be included in the contracts signed between the Firm and the third parties; besides, non-compliance may result in penalties.

IX.3. Information Security and Best Practices

The Firm also has an Information and Technology Security Management Policy, based on which it employs appropriate and reasonable technical and organisational measures in the personal data processing. The Firm's Information Technology Department, composed of specialised professionals, is responsible for the management of this Policy.

The Firm makes every necessary effort to protect personal data against unauthorised access, loss, destruction, and unauthorised sharing, employing security systems commonly adopted to minimise the risks of data exposure, such as periodic backup of its servers, considering the criticality of the system, and firewall tailored to its system needs.

X. SHARING OF PERSONAL DATA

The personal data processed by the Firm may be shared with other data processing agents in cases where such sharing is necessary for:

a) The fulfilment of the processing purpose;

b) Safeguarding and protecting the rights of the Firm; and

c) Competent judicial, administrative, or government authorities when there is legal authorization or a competent court order.

Among others, the Firm may share data with the following data processing agents:
(i) Financial institutions for banking services; *(ii)* Public authorities (judicial and extrajudicial), regulatory or tax agencies, before which the Firm is subject to legal or regulatory obligations; *(iii)* Legal correspondent *(iv)* Information technology specialist companies; *(v)* Cloud computing; *(vi)* Accounting professionals; and *(vii)* Health insurance providers.

Our partners will only be authorised to process personal data within the limits and for the specific purposes set to achieve the desired objective. Data sharing will only happen when it is essential for

the execution of the services provided by the Firm, as set forth in this Policy.

XI. INTERNATIONAL TRANSFER

The Firm may transfer personal data collected in Brazil to other countries. Such transfer also extends to cloud service providers used by the Firm, ensuring that we always adopt third-party services with the best practices and industry standards regarding privacy and personal data protection.

Additionally, the Firm may share personal data located in Brazil with its unit located abroad (United Kingdom). When doing so, the Firm will take appropriate measures to ensure the adequate protection of your personal data in accordance with Brazilian legal requirements.

XII. STORAGE OF PERSONAL DATA

The personal data processed by the Firm are stored in secure and controlled environments, whether physical or virtual, for no longer than is necessary to fulfil the purpose for which it was processed, and they are deleted after the completion of the processing.

The personal data collected are stored on an internal server or in cloud computing with restricted access. There may also be storage of personal data in physical databases managed by the Firm or by third parties, always in compliance with this Policy and applicable legislation.

XIII. TRAINING

Firm employees whose roles involve personal data processing must participate in periodic training on personal data protection and this policy. All third parties who process personal data on behalf of the Firm or have any relationship with the Firm as data processing agents must also undergo training whenever required by the Firm.

XIV. REVIEW AND MONITORING OF THE POLICY

The Firm reserves the right to change this Policy by publishing the updated version whenever necessary to reflect changes in current legislation, regulations issued by the ANPD (Brazilian National Data Protection Authority), or other competent authorities, as well as in response to the emergence of new technologies and modifications in data processing processes carried out by the Firm.

XV. DATA PROTECTION OFFICER

There is a Data Protection Officer of the Firm, identified as follows:

Name: Nayron Sousa Russo

Contact: dpo@aroeirasalles.com.br

Address: Funchal Street, No 129, 10th floor, Room 10B, Vila Olímpia, Zip Code 04551-060

The Data Protection Officer shall have the following functions, among others assigned by applicable law and regulations:

a) Evaluate requests and other communications from data subjects, provide explanations, and take appropriate actions;

b) Receive communications from the ANPD and take actions;

c) Conduct training on this Policy and the legislation on personal data protection;

d) Clarify doubts of Firm members or third parties who process personal data on behalf of or at the request of the Firm;

e) Promote continuous monitoring of compliance with the provisions of this Policy, proposing measures deemed necessary to enhance the Firm's personal data management system;

f) Manage compliance with obligations assumed by the Firm with third parties concerning privacy and personal data protection; and

g) Perform other duties determined by the controller or established in complementary regulations.

The Firm's Shareholders' Assembly will grant the Data Protection Officer the autonomy, authority, and resources necessary for the proper exercise of their functions.

XVI. REPORTING

The Firm encourages anyone who becomes aware of any act that contravenes the provisions of this Policy or of any illegality involving the rules on the protection of privacy and the protection of personal data to report the fact to the Firm's Whistleblowing Channel by the following means:

a) Sending an email to the external email address: denuncias@aroeirasalles.com.br

b) Sending a correspondence titled "Reporting Channel/Aroeira Salles Advogados" to the following address: "Dos Timbiras Street, No 1754, 12th e 13th floors, Lourdes, ZIP Code 30140-061"

c) Sending an email to the Firm's Personal Data Protection Officer: dpo@aroeirasalles.com.br

d) **Phone:** (+55 31) 3248 2300.

All information provided in the report will be treated with absolute confidentiality and the anonymity of the reporter will be ensured if they so desire. The investigation of the report will follow the provisions of the Firm's Whistleblowing Channel Policy.