Policy for Reporting Incidents Involving Personal Data

This Policy for Reporting Incidents Involving Personal Data ("Policy") comprises the principles and standards of conduct that will guide the actions of the BUSINESS MEDIATION AND ARBITRATION CHAMBER – BRAZIL (CAMARB) ("CAMARB"), with regard to possible information security incidents, establishing the rules for the continuity of CAMARB's business.

This Policy is subordinate and complementary to CAMARB's Privacy and Personal Data Protection Governance Policy and must be interpreted in accordance with the guidelines and principles of that policy.

1. SCOPE

1.1. Security incidents, subject to this Policy, are any unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or any form of inadequate or unlawful processing of personal data under CAMARB's control ("Incidents").

1.2. Personal data subject to this Policy, in accordance with applicable legislation, is any and all information related to an identified natural person or that can be identified through reasonable efforts by CAMARB, or that can be individualized through the processing of such information by CAMARB, even without being identified. This includes information about directors, employees, customers, suppliers and service providers, as well as other people who have a relationship with CAMARB.

1.3. This document covers the response to security incidents involving personal data processed by CAMARB, and its communication to affected individuals or legal entities, following the principles and rules outlined in CAMARB's Privacy and Personal Data Protection Governance Policy in order to ensure the appropriate and timely management of security incidents and the mitigation or elimination of any losses arising therefrom, including the eventual disposal and/or deletion of information and documents containing personal data held by CAMARB, its contractors and subcontractors.

2. APPLICATION

2.1. The Policy applies to all employees, directors, advisors, partners, suppliers and service providers involved in personal data processing operations carried out by CAMARB.

3. OBJECTIVES

3.1. The objectives of this Policy are:

a) Ensure that CAMARB responds quickly and effectively to Incidents involving personal data, in order to comply with the General Personal Data Protection Law – LGPD (Law No. 13.709, of August 14, 2018) and other applicable laws and regulations;

b) Objectively define the risk assessment and decisions regarding the need to report Incidents, as determined by law;

c) Avoid harmful consequences of Incidents addressed by this Policy to the privacy of personal data holders and to the image and market value of CAMARB;

d) Instruct CAMARB employees, directors, advisors, partners, suppliers and service providers regarding the need and importance of information security and the effective response and communication of incidents involving personal data; and

e) Define the attributions, authorities and responsibilities in the information sharing process.

4. INFORMATION SECURITY AND PERSONAL DATA PROTECTION COMMITTEE

4.1. As defined by CAMARB's management, the CAMARB Information Security and Personal Data Protection Committee ("Committee") was established, with a two-year term and composed of the Personal Data Processing Officer and representatives of the board of directors and the Legal, Human Resources and Technology sectors of CAMARB.

5. RESPONSE TO SECURITY INCIDENTS INVOLVING PERSONAL DATA

5.1. The security incident response procedure will be carried out with the highest priority and urgency, including non-business days and/or the normal working hours of the Committee members.

5.2. Any event that may constitute an Incident must be forwarded to the Committee, which will be responsible for establishing procedures for its resolution within 2 (two) business days from the date of becoming aware of the Incident. By decision of the Committee, representatives from other CAMARB's departments may be involved.

5.2.1. If it is not possible to meet this deadline, the reason for the impossibility must be recorded by the Person in Charge and, if it is decided to communicate the Incident, it must also be informed to the National Personal Data Protection Authority – ANPD.

5.3. Under the Committee's guidance, CAMARB will mobilize external advisors in information technology, public relations (press) and law to assist it in responding to the Incident, as necessary.

5.4. Once the Incident has been configured, the Committee will be responsible for adopting the necessary actions to interrupt the incident, recover affected personal data and communicate the incident in accordance with this Policy and in compliance with CD/ANPD Resolution No. 15/2024.

5.5. In parallel with the deliberation on emergency measures, the Committee will designate an employee from CAMARB's Information Technology sector to check the compromised repositories and systems, and the Person in Charge will be responsible for checking the Personal Data Processing Operations Records for the categories of personal data controlled by CAMARB and their respective affected data subjects, in order to delimit the extent of the Incident and the potential risk to data subjects, third parties and CAMARB.

5.6. The Officer will prepare a report on the measures taken by CAMARB to respond to the Incident, including its extent and potential risks. Based on this report, the Committee will issue a reasoned opinion on the Incident to CAMARB's management, with the relevant recommendations, in particular with its understanding of the potential risks to data subjects and the need to communicate the Incident in accordance with art. 48 of the LGPD. Said opinion will adopt the risk matrix recommended by the ANPD or, in the absence of such, another risk matrix that, in its opinion, is consistent and appropriate.

5.7. It will be up to the CAMARB Board of Directors to decide whether to accept, in whole or in part, the Committee's opinion, or to reject it, according to its opinion on the risks to CAMARB's image. The decision will be promptly communicated to the Committee, and the person in charge will be responsible for recording it.

5.8. In the event of communication of the Incident, the Committee, together with external public relations and press advisors, will be responsible for preparing the draft of the communication, which will be validated by CAMARB's management and then disclosed to the market and/or to affected or potentially affected holders, as the case may be.

5.9. In the same case, the Committee, together with CAMARB's legal department advisors, will arrange for the Incident to be communicated to the ANPD through institutional means and channels, notably the “Personal data security incident communication form to the National Personal Data Protection Authority”, and must take the measures required by the ANPD.

5.10. The Officer, on behalf of the Committee, will be the spokesperson for CAMARB for the purposes of this Policy and the only authorized person to comment and make public announcements regarding Incidents. All other employees, directors, advisors and partners of CAMARB are prohibited from commenting publicly on the matter.

6. OPERATORS AND OTHER CONTROLLERS OF PERSONAL DATA

6.1. Any third parties acting as operators or controllers of personal data relating to CAMARB, or obtained through it, must undertake to follow this Policy in the event of Incidents, as well as to:

a) Inform the Manager immediately after becoming aware of an Incident;

b) Cooperate with CAMARB to respond to the Incident, immediately providing all necessary information and assistance;

c) Refrain from responding to the Incident on their own, and must respond jointly with CAMARB if they are a personal data controller, or limit themselves to following CAMARB's instructions if they are an operator.

6.2. If CAMARB acts as a data processor of personal data controlled by third parties, it will be responsible for cooperating with the third party in communicating the Incident, with this Policy applying in a subsidiary manner, in cases where there is a risk of loss, damage or harm to CAMARB, or of CAMARB being held liable for the inaction of the third party controller.

6.3. CAMARB shall provide mechanisms for third party consent to this Policy.

7. RESPONSIBILITIES

7.1. Each employee, director, advisor, service provider and contractor of CAMARB is responsible for their own actions in relation to compliance with this Policy, in accordance with the activities they perform at CAMARB, for compliance with this Policy and other applicable standards, as well as for enabling the proper performance of the work of the Person in Charge and the Committee. Directors, advisors and managers are also responsible for ensuring compliance with this Policy by employees and third parties under their responsibility, in accordance with their attributions.

7.2. Failure to comply with this Policy will be punished according to the nature of the offender's relationship with CAMARB, the severity of the violation and CAMARB's internal rules, and may lead to the offender's termination or dismissal, without prejudice to compensation for losses and damages caused to CAMARB.

8. MISCELLANEOUS

8.1. This Policy will be communicated to CAMARB’s employees and will be subject to review at least annually.