

Privacy and Personal Data Protection Governance Policy

This Privacy and Personal Data Protection Governance Policy (“Policy”) comprises the principles and standards of conduct that will guide CAMARB – CÂMARA DE MEDIAÇÃO E ARBITRAGEM EMPRESARIAL – BRASIL (“CAMARB”) in relation to personal data under its control, including data of its directors, employees, suppliers, service providers, partners and any other persons, regardless of the means by which such personal data was collected, received, or generated by CAMARB.

This Policy imposes and demonstrates that the management and processing of personal data by CAMARB observes the guiding principles of personal data protection, as regulated in the General Law for the Protection of Personal Data - LGPD (Law No. 13.709, of August 14, 2018), in the Brazilian Internet Bill of Rights (Law No. 12.965, of April 23, 2014), in the Federal Constitution of 1988 and in the Resolutions published by the National Authority for the Protection of Personal Data, indicating the applicable procedures, and establishing a responsibility structure focused on the implementation and maintenance of privacy governance practices.

1. SCOPE

Personal data subject to this policy, in accordance with applicable legislation, is any and all data related to an identified natural person or that can be identified through reasonable efforts by CAMARB, or that can be individualized through the processing given by CAMARB to this information, even without being identified.

2. APPLICATION

This Policy applies to all employees, directors and administrators, partners, suppliers, representatives and service providers when, in the exercise of their functions, they are involved, participate or, in any way, interfere in the processing of personal data controlled by CAMARB.

3. OBJECTIVES

CAMARB respects the privacy and informational self-determination of individuals whose personal data is under its control, always guided by good faith and the ethical use of such data. CAMARB does not sell personal data and acts to preserve the rights and freedoms of data subjects and third parties affected by the processing of personal data by CAMARB.

4. PRINCIPLES

Practices related to the collection, use, sharing, maintenance, deletion and, ultimately, all personal data processing operations by CAMARB will observe the following principles:

- **Purpose:** the processing of personal data will always be carried out for legitimate, specific, explicit purposes and informed to the holder, when requested, and compatible with the interests and activities of CAMARB, in accordance with the objectives of its business, without the possibility of subsequent processing in an incompatible manner with these purposes;
- **Adequacy:** the processing of personal data will always be appropriate for its purpose, according to the context of the processing;

- **Need:** the processing of personal data, including its collection and storage by CAMARB, is limited to the minimum necessary to achieve its purposes, covering pertinent, proportional and non-excessive data in relation to such purposes;
- **Free access:** CAMARB will guarantee to the holders, as indicated below, easy and free consultation on the form and duration of the processing of their respective personal data, as well as, to the extent possible, access to their personal data processed by CAMARB, except in cases where it is legitimate to refuse them such access due to the purposes and circumstances of the use of such personal data;
- **Data quality:** CAMARB will keep personal data accurate, clear and up to date;
- **Transparency:** within the limits provided for by law, CAMARB will provide clear, precise and easily accessible information on the processing of personal data to the respective holders, as well as the respective processing agents, in the manner identified below;
- **Security and confidentiality:** CAMARB will adopt technical and administrative measures capable of protecting personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or dissemination, always applying appropriate security standards to the specific risks of each activity and observing the state of the art and best applicable market practices;
- **Damage prevention and mitigation:** CAMARB will make its best efforts to prevent damage from occurring due to the processing of personal data and to mitigate or repair it if it occurs;
- **Non-discrimination and ethical treatment of personal data:** no treatment will ever be carried out for discriminatory, unethical, illicit or abusive purposes; and
- **Accountability and Transparency:** CAMARB will adopt mechanisms to confirm and demonstrate the effectiveness of its governance program in privacy and data protection, including in compliance with applicable legislation.

5. GUIDELINES FOR THE PROCESSING OF PERSONAL DATA

Any and all processing of personal data collected, received or generated by CAMARB must be carried out for one or more legitimate purposes, duly mapped, recorded and, if necessary, communicated to the respective holders. No personal data will be subject to processing if it is not necessary for one or more purposes. All personal data will have its life cycle monitored and recorded from the moment CAMARB gains control over it until the moment it is definitively discarded.

CAMARB controls and processes various types of personal data, namely:

- Data on its directors and administrators for making and recording administrative and legal management decisions at CAMARB, as well as changing its corporate documents;



- Data of its employees and service providers related to the fulfillment of their employment and service provision contracts, the respective payment, internal communication and the management of the work carried out, as well as those data necessary for the production of reports on compliance with the contract to the competent entities and inspection authorities in accordance with the law and for the exercise of the corresponding rights;
- Biometric data and other personal data of employees and other people who have access to CAMARB's premises, networks and systems, for the purpose of managing access, ensuring their security and preventing fraud in relation to the use of CAMARB's resources;
- Employee and dependent data required to manage contractual and social security benefits;
- Data from suppliers of goods and services related to the fulfillment of contracts signed with CAMARB and the exercise of corresponding rights;
- CAMARB website user data, collected for their specific purposes in the form of their respective notices and privacy policies;
- Data of representatives, lawyers and attorneys who act in defense of CAMARB's interests, as necessary for the exercise of rights and for the management of judicial, administrative and arbitration procedures;
- Personal data obtained through CAMARB communication networks, for contact management, advertising and internal statistics;
- Personal data transmitted and/or circulated within the scope of procedures administered by CAMARB, regardless of their nature (arbitration, mediation or DRB), for the necessary period for the complete management of the respective procedures; and
- Personal data of participants in events promoted by CAMARB, including the Brazilian Business Arbitration and Mediation Competition – CAMARB.

The personal data processing activities carried out by CAMARB are supported by legal provisions and recorded in specific documents or systems to control the risks of their processing, adopt measures to mitigate these risks and limit the internal and external circulation of personal data. These documents are available for consultation by the competent authorities.

Only people who have a strict need to access certain categories of personal data will have access to them, taking into account the role they play in CAMARB, reducing the accessed information to the minimum necessary through appropriate technical and organizational measures.

Physical and digital documents containing personal data will be stored for as long as their processing purposes subsist, in accordance with applicable legislation. Personal data, on any media, will be deleted securely and in the most irretrievable manner possible, immediately after all their purposes have been exhausted, provided that the safeguard period for compliance with legal obligations or exercise of rights has been reached, or in the event of a request from the respective holder requiring CAMARB to delete such personal data.

Any and all processing of personal data in which CAMARB identifies a likely impact on the fundamental rights and freedoms of the holders or the processing of sensitive personal data, under the terms of the Law, will be subject to an impact assessment on the protection of personal data in which the expected risks and appropriate measures for their mitigation, prevention or elimination will be raised.

CAMARB, with the assistance of the Data Protection Officer (“DPO”), will work on developing good practice standards to ensure the appropriate processing of personal data under the terms above.

6. COOKIES POLICY

When accessing the CAMARB website, the user’s computer receives so-called “cookies”. These text files are sources of some information collected and stored automatically by CAMARB. The CAMARB website uses cookies for the following purposes:

- “_gat_gtag_UA_140387405_1” necessary for the website to function (essential cookies), developed by Google Analytics and implemented by the website itself (first party). These are non-persistent cookies with an expiration of 54 seconds used to control the rate of requests that a browser or device makes to a web server in a given period. They are mainly used to manage server load and prevent abuse or overload;
- “_gid” necessary for website performance, developed by Google Analytics and implemented by the website itself (first party). These are non-persistent cookies that expire daily and are intended to generate unique identifiers for each page, in order to identify the most accessed pages and any technical problems on less accessed pages;
- “ga_zdxg7fw4sf” used to provide the website with additional functionalities, developed by Google Analytics and implemented by the website itself (first party). These are persistent cookies with monthly expiration and the purpose of temporarily saving the session in order to avoid reloading the website;
- “_ga” used to provide the website with additional functionalities, developed by Google Analytics and implemented by the website itself (first party). These are non-persistent cookies that expire monthly and are intended to generate random numbers for each user as a way of obtaining visitation and session data.

Except for cookies required for the website to function, cookies will only be saved on the device and will start collecting user data upon the data subject’s consent. There is no obligation to accept them and consent can be withdrawn at any time. In addition, the user’s browser can be configured to refuse to receive cookies and has functions to remove them at any time. The options and tools are available in the respective menu.

7. SHARING PERSONAL DATA WITH THIRD PARTIES

Personal data is shared, transferred or disclosed by CAMARB to third parties, as strictly necessary for the fulfillment of legitimate, specific, expressed and registered purposes by CAMARB and through the use of instruments that bind the third party to the Policy, and that establish inspection and audit rules by CAMARB, or third parties contracted by it.

Additionally, CAMARB adopts procedures to, as far as possible, ensure that it only shares personal data with third parties that adopt sufficient technical and administrative measures to guarantee adequate security and protection of personal data in accordance with the risks to which they are exposed, the safeguarding of the fundamental rights and freedoms of the respective holders and the accountability of the third party before CAMARB for the actions and omissions they carry out.

The sharing, transfer and disclosure of personal data to public authorities and government entities is limited to what is necessary to comply with legal and regulatory obligations, to comply with court orders and requests from competent authorities, and to defend or exercise the rights of CAMARB or third parties. Under these conditions, the legality and legitimacy of the order or obligation, the competence of the requester, the extent of the duty and the respective consequences are assessed before granting access to the data to the authorities or public bodies in question.

8. INFORMATION SECURITY

CAMARB adopts technical and organizational information security measures compatible with the state of the art and the assessed level of risk to guarantee the confidentiality, integrity, availability and resilience of its computer systems, databases, physical files and other information repositories, in order to prevent unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or dissemination of personal data.

CAMARB also maintains a security incident response plan that ensures rapid assessment, interruption, remediation and, when necessary, mitigation and repair of any damages caused by incidents. Records of security incidents will be kept, identifying the categories and personal data holders that may be affected, to enable immediate communication of such incidents to the competent authorities and to the respective holders in accordance with the law, with CAMARB undertaking to assist them in good faith in mitigating or repairing any damages actually suffered.

9. PERSONAL DATA HOLDER RIGHTS

CAMARB undertakes to adopt effective measures to guarantee all rights of personal data holders controlled by it, as specified by the General Personal Data Protection Law and other Brazilian laws and regulations applicable to privacy and personal data protection. The legal rights of personal data holders are:

- Confirmation of the existence of processing of your personal data by CAMARB and access to the data;
- Correction of incomplete, inaccurate or outdated personal data under CAMARB's control;
- Anonymization, blocking or deletion of unnecessary, excessive personal data or data processed by CAMARB in non-compliance with the provisions of this Law, as well as opposition to the processing of personal data by CAMARB in the same circumstances;
- Portability of data to another provider of services similar to those of CAMARB, upon express request and in compliance with CAMARB's business secrets, as this right may be regulated by the public authorities;

- Information on public and private entities with which CAMARB may share personal data;
- Information on the possibility of not providing consent for the processing of personal data by CAMARB and on the consequences of refusing consent, as well as the rights to withdraw such consent at any time and to delete the personal data processed based on it, such data being able to be kept by CAMARB for exclusive use in other lawful purposes that do not depend on consent or through anonymization; and
- Possibility of reviewing decisions that affect your interests and are taken by CAMARB solely based on automated processing of personal data.

CAMARB adopts updated standards, controls and processes that ensure the presentation of the appropriate information to the respective personal data holders, preferably at the time or in the context of the collection of such data or at the first opportunity after its receipt or obtaining, limited to cases in which it is not feasible or there is just cause for not delivering certain information to the holders. CAMARB also adopts updated standards, controls and processes that ensure the response to the rights of the holders without delay, within 15 (fifteen) days or in longer periods if provided for by law or in the applicable regulations for such response, free of charge and upon prior and adequate confirmation of the identity of the requesting holder.

Direct contact channels with the DPO will be maintained so that holders can exercise their rights, make complaints and requests, as well as send suggestions regarding CAMARB's practices.

10. RESPONSIBILITIES

Each employee, director and administrator, service provider and contractor of CAMARB is responsible for their own actions in relation to personal data processing activities, for compliance with this Policy and other applicable standards, as well as for enabling the proper performance of the work of the Personal Data Processing Officer and the Privacy Committee. Managers and individuals in supervisory positions are also responsible for ensuring good personal data processing practices by employees and third parties under their responsibility, in accordance with their duties. The Personal Data Protection Officer will only be liable for their actions when and if they act with intent or bad faith in their duties, and will be protected against personal liability for the executive actions and decisions of CAMARB.

11. PRIVACY AND DATA PROTECTION COMMITTEE

As defined by CAMARB's management, the CAMARB Information Security and Personal Data Protection Committee ("Committee") was established, with a three-year term and composed of the DPO, and representatives of CAMARB's administrative, financial, institutional and technology departments, in addition to its CEO and its Secretary-General. The initial term of the members will coincide with the term of the institution's board of directors, currently in progress.

12. PERSON RESPONSIBLE FOR PERSONAL DATA PROCESSING

CAMARB maintains as its Data Protection Officer an external employee or consultant with theoretical and practical knowledge of personal data protection and information security, whose duties will be:



- Advise CAMARB's decision-making bodies regarding communications, requests and summons from the National Data Protection Authority ("ANPD") and other authorities, requests and complaints from data subjects and security incidents, as well as other decisions that may have an impact on the privacy or protection of Personal Data of any person;
- Bring issues related to privacy and personal data protection to the Committee for discussion and approval, such as the need to evaluate, implement or review new standards, processes and policies;
- Receive and forward internal communications, requests and summons from the ANPD, as well as present a response to the ANPD, in accordance with the Policy for Responding to Requests from Personal Data Holders and Requests from Authorities;
- Receive and forward internally requests and complaints from personal data holders, as well as present a response from CAMARB, in accordance with the Policy for Responding to Requests from Personal Data Holders and Requests from Authorities;
- Clarify doubts of personal data holders regarding CAMARB's practices in relation to their Personal Data, in accordance with the Policy for Responding to Requests from Personal Data Holders and Requests from Authorities;
- Guide CAMARB's employees, contractors and outsourced workers regarding current policies and practices regarding privacy and protection of personal data;
- Coordinate security incident response teams and communicate them to the ANPD and affected data subjects on behalf of CAMARB when necessary, after approval by the Privacy Committee;
- Participate as a consultant in the review and establishment of CAMARB processes that may pose a relevant risk to the privacy or protection of personal data of any person (e.g. leaks, misuse of purpose and unlawful processing of personal data);
- Participate in the preparation and review of clauses, minutes and documents related to the sharing and transfer of personal data and CAMARB's privacy policies and notices for employees, consumers, intranet, website users, etc.;
- Control the frequency and coordinate reviews of personal data processing operation records and internal rules relating to privacy, personal data protection and information security;
- Coordinate implementation projects and audit processes and practices related to privacy, personal data protection and information security, taking its conclusions to the Privacy Committee;
- Participate in the selection and audit of service providers with potential relevant risk to the privacy and protection of Personal Data;



- Recommend and direct the carrying out of legitimate interest assessments, privacy impact assessments and other risk assessments related to the protection of personal data, discuss their results with the leaders of the affected projects and, if necessary, bring their conclusions to the decision-making bodies;
- Recommend and direct the preparation of reports on the impact on the protection of personal data and forward them to the ANPD after approval by the Privacy Committee;
- Participate in the establishment and review of processes and guidelines for minimizing Personal Data, eliminating personal data, “privacy by design” (i.e. ensuring the protection of personal data from the conception of a project/activity) and “privacy by default” (i.e. ensuring the highest level of privacy possible when there are alternatives or choices);
- Be informed of all new CAMARB activities and processes that have the potential to pose a significant risk to privacy and the protection of personal data; and
- Compose and direct the work of the Privacy team, as well as form and participate in working groups related to improvements in privacy management and mitigation of risks to privacy and protection of personal data.

All CAMARB employees, service providers and contractors will assist, as far as possible, the DPO in their duties and in ensuring CAMARB's governance and good privacy and personal data protection practices.

CAMARB's management undertakes to guarantee the independence of the DPO in carrying out their duties and direct access to all executive bodies of CAMARB so that the necessary decisions can be made regarding issues that impact the privacy and protection of personal data under CAMARB's control. The DPO will also be guaranteed access to all information about new activities and processes of CAMARB that have the potential to pose a significant risk to the privacy and protection of personal data and other information relevant to their duties, regardless of its confidentiality classification, provided that the applicable corporate policies and standards are observed to ensure its confidentiality and security.

The DPO will act with independence, impartiality, decorum and good faith, maintaining strict confidentiality on matters relating to discussions held within the Committee.

13. COMMUNICATION

CAMARB will maintain controls and processes that ensure prompt response to the rights of data subjects and requests from competent authorities regarding the protection of personal data. The following channels of direct contact with the DPO are available so that data subjects can exercise their rights, make complaints and requests, as well as send suggestions:

CAMARB – BUSINESS MEDIATION AND ARBITRATION CHAMBER – BRAZIL

Data Controller

Address: Rua Paraíba, 550, 9th floor, Funcionários, Belo Horizonte, MG

Email: tecnologia@camarb.com.br