

LUÍS FERNANDO DE LIMA CARVALHO  
ANDRÉ CARVALHO SICA  
ANDRÉ MUSZKAT  
OCTÁVIO SOUTO VIDIGAL FILHO  
THEREZA CRISTINA CARNEIRO

FLÁVIO DE HARO SANCHES  
GRACIEMA ALMEIDA  
JOÃO FERNANDO A. NASCIMENTO  
ANA CAROLINA MONGUILOD

CONSULTORES:  
PAULO PINOTTI  
JOANA BONTEMPO



## **PRIVACY AND DATA PROTECTION POLICY CARVALHO, SICA, MUSZKAT, VIDIGAL E CARNEIRO SOCIEDADE DE ADVOGADOS**

### **1. Privacy Statement**

This Privacy and Data Protection Policy ("Policy") of Carvalho, Sica, Muszkat, Vidigal e Carneiro Sociedade de Advogados ("CSMV" or "Firm") aims to provide transparency regarding the manner in which CSMV collects, uses, shares or otherwise processes the personal data to which it has access in the context of its activities as a law firm.

Thus, the Processing of personal data by CSMV may occur (i) when our website "www.csmv.com.br" ("Website") is accessed; (ii) during the process of registering candidates for job positions at CSMV (through our Website or e-mail); (iii) when our services are contracted (including personal data eventually shared during prospecting and work meetings); or (iv) when contracting service providers and business partners, sending related communications and fulfilling the obligations contracted.

This Policy reaffirms CSMV's commitment to ensuring the privacy and protection of personal data under its custody, in compliance with Law No. 13,709/18, the General Data Protection Law ("LGPD") and Law No. 12,965/2014 ("Marco Civil da Internet" [Internet Civil Milestone]), specifically in relation to our relationship channels through the internet, as well as the professional secrecy applicable to the relationship of CSMV and our members with clients, pursuant to the Code of Ethics and Discipline of the Brazilian Bar Association and Law No. 8,906/1994 ("Statute of the Legal Profession").

In case of any questions regarding this Policy, as well as for any requests, please contact our Personal Data Processing Officer, using any of the communication channels below:

Mailing:

CARVALHO, SICA, MUSZKAT, VIDIGAL E CARNEIRO SOCIEDADE DE ADVOGADOS

Av. Brig. Faria Lima, 1.461, Torre Sul, 9º andar, cjs. 91/94

São Paulo - SP

CEP-01452-002

c/o: Personal Data Controller

E-mail: dpo@csmv.com.br

## 2. Definitions

The following definitions have been used in the development of this Policy:

**Personal Data.** Information relating to an identified or identifiable individual, representing all data that identifies an individual or through which an individual can be identified. Personal Data can be a photo, full name, number of any of the personal identification document (CPF, ID, Voter's Card, Working Papers, etc.), information on nationality, profession, address, gender, geographical location, bank details, internet browsing data and others.

**Sensitive Personal Data.** Personal data concerning racial or ethnic origin, religious conviction, political opinion, membership of a trade union or religious, philosophical or political organization, data concerning health, sexuality, genetic or biometric data, when linked to a natural person. Sensitive Personal Data, in addition to identifying an individual, may also reveal other information associated with that individual. For the purposes of this Policy, Sensitive Personal Data is a specific type of Personal Data.

**Database.** Structured set of Personal Data, established in one or several locations, in electronic or physical support, comprising all locations (virtual or physical) in which CSMV stores Personal Data.

**Data Subject.** The natural person to whom the Personal Data being processed refers, thus considered any individual who has their data collected by CSMV, as well as any individual who has their Personal Data shared with our Office.

**Controller.** Natural person or legal entity, of public or private law, who is responsible for decisions regarding the processing of Personal Data, which, for the purposes of this Policy, will generally be CSMV, except in cases where CSMV acts solely as the Personal Data Operator.

**Operator.** Natural person or legal entity, of public or private law, who carries out the Processing of Personal Data on behalf of the Controller, which will correspond in some cases to CSMV.

**Processing.** Any operation carried out with Personal Data, such as those relating to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, deletion, evaluation or control of information, modification, communication, transfer, dissemination or extraction, within the scope of CSMV's activities as a law firm.

**Personal Data Processing Officer.** Person appointed by the Controller/Operator to act as a communication channel between the Controller/Operator, the Data Subjects, and the National Data Protection Authority ("ANPD").

**Consent.** Free, informed, and unequivocal manifestation by which the Data Subject agrees to the Processing of their Personal Data for a specific purpose.

**Security Incident.** Adverse event related to a breach in the security of Personal Data, such as unauthorized, accidental, or unlawful access resulting in the destruction, loss, alteration, leakage, improper publication of protected information or any form of inappropriate or unlawful data processing, which may result in a risk to the rights and freedoms of the Personal Data Subject.

## 3. Compliance with Data Processing Principles

CSMV processes Personal Data only for legitimate, specific, explicit, appropriate and necessary purposes for the provision of legal services, for institutional communications directed to its clients (when so authorized), for the recruitment and selection of its employees, and for the hiring of service providers and business partners, without the possibility of further processing in a manner incompatible with the above purposes.

CSMV guarantees the Data Subjects free access to their Personal Data, so that their consultation of such data is carried out in a facilitated manner, also ensuring for the Data Subjects transparency in the provision of accurate and complete information on the form and duration of the Processing of Personal Data.

CSMV uses all necessary technical and administrative measures to protect the Personal Data being Processed from (i) unauthorized access and (ii) accidental or unlawful destruction, loss, alteration, communication, or disclosure, and also adopts measures to prevent any damage to Data Subjects arising from the Processing of Personal Data, as well as to prevent any Processing of Personal Data for discriminatory, unlawful or abusive purposes.

#### 4. Data Collected, Purpose and Means of Collection

Below are examples of Personal Data that may be collected by CSMV within the scope of its activities, their purpose and means of collection:

Personal Data	Purposes	Means of Collection
<ul style="list-style-type: none"> <li>Name</li> <li>Personal Documents</li> <li>Email</li> <li>Address</li> <li>Phone</li> <li>Academic Data</li> <li>Professional Data</li> <li>Bank details</li> </ul>	<ul style="list-style-type: none"> <li>Provision of Legal Services</li> <li>Supplier Management</li> <li>Customer Management</li> <li>Institutional Communication*</li> <li>Website Monitoring</li> <li>Compliance with Legal Obligations</li> <li>IT Security</li> <li>Recruitment and Selection</li> </ul>	<ul style="list-style-type: none"> <li>Website Registration</li> <li>Conference Calls</li> <li>Virtual Meetings</li> <li>Face-to-face meetings</li> <li>Emails</li> <li>Physical Copies of Docs.</li> <li>Virtual Folders (Cloud)</li> </ul>

(\*) Consent for institutional communication actions will always be obtained prior to the start of the actions and customers are always offered an “opt-out”.

#### 5. Sensitive Personal Data Collected, Purpose and Means of Collection

Considering the legal activity performed by CSMV, the Firm will sometimes have consented access to certain Sensitive Personal Data of its clients, service providers and business partners. In this regard, below are some examples of Sensitive Personal Data that may be collected by CSMV within the scope of its activities, its purposes and its means of collection:

Sensitive Personal Data	Purposes	Means of Collection
<ul style="list-style-type: none"> <li>Blood Type</li> <li>Ethnic Origin</li> <li>Trade Union Membership</li> <li>Genetic Data</li> <li>Biometric Data</li> <li>Health Data</li> </ul>	<ul style="list-style-type: none"> <li>Provision of Legal Services</li> </ul>	<ul style="list-style-type: none"> <li>Conference Calls</li> <li>Virtual Meetings</li> <li>Face-to-face meetings</li> <li>Emails</li> <li>Physical Copies of Docs.</li> <li>Virtual Folders (Cloud)</li> </ul>

#### 6. Personal Data Generated by CSMV

As a product of the legal services provided to clients, or even in the context of applications for vacant positions at CSMV through our Website, CSMV may generate Personal Data, which will be collected and stored under the terms of this Policy.

Such data may be generated, for example, when preparing reports or opinions for clients, which consist of

the analysis and processing/organization of Personal Data, or in the context of candidate selection processes in which there are tests applied by automated tools through the internet.

In all cases, whenever there is Personal Data generated by CSMV, this Policy will apply in all its terms.

## 7. Legal Basis for the Collection and Processing of Personal Data

CSMV will always use one of the legal bases provided for in the LGPD for the Processing of Personal Data. Thus, among the possible legal bases, in the exercise of its activities CSMV may use:

*Consent* - the Processing of Personal Data will result from the express Consent of the Data Subject, obtained when contracting our services or when a candidate registers for vacant positions on our Website, always with the previously established and informed purpose of Processing. In the case of our clients, Consent is included in a specific clause in our proposals and contracts. For applicants, Consent will be obtained through *opt in checkboxes* upon completion of registration.

*Legal or Regulatory Obligation* - the Processing of Personal Data will arise from applicable law or regulation. In this case, the Data Subject will be informed by CSMV that his/her Personal Data will be processed based on this legal basis.

*Performance of Contract* - the Processing of Personal Data will derive from an obligation under a contract with CSMV where the Processing of Personal Data is part of the scope of the contract or of the preliminary procedures related to the contract with CSMV.

*Regular Exercise of Rights in Legal Proceedings* - the Processing of Personal Data will occur in the context of the exercise or defense of rights in legal proceedings, a typical activity of law firms.

## 8. Sharing Personal Data with Third Party Providers

CSMV may share Personal Data from our Database with third party suppliers, specifically in the cases provided for in this Policy and always within the applicable legal and regulatory limits. Below are the hypotheses for sharing Personal Data with third parties:

Shared Personal Data	Third Party Suppliers
Customer Personal Data - Database Generated Personal Data - Database Personal Data of Applicants - Database	Legal Services - Correspondents Services - Paralegal Services - Accounting Services - Experts and Technical Assistants Services - IT Support Services - IT Security Services - IT Maintenance Services - IT Storage Services - IT Customized Solutions Services - IT Document Management Services - IT Printing Systems Services - IT Website Hosting Services - IT Recruitment Services - Recruitment Services - Physical Archive Services - Institutional Communications *

(\*) Consent for institutional communications will always be obtained prior to the actions and clients are always offered an “opt-out”.

In any case of sharing Personal Data with third parties, the third parties will be informed that such Personal Data shall always be used in accordance with this Policy.

## **9. Sharing of Personal Data with Public Authorities**

CSMV may share Personal Data stored in our Database with Public Authorities in certain specific situations, when such sharing arises from a legal or regulatory obligation, or when the sharing of Personal Data is necessary for the (i) preparation of impact reports on the protection of Personal Data; (ii) conducting investigations; (iii) compliance with court orders; and (iv) to avoid and/or take measures to prevent the practice of suspicious or illegal activities (always respecting our duty of professional secrecy under the Statute of the Legal Profession).

In these cases, the order or directive to share Personal Data will come directly from the Government entity.

## **10. Data Storage and Security**

Personal Data collected by CSMV may be stored (i) physically at CSMV's office; (ii) in physical media in the contracted spaces of third party providers for document archiving; (iii) in electronic media on local servers located at CSMV's office; or (iv) in electronic form on virtual servers (cloud) contracted from third party providers of virtual environments.

In any case of storage, CSMV hereby represents and warrants to its clients and suppliers, and to candidates who share their Personal Data in selection processes, that adequate physical and virtual security measures are adopted to preserve the confidentiality, security and integrity of the Personal Data collected, as well as to prevent any attack, unauthorized access or disclosure, tampering, loss and / or any other data security incidents.

In this context, we employ technological security solutions in our Database, including firewalls, inspection, scanning and filtering of internet browsing content and emails, antivirus software, malware protection, intrusion and threat detection and prevention, and application control.

With regard to access to Personal Data, we restrict physical and virtual access to the smallest possible number of staff and third-party professionals engaged to handle a particular case or to provide a particular legal service.

It is important to stress that there are currently no technological means to guarantee the impenetrability of systems. While we believe that the measures set forth above are sufficient to preserve the Personal Data collected, we cannot provide absolute assurances that our Database will not be hacked and that, in the event of a hack, Personal Data will not be accessed, disclosed, altered, or destroyed.

## **11. Personal Data Retention Periods**

Under the LGPD there is no specific minimum or maximum period for retention of Personal Data by the Controller. The legal rules only establish a "*processing period*" at the end of which the Personal Data collected may be kept by the Controller for specific purposes.

In view of the nature of CSMV as a legal services provider, we understand that the Personal Data we collect should be kept in our Database for as long as necessary to fulfill our professional, legal and/or regulatory obligations.

In this regard, below are the types of Data Subjects whose Personal Data we collect, as well as the legal storage periods, start date and legal basis:

Subject	Withholding period	Start Date	Legal Basis**
Customers (Litigation)	5 years	Termination of Services	Art. 206, §5, II CC
		Termination of Contract	Art. 202, I CC
		Termination of Mandate	Art. 240, §1 CPC
Customers (Advisory)	5 years	Termination of Services	Art. 206, §5, II CC
		Termination of Contract	Art. 202, I CC
		Termination of Mandate	Art. 240, §1 CPC
Customers (Institutional Communications)	1 year*	Opt-out	Art. 6, III LGPD Art. 15, II LGPD
Suppliers	10 years	Termination of Contract	Art. 205 CC
Suppliers (Consumption)	5 years	Termination of Contract	Art. 27 CDC
Applicants (HR)	1 year	Website Registration	Art. 6, III LGPD Art. 15, II LGPD

(\*) There is no specific deadline in the LGPD, 1 (one) year was considered due to the nature of the data collected for institutional communication as registration data (name, title, company, email, telephone, contact address).

(\*\*) CC - Law 10.406/2022 - Civil Code.  
CPC - Law 13.105/2015 - Civil Procedures Code.  
CDC - Law 8.078/1990 - Consumer Protection Code.

## 12. Rights of Subjects

Data Subjects have rights guaranteed by the LGPD in relation to their Personal Data collected, which are listed below:

*Confirmation of Processing* - the right to request confirmation of whether or not Personal Data Processing activities are taking place. The following information about the Personal Data Processing activities may be requested by Data Subjects: (i) which Personal Data are being processed; (ii) the origin of the Personal Data processed; and (iii) the purpose of the Personal Data Processing activities.

*Access* - the right to request access to Personal Data in our Database and may request a full statement about the Processing activities and additional information about the activities carried out.

*Correction* - right to request correction, amendment or update of Personal Data in our Database when it is incorrect or incomplete.

*Anonymization, Blocking or Deletion of Unnecessary Data* - anonymization, blocking or deletion of unnecessary data in our Database, excessive or processed in noncompliance with the provisions of the LGPD.

*Deletion of Data Processed Without Consent and Without a Legitimate Basis* - right to request the deletion of Personal Data stored without Consent and without a legitimate legal basis for its use.

*Portability* - the right to request that Personal Data collected be transferred to another service provider.

*Revocation of Consent* - revocation of Consent to Processing of Personal Data at any time.

*Opposition to Processing* - right to object to the Processing of Personal Data carried out, in case of noncompliance with the provisions of the LGPD or for reasons related to your particular situation.

The rights of the Subjects may be exercised at any time, free of charge by request via e-mail directed to our Personal Data Processing Officer, at [dpo@csmv.com.br](mailto:dpo@csmv.com.br).

### **13. Security Incident Response Policy**

CSMV maintains a strict damage reduction policy in the event of a Security Incident with Personal Data and adopts tools and techniques to mitigate the risks and effects of security incidents, such as strong passwords, encryption, minimization of collected data, constant updating of applications, technical security tools, among others.

However, if verified the occurrence of a Security Incident with Personal Data, CSMV will internally assess the incident, within the first twenty-four (24) hours of its occurrence, with the aim of obtaining information on the nature, category and quantity of Data Subjects and Personal Data affected, as well as the concrete and probable consequences of the incident for the Personal Data Subjects and for CSMV, ensuring the preservation of all evidence of the Security Incident.

In the event of a confirmed breach of the security of Personal Data, CSMV will notify the affected Personal Data Subject and ANPD within forty-eight (48) hours of its occurrence, without prejudice to notification to third parties, such as the police, regulatory authorities, insurers or business partners.

Nevertheless, CSMV will immediately adopt effective measures for the containment, eradication and recovery of Personal Data and will follow all guidance that will be provided by the national authority in order to mitigate the effects of the Security Incident. The affected Personal Data Subject will be guided by CSMV and duly informed about all the steps of the procedure related to the occurrence of the Security Incident.

### **14. Changes to this Privacy and Data Protection Policy**

CSMV reserves the right to amend all or part of this Policy at any time (subject always to the applicable law), by entering your last update date.

We recommend that you consult this Policy periodically to check for any changes. The use of the Website or the provision of Personal Data to CSMV by any other means presupposes the agreement of the Data Subject to this Privacy and Data Protection Policy.

\*\*\*