Privacy Series

5 THE PROCESSING OF PERSONAL DATA AND THE PRINCIPLES ESTABLISHED BY THE LGPD

VEIRANO ADVOGADOS



This is the fourth chapter of the Data Privacy Series. Click Here to access the chap. 4.



In 2023, the Brazilian General Data Protection Law (Law No. 13,709/2018 or "LGPD") celebrates 5 years of its publication - now also including the possibility of the application of administrative sanctions by the ANPD since August 2021. The Brazilian National Data Protection Authority ("ANPD") has been active in fostering discussions and disseminating concepts, practices and principles of privacy and data protection, through the publication of several materials for awareness and regulation of the LGPD since its creation.

Veirano Advogados has been following and participating in discussions regarding these issues. For this reason, our Data Protection & Privacy team has prepared the **Privacy Series**, in which we will periodically publish on different topics related to privacy, bringing not only LGPD concepts, but also ANPD publications on the subject, relevant considerations, among other contents



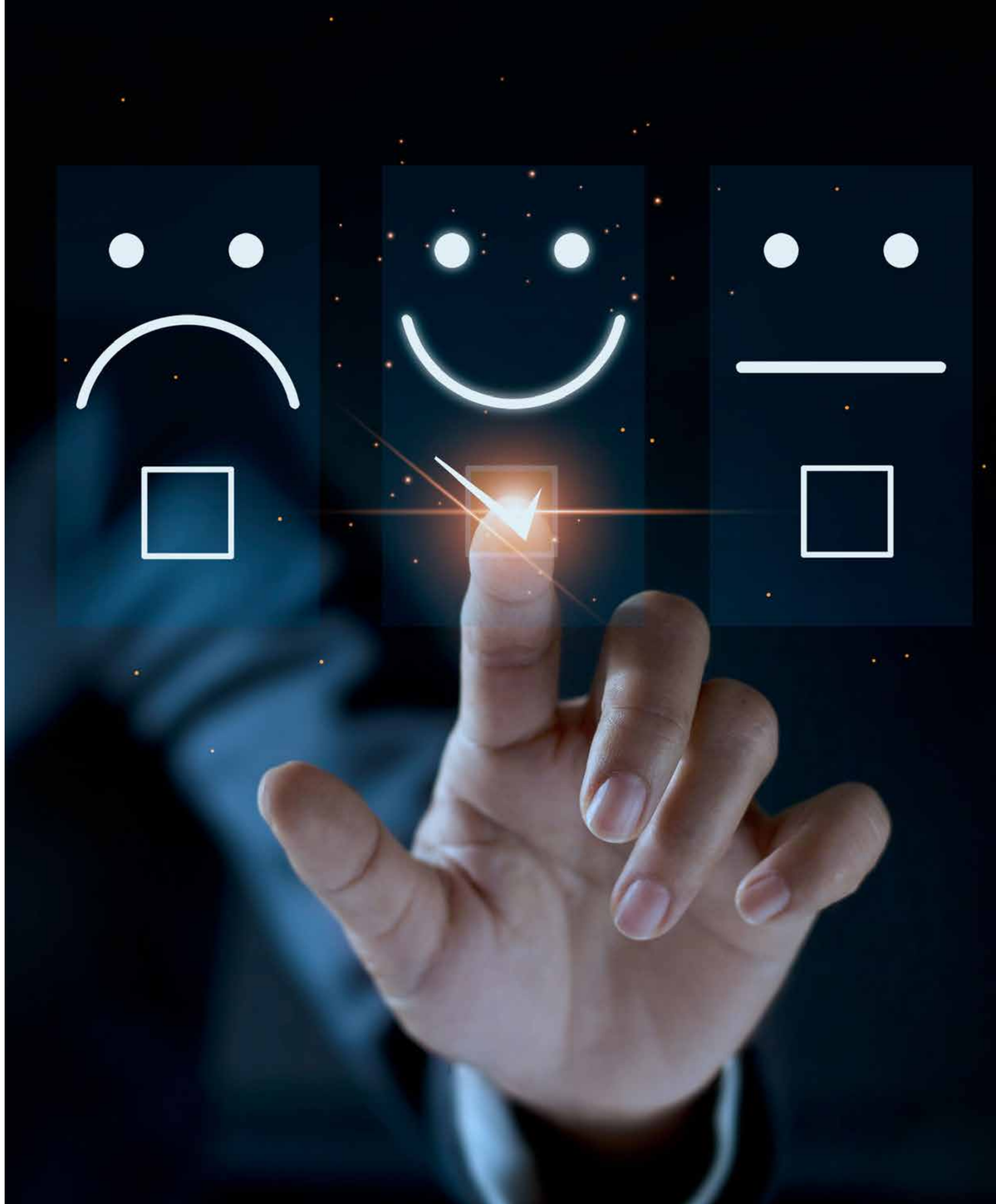
Processing of Personal Data

In general terms, Processing involves everything that Processing Agents can do with the Data Subject's Personal Data.

Article 5, item X of the LGPD defines "Processing" as *any operation carried out with personal data, such as those referring to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation or control of information, modification, communication, transfer, dissemination, or extraction*. Find below the meaning of each of these actions:

- **Access** - ability to communicate with a device, storage medium, network unit, memory, registry, file, etc., in order to receive, provide, or delete Personal Data.
- **Storage** - action or result of maintaining or conserving Personal Data in a physical or digital repository.
- **Archiving** - act or effect of keeping registered Personal Data, even if they have already expired.
- **Valuation** - act or effect of calculating value on one or more Personal Data.
- **Classification** - way of ordering Personal Data according to some established criteria.
- **Collection** - collection of Personal Data for a specific purpose.
- **Communication** – transmit information relevant to action policies on Personal Data.
- **Control** - action or power to regulate, determine or monitor actions on Personal Data.
- **Diffusion** - act or effect of disclosure, propagation, or multiplication of Personal Data.

- **Distribution** - act or effect of disposing of Personal Data according to some established criteria.
- **Deletion** - act or effect of deleting or destroying Personal Data from the repository.
- **Extraction** - act of copying or removing Personal Data from the repository in which they were found.
- **Modification** - act or effect of alteration of Personal Data.
- **Processing** - act or effect of processing Personal Data.
- **Production** - creation of goods and services from the Processing of Personal Data.
- **Reception** - act of receiving Personal Data at the end of the transmission.
- **Reproduction** - copy of pre-existing Personal Data obtained through any process.
- **Transfer** - moving Personal Data from one storage area to another, or to a third party.
- **Transmission** - movement of Personal Data between two points by means of electrical, electronic, telegraphic, telephone, radioelectric, pneumatic devices etc.
- **Use** - act or effect of using Personal Data.



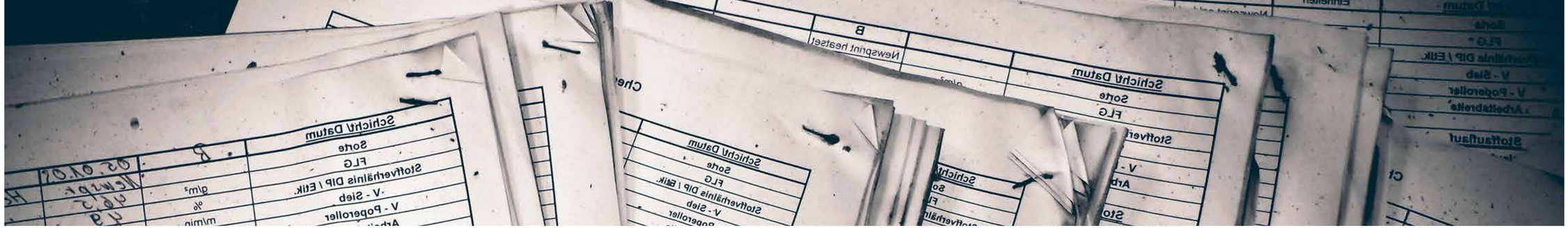


Legal Bases for the Processing of Personal Data

In addition to the need to observe the application of the principles set forth by the LGPD (see **LGPD Principles**, below), any and all Processing of Personal Data must necessarily be based on at least one of the Processing hypotheses established in the LGPD, also known as "legal bases".

Personal Data [Non-Sensitive]

Legal basis	Description
Consent	For the Consent to be applicable, it must be freely, informed, unequivocal, and specific issued by the Data Subject. *Example: Sending promotional emails with news about the company and available products.*
Legitimate interest	Applicable when necessary to serve the legitimate interests of the Controller or third parties - such as to promote activities of the Controller or to provide services that benefit the Data Subject. The application of legitimate interest as a legal basis must always observe and respect the legitimate expectations and fundamental rights and freedoms of the Data Subject. *Example: Data analysis for the purpose of improving the tools and/or products made available by the company.*
Compliance with legal and/or regulatory obligations	There are several legal and/or regulatory obligations which can only be complied with regularly by the Processing Agents if Personal Data are processed. To this end, the LGPD established a specific legal basis that can support all Processing strictly necessary to fulfill these obligations. *Example: Granting of benefits established by labor legislation, such as bonus.*
Credit protection, under the terms of the Brazilian Consumer Protection Code ("CDC")	It is worth remembering that, even with the adoption of this legal hypothesis, Processing Agents must observe the application of the principles of the LGPD, which include the **Principle of Non-Discrimination** and the **Principle of Necessity**. *Example: Credit analysis carried out by financial institutions to grant loans to the Data Subject.*



Execution of agreement (or preliminary procedures relating to an agreement)	The execution of an agreement with the Data Subject also legitimizes the Processing of his Personal Data. However, only the Personal Data essential for the establishment of the agreement and/or the provision of services may be processed based on this legal hypothesis. *Example: Delivery of a product purchased by the Data Subject.*
Regular exercise of rights in judicial, arbitral, or administrative proceedings	The hypothesis of Processing for the regular exercise of rights aims to ensure that individuals have full access to justice, legitimizing the Processing of Personal Data to ensure full defense and due process of law. It is important to note that the retention periods established in the applicable legislation must be taken into account. *Example: Defense of the company in labor and/or consumer lawsuits.*
Health protection	Personal Data may be Processed by health professionals, health services or health authorities, during the performance of medical procedures. *Example: Conducting tests in medical laboratories.*

Public policies	The Public Administration may process Personal Data to ensure the constitutional rights of the Data Subject. *Example: The Ministry of Health and/or other health departments in Brazilian states need to verify information about the vaccinated population to create a vaccine distribution policy.*
Protection of life or physical integrity	Personal Data may be Processed to ensure the protection of life or physical integrity of the Data Subject and/or third parties. *Example: Warn family members about the occurrence of an accident during working hours (emergency contact).*
Performance of studies by research bodies	Anonymization is not a requirement for the application of this Processing hypothesis, however, the law determines that, whenever possible, Personal Data must be anonymized. *Example: Carrying out statistical studies by the Brazilian Institute of Geography and Statistics ("IBGE").*



Legal Bases for the Processing of Sensitive Personal Data

Within the genus "**Personal Data**" is the species "Sensitive Personal Data" (for complete definitions, see item 1.5 of Chapter 2 – Why Should I Be Concerned with the LGPD?)

In other words, Sensitive Personal Data is Personal Data relating to:

- Racial origin
- Ethnic origin
- Religious conviction
- Political opinion
- Union membership
- Affiliation to religious, philosophical, or political organizations
- Health
- Sex life
- Genetic data
- Biometric data

In view of its potential discriminatory nature, Sensitive Personal Data have specific legal bases and, therefore, not all the hypotheses listed in the table above have the power to legitimize the Processing of Sensitive Personal Data.

Sensitive Personal Data

Legal basis	Description
Consent	Consent also has the power to legitimize the Processing of Sensitive Personal Data of individuals, and all specific requirements and guidelines related to this legal basis must be complied with. *Example: Availability of inclusive vacancies for candidates who identify as LGBTQIAP+.*

Compliance with legal and/or regulatory obligations	Sometimes, in order to comply with a legal obligation, it will be necessary to Process Sensitive Personal Data, such as health data and data relating to trade union membership. *Example: Fulfillment of obligations relating to the Brazilian Quota Law, applicable to vacancies occupied by Persons with Disabilities ("PwD").*
Performance of studies by research bodies	It may be necessary for research agencies to include in the scope of their studies Sensitive Personal Data, as is the case of the collection and processing, by the Brazilian Institute of Geography and Statistics ("IBGE"), of Personal Data related to health, religion, sexuality of the Data Subject, among others.
Regular exercise of rights **(including in agreements and in judicial, administrative, and arbitration proceedings)**	The regular exercise of rights applies to the Processing of Personal Data and Sensitive Personal Data, however, this legal basis also encompasses the exercise of rights established in agreements, which does not occur in the case of the Processing of Non-Sensitive Personal Data, given the existence of a specific legal basis for this. *Example: Storage of data related to the health and disability condition of PWD employees, to ensure the defense of the company's interests in any labor lawsuits.*
Health protection	If a Data Subject goes to a medical laboratory to perform a surgical procedure, the providers of said service also have legitimacy to process the patient's Sensitive Personal Data, such as pre-existing diseases, use of medicines, genetic data, among others.
Public policies	The Public Administration may process Sensitive Personal Data to manage public policies and ensure compliance with the constitutional rights of the Data Subject. *Example: The Brazilian Social Security Institute ("INSS") may process Sensitive Personal Data, related to physical disabilities of the Data Subjects, to ensure the receipt of social security benefits by the insured.*
Protection of life or physical integrity	If any of the employees of a company suffer an accident during working hours, for example, the company may need their Sensitive Personal Data, such as blood type, existence of diseases, and/or disabilities etc.
Fraud prevention and security guarantee for data subjects	The legal basis for ensuring fraud prevention and the security of the Data Subject applies only to the Processing of Sensitive Personal Data in the processes of identification and authentication of registration in electronic systems. *Example: Collection of biometric data for access control purposes in concierges.*

In short...

	Personal data	Sensitive Personal Data
Fulfillment of a legal and/or regulatory obligation	☑	☑
Consent	☑	☑
Health protection	☑	☑
Studies performed by research institutes	☑	☑
Regular exercise of rights (*)	☑	☑
Life protection or preserving physical integrity	☑	☑
Execution of public policies	☑	☑
Assurance of fraud prevention and security	☒	☑
Credit protection	☑	☒
Legitimate interest	☑	☒
Execution of agreement	☑	☒

It is worth mentioning that, although there may be disagreements about which legal basis should be applied, there should be no prevalence or hierarchy of importance between them, and the analysis of the concrete case should be used in order to define the applicable legal basis.

BE AWARE: Considering the various questions and controversies about the application of the legal bases of Consent and Legitimate Interest, we will detail in **Chapter 6 - Consent** and **Chapter 7 - Legitimate Interest** of our series the specificities and main guidelines on these legal hypotheses, including the issue of the Processing of Personal Data of children and adolescents.



LGPD PRINCIPLES

Regardless of the applicable legal basis, in any and all activities involving the Processing of Personal Data, the Processing Agents shall act in line with good faith and observe the principles brought forth in Article 6 of the LGPD, described below:

Principle	Description
Principle of Purpose	The Processing of Personal Data may only take place for legitimate, specific, explicit, and informed purpose, which must be previously informed to the Data Subject. Moreover, this principle prohibits the possibility of further Processing in a manner incompatible with the original purposes.
Principle of Adequacy	The activity carried out with Personal Data must be compatible with the purpose informed to the Data Subject.
Principle of Necessity	The Processing must involve the minimum of Personal Data necessary for the accomplishment of the purposes (see **Principle of Purpose**). Thus, the Processing activity should only cover pertinent, proportionate, and not excessive Personal Data.
Principle of Free Access	The Data Subject has the right to make facilitated and free of charges consultations regarding the form and duration of the Processing of his Personal Data.
Principle of Data Quality	The Personal Data of the Data Subject must be kept up-to-date, clear, and accurate.
Principle of Transparency	The Data Subject must have easy access to clear and accurate information about the Processing of his Personal Data and the respective Processing Agents involved.
Principle of Security	The Processing Agents must use technical and administrative measures capable of protecting the Personal Data from unauthorized access and from accidental or unlawful situations of destruction, loss, alteration, communication, or dissemination.
Principle of Prevention	The Processing Agents must adopt measures, such as periodic audits and training, to prevent the occurrence of damage to Personal Data.
Principle of Non-Discrimination	It is forbidden to carry out Processing for discriminatory, unlawful, or abusive purposes.
Principle of Accountability	The Processing Agents must be able to prove the adoption of effective measures in compliance with the rules of protection of Personal Data.

ATTENTION: The idea that Processing Agents should only inform the Data Subject about the Processing when it is necessary to obtain their Consent is **incorrect**. Given that transparency is a principle applied to all Processing activity, it is imperative that the Data Subject has access to clear and accurate information about the use of his Personal Data, even if the Processing is not based on Consent (see **Principle of Transparency**).



The Veirano Experience has a holistic, multidisciplinary, and business-oriented approach. In order to cover all the needs related to Compliance with LGPD, our Data Protection & Privacy team have developed several project formats, which comprise different scopes of work and meet specific demands of each client, whether national or international:

1. Full Compliance

With the performance of a multidisciplinary team, this project is aimed for clients whose goal is to identify and assess all ongoing processing activities within the company and based on that, identify vulnerabilities and structure an action plan for the creation of an effective privacy and data protection program based on legal, procedural, information security, and corporate governance pillars.

2. DPO as a Service

In this model, we take on the role of Data Protection Officer (DPO) on behalf of the client. To this end, we allocate a professional to perform the activities of managing and monitoring the client's data protection and privacy program.

3. M&A Legal Assistance

Designed to assist clients in the legal due diligence of merger and acquisition transactions, in order to identify relevant legal issues (red flags) and mitigate potential risks related to data protection and personal data security issues of the target company.

4. LGPD Pocket

A “pocket” advisory service for the adequacy of the activities and/or products developed by the company, regardless of its size or field of business, considering a reduced number of deliverables.

5. LGPD on Demand

LGPD On Demand is aimed at organizations that wish to have multidisciplinary advisory service on legal, information security, and corporate governance issues, with specific and timely action related to the protection of personal data.

6. LGPD Legal Helpdesk

The Helpdesk is designed to assist clients with LGPD legal consultations and demands within a monthly package of hours, either before, during, or after the initial compliance process.

7. Task Force For Security Incident Assessment And Reporting (VA Cybersecurity)

Specific and multidisciplinary legal advice in aspects related to the suspicion or occurrence of a security incident, in accordance with the most updated instructions from the ANPD and other applicable laws and regulations.

8. Representation in Administrative and Judicial Actions Involving Data Protection

Representation of clients in any administrative and/or judicial actions or potential actions involving data protection.

9. Analysis of Administrative and Judicial Decisions on Data Protection Matters

Periodic monitoring of decisions rendered in judicial and administrative proceedings involving the company or not, in order to present the authorities’ understanding and the impacts for the company or economic sector to the client in a summarized format.

10. Development and Updating of a Data Protection Impact Report

The ANPD may request from the controller to prepare a personal data protection impact report ("RIPD" or DPIA). Our team has expertise on the subject and can assist the company with the preparation and updating of the RIPD.

11. Development of Workshops

Development and application of training about the main concepts related to privacy and data protection to train its employees.

12. Playbook for Negotiating Commercial Contracts

Creation of playbooks for the negotiation of commercial contracts, to facilitate and speed up internal processes of commercial, technical, and legal teams.

13. Handbook to Reply the Data Subjetcs

Development of materials to assist the companies in prompt answering the data subjects' requests, as well as in the procedure to be followed by the company when answering the data subject, according to the business model developed by the company.

14. International Data Transfer

We help clients to understand the context of the international transfer, adapt it to the applicable legal basis, assess data localization requirements, add contracts, draft and review intra-group data sharing agreements, and generally respond to queries related to the harmonization of foreign with Brazilian regulations.

15. Privacy and Data Protection Auditing

We conduct audits to evaluate the company's level of maturity, presenting recommendations for risk mitigation.

16. Development and Review of Documents Pursuant to the Financial Sector

Our team has expertise in drafting security policies in accordance with the Central Bank's specific information security regulations, and in answering questions on the subject.

We are at your disposal in case of any questions or in the need of any additional information.



FÁBIO PEREIRA
+55 11 2313 5906
fabio.pereira@veirano.com.br



CINTIA ANDRADE
+55 21 3824 4655
cintia.andrade@veirano.com.br



DENISE LOUZANO
+55 11 2313 5912
denise.louzano@veirano.com.br



ISABEL HERING
+55 11 2313 5726
isabel.hering@veirano.com.br



PAOLA LORENZETTI
+55 11 99976 8480
paola.lorenzetti@veirano.com.br

This material was last updated on March 29, 2023 and published on March 30, 2023.
For more updated information please contact us.