Privacy Series

2 WHY SHOULD I BE CONCERNED WITH THE LGPD?

VEIRANO ADVOGADOS



This is the second chapter of the Data Privacy Series. Click Here to access the chap. 1.



In 2023, the Brazilian General Data Protection Law (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 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.



The statement that we live in a data-driven society is no longer new. As a result, and in order for companies to use Personal Data and remain competitive in the marketplace, **avoiding Personal Data breaches**, fines, and potential reputational damage, as well maintaining compliance with privacy and data protection rules has become part of corporate discussions globally.

The Covid-19 pandemic played an essential role in such process, by evidencing the importance of **cyber security** and **data protection**, especially due to the need for sharing and disclosing health data, such as alternatives to combat the pandemic.

The Brazilian General Data Protection Law (Law No. 13.709/2018 or "LGPD") is a part of this global context, impacting all economic sectors and companies, of any size, yet maintaining its own particularities. Therefore, although it was inspired by the European Data Protection Regulation ("Resolution no. 2016/279 or "GDPR"), compliance with GDPR does not guarantee compliance with the LGPD.

COMPLIANCE WITH THE GDPR DOES NOT ENSURE COMPLIANCE WITH THE LGPD.

In fact, the LGPD is a legislation that protects the Data Subject and classifies the Personal Data Processing as a "risk operation", including administrative responsibility for the Processing Agents. For these reasons, it is of utmost importance that companies that develop activities within the scope of applicability of LGPD are in compliance with the law, which includes maintaining technical and administrative measures capable of ensuring the security of Personal Data processed, deleting Personal Data when there is no legal basis authorizing the Processing, complying with the rights of Data Subjects, providing clear, accurate and easily accessible information about the Processing performed by the company, among other legal requirements.

It is worth mentioning that, especially in relation to the Processing of consumer data, companies shall be even more careful, considering that, in addition to LGPD, they must comply with the provisions of the **Consumer Protection Code** (CDC) and all other regulations of the National Consumer Protection System. Moreover, although the enforcement of sanctions set forth in the **LGPD** is **ANPD's** competence, consumer regulatory authorities (Senacon, PROCONs, Public Prosecutor's Office, etc.) are authorized to and have been inspecting companies on the basis of the CDC, including the application of fines for non-compliance with the Consumer Protection Code.

1. WHAT DO I NEED TO KNOW ABOUT THE LGPD?

1.1. What is LGPD?

LGPD is the regulatory framework for Personal Data protection in Brazil, which regulates the Processing of transactions involving Personal Data, whether through digital means or otherwise, within and outside of the internet.

The LGPD was largely inspired by the **GDPR**, addressing, as does the GDPR, the rights of Data Subjects, the obligations of Data Controllers, the responsibilities of the Data Protection Officer, the parameters for data security, the requirements for the international transfer of data, and the instructions regarding the actions of the National Data Protection Authority, among other topics.

With the LGPD, Brazil is now included in the group of Latin American countries that have a general data protection law, alongside Argentina, Mexico, Uruguay, Colombia, Chile, Panama and Peru.



1.2. Overview of Privacy in Brazil

The enactment of the LGPD, on September 18, 2020, has caused, and will continue to cause, a significant impact on how companies use Personal Data in the course of business. Despite the common understanding, the LGPD is not the sole legislation that addresses how Personal Data must be processed in Brazil.

The Brazilian legal panorama on privacy and data protection is complex and includes specific sector laws, i.e., the LGPD must be understood and interpreted as part of a system and not as an isolated law.

> **"The LGPD must be understood and construed as part of a system and not as an isolated law."**

In view of that, when Processing data in Brazil, it is necessary to ensure compliance with various laws, which may apply to all companies, as is the case of the Internet Act, or to companies within specific industries.

Brazilian Constitution ("CF")	establishes the right to privacy as a fundamental right and determines the protection of personal life, honor, image and confidentiality of personal information and communications. in addition, the National Congress recently enacted Constitutional Amendment no. 115/2022, including the protection of Personal Data among the fundamental rights and guarantees provided for in the Brazilian Constitution.
Consumer Protection Code (Law No. 8.078/1990)	governs consumers' data privacy and protection to ensure that consumers have full access to their information (article 43).
Wiretap Act (Law No. 9.296/1996)	determines that the interception of communications is subject to legal authorization for purposes of criminal investigation.
Habeas Data Law (Law No. 9.507/1997)	provides for the right of individuals to access or change personal information stored in federal databases.
Telecommunication Act (Law No. 9.472/1997)	governs the consumers' rights to confidentiality regarding the telecommunication services.
Bank Secrecy Law (Supplementary Law No. 105/2001)	provides for the confidentiality of financial data, which disclosure is solely authorized upon legal order issued for purposes of investigation of unlawful acts.
Civil Code (Law No. 10.406/2002)	sets forth that the personal life of individuals shall not be violated, as an inherent "personality right."
Positive Registry Law (Law No. 12.414/2011)	creates a list of "good payers" and provides for that Personal Data can be used and disclosed for credit risk analysis not subject to prior approval, except for sensitive data or data deemed unnecessary or incompatible with the respective purpose.
Access to Information Law) (Law No. 12,527/2011 and Decree n°7,724/2012)	governs the constitutional right of citizens to access public information, applicable to states, Distrito Federal and municipalities.

Internet Civil Act (Law No. 12,965/2014 and Decree No. 8,771/2016)	governs the Processing of Personal Data collected on the Internet, specifically by connection and internet service providers.
Resolution No. 4.474/2016 of National Monetary Council	governs the scanning of documents.
Resolution CMN No. 4.658/2018 of Brazilian Central Bank	governs the obligations applicable to the financial institutions to implement cyber security policies and the requirements to be complied by these institutions in the contracting of data storage, data Processing and cloud storage services.
Medical Conduct Code (Resolution No. 2.217/2018 of the Federal Medicine Council)	protects the confidentiality of information of patients and medical records, subject to limited exceptions, and governs the use of computer systems to handle and retain such data, authorizing the scanning and electronic storage of medical records.
Resolution No. 4.753/2019 of National Monetary Council	provides for the opening, maintenance and closing of deposit accounts.
Legal Framework for Artificial Intelligence (PL No. 21/2020)	defines the provisions, principles and guidelines for development and application of Artificial Intelligence (AI) in Brazil, in addition to other provisions. The proposal defines that the use of the AI shall be based on respect to data protection. The AI agents shall comply with several obligations, such as ensuring that the data is used in conformity with the LGPD.
Resolution CMN No. 4.893/2021 of Brazilian Central Bank	provides for the cyber security policy and requirements for the hiring of data Processing storage and cloud services to be complied by the institutions authorized to operate by the Central Bank of Brazil. The Resolution became effective on July 1st, 2021 and set forth the amendment to the existing regulations and revoked Resolutions No. 4.658/2018 and 4.752/2019. However, the new Resolution does not change the provisions set forth in Resolution No. 4.658/2018, considering that the main difference in the new Resolution refers to crisis management.

Resolution CMN No. 85/2021 of Brazilian Central Bank	provides for the cyber security policy and requirements for the hiring of data processing, storage and cloud services to be complied by the payment institutions authorized to operate by the Central Bank of Brazil. The Resolution became effective on August 1st, 2021, and revoked articles 1 to 26 of Circular Letter No. 3.909/2018 and Circular Letter No. 3.969/2019. Contrary to CMN Resolution No. 4.893/2021 above, Resolution No. 85/2021 is applicable to payment institutions only.
Law No. 14.289/2022	provides for confidentiality protection of individuals suffering from HIV, HBC,HCV, leprosy and tuberculosis.

1.3. LGPD's entry into force

Published on August 14, 2018, the original wording of LGPD set forth that the companies should implement the necessary measures to comply with LGPD within 24 months before the actual entry into force of the text. However, due to the pandemic, the House of Deputies postponed the authority (ANPD) to impose administrative sanctions through August 1st, 2021. The President also enacted Provisional Measure No. 959/2020 to postpone the effectiveness of other articles of the LGPD through May 3rd, 2021, which was not approved by the Legislative power. Therefore, **the LGPD became effective on September 18, 2020**.

1.4. To whom does the LGPD apply?

LGPD is applicable to any agent (individual, legal entity, or public body) that processes Personal Data – and the term "Processing" is defined in the Law as "any Personal Data operation". To learn more about the activities covered by Processing, go to **General Definitions**.

The simple access to an employee's information, or even the storage of any agreement that includes Personal Data of a witness, the transfer of supplier's information to the company's database, classification of identifiable consumers' profiles, exclusion of any personal information no longer necessary, as well as any other type of Personal Data processing are operations designated as data Processing under the Brazilian Law.

Finally, the Brazilian Law is based on the principle of extraterritoriality in its application. As a result, the new rules apply not only to companies established in Brazil, but also to entities that process or collect data within the Brazilian territory and to companies that aim to offer or supply goods and services to individuals located in Brazil.

1.5. General Definitions

Processing Agents: the Controller and the Processor, defined below.

Small-Sized Processing Agents: micro-enterprises small-sized companies, startups, private legal entities, including non-profit legal entities, under the terms of the legislation in force, as well as individuals and entities without legal personality that perform Personal Data Processing, taking over obligations commonly applicable to Controllers or Processors, under the ANPD regulation. For further information on small-sized Processing agents, click here.

Anonymization: the use of reasonable technical means available at the time of Processing, by means of which a data may no longer be directly or indirectly associated to an individual. The LGPD does not apply to the anonymous data; however, the definition of Personal Data includes also identifiable data and, therefore, the individual may be identified based on a combination of information and association with identifying factors.

Data Controller: individual or legal entity, governed by public or private law, in charge of making decisions about the Processing of Personal Data. Among these decisions are the instructions given to operators contracted to carry out a specific type of Personal Data Processing. Individuals acting as professionals subordinate to a legal entity or as members of its bodies are not Controllers.

Personal Data: any information on any identified or identifiable individual. Therefore, although the data used individually or directly does not identify the individual, it is necessary to analyze whether the individual could be identified when such data is combined with other information.

Sensitive Personal Data: Personal Data regarding race, religious belief, political opinion, association with any trade union or religious, philosophical or political organization, health or sexual life, genetic or biometric data. Considering the possible discriminatory nature thereof, such data is subject to more specific Processing rules.

Data Protection Officer (DPO): person indicated by the Controller or Processor to act as the communication channel between the Controller, the Data Subjects, and the Brazilian Personal Data Protection Authority (ANPD). All companies must indicate a Data Protection Officer, and the ANPD must determine when such a Data Protection Officer is not required.

Processor: individual or publicly- or privately held legal entity, responsible for data Processing on behalf of the Controller.

Personal Data Protection Impact Report (RIPD or DPIA): Controller documentation that contains the description of the processes for Processing Personal Data that may give rise to risks to civil liberties and fundamental rights, as well as risk mitigation measures, safeguards and mechanisms.

Data Subject: individual to whom the Personal Data refers to. Considering that the Personal Data refers solely to individuals, information on (i) companies; and (ii) deceased individuals are not included in the scope of the law. According to the LGPD, the Data Subjects are entitled to several rights regarding Personal Data, which must be complied with by the Processing agents.

International Data Transfer: transfer of Personal Data to a foreign country or international entity.

Processing: any operation involving Personal Data, such as the collection, production, receipt, classification, use, access, reproduction, transmission, distribution, Processing, filing, storage, elimination, evaluation or control, modification, communication, transfer, disclosure or removal of information. In this regard, mere access to Personal Data is considered as Personal Data Processing and, therefore, subject to the principles and guidelines set forth in the LGPD.

Data Breach: A Personal Data breach is any confirmed adverse event related to a breach of Personal Data security, such as unauthorized, accidental, or unlawful access resulting in destruction, loss, alteration, breaches, or any form of inappropriate or unlawful data Processing that could result in a risk to the rights and freedoms of the Data Subject.

Brazilian Data Protection Authority (ANPD): public administration body, under the Presidency of Republic, that, although not having its own legal personality, is endowed with technical autonomy and decision-making authority. The ANPD has, among others, the competence to ensure the protection of Personal Data in order to protect the fundamental rights of freedom and privacy and the free development of the personality of the individuals, as provided in the LGPD.

» SENACON: Brazilian Consumer Secretary.

» PROCON: Brazilian Consumer Protection and Defense Program.

» CADE: Brazilian Administrative Council for Economic Defense.



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



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



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



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



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

Contribution by Fernanda Azarite.

This material was last updated on February 08, 2023 and published on February 10, 2023.
For more updated information please contact us.