Privacy Series

12 HOW DO I ENSURE COMPLIANCE?

VEIRANO ADVOGADOS



This is the twelth chapter of
the Data Privacy Series. Click here
to access the chapter 11.



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.

INTRODUCTION:
THE CURRENT BRAZILIAN SCENARIO

Analyzing the current Brazilian scenario, only 36% of the companies claim to be fully adequate, as shown in the IT Trends Snapshot 2023 study, conducted by Logicalis. On the other hand, a large portion of the companies (43%) are still in the adoption phase, but already present concrete implementation initiatives.

Nevertheless, the sense of urgency in the race for compliance intensified even more after the application of the 1st fine by the ANPD, in a decision published on July 06, 2023 (Case No. 261.000489/2022-62). Contrary to the expectation of most experts, the first fine was applied against a micro company that failed to comply with objective requirements of the law, reinforcing that the adequacy to LGPD should not be a concern only for Big Techs.

For this reason, Chapter 12 of the Privacy Series will help you understand how to comply with the LGPD, covering the initial steps, the key measures to compliance, and the documents you may need in this process.





DATA PROTECTION CHECKLIST: WHERE TO START?

Before starting your compliance journey, you should review the measures and practices already adopted by your company. That way you will be able to verify and map the changes that must be made to ensure compliance with the applicable data protection legislation, as well as identify the next steps regarding your company's compliance.

To help you, below is a checklist so you can understand your company's maturity level:

- ☐ Do you understand the basic concepts established by the LGPD and are you aware that you must adapt to them?
- ☐ Is the personal data collected during the provision of services limited to what is necessary?
- ☐ Has your company's data protection officer (DPO) been appointed?
- ☐ Does your company have an established deadline for data retention and deletion?
- ☐ Has the "Privacy team", composed of the company's top management, been created?
- ☐ Do data subjects have a means of exercising their rights in relation to the processing of data?

- [ ] Does your company already adopt information security measures such as firewalls, antivirus, encryption, and double authentication?
- [ ] Have the main risks related to personal data processing been identified and measures for their mitigation already indicated?
- [ ] Has your company already developed a privacy strategy? Do you already know what your data protection priorities are?
- [ ] Have the Terms of Use and Privacy Policies used by your company already been revised and updated?
- [ ] Has your company already carried out training to contextualize and inform employees about the law and internal adjustments?
- [ ] Does your company already have a procedure for responding to requests from data subjects and the ANPD?
- [ ] Have the processing activities carried out by your company already been mapped and has the record of processing activities already been prepared?
- [ ] Has the procedure for responding to data protection incidents already been created?
- [ ] Are the data subjects (company employees, clients, vendors, service providers, etc.) aware of your company's processing of data? Do they know how and what their data is used for?
- [ ] Do the contracts entered into by your company with third parties (employees, service providers, clients, vendors, etc.) already have an applicable data protection provision? And what about the contracts that precede the LGPD, have they been amended yet?
- [ ] Do you know your responsibilities regarding data processing?
- [ ] Is there international transfer of data in the context of the provision of your company's services? Have the applicable guarantees already been implemented?

Based on the topics you have indicated as already met, it will be possible to identify pending issues and topics to be addressed in order to ensure compliance.

Please note that the purpose of the checklist above is to guide the actions taken to ensure compliance by your company and contains some of the main issues that must be observed, but it does not exhaust all issues related to personal data processing.

KEY MEASURES TO ENSURE COMPLIANCE

Considering the points covered in the preceding item, we have established below some of the main actions to be adopted to ensure compliance:



1. Appoint the data protection officer (DPO) or, if you qualify as a Small Processing Agent, you may just designate a channel for communication with data subjects (read Chapter 3 of the Privacy Series to learn more);
2. Appoint the persons responsible for data protection issues in each of the departments;
3. Understand the flow of personal data within the company;
4. Document the identifies flows in each area (collection, sharing, purpose of processing etc.);
5. Identify the legal bases applicable to each processing activity;
6. Identify what must be changed in relation to data processing;
7. Identify the appropriate mechanisms to ensure that the international transfer of data is compliant;
8. Establish how changes will be implemented;
9. Implement the identified measures and prepare a report for processing high-risk data;
10. Review the relevant documents;
11. Create procedures and tools to detect data breaches or leaks;
12. Create internal procedures and tools to respond to data subjects and national authorities to ensure exercise of right;
13. Prepare a personal data governance policy and culture;
14. Give your employees subsidies and information so that they can handle data more consciously and appropriately.

DOCUMENTS YOU MAY NEED

The LGPD does not provide a list of documents to ensure the handling agents are complying with the law. However, to ensure compliance with applicable data protection legislation, it will be necessary to implement new measures and update the corporate standards to ensure that all principles and requirements are being duly observed when processing data on individuals involved in the company's activities, whether they are employees, clients, vendors, etc.

There are up to thirty (30) different documents that your company may have to prepare depending on the activities adopted by your company. Some of these documents include:

Privacy Policies for data subjects	Templates of standard personal data protection clauses	Consent instruments
Procedures to answer requests submitted by data subjects and by ANPD	In-house protocols in case of security incidents with personal data	Codes of Conduct and Good Practice Guides



MONITORING AND IMPORTANCE OF THE CONCEPT OF PRIVACY BY DESIGN

Like the company itself, internal processes are changeable and are being improved and modified on a regular basis. For this reason, it is important to consider that even after the LGPD Compliance project has been carried out, it will be necessary to monitor the company's processing of personal data and update the internal rules and even the personal data inventory, to ensure that the activities adopted by the company are taking into account the requirements and guidelines of the applicable legislation.

In addition, it is important to note that merely updating policies and documents within the company does not guarantee compliance with the law.

It is essential that the company also establish a culture of data governance that adopts all operational and information security measures to ensure the integrity of the personal data processed during the performance of its activities. Thus, it is also vital that all employees and service providers are involved and are aware of all practices adopted by the company to ensure that the privacy and personal data of the data subjects are being properly protected.

The GDPR defines the terms Privacy by Design and Privacy by Default and, although the LGPD does not expressly adopt them, these concepts are very similar to the provisions of the Brazilian law and can assist in complying with applicable data protection legislation:

Privacy by Design
Consider the nature, purposes, context and scope of data processing when creating products and providing services, implementing risk-based security measures.

Privacy by Default
Standard configurations of products or services should protect the data subject to the greatest extent possible, both at a technical and operational level, ensuring that the minimum of personal data is handled.

"**Privacy by Design**" consists of applying the concepts and principles of data protection from the start of creation of a technology, so that these are intrinsically integrated into its functionality.

"**Privacy by Default**", on the other hand, requires controllers to implement appropriate measures, both at a technical and organizational level, to ensure that technologies work, naturally and automatically, in order to process only the minimum personal data required to fulfill their specific purpose. This development model seeks to avoid excessive processing and to help control data storage and accessibility.

The main difference between these concepts is that they are based on a preventive approach, not on a reactive one, as companies usually adopt. Therefore, companies must analyze all of the structure and security mechanisms inserted in the product before it is even released to the public, implementing all possible measures to prevent any data breach from occurring.

Note!

What is important to do after completion of the project?

- Establish or structure a department responsible for matter related to data protection;
- Closely monitor and supervise employees to verify compliance with the new guidelines;
- Regularly update the mapping;
- Improve and implement new processes in relation to requests by data subjects and/or the ANPD;
- Conduct periodic training on the main data protection topics (requests from data subjects; use of consumer data; securing consent, etc.);
- Keep the Governance Program active, providing all employees with subsidies to ensure protection of the data subject´s personal data;
- Comply with the new guidelines and/or normative rules issues by the NAPD related to data processing;
- Inform new employees of the importance of data proception for the company and instruct them on the Data Governance Program implemented and adopted by the company, though training programs, which may be recorded for this exclusive purpose.



VEIRANO ADVOGADOS

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



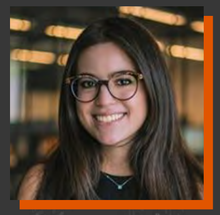
DENISE LOUZANO
+55 11 2313 5912
denise.louzano@veirano.com.br



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



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



HELOISA HELENA DE PAULA CUNHA
+55 11 2313-3830
heloisa.cunha@veirano.com.br

This material was last updated on July 20, 2023 and published on July 21, 2023.
For more updated information please contact us.