Privacy Series

3 PROCESSING AGENTS

VEIRANO ADVOGADOS



This is the third chapter of the Data Privacy Series. Click Here to access the chap. 2.



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



In any relationship established between your company and third parties, in which **Personal Data is Processed**, **each party shall be deemed a Processing Agent,** whether as Controller, Processor or both.

We set forth below the **main characteristics** concerning each of these figures, as provided for in the LGPD and the **Guideline for Definitions of Data Processing Agents and the Controller ("Guideline")**, as well as the definition of a **Small-Sized Processing Agent** and the consequences of being considered as a Small-Sized Processing Agent.

If you do not know your position in the Data Processing Operation, click here.

CONTROLLER

What is a Controller?

The individual or legal entity, under public (government) or private law (company or individual), responsible for making decisions regarding the processing of personal data (item VI, article 5 of the LGPD). Controllers are not individuals who act as professionals subordinate to a legal entity or as members of its bodies;

Controller's Duties/ Obligationsr

Controllers must comply with data protection principles and take appropriate technical and organizational measures to ensure that processing is carried out in accordance with the LGPD;

Controller's Attributions

(i) Assess the existence of at least one of the legal grounds for performance of each personal data processing (article 7, for personal data, and article 11, for sensitive data, of the LGPD);

(ii) Monitor the complete data cycle, by excluding or ensuring the exclusion of the Personal Data upon completion of the data Processing;

(iii) Appoint the Data Protection Officer (article 5, VIII, and article 4, of the LGPD);

(iv) Prepare the Personal Data Protection Impact Report (article 5°, XVII, of the LGPD);

(v) Be responsible for the burden of proof regarding the Data Subject's authorization (article 8, paragraph 2, of the LGPD);

(vi) Comply with the Data Subjects' rights (article 18, of the LGPD);

(vii) Maintain the registry of the Personal Data Processing operations (article 37 of the LGPD);

(viii) Demonstrate the adoption of effective measures that are capable of proving the compliance with the Personal Data protection rules, including the effectiveness of these measures (article 6, X, of the LGPD);

(ix) Provide the instructions for data Processing to the Processors (article 39 of the LGPD);

(x) Comunicate the ANPD and the Data Subject of the occurrence of any security incident that may represent significant risk or damage to the Data Subjects (article 48, of the LGPD);

(xi) Define and apply the good practice and governance rules to Personal Data protection, taking into account, in relation to the Processing and to the data, the nature, scope, purpose, probability and severity of the risks and benefits arising from the Processing of the Data Subject's Personal Data (article 50, of the LGPD);

(xii) Adopt security, technical and administrative measures to protect the Personal Data from non-authorized access and accidental or unlawful events of destruction, loss, modification, communication or any other type of improper or unlawful data Processing (article 46, of the LGPD).



Responsability

The Controller who, by virtue of the exercise of the activity of Processing of Personal Data, causes pecuniary, moral, individual or collective damage to another person, in violation of the legislation for the protection of Personal Data, is obliged to repair it. All Controllers directly involved in data Processing operations which cause damage to the data subject shall be jointly and severally liable. **Unless the Controllers can comprove that:**

(i) they have not Processed the Personal Data attributed to them;

(ii) despite Processing the Personal Data attributed to them, the provisions of the LGDP were not violated; or

(iii) the damage resulted from the exclusive fault of the Data Subject or a third party.

It is possible in a business relationship to have two Controllers. The ANPD has called this co-controllership a "joint controllership":

JOINT CONTROLLERSHIP

When two or more persons responsible for the data Processing determine jointly the purposes (common or not) and essential aspects for Personal Data Processing through an agreement that sets forth the respective responsibilities regarding the compliance with the LGPD. The joint Controllership is established upon compliance with the following criteria:

1. More than one Controller has the decision-making power regarding the data Processing;

2. Two or more Controllers have the same interests regarding the same data Processing;

3. Two or more Controllers undertake common decisions or not regarding the purposes and essential aspects of the data Processing.



PROCESSOR

What is a Processor?

The Processor is the individual or legal entity, publicly held (federal government) or privately held (company) responsible for the Personal Data Processing on behalf of the Controller (item VII, article 5 of the LGPD).

Subprocessor

Although there is no legal provision on the concept in the LGPD, the term may be used as a parameter in more complex data Processing chains. The Subprocessor is contracted by the Processor to perform the Processing on behalf of the Controller. The Subprocessor reports directly to the Processor rather than the Controller. However, regardless of the institutional agreements between the Processor and Subprocessor, for purposes of the LGPD, both may act, as applicable, as the Processor and report to the ANPD.

Moreover, in the European context, the GDPR provides that the Processor must inform the list of Sub-Processors to the Controller. Notwithstanding the LGPD being silent on the subject, such information is a recommended measure, when possible.

Pocessor's Obligations

The Processors shall comply with data protection principles and Controllers' instructions, as well as adopt proper technical and organizational measures to ensure that the data Processing is performed in accordance with the LGPD.

Processor's Duties

(i) Maintain the registry of the Personal Data Processing operations (article 37 of the LGPD);

(ii) Demonstrate the adoption of effective measures that are capable of proving the compliance with the Personal Data protection rules, including the effectiveness of these measures (article 6, X, of the LGPD);

(iii) Define and apply the good practice and governance rules to Personal Data protection, taking into account, in relation to the Processing and to the data, the nature, scope, purpose, probability and severity of the risks and benefits arising from the Processing of the Data Subject's Personal Data (article 50, of the LGPD);

(iv) Decide which IT systems or other methods to be adopted to collect Personal Data;

(v) Decide how to store the Personal Data;

(vi) Decide how data will be transferred from one organization to another;

(vii) Define the IT systems or organizational methods to be implemented so that the Data Subjects are able to exercise the rights protected by the LGPD;

(viii) Decide how it will delete or discard data, as well as how it will ensure compliance with a retention schedule.

Responsability

The Processor is jointly responsible for damages caused by virtue of the Personal Data Processing, upon (i) violation of the LGPD; (ii) non-compliance with the Controller's instructions, except if:

(i) they have not processed the Personal Data attributed to them;

(ii) despite of the Personal Data Processing, the provisions of the LGDP were not violated by the Processors; or

(iii) the damage resulted from the exclusive fault of the Data Subject or a third party.

Small-Sized Processing Agents

As we have seen in this chapter, the LGPD establishes several requirements and obligations for Controllers. However, through this law, the legislator indicated the need for specific regulation to enable the adaptation of micro and small enterprises, as well as startups or innovation companies to the LGPD.

Thus, on January 28, 2022, the ANPD Board of Directors published CD ANPD Resolution No. 2, which approves the LGPD Enforcement Resolution for Small-Sized Processing Agents.



The Resolution lists the following entities as Small Treatment Agents under current legislation:

- Micro Companies;
- Small Companies;
- Startups;
- Legal Entities of Private Law, including non-profit ones;
- Natural People; and
- Unpersonalized Private Entities.

The Resolution brings flexibilities that concern the possibility of adopting simplified and differentiated procedures, in order to facilitate the compliance of this group to LGPD and contribute to the dissemination of the culture of personal data protection.

The entities that are members of the above mentioned group can benefit from several flexibilities, such as:

- The possibility of keeping the register of personal data processing operations (Art. 37 of LGPD) in a simplified form, in a model to be provided by ANPD (Art. 9 of the Resolution);

- The exemption to nominate the person in charge (Art. 41 of the LGPD and Art. 11 of the Resolution);

- The granting of doubled time in cases provided for in the Resolution, such as the provision of a clear and complete statement in the case of a request for access and/or confirmation of processing by the data subject.

It is worth noting that the Resolution itself states that the application of the relaxations "**does not exempt small-sized processing agents from complying with the other provisions of LGPD,** including the legal bases and principles, other legal, regulatory and contractual provisions relating to the protection of personal data, as well as rights of the data subjects."

In addition, the measures provided for in the Resolution **do not apply** in the following hypotheses:

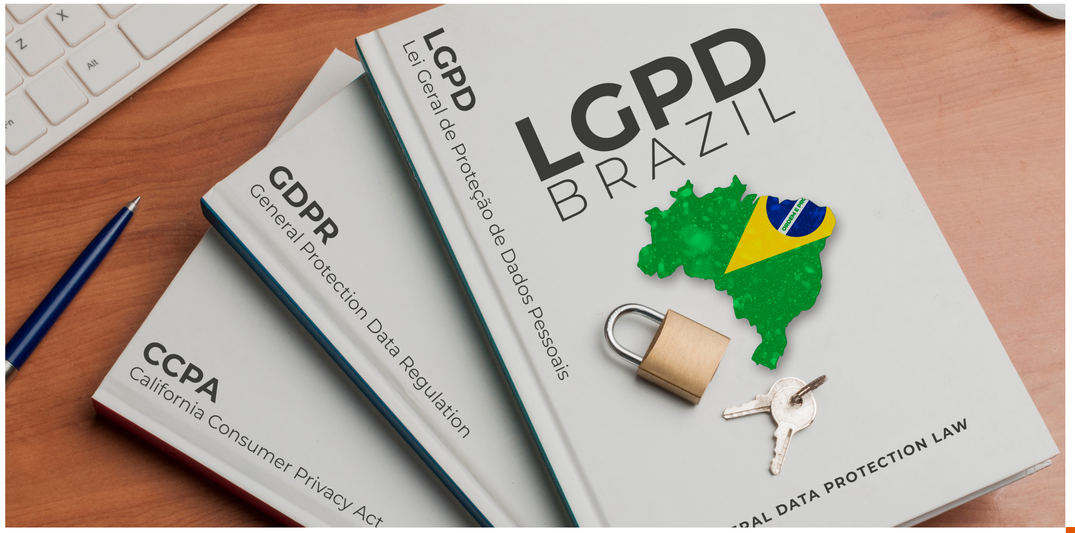
(i) the processing of personal data carried out by a natural person for exclusively private, non-economic purposes;

(ii) the data processing hypotheses foreseen in Art. 4 of LGPD; and

(iii) to Small-Sized Processing Agents that (a) perform high-risk processing for the holders, (b) earn gross revenue exceeding the limit established in Art. 3, II, of Complementary Law No. 123/2006 or, in the case of startups, in Art. 4, § 1, I, of Complementary Law No. 182/ 2021; or (c) belong to an economic group in fact or in law, whose global revenue exceeds the limits referred to in item (b).

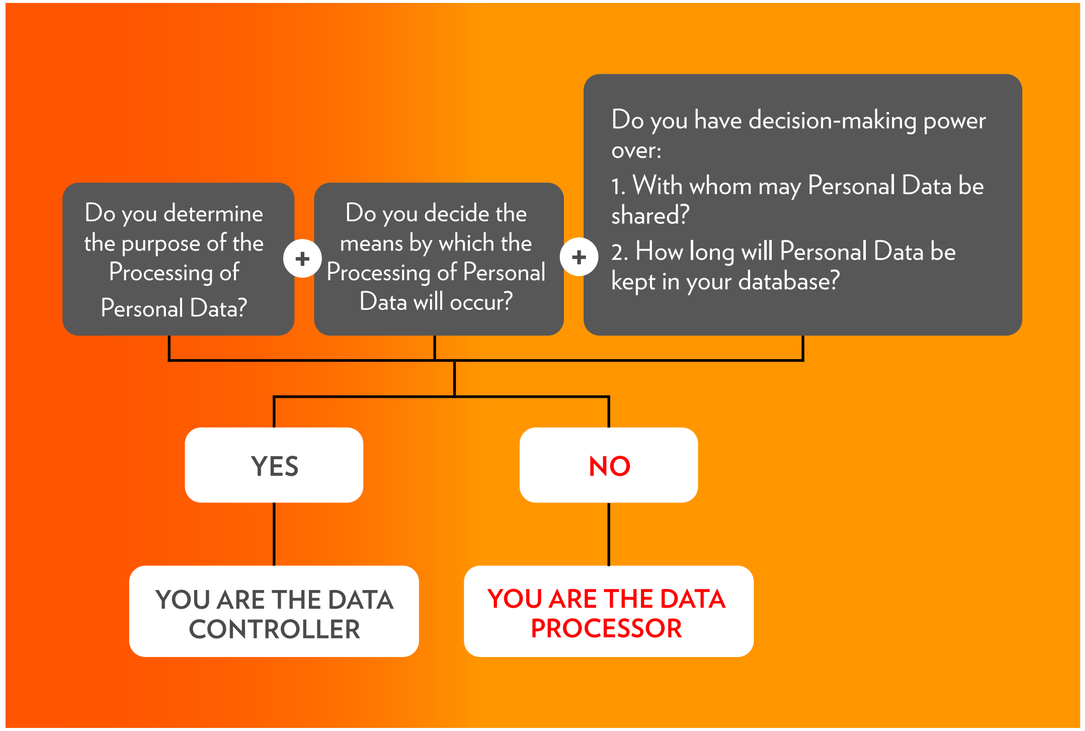
Also, in the context of the ANPD's initiatives to assist Small-Sized Processing Agents in complying with LGPD, ANPD published the Information Security Guidelines for Small-Sized Processing Agents. In order to provide further guidelines to Small-Sized Processing Agents, between November 4, 2022, and January 3, 2023, a call for submissions was opened to define the simplified model for registration of personal data processing operations.

Finally, considering the recent closure of the intake of subsidies on the simplified model of registration of personal data processing operations, as well as the absence of definition of what would be considered as "high risk", it is expected that soon we will have new guidelines from the ANPD on the subject.



Am I a data Controller or Processor in the context of Processing?

The flowchart below indicates the events when you may be deemed a Controller or a Processor:





The agreement entered into between the Controller and the Processor shall bind the parties, however **the information included therein is not essential to define the effective condition** of the parties during the data Processing.

That is, although the agreement may establish that party X is the Processor, if during the data Processing party X acts as the Controller, regardless of the contractual provisions, party X shall be deemed responsible as Controller.

Therefore, it is important to be aware of the position and responsibilities that each party actually has, so that the determinations established in the contract reflect the reality of Processing.

It is worth mentioning that even though the LGPD does not expressly state that it is mandatory to sign a contract between the Controller and the Processor, as in the case of the GDPR, the Guideline states that such an agreement is a good processing practice, since the contractual clauses impose limits on the Processor's activities, set parameters for accountability between the parties, and reduce the risks arising from the processing of Personal Data.

Finally, in addition to the Processing Agents mentioned in this chapter, the **LGPD brings another important figure** in the context of personal data protection. **The figure of the Data Protection Officer** was also addressed in the Guidelines and will be addressed in the next chapter of the **Privacy Series.**



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.