

PERSONAL DATA PROTECTION



Summary



04 **INTRODUCTION**

10 **PRINCIPLES AND PENALTIES**

14 **CASES FOR DATA
PROCESSING**

18 **RECOMMENDATIONS**

Introduction

Are you aware of the Brazilian General Data Protection Law (LGPD)?

Do you know how it affects your personal life and daily work?

Have you ever stopped to think about the amount of data we provide daily in commerce, on websites, apps, and social networks? And what is the destination of this data? Who collects this information, where is it stored, how is it used, and what is it for? Why do we receive so many unwanted messages in our mailboxes?

In the end, **what are we willing to give up from our privacy in exchange for convenience and benefits?**

Data forms the foundation of a new economy. Currently, every institution, to a greater or lesser extent, process personal data, as it collects, stores, and uses information from people around the world. **To protect citizens from the improper use and exposure of their personal information, the Brazilian General Data Protection Law (No. 13,709/2018) was enacted.** Companies had until August 16, 2020, to comply with the LGPD.

The Law deals with the processing of personal data, including in digital media. In other words, every operation carried out with the personal data of any individual is subject to the LGPD.

When a personal data is collected, produced, received, classified, used, accessed, reproduced, transmitted, distributed, processed, archived, stored, deleted, evaluated, controlled, modified, communicated, or transferred, it is being processed.

The Law has extraterritorial application, meaning that foreign companies that collect or process data within the national territory or offer goods or services to individuals located in Brazil are also subject to the application of the LGPD.

What is personal data?





Personal data is any information that, either alone or when combined with other data, can identify an individual, such as name, address, email, IP address, internet browsing behavior, consumption habits, etc. Therefore, it encompasses **any** information related to a natural person and **not only data related to private life**.

Sensitive personal data relates to racial or ethnic origin, religious or philosophical beliefs, political opinions, union membership, genetic or biometric data, and information about health or sexual life if linked to an individual. Due to their nature, they may subject their owner to discriminatory practices and, therefore, must be treated in a more secure and restrictive manner.

Data Subject

The data subject is the person to whom the personal data being processed refers. The rights of the data subject include: confirmation of data processing; access to the data; data correction; anonymization; blocking or deletion of unnecessary, excessive, or unlawfully processed data; data portability; obtaining information about data sharing; withdrawal of consent and deletion of data processed on this basis.

In addition to the Data Subject, the Law also defines the roles of the Controller, Processor, Data Protection Officer (DPO), and Data Protection Authority. In practice, it works like this:

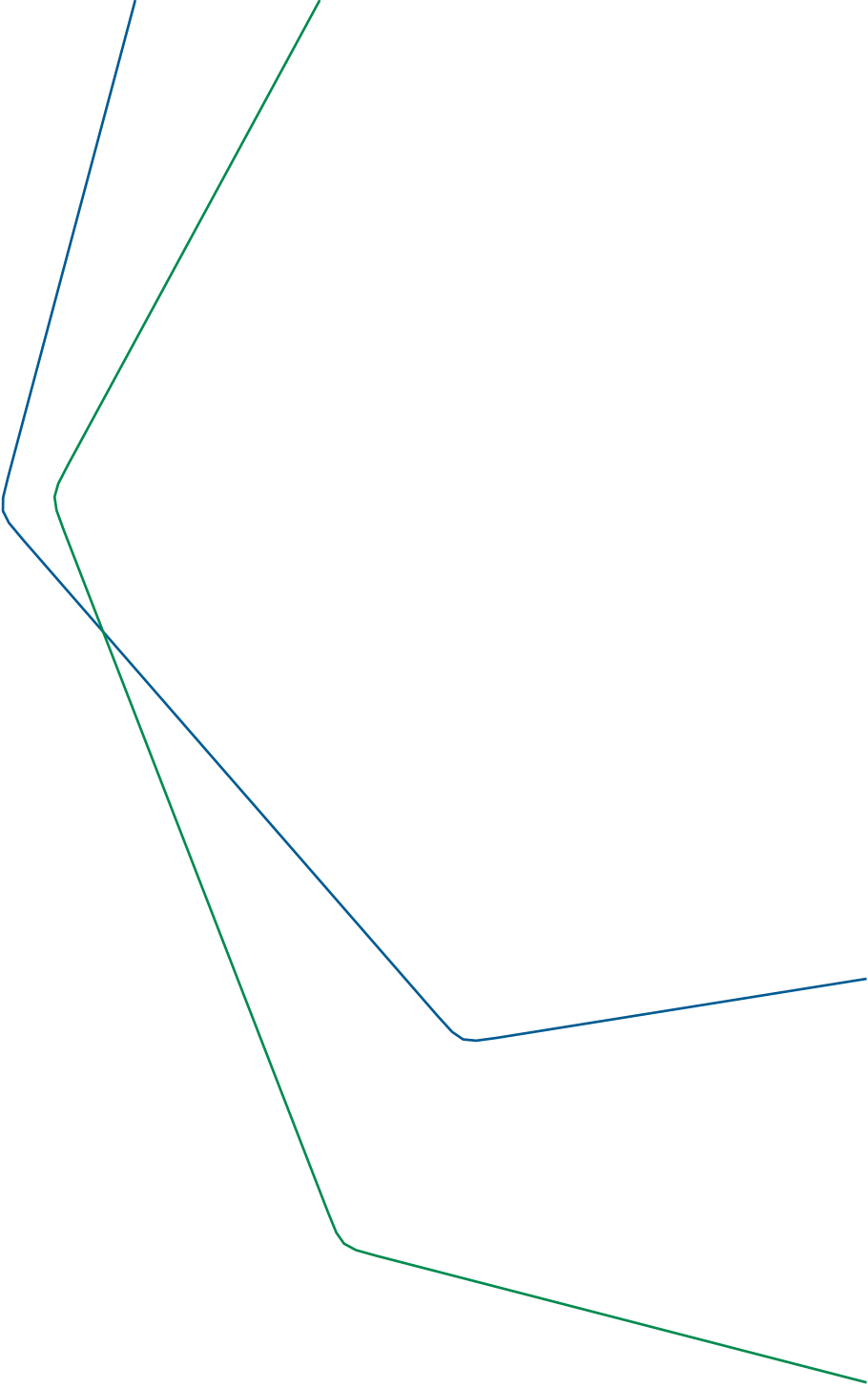
	<p>When you go to the pharmacy and register yourself to receive a discount, you are the Data Subject, and the pharmacy is the Controller.</p>
	<p>The pharmacy hires a company to manage the database, and this company is the Processor.</p>
	<p>The pharmacy has a Data Protection Officer, who serves as the communication channel with you regarding your data.</p>
	<p>The Brazilian Data Protection Authority (ANPD) issues rules that complement the LGPD. It oversees the pharmacy and the systems company, and accepts complaints if you identify that your data has been processed in a way with which you do not agree.</p>

In the case of Petrobras, as a general rule, the company acts as the **controller**, as it makes decisions regarding the processing of personal data and **carries out** this processing itself or through contracted companies for this purpose.

The **Data Protection Officer** is the **General Manager of Privacy** and has the following activities:

- *Accept complaints and communications from data subjects, provide clarifications, and take action;*
- *Receive communications from the national authority and take action;*
- *Guide employees and contractors of the entity regarding practices to be taken concerning the protection of personal data;*
- *Perform other duties determined by the controller or established in complementary regulations.*

The **Brazilian Data Protection Authority** is the public administration body responsible for safeguarding, implementing, and supervising compliance with the LGPD.



Principles and Penalties

LGPD provides that all processing of personal data must consider good faith and the following principles:



PURPOSE

Collect and process personal data for specific, legitimate, and informed purposes communicated to the data subject.



TRANSPARENCY

Ensure that the data subject is properly informed about the processing: purpose, duration of processing, entities involved, etc.



ADEQUACY

Collect and process only data that are compatible with the purpose informed to the data subject.



NECESSITY

Collect only information strictly necessary for the accomplishment of the purpose.



DATA QUALITY

Ensure that the personal data under its custody are always accurate, updated, and relevant for the fulfillment of the purpose of their processing.



NON-DISCRIMINATION

Never process personal data for discriminatory, unlawful, or abusive purposes.



FREE ACCESS

Ensure the right of the Data Subject to access their data. The Data Subject may easily and free of charge consult all the information that the organization holds about them and everything that has been done with this information.



SECURITY

Implement technical and administrative measures capable of protecting personal data from unauthorized access and from accidental or unlawful destruction, loss, changes, communication, or dissemination.



PREVENTION

Adopt measures to prevent damage resulting from the processing of personal data.



ACCOUNTABILITY

Demonstrate the adoption of effective measures capable of proving compliance with data protection regulations, including the effectiveness of these measures.

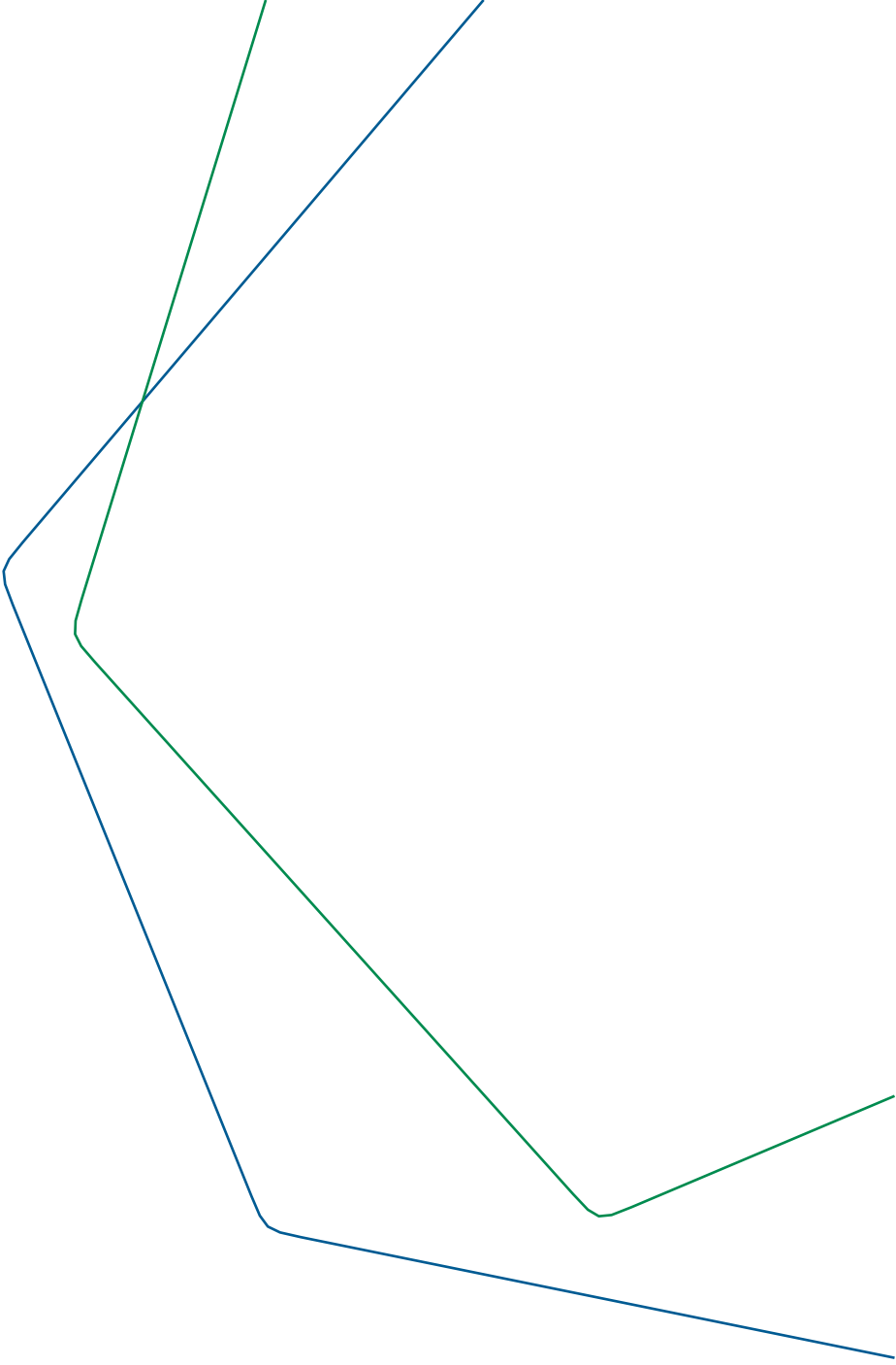


Minimization: Collecting the minimum amount of necessary information.

Hygiene: Keeping the database consistently updated and organized.

Non-compliance with LGPD regulations can cause implications in legal, operational, and reputational spheres, affecting our businesses.

LGPD provides for sanctions such as warnings, disclosure of the violation, blocking or deletion of the data that originated the violation, as well as fines of up to 2% of the gross revenue of the previous year, limited to R\$ 50,000,000.00 per violation.



Cases for Data Treatment

Each one of us plays an important role in ensuring the company's compliance, as every **physical or electronic** file containing personal data will be subject to the LGPD. To process non-sensitive personal data, it is necessary for at least one of the following situations to be present:

- *Data subject consent;*
- *Compliance with a legal or regulatory obligation by the data controller;*
- *By the public administration, for the processing and shared use of data necessary for the execution of public policies;*
- *For conducting studies by research organizations;*
- *For the execution of a contract or preliminary procedures related to a contract of which the data subject is a party;*
- *For the regular exercise of rights in judicial, administrative, or arbitral proceedings;*
- *For the protection of the life or physical integrity of the data subject or a third party.*

- *For the safeguarding of health, exclusively, in procedures carried out by healthcare professionals, healthcare services, or health authorities;*
- *When necessary to meet the legitimate interests of the data controller or a third party, considering specific situations, except where fundamental rights and freedoms of the data subject prevail, requiring the protection of personal data;*
- *For credit protection.*

The consent of the data subject is the freely given, informed, and unambiguous expression by which the data subject agrees to the processing of their personal data for a specific purpose. In the case of sensitive personal data, consent must be highlighted and may only be waived in the following circumstances:

- *Compliance with a legal or regulatory obligation by the data controller;*
- *Shared processing of data necessary for the public administration to execute public policies as provided for in laws or regulations;*

- *Conducting studies by research organizations;*
- *Regular exercise of rights, including in contracts and in judicial, administrative, and arbitration proceedings;*
- *Protection of the life or physical integrity of the data subject or a third party;*
- *Safeguarding of health, exclusively in procedures carried out by healthcare professionals, health services, or health authorities; or*
- *Ensuring prevention of fraud and security of the data subject, in identification and authentication processes for registration in electronic systems, except where fundamental rights and freedoms of the data subject prevail, requiring the protection of personal data.*

Recommendations

Tips that you can adopt in your daily life:

- Research the source and reliability of programs and applications before their installation and keep them updated;
- Make sure your internet browser and antivirus are always up to date, with the latest available version installed;
- Evaluate the reliability of websites and links, especially those received via email, before accessing them;
- If you access your personal account on a website, social network, or app on a device that is not yours, including public devices, remember to log out before ending the browsing session;
- Be aware of what will be done with your personal data before sharing it;
- Ensure access to personal information is only granted to those who truly need to know them; and
- Strive to use only the personal data necessary for your activities.

