upLexis® TECNOLOGIA

# LGPD / GDPR
## How upLexis positions itself in relation to the new Law

Version 2 - March 27th, 2023

# ÍNDICE


Introduction ..... 03
Similarities and Differences between the GDPR and the LGPD ..... 04
Five frequently asked questions about LGPD ..... 05
Top 10 LGPD terms ..... 09
Strategic priority to ensure transparency and security for our customers ..... 11
Our position about LGPD / GDPR ..... 12
Details on internal communication processes and actions ..... 15
UpLexis and LGPD FAQ ..... 16
About upLexis ..... 19

## INTRODUCTION

The General Data Protection Law (LGPD - - Law No. 13.709 / 2018) is a set of rules that were created to **regulate the use of personal data** by companies (public and private), ensuring that Brazilians have more control, security and transparency over their information.

Approved in February 2018, the LGPD entered into force precisely on **18.09.2020,** with which companies had about 20 months to prepare and implement the new controls.

In this material, we will explore some main issues to be discussed in the scope of data security, as part of an ecosystem that values and benefits from them, and we will also give upLexis a position in the face of this challenging new reality.

## SIMILARITIES AND DIFFERENCES BETWEEN THE GDPR AND THE LGPD

**"Brazil's General Data Protection Law (or LGPD)** brings sorely needed clarification to the Brazilian legal framework. The LGPD attempts to unify the over 40 different statutes that currently govern personal data, both online and offline, by replacing certain regulations and supplementing others. This unification of previously disparate and oftentimes contradictory regulations is only one similarity it shares with the EU's GDPR, a document from which it clearly takes inspiration.

Another similarity is that the LGPD applies to any business or organization that processes the personal data of people in Brazil, regardless of where that business or organization itself might be located. So, if your company has any customers or clients in Brazil, you should begin preparing for LGPD compliance. Fortunately, you still have time before the law takes effect. And if you are already GDPR compliant, then you have already done the bulk of the work necessary to comply with the LGPD.

To get more details about similarities and differences between LGPD and GDPR, please access: https://gdpr.eu/gdpr-vs-lgpd/ "

## FIVE ASKED QUESTIONS FREQUENTLY ABOUT LGPD:

### 1 What is LGPD?

The LGPD was created to **strengthen data protection for Brazilian individuals.** Very inspired by the European GDPR, it brings privacy to citizens' information within the national territory.

With this new law, organizations need to adopt stricter controls, specify procedures and a timetable in the event of a system breach or breach. It also involves the **freedom and privacy** that an individual has to express their willingness to delete or remove their personal data from a certain database.

Failure to comply with any of these basic LGPD requirements may result in millionaire fines for those responsible.

### 2 What is the period for adaptation?

In September, President Jair Bolsonaro signed Provisional Measure 959, which dealt with the term of the General Personal Data Protection Law (LGPD). As the Senate had determined its immediate effectiveness, the **law came into force on 9.18.2020.**

Although administrative sanctions will not take effect until August 2021, a number of obligations are already in place. Therefore, companies that are not yet adequate, should run in relation to this and focus on processing data on a legal basis, following the principles of the law and guaranteeing the rights of the holders.

## 3 Which organizations are affected?

The LGPD is applied to **all businesses or public institutions that store and / or process data** from Brazilian individuals, thus affecting the relationships between customers and suppliers of products and services, employee and employer, national commercial relationships, in addition to other relationships in which personal information is collected.

## 4 What types of data does LGPD protect?

Unlike other compliance standards, the LGPD brings a much wider range of data to the discussion, ensuring the privacy of the individual in more areas.

In addition to the usual CPF and credit card numbers, which can be used in fraudulent transactions, other data such as: online browsing, political positioning, ethnic origin, religious belief, information regarding the individual's health or sexual, genetic or biometric life, are relevant and sensitive to LGPD.

Therefore, if the public organization or institution in question deals with any information that can expose the individual, in any way, it is important that it complies with the LGPD, through stricter controls, specifying the procedures and creating a schedule before any type failure or system failure.

## 5 How do LGPD fines work?

Failure to comply with the LGPD or the leakage of information after this new guideline can bring millionaire fines to organizations. The payment for these slips will be **2% of the company's total revenue, limited to R $ 50 million,** in addition to going through non-monetary implications such as the difficulty in closing partnerships with other organizations, loss of credibility in the market and generating a relationship of distrust. with the client.

## TYPES OF DATA AND SPECIFICATIONS ACCORDING TO LGPD:

- **Personal data:** Information related to an identified or identifiable natural person;
- **Sensitive personal data:** Race and ethnicity, religious belief, political opinion, union affiliation, health data, sexual option, genetic-biometric or child data;
- **Anonymized data:** Anyone whose title cannot be identified, considering the use of reasonable technical means available at the time of treatment.

## EXCEPTIONS TO THE APPLICATION OF THE LAW:

The law is not imposed on the processing of personal data carried out:

- By a natural person for exclusively private and non-economic purposes;
- For journalistic, artistic or academic purposes;
- For the exclusive purposes of: public security, national defense, State security, investigative activities and prosecution of criminal offenses, coming from outside the national territory (which are not the subject of communication, shared use of data with Brazilian treatment agents or object of international data transfer with a country other than the country of origin, provided that the country of origin provides an adequate degree of protection of personal data as provided for in this Law).

## 10 MAIN LGPD TERMS

1. **Database:** structured set of personal data, established in one or several locations, which may be in electronic or physical support.

2. **Data processing:** every action performed with personal data, some examples: access, storage, filing, evaluation, collection, classification, among several others.

3. **Data anonymization:** activity carried out in the treatment process that allows data to lose the possibility of association, directly or indirectly, with an individual.

4. **Data elimination:** deletion of information or a set stored in a database, without taking into account the procedure adopted.

5. **Holder:** natural or legal person to whom the personal data refer being processed.

6 **Controller:** is responsible (individual or legal entity) for making decisions regarding the processing of personal data.

An easier way to explain this term is to compare it to the figure responsible for LGPD, that is, the company that determines or performs the treatment, and can also only guide the operator to do the job.

7 **Operator:** can be considered a subcontractor of LGPD, that is, it is he who performs the processing of data following the guidelines of the controller and the requirements of the law.

8 **Person in charge or DPO (Data Protection Officer):** person appointed by the controller to be the communication channel between all data holders and the National Data Protection Authority.

9 **Impact report on the protection of personal data:** it is a document made by the controller that contains the description of the processes for processing data personal that may cause risks to civil liberties and fundamental rights of the individual.

10 **Data breach:** any incident related to the data and which was caused by a breach in security, resulting in a breach of confidentiality, availability or integrity of the information.

## STRATEGIC PRIORITY TO ENSURE TRANSPARENCY AND SECURITY FOR OUR CUSTOMERS

We understand this issue as a strategic priority and because of that, we have positioned ourselves previously, investing capital, time, focus and effort in this extremely relevant topic for the company, starting a detailed work together with a consultancy. specialized in digital law and LGPD legislation to assist us in guiding, analyzing and conducting the topic within the business context of upLexis.

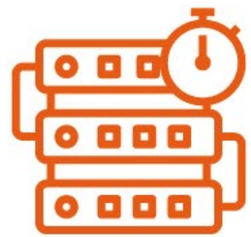
This work began with a detailed mapping of numerous indicators in our databases and information collection processes, such as:

**Analysis of the Data Collection / Capture Model**

**Analysis of the Data Storage Model**

**Analysis of the Purpose of Data Use**

**Evaluation of the Data Transfer Process**



**Analysis of Dwell Time and Data Disposal**

**Review of Contracts with Customers and Suppliers**

## OUR POSITION ABOUT LGPD / GDPR:

“By providing the final solution to the market, upLexis positions itself as the Operator of the Processing of Personal Data.”

We basically work as a data integration hub, capturing data from different sources (public / private), then we organize and start to deliver this material to our clients that will use this data on their own.

**UpLexis** does not store or even capture data that is not explicitly as using to specificly combate fraud, corruption, operational losses due to uncalculated risks, credit recovery and analysis and compliance with regulatory bodies such as BACEN / COAF / CVM and others.

## OUR POSITION ABOUT LGPD / GDPR

by providing the final solution to the market, upLexis positions itself as the **Operator of the Processing of Personal Data.**

**Private and / or public suppliers** from where upLexis collects and transforms data → The data sources (public and / or private) are considered to be **Controllers of their respective data.**

**Customers who hire upLexis solutions to resell them** to the market → They are characterized as **Controllers of the Processing of Personal Data.**

## DETAILS ON INTERNAL COMMUNICATION PROCESSES AND ACTIONS

Our data already respect the strictest information security protocols and are in a cloud environment, but our focus on this maneuver is to further improve **security layers** with an **emphasis on data protection,** access, encryption, backups and additional controls.

We want to assure our customers that we are in compliance with the LGPD, we act with **transparency in relation to their information** and we are willing to continue implementing all necessary additional controls, whether as an operator or controller of the data.

Another important point in our process of adapting to LGPD was the encouragement of a **new culture within the company** that values data security, and where everyone is aware of the changes and responsibilities that have emerged with the law.

**Internal communication, specific training on the topic and availability of materials for reading** were some of the main actions adopted within the company for all our employees.

We consider the protection of privacy and the confidentiality of personal information our priority, and for this reason we guarantee the best possible technical infrastructure to comply with all stipulated standards and the good conduct of everyone in the company on the subject.

If you have questions, criticism or suggestions about the positioning of the front UpLexis LGPD, provide a channel for contact: privacidade@uplexis.com.br

## FAQ UPLEXIS AND LGPD:

About Information Security:

**There is security awareness process information and privacy of Data in the company? How does it work and what does it cover?**

We promote annual training and workshops with our employees, in addition to the mandatory onboarding integration process for new employees.

---

**Is there a process for disposing of sensitive information?**

Yes, the company has a process for disposing of sensitive information, as well as its guidelines are provided for in the Information Security Policy, the last version of which is June 2018.

---

**Does upLexis use a DLP tool to monitor or restrict the leakage of sensitive information?**

We adopt tools such as Firewall, Antivirus and WAF services throughout our infrastructure, as well as we carry out penetration tests (pentest) regularly, carried out by an independent and approved company, once or twice a year.

## FAQ UPLEXIS E LGPD:

**Has the company implemented appropriate technical and organizational measures to demonstrate data protection precautions in its processing activities? Which?**

The organization has internal policies on Information Security, Privacy and Data Protection, as well as periodic training with its employees. In addition, the operation is hosted in a certified environment, has processes with strong encryption, procedure for meeting the requests of Holders and has a Data Protection Officer appointed.

## FAQ UPLEXIS E LGPD:

On compliance with the main standards

**Does upLexis have sensitive customer data stored?**

We do not work with sensitive customer data. We only collect data that is strictly essential for registering users with access to the platform and technical information for billing and communication with the customer / users.

---

**Is the data storage location encrypted?**

Yes, the structure used has adequate levels of security, encryption and security certification appropriate.

---

**What legal basis will be followed for storage / treatment to adhere to the LGPD?**

UpLexis treats its customers' data in accordance with the Legal Basis of consent.

---

**Does the company have a security system / processes to keep personal data in an integral, reliable and available way? Inform which.**

Yes. UpLexis uses secure communication, https and encryption protocols for the traffic of information that can be verified through the "lock" in the browser bar, as well as maintaining all sensitive data in cloud infrastructure with database encryption, services data protection, audits, penetration testing and backup policies well-defined.

UpLexis is a company specialized in emergent technologies and interpretation of a great data volume (Big Data) extract from internet and others source of knowledge Our mission is to provide intelligence to business operations where the relevant information has a critic role in the decision making process, in obtaining competitive advantage and improving organizational efficiency
We gathered talent professionals and unique skills to the production of technology in software applied to acquisition, organization, storage and information access, owning a few area patents

REQUEST A TEST

uplexis®
TECNOLOGIA

www.uplexis.com
comercial@uplexis.com.br