Your Guide to the LGPD - Brazil's Privacy Act

Author : Cat

Date : January 17, 2020

What is the LGPD?

The LGPD is the Brazilian version of the GDPR (General Data Protection Regulation). In Portuguese it is *Lei Geralde Proteçãode Dados*, or in English, *General Law of Personal Protection*. It is a framework of legal guidelines for collection and processing of personal info of individuals within Brazil. Or, in short, it's a set of rules that companies need to follow to collect and protect a user's data. The regulation is set to be official mid-2020. At that point, any company, group, or individual, that handles Brazilian data, or resides in Brazil, must comply with LGPD.

LGPD was based on both existing privacy legislation and GDPR. Four terms to understand:

Personal Data - any identifying information . This includes submitted information such as your name, email, SIN, address, phone number, biometrics, or account numbers. It also includes information that could be used to identify you indirectly such as location data.

Data Subject - simply put it is the user or the person who is identified by the information.

Data Controller - the person or company who determines the purpose and use of the collected data.

Data Processor - the person or company who processes the data. This includes analytics, marketing, as well as storage such as cloud services.

The *controller* and *processor* can be the same or separate. For example, my company collects email addresses for our newsletter. That makes us the *controller*. We can chose to store these addresses on our own machines, that makes us the *processor.* Alternatively we can chose to store them in Mailchimp, which is a newsletter app, or perhaps on a document in Google Drive, which is the cloud. Now we have chosen an outside *processor*. As the *controller*, we are responsible for LGPD compliance for both our company and our chosen *processor.*

New Security and Privacy Features

The full regulation is quite lengthy and includes your rights as a *data subject* as well as regulations around how *controllers and processors* are required to protect your data.

The basis of LDPD is *consent, s*econd to that is *User Rights*, and finally *privacy incident response*.

These 5 highlights from the regulation appear in both LGPD and the GDPR:

Consent - For all data collection, the *data subject* has to have the ability to both opt in AND withdraw consent. *Controllers* also have to present the information to support *right of access.* I like to break these down as the 5 Ws:

- WHO - Details of the recipients of the data including links to the *controller (*names of *processors* are optional)
- WHAT - List of the data being collected
- WHY - Reason for the collection (*known as legal basis*)
- WHEN - The duration for which the data will be retained
- WHERE - Clear links provided so user knows where to go to enact requests

There is a list of specific pieces of information that must be included according to the *Right to Information.* The simplest way to satisfy this right is to put all the information in your *Privacy Policy.*

Right to be forgotten - This is the most talked about and least understood. It is the right for a user to retract their data from storage or processing, from any company at any time. When the Cambridge Analytica scandal broke with Facebook in 2018, people wanted to delete their accounts but there was no regulation to dictate that that Facebook had to delete their data as well. This ruling would have forced both Facebook and Cambridge Analytica to delete the data they had on any qualifying individual that requested it (Facebook as the *Controller* and CA as the *Processor*). Note: This right is not an opportunity to have unflattering articles or reviews removed. The rule allows for personal mentions if they fall under freedom of expression, public interest, public health, or research.

Right of access - As a *data subject*, this is your right to ask about the purpose for the collected data, the *processors* involved, and even if the data is being manipulated with artificial intelligence or machine learning. All these answers *should* be covered in the new consent request (see below).

Right of restricton of processing - You know those pesky ads that follow you from one website to another? That's called direct marketing. The *restriction of processing* means you can indicate specifically that you do not want your data used in direct marketing campaigns.

Privacy Incident Management and Breaches - In terms of protection of data, this is a big one. In the past there was NO regulation that a company had to report a privacy breach. Uber took 6 months to report their 2018 data breach. Now compliant companies have to report any breaches to the data privacy authority and in some cases to the individuals as well.

For Businesses and Corporations

Any organization that "processes or stores large amounts of personal data, whether for employees, individuals outside the organization, or both" is required to designate a **Data Protection Officer.** That person is responsible for ensuring compliance of LGPD. Only the *Controller* company is required to have this role but it is suggested any processor company assign a DPO as well.

If a company is caught in non-compliance then they face a fine. Depending on the infraction, a simple (one time) or daily fine may apply. Fines may be as high as 50 Million Brazilian Reais (~$12M USD).

Every applicable company should run a **DPIA,** or *Data Protection Impact Assessment,* that includes an explanation why they are collecting the data requested, an assessment of risks to the rights and freedoms of data subjects, and documented proposed measures for safety and security of the collection.

Global Privacy Regulation Compliance is largely what WE do as a company. From DIY checklists to templates to having us do it for you, contact us for more information on how we can help.

For Small Business, Charities & Clubs

Unfortunately even small businesses, groups, not-for-profits, and charities fall under these regulations. If you run or are part of a group that collects information (newsletters, databases, list serves, forums, etc.) then this could apply to you. Fortunately most of the individual tools that small business uses, like cloud servers, Newsletters, and CRMs, have updated their terms to comply.

What you should do:

- Make a list of all of the software and services you use (good to have this anyway)
- Consider each one for data collection, storage, and processing
- For those that do, type the name of the service and 'GDPR' in to Google for instructions

More Help and Information

Due to the fact that LGPD is written in Portuguese, it is difficult to find a full version in English. A good over view can be found on the International Association of Privacy Professional's page.

For a full picture of what compliance looks like for LGPD, download our FREE Global Regulation overview page of all ten areas on which you need to focus.

If you want help from our consultants, have any questions or find something we've missed let us know!