CEP Magazine - March 2021
Brazil's general data protection law: What has it done?

By Marcelo Crespo, PhD, CCEP-I, and Guilherme Beloto

Marcelo Crespo (marcelocrespo@pgadvogados.com.br) is a partner specializing in digital law at PG Advogados in São Paulo, Brazil. **Guilherme Beloto** (gcbeloto@gmail.com) is a political scientist and lawyer based in Luxembourg, currently specializing in privacy and data protection.

In January 2020, we published an article on the key challenges in developing a privacy compliance program in 2020 (and beyond).[1] At that time, we urged organizations to overcome the difficulties of implementing such a program, as there was a pressing need to comply with data protection laws that were becoming increasingly available, and, specifically in Brazil, it was expected that such a law would come into force.

Now let us look at what has happened over the past year regarding Brazil's move toward data protection legislation and what we can expect for the future.

A brief history of the LGPD

Lei Geral de Proteção de Dados[2] (LGPD) is the Brazilian equivalent of the European Union's General Data Protection Regulation[3] (GDPR). It is the national data protection regulation in Brazil, valid throughout the country. Its origins can be traced back to 2010, when the federal government created an online platform to receive opinions via a public consultation, gathering suggestions on what a data protection legislation should entail. A second round of consultations occurred in 2015.

By 2016, the federal government considered itself ready and sent a bill to be discussed in Congress, and, in 2018, it enacted the LGPD. Initially, the legislation foresaw a transition period for organizations to adapt and acquire compliance to the new requirements. The LGPD was planned to enter into force in February 2020; before that deadline was reached, however, the president enacted a provisional measure (*Medida Provisória*) that delayed the implementation of LGPD by six months.[4]

And then...COVID-19 changed the world. And with the global pandemic, the legislator decided to postpone the entry into force of the LGPD once more. After amendments to the original text, the final version of the LGPD finally came into force on September 18, 2020. Administrative fines will apply as of August 2021.

An overview of the LGPD

It is essential to realize that data protection legislations are not only about personal data breaches or security incidents, though these are essential topics to consider when analyzing them. It should be expected that, at some point, every organization will face a personal data breach. We have been advocating for some time now that organizations should engage this topic with a hands-on approach, as the denial only delays essential preparatory work that should enable the organization to quickly tackle the challenges that come with a data breach.

The Brazilian legislation also addresses information security, which is closely connected to (personal) data protection and highlights the need to protect fundamental rights, specifically freedom, privacy, and the free development of the personality of individuals (Article 1, LGPD):

The legislation is structured in 10 chapters:

- Chapter I: Preliminary provisions
- Chapter II: Processing of personal data
- Chapter III: Data subjects' rights
- Chapter IV: The processing of personal data by the public authorities
- Chapter V: International data transfer
- Chapter VI: Personal data processing agents
- Chapter VII: Security and good practices
- Chapter VIII: Supervision
- Chapter IX: The National Data Protection Authority (ANPD) and the National Personal Data Protection and Privacy Board
- Chapter X: Final and transitional provisions

In a similar way to the GDPR, the LGPD does not prevent the processing of personal data in an absolute way. On the contrary, it merely requires that organizations have proper governance over the personal data being processed. Privacy is being protected by the protection of personal data.

It is important to differentiate privacy both as a "negative" and as a "positive" right. Briefly put, in the former, there is an essential individual dimension to be free from abuse, embarrassment, and physical harm. It is every person's right to be able to withdraw from public life, the right to be left alone. In its positive conception, it is the right to act, and in the context of this article, it is the right to have the data that can identify oneself. This concept is intertwined with the personal life of the individual and adds a layer of procedural aspects.

The LGPD is based on a series of principles laid down in Article 6. Most of them have a parallel with the principles of the GDPR, such as lawfulness, purpose limitation, data minimization, accuracy, integrity and confidentiality, and accountability. The two main differences are that (i) free access, which is a *principle* in the LGPD laid down in Article 6(IV) is considered a *right* in the GDPR (Article 13), and (ii) storage limitation, a *principle* in the GDPR set forth in Article 5(1)(e), is in Article 16 of the LGPD as the *obligation* to delete personal data after processing is finished. Although it might be easier to enforce a provision that commands an obligation, a *principle* must always be observed. This difference, which seems small, may imply a different kind of response to the national authority.

Being mainly based on principles, the LGPD lacks some of the specific instructions that can be found in other data protection legislation. Article 2 provides for the basis of the data protection, such as the respect for privacy; informative self-determination; freedom of expression, information, communication, and opinion; inviolability of intimacy, honor, and image; economic and technological development and innovation; free enterprise, free competition, and consumer protection; and human rights, the free development of personality, dignity, and the exercise of citizenship by natural persons.