Brazil's New Data Protection Law: An Overview and Four Key Takeaways for U.S. Companies

CYBERSECURITY AND PRIVACY | INTERNATIONAL | INTERNATIONAL: BRAZIL | INTERNATIONAL: LATIN AMERICA | APRIL 29, 2019

Steven Blickensderfer

Joseph W. Swanson

2018 was a watershed year for data privacy regulation. While Europe's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA) garnered the most attention from the public and businesses worldwide, Brazil also passed a new privacy law that makes sweeping changes to its existing data protection regime and promises to impact many businesses operating there, even those without a physical presence in Brazil.

In August 2018, Brazil passed its first comprehensive data protection regulation, the Lei Geral de Proteção de Dados (General Data Protection Law, or LGPD). Like the GDPR, the LGPD imposes new rules regarding the collection, use, processing, and storage of personal data in electronic and physical form and will affect all industries and sectors of the Brazilian economy. Before the LGPD, the data protection regulatory framework in Brazil was sector-based and primarily regulated by the country's Civil Rights Framework for the Internet (Internet Act) and Consumer Protection Code, among others. Shortly after passing the LGPD, Brazil provisionally created the Brazilian National Data Protection Authority to enforce the LGPD, and extended the compliance period to August 2020.

This article is intended to help businesses understand the LGPD and its effects by: (1) providing a general overview of the rights and obligations the LGPD creates and the scope of its application and extraterritoriality; (2) highlighting notable differences from the GDPR; and (3) presenting key takeaways for businesses in the United States that may be affected by this new regulation.

What Does the LGPD Regulate?

The LGPD regulates the collection and use of "personal data," defined broadly as information relating to an identified or identifiable natural person, in both digital and non-digital form. Unlike many other privacy laws, this definition does not include examples of "personal data." The LGPD further regulates "sensitive personal data," which is defined as data relating to racial or ethnic origin, religious belief, political opinion, union membership, philosophical or political organization, health, sexual orientation, and genetic or biometric data.

There are notable exceptions to the law's application to personal data, much like the GDPR. The LGPD generally does not apply to processing of anonymous data or personal data used for household, artistic, journalistic, academic, or national security purposes. The law also does not regulate business-to-business (B2B) information.

Whom Does the LGPD Affect?

Like the GDPR, the LGPD regulates controllers and processors of personal data. Controllers are the natural or legal entities who decide how and why to collect and process personal data. Processors are the entities who process the data according to the controller's instructions.

Much like the GDPR and the CCPA, the LGPD applies across industry sectors and has extraterritorial application. There are two main aspects to its application. The LGPD applies to any individual or organization, private or public, regardless of residency:

1. collecting or processing personal data in Brazil; or
2. intending to offer or provide goods or services to individuals in Brazil.

Thus, a business collecting or processing personal data need not be headquartered, or even have a physical presence, in Brazil for the LGPD to apply. The consequences of non-compliance with the LGPD can be just as severe as non-compliance with the GDPR. Violations of the LGPD can result in fines of up to 2 percent of the company's gross revenues derived from Brazil, or 50 million reais (approximately $13 million), per infraction.

How Does the LGPD Differ From the GDPR?

Although inspired by the GDPR, the LGPD and the GDPR differ in several notable ways. First, the LGPD includes additional legal bases for processing personal data than the GDPR, such as an additional basis related to the protection of credit. Second, with respect to the "legitimate interest" legal basis for processing, which is provided in both laws, the LGPD's standard is satisfied where the processing of personal data can be shown to support and promote the controller's activities after balancing the data subject's privacy rights. Under the GDPR, the legitimate interests of the controller cannot override the fundamental rights and freedoms of the data subject. These differences arguably make the LGPD more flexible in terms of justifying the processing of personal data when compared to the GDPR.

All organizations governed by the LGPD as controllers will also need to appoint a data protection officer, absent future clarifications from the Brazilian National Data Protection Authority. This differs from the GPDR, which only requires a data protection officer in certain circumstances. Data protection officers do not need to be natural persons, meaning companies can serve in that capacity, and it is unclear whether they need to reside in Brazil. The appointment of a data protection officer may be a new and unexpected expense for some companies, particularly those in the United States without a presence in Brazil or the EU. The LGPD, however, does not require the designation of a representative in Brazil in the same way the GDPR requires one for United States businesses offering goods and services in the EU.

It is also uncertain whether the LGPD will require data processing agreements between the collectors and processors, as is required by GDPR Article 28. There is no functional equivalent of GDPR Article 28 in Brazil's new law. Nevertheless, it is recommended to implement a data processing agreement so that the parties fully understand their respective responsibilities with respect to the collection, use, and protection of personal data, and if there is ever an incident involving personal data. This is particularly true under the LGPD, where liability is joint and several absent an agreement limiting a processor's liability.

Additionally, when it comes to reporting data breaches to the data protection authority, the LGPD requires reporting within a "reasonable time." This is considered less rigid than the GDPR's 72-hour deadline.

Key Takeaways

There are four key takeaways for U.S.-based businesses evaluating whether, and to what extent, the LGPD affects their business.

1. The LGPD, like the GDPR and the CCPA, applies extraterritorially, meaning it impacts businesses that do not necessarily have a physical presence in Brazil. The key questions in determining whether the LGPD applies to a U.S.-based business are: (1) whether any data collection or processing activities occur in Brazil; and (2) whether the business intends to offer or provide goods or services to individuals in Brazil. If a business satisfies either factor, then all of the LGPD's provisions apply.
2. The LGPD, again like the GDPR and the CCPA, does not apply to non-personal data, such as B2B data. A good first step for any business asking whether these data protection laws apply is to conduct a data-mapping analysis to understand the different types of data flowing into the business from inception through the end of the data's life cycle. A proper data map requires input from the business's data-driven departments, such as marketing and human resources.
3. It is important to remember that the LGPD, like the GDPR and the CCPA, is technology-blind and does not hinge on whether personal data is in hard copy or digital form. These statutes are intended to apply for years to come, regardless of the changes in technology. This is already proving to be a challenge for industry-altering forms of technology, such as artificial intelligence and blockchain technologies. Businesses should keep this in mind when determining whether and to what extent these laws apply to their data collection and processing activities, and when determining whether to engage in new products and services.
4. A business that has implemented measures to comply with the GDPR and the CCPA can use many of the same measures to comply with the LGPD. For example, the mechanisms through which a business responds to subject access requests (SARs) are largely the same. Moreover, while the LGPD does not specify that data processing agreements are required, entering into such agreements will aid in demonstrating compliance and protecting your business's interests.

Questions?

Businesses have until August 2020 (in the event the provisional measure is ratified) to come into compliance with the LGPD. And many of the actions companies are taking to demonstrate compliance with the GDPR can be used to demonstrate compliance with the LGPD. If you have questions about the LGPD and whether it applies to your business or compliance, please contact the authors of this article.