Brazilian Government Makes the LGPD Effective Imminently

Article By

Aaron K. Tantleff  
Stephanie Pierce  
Steven Millendorf

Foley & Lardner LLP

Related Practices & Jurisdictions

- Administrative & Regulatory  
- Communications, Media & Internet  
- Global  
- Election Law / Legislative News  
- Brazil

Thursday, September 10, 2020

On August 14, 2018, the Brazilian government approved the Brazilian General Data Protection Law, known as the Lei Geral de Proteção de Dados Pessoais (“LGPD”). Enforcement was set to begin on August 15, 2020 but then, due to COVID-19 was delayed until May 2021. Later, the delay was shortened to December 31, 2020, but eventually overturned by the Brazilian Senate, reverting to the original enforcement date resulting in the LGPD coming into effect very soon. Notwithstanding the immediacy of the LGPD, penalties and sanctions for non-compliance provided therein will not be enforced until August 1, 2021.

LGPD in a Nutshell
• Extraterritorial scope – applies to organizations in Brazil as well as organizations that process personal data for the purpose of offering or supplying goods and services to individuals in Brazil.

• Relatively broad definition of personal data, but with significant exclusions.

• Companies must appoint a DPO to be within the “channel of communication” between the financial controller, the data subjects, and regulators.

• Must have at least one of 10 lawful bases for processing.

• Parental consent required when processing personal data of a child under 12. Processing of personal data for children under 18 must be in their best interest.

• Detailed guidance for the use of consent as a lawful basis for processing.

• Data subjects have the right to request information about the data the company collects about them and what will happen if they do not grant consent to the controller in order to process their personal data.

• Data breach notification to regulators within a reasonable period of time.

• Exports of personal data from Brazil only permitted if level of protection can still be maintained, including through adequacy decisions, binding corporate rules, codes of conduct, or consent.

• Individuals have the right to be informed of the nature of the processing of their personal data. Individuals also have the right to access, correct, delete, anonymize, and to obtain a portable copy of their personal data.

• Significant fines for violations – up to 2% of revenue in Brazil, capped at R$ 50MM per violation (roughly US$9.4MM as of September 10, 2020).

With Brazil representing almost half of all IT spend in Latin America, the largest market for software outsourcing in Latin America, a sizeable workforce providing outsourced software and services, and manufacturing products like commercial airplanes and cars, many U.S. companies operate in Brazil, directly, or indirectly through joint ventures, affiliates, or outsourcing. Whether the personal data remains in Brazil or is exported back to the U.S., companies should be aware of the requirements of the LGPD. The LGPD, like the EU’s General Data Protection Regulation (“GDPR”) is extraterritorial in scope. The LGPD applies to any company, public or private, that processes personal data in Brazil, collects or processes the personal data of individuals in Brazil, or processes data for the purpose of offering or supplying goods or services in Brazil. This means that it applies to any company located within Brazil, as well as those outside of Brazil that process personal data of individuals residing in Brazil or otherwise marketing goods or services to people in Brazil. Accordingly, any company located in or marketing goods or services to individuals in Brazil should be aware of the LGPD and consider whether any immediate action on becoming compliant with the LGPD is appropriate.

For companies that undertook efforts to comply with the GDPR, they will find several similarities between the LGPD and the GDPR, though there are several differences
between the two that are worth noting.

Requirements of the LGPD

Companies are required to appoint a data protection officer (“DPO”) to be the “channel of communication” between the financial controller, the data subjects (e.g., employees) and the National Data Privacy Agency (“ANPD”), the data protection authority created by Presidential’s executive order. This individual is responsible for overseeing compliance efforts, as well as training, for an organization. The name and contact information of the DPO must be clearly posted on the company’s website. (Art. 41.)

Lawful Bases For Processing Personal Data under LGPD

- upon owners’ consent;
- in order to comply with a legal or regulatory obligation by the controller;
- under some circumstances, by the public administration for the implementation of public policies;
- by survey organizations provided that the individualization of the personal data shall be prevented;
- if necessary for the performance of a contract or preliminary proceedings related to a contract to which the owner is a party, upon the owner’s request;
- for the enforceability of rights in lawsuits, administrative proceedings or arbitration;
- for the protection of the owner’s or third party’s life and physical capability;
- for health care, exclusively, by health care physicians, health care providers and sanitary authorities;
- whenever it is necessary to serve legitimate interests of the controller and third parties, except when fundamental owner’s rights for data protection prevail; or
- for credit protection, including as provided in the specific legislation.

The LGPD defines personal data relatively broadly, in that under the LGPD, personal data is any information that is related to an identified or identifiable individual. (Art. 5, 1.) Like GDPR, this includes information that could be used to identify an individual, even if the information does not facially do so. While the LGPD takes a slightly broader approach to defining personal data, there are a greater number of categories of data that are excluded from compliance under the LGPD. Publicly available information and personal data that is processed by a natural person and used exclusively for private non-economic reasons, for journalistic, artistic, or academic purposes, or used exclusively for public security, national defense, and data processed for state security or criminal investigations or prosecution are all
exempt under the LGPD. (Art. 4.) The LGPD does define a subset of personal data as “sensitive data” as personal data that relates to one’s racial or ethnic origin, religious and political views, union, religion, philosophical or political affiliations, health, sexual, or biometric or genetic data.” This sensitive data is afforded higher protections and only a subset of the lawful bases may be used to process sensitive data.

The ability of a company to process personal data, like the GDPR, requires a lawful basis for processing. The LGPD contains the same 6 lawful basis of processing as the GDPR, but also includes four additional lawful basis for processing: for the protection of life or physical safety; the protection of health in procedures conducted by health professionals or health entities (including certain sensitive personal data); as necessary for pharmaceutical care and health care in relation to data portability and transactions benefiting data subjects; or as required to protect credit. (Art. 7, I-X.).

Although the EDPB and the WP29 have provided significant guidance over the years regarding the permissibility of consent under the GDPR, the LGPD itself provides significant restrictions on the use of consent as a lawful basis for processing. Under the LGPD, consent is defined as “voluntary, informed and unquestionable manifestation under which the owner of the data agrees to its personal data processing for a specific purpose.” (Art. 5, XII.) The LGPD goes further to require that consent must be either in writing or by any other means that demonstrate the manifestation of consent by the individual with the rules described in the callout box below.

**Consent Requirements under the LGPD**

- If the consent is in writing, it shall be highlighted among the other contractual provisions.
- Burden of proof that consent was manifested in accordance with the LGPD rests on the controller.
- Manifestation of consent under duress is strictly forbidden.
- Consent shall be manifested upon specific purpose and general consent for personal data processing shall be deemed null and void.
- Consent shall be revoked at any time upon express manifestation from the owner at no cost and personal data processing before such express manifestation remain valid.
- In the event of any change on the information subject to the manifestation of consent, the controller shall notify the owner and the owner may revoke its consent in case it disagrees with the changes.

The LGPD also imposes significant technical and administrative security obligations on businesses to protect personal data from unauthorized access and accidental or illegal destruction, loss, alteration, communication, or dissemination, and minimum requirements may be imposed by the ANPD. However, unlike the GDPR, the LGPD
provides a more lenient notification requirement in the event of a data breach. Data breach notifications to the ANPD and affected individuals under the LGPD must be given within a reasonable period of time, which is to be defined by the ANPD, whereas under the GDPR, notifications of a data breach are to be provided to the supervisory authorities within 72 hours. (Art 48.)

The LGPD also provides individuals with certain rights regarding the processing of their personal data. Besides the right to be informed of the processing of their personal data through privacy notices with certain minimum content, individuals also have the right, subject to certain conditions, to access, correct, obtain a portable copy of, anonymize, and delete their personal data. Both the GDPR and the LGPD provide individuals with the right to request information about the data that is collected from them. However, the LGPD also provides an individual with the right to request information about what will happen if the individual does not grant consent to the controller in order to process their personal data.

A company may export personal data to another country where such foreign country or organization provides adequate level of data protection or provides assurance of data protection through contractual clauses, Binding Corporate Rules (BCRs), or regularly issues codes of conduct certifications and seals. Personal data may also be exported where the data subject explicitly consents or there such export is necessary for international cooperation with intelligence, investigative, and prosecutorial agencies. (Art. 33.) It is not clear whether the ANPD will take a strict or a liberal view towards exports to the United States in light of the concerns raised in the Schrems II decision in the European Union.

The LGPD also differs from the GDPR with respect to the processing of personal data of a minor, which, under Brazilian law defines a child as anyone below the age of 12 and an adolescent as one between the age of 12 and 18. For a child, consent must be obtained from the child’s parents or guardians. One must make a reasonable effort to verify that the consent was given by the child’s parent or guardian. With respect to the processing of any personal data of a child or adolescent, any such processing must be in their best interest and any information about the processing must be provided in a simple, clear, and accessible manner. (Art. 14.)

Like the GDPR, violations of the LGPD are potentially subject to rather significant fines. A violation of the LGPD can result in administrative sanctions, which include, warnings, fines up to two percent (2%) of a company’s revenue for the preceding fiscal year in Brazil, capped at BRL 50 million per violation. Unlike the GDPR, the calculation of the fine is based upon revenues in Brazil and not on a global basis. A company may also be subject to having their name, along with the nature of the violation, published, as well as blocking or deleting access to the personal data used in violation of the LGPD. (Art. 52).

Impacts to Businesses

Although penalties and sanctions for non-compliance with the LGPD will not be enforced until August 1, 2021, organizations that were already subject to GDPR should review their privacy policies and procedures and revise them as necessary for the LGPD. All other organizations that were not previously subject to GDPR but are
subject to the LGPD should immediately adapt to it. These may include the following:

- a data mapping and data governance exercise to understand what personal data processing activities (if any) the business performs that may be subject to the LGPD;

- identifying any gaps where the business’ processing activities do not currently comply with the requirements of the LGPD and developing a remediation plan;

- revising (or creating) any policies and procedures for compliance with the LGPD, including any policies and procedures related to complying with requests from individuals exercising their rights;

- reviewing applicable processing activities to ensure that there is at least one lawful basis for each processing;

- appointing a DPO;

- revising and adopting or reviewing the businesses’ incident response policies to ensure that they can comply with their breach notification obligations.

Businesses should also pay close attention to any processing that involves an export of personal data from Brazil and begin to put appropriate measures in place to ensure continued protection for such personal data.

© 2021 Foley & Lardner LLP

National Law Review, Volume X, Number 254

Source URL: https://www.natlawreview.com/article/brazilian-government-makes-lgpd-effective-imminently