The Brazilian Data Protection Law—LGPD

August 20, 2018

Last week, Brazil enacted its long-awaited Data Protection Law (Law 13,709/2018), known as Lei Geral de Proteção de Dados or LGPD. The LGPD was inspired by and is similar to the EU General Data Protection Regulation (GDPR).

Does the LGPD Apply to My Company? The LGPD applies to all processing of personal data by private entities, individuals and the government, if (1) the data is collected or processed in Brazil or (2) the processing is for the purpose of offering or providing goods or services in Brazil. The LGPD does not apply to data processed exclusively for an individual's personal use, for artistic, journalistic or academic work, or for the purpose of national security.

Debevoise & Plimpton

The LGPD applies, of course, to companies present and operating in Brazil. Similarly to the GDPR, the LGPD also explicitly aims to have extraterritorial reach: Article 3 makes the LGPD applicable to companies "irrespective of . . . the country in which [an entity's] headquarters is located or the country where the data are located," if the data processing happens in Brazil, if the purpose of the processing is to offer or provide goods or services in Brazil or if the data being processed is collected in Brazil. It remains to be seen how Brazilian authorities would seek to enforce the LGPD against a company outside the country.

The new law affects companies in all sectors doing business in or with Brazil. Financial, technology, healthcare, insurance, airline and hotel companies are among those that will likely face substantial compliance obligations. Companies not operating directly in Brazil also may be impacted, for example if receiving data from businesses operating in Brazil. Companies both inside and outside Brazil will need to consider, among other things, whether to require their contractual counterparties to comply with the LGPD.

What Data Is Covered by the LGPD? The LGPD defines personal data broadly as "information related to an identified or identifiable individual." The term "identifiable" broadens the LGPD's scope beyond information that explicitly identifies an individual. Like the GDPR and the new California Consumer Privacy Act (CCPA), the LGPD aims to reach information that could be used to identify a person even if the information on its face does not do so.

Also akin to the GDPR and CCPA, the LGPD defines a subset of personal data as "sensitive data" and provides special protections for it. Sensitive data is "personal data related to one's racial or ethnic origin, religious and political views, union, religious, philosophical or political affiliations, health, sexual, biometric or genetic data."

Principles and Legal Bases for Processing. Similarly to the GDPR, the LGPD sets out general principles that must underpin all processing of personal data, and then builds on those principles by identifying specific legal bases that can be relied on to support particular acts of data processing.

The ten general principles applicable to all data processing are spelled out in Article 6. A key principle is purpose limitation—*i.e.*, all processing must be "for legitimate, specific and explicit purposes of which the data subject is informed." The principle of necessity likewise requires "limitation of the processing to the minimum necessary to achieve its purposes." Other key principles include free access and transparency to the data subject, and data quality—*i.e.*, the "accuracy, clarity, relevance and updating" of the personal data. The "accountability" principle requires demonstrating the adoption of effective measures to ensure protection of personal data.

Importantly, while the LGPD focuses mostly on data *privacy*, the principles also impose substantive data *security* requirements: companies must adopt "technical and administrative measures to protect personal data from unauthorized access and accidental or illegal destruction, loss, alteration, communication or dissemination."

The ten legal bases available to support particular acts of data processing are set out in Article 7. For companies, the key bases include:

- Consent, when clearly manifested—if in writing, "highlighted so as to stand out from other contractual clauses"—and where based on a clear disclosure of the "particular purposes" of the processing;
- Fulfillment of legal, regulatory or contractual obligations; and
- For "the legitimate interests of the controller or a third party," where those interests outweigh, on balance, the data subject's rights and liberties.

Every act of processing must comply with *all* of the Article 6 principles and *at least one* of the Article 7 bases.

What Obligations Does the LGPD Impose on Companies? Among other things, the LGPD requires that companies:

- Inform, correct, anonymize, delete or provide a copy of the data if requested by the data subject;
- Delete data after the relevant relationship terminates, unless expressly permitted to retain the data;
- As noted, adopt technical and administrative data security measures to protect personal data from unauthorized access, accidents, destruction, loss and alteration;
- Appoint a data protection officer responsible for receiving complaints and communications, and for providing orientation within the company on best practices; and
- Notify the data subjects and Brazilian authorities following a data breach.

Penalties and Liability. Similarly to the GDPR, the LGPD establishes separate obligations and liabilities for data controllers (companies that control the data and decide how it will be used) and for data processors (companies, such as cloud storage, marketing or analytics firms, that handle data on behalf of the controllers). In part because the LGPD's language differentiating processors and controllers is not the same as the language in the GDPR, and in part because additional regulation is likely to be forthcoming, it remains to be seen how the LGPD will govern interactions between controllers and processors.

Under the LGPD, violations are subject to penalties ranging from warnings to fines up to 2% of the company's or economic group's gross revenue in Brazil in the previous year, limited to R$ 50 million per violation (approximately 12.7 million USD at the time of writing). Note that the penalty is calculated on Brazilian revenue only, not global revenue as under the GDPR.

The Brazilian legislative process allows the president to approve legislation while vetoing specific parts of it. When approving the LGPD, President Temer vetoed provisions in the legislation that would have allowed for partial or total suspension of violators' permission to process data and broader prohibitions of violators' activities.

President Temer also vetoed the provision that would have created an independent National Data Protection Authority. But he stated that he would send a bill to the Congress providing for a new data protection authority on similar terms. That new agency, if created, presumably will issue further guidance on the LGPD. Until a

regulatory agency is created, it is uncertain how the enforcement of the LGPD will be carried out. Local commentators have noted that a presidential bill creating an enforcement agency would likely pass.

Cross-Border Transfers. With the LGPD, Brazil joins the European Union and many other jurisdictions (but not the United States) that limit the transfer of personal data outside their borders. The default rule, under Article 33 of the LGPD, is that such transfer is prohibited, absent certain enumerated exceptions.

The LGPD's enumerated transfer mechanisms closely resemble those available under the GDPR. Cross-border data transfers out of Brazil are permitted, for example:

- Where the receiving country or organization provides a level of data protection comparable to the LGPD's (although no designations of comparability have yet been made, the EU presumably would be deemed comparable in light of the GDPR);
- The non-Brazilian data importer is bound by contract (either bespoke, or "standard contractual clauses") or by global corporate policy to provide and demonstrate a level of data protection comparable to the LGPD's;
- For international legal cooperation between government agencies; and
- Where the data subject has given specific consent to the transfer, "distinct from other purposes."

COMPARISON CHART: LGPD, CCPA AND GDPR

LGPD	CCPA	GDPR
Covers processing of data by individuals and entities, in or out of Brazil, provided that either the data is collected or processed in Brazil or processing is for the purpose of offering or providing goods or services in Brazil.	Covers only for-profit entities meeting one of three threshold criteria: $25 million in revenue, 50,000 California consumers or more than half of revenue generated from personal data sales.	Covers processing of personal data by all entities (for-profit or nonprofit) with an "establishment" in the European Union, or entities outside of the European Union that offer goods and services to individuals in the European Union or trace their data.

LGPD	CCPA	GDPR
Defines "personal data" broadly to include information related to an identified or identifiable individual. Publicly available information is included in the definition, but with limitations allowing for use consistent with the purposes for which the information was made public.	Defines "personal information" broadly to include categories of data that directly or indirectly identify a person. Publicly available information is excluded.	Defines "personal data" broadly to include categories of data that directly or indirectly identify a person. Publicly available information is included.
Third-party vendors reviewing documents are bound to the same principles as the entity requesting the data treatment.	Third-party vendor agreements may include a statutorily defined set of commitments to establish an exemption from the CCPA's general provisions.	Third-party vendor agreements must contain a standard set of EU-approved commitments.
Grants consumers the right to be informed of, access, correct, obtain a portable copy of, anonymize and delete their personal data.	Grants consumers the right to be informed of, access and (in more limited circumstances) delete or obtain a portable copy of their personal data.	Grants consumers the right to be informed of, access, correct and (in more limited circumstances) delete, restrict processing of or obtain a portable copy of their personal data.
Requires entities to have a lawful basis for processing information if not seeking subjects' consent.	Grants consumers the right to opt out of the sale of their personal information.	Requires entities to have a lawful basis for processing information if not seeking subjects' consent.

What Should Companies Do Now? The LGPD will come into force in February 2020, giving companies 18 months to get ready. In that time, appropriate steps might include the following, as to which counsel can be helpful:

- A diligence process to identify what personal data processing activities, if any, the company is engaged in (including via vendors) that are covered by the LGPD;
- A gap analysis to identify where any of these data processing activities do not satisfy the LGPD's requirements;
- A remediation process to close any identified gaps;
- Revision (or creation), implementation and testing of any internal policies and procedures needed to comply with the LGPD, including for responding to data subject requests for access, correction and deletion; and
- Revision or creation of appropriate vendor agreements.

Companies and their counsel that have gone through exercises like these in connection with the GDPR, or have them underway for the CCPA, should find that experience on point for the LGPD.

* * *

We are available to discuss the LGPD with our clients and friends.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Maurizio Levi-Minzi
mleviminzi@debevoise.com

Andrew M. Levine
amlevine@debevoise.com

Dietmar W. Prager
dwprager@debevoise.com

Will Bucher
wwbucher@debevoise.com

Fabio Rawet Heilberg
frheilberg@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

LONDON

Jane Shvets
jshvets@debevoise.com

FRANKFURT

Dr. Thomas Schürrle
tschuerrle@debevoise.com