CARLTON FIELDS

Brazil’s LGPD: What You Need to Know Before 2021

October 29, 2020

Overlooked in a year dominated by a "wait-and-see" dynamic with both the finalization and enforcement of the California Consumer Privacy Act (CCPA), Brazil's General Data Protection Law-Lei Geral de Proteção de Dados (LGPD)-is another major privacy compliance obligation that must be undertaken for 2021.

The following are some key points that compliance teams should evaluate when integrating LGPD requirements into their larger privacy compliance infrastructure.

What is the LGPD's effective date?

The law took immediate effect on September 18, 2020. Brazil's data protection authority, Autoridade Nacional de Proteção de Dados (ANPD), will oversee enforcement of the law.

How is "personal data" defined?

Personal data is defined quite ambiguously and broadly under the LGPD: "any information related to an identified or identifiable natural person."

What rights do consumers have under the law?

1. Notice. Like the CCPA and GDPR, the consumer has been given a right under Article 9 of the LGPD to meaningful notice, which includes notification on matters such as the specific purposes of the processing, the type and time period of processing, the identity of the processing entity and contact information, the nature and purpose of any data shared with third parties, the responsibilities of the entity processing the data, and information regarding the consumer's rights.

2. Right to Know. Under Article 18, the consumer is given a series of rights akin to the GDPR. The first of these rights, the right to know, addresses businesses having a distinct responsibility to provide information to the consumer about what data, if any, is being processed by the entity.

3. Right to Correct. Consumers have the right to correct inaccurate information.

4. Data Portability. Consumers have the right to a copy of their data to port from a data processing system.

5. Data Deletion. Consumers have a right to have their data deleted, subject to certain exceptions.

6. Consent. Much like the GDPR, consent must be express, informed, and clear. Consumers must be given information about what giving their express consent means as well as the consequences of denying or revoking consent to the processing of their personal data.

What is additionally required of businesses?

1. Data Protection Impact Assessments. If your business has not engaged in data mapping and conducted a Data Privacy Impact Assessment, the LGPD is the latest data protection law to make this a distinct requirement.

2. Appointing a Data Protection Officer. This is a must for businesses that need to comply with the LGPD.

What are distinctions that businesses may overlook as compared with the GDPR?

Three key areas should be focused on when parsing distinctions between the LGPD and the GDPR: 1) Legal basis for processing data; 2) Response periods to data subject access requests; and 3) Response periods for data breach notifications.

Legal Basis for Processing Data

The LGPD adds additional legal bases for the processing of personal data. The following list provides the six legal bases that businesses may be with familiar with due to GDPR compliance and highlights the four additional legal bases for processing set forth under the LGPD.

- Explicit consent
- Contractual necessity
- Legitimate interests
- Legal obligations
- Vital interest
- Public interest
- **Studies by research entities**
- **Exercise of rights in legal proceedings**
- **Health protection**
- **Protection of financial credit**

Time Frame for Response to Consumer Requests

The LGPD provides for a tighter window of time from the receipt of a data subject access request to when a response to the data subject is required. The table below highlights these differences.

Requirement	LGPD	GDPR
Time Frame for Response to Consumer/Data Subject	15 days	30 days
Administrative Fees for Response to Requests	Must be provided free of charge	Must be provided free of charge (with an exception related to burdensome requests)

Time Frame for Data Breach Notifications and Consumer Obligations

The LGPD, much like U.S. state-level data breach notification laws, has a consumer notice requirement, unlike the GDPR. The table below highlights key differences.

Requirement	LGPD	GDPR
Time Frame for Notice to Regulator	Reasonable amount of time	Notify EDPA within 72 hours
Notice to Consumers/Data Subjects	Yes	Dependent on circumstances

What are the penalties for non-compliance?

Like the GDPR, there are distinct penalties that are enumerated for violations of the LGPD. Penalties can include:

1. Fines. 2% of a private legal entity's, group's, or conglomerate's revenue in Brazil, for the prior fiscal year, excluding taxes, up to a total maximum of 50 million reais.
2. Corrective Actions That Can Be Taken by the ANPD. In addition to fines, the following corrective actions also can be taken by the ANPD:
    1. Issuing a warning and providing a cure period
    2. Publicizing the data violation
    3. Blocking or deleting processing activities or personal data related to the LGPD violation, which may equivocate to an effective surrender of that personal data entirely for the business
    4. Suspension of databases, which could mean up to a six-month period where the data related to the LGPD violation cannot be used by the business
3. Civil Action. Consumers also can seek civil remedies for violations of the LGPD.

Punchline: You can't hide from data privacy laws-the globalization of consumer privacy rights

The LGPD is just the latest regulation to become effective with a laundry list of compliance obligations for businesses. Canada is currently seeking to upgrade its privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), and earlier this year Australia announced plans to upgrade its privacy law, the 1988 Privacy Act. These laws reflect a global trend in moving toward frameworks that parallel the GDPR and CCPA, and will create distinct compliance obligations.

It is important to adjust your compliance framework as these laws are in development, and certainly once implemented.

Related Practices

Cybersecurity and Privacy
International