Brazil's General Data Protection Law Turns Five

17.09.2025 3 min read

Authors

Felipe Palhares

Fernanda Villela

Related areas

Data Privacy and Cybersecurity

Topics

BMA Review GDPR

On September 18, 2025, Brazil's General Data Protection Law (LGPD – *Lei Geral de Proteção de Dados Pessoais*) will have been in force for five years. If a song could capture how the legislation has been interpreted over that time, it might well be David Bowie's Changes: in the first five years, the LGPD has undergone significant shifts in its interpretation and application by the National Data Protection Authority (ANPD – *Autoridade Nacional de Proteção de Dados)*.

Five developments stand out because of the impact they have on the privacy programs of any type of organization:

1. Data Protection Officer (DPO)

The ANPD's Regulation on the role of the Data Protection Officer (Encarregado) clarified expectations for the position and introduced new requirements not found in the LGPD.

In addition to appointing a primary DPO, organizations must designate a substitute to cover absences, vacancies, and other cases when the primary DPO is unable to act. The identities of both DPOs must be disclosed in privacy policies/notices, and both must be fluent in Portuguese. Before appointing their primary and substitute DPOs, organizations are expected to assess potential conflicts of interest that could interfere with the performance of their role.

2. Security Incident Reporting

In April 2024, the ANPD issued its Security Incident Reporting Regulation, setting out the requirements for notifying both the Authority and affected data subjects. Organizations must report incidents within three business days of becoming aware of them.

The regulation also establishes criteria for data controllers to assess whether an incident poses a material risk or harm to the data subjects, and introduces new documentation requirements, including the obligation to maintain a record of all security incidents over the past five years.

3. International Data Transfers

Organizations that transfer personal data outside Brazil must comply with the ANPD's Regulation on International Data Transfers, published in August 2024.

One important requirement under the regulation is that privacy policies/notices must include a dedicated section on international transfers, clearly identifying the destination countries. In addition, transfers must be based on a valid legal mechanism, such as the standard contractual clauses approved by the ANPD.

4. Legal Bases for Processing

The LGPD does not explicitly require organizations to inform data subjects of the legal bases used to justify data processing. Article 9, for example, does not list legal bases among the mandatory disclosures in privacy notices.

Even so, the ANPD has taken the position that this information should be provided. It may therefore be worth revisiting your privacy notice to include the legal basis for each processing activity, aligning your practices with the Authority's expectations.

5. Data Protection Impact Assessments (DPIAs)

Although the ANPD has not yet issued formal rules specifying when DPIAs are mandatory, a recent statement by the Authority suggests that a report should be prepared whenever a processing activity presents a high risk to data subjects' rights.

According to the ANPD, the principles of prevention, security, and accountability are sufficient to justify requiring a DPIA, even in the absence of specific regulation.

The developments of the past five years make it clear that LGPD compliance isn't a race with a finish line – it's an ongoing process. As the regulatory landscape continues to evolve, organizations will need to treat privacy governance as a continuous effort, adapting policies and practices to stay aligned with the ANPD's expectations.

>>> This content is part of BMA Review #88. Click here for more.

› PROFESSIONALS

Professionals who combine legal insight and market perspective

Felipe Palhares

Fernanda Villela